Revista de Investigación "Pensamiento Matemático"
Universidad Politécnica de Madrid
ISSN 2174-0410 Volumen III, Número 1, Abril 2013

G.I.E Pensamient Matemátic

MAIC

EXPERIENCIAS DOCENTES

LA WEB, LAS APLICACIONES DE LAS MATEMÁTICAS Y LAS METODOLOGÍAS ACTIVAS: UNA PROPUESTA PARA EL AULA

COMPETENCIAS EN LÍMITES: ESQUEMAS CONCEPTUALES Y RESOLUCIÓN DE EJERCICIOS

DISEÑAR UNA OBRA EN ARQUITECTURA DESDE UN PUNTO DE VISTA MATEMÁTICO

HISTORIAS DE MATEMÁTICAS

CRIPTOLOGÍA NAZI. LOS CÓDIGOS SECRETOS DE HITLER

LAS "LECCIONES ACADÉMICAS" DE EVANGELISTA TORRICELLI

JUEGOS MATEMÁTICOS

UN JUEGO COMPETITIVO BASADO EN UN PROBLEMA MATEMÁTICO

INVESTIGACIÓN

NNTEX: A TOOLBOX TO USE THE NEURAL NETWORKS IN AN EASY WAY

CREACIÓN DE ESCULTURAS INSPIRADAS EN EL ANÁLISIS MATEMÁTICO DE LA OBRA DE JAUME ESPÍ

MATEMÁTICAS DE SOCIEDAD Y SÍNDROMES SOCIALES

MATEMÁTICAS EN LA CONSTRUCCIÓN DE ESCALAS MUSICALES

CRÍTICAS

TTOETAS, POESÍA CON MATEMÁTICAS

CUENTOS MATEMÁTICOS

DE CLAVOS Y OTROS SERES

ENTREVISTA A:

CARLOS ÓSCAR SORZANO: ENTRE LA INVESTIGACIÓN Y LA DOCENCIA

Revista Pensamiento Matemático

ISSN - 2174 - 0410

Volumen III, Número 1, Abril 2013

Grupo de Innovación Educativa Pensamiento Matemático y
Grupo de Investigación Matemática Aplicada a la Ingeniería Civil

Producción / GIE Pensamiento Matemático y GI MAIC
Diseño de portada y Maquetación / José Manuel Sánchez Muñoz

Universidad Politécnica de Madrid

$$\frac{\pi}{2} = \sum_{k=0}^{\infty} \frac{k!}{(2k+1)!!} = \sum_{k=0}^{\infty} \frac{2^k k!^2}{(2k+1)!}$$
$$= 1 + \frac{1}{3}\left(1 + \frac{2}{5}\left(1 + \frac{3}{7}(1 + \cdots)\right)\right)$$

Revista Pensamiento Matemático

Grupo de Innovación Educativa Pensamiento Matemático

y

Grupo de Investigación Matemática Aplicada a la Ingeniería Civil

Universidad Politécnica de Madrid

Volumen III, Número 1, ISSN 2174-0410

1 de abril de 2013

$$\pi = 6\arcsin\frac{1}{2} = 3\sum_{k=0}^{\infty}\frac{\binom{2k}{k}}{16^k(2k+1)}$$
$$= 6\left(\frac{1}{2^1\cdot 1} + \left(\frac{1}{2}\right)\frac{1}{2^3\cdot 3} + \left(\frac{1\cdot 3}{2\cdot 4}\right)\frac{1}{2^5\cdot 5} + \left(\frac{1\cdot 3\cdot 5}{2\cdot 4\cdot 6}\right)\frac{1}{2^7\cdot 7} + \cdots\right)$$
$$= 3 + \frac{1}{8} + \frac{9}{640} + \frac{15}{7168} + \frac{35}{98304} + \frac{189}{2883584} + \frac{693}{54525952} + \frac{429}{167772169} + \cdots$$

Índice de Artículos

Editorial del Número 1 (Vol. III)

Equipo Editorial

Revista de Investigación

Volumen III, Número 1, pp. 001–008, ISSN 2174-0410
Recepción: 27 Mar'13; Aceptación: 28 Mar'13

1 de abril de 2013

Resumen

Presentamos en este nuevo número de la Revista Pensamiento Matemático varios artículos que destacan la relevancia de las matemáticas en campos tan dispares como la pedagogía educativa, la arquitectura o la escultura, la criptología, la topografía, las ciencias sociales, la música, las estrategias colaborativas en la teoría de juegos o incluso la poesía.

Abstract

In this new issue of the Mathematical Thinking Journal, we present several articles which focus on the relevance of maths in different fields like educational pedagogy, arquitecture or sculpture, criptology, topography, social sciences, music, collaborative estratagies in theory of games or even poetry.

Introducción

Cuando algunos de los que formamos parte del Equipo Editorial nos "enrolamos" en este proyecto, lo hicimos con la intención de crear una publicación seria, de calidad, que a medio plazo se convirtiera en un referente. Llevamos la mitad del camino recorrido y a todas luces empezamos a vislumbrar la consecución de parte de los objetivos que nos habíamos marcado. Con este nuevo número continuamos nuestra particular cruzada y publicamos el tercer volumen, es decir emprendemos la marcha del tercer año de la publicación. Estos dos últimos años han estado llenos de enriquecedor trabajo, ilusión y constancia. Pudiéramos pensar que nuestra revista comienza a afianzarse, lo cual no deja de ser cierto, pero nosotros preferimos pensar que nos queda un largo camino por recorrer para que el público considere que PM es suficientemente digna de su atención. Afortunadamente, y a pesar de los momentos difíciles que nos toca vivir, resultan numerosas las comunicaciones de lectores felicitándonos y animándonos a continuar en esta línea de trabajo, que lejos de hacernos considerar que ya tenemos todo hecho, nos hace tener la obligación moral de esforzarnos aún más y ratificar el compromiso que adquirimos con nuestros lectores, si cabe la posibilidad, con mayor confianza y fe en este proyecto. Nuestros artículos comienzan a ser referenciados en otras publicaciones, investigaciones y trabajos, lo cual debiera significar a todas luces que los contenidos de la revista son de interés para la comunidad educativa y el público en general. Nos complace comprobar además, que los cambios introducidos en anteriores números han servido para aumentar la calidad de nuestra publicación, y por ende que el número de lectores aumenta progresivamente.

Vivimos momentos delicados para la subsistencia e integridad del sistema educativo universal tal y como fue concebido en el pasado y debiera ser planificado en el futuro. La reducción

de los gastos y los recortes indiscriminados le suponen al sistema educativo auténticas dificultades para mantener la viabilidad de multitud de proyectos de investigación e innovación, y por supuesto nuestro grupo no es una excepción. 300.000 de nuestros mejores licenciados han tenido que marchar al extranjero en busca de mejores posibilidades, lo cual significa una descapitalización de nuestros recursos humanos y un lastre para nuestra capacidad de crecimiento y desarrollo. Nuestros dirigentes consideran que todo ello debe ser suplido exclusivamente con mayor trabajo, esfuerzo, dedicación y menor cantidad de recursos humanos y materiales. Aunque la herida en nuestro sistema ya está abierta y está intentando ser suturada con puntadas más o menos torpes, deseamos poder mirar a nuestro futuro inmediato con cierta perspectiva optimista, aquello que se dice de "ver el vaso medio lleno y no medio vacío", y esperar que el daño causado pueda ser reparable.

Esta revista es un ejemplo de perseverancia a pesar de todas las dificultades con las que diariamente nos enfrentamos. Como cualquier proyecto educativo, necesita cierto mecenazgo que asegure el respaldo suficiente para poder subsistir como tal. Si existe un momento idóneo para apostar por este tipo de proyectos, ése debe ser ahora mismo. Ojalá este respaldo llegue más pronto que tarde.

Volumen III, Número 1 - Pensamiento Matemático.

Experiencias Docentes

Premio del concurso.

Con el objetivo de implicar a los estudiantes en su aprendizaje y de que relacionen los contenidos que se imparten en las clases de matemáticas, en *"La web, las aplicaciones de las Matemáticas y las metodologías activas: Una propuesta para el aula"*, se explica el proceso de como se ha creado una pequeña práctica de aula en primero de Ingeniería Civil de la Universidad Politécnica de Valencia. En la tarea, los estudiantes investigan en grupo las aplicaciones de las cónicas y las cuádricas a través de la red. Posteriormente eligen varias aplicaciones y elaboran una pequeña presentación que comparten con el resto de grupos. Finalmente realizan la evaluación de la tarea, que ha sido una responsabilidad compartida entre el

profesor y los grupos y se ha organizado en forma de concurso con un premio para el mejor. En el artículo se muestra la descripción detallada del proceso, los resultados obtenidos, el grado de satisfacción de los alumnos y del docente, los problemas que surgieron y las propuestas de mejora.

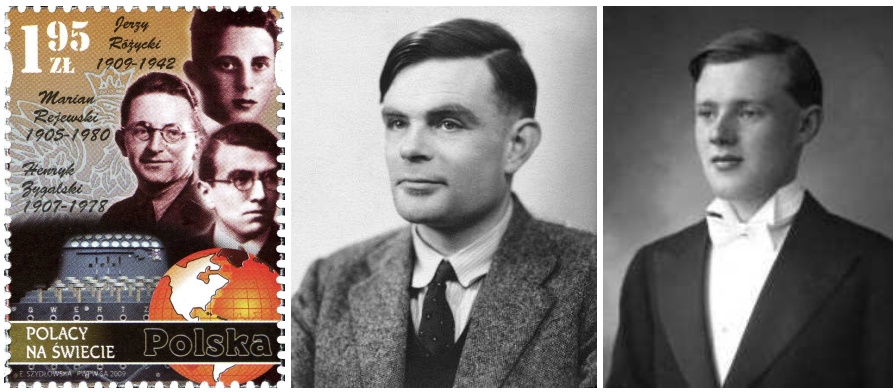
En *"Competencias en límites: esquemas conceptuales y resolución de ejercicios"*, se considera, por un lado la capacidad de los alumnos de primero de Bachillerato (16-17-años) para la resolución de ejercicios de límites y, por otro lado las nociones que dichos alumnos han adquirido acerca de los límites en la unidad didáctica de límites y continuidad. Para ello se realiza un cuestionario a dos grupos de alumnos y se analizan las respuestas obtenidas.

El artículo *"Diseñar una obra en arquitectura desde un punto de vista matemático"*, trata de poner de manifiesto la casi omnipresencia de las matemáticas en muchos aspectos de la arquitectura. La presencia más obvia es su uso como herramienta en cálculo de estructuras, instalaciones, etc. Quizás la vertiente menos explotada es su presencia en el diseño de espacios arquitectónicos y este es precisamente el tema en el que centramos la comunicación que presentamos. Los autores del artículo presentan de forma muy acertada la utilización de software a priori puramente matemático para el diseño de nuevas obras arquitectónicas, siendo dichas propuestas una mezcla de imaginación y conocimientos técnicos.

Renderizado final del Partenón con la intervención planteada.

Historias de Matemáticas

En *"Criptología Nazi. Los Códigos Secretos de Hitler"*, se lleva a cabo un repaso básico de la evolución histórica de los códigos secretos más notables utilizados hasta la 2ª Guerra Mundial, y a continuación se trata la importancia de la desencriptación de los Códigos Enigma y Lorenz alemanes por parte de los aliados gracias al trabajo analítico de multitud de matemáticos, cuyo resultado fue vital para la derrota de los nazis en la 2ª Guerra Mundial, acortando ésta al menos en dos años. Este es el segundo, y esperemos que no el último, de la saga que centra su tema de interés son por supuesto las matemáticas, pero con el conflicto bélico anteriormente



De izq. a drcha., Miembros del BS4 polaco, Alan Turing y Bill Tutte.

mencionado como telón de fondo.

"Las "Lecciones Académicas" de Evangelista Torricelli", trata la forma en que Torricelli a la manera divulgativa dibujó un boceto de bastantes de sus ideas científicas, algunas novedosas, como la circulación general de la atmósfera. El estilo culto e irónico, pero informal, que utilizó le permitió exponer conceptos que de otra manera, dadas las circunstancias, hubiera sido casi imposible. En estas notas muestro algunos ejemplos.

Portada de las "Lezioni accademiche" publicadas póstumamente en 1715.

Cuentos Matemáticos

A través de *"De clavos y otros seres"*, el lector se pone en contacto con el mundo de la Topografía y más concretamente con La Red Española de Nivelación de Alta Precisión (REDNAP). Se trata de un cuento fantástico en el que autor, lector y elementos topográficos dialogan.

Los "protagonistas": el clavo viejo, el nodo, el nuevo y la "chica" (señal secundaria).

Investigación

En *"NNtex: A toolbox to use the Neural Networks in an easy way"*, se presenta NNtex, una toolbox para Matlab desarrollada para trabajar con redes neuronales de una manera sencilla y óptima. Con NNtex, los usuarios pueden procesar y calcular resultados a través de operaciones simples además de obtener salidas que incluyen tablas y figuras. Al mismo tiempo, mediante la elección automática del algoritmo, los modelos utilizan menos memoria y tiene un funcionamiento rápido, computacionalmente hablando, esto permite el trabajo con bases de datos grandes. NNtex puede ser usada en cualquier disciplina científica y ser utilizado por personal científico o técnico de forma sencilla.

"Creación de esculturas inspiradas en el análisis matemático de la obra de Jaume Espí" hace un estudio matemático de alguna de las obras del escultor Jaume Espí donde se pone de manifiesto la relación tan estrecha que existe en algunos casos entre matemáticas y escultura. En este trabajo los autores también presentan dos obras escultóricas de manufactura propia, en cuya concepción y diseño ha sido fundamental el uso de matemáticas.

Izquierda: Clarobscur I. Medidas b 170 × 170 × h 480 mm. Central: Babel. Medidas b 170 × 170 × h 680 mm. Derecha: Pedra de toc 4. Medidas b 20 × 20 × h 50 mm.

En *"Matemáticas de Sociedad y Síndromes Sociales"*, se trata una situación de interacción social en que cada individuo está afectado por las decisiones de los demás hay dos cuestiones fundamentales: qué es lo previsible que suceda, y qué es lo deseable. Cuando la conducta de los individuos responde a sus propios incentivos y el resultado previsible es indeseable socialmente se produce un síndrome social. La teoría de juegos –las matemáticas de sociedad– ha proporcionado el armazón teórico para esas cuestiones. Aquí se presentan algunos sencillos ejemplos que se producen en situaciones cotidianas y sirven de paradigma de otras patologías sociales.

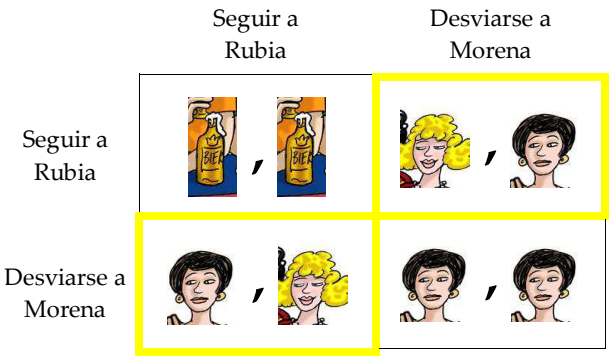


Tabla del gallina.

En *"Matemáticas en la construcción de escalas musicales"* se dan algunas pinceladas matemáticas sobre la determinación de las notas de la escala y la noción de consonancia de notas simultáneas.

"Teorica Musice", cap. 8, Libro I, de Franchinus Gaffurius (Milán, 1492). La imagen mostrada es muy representativa del fuerte dogmatismo aritmético pitagórico presente aún en la música del siglo XV.

Juegos Matemáticos

En *"Un juego competitivo basado en un problema matemático"*, se presenta un problema propuesto en la competición matemática IMC como ejemplo de reto matemático combinado con un juego competitivo entre dos agentes.

Críticas

En *"πoetas, poesía con matemáticas"*, se repasan las relaciones que se han dado en la historia entre matemáticas y poesía y se recoge la obra de autores vivos y en español que siguen y acrecen esa tradición.

Entrevistas

En esta sección conocemos a Carlos Oscar Sorzano, investigador del CSIC (Consejo Superior de Investigaciones Científicas), donde coordina el centro de procesamiento de imágenes. Además es profesor de la Escuela Politécnica Superior de la Universidad San Pablo CEU donde coordina el nuevo grado de Ingeniería Biomédica. Dedica así su vida profesional a la investigación más puntera y a la docencia universitaria. Hablamos con él para cambiar impresiones sobre estos dos aspectos.

Nos gustaría finalizar la presentación de este nuevo número agradeciendo a todos vosotros lectores vuestra fidelidad y consideración hacia nuestra joven publicación. Del mismo modo desde aquí os queremos hacer llegar nuestros mejores deseos para que entre todos rememos en una única dirección y podamos dejar atrás cuanto antes nuestra particular travesía por el desierto.

"Sin crisis no hay desafíos, sin desafíos la vida es una rutina, una lenta agonía. Sin crisis no hay méritos."

Albert Einstein

"El hombre se descubre cuando se mide contra un obstáculo."

Antoine de Saint-Exupery

"En esta vida hay que morir varias veces para después renacer. Y las crisis, aunque atemorizan, nos sirven para cancelar una época e inaugurar otra."

Eugenio Trías

¡Mucho ánimo a todos y hasta la próxima!

El Comité Editorial

Experiencias Docentes

La web, las aplicaciones de las Matemáticas y las metodologías activas: Una propuesta para el aula

The net, Mathematics applications and active metodologies: A proposal for the classroom

María José Pérez Peñalver, Cristina Jordán Lluch
y Esther Sanabria Codesal

Revista de Investigación

Volumen III, Número 1, pp. 009–018, ISSN 2174-0410
Recepción: 10 Oct'12; Aceptación: 1 Feb'13

1 de abril de 2013

Resumen

Con el objetivo de implicar a los estudiantes en su aprendizaje y de que relacionen los contenidos que se imparten en las clases de matemáticas, se ha creado una pequeña práctica de aula en primero de Ingeniería Civil de la Universidad Politécnica de Valencia. En la tarea, los estudiantes investigan en grupo las aplicaciones de las cónicas y las cuádricas a través de la red. Posteriormente eligen varias aplicaciones y elaboran una pequeña presentación que comparten con el resto de grupos. Finalmente realizan la evaluación de la tarea, que ha sido una responsabilidad compartida entre el profesor y los grupos y se ha organizado en forma de concurso con un premio para el mejor. En el artículo se muestra la descripción detallada del proceso, los resultados obtenidos, el grado de satisfacción de los alumnos y del docente, los problemas que surgieron y las propuestas de mejora.

Palabras Clave: web, webquest, metodologías activas, aplicaciones matemáticas, trabajo en grupo, evaluación compartida.

Abstract

With the aim to involve students in their learning process so that they can identify the need for the contents of our Mathematical lectures, we have designed a short practical classroom task in the first course of the Civil Engineering degree at the Universidad Politécnica de Valencia. The students have to do a research in small groups about the applications of conics and quadrics through web. After that task, they must choose several applications and elaborate a small presentation to share with the rest of groups. The last thing they have to do is to assess the task, which has had a shared responsibility between the lecturer and the groups and it has been organised as a contest, including a prize for the best group. In this paper, we will show the detailed description of the process, the results that we have obtained, the degree of satisfaction of the students and the staff with the experience, the problems that we have detected and the proposals of improvement.

Keywords: Web, webquest, active methodologies, mathematical applications, group work, shared evaluation.

1. Introducción

Como docentes de asignaturas de matemáticas básicas en escuelas técnicas, nos sucede que muchas veces los alumnos no encuentran el sentido de los temas y cuestiones que les proponemos porque no logramos transmitirles suficientemente que tiene relación con la realidad y aplicabilidad en materias relacionadas con la ingeniería.

Muchas veces los profesores de matemáticas echamos la culpa a diferentes circunstancias. Una veces argumentamos que el tiempo muy ajustado para desarrollar medianamente los contenidos, otras veces llamamos la atención sobre que el alumno de primeros cursos no está preparado todavía para comprender ciertas aplicaciones interesantes, otras veces decimos que hacer una lista de aplicaciones no sirve de nada si no se explica medianamente y otras no queremos profundizar en un tema de otra materia porque no lo conocemos suficientemente y nos produce inseguridad.

Además de esto, es habitual que se justifiquen las aplicaciones en una clase expositiva o magistral pero no se trabajen después con el alumnado.

La asignatura en la que se aplica el caso, Métodos Matemáticos de la Ingeniería Civil, es del segundo cuatrimestre de primer curso de grado, en ella se estudian temas de Álgebra y Cálculo, y cuyas prácticas de aula se trabajan en grupos de 6 estudiantes estables durante todo el cuatrimestre.

Por lo tanto, el contexto en que se mueven los estudiantes de esta asignatura es activo y participativo. La profesora de esta asignatura pertenece al Grupo de Innovación en la Evaluación para la mejora del aprendizaje Activo (IEMA) y, junto con las coautoras de este artículo, llevan tiempo proponiendo en sus clases el trabajo colaborativo además de otras metodologías activas y estudiando los resultados ([9], [10], [12], [7]). M. A. Andreu-Andrés et. al. definen estas propuestas pedagógicas:

> *Por metodologías activas se entiende hoy en día aquellos métodos, técnicas y estrategias que utiliza el docente para convertir el proceso de enseñanza en actividades que fomenten la participación activa del estudiante y lleven al aprendizaje ([1]).*

Los objetivos que se plantean al utilizar este tipo de estrategias son principalmente mejorar las competencias transversales que demanda el mercado de trabajo y la sociedad, aumentar la motivación de los estudiantes y finalmente que los estudiantes se impliquen y se comprometan en su formación para que se produzca un aprendizaje de más alto nivel cognitivo. Como dice A. Fernandez-March en [4]:

> *Se puede afirmar que los métodos de enseñanza con participación del alumno, donde la responsabilidad del aprendizaje depende directamente de su actividad, implicación y compromiso y son más formativos que meramente informativos, generan aprendizajes más profundos, significativos y duraderos y facilitan la transferencia a contextos más heterogéneos.*

Ideas que se plasman muy bien en el cono del aprendizaje o de la experiencia de E. Dale [2], cuyo vértice representa las experiencias más pasivas y, a medida que se desciende hacia la base, las más activas y profundas:

Con estas premisas, queríamos crear una tarea en la que el alumno participara de forma activa en descubrir aplicaciones, trabajando en grupo pero dedicándole un tiempo relativamente corto de las prácticas de aula.

Algunas compañeras que imparten docencia en la escuela de arquitectura llevaban trabajando las aplicaciones de las cuádricas a la arquitectura con sus alumnos, y organizando actividades en forma de concurso y nos proporcionaron el germen de la idea sobre la que trabajar ([5], [6]).

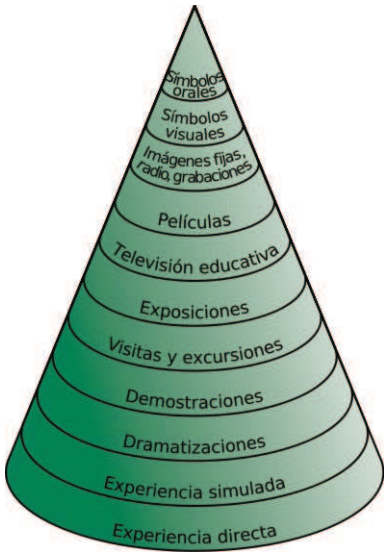


Figura 1. Cono de aprendizaje.

También conocíamos el procedimiento de la WebQuest ([13]), como la define su creador B. Dodge en [3]:

> *Una actividad de investigación en la que la información con la que interactúan los alumnos proviene total o parcialmente de recursos de Internet.*

Un procedimiento que, aunque atractivo, no nos habíamos decidido a aplicar por la imposibilidad de tener varios ordenadores en el aula habitual. Pero en la actualidad esa problemática no existe porque ya es factible pedir a nuestros alumnos que traigan al aula varios ordenadores portátiles, uno o dos por grupo de trabajo.

Con toda esta tormenta de ideas, se ha diseñado una actividad sencilla en grupo, sobre aplicaciones de las cónicas y las cuádricas, con forma de concurso, utilizando los recursos que proporciona la web y con una evaluación compartida.

2. La experiencia

El contexto es un grupo de 54 alumnos de primero del grado de Ingeniería Civil de la escuela de Ingenieros de Caminos Canales y Puertos de Valencia, que cursan la asignatura de Métodos Matemáticos de la Ingeniería Civil en el segundo cuatrimestre. Previamente ya han dado una asignatura de matemáticas en el primer cuatrimestre, Fundamentos Matemáticos de la Ingeniería Civil, previa a esta asignatura y con contenidos básicos de álgebra y cálculo (fundamentalmente funciones de una variable y espacios vectoriales). En la asignatura del segundo cuatrimestre se amplían los contenidos de álgebra (matrices simétricas y ortogonales, formas cuadráticas, cónicas y cuádricas) y de cálculo (funciones de varias variables y ecuaciones diferenciales). Los estudiantes han estudiado física en primer cuatrimestre, están estudiando mecánica en el segundo, y reciben también asignaturas matemáticas, estadística y métodos numéricos.

En este grupo, las prácticas de aula se trabajan en 9 grupos de 6 alumnos cada uno. Para cada tema el profesor propone una serie de ejercicios que se realizan en grupo y después de corregidos se comparten con toda la clase en la plataforma Poliformat de la Universitat Politècnica de València ([11]).

Para el tema de formas cuadráticas, cónicas y cuádricas la profesora pidió a los estudiantes que trajeran un ordenador portátil o dos por grupo de trabajo en el que se pudieran conectar a la red de la universidad. En la práctica de aula propuso una primera parte de ejercicios habituales de cónicas y cuádricas y una segunda parte en la que se trataba de que buscaran en la red aplicaciones de las cónicas y las cuádricas. Para motivar al alumnado se organizó en forma de concurso en el que cada grupo tenía que elaborar una presentación de máximo 25 diapositivas con las aplicaciones que les parecieran más interesantes. Después cada grupo sería juzgado por tres de los otros grupos siguiendo tres criterios:

1. Orden, claridad de la presentación e información bien referenciada.
2. Originalidad de las aplicaciones.
3. Contenido Matemático

Donde cada criterio se puntuaría con tres niveles (1=Deficiente, 2=Medio y 3=Destacado).

El premio del concurso se gestionó desde diferentes servicios de la Universidad: La escuela dio financiación 70 euros (con los que se compraron vales para hacer fotocopias) y 7 bolígrafos con el logo de la escuela, el Servicio de Medio ambiente que dio una bolsas de tela reutilizables, el vicerrectorado de Cultura facilitó libros de una exposición del ingeniero de estructuras Mamoru Kawaguchi ([8]) y el congreso INTED 2012 nos proporcionó almohadillas para ordenador. También se obtuvieron más detalles de la oficina de información y del servicio de Normalización lingüística que se utilizarán en otra ocasión.

Figura 2. Premio del concurso.

Finalmente para analizar el grado de satisfacción de la tarea se les pasó una miniencuesta con dos preguntas cerradas y dos abiertas.

3. Resultados

Todos los grupos realizaron su presentación, aunque pidieron que se aplazara la fecha límite. Esto desvirtuó un poco la idea de que fuera una pequeña tarea que no ocupara mucho tiempo. El resultado en cuanto a contenidos fue, como es natural, desigual, pero en general bastante por encima de las espectativas esperadas, es decir, que el objetivo de que investigaran por sí mismos las innumerables aplicaciones de las cónicas y las cuádricas se ha visto ampliamente cubierto.

Figura 3. Ejemplo de diapositiva.

Por otro lado, se han detectado algunos errores matemáticos, principalmente, confusiones de cuádricas con formas cuadráticas. Además prácticamente todos los grupos podrían haber referenciado mejor las fuentes, generalmente páginas web, de las que han sacado la información.

Lo que peor resultado dió fue la tarea de evaluación del resto de grupos. Primero porque no todos los grupos rellenaron la parrilla que juzgaba a tres grupos y segundo porque la sensación que se percibió es que no se lo tomaron en serio. Por ello, se tomó la determinación de descalificar a los grupos que no habían hecho esta parte de la tarea (los grupos 2, 3, 4, 5 y 6) y finalmente la profesora dictaminó el fallo del concurso: Los mejores trabajos fueron los de los grupos 9 y 1, y en ese orden.

Estudiamos a continuación los resultados de la encuesta. El primer item de la encuesta preguntaba si les había parecido interesante el trabajo y el segundo si les parecía adecuado para conocer aplicaciones de las cónicas y las cuádricas, ambas con una escala Likert de 1 a 5.

Los estadísticos descriptivos que se obtuvieron son los que aparecen en la Tabla 1.

Tabla 1. Tabla de estadísticos descriptivos.

	N	Mínimo	Máximo	Media	Desv. típ.
Pregunta 1	54	2	5	3,57	0,716
Pregunta 2	54	2	5	3,70	0,768

En los gráficos de las Figuras 4 y 5 se muestran los porcentajes obtenidos.

Podemos observar respecto a la primera pregunta, que a nadie le ha parecido nada interesante el trabajo, que un poco más de la mitad lo encuentran bastante o muy interesante y que solo un 3.7 % lo considera poco interesante.

Respecto a la segunda pregunta, la media es más alta que en la primera y casi un 60 % piensan que es adecuado para ver aplicaciones de las cónicas y las cuádricas con otras disciplinas.

También puede ser interesante analizar las respuestas por grupos, mirando los diagramas de caja representados en las Figuras 6 y 7.

Es curioso que los grupos que tienen la mediana más alta en la primera pregunta (en general a sus miembros les ha parecido bastante interesante el trabajo) son precisamente los grupos ganadores y que los grupos que les ha parecido menos interesante, el 3 y el 4, están entre los grupos que no evaluaron a sus compañeros, es decir no acabaron del todo la tarea.

Respecto a los comentarios cualitativos que formularon los alumnos, como aspectos positi-

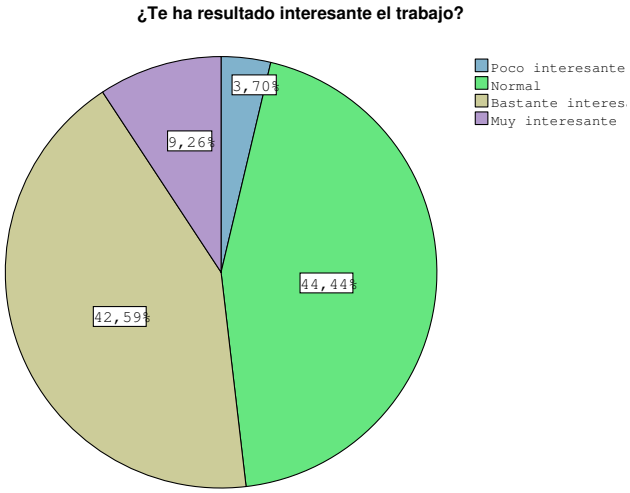


Figura 4. Porcentajes obtenidos (I).

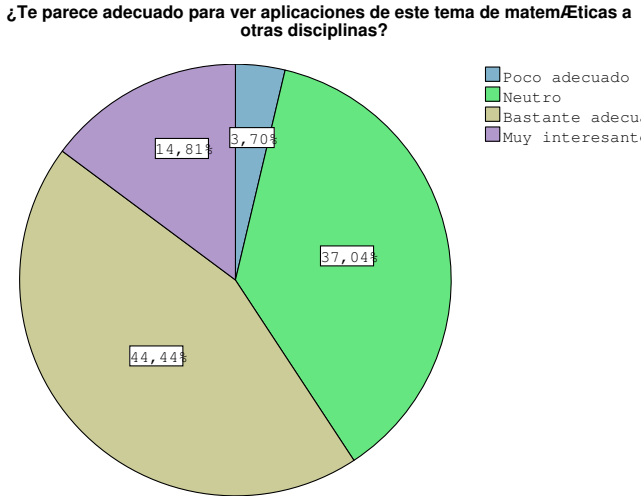


Figura 5. Porcentajes obtenidos (II).

vos citaron muchos:

- Descubrir las cientos de aplicaciones de las matemáticas
- Amplía nuestra cultura y nos acerca a nuestra profesión el día de mañana.
- Nos prepara para asignaturas en las que hay que realizar una presentación.
- Aplicar conceptos matemáticos a casos de la vida cotidiana. De esta manera te imaginas más las cosas y no son solo números.
- Hace ver las matemáticas desde otro punto de vista lo cual hace que te las tomes con más interés.
- Es una forma diferente de aprender la asignatura. Descubrir las aplicaciones de las cónicas y las cuádricas en la vida real.

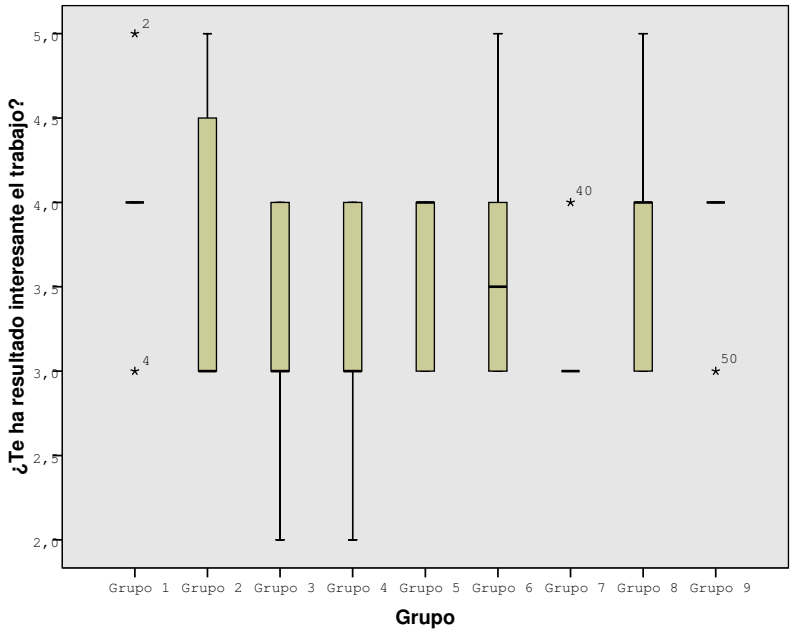


Figura 6. Diagrama de caja (I).

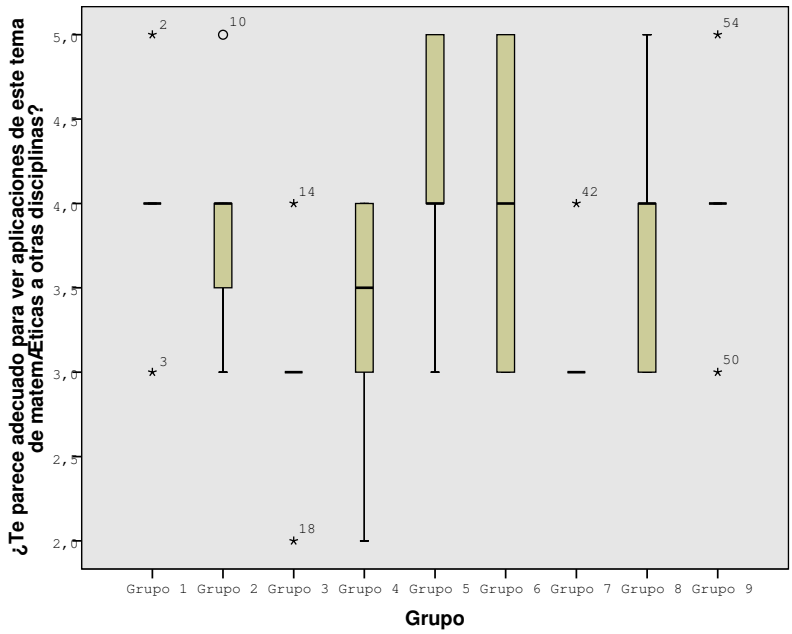


Figura 7. Diagrama de caja (II).

- Nos da una visión general y nos ayuda a comprender mejor el tema al poder ver ejemplos.
- Dedicar tiempo a buscar información sobre temas matemáticos.
- A medida que recapitulas información, te entra más curiosidad por saber y averiguar aspectos interesantes del día a día sobre las cónicas y las cuádricas que no habíamos prestado atención.
- Hemos visto la aplicación de las cuádricas y las cónicas a la realidad para ver que lo que

estudiamos sirve para algo. Nos permiten conocer edificios, estructuras y otros objetos de la realidad que se relacionan con las cuádricas y las cónicas.

- Nos ayuda a aclarar ideas y a conocer las matemáticas desde otro punto de vista.
- Colaboración, investigación personal.
- Interesarse por el tema y darse cuenta de las aplicaciones, de este modo motiva el estudio de la materia.
- Trabajar en equipo.
- Etc.

Es decir, en general, entre los aspectos positivos destacan que, con el trabajo se conectan las matemáticas con la vida real, también que les motiva y les hace más ameno el estudio de la asignatura y que al trabajar en grupo comparten ideas y se ayudan entre compañeros.

Entre los aspectos mejorables que citan los estudiantes, hablan de falta de tiempo para realizar el trabajo en clase, que tenga un porcentaje de la nota de la asignatura de nota, que haya premios para todos, objetivos más claros y que se den unas directrices más concretas.

4. Conclusiones

La primera conclusión es que se pueden realizar actividades de este tipo para motivar a los alumnos a conocer las aplicaciones de las matemáticas, y, en particular de las cónicas y las cuádricas, y que el resultado es satisfactorio tanto para los docentes como para los estudiantes. Con ello aumentamos la motivación y la participación de los alumnos y ven las matemáticas desde otra perspectiva.

Respecto al diseño concreto de la tarea se puede pensar como una tarea más larga o más corta, dependiendo del tiempo que le queramos dedicar. Si le queremos dedicar poco tiempo (1h en el aula y otra fuera) debemos poner unos objetivos más claros y unas directrices más concretas. Por ejemplo, pedirles un número concreto de aplicaciones (por ejemplo 3), reducir el número de diapositivas o que las pongan en un póster y/o concretar lo que queremos que pongan de cada aplicación. Y si se propone como una tarea más larga, se puede hacer más abierta, y se les puede pedir incluso que la expongan al resto de la clase, pero quizás en este caso, se le deba poner además un porcentaje de nota de la asignatura.

Respecto a la evaluación entre grupos, si la utilizamos, debemos diseñarla mejor, avisar que será descalificado el grupo que no judgue al resto de grupos y medir mejor los tiempos para realizarla.

Agradecimientos

El primer autor cuenta con el soporte financiero de la Unión Europea y de la Universitat Politècnica de València mediante dos proyectos: 518132-LLP-1-2011-1-FI-ERASMUS-FEXI *INCODE - Innovation Competencies Development* y el proyecto PYME A13/11 2012 *Desarrollo de rúbricas y situaciones de evaluación para competencias transversales relacionadas con la innovación*.

Referencias

[1] ANDREU-ANDRÉS, M. A. et. al. *Metodologías Activas. Grupo de Innovación en metodologías activas GIMA* en *Prólogo*, M.J. Labrador-Piquer y M. A. Andreu-Andrés, (ed.) Ed. Universidad Politècnica de Valencia, pp. 5-6 Valencia, 2008.
`http://www.upv.es/contenidos/EQIN/info/U0553826.pdf`

[2] DALE, E., *Audio-Visual Methods in Teaching*. 3rd ed., Dryden Press. Holt, Rinehart Winston, New York, 1969. (1st ed. 1946)

[3] DODGE, B., *WebQuests: a technique for Internet-based learning*. Distance Educator, Nº 1 (2): pp. 10-13, 1995.

[4] FERNÁNDEZ, A.*Metodologías activas para la formación de competencias*. Educatio siglo XXI, Nº 24: pp. 35-56, 2006.

[5] GÓMEZ-COLLADO, M. C.,SANZ-TORRÓ, F. J., TRUJILLO, M. y VICENTE-ALUJER, T. *How to relate quadrics in mathematics and architecture?*, Actas del congreso Internacional Conference on Education and New Learning Technologies. EDULEARN 09, Barcelona, 2009.

[6] GÓMEZ-COLLADO, M. C. y TRUJILLO, M. *Superficies cuádricas en la Ciudad de Valencia: modelización con DPGraph*, Actas del congreso Promotion and Innovation with new technologies in engineering education FINTDI 2011 International Conference, Teruel 2011.

[7] JORDÁN LLUCH, C., *Evaluación continua en la asignatura Estructuras Matemáticas para la Informática II*, Actas de las IX Jornadas Redes de Investigación en Docencia Universitaria, Alicante, 2011.

[8] *Mamoru Kawaguchi: ingeniero de estructuras (Catálogo de exposición)*. Sala de exposiciones de la Universidad Politècnica de València. Editorial de la Universitat Politècnica de València, Valencia, 2009.

[9] PÉREZ-PEÑALVER, M. J., *Experiencias de evaluación de trabajo en grupo en el área de matemáticas.* en *La evaluación compartida: investigación multidisciplinar*, F. Watts and A. García-Carbonell, (ed.) Ed. Universidad Politècnica de Valencia, pp. 91-107 Valencia, 2006.
`http://www.upv.es/gie/LinkedDocuments/descargarlibro.pdf`

[10] PÉREZ-PEÑALVER, M. J., AZNAR-MAS, L. E., *Peer-Assessment of groupwork to evaluate the participation: What the student think,* Actas del congreso International Conference on Engineering and Mathematics (ENMA 2011), Bilbao, 2011.

[11] POLIFORMAT.
Plataforma de la Universitat Politècnica de València.
`https://poliformat.upv.es`

[12] SANABRIA CODESAL, E., MONSERRAT DELPADILLO, F. E., *El trabajo en grupo en asignaturas de matemáticas*, Actas de las IX Jornadas Redes de Investigación en Docencia Universitaria, Alicante, 2011.

[13] WEBQUEST.
Página dedicada a las webquest: Información, repositorio y creación de webquest.,
`http://www.webquest.es/`

Sobre las autoras:

Nombre: María José Pérez Peñalver
Correo Electrónico: mjperez@mat.upv.es
Institución: Universitat Politècnica de València.

Nombre: Cristina Jordán Lluch
Correo Electrónico: cjordan@mat.upv.es
Institución: Universitat Politècnica de València.

Nombre: Esther Sanabria Codesal
Correo Electrónico: esanabri@mat.upv.es
Institución: Universitat Politècnica de València.

Experiencias Docentes

Competencias en límites: esquemas conceptuales y resolución de ejercicios

Competences in limits: conceptual frameworks and exercises solving

Daniel de la Barrera Mayoral

Revista de Investigación

Volumen III, Número 1, pp. 019–048, ISSN 2174-0410
Recepción: 07 Oct'12; Aceptación: 12 Feb'13

1 de abril de 2013

Resumen

En este documento se considera, por un lado la capacidad de los alumnos de primero de Bachillerato (16-17-años) para la resolución de ejercicios de límites y, por otro lado las nociones que dichos alumnos han adquirido acerca de los límites en la unidad didáctica de límites y continuidad. Para ello se realiza un cuestionario a dos grupos de alumnos y se analizan las respuestas obtenidas.

Palabras Clave: enseñanza de las matemáticas, análisis funcional, enseñanza secundaria, dificultad en el aprendizaje, límite, continuidad, competencia.

Abstract

In this document, it is considered, on the one hand, the skills of the students of first year of Bachillerato (16- 17 years old) in solving exercises involving limits, and in the other hand, the notions which these students have acquired in the "Limits and continuity" didactic unit. For that purpose, a questionnaire is proposed to those pupils, and the answers are analyzed.

Keywords: mathematics education, functional analysis, secondary education, learning disabilities, limit, continuity, literacy[1].

[1] El término literacy ha sido obtenido del informe PISA 2003, en el cuál se denota scientific literacy la competencia científica, y del informe PISA 2009, en el que se denota por Reading literacy a la competencia en comprensión lectora.

1. Objetivo

El objetivo de esta investigación es comprobar si existe alguna relación entre las habilidades que tienen los alumnos en el campo de la ejecución de ejercicios rutinarios y los conceptos e ideas sobre las nociones de límite puntual o en el infinito de una función (finito o infinito) y en la noción de continuidad, que deben haber adquirido en la unidad didáctica correspondiente.

Para ello me marco los siguientes objetivos concretos:

(O1) Estudiar las competencias que ha adquirido el alumnado de 1º de Bachillerato en torno a los límites y la continuidad.

(O2) Estudiar si existe alguna relación entre la capacidad de ejecución correcta de ejercicios rutinarios y la competencia, por parte del alumnado, en la comprensión de las nociones de límite y continuidad.

2. Fundamentación Teórica. Estado de la Cuestión.

El currículo de la Educación Secundaria Obligatoria (E.S.O.) del Sistema Educativo español inicia al alumnado en el estudio de los límites de una sucesión en el cuarto curso de la E.S.O ([6]) y, posteriormente en primero de Bachillerato ([7]) se estudian los límites de funciones y la continuidad de funciones. Por tanto, es un tema de gran relevancia en el modelo de educación española actual.

Las competencias básicas de la educación Secundaria Obligatoria, contempladas en la L.O.E ([9]), proporcionan un interés para conocer si el actual modelo educativo logra los objetivos de adquisición de competencias. Para el presente trabajo destaco la competencia matemática, aunque se puede también referenciar la competencia lingüística.

La competencia matemática "implica el conocimiento y manejo de los elementos matemáticos básicos" ([9]). En este trabajo no considero el concepto límite como un concepto básico; sin embargo, este concepto está integrado por esta competencia si se considera como conocimiento y manejo de elementos matemáticos. De hecho considero, de manera similar a otros autores como Tall y Blázquez que es un concepto avanzado de las Matemáticas y que conlleva muchas dificultades a los estudiantes.

A partir de los años noventa, en la didáctica de las matemáticas se comienza a considerar la problemática del aprendizaje de las matemáticas en términos de procesos cognitivos. ([1])

Se considera también para esta fundamentación la didáctica del análisis. Resulta interesante comprobar como uno de los grupos más importantes, en la actualidad, de la didáctica del análisis nació en un congreso a caballo entre psicología y didáctica de las matemáticas. Este grupo, nacido en 1985 en el seno del Psychology of Mathematics Education, consideró el estudio del llamado Pensamiento Matemático Avanzado. "En particular, tratan de profundizar en las investigaciones cognitivas acerca de los procesos de enseñanza y aprendizaje de temas relacionados con el cálculo infinitesimal ([1]). Siguiendo a autores como Azcárate y Tall, se pueden establecer dos niveles en las matemáticas. Por un lado las

matemáticas formales y los conceptos que los estudiantes (sean de un nivel educativo u otro) tienen sobre dicho concepto. En las matemáticas formales se incluyen las definiciones formales y las definiciones que cada persona tiene. En el segundo nivel, se considera la idea que se forma acerca de la definición del objeto matemático. En el presente trabajo, intentaré comprobar cómo el desarrollo de las primeras, no conllevan necesariamente el desarrollo satisfactorio de las segundas. En particular considero los objetos de límite de una función y continuidad de una función.

En el artículo de Azcárate y Camacho ([1]) traducen por esquema conceptual, la expresión original "concept image" que se utiliza para designar las ideas que los estudiantes generan a partir de las matemáticas formales.

Por otro lado Tall ([15]), propone que "el crecimiento matemático comienza con las percepciones de y acciones sobre un objeto en el entorno. El éxito en las percepciones deriva en representaciones visuo-espaciales. Las acciones sobre objetos utilizan representaciones simbólicas (que denominará procepts) que se utilizarán sobre todo en aritmética y álgebra." Estos procepts son el camino que un estudiante necesita realizar para pasar de un proceso o actividad que se puede considerar rutinaria al concepto que posteriormente utilizará para su posterior vida matemática.

En el campo concreto de la didáctica de las funciones se encuentra un interesante artículo de Tall ([14]). En dicho artículo se resumen varias investigaciones acerca de conceptos matemáticos avanzados como función, límite y demostración. Se establece además la diferencia entre las matemáticas escolares y las matemáticas universitarias.

Pone de manifiesto, además que cada generación tiene sus propios "problemas internos" que van pasando a posteriores generaciones. Ello conlleva ciertos conflictos para el alumnado, como la definición de función como objeto en el que cada x le corresponde una única y, entra en conflicto con que la ecuación $x^2 + y^2 = 1$ represente una función. En consecuencia, "cuando se confronta a un alumno por primera vez con definiciones matemáticas es", según Tall, "casi inevitable que solamente conozca un rango reducido de posibilidades que forma sus imágenes conceptuales en un modo que provocará un conflicto cognitivo en el futuro" ([14]). En estos casos se debe tratar de dar una imagen aproximada del concepto, para posteriormente ir encontrando mejores aproximaciones.

Por ello quiero comprobar si el enfoque actual consigue este objetivo de proponer una aproximación a la noción de límite y continuidad en una función.

En el mismo artículo, Tall propone las dificultades a las que se enfrenta el entendimiento del concepto de límite. Estas dificultades se mantienen en la actualidad, como se podrá comprobar a lo largo de este trabajo.

Aunque los límites aparecen de diferentes maneras en la literatura matemática, los diferentes casos (límite finito de una sucesión, límite puntual de una función, etcétera…) presentan dificultades comunes para los alumnos principiantes (p. 11, en [14]). Por ello he querido tratarlos en este trabajo como un único tipo de problemas.

En investigaciones posteriores sobre este problema, se pueden leer dos artículos de Blázquez ([3], [4]), así como su tesis doctoral ([2]). Las tres publicaciones versan sobre la

noción de límite y las diferentes concepciones que tienen los estudiantes de secundaria y bachillerato sobre los límites.

En 2000, los autores proponen primero explicar el límite de sucesiones para posteriormente pasar al límite de funciones. ([3]). En el caso de este trabajo, la población que es objeto del estudio son alumnos de primero de bachillerato, que ya conocen los límites de sucesiones, y además recientemente han sido introducidos en los límites de funciones en un punto y límites en el infinito de una función.

En 2001, los mismos autores escriben otro artículo en el que proponen a los estudiantes un cuestionario sobre límites y posteriormente realizan unas entrevistas con los alumnos. Aquí realizan la hipótesis inicial de que el concepto límite acarrea una gran cantidad de dificultades intrínsecas a la noción de límite y que por tanto son independientes de la definición que se utilice ([4]).

En el año 2000, Espinoza y Azcárate, proponen una aproximación al problema a través de la Teoría Antropológica de la didáctica ([10]). La investigación en ese artículo se centra más en lo que el profesor es capaz de hacer para facilitar la comprensión por parte de los alumnos de los límites de funciones.

Otra noción muy íntimamente ligada a la noción de límite es la noción de infinito. Respecto a esta noción se pueden encontrar los trabajos de Sabrina Garbín. En su artículo conjunto con Carmen Azcárate, presentan "algunos resultados, reflexiones y aportaciones de un trabajo de investigación que se centra en identificar las inconsistencias y representar, categorizar y analizar las situaciones de coherencia que manifiestan los alumnos en relación con sus esquemas conceptuales asociados al concepto de infinito actual." (pág. 1, [12]). Por otro lado constatan que "en las preguntas en que está implicado un proceso de infinitud, los estudiantes no siempre responden teniendo en cuenta el proceso infinito" u ofrecen una solución "evadiendo la infinitud, respondiendo de manera finita." En el presente trabajo se observa también esta actitud frente a algunas actividades de esta índole.

En el citado artículo se propone un cuestionario con preguntas acerca del infinito (de hecho algunas son similares a las que se encontrarán en este trabajo) cuyo estudio se realiza desde un punto de vista cualitativo. A continuación cada alumno puede modificar con un bolígrafo de otro color las respuestas que ha dado, o incluso rellenar las preguntas que no ha contestado, pero justificando las respuestas. Por último se realizaron algunas entrevistas a los alumnos para comprobar las conexiones que han formado a la hora de contestar las cuestiones propuestas y conocer los esquemas mentales de los alumnos.

En [11] se proponen motivos para la introducción de la geometría fractal en el currículo de educación secundaria y se propone como una de las actividades motivadoras el conjunto de Cantor. Así, se pone de manifiesto la necesidad de una mayor relación entre los distintos campos de la Matemática a la hora de presentárselos a los estudiantes en el aula.

3. Metodología

Propongo el uso de la siguiente metodología para la consecución de los objetivos citados en la sección 1 de este trabajo.

Para el objetivo (O1) se ha entregado el cuestionario que se adjunta en el apartado anexos a dos grupos de alumnos de 1º de Bachillerato para que lo completen. Uno de los grupos es del Bachillerato de Ciencias Naturales y el otro de Bachillerato de Ciencias Sociales.

La población considerada es de 60 estudiantes de Bachillerato de Ciencias (Bachillerato Ciencias de la Naturaleza) y 20 estudiantes de Bachillerato de Sociales (Bachillerato de Ciencias Sociales).

En lo sucesivo el uso de Ciencias y Sociales se referirá respectivamente al grupo de Bachillerato de Ciencias Naturales y al grupo de Bachillerato en la rama de Ciencias Sociales.

Las respuestas a las preguntas del cuestionario tendrán un carácter cualitativo, y serán clasificadas atendiendo a criterios que detallo en la sección análisis de resultados. Posteriormente en la sección 4 se puede leer un estudio de los resultados obtenidos.

Para el objetivo (O2) se entrega la hoja de ejercicios rutinarios sobre límites que se adjunta en el anexo del presente documento, para su resolución por parte del alumnado. Para el objetivo (O2) se compararán los resultados obtenidos en el cuestionario utilizado en el objetivo (O1) con los obtenidos en esta tanda de ejercicios, para constatar si existe alguna relación entre la ejecución rutinaria de ejercicios de límites y la comprensión de las nociones de límite y continuidad.

Para ello consideraré las variables cualitativas cuestionario y ejercicios. En ambos casos consideraré los siguientes grados competenciales: grado muy alto de comprensión / ejecución de ejercicios, grado alto, grado bajo, grado muy bajo. Posteriormente realizaré una comparativa de los resultados de ambas variables en cada uno de los estudiantes del grupo Naturales. Esta parte del estudio solamente se realiza con el grupo de Naturales, debido a que en el grupo de Sociales la unidad didáctica correspondiente se estudió seis meses antes de la realización de esta experiencia.

El autor del presente trabajo quiere destacar que las posibles conclusiones de esta investigación no tendrán una validez universal, debido a que se realizan con un único grupo de estudiantes y bajo unas condiciones muy particulares. Es decir, los resultados obtenidos serán difícilmente extrapolables a otros centros / grupos de alumnos sin el desarrollo de esta u otra investigación similar.

3.1 Pertinencia de las cuestiones planteadas en el cuestionario

Añado este apartado debido a que parte del alumnado consideraba que varias de las preguntas eran iguales. Dedicaré por ello un par de líneas a cada pregunta para justificar desde un punto de vista matemático – didáctico el por qué de esta aparente repetición.

En la primera pregunta (*¿Qué entiendes por límite?*) trato de obtener los posibles esquemas mentales respecto al concepto de límite. Considero muy posible que la respuesta sea muy similar a la explicación de los profesores en los diferentes grupos.

En la segunda pregunta (*¿Qué quiere decir qué* $\lim_{x\to 4} f(x) = 5$ *?*) quiero comprobar el grado de competencia a la hora de expresar verbalmente el concepto de límite puntual finito de una

función. A continuación en la tercera pregunta (*¿Qué puedes decir gráficamente de una función que cumple* $\lim_{x\to 7} f(x) = 2$ *?*) busco esa misma idea, pero en esta ocasión gráficamente.

En la cuarta (*¿Qué quiere decir qué* $\lim_{x\to 4} f(x) = \infty$ *?*) pregunta quiero ver el entendimiento de dos conceptos. Por un lado el concepto de límite puntual infinito y por otro lado el propio concepto de infinito. Con la quinta pregunta (*¿Qué puedes decir de una gráfica que cumple qué* $\lim_{x\to 4} f(x) = \infty$ *?*) pretendo comprobar el entendimiento de los mismos conceptos pero desde un punto de vista gráfico.

En las preguntas 2 y 4 se esperan respuestas que tengan que ver con sustituir valores en la función y que la solución sea un número o infinito, respectivamente. En este caso es posible que muchos estudiantes consideren el infinito como un número.

De manera análoga, la pregunta seis (*¿Qué quiere decir qué* $\lim_{x\to\infty} f(x) = 2$ *?*) pretende conocer las competencias adquiridas en torno al concepto de infinito y límite (finito) en el infinito de una función. La pregunta 7 (*¿Cómo se comporta una función que cumpla qué* $\lim_{x\to\infty} f(x) = 4$ *?*) es similar pero busco una respuesta gráfica.

He considerado importante realizar la separación entre explicación verbal y gráfica de los conceptos debido a que existen dos visiones principales: analítica y geométrica.

La pregunta 8 (*¿Qué quiere decir qué* $\lim_{x\to\infty} f(x) = \infty$ *?*) pretende conocer si el alumnado es capaz de diferenciar el caso 6 del caso en el que el límite sea infinito en el infinito.

La pregunta nueve (*¿Qué quiere decir que una función sea continua?*) trata de comprobar la capacidad para reconocer funciones continuas. Para ello se pide que definan con sus propias palabras el término continuidad de una función.

En la pregunta diez (*¿Qué podemos decir de la gráfica de una función que sea continua en* $x = x_0$ *?*) intento comprobar si entiende que una función sea continua en un punto.

En la pregunta 11 (*¿Qué condiciones debe cumplir una función para ser continua en* $x = x_0$ *?*) se pide que escriban qué condiciones teóricas cumple una función que sea continua en un punto.

En la pregunta 12 (*Representa una función que sea continua.*), se pide la representación de una gráfica continua para comprobar el grado de dificultad que los estudiantes utilizan a la hora de representar este tipo de funciones. Se espera que la mayor parte del alumnado emplee para responder a esta cuestión funciones lineales o cuadráticas, y en cualquier caso derivables.

En las preguntas 13 (*Representa una función con una discontinuidad de salto finito.*) y 14 (*Representa una función con una discontinuidad de salto infinito.*) se comprueba la competencia en la adquisición de los conceptos discontinuidad de salto finito y discontinuidad de salto infinito. Se tratará de diferenciar esta última de la discontinuidad esencial.

Las preguntas de 1 a la 14 tienen una relación directa con las competencias que los alumnos deberían haber adquirido en la realización de la unidad didáctica Límites y Continuidad.

Sin embargo, las siguientes preguntas (de la 15 a 17) tienen un grado de dificultad añadido que se detalla a continuación:

En la pregunta 15 (*¿Cuál es el límite de la siguiente sucesión: triangulo equilátero, cuadrado, pentágono regular, hexágono regular, heptágono regular,…? ¿Por qué?*) se pregunta por el posible límite de una sucesión de figuras planas regulares. Considero el círculo como "polígono regular de infinitos lados" debido a que si inscribimos los polígonos en sus respectivas circunferencias circunscritas, la forma y longitud / perímetro, se aproximan a la de la circunferencia.

La pregunta 16 (*Tomamos el intervalo* [0, 1]. *Lo dividimos en tres partes iguales, quitamos el intervalo central. En cada uno de los intervalos que tenemos repetimos la misma operación: dividimos en tres subintervalos y quitamos el central. Si repetimos indefinidamente la operación, ¿qué obtenemos?*) es una aproximación al conjunto de Cantor. Se pretende comprobar si los estudiantes tienen la capacidad de construir conjuntos a partir de sus definiciones y consiguen abstraer al límite.

El problema 17 (*Mezclamos un litro de pintura blanca con un litro de pintura azul. ¿Qué proporción de pintura blanca tendremos en la mezcla? Si añadimos, otro litro de pintura azul, ¿qué proporción de pintura blanca tendremos? Si añadimos, 40 litros más de pintura azul, ¿qué proporción de pintura blanca tendremos? Si seguimos añadiendo pintura azul, ¿a qué tiende la proporción de pintura blanca en la mezcla? ¿Habrá algún momento en el que la proporción de pintura blanca sea exactamente cero?*) trata sobre proporciones, que es un tema ampliamente estudiado a lo largo de la Educación Secundaria, y se quiere comprobar las posibles conexiones que los alumnos generan entre estos dos temas.

4. Análisis e interpretación de los resultados obtenidos

En este apartado se encuentra el análisis de los datos recogidos. El análisis se realizará de la siguiente manera. Primero un análisis de las respuestas obtenidas en el cuestionario del apartado *3. Metodología*. Después se realiza un análisis del objetivo (O1). Posteriormente del objetivo (O2).

El desarrollo de la unidad didáctica fue el siguiente: En una primera sesión se explicó de manera gráfica qué es el límite de una función. Posteriormente se explicó como calcular límites de funciones que están definidas sobre los reales y existen en el punto en que se pretende hallar el límite. Posteriormente se comenzaron a tratar los diferentes tipos de indeterminaciones y como resolverlos. En ningún momento se habló de la definición formal, ya que los estudiantes no están familiarizados con los términos para todo, existe y otros formalismos.

Además en ninguno de los casos hemos observado respuestas que incluyan expresiones como estar "suficientemente cerca".

4.1. Análisis de las respuestas del cuestionario

Como he observado anteriormente, en el grupo de Sociales ha transcurrido un tiempo de seis meses entre la unidad didáctica y la realización del cuestionario. Por ello el porcentaje de

respuestas en blanco es siempre superior al obtenido en el grupo de Naturales en las preguntas relacionadas con los límites. En las preguntas directamente relacionadas con la continuidad estas diferencias tienden a desaparecer. Además al haber transcurrido tanto tiempo, no han realizado los límites para el objetivo (O2).

En el análisis de las preguntas se siguen unas clasificaciones similares a las que dan Blázquez ([2]) y Garbín ([12], [13]).

PREGUNTA 1 (*¿Qué entiendes por límite?*).

En esta pregunta clasifico las respuestas en:

- Sin respuesta.
- Respuestas en las que aparece la expresión **acercar sin tocar** (o similares)
- Respuestas en que no aparece la expresión sin alcanzar (o similares).
- Respuestas que no tienen sentido desde el punto de vista didáctico-matemático.

Los resultados aparecen en la Tabla 1.

Tabla 1. Pregunta 1 del cuestionario.

	NATURALES	SOCIALES	TOTALES
SIN RESPUESTA	3	5	8
SIN SENTIDO	7	2	9
ACERCAR SIN TOCAR	16	4	20
APROXIMACIÓN	34	9	43

Como ya observan Blázquez ([3], [4]) y Garbín ([12]), existen diferencias entre estudiantes que hablan de "sin tocar", o los que hablan de que "la función no supera". En ambos casos solamente consideran funciones monótonas en sus argumentos.

Entre estas respuestas destaca una en la que el alumno habla de imagen de una función y de dominio. Sin embargo, este tipo de casos es muy extraño. Otra estudiante escribe ideas sobre una aproximación a un número real. Ello lleva a pensar que no tiene nada claro el concepto de límite.

Como se puede observar en la tabla 1, la mayor parte de los alumnos tiene el concepto de límite adquirido como una aproximación. Como ya destacaban en sus trabajos autores como

Blázquez, los estudiantes tienen la idea de que un límite no puede ser alcanzable ni superable, considerando solamente funciones monótonas.

PREGUNTA 2 (*¿Qué quiere decir que* $\lim_{x\to 4} f(x) = 5$ *?*).

En esta pregunta considero las siguientes categorías:

- Sin respuesta
- Respuestas parecidas a "si la x tiende a 4, la y tiende a 5" (tendencia).
- Respuestas similares a "si sustituyes la x por 4 la y te queda 5" (sustitución).
- Respuestas "tiende a, pero sin tocar" (tendencia sin contacto).
- Ejemplos de funciones que cumplen el límite (ejemplo).
- Respuesta sin sentido.

Los resultados se recogen en la Tabla 2.

Tabla 2. Pregunta 2 del cuestionario.

	NATURALES	SOCIALES	TOTALES
SIN RESPUESTA	2	5	7
SIN SENTIDO	12	3	15
TENDENCIA	17	3	20
TENDENCIA SIN CONTACTO	5	1	6
EJEMPLO	2	1	3
SUSTITUCION	22	7	29

La respuesta "tendencia" implica un mayor grado de competencia en la comprensión del concepto límite que la respuesta "sustitución" debido a que la segunda no se tiene en cuenta que la función puede no existir en el punto $x = 4$.

En esta pregunta algunos alumnos escriben una función que cumple la igualdad del enunciado como por ejemplo $f(x) = x+1$.

En el grupo de Naturales se observa como la mitad del alumnado da una respuesta con sentido, utiliza una respuesta de "tendencia" (con o sin contacto) y la otra mitad de

sustitución. Esto puede ser debido a que en la resolución de los límites el profesor lo primero que dice es que antes que nada hay que sustituir la x en la fórmula y ver si resulta un valor.

En el grupo de Sociales hay un porcentaje superior en el grupo que da una respuesta de "sustitución" respecto al grupo que da una respuesta de "tendencia".

PREGUNTA 3 (*¿Qué puedes decir gráficamente de una función que cumple* $\lim_{x\to 7} f(x) = 2$ *?*).

En esta pregunta, considero las siguientes respuestas:

- Sin respuesta.
- Representación del punto (7,2) pero ninguna función. (Punto)
- Función que pasa por el (7,2). (Función)
- Que es una función de salto finito/infinito. (Discontinuidad)
- Respuesta sin sentido, respuesta "que es continua", o respuestas no gráficas. (Sin sentido)

Las respuestas de cada tipo vienen recogidas en la Tabla 3.

Tabla 3. Pregunta 3 del cuestionario.

	NATURALES	SOCIALES	TOTALES
SIN RESPUESTA	16	11	27
PUNTO	6	1	7
FUNCIÓN	11	2	13
DISCONTINUIDAD	5	1	6
SIN SENTIDO	22	5	27

Debido al alto número de respuestas en blanco del grupo de Sociales no se puede extraer ninguna conclusión sobre este grupo.

En el grupo de Naturales se observa que la mayor parte de los estudiantes que están en la categoría "sin sentido" repiten la respuesta verbal de la pregunta 2, cambiando los datos correspondientes. Ello quiere poder decir que no tienen la competencia de representar funciones que cumplan que el límite puntual de dicha función en un punto sea un número real.

Por otro lado se observa que una porción importante del grupo Naturales responde en el grupo de discontinuidad; pero, ninguno advierte la posibilidad de que sea una discontinuidad evitable.

PREGUNTA 4 (*¿Qué quiere decir qué* $\lim_{x\to 4} f(x) = \infty$ *?*).

En esta cuestión se puede constatar cómo es un error frecuente considerar el infinito como un número más. Se han recogido respuestas bastante similares a la pregunta 2. Categorizo las respuestas de la siguiente manera:

- Sin respuesta.
- Respuestas que incluyen tiende o se aproxima. (Tendencia)
- Si la $x = 4$, entonces la $y = \infty$. (Sustitución)
- Es una indeterminación. (Indeterminación)
- No tiene límite (sin límite)
- Respuesta sin sentido. (Sin sentido)

Las respuestas de cada tipo están recogidas en la Tabla 4.

Tabla 4. Pregunta 4 del cuestionario.

	NATURALES	SOCIALES	TOTALES
SIN RESPUESTA	9	9	18
SIN SENTIDO	9	3	12
TENDENCIA	16	3	19
SUSTITUCIÓN	16	3	19
INDETERMINACIÓN	4	0	4
SIN LÍMITE	6	2	8

Destaca la respuesta de una estudiante que sí considera el infinito como "un número que no se puede alcanzar".

Como se puede observar en la tabla 4, la mayor parte del alumnado de Sociales no responde o lo hace con repuestas que no tienen sentido (puntos de corte).

En el grupo de Naturales, se tiene de nuevo la mitad de los estudiantes que consideran el límite como una mera sustitución, sin considerar que la función podría no estar definida en el punto, y la otra mitad dan respuestas de tendencia.

La mayor parte de la población identifica este límite como una indeterminación pero sin decir nada acerca de las características que pueden tener las funciones que cumplen la condición del enunciado.

PREGUNTA 5 (*¿Qué puedes decir de una gráfica que cumple qué* $\lim_{x\to 4} f(x) = \infty$ *?*).

En esta pregunta se considera como respuesta óptima la representación de una gráfica con una asíntota vertical en $x = 4$. Se clasifican las respuestas en las siguientes categorías:

- Sin respuesta.
- Respuestas verbales similares a las obtenidas en la pregunta 4 (Verbal) En este apartado incluimos respuestas como "es discontinua".
- Respuesta sin sentido. (Sin sentido)
- Respuesta gráfica correcta (Gráfica)

Las respuestas están recogidas en la Tabla 5.

Tabla 5. Pregunta 5 del cuestionario.

	NATURALES	SOCIALES	TOTALES
SIN RESPUESTA	18	11	29
SIN SENTIDO	16	6	22
VERBAL	25	1	26
GRÁFICA	1	2	3

Destaca, negativamente, el hecho de la aparición de la respuesta "es continua" en varios estudiantes del grupo de Naturales.

En el grupo de Naturales, dos estudiantes representan la gráfica de la recta $y = 4$ con un agujero en $x = 4$. Esta respuesta ha sido catalogada en la categoría sin sentido.

En esta pregunta la mayor parte del alumnado da una respuesta verbal, dejando de manifiesto que aún no se ha adquirido las competencias necesarias respecto a los límites y al infinito que son necesarias para poder resolver a esta cuestión de una manera satisfactoria.

PREGUNTA 6 (*¿Qué quiere decir qué* $\lim_{x\to\infty} f(x) = 2$ *?*).

Clasifico las respuestas en las siguientes respuestas-tipo:

- Sin respuesta.
- Respuestas que incluyen tiende o se aproxima. (Tendencia)
- Si la $x = \infty$, entonces... (Sustitución)
- Es una indeterminación. (Indeterminación)
- No tiene límite (sin límite)
- Respuesta sin sentido. (Sin sentido)

Tabla 6. Pregunta 6 del cuestionario.

	NATURALES	SOCIALES	TOTALES
SIN RESPUESTA	17	9	26
SIN SENTIDO	1	3	4
TENDENCIA	19	5	24
SUSTITUCIÓN	16	3	19
INDETERMINACIÓN	7	0	7

Una estudiante sustituye el valor ∞, pero a la vez dice que no existe. Ello demuestra inconsistencias en la adquisición del concepto límite, ya que el concepto de infinito parece estar bien adquirido debido a que reconoce que no existe.

En esta pregunta, sin embargo, se puede observar como la mayor parte del alumnado no tiene adquirido un grado de competencia suficiente en el uso del infinito, ya que una cantidad significativa del grupo utiliza expresiones como "cuando x tiende a ∞". Otra cantidad significativa trata de sustituir el valor de infinito en la función.

También reaparecen respuestas que dan a entender que los estudiantes consideran que un límite no puede ser alcanzado.

En el grupo de Sociales una estudiante parece no tener la competencia suficiente respecto a las funciones debido a que dice que una función tiene infinitos valores.

PREGUNTA 7 (*¿Cómo se comporta una función que cumpla qué* $\lim_{x\to\infty} f(x) = 4$ *?*).

En esta pregunta considero las siguientes categorías de respuestas:

- Sin respuesta.
- Respuesta verbal (Verbal)
- Respuestas sobre discontinuidades o continuidad. (Continuidad)
- Respuestas sin sentido, diferentes a las de continuidad (Sin sentido)
- Respuesta gráfica correcta (Gráfica)
- Ejemplo analítico particular.(Ejemplo)

Para ver los resultados consultar Tabla 7.

Tabla 7. Pregunta 7 del cuestionario.

	NATURALES	SOCIALES	TOTALES
SIN RESPUESTA	29	9	38
SIN SENTIDO	3	3	6
VERBAL	13	7	20
CONTINUIDAD	9	0	9
GRÁFICA	5	0	5
EJEMPLO	1	1	2

En esta pregunta la inmensa mayoría de los estudiantes deja la pregunta en blanco o da una respuesta verbal que mantiene los argumentos que se encontraban ya en respuestas anteriores.

Del grupo restante la mayor parte escribe que la función es continua / discontinua. Ello indica que tienen ciertas nociones adquiridas, pero no saben relacionarlas de una manera correcta. Es decir, saben que los límites y la continuidad están relacionados por unas "normas" que ellos no tienen interiorizadas.

Un grupo reducido da una respuesta gráfica. Es destacable que todos consideran funciones constantes o monótonas crecientes, dejando de manifiesto una vez más que los estudiantes no consideran que un límite sea superable o alcanzable.

PREGUNTA 8 (*¿Qué quiere decir qué* $\lim_{x\to\infty} f(x) = \infty$ *?*).

En esta pregunta se admiten tanto respuestas verbales como respuestas gráficas. Las respuestas son clasificadas en los siguientes tipos:

- Sin respuesta.
- Sustitución del valor en la función. (Sustitución)
- Tendencia de las variables dependiente e independiente (Tendencia)
- Ejemplo concreto (Ejemplo)
- Respuestas sin sentido (Sin sentido)

Los resultados están recogidos en la Tabla 8.

Tabla 8. Pregunta 8 del cuestionario.

	NATURALES	SOCIALES	TOTALES
SIN RESPUESTA	19	10	29
SUSTITUCIÓN	17	4	21
TENDENCIA	13	2	15
EJEMPLO	4	1	5
SIN SENTIDO	7	3	10

Se observa como la mayor parte del alumnado que contesta lo hace en términos de sustitución. Por ello se deduce que se considera el infinito como un número real al que se le pueden aplicar unas operaciones perfectamente definidas. Sin embargo, algunos estudiantes consideran que no puede existir una función que cumpla dichas condiciones.

PREGUNTA 9 (*¿Qué quiere decir que una función sea continua?*).

Casi todos los estudiantes responden que una función continua es aquélla que se puede representar sin levantar el lápiz del papel. No es de extrañar esta definición ya que es la definición que se suele dar en las aulas del primer curso de Bachillerato en cualquiera de las especialidades.

Un estudiante confundió continua con constante y respondió de manera correcta a esta última noción. Otro añadió las condiciones que debe cumplir una función para que sea continua en un punto.

Un pequeño grupo utiliza expresiones como “no se para” o “no se corta” para referirse a la continuidad.

PREGUNTA 10 (*¿Qué podemos decir de la gráfica de una función que sea continua en* $x = x_0$ *?*).

Clasifico las respuestas en las siguientes categorías (Para ver las respuestas de cada tipo consultar la Tabla 9):

- Sin respuesta.
- Es una recta (Recta).
- No se levanta el lápiz del papel en ese punto. (Particularización)
- Respuestas sin conexión aparente con el enunciado de la pregunta (Sin sentido).
- Condiciones teóricas / existencia del límite.

Tabla 9. Pregunta 10 del cuestionario.

	NATURALES	SOCIALES	TOTALES
SIN RESPUESTA	20	14	34
RECTA	6	2	8
PARTICULARIZACIÓN	11	2	13
SIN SENTIDO	14	2	16
CONDICIONES TEÓRICAS	9	0	9

Varios estudiantes responden "que es una recta". Esto denota la dificultad que tienen estos para pensar en funciones continuas que no sean polinomios de grado bajo.

Una persona responde que es continua en el origen al no estar familiarizada con la notación $x=x_0$ para denotar puntos. Por ello propongo una modificación de la pregunta para posibles repeticiones del cuestionario.

Otros identifican $x = x_0$ con un intervalo al responder que la función es continua en el intervalo.

Un estudiante de Naturales escribe la definición de derivada para responder a esta pregunta. Esta respuesta puede deberse a que en la semana que se rellenó el cuestionario, el alumnado estaba estudiando la introducción a las derivadas en clase y en dicha definición aparece un límite.

Se observa que ningún estudiante del grupo de Sociales da una respuesta con las condiciones teóricas, debido a, con casi total seguridad, que el aprendizaje no ha sido significativo; es decir, no ha dejado "huella" en el alumnado.

También se puede constatar que los estudiantes que ponen algún tipo de condición teórica en sus respuestas no escriben que la función debe valer lo mismo que el límite o no ponen que debe existir el límite.

PREGUNTA 11 (*¿Qué condiciones debe cumplir una función para ser continua en* $x = x_0$ *?*).

Clasifico las respuestas en los siguientes tipos (Para ver las respuestas de cada tipo consultar la Tabla 10):

- Sin respuesta.
- Respuestas sin conexión aparente con el enunciado de la pregunta (Sin sentido).
- Condiciones teóricas / existencia del límite.
- Repuestas en las que se entiende que los límites laterales existen y coinciden, pero no incluyen nociones acerca del valor de la función en el punto (Límites laterales).
- Respuestas en las que se tiene en cuenta el valor de la función (o la existencia de la misma) pero no se hace referencia a los límites laterales de la función en el punto (Valor de función).

Tabla 10. Pregunta 11 del cuestionario.

	NATURALES	SOCIALES	TOTALES
SIN RESPUESTA	23	12	35
SIN SENTIDO	8	4	12
CONDICIONES TEÓRICAS	12	1	13
LÍMITES LATERALES	9	1	10
VALOR DE FUNCIÓN	8	2	10

Aunque la mayor parte de los estudiantes que contestan han dado una respuesta que, en mayor o menor grado, incluyen las condiciones teóricas pedidas. En esta pregunta existen

respuestas como "que x sea igual a x_0". Por ello añadimos una modificación a la pregunta 7 en el apartado correspondiente a modificaciones del cuestionario.

En las respuestas de condiciones teóricas se encuentran dos tipos de respuestas: aquellos estudiantes que han adquirido un mayor grado de competencia en el uso de la terminología y notación en torno a los límites, utilizando términos como límites laterales y otro grupo que se expresa con frase cómo "toman el miso valor que la función".

En esta pregunta se han encontrado algunos ejemplos de funciones continuas, pero al no haber añadido un punto particular, no se ha considerado la posible categoría "ejemplo". Estas respuestas han sido consideradas en la clasificación sin sentido.

PREGUNTA 12 (*Representa una función que sea continua.*).

En esta pregunta no se ha determinado el dominio de la función. Por ello, se encuentran gráficas cuyo dominio son todos los reales, otras gráficas solamente los reales positivos.

Los 80 estudiantes representan una función continua. La inmensa mayoría representan la gráfica de un polinomio de grado menor o igual que 2. Tres de ellos representan el logaritmo neperiano. Solamente uno representa una función que no es derivable.

Se puede pensar, por tanto, que el concepto de función continua es una noción en la que resulta relativamente sencillo alcanzar un grado competencial satisfactorio.

PREGUNTA 13 (*Representa una función con una discontinuidad de salto finito.*).

En esta pregunta se encuentran los siguientes tipos de respuestas:

- Respuesta en blanco.
- Gráfica de una función con una discontinuidad de salto finito. (Salto finito).
- Gráfica de una función continua (Continua).
- Gráfica de una función con una discontinuidad evitable (Evitable)
- Grafica de una función cuyo dominio es el conjunto de los reales menos un intervalo (Intervalo)
- Gráfica de una función con una discontinuidad de salto infinito (Infinito)

Tabla 11. Pregunta 13 del cuestionario.

	NATURALES	SOCIALES	TOTALES
SIN RESPUESTA	3	0	3
SALTO FINITO	31	11	42

Tabla 11. Pregunta 13 del cuestionario (cont.).

	NATURALES	SOCIALES	TOTALES
CONTINUA	1	1	2
EVITABLE	16	0	16
INTERVALO	9	7	16
INFINITO	0	1	1

Se observa como más de la mitad del alumnado es capaz de representar una función que tenga una discontinuidad de salto finito. Sin embargo, hay un porcentaje relativamente alto que confunde este tipo de discontinuidad con las discontinuidades evitables. Existe un tercer grupo amplio que no tiene la habilidad de distinguir una discontinuidad de un intervalo en el que la función no está definida.

PREGUNTA 14 (*Representa una función con una discontinuidad de salto infinito*).

Considero las mismas categorías que en la pregunta anterior, cambiando la respuesta evitable por la esencial, que es considerar una función con una discontinuidad de tipo esencial.

Tabla 12. Pregunta 14 del cuestionario.

	NATURALES	SOCIALES	TOTALES
SIN RESPUESTA	10	5	15
SALTO FINITO	4	2	6
CONTINUA	3	0	3
ESENCIAL	0	1	1
INTERVALO	17	7	24
INFINITO	26	5	31

Se comprueba que la mitad de los estudiantes que contestan, representan, efectivamente, la gráfica de una función con una discontinuidad de salto infinito.

El estudiante que en la pregunta anterior representó una gráfica de una función con una discontinuidad de salto infinito, en esta ocasión representó una con un salto finito.

PREGUNTA 15.

Esta pregunta, al ser más compleja y abierta, recoge una mayor variedad de respuestas. Trato de clasificarlas en las siguientes categorías:

- Sin respuesta.
- El círculo /la circunferencia con explicación. (completa)
- El círculo / la circunferencia pero sin dar una explicación. (Parcial)
- Polígono de infinitos lados. (Polígono)
- "No puede haber límites de figuras geométricas" (Geométricas)
- Infinito.
- Otro tipo de respuestas (Sin sentido)
- Octógono regular.

Tabla 13. Pregunta 15 del cuestionario.

	NATURALES	SOCIALES	TOTALES
SIN RESPUESTA	16	14	30
COMPLETA	11	0	11
PARCIAL	4	0	4
POLÍGONO	3	0	3
GEOMÉTRICAS	2	0	2
INFINITO	9	0	9
SIN SENTIDO	15	2	17
OCTÓGONO	0	4	4

En este caso, se han recogido expresiones como $\lim_{x\to\infty} x$ porque hay infinitos lados, o respuestas similares. Esto se puede ver como un intento de transformar el enunciado del problema en una función real de variable real. Sin embargo, en ninguno de los casos se obtiene un resultado que se pueda considerar adecuado.

Una estudiante de Naturales ofrece la siguiente respuesta: "Un círculo, porque cuantos más lados tiene un polígono más se asemeja a éste, y un polígono de infinitos lados sería un círculo, porque los lados serían los infinitos puntos que forman el círculo". Aparte del pequeño error de confundir círculo con circunferencia, demuestra un alto grado de competencia en varios campos de las matemáticas; en particular, en los límites y en la geometría plana. Además es capaz de identificar los lados de ese "límite" con los puntos de una circunferencia.

Otro estudiante defiende que la respuesta es un círculo, ya que "llegará un momento que sean infinitos los lados de los polígonos, más o menos un círculo". En esta respuesta se encuentra de nuevo la idea de límite como una aproximación, en este caso, de figuras geométricas a otra dada.

Otro estudiante de Naturales justifica que dicho límite sería un "círculo, porque los vértices de los polígonos regulares están a la misma distancia del centro. Así que si hay infinitos lados todos los puntos de la figura equidistarán del centro, ya que los lados serían puntos al ser infinitos".

La respuesta octógono regular denota una baja competencia en la adquisición de nociones como sucesión y límite de una sucesión, ya que solamente consideran el siguiente elemento de la sucesión y le toman como límite.

PREGUNTA 16.

Esta pregunta, sin duda la más compleja para los alumnos por el grado de abstracción necesario, tiene una gran variedad de respuestas diferentes. Por tanto, presento a continuación las más interesantes desde el punto de vista del trabajo. Las partes entre comillas son las respuestas literales de los estudiantes.

RESPUESTA 1

"$\begin{cases} x < (0,1) \\ x = (0,1) \\ x > (0,1) \end{cases}$ Una función de salto infinito."

En esta respuesta existe un afán por responder la pregunta mediante la búsqueda de una función. Es evidente que esta respuesta no tiene corrección suficiente para ser una función, ya que iguala la x a un intervalo, o no da un valor a la función.

REPUESTA 2

"Intervalos muy pequeños que se acercan a cero."

En esta respuesta se observa un proceso de límite que es correcto, ya que el alumno entiende que se tienen intervalos de longitud cada vez más pequeña, pero no considera la infinitud de intervalos que tiene en cada paso del proceso.

RESPUESTA 3

"Pues, que se hace pequeño y tiende a 1 y a 0."

Esta estudiante también muestra procesos correctos, pero nuevamente no considera todos los intervalos, aunque si considera que alguno de estos se puede aproximar a 1.

RESPUESTA 4

"Infinitos intervalos divididos en los intervalos $\left[0,\frac{1}{9}\right]\cup\left[\frac{2}{9},\frac{3}{9}\right]\cup\left[\frac{6}{9},\frac{7}{9}\right]\cup\left[\frac{8}{9},1\right]$"

Este estudiante comienza el proceso y contempla que hay que seguir realizando divisiones, pero no considera que en el límite, no habrá intervalos, habrá puntos que pertenezcan o no al límite.

RESPUESTA 5

"Al final obtendremos un intervalo demasiado pequeño, de microtamaño, y habrá un momento en el que no se puedan dividir más los intervalos porque la distancia del 0 al 1 no es infinita"

Este estudiante, que cursa la optativa de dibujo técnico, considera que llegará un momento en el que los intervalos serán indivisibles. Esta visión se puede deber a que el alumno se imagina una división con regla y compás y naturalmente los útiles de dibujo no van a poder dividir intervalos muy pequeños.

RESPUESTA 6

"Quedan infinitos intervalos muy pequeños. Al final quedan puntos (de longitud cero)"

En esta ocasión, el proceso de límites se realiza de una manera correcta, al identificar los puntos como intervalos cuya longitud es cero.

RESPUESTA 7

"Se obtiene $\left[0,\frac{1}{3}\right)\cup\left(\frac{2}{3},1\right]$"

En esta respuesta solamente se considera el primer paso y se propone como solución final. Por tanto, se constata que este estudiante no ha entendido el problema como un problema en el que hay que considerar límites, si no como una sencilla operación que se realiza una única vez.

RESPUESTA 8

"Obtenemos 0. Como 0 dividido por 3 es 0 y 1 dividido entre 3 en 0.33, se aproxima a 0".

Esta estudiante solamente considera un intervalo de los dos que nos quedan en cada iteración. Por ello únicamente tendrá un punto, que efectivamente será el 0.

RESPUESTA 9

"Que se acerca al valor 0,5 cada vez más y más."

Esta estudiante considera otro problema diferente, en el que en vez de eliminar el intervalo central, se queda con el central y elimina los laterales.

RESPUESTA 10

"Que al final nos quedamos sin intervalo que dividir"

Esta estudiante considera el límite de las iteraciones como el final, lo cual nos dice que tiene un buen grado de competencia en la noción límite. Además dado que la alumna es del grupo de Sociales, en este caso es una competencia consolidada.

PREGUNTA 17.

En esta pregunta se observa que la mayor parte de las respuestas son correctas. Sin embargo, se encuentra alguna respuesta que dice que la proporción de pintura será 0 en el infinito, que nuevamente proporciona la idea de una sustitución en una función. Otras justificaciones dicen que la pintura blanca siempre estará ahí.

Por tanto, se siguen encontrando los mismos errores de entender el límite como una mera sustitución y como una cota que no se puede alcanzar.

4.2 Análisis del Objetivo (O1)

Para comprobar las competencias adquiridas, contemplo, por un lado las competencias demostradas en el cuestionario (variable cuestionario), y por otro lado en los ejercicios entregados (variable ejercicios).

En cuánto los cuestionarios considero las siguientes graduaciones:

- MUY ALTO: Más de 14 respuestas que se puedan considerar correctas desde un punto de vista matemático-didáctico.
- ALTO: Entre 9 y 13 respuestas que tengan sentido matemático didáctico.
- BAJO: Entre 6 y 8 respuestas.
- MUY BAJO: Menos de 6 respuestas.

Los datos están recogidos en la Tabla 14.

Tabla 14. Competencias en cuestionario.

GRADO DE COMPETENCIA EN CUESTIONARIO	ESTUDIANTES
MUY ALTO	4
ALTO	13

Tabla 14. Competencias en cuestionario (cont.).

GRADO DE COMPETENCIA EN CUESTIONARIO	ESTUDIANTES
BAJO	41
MUY BAJO	22

Se observa como en este caso se consideran a los 80 alumnos de la muestra, y de ellos 63 (más del 75%) tienen un grado de competencia bajo o muy bajo en los conceptos asociados a límites y continuidad.

Para la variable de los ejercicios se han considerado los siguientes grados:

- MUY ALTO: Más de 10 límites correctamente resueltos.
- ALTO: Entre 8 y 10 límites correctamente resueltos.
- BAJO: Entre 4 y 7 límites correctamente resueltos.
- MUY BAJO: Menos de 4 límites correctos.

Tabla 15. Capacidad de resolución de ejercicios rutinarios

CAPACIDAD DE RESOLUCION DE EJERCICIOS	ESTUDIANTES
MUY ALTO	37
ALTO	15
BAJO	4
MUY BAJO	4

Si se observa la tabla 15, se ve que 52 de los 60 estudiantes tienen un alto grado de competencia en la resolución mecánica de límites. Esto representa al 86% del alumnado de Naturales que ha realizado los ejercicios.

4.3. Análisis del Objetivo (O2)

Se ha considerado para este objetivo las variables y grados considerados en la sección metodología. Incluyo los datos en la tabla 16. Se recuerda al lector que para este objetivo únicamente se considera el alumnado de Naturales.

Los grados de la variable cuestionario tienen color rojo y los de la variable ejercicio tienen color verde

Tabla 16. Comparativa entre ejercicios y cuestionario

EJERCICIOS CUESTIONARIO	MUY ALTO	ALTO	BAJO	MUY BAJO	TOTALES CUESTIONARIO
MUY ALTO	2	0	0	0	2
ALTO	4	1	2	0	7
BAJO	25	12	0	2	39
MUY BAJO	6	2	2	2	12
TOTALES EJERCICIOS	37	15	4	4	60

En esta tabla se observa cómo el 86% (52 de 60) de los alumnos tienen un grado de competencia en resolución de límites alto o muy alto. Esto quiere decir que son capaces de resolver ejercicios rutinarios sin grandes dificultades. De hecho, la lista de ejercicios propuestos, son en su totalidad indeterminaciones que deben ser resueltas con métodos que el alumnado acaba de aprender.

Por otro lado el 85% de los estudiantes considerados, tienen un grado bajo o muy bajo en la adquisición del concepto límite. Si el estudio se ciñera exclusivamente a la competencia de la representación gráfica de límites, este porcentaje se vería aumentado aún más. Esta afirmación surge de la observación de las respuestas obtenidas en las preguntas 3, 5 y 7 del cuestionario de la sección 7 de este documento.

Por ello se puede decir que, efectivamente, los estudiantes saben resolver límites de manera mecánica pero que no trae relacionado la correcta comprensión de las nociones relacionadas con límites.

No se puede decir que esta afirmación sea extrapolable a otros casos, pero es un punto de partida para otras investigaciones que consideren también alumnos de Naturales y no solamente alumnos de ciencias Sociales ([2]).

4.4. Mejoras para el cuestionario

En la pregunta número 1 no queda muy claro si el límite debe ser el de una función o es de una sucesión. Para trabajos acerca de límites finitos de sucesiones ver, por ejemplo, la tesis de F.J. Claros ([5]). Para el siguiente uso del cuestionario, añadir "de una función" al enunciado de esta pregunta.

Sustituir la pregunta número 3 por "Representa una función que cumpla $lím_{x\to 7} f(x) = 2$."

Hacer una sustitución en la pregunta 5 análoga a la realizada en la pregunta 3.

Sustituir la pregunta 7 por "Representa una gráfica que cumpla $lím_{x\to \infty} f(x) = 4$."

Añadir la siguiente pregunta tras la número 8: "¿Qué entiendes por x tiende al infinito?"

Modificar la pregunta 10, para que ponga en un "$x = 0$" en lugar de "$x = x_0$".

Modificar la pregunta 11 a "Enuncia las condiciones teóricas que debe satisfacer una función para ser continua en $x = 0$."

5. Conclusiones

La mayor parte del alumnado tiene una visión muy particular de los límites. Para ellos, se puede considerar que los límites son aproximaciones a un punto que es una cota inalcanzable. Además, casi siempre consideran que las funciones que se utilizan son monótonas crecientes. Ambas afirmaciones provocarían que los estudiantes no entendieran el límite de funciones como $\frac{\text{sen } x}{x}$, ya que el límite de la función en el infinito es 0, pero la función toma infinitos valores positivos y negativos para valores grandes de x.

Por otro lado, una gran parte de los estudiantes consideran los límites como meras sustituciones de un valor en una fórmula, como se puede observar en las preguntas 2, 4, 6 y 8. En las preguntas 3, 5 y 7 se puede contemplar que el alumnado no tiene, en general, un alto grado de competencia en la representación de funciones que cumplan ciertas condiciones; en este caso que el límite puntual o infinito de la función tenga un valor dado.

De las preguntas 15 y 16 se desprende que los estudiantes tienen serias dificultades para considerar los límites en otras situaciones. No es de extrañar esta situación debido a que durante la unidad didáctica todos los límites son relativos a una función y además durante la mayor parte de dicha unidad, solamente interesa resolver indeterminaciones.

En contraste, casi todo el alumnado ha logrado responder de una manera satisfactoria la última pregunta, debido a que tienen una mayor familiaridad con las proporciones en mezclas.

Se podría decir que el grado de competencia en la noción límite no es muy alto en los estudiantes considerados en este trabajo.

Sin embargo, el grado de competencia en los términos de continuidad es mayor. Casi todos son capaces de distinguir y representar los distintos tipos de discontinuidades.

En relación con el objetivo (O2) se observa que los estudiantes realizan bien los ejercicios rutinarios, pero sin adquirir los conceptos en el grado que sería deseable.

Agradecimientos

El autor quisiera agradecer al centro la Inmaculada PP. Escolapios de Getafe por brindarle la oportunidad de realizar este estudio en sus aulas. También quisiera agradecer al profesor D. Carlos de Castro Hernández por las aportaciones realizadas.

Bibliografía

[1] AZCÁRATE, C. y CAMACHO, M. (2003). Sobre la Investigación en Didáctica del Análisis Matemático. *Boletín de la Asociación Matemática Venezolana*, Vol. X, Nº 2, 135-149. Disponible en http://www.emis.de/journals/BAMV/conten/vol10/matias-carmen.pdf. Consulta realizada el 5 de Mayo de 2012.

[2] BLÁZQUEZ, S. (2000). Noción de límite en Matemáticas Aplicadas a las Ciencias Sociales. Tesis doctoral. Universidad de Valladolid. Valladolid.

[3] BLÁZQUEZ, S. y ORTEGA, T. (2000). El concepto de límite en la educación secundaria. *En* El futuro del cálculo infinitesimal. México, D.F.: Grupo Editorial Iberoamérica. Disponible en http://www4.uva.es/didamatva/investigacion/Publicaciones/concept_limite_educ_secund.pdf Consulta realizada el 5 de Mayo de 2012.

[4] BLÁZQUEZ, S. y ORTEGA, T. (2001). Rupturas en la comprensión del concepto de límite en alumnos de bachillerato. *Aula*, vol. 10, 117-133. Disponible en http://dialnet.unirioja.es/servlet/articulo?codigo=122572 Consulta realizada el 5 de Mayo de 2012

[5] CLAROS, F. J. (2010). Límite finito de una sucesión: Fenómenos que organiza; tesis doctoral. Disponible en http://documat.unirioja.es/servlet/tesis?codigo=22293 Consultado el 14de Mayo de 2012

[6] Comunidad Autónoma de Madrid. (2007). DECRETO 23/2007, de 10 de mayo, del Consejo de Gobierno, por el que se establece para la Comunidad de Madrid el currículo de la Educación Secundaria Obligatoria. B.O.C.M. Núm. 126, 48 - 139. Disponible en: http://www.madrid.org/dat_capital/loe/pdf/curriculo_secundaria_madrid.pdf. Consultado el 22 de Agosto de 2012.

[7] Comunidad Autónoma de Madrid. (2008). *DECRETO 67/2008, de 19 de junio, del Consejo de Gobierno, por el que se establece para la Comunidad de Madrid el currículo del Bachillerato.* B.O.C.M. Núm. 152, 6 - 84. Disponible en http://www.ucm.es/cont/descargas/documento32723.pdf Consultado el 22 de Agosto de 2012.

[8] CORNU, B. (1991). Limits. *En* D. Tall (ed.): Advanced Mathematical Thinking. Dordrecht: Kluwer, 153-166.

[9] España. (2006). REAL DECRETO 1631/2006, de 29 de diciembre, por el que se establecen las enseñanzas mínimas correspondientes a la Educación Secundaria Obligatoria. B.O.E. Núm. 5, 677 - 773. Disponible en http://www.boe.es/boe/dias/2007/01/05/pdfs/A00677-00773.pdf Consultado el 22 de Agosto de 2012.

[10] ESPINOZA, l. y AZCÁRATE, C. (2000). Organizaciones matemáticas y didácticas en torno al objeto "límite de función": una propuesta metodológica para el análisis. Enseñanza de las *Ciencias*, 18(3), 355-368. Disponible en http://dialnet.unirioja.es/servlet/articulo?codigo=95017 Consultado el 5 de Mayo de 2012.

[11] FIGUEIRAS, L.; MOLERO, M.; SALVADOR, A. y ZUASTI, N (2000). Una propuesta metodológica para la enseñanza de la geometría a través de los fractales. Revista SUMA. Nº 35, 45-52.

[12] GARBÍN, S. y AZCÁRATE, C. (2001). Infinito actual e inconsistencias**:** acerca de las incoherencias en los esquemas conceptuales de los alumnos de 16-17 años. Enseñanza de las Ciencias, 2002, 20 (1), 87-113. Disponible en http://ensciencias.uab.es/revistes/20-1/87-113.pdf Consultado el 5 de Mayo de 2012.

[13] GARBÍN, S. (2005). ¿Cómo piensan los alumnos entre 16 y 20 años en el infinito?,RELIME Vol. 8, No. 2 169-194. Disponible en http://dialnet.unirioja.es/servlet/articulo?codigo=2096328 Consultado el 5 de Mayo de 2012.

[14] TALL, D. (1992). The Transition to Advanced Mathematical Thinking: Functions, Limits, Infinity, and Proof, in Grouws D.A. (ed.) Handbook of Research on Mathematics Teaching and Learning, Macmillan, New York, 495-511. Disponible en http://homepages.warwick.ac.uk/staff/David.Tall/pdfs/dot1992e-trans-to-amt.pdf Consulta realizada el 3 de Mayo de 2012

[15] TALL, D. (1995). Cognitive Growth in Elementary and Advanced Mathematical Thinking. Plenary lecture, Proceedings of PME 19, Recife (Brasil). Disponible en http://digilander.libero.it/leo723/materiali/algebra/dot1995b-pme-plenary.pdf Consultado el 6 de Mayo de 2012.

6. Anexos

6.1 Cuestionario

1) ¿Qué entiendes por límite?

2) ¿Qué quiere decir qué $\lim_{x\to 4} f(x) = 5$ *?*

3) ¿Qué puedes decir gráficamente de una función que cumple $\lim_{x\to 7} f(x) = 2$ *?*

4) ¿Qué quiere decir qué $\lim_{x\to 4} f(x) = \infty$ *?*

5) ¿Qué puedes decir de una gráfica que cumple qué $\lim_{x\to 4} f(x) = \infty$ *?*

6) ¿Qué quiere decir qué $\lim_{x\to \infty} f(x) = 2$ *?*

7) ¿Cómo se comporta una función que cumpla qué $\lim_{x\to \infty} f(x) = 4$ *?*

8) ¿Qué quiere decir qué $\lim_{x\to \infty} f(x) = \infty$ *?*

9) ¿Qué quiere decir que una función sea continua?

10) ¿Qué podemos decir de la gráfica de una función que sea continua en $x = x_0$ *?*

11) ¿Qué condiciones debe cumplir una función para ser continua en $x = x_0$ *?*

12) Representa una función que sea continua.

13) Representa una función con una discontinuidad de salto finito.

14) Representa una función con una discontinuidad de salto infinito.

15) ¿Cuál es el límite de la siguiente sucesión: triangulo equilátero, cuadrado, pentágono regular, hexágono regular, heptágono regular,…? ¿Por qué?

16) Tomamos el intervalo [0, 1]. *Lo dividimos en tres partes iguales, quitamos el intervalo central. En cada uno de los intervalos que tenemos repetimos la misma operación: dividimos en tres subintervalos y quitamos el central. Si repetimos indefinidamente la operación, ¿qué obtenemos?*

17) Mezclamos un litro de pintura blanca con un litro de pintura azul. ¿Qué proporción de pintura blanca tendremos en la mezcla? Si añadimos, otro litro de pintura azul, ¿qué proporción de pintura blanca tendremos? Si añadimos, 40 litros más de pintura azul, ¿qué proporción de pintura blanca tendremos? Si seguimos añadiendo pintura azul, ¿a qué tiende la proporción de pintura blanca en la mezcla? ¿Habrá algún momento en el que la proporción de pintura blanca sea exactamente cero?

6.2 Ejercicios

A) $\lim_{x\to \infty} \left(\sqrt{x+1} - \sqrt{x}\right)$

B) $\lim_{x\to \infty} \left(\sqrt{x^2 - 3x} - \sqrt{x^2 + x}\right)$

C) $\lim_{x\to \infty} \left(\frac{x+3}{x+1}\right)^{x+5}$

D) $\lim_{x\to \infty} \left(\frac{x+1}{x+7}\right)^{x}$

E) $\lim_{x\to \infty} \left(\frac{x^2+2x+5}{x^2+3x}\right)^{\frac{x^2+3}{x+1}}$

F) $\lim_{x\to \infty} \left(\frac{x+5}{\sqrt{4x^2 - x + 2}}\right)$

G) $\lim_{x\to \infty} \left(\frac{\sqrt[3]{8x^3 - 3x^2} - 3}{2x+1}\right)$

H) $\lim_{x\to \infty} \left(\frac{x^2 - 6}{\sqrt[5]{x^{13} - x^5}}\right)$

I) $\lim_{x\to\infty}\left(\frac{1}{\sqrt{x+1}-\sqrt{x-1}}\right)$ J) $\lim_{x\to 1}\left(\frac{x-1}{x^2-2x+1}\right)$

K) $\lim_{x\to\infty}\left(\frac{x^2+3x}{x^2+3}\right)^{\frac{1}{x}}$ L) $\lim_{x\to a}\left(\frac{x^2-a^2}{\sqrt{x}-\sqrt{a}}\right)$

M) Hallar a para que $\lim_{x\to\infty}\left(\frac{ax+3}{3x}\right)=25$

Sobre el autor:
Nombre: Daniel de la Barrera Mayoral
Correo Electrónico: dbarrera@mat.ucm.es
Institución: Departamento geometría y topología. Facultad Matemáticas. Universidad Complutense de Madrid, España.

Experiencias docentes

Diseñar una obra en arquitectura desde un punto de vista matemático

Designing an architectural work from a mathematical viewpoint

M. Carmen Gómez-Collado, Jaume Puchalt, Joel Sarrió, Macarena Trujillo

Revista de Investigación

Volumen III, Número 1, pp. 049–058, ISSN 2174-0410
Recepción: 31 Ene'13; Aceptación: 25 Mar'13

1 de abril de 2013

Resumen

Las matemáticas están presentes en muchos aspectos de la arquitectura. La presencia más obvia es su uso como herramienta en cálculo de estructuras, instalaciones, etc. Quizás la vertiente menos explotada es su presencia en el diseño de espacios arquitectónicos y este es precisamente el tema en el que centramos la comunicación que presentamos.

Palabras Clave: Matemáticas, arquitectura, diseño, venustas.

Abstract

Mathematics is related to many aspects of architecture. The most obvious relationship is as a computation tool in the structures or installation analysis. However, the use of maths in the design of architectural works is not an issue as usual and just it is the topic of our study.

Keywords: Mathematics, architecture, design, venustas.

1. Introducción

Que las matemáticas han estado presentes en la vida del hombre desde que éste tiene uso de razón es algo innegable. En Occidente esta existencia tiene incluso carácter místico y trascendental con los pitagóricos en la ya temprana Grecia Clásica. Así los números cobran un valor mágico y en palabras de Pitágoras "son el origen de todas las cosas" estableciendo los cánones y proporciones de la belleza en el arte, música y arquitectura griega.

Vitrubio, arquitecto romano al que se le atribuye el primer tratado de arquitectura de la historia, recoge la triada vitruviana: firmitas, utilitas y venustas. Tres conceptos que definen aún a día de hoy los tres pilares básicos del arte de construir que es la arquitectura. De estos, el que realmente diferencia una obra de arquitectura de un edificio de ingeniería es el tercero, venustas. Este concepto hace alusión a la belleza, a las proporciones de las que ya hablaban los pitagóricos, a aquello que hace que encontremos bello o no a un edificio. Nuestro puente, el lazo de unión entre las matemáticas y la arquitectura no es otro que éste: las proporciones y relaciones matemáticas que generan placer al ojo humano, que permiten deleitarse con ellas al ser observadas.

Para nosotros, IMAE (Investigación Matemática en Arquitectura y Escultura), la hipótesis de partida es que las matemáticas y el software matemático existente son una poderosa herramienta en el análisis y diseño de obras de arquitectura y escultura, aunque en esta comunicación mostraremos únicamente el trabajo realizado en la línea de arquitectura. Fundamentalmente, la rama de las matemáticas con la que trabajamos es la geometría de curvas y superficies. No obstante, también hacemos uso proporciones matemáticas como es el caso del número de oro.

Nuestras actuaciones van en una sola dirección siguiendo el objetivo mencionado, pero en dos sentidos: 1) de las matemáticas a la arquitectura y 2) de la arquitectura a las matemáticas. En el primer sentido proponemos nuevas obras arquitectónicas a partir de conceptos, curvas y superficies matemáticas. Pretendemos poner de manifiesto las posibilidades en innovación y estética que puede tener una obra concebida puramente desde un punto de vista matemático. En el segundo sentido escogemos obras ya existentes y proponemos la incorporación de nuevas curvas, superficies y conceptos matemáticos. Así, damos una nueva visión de obras conocidas que puedan ser reinterpretadas y obras que necesiten una restauración o mejora por alguna problemática concreta.

Para la consecución de nuestro objetivo, hemos recurrido al uso de dibujos y la creación de maquetas que pensamos juegan un papel esencial como primer paso para la reinterpretación de una obra o la creación de una obra nueva. Mediante estas dos técnicas rápidas y económicas hacemos un esbozo de lo que realmente queremos cambiar o crear para pasar después al uso de programas informáticos. La importancia de una visión previa de lo que se quiere representar es que a grandes rasgos (aunque no con exactitud) permite visualizar el resultado y por tanto, aceptar o rechazar diferentes propuestas desde un primer momento sin necesidad de recurrir a técnicas más costosas de representación. Concebida la idea de la curva o superficies matemáticas que queremos utilizar es necesario representarlas mediante un software matemático que nos permita exportar posteriormente las figuras a programas más aplicados al diseño arquitectónico. El programa que vamos a utilizar es el programa de cálculo simbólico Mathematica 8.0 (Wolfram Research, Champaign, Illinois, EEUU) por sus posibilidades gráficas, potencia en los cálculos y el amplio abanico de opciones para exportar figuras a archivos con diferente extensión. Por último, las obras arquitectónicas en las que nos vamos a centrar tienen que estar representadas mediante software de carácter arquitectónico que nos posibilite la introducción de las nuevas superficies y curvas matemáticas y que nos permita ver el resultado en el diseño de la obra de esta inclusión. Hemos elegido por las posibilidades de representación que cada uno de ellos ofrece los programas 3DStudioMax, Autocad (Autodesk Inc., San Rafael, CA, EEUU) y Photoshop (Adobe Systems Inc., San Jose, CA, EEUU). A continuación hablaremos brevemente de las dos

líneas en las que hemos trabajado y explicaremos un ejemplo de los resultados conseguidos en cada una de ellas.

2. De matemáticas a arquitectura

El objetivo que perseguimos con esta línea de trabajo era diseñar una nueva obra de arquitectura con la ayuda de software matemático. ¿La invención de un nuevo diseño es puramente fruto de nuestra imaginación o resulta de la aplicación de nuestros conocimientos previos obtenidos en nuestra formación técnica? Nosotros creemos que una combinación de ambos, ya que entre ellos se retroalimentan. Y con esta idea es con la que nos hemos planteado nuestros diseños. Las obras que proponemos son una mezcla de nuestra imaginación y nuestros conocimientos técnicos.

Uno de los proyectos en los que hemos trabajado dentro de esta línea ha sido un estadio de fútbol.

2.1 El estadio

¿Por qué elegimos un estadio? Porque es un volumen muy versátil en cuyo diseño pueden plantearse diferentes superficies como es el caso de las superficies cuádricas o las de Bézier. En definitiva, en el proceso de diseño de un estadio podíamos llevar a cabo nuestro particular juego de matemáticas y arquitectura. Por otro lado, en los tiempos que vivimos el fútbol se ha convertido en un fenómeno de masas. Podríamos decir que es el "deporte de moda". Y como no, la arquitectura como reflejo de la sociedad también se ha visto salpicada por esta tendencia. De ahí que la transformación de un estadio para aumentar su aforo o el construir nuevas instalaciones para eventos futbolísticos sean parte del contenido de publicaciones recientes de arquitectura [1]-[3].

En un principio pensamos que el estadio fuera un ejemplo de volumen formado sólo por la intersección de superficies cuádricas. Así podría constituir un ejemplo de cómo combinando únicamente superficies cuádricas podría obtenerse una obra arquitectónica con cierto atractivo. Con ayuda de algunos dibujos esbozamos el diseño del estadio (Figura 1).

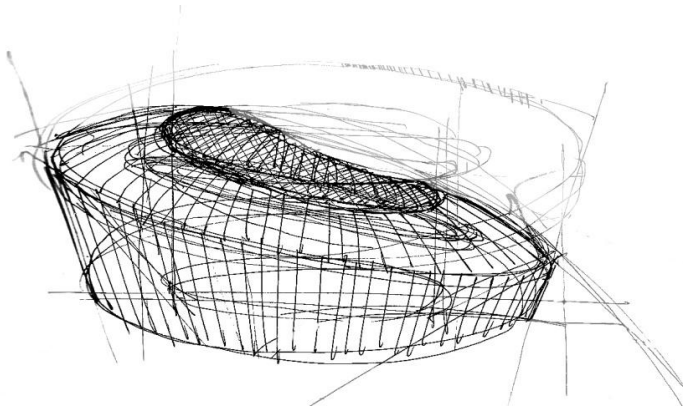


Figura 1. Primeros dibujos del estadio.

Como una primera aproximación pensamos en un volumen generado por una superficie cónica seccionada por dos planos y con una cubierta esférica intersectada por un cilindro y un plano. El centro del cono estaba situado en el eje del cilindro, pero el centro de la esfera estaba desplazado con respecto a dicho eje.

Construimos una maqueta donde reflejar parte de la idea inicial (intersección cono-esfera) para obtener una primera representación y una forma tangible con la que evaluar el diseño que se muestra en la Figura 2. Para conseguir nuestro objetivo el cono tenía que tener sección circular para que el maridaje con el casquete esférico fuese posible. Además, había un intercambio de los dos planos que seccionaban al cono con respecto a la idea inicial. Es decir, el plano que tenía que cortar al cono perpendicularmente a su eje era ahora el plano en el que se unían el casquete esférico y la base cónica. Y el plano que cortaba oblicuamente el cono tenía que ser ahora el que delimitaba inferiormente el estadio. El resultado obtenido no fue de nuestro agrado porque no reflejaba nuestra concepción inicial. El intercambio de roles de los planos que seccionaban el cono no suponía ningún problema, pero perseguíamos la idea de que la planta del estadio fuese elíptica.

Figura 2. Primera maqueta del estadio construida con corcho.

Intentando acercarnos más a nuestro planteamiento inicial jugamos con la unión de una cubierta elipsoidal y un cono de sección elíptica, pero los resultados tampoco fueron satisfactorios en tanto que no era lo que buscábamos (Figura 3).

Figura 3. Maqueta de plastilina que representa el volumen delimitado por una cubierta elipsoidal, un cono de sección elíptica y un cilindro.

Elaboramos una tercera maqueta que fuese más fiel al diseño que esbozamos en los dibujos, aunque no estuviera hecha íntegramente a partir de superficies cuádricas. Como puede observarse en la Figura 4 el lateral del estadio seguía siendo un cono seccionado en su parte inferior por un plano perpendicular a su eje longitudinal y en la parte superior por un plano oblicuo, tal y como nos planteamos inicialmente. A diferencia de las maquetas anteriores, la forma de la cubierta no respondía a ninguna superficie cuádrica concreta, aunque sí seguía seccionada por un cilindro de base elíptica. Esta maqueta sí respondía a nuestra idea inicial.

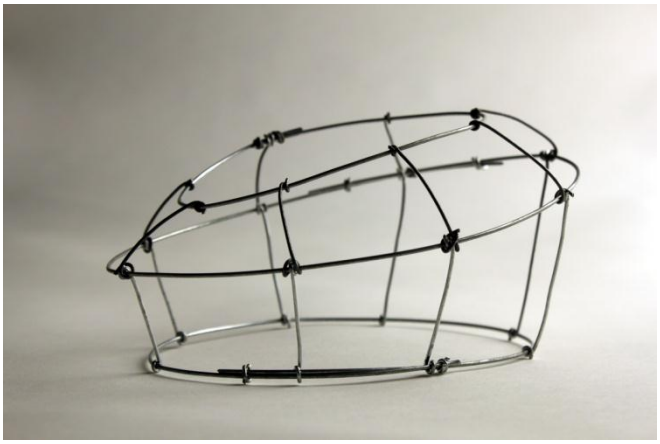


Figura 4. Maqueta definitiva del estadio hecha con alambres.

La manera de elaborar la maqueta de la Figura 4 fue nuestra guía para dibujar el estadio con Mathematica. El lateral la construimos uniendo dos elipses mediante rectas. Concretamente, utilizamos la representación paramétrica de las elipses y las rectas que las unen y el comando ParametricPlot3D de Mathematica para dibujar la superficie resultante. La cubierta la construimos también a partir de la unión de dos elipses, pero en este caso, unidas por superficies cuadráticas de Bèzier. De nuevo utilizamos el comando ParametricPlot3D para representarla. La naturaleza de las superficies de Bèzier hace necesario construir una curva auxiliar. Jugando con el tipo y la posición de la curva auxiliar obtuvimos diferentes tipos de cubiertas. En la Figura 5 se recoge una de ellas.

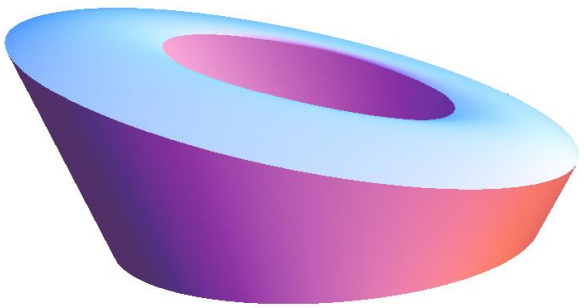


Figura 5: Estadio hecho con Mathematica.

Para la imagen final del estadio se optó por una vista de pájaro a media altura en la que poder distinguir sin problemas la base formada por un cono y el encuentro con la cubierta, formada a partir de superficies de Bèzier.

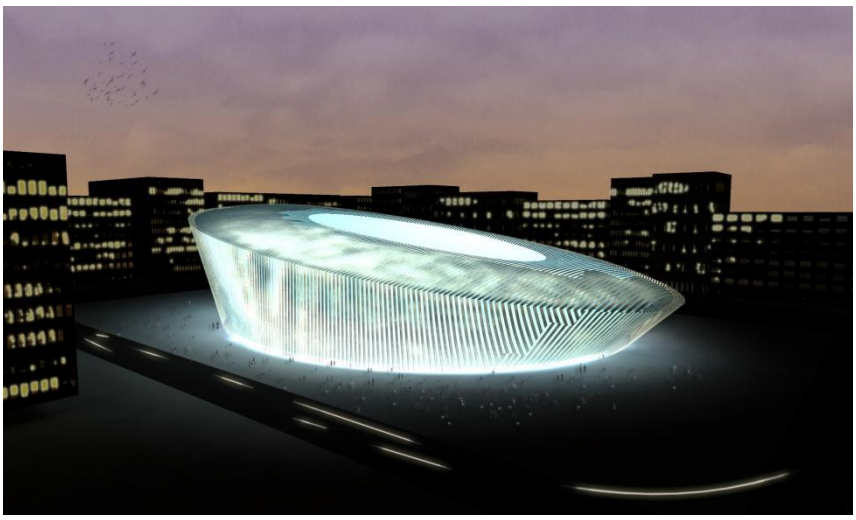


Figura 6: Renderizado del estadio con el software 3DStudio.

El resultado último no es más que una vibración más definida que resulta de todos los cambios habidos desde el proyecto inicial hasta la construcción final.

Enric Miralles
Arquitectos del tiempo. Miralles & Tagliabue.
Ed. Gustavo Gili. Barcelona, 1999, p.62

3. De arquitectura a matemáticas

La línea de trabajo aquí es totalmente opuesta al camino anterior. Ahora el reto era completamente diferente, la idea era partir de un edificio consolidado y crear en él una serie de cambios por medio del uso de las matemáticas. Ahora las matemáticas se vuelven al servicio de la arquitectura para responder a las voluntades del diseño. Por tanto la manera de operar aquí es sencilla, se escoge un edificio representativo de la historia de la arquitectura, se estudian posibles intervenciones siempre con el objetivo de mejorar estéticamente la obra seleccionada, queremos demostrar que aún siendo bellos por si solos pueden serlo más y se realizan primero bocetos que posteriormente se traducirán con matemáticas. De esta manera las matemáticas son el lenguaje que materializan de manera exacta las trazas arbitrarias de una mano creadora.

La obra seleccionada para mostrar en este trabajo como ya se ha dicho es un edificio representativo. Por un lado son el atrevimiento de acometer sobre obras insignes que de otra manera nunca pensaríamos si quiera en intervenir en ellas, por otra, suponen el vivo y claro contraste del desparpajo de una curva frente a la rectitud y ortogonalidad que les ha

legitimado el paso del tiempo. Así evocan el espíritu de la disonancia entre lo nuevo y lo clásico en un tono conciliador, armónico que creemos puede resultar atractivo. Con estas pretensiones escogemos el edificio del Partenón. Nos inclinamos por esta elección al ser un edificio ampliamente conocido y aceptado, por poseer un gran número de relaciones matemáticas y constituir en sí mismo un modelo de belleza.

3.1 El Partenón

La intervención propuesta viene dada por esta vocación de rebeldía al proponer la "ruptura de la caja del Partenón". Si se analiza de forma abstraída es fácil entenderlo como un prisma de base rectangular, una gran caja que nosotros proponemos abrir, romper hacía el exterior para generar en su interior un juego de rebotes de luz que ofrezcan nuevos matices a las piedras que lo envuelven. Para conseguir la ruptura se esbozan unas trazas que parten de los muros que conforman la naos del templo y buscan la luz en el exterior dibujando una curva circular que al extrusionarla alrededor del perímetro conforma la superficie final propuesta (Figura 7).

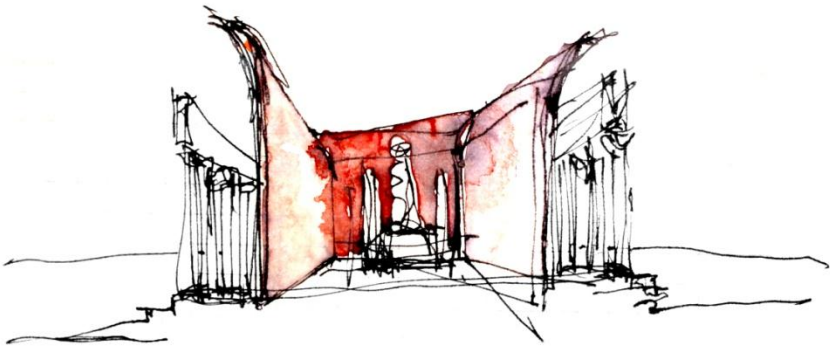


Figura 7. Sección del Partenón por la naos con vista de la estatua de Atenea.

El procedimiento pasa en sus inicios por un grupo de esbozos sin preocupación, siempre persiguiendo la curva más bella y proporcionada con la preexistencia (Figura 8).

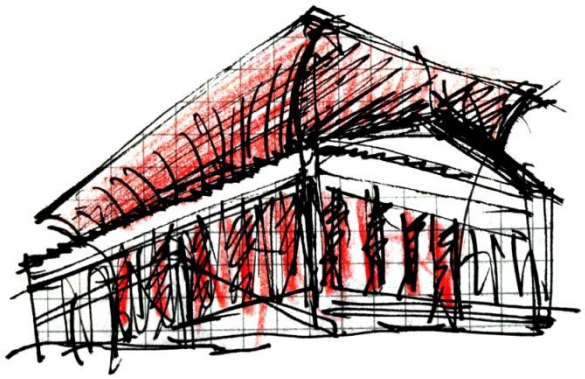


Figura 8. Esbozo del Partenón que muestra la intervención que queríamos hacer en el mismo.

Posteriormente, una vez decididos por un dibujo se pasa a buscar la curva conocida que mejor definan estas primeras intenciones y se trasladan a una representación simulada en Mathematica con unos resultados exactos. El siguiente paso es simular en una infografía el espacio generado en el Partenón por esta nueva superficie y valorar así el impacto que se genera. El renderizado se muestra en la Figura 9.

Figura 9. Renderizado final del Partenón con la intervención que planteamos.

4. Conclusiones

Vistos dos ejemplos significativos de lo que hasta ahora está siendo nuestro trabajo estamos en situación de valorar las aportaciones del uso de las matemáticas en el diseño arquitectónico.

En un primer lugar, las matemáticas nos ofrecen control en el ámbito constructivo ya que nos aportan la capacidad de poder cuantificar, de medir, de valorar,… De modo análogo sucede con el cálculo estructural, que se simplifica al responder a leyes matemáticas concretas.

Como se ha visto con la ideación del estadio, el uso de las matemáticas como herramienta de diseño permite un vasto campo de posibilidades para crear diferentes formas y además con el aliciente de que el resultado final queda respaldado por la seguridad que otorgan los números.

Otra virtud es la comodidad en la que permite desenvolverse con el uso de las distintas proporciones que sugieren la idea de venustas al imponer su carácter numérico en el diseño arquitectónico. Si estas proporciones se resumen a reglas matemáticas y el proyecto se trabaja en este mismo lenguaje resulta mucho más sencillo exprimir sus posibilidades que si tratamos de imponerlas sin esta base previa. Así mismo, cabe mencionar también que muchas de las propias superficies poseen de manera natural este concepto de belleza obviando la necesidad de tener que buscarlo.

Dicho lo anterior podemos concluir afirmando que las matemáticas sí son capaces de ayudar a la arquitectura en cuestiones de diseño como demuestra un estadio que no tiene nada que envidiar a sus homólogos concebido enteramente a través de las matemáticas o la

intervención en el Partenón que partiendo de unas trazas arbitrarias es capaz de respaldarlas y dotarlo de cuerpo y sentido legitimando la dualidad entre razón y corazón de la que pueden presumir la exactitud de los números.

Agradecimientos

Este trabajo ha sido financiado parcialmente con la Ayuda de Innovación Docente del Dpto. de Matemática Aplicada de la UPV (PID-DMA2012).

Referencias

[1] Arquitectura Viva 118-119, pp. 48-67, 2008.

[2] AV Proyectos 023, pp. 4-23, 2007.

[3] AV Proyectos 007, pp. 11-25, 2005.

Sobre los autores:

Nombre: María del Carmen Gómez Collado
Correo Electrónico: cgomezc@mat.upv.es
Institución: Instituto Universitario de Matemática Pura y aplicada (IUMPA), Universidad Politécnica de Valencia, España.

Nombre: Jaume Puchalt Lacal
Correo Electrónico: jaume.jpl@gmail.com
Institución: ETS de Arquitectura, Universidad Politécnica de Valencia. Jaume Espí escultura, España.

Nombre: Joel Sarrió
Correo Electrónico: sarriopuig@gmail.com
Institución: ETS de Arquitectura, Universidad Politécnica de Valencia, España.

Nombre: Macarena Trujillo Guillén
Correo Electrónico: matrugui@mat.upv.es
Institución: Instituto Universitario de Matemática Pura y Aplicada (IUMPA), Universidad Politécnica de Valencia, España.

Historias de Matemáticas

Criptología Nazi. Los Códigos Secretos de Hitler

Nazi Cryptology. Hitler's Secret Codes

José Manuel Sánchez Muñoz

Revista de Investigación

Volumen III, Número 1, pp. 059–120, ISSN 2174-0410
Recepción: 23 Nov'12; Aceptación: 6 Feb'13

1 de abril de 2013

Resumen

Este artículo trata la importancia de la desencriptación de los Códigos Enigma y Lorenz alemanes por parte de los aliados gracias al trabajo analítico de multitud de matemáticos, cuyo resultado fue vital para la derrota de los nazis en la 2ª Guerra Mundial, acortando ésta al menos en dos años.

Palabras Clave: Nazis, Matemáticas, 2ª Guerra Mundial, criptología, Enigma, Bomba, Lorenz, Colossus, Bletchley Park.

Abstract

This article considers the importance of the German Enigma and Lorenz codes cracking by the allies through the analitical work developed by many mathematicians, which had vital consequences for the nazi defeat in the 2nd World War, shortening it by around two years.

Keywords: Nazis, Mathematics, World War Two, criptology, Enigma, Bombe, Lorenz, Colossus, Bletchley Park.

1. Breve evolución histórica de la criptología hasta la 2ª Guerra Mundial

A lo largo de la historia, el hombre ha sentido la necesidad de codificar sus mensajes con la mera intención de que estos pasaran inadvertidos a los ojos de curiosos y mantener intacto el secretismo de los mismos. Surgieron así los primeros mensajes ocultos primitivos que rápidamente encontraron un nicho de utilidad en aquellas comunicaciones cuya privacidad debía ser garantizada. A esta comunicación secreta lograda mediante la ocultación se la denomina *esteganografía*, derivada del *steganos* o "encubierto" y *graphein* o "escribir". La principal desventaja de esta ciencia era que cualquiera podría interceptar un mensaje oculto y comprometer la seguridad de la comunicación.

Paralelamente a la *esteganografía*, surgió la ciencia de la *criptografía*, del griego *kryptos* o "escondido", cuya finalidad consistía más que en ocultar el mensaje, ocultar su significado mediante un proceso de codificación. De forma añadida surgieron las primeras técnicas de análisis cuya

finalidad principal consistía en desenmascarar el contenido secreto de los mensajes cifrados, lo que se denominó *criptoanálisis*. La evolución de las técnicas criptográficas supuso el avance y desarrollo de nuevas técnicas de análisis críptico.

Desde su inicio, la criptografía encontró su principal utilidad en el arte de la guerra. Algunos de los testimonios más antiguos que narran la utilización de escrituras secretas se remontan a Herodoto que escribió una crónica acerca de los conflictos entre Grecia y Persia en el siglo V a.C. Gracias a la mera ocultación de un mensaje de aviso del griego Demarato que vivía en la ciudad persa de Susa, donde se revelaban los planes estratégicos de invasión del archipiélago heleno del líder persa Jerjes, Grecia tomó una clara ventaja y pudo hacerse con la victoria y evitar la invasión en el año 480 a.C.

Los métodos criptográficos se pueden clasificar en métodos de encriptación *simétricos* y *asimétricos*. En los primeros se utiliza la misma clave para cifrar y descifrar los mensajes encriptados, al contrario que los segundos que utilizan diferentes claves. Los métodos *asimétricos* nacieron a finales del siglo XX y revolucionaron la ciencia de la criptografía. Dentro de los *métodos simétricos* de cifrado podemos encontrar los métodos de *sustitución* y *transposición*.

1.1. Métodos de Sustitución

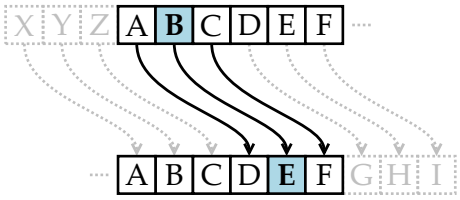


Figura 1. Cifrado de César

El primer ejemplo documentado de un *método de sustitución* de encriptación fue utilizado por Julio César en *La guerra de las Galias*, para enviar un mensaje a Cicerón que estaba sitiado y a punto de rendirse, sustituyendo las letras romanas por griegas haciendo ininteligible el mensaje. Para cifrar un mensaje mediante el *Cifrado de César*, cada letra de dicho mensaje era reemplazada con la letra de tres posiciones después en el abecedario. Por tanto, la A sería reemplazada por la D, la B por la E, la C por la F, y así sucesivamente. Por último la X, la Y y la Z serían reemplazadas por la A, la B y la C respectivamente. De ahí, que por ejemplo, "ATACAR" se cifraría como "DWDFDU". César rotaba el abecedario de tres en tres letras pero en general funcionaba con cualquier número acordado entre el emisor y el receptor del mensaje.

Figura 2. Sello conmemorativo sirio de Al Kindī (1994).[1]

Durante siglos este tipo de cifrado monoalfabético se consideró prácticamente imposible de romper, sin embargo con el paso del tiempo surgieron las técnicas de análisis criptográfico nacidas en el seno de la civilización musulmana. Aunque no se conoce el autor originario de la *técnica de análisis de tablas de frecuencia*, parece que al final del siglo IX d.C., Abũ Yũsuf Ya'qũb ibn Ishũq Al Kindī (801-873), conocido como *el filósofo de los árabes*, fue el primero en documentar dicho análisis en su libro *Sobre el descifrado de mensajes criptográficos* descubierto de forma casual en el Archivo de Estambul en 1987. Al Kindī que trabajó en filosofía, astrología, astronomía, cosmología, química, lógica, matemática, música, medicina, física, psicología y meteorología, manifestaba en dos breves párrafos:

> *"Una manera de resolver un mensaje cifrado, si sabemos en qué lengua está escrito, es encontrar un texto llano diferente escrito en la misma lengua y que sea lo suficientemente largo para llenar alrededor de una hoja, y luego contar cuántas veces aparece cada letra. A la letra que aparece con más frecuencia la llamamos «primera», a la siguiente en frecuencia la llamamos*

[1] http://jeff560.tripod.com/stamps.html

> *«segunda», a la siguiente «tercera», y así sucesivamente, hasta que hayamos cubierto todas las letras que aparecen en la muestra de texto llano.*
>
> *Luego observamos el texto cifrado que queremos resolver y clasificamos sus símbolos de la misma manera. Encontramos el símbolo que aparece con más frecuencia y lo sustituimos con la forma de la letra «primera»de la muestra de texto llano, el siguiente símbolo más corriente lo sustituimos por la forma de la letra «segunda», y el siguiente en frecuencia lo cambiamos por la forma de la letra «tercera», y así sucesivamente, hasta que hayamos cubierto todos los símbolos del criptograma que queremos resolver."*

La técnica de Al Kindī consiste en examinar un fragmento extenso de texto normal, o quizás varios, para establecer la frecuencia de cada letra del alfabeto. En castellano, dicha frecuencia se ve representada por la Tabla 1. A continuación, es necesario examinar el texto cifrado y determinar la frecuencia de cada letra. Si la letra más corriente en el texto cifrado es, por ejemplo, la J, entonces parecería probable que sustituyera a la E (que es la más comúnmente utilizada en español). Y si la segunda letra más frecuente en el texto cifrado es la P, probablemente sustituya a la A, y así sucesivamente. La técnica de Al Kindī, conocida como *análisis de frecuencia*, muestra que no es necesario revisar cada una de las billones de claves potenciales. En lugar de ello, es posible revelar el contenido de un mensaje codificado analizando simplemente la frecuencia de los caracteres en el texto cifrado, y realizando una comparativa con la tabla de frecuencias de un texto en el idioma considerado.

Tabla 1. Frecuencias de caracteres en castellano.[2]

Frecuencia Alta		**Frecuencia Media**		**Frecuencia Baja**	
Letra	**Porcentaje**	**Letra**	**Porcentaje**	**Letra**	**Porcentaje**
E	13,68	C	4,68	Q	0,88
A	12,53	T	4,63	H	0,70
O	8,68	U	3,93	F	0,69
S	7,98	M	3,15	Z	0,52
R	6,87	P	2,51	J	0,44
N	6,71	B	1,42	Ñ	0,31
I	6,25	G	1,01	X	0,22
D	5,86	V	0,90	W	0,02
L	4,97	Y	0,90	K	0,01

1.2. Métodos de Transposición

Tras el análisis de frecuencia, la criptografía continuó su avance surgiendo entonces nuevos métodos simétricos de encriptación cada vez más y más sofisticados, denominados *Métodos de Transposición*, que consisten como su definición indica en transponer los textos, es decir que ahora no son las letras las que cambian, sino su orden.

Pongamos un ejemplo; imaginemos que tanto el emisor del lenguaje cifrado como el receptor consideran en principio un número menor de nueve dígitos como clave, por ejemplo el 231[3]. Dicha clave ponía de manifiesto que el texto debía ser escrito en tres columnas (en principio sin considerar espacios entre palabras). De este modo el emisor codificaría la frase "DESEMBARCAR AL AMANECER",

[2] FLETCHER, P., *Secret and Urgent: the Story of Codes and Ciphers*, pp. 254-255, Blue Ribbon Books, 1939.

[3] En ocasiones se utilizaban como clave letras del alfabeto, de tal modo que si a la A le corresponde el 1, a la B el 2 y así sucesivamente, si se hacía uso por ejemplo la palabra EVA, la clave de codificación se correspondía al número 5-23-1, codificado de texto de tres columnas, en la que la primera ha de colocarse en el tercer grupo de letras del mensaje cifrado, la segunda en el grupo inicial de dicho mensaje, y la tercera en el segundo grupo del mensaje.

1	2	3
D	E	S
E	M	B
A	R	C
A	R	A
L	A	M
A	N	E
C	E	R

$\Rightarrow$

2	3	1
E	S	D
M	B	E
R	C	A
R	A	A
A	M	L
N	E	A
E	R	C

$\Rightarrow$ "EMRRANE SBCAMER DEAALAC"

De esta forma el receptor recibía dicho mensaje y colocaba dicho grupo de letras en tres columnas, de modo que el primer grupo de letras correspondía con la segunda columna del lenguaje original, el segundo se correspondía con la tercera columna, y el tercer grupo se correspondía con la primera columna.

1.3. El Disco de Alberti

Durante siglos, la cifra de sustitución monoalfabética simple había resultado lo suficientemente complicada para garantizar su indescifrabilidad. Sin embargo las técnicas de análisis de frecuencias desarrolladas por Al Kindī fueron rápidamente transmitidas al mundo occidental, comprometiendo seriamente la integridad de los mensajes cifrados. Comenzaba a ser evidente que la batalla entre los criptógrafos y los criptoanalistas estaba comenzando a ser ganada por el segundo grupo. Es así cuando en torno a 1460, el erudito renacentista natural de Florencia, Leon Battista Alberti (1404-1472) comenzó a trabajar en una nueva técnica de cifrado de mensajes. Mientras gozaba de una conversación durante un paseo por el Vaticano, su amigo, y a la sazón secretario pontificio, Leonardo Dato, puso al corriente a Alberti de los últimos adelantos en cuanto a criptografía se refería. Esta conversación fortuita animó a Alberti a investigar, llegando a la conclusión de que era necesario utilizar dos o más alfabetos cifrados, alternando entre ellos durante la codificación con el fin de fortalecer la encriptación y confundir así a los potenciales criptoanalistas.

De 1466 a 1467 escribió su tratado *De Componendis Cyphris*, considerado como el escrito sobre criptología más antiguo del mundo occidental. En dicho tratado explica el desarrollo de las técnicas polialfabéticas. A partir de ahí, Alberti analiza diversos procedimientos: sustituciones de tipos diferentes, transposiciones de letras dentro de palabras y mensajes obtenidos marcándose las posiciones de ciertas letras en un texto inocente. Finalmente concluye su introducción con la descripción de su invención, *el disco cifrante*, también conocido como *Disco de Alberti*.

> *"Fijo dos discos en una placa de cobre. Uno, el mayor, será fijo y el otro, el menor, movible. El diámetro del disco fijo es superior en un noveno al del disco móvil. Divido la circunferencia de cualquiera de los dos en veinticuatro partes iguales llamadas sectores. En cada uno de los sectores del disco grande escribo en orden alfabético normal una letra mayúscula roja: primero A, a continuación B, después C, etc, omitiendo H y K que no son indispensables."*

De este modo, Alberti obtuvo un total de 20 letras, pues J, U, W e Y tampoco figuraban en su alfabeto. En los cuatro sectores restantes escribió los números 1, 2, 3 y 4. Haciendo referencia a los veinticuatro sectores del disco pequeño escribió:

> *"...una letra minúscula, en negro, no en la orden normal como en el disco fijo, pero en una orden incoherente. De esta forma, se puede suponer que la primera letra será a, la décima segunda g, la décima tercera q y así sucesivamente, de modo que todos los veinticuatro sectores sean llenados porque el alfabeto latino posee veinticuatro caracteres, siendo el vigésimo cuarto &. Efectuados estos arreglos, se coloca el disco pequeño sobre el grande, de modo que*

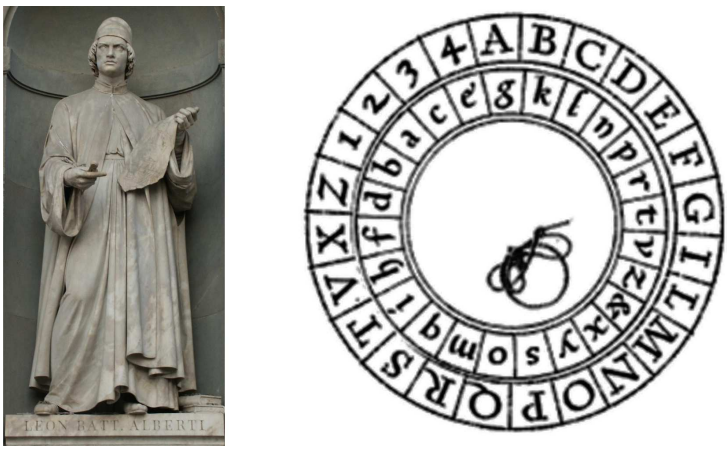


Figura 3. Estatua de Leon Battista Alberti en la Galería Uffizi, Florencia, y Disco de Alberti (imagen del manuscrito original "De Componendis Cyphris", 1466).

> *una aguja pasada por los dos centros sirva como un eje común alrededor del cual girará el disco móvil."*

Se considera una de las letras del disco móvil como letra llave o letra índice, por ejemplo k. Hecho esto el emisor alinea esta letra llave con cualquier letra del disco externo e informa de la posición del disco móvil al receptor escribiendo la letra escogida. Alberti usó el ejemplo de k alineada con B.

> *"Usando este punto de partida, cada letra del mensaje representará la letra fija por encima de ella. Después de escribir tres o cuatro letras, puedo cambiar la posición de la letra-índice de modo que k esté, por ejemplo, sobre D. Después, en mi mensaje, escribiré una D mayúscula y, a partir de este punto, k no significará más B y sí D, y todas las letras del disco fijo tendrán nuevas letras equivalentes."*

1.4. La Cifra Vigenère

Alberti puede ser considerado como el inventor del cifrado polialfabético y sus estudios sirvieron de base para trabajos posteriores como los de Johannes Trithemius que inventó *la tábula recta*, Giovanni Porta y sobre todo del diplomático francés de mediados del siglo XVI Blaise Vigenére (1523-1596), que a diferencia de Alberti utilizó la enorme cantidad de 26 alfabetos cifrados. Vigenère utilizó como base *la tábula recta* de Trithemius, y la amplió generando *la tábula de Vigenère*, que se muestra en la Tabla 2.

Figura 4. Blaise de Vigenère Bovrbonois (1515).[4]

Desde el punto de vista de su funcionamiento, se numeran las 26 letras del abecedario de forma que A = 0, B = 1, ..., Z = 25. En términos matemáticos puede expresarse como:

$$Y_i = (X_i + Z_i) \, mod \, T$$

donde T representa el número total de letras del alfabeto considerado (en general 26), X_i representa el ordinal de las letras de la palabra clave considerando las filas de la Tabla 2, es decir, que a P le

[4] Retrato de Thomas de Leu. Edificio Stephen A. Schwarzman. División de Arte, Pinturas y Fotografías Miriam e Ira D. Wallach.

Tabla 2. Tábula de Cifrado Vigenère

Llano	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
(5º) 4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
(1º) 13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
(2º) 14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
(3º) 17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
(4º) 19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

corresponde al numero 15 en modo horizontal, y Z_i representa el ordinal de la letra de texto plano (sin cifrar) considerada, que se corresponde con las columnas de la Tabla 2, esto es, la L en modo vertical le corresponde al numero 11. Finalmente Y_i representa el ordinal de la letra cifrada en el alfabeto considerado. Entonces la ecuación quedará de la siguiente manera $Y_i = (15 + 11)\ mod\ 26$. El resultado es 0, donde 0 es igual a A en modo horizontal. Haciendo uso de la Tabla 2, vamos a ilustrar cómo el emisor generaba un mensaje cifrado y el receptor descifraba dicho mensaje utilizando una codificación-descodificación por medio de una palabra clave. Imaginemos que el emisor quiere cifrar la orden *"movilizar las tropas dos km al sur"* considerando como clave la palabra "norte". La palabra "norte" especifica que se utilizará la codificación de los alfabetos 13, 14, 17, 19 y 4 en ese orden hasta finalizar el texto llano original. De este modo el emisor haría uso de la Tabla 2 y para la primera letra del mensaje original "m" se corresponde en el alfabeto 13 con la "Z", la segunda letra "o" se corresponde en el alfabeto 14 con la "C", la "v" se corresponde en el alfabeto 17 con la "M", la "i" se corresponde en el alfabeto 19 con la "B", y la "l" se corresponde en el alfabeto 4 con la "P", a partir de aquí el emisor continuaría con el proceso de encriptación volviendo a hacer uso de la secuencia de alfabetos 13, 14, 17, 19 y 4, y así sucesivamente. Con todo lo anterior el mensaje cifrado tendría el aspecto especificado en la Tabla 3.

El receptor del mensaje cifrado podría invertir el proceso de encriptado repitiendo la operación en la Tabla 2, entrando primero en el alfabeto 13 y mirando en el alfabeto llano que la "Z" se corresponde con la "m", la "C" del alfabeto 14 se corresponde en el alfabeto llano con la "o", y así sucesivamente.

Este sistema de cifrado tenía dos ventajas fundamentales respecto a los sistemas de encriptación conocidos hasta ese momento. La primera era que aparentemente resultaba inexpugnable al análisis de frecuencias, ya que una misma letra no tenía porqué repetir un patrón de re-

Tabla 3. Encriptación de mensaje mediante el Cifrado de Vigenère (I).

Texto Llano Orig.	m o v i l i z a r l a s t r o p a s d o s k m a l s u r
Clave	N O R T E N O R T E N O R T E N O R T E N O R T E N O R
Texto Cifrado	Z C M B P V N R K P N G K K S C O J W S F Y D T P F I I

petición, y aparecía cifrada con diferentes letras. La segunda era la enorme combinación de posibilidades a barajar. Todas estas ventajas tendrían que haber sido suficientes para que todos los secretarios de cifra de Europa hubieran adoptado este método como sistema oficial de encriptación, sin embargo esta cifra, a todas luces perfecta, permanecería prácticamente ignorada durante los dos siglos y medio posteriores, seguramente debido a la complejidad de su aplicación a nivel práctico, que supondría tener que realizar un gran esfuerzo tanto a emisores como a receptores de mensajes cifrados con dicho método.

Durante algo más de doscientos cincuenta años, la Cifra Vigenère fue considerada prácticamente impenetrable, sin embargo la aparición en escena en la primera mitad del siglo XIX de la excéntrica figura del inglés Charles Babbage (1791-1871) como el principal protagonista del criptoanálisis de la época supuso un punto de inflexión. Babbage, entre otras cosas, es considerado como uno de los precursores de la que hoy consideramos una de las herramientas cotidianas más importantes como es el ordenador. Babbage se interesó por la desencriptación desde que era muy joven. En una ocasión, recordó cómo esa afición de su infancia le había proporcionado en ocasiones más de un quebradero de cabeza:

> *"Los chicos mayores hacían cifras, pero si yo conseguía unas pocas palabras, generalmente descubría la clave. En ocasiones, la consecuencia de este ingenio resultó dolorosa: los dueños de las cifras detectadas a veces me daban una paliza, a pesar de que la culpa la tenía su propia estupidez."*

Estas palizas no le desanimaron, al contrario, sirvieron de acicate para continuar cautivado por el criptoanálisis. En su autobiografía escribió *"... descifrar es, en mi opinión, una de las artes más fascinantes"*.

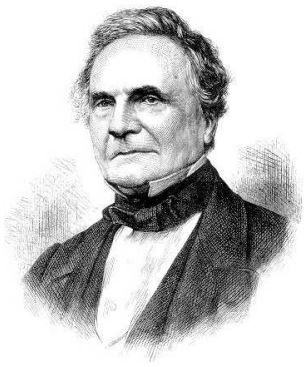


Figura 5. Charles Babbage.[5]

El interés de Babbage por la Cifra Vigenère se había producido en cierto modo de una manera fortuita, gracias a la intervención de un dentista de Bristol aficionado a la criptografía llamado John Hall Brock Thwaites. Resulta que en 1854, Thwaites afirmó haber inventado una nueva cifra, que en su desconocimiento de la Cifra Vigenère, resultaba similar a ésta, y escribió sobre sus avances en el *Journal of Society of Arts*, con la firme intención de patentar su descubrimiento. Babbage escribió a esa sociedad poniendo de manifiesto que Thwaites llegaba con varios siglos de retraso manifestando *"la cifra ... es muy antigua, y aparece en multitud de libros"*. En lugar de retractarse Thwaites adoptó una posición desafiante y no pidió ningún tipo de disculpas instando a Babbage a que aceptara el reto de descifrar una de las cifras generadas con su idea. Descifrable o no, no tenía relación alguna con el hecho de que fuera o no nueva, pero este nuevo reto despertó la curiosidad de Babbage que se embarcó en la búsqueda de un punto débil en la Cifra Vigenère.

¿Pero cómo fue capaz Babbage de desencriptar una cifra supuestamente indescifrable? Pongamos un ejemplo para comprender el proceso. Imaginemos que nuestra palabra clave es "SUR", y que el mensaje que queremos encriptar es "El adulto y el joven en el espejo". Nuestro mensaje se encriptaría haciendo uso de los alfabetos cifrados 18, 20 y 17, repitiendo este ciclo hasta concluir el mensaje. En la Tabla 4 podemos observar que los tres determinantes "el" del texto

[5] http://es.wikipedia.org/wiki/Charles_Babbage

Tabla 4. Encriptación de mensaje mediante el Cifrado de Vigenère (II).

Texto Llano Orig.	E l a d u l t o y e l j o v e n e n e l e s p e j o
Clave	S U R S U R S U R S U R S U R S U R S U R S U R S U
Texto Cifrado	W F R V O C L I P W F A G P V F Y E W F V K J V B I

llano original, se repiten en el mensaje cifrado. Esto es porque sus letras ocupan las posiciones 1-2, 10-11 y 19-20, es decir cada determinante está separado 9 posiciones del otro, que resulta múltiplo de la palabra clave "SUR" que es de 3 letras. Estas repeticiones no pasaron desapercibidas para Babbage y le proporcionaron un punto de partida desde el que comenzar a romper la Cifra Vigenère.

La brillante técnica empleada por Babbage consistía en una especie de estudio de frecuencias pero adaptada a la particularidad de la Cifra Vigenère. Imaginemos que se ha interceptado el mensaje de la Tabla 5, del cual únicamente se sabe que ha sido encriptado con la Cifra Vigenère, pero del que se desconoce la palabra clave utilizada.

La primera fase del ataque al código llevada a cabo por Babbage, consistió en buscar secuencias de letras que aparecieran más de una vez en el texto, esto es buscar patrones de repetición de caracteres, y una vez encontrado alguno ver la distancia de separación entre uno y otro para ver la multiplicidad de dicha distancia y de este modo establecer una hipótesis sobre la longitud de la palabra clave.

Tabla 5. Texto cifrado interceptado con patrones de repetición resaltados.

K F Z G N **H I S I E K A** **T I Q** L R A D L X A I C R A G F Q C G Q R **T I Q** I J V A H B F V V X I
V H M I E G L **V O X S E** E U D B P S G Q D U W M Q F U H D P X E I G N P W P I J R A F V A
X V P E L G D E Q Q N V S Z S I T E V D A R U K O **H I S I E K A** K O O M V P **D R G** Q R R
N A V I B E U T E G S C Y V R O G W M W V P T D F E I P C C D P M M J F E K O O I I O E G
C E T I G G X B F E J S U H F Q W L O E Q H A H R N A F C Z Z V T S D Q U S E S U H J M Q
F U A W S Z I I X O B O O S E V E V H M V R N A V R A W P E O Q H D E C C C R G F Y D D
R H O Z X V U A O O E I X W N G O O S D Q A O O Y I E Q S F C Y T C G J D V Q I C G G L R
A I J V E **V O X S E** C F L B P I V X I W O D P R U I P D D I J K O Q S E H V U A J F M H R D L
H G K P R U I Q T X Y V P C L O E H V N D H G B E T J O G S G R S C N **T I Q** V F C Q X S X
P F U L L P D S J F E F O V E G Q R G C D E U Q S **T I Q** W V C N D E G I C N O V Q M N F P
E V Q Q V I C **D R G** O S D Q P X S D X R U D H T A V K C L H N M W R S U H Z X S J D I O
Z Q X V U D H P M R T Q Q X S H M V P E Q W S R F T O G S P S E F E O O Y Y C V I W I P H
V E A U H M W U G I Q U X E K G R U O T S C C N G O Q W G C N D Z M W Z P D L O E P
R E H L B M C V N P H F G I A G R F S Z Y E G X W F M S I F I Q O D M F K N I Z G N F G N
H Z M R Z O O G S G R G C D U S K P V J A F S Z S C X I G O D U L G H D M Q R V N M X B
P S L P I Q H Q V V U M D M A V P O A V G M K I C D R E G I C C P R G U G Z Q N V C O M
R N Y O O A T Z P I R B P I J W S F C Y M K G N W S E L V G L H U U H F G S W S E E C Q N
T I Q Z V K S W O Z E C G G U S O S E U U V A M K E K F L Q A W T W A G F A W M W E V
H D S I G T U O F S V N M L C Q P U G M L A M H I G Y W C P E T N A V S P I G C I V O V I
J V E Q U A Q L E H D Q A R W K A Q N M I E G L S C P I I F E O O E M D R R H G U S E G S
H L F I I P A V H M P M G Z P S Q U L K V R E G I T Q N U S E T V E T R O H S J R E U C C Y
V S U H F Q M J P O V S D M R C R W W E X R U I Q C F Y M K E V S U P L U I R B Q W

Analizando el texto cifrado, se procedería a construir una tabla de observación de patrones de repetición de caracteres, y la separación entre ellos, donde se representa la multiplicidad de esta separación (Tabla 6).

Aunque todavía no se tenga demasiada información sobre el mensaje cifrado, tras enumerar qué secuencias se repiten, así como los espacios que hay entre las repeticiones, el resto de la Tabla 6 trata de identificar los factores de los espaciamientos: la división entera de estos espaciamientos. Por ejemplo, la secuencia HISIEKA se repite tras 112 letras, por lo que los números

Tabla 6. Patrones de repetición de caracteres y espaciado entre ellos.

			Posible longitud de la clave (o factores)																	
Secuencia	Repetición	Separación	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
HISIEKA	2	112	✓		✓			✓	✓						✓		✓				
TIQ	5	21		✓				✓													
		35				✓		✓													
		329						✓													
		364	✓		✓			✓						✓	✓						
		385				✓		✓				✓									
		399		✓				✓												✓	
		420	✓	✓	✓	✓	✓	✓			✓		✓		✓	✓					✓
		728	✓		✓			✓	✓		✓			✓	✓						
		749						✓													
DRG	2	329						✓													
VOXSE	2	266	✓					✓							✓					✓	

2, 4, 7, 8, 14 y 16 son factores, ya que pueden dividir exactamente a 112 sin dejar decimales. Parece lógico considerar que la palabra clave tiene una longitud de 7 caracteres, ya que este factor se repite en todas las secuencias. En principio no conocemos aún la palabra clave con la que el mensaje ha sido cifrado, por lo que consideraremos que se trata de la palabra X1-X2-X3-X4-X5-X6-X7. Cada una de estas letras proporciona un alfabeto de cifrado, de forma que el cifrado polialfabético puede ser considerado como una combinación de 7 cifrados monoalfabéticos responsables cada uno de ellos de un séptimo de la codificación del total del mensaje. Luego las letras 1^a, 8^a, 15^a, 22^a, ..., estarán codificadas por el alfabeto cifrado correspondiente a X1. Parece evidente que conocer la palabra clave tanto para el emisor como para el receptor es una fase crucial en el desencriptado del texto llano original. Llegado a este punto podemos recurrir al análisis de frecuencias monoalfabético ya visto anteriormente. Para ello se lleva a cabo en el texto cifrado un "conteo" de las frecuencias de aparición de cada uno de los caracteres del alfabeto correspondiente al carácter X1 (Figura 6).

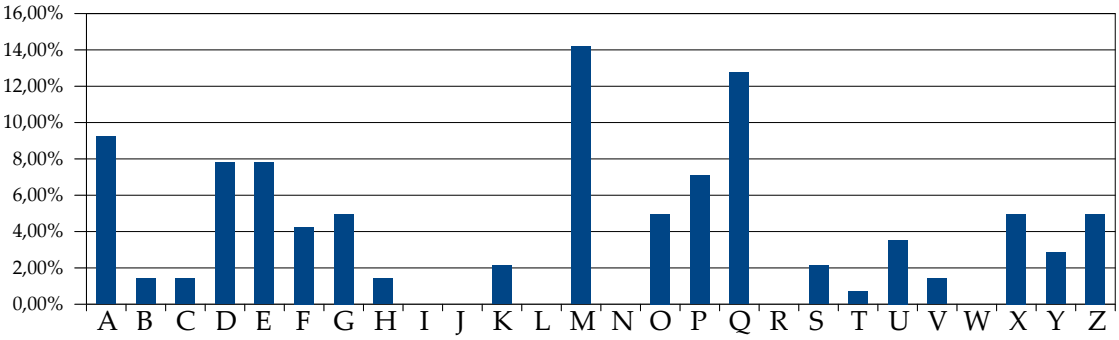


Figura 6. Distribución de frecuencias para las letras del texto cifrado, codificado utilizando el alfabeto cifrado X1 (porcentaje de apariciones).

En este punto ha de recordarse que cada alfabeto cifrado del cuadro Vigenère es simplemente un alfabeto normal desplazado entre 1 y 26 posiciones. Por esta razón, la distribución de frecuencias de la Figura 6 debería tener rasgos similares a la distribución de frecuencias de un alfabeto normal, excepto que habrá sido desplazado unas cuantas posiciones.

Si se realiza una comparativa gráfica de las Figuras 6 y 7, ambas debieran superponerse aunque con un desplazamiento, ya que recordemos que los alfabetos cifrados de la Tábula de Vigenère son generados por el desplazamiento de varios caracteres con respecto al alfabeto

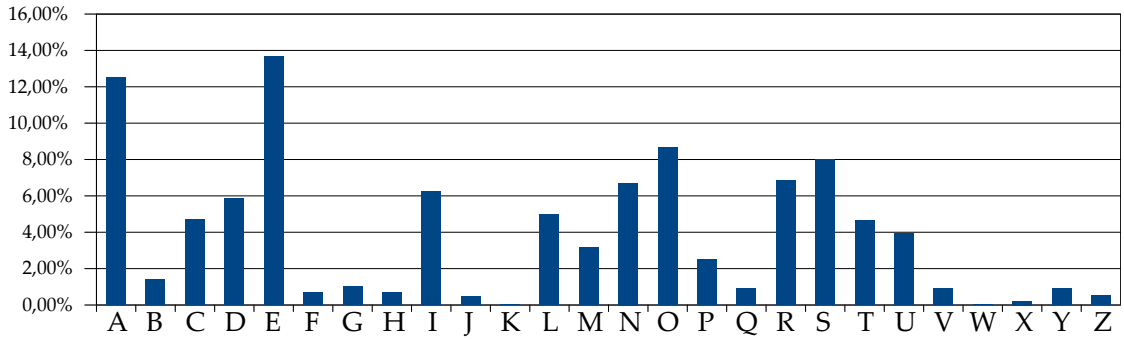


Figura 7. Distribución de frecuencias de caracteres para el idioma castellano.

llano original. Fijándonos en los patrones más representativos podemos ver que los bloques "MNOPQ", "XYZA" y "DEFGH" del alfabeto cifrado, se corresponden respectivamente con los bloques "ABCDE", "LMNO" y "RSTUV" del alfabeto llano. De este modo podemos considerar que el alfabeto llano se corresponde con el alfabeto cifrado identificado por la letra "M", es decir el número 12.

Identificado este primer alfabeto, procederíamos del mismo modo con el resto de caracteres de la palabra clave, esto es X2, X3, . . . , actividad que proponemos al lector como juego de entrenamiento. Llegaríamos a la conclusión de que el texto cifrado interceptado puede encriptarse-desencriptarse con la palabra clave "MERCADO". Descubierta la palabra clave el resto es una tarea relativamente sencilla.

Tabla 7. Texto original desencriptado (de la novela de Alejandro Dumas "El Conde de Montecristo").

Y B I E N E U G E N I A Q U E H A Y D I J O E L P A D R E Y P O R Q U E E S T A E N T R E V
I S T A E N E L S A L O N C U A N D O P O D R I A M O S H A B L A R E N M I D E S P A C H
O T E N E I S R A Z O N S E N O R R E S P O N D I O E U G E N I A H A C I E N D O S E N A
L A S U P A D R E D E Q U E P O D I A S E N T A R S E Y A C A B A I S D E H A C E R M E D
O S P R E G U N T A S Q U E R E S U M E N T O D A L A C O N V E R S A C I O N Q U E V A
M O S A T E N E R V O Y A C O N T E S T A R A L A S D O S Y C O N T R A L A C O S T U M
B R E A N T E S A L A S E G U N D A C O M O A L A M E N O S C O M P L E J A H E E L E G
I D O E S T E S A L O N A F I N D E E V I T A R L A S I M P R E S I O N E S D E S A G R A D A
B L E S Y L A S I N F L U E N C I A S D E L D E S P A C H O D E U N B A N Q U E R O A Q U
E L L O S L I B R O S D E C A J A P O R D O R A D O S Q U E S E A N A Q U E L L O S C A J O
N E S C E R R A D O S C O M O P U E R T A S D E F O R T A L E Z A S A Q U E L L O S B I L L
E T E S D E B A N C O Q U E V I E N E N I G N O R O D E D O N D E L A M U L T I T U D D E
C A R T A S D E I N G L A T E R R A H O L A N D A E S P A N A L A S I N D I A S L A C H I
N A Y E L P E R U E J E R C E N U N E X T R A O R D I N A R I O I N F L U J O E N E L A N I
M O D E U N P A D R E Y L E H A C E N O L V I D A R Q U E H A Y E N E L M U N D O U N
I N T E R E S M A Y O R Y M A S S A G R A D O Q U E L A P O S I C I O N S O C I A L Y L A
O P I N I O N D E S U S C O M I T E N T E S H E E L E G I D O E S T E S A L O N Q U E V E I S
T A N A L E G R E C O N S U S M A G N I F I C O S C U A D R O S V U E S T R O R E T R A T
O E L M I O E L D E M I M A D R E Y T O D A C L A S E D E P A I S A J E S T E N G O M U C
H A C O N F I A N Z A E N E L P O D E R D E L A S I M P R E S I O N E S E X T E R N A S T A
L V E Z M E E Q U I V O Q U E C O N R E S P E C T O A V O S P E R O Q U E Q U E R E I S N
O S E R I A A R T I S T A S I N O T U V I E S E I L U S I O N E S

Es muy probable que la técnica de criptoanálisis de la cifra Vigenère utilizada por Babbage se realizara en torno a 1854, poco después de su altercado con Thwaites, sin embargo su descubrimiento no tuvo ningún tipo de repercusión ya que nunca publicó sus logros. El descubrimiento

no se conoció hasta 1920, cuando gran parte de los trabajos de Babbage fueron examinados por un grupo de investigadores. De forma paralela pero independiente, el oficial retirado del ejército prusiano Friedrich Wilhelm Kasiski (1805-1881) desarrolló una técnica criptográfica similar a la de Babbage, que publicó en 1863 en *"Die Geheimschriften und die Dechijfrirkunst"* (*"La escritura secreta y el arte del desciframiento"*), y que hoy día es conocida como la *Prueba Kasiski*. Según algunos historiadores, es posible que Babbage, aparte de que tenía el hábito de no finalizar la mayoría de proyectos en los que se embarcaba, no publicara sus descubrimientos debido a presiones recibidas por parte de la inteligencia británica, ya que la guerra de Crimea había estallado recientemente, lo que hace muy probable que los británicos quisieran gozar de una ventaja sobre sus enemigos rusos, obligando a Babbage a mantener su secreto.

2. Las máquinas de cifrado y Enigma

2.1. El origen de Enigma

Al final de la 1ª Guerra Mundial se produjo la aparición y proliferación de las máquinas de cifrado de rotores. Estas máquinas fueron desarrolladas de forma independiente por varios inventores de diferentes países en un lapso temporal de varios años. La inclusión de varios rotores se produjo con el fin de complicar el algoritmo de cifrado. Este tipo de máquinas daban la posibilidad además de simplificar al máximo su operatividad y funcionamiento. Algunas de estas máquinas se utilizaron ampliamente durante la 2ª Guerra Mundial, y algunos ejemplos son la Enigma alemana, la máquina púrpura japonesa, o la estadounidense M-209. Casi todas fueron crackeadas por el enemigo. Una de las que sin lugar a dudas tuvo más impacto mediático por su repercusión y todas las connotaciones que surgieron en torno a ella fue la alemana Máquina Enigma.

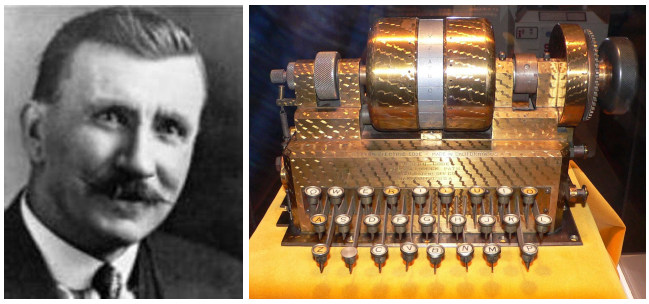


Figura 8. Edward Hugh Hebern (izq.) y Máquina Hebern (drcha.).[6]

La primera máquina de cifrado de rotores fue inventada en los EE.UU por Edward Hugh Hebern (1869-1952). Entre 1912 y 1915 patentó varios dispositivos de cifrado como un teclado de cifrado y dos máquinas de escribir eléctricas conectadas con un cableado de 26 conexiones para el cifrado monoalfabético automático. Hebern construyó su primera máquina cifrado en 1917, la cual tenía únicamente un rotor que podía ser extraído y cambiar su orientación con el fin de ser utilizado para cifrar y descifrar mensajes. Hebern mejoró su máquina implementándola con nuevos rotores hacia 1921, cuando solicitó su patente y fundó la Hebern Electric Code Company. El criptoanalista estadounidense William Friedman, que conseguiría romper la japonesa máquina púrpura, mejoró el diseño original de Hebern con la invención de la SIGABA. La máquina de Hebern tenía un rotor que giraba y mantenía fijos los otros para 26 caracteres de un mensaje, haciéndola vulnerable al criptoanálisis. La SIGABA tenía una rotación irregular, lo que hizo que fuera una de las pocas máquinas de cifrado cuyo código no fue roto durante la 2ª Guerra Mundial. Hebern únicamente vendió una docena de máquinas antes de llegar a la bancarrota, lo que provocó su entrada en prisión por haber defraudado a sus inversores.

[6] http://ciphermachines.com/types.html
[7] http://dactilografo.blogspot.com.es/2011/02/me-guarda-un-secreto-el-funcionamiento.html

Figura 9. Arthur Scherbius.[7]

La segunda máquina de cifrado de rotores fue inventada en 1918. Ese año el ingeniero alemán Arthur Scherbius (1878-1929) y su íntimo amigo Richard Ritter fundaron la compañía *Scherbius & Ritter* (más tarde rebautizada en julio de 1923 como *Chiffriermaschinen Aktien Gesellschaft*), una innovadora empresa de ingeniería que cubría un amplio rango de invenciones. Scherbius era el encargado de lo que hoy denominamos I+D, buscando continuamente nuevas oportunidades. Uno de sus proyectos preferidos era sustituir los inadecuados sistemas manuales de criptografía empleados en la 1ª Guerra Mundial por una codificación mecánica y automática que mejorara las posibilidades de cifrado, aumentando la cifra de permutaciones posibles, y simplificando en gran medida la labor del emisor del mensaje cifrado. Scherbius había estudiado ingeniería eléctrica en Hannover y en Múnich, y desarrolló una pieza de maquinaria criptográfica que era esencialmente una versión eléctrica del disco de cifras de Alberti. Nadie podía sospechar que el invento de origen civil de Scherbius, se convertiría en el más temible sistema militar de codificación de la historia.

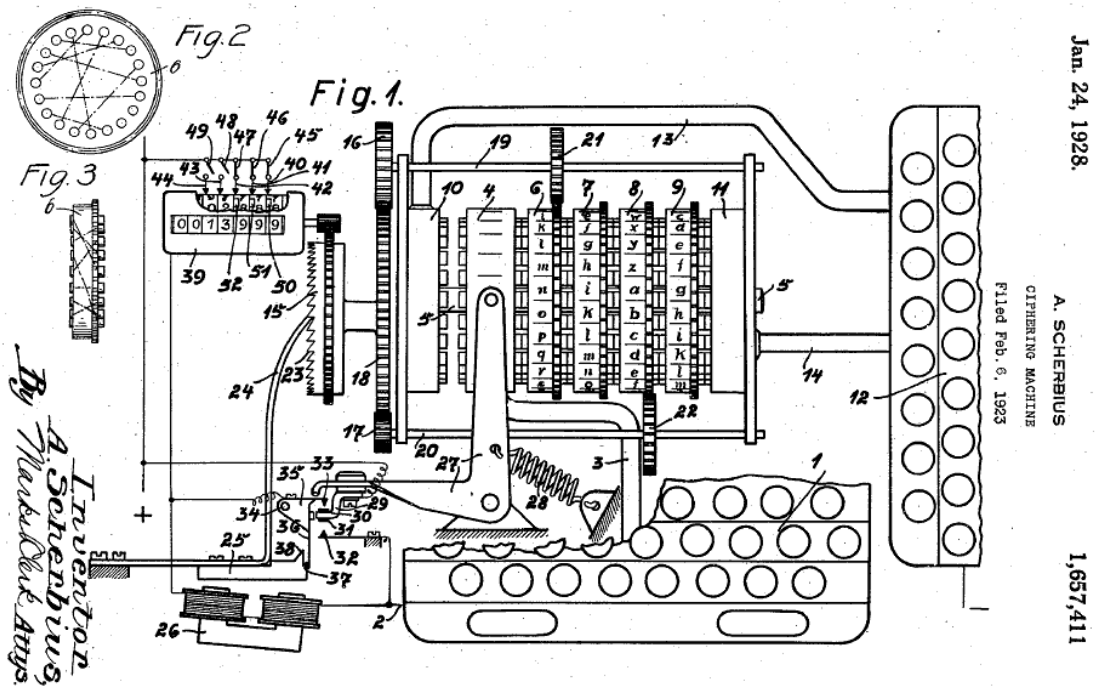


Figura 10. Patente americana (US - 1.657.411) de Enigma (A. Scherbius, 24 Enero - 1928).[8]

El 23 de Febrero de 1918, Scherbius solicitó la primera patente de la máquina comercial Enigma, con el fin de crear una máquina que mantuviera en secreto las principales transacciones de información en el mundo empresarial. Enigma era relativamente fácil de transportar y muy potente, rápida y cómoda a la hora de generar mensajes cifrados. La primera versión comercial, conocida con el nombre de Enigma-A, fue puesta a la venta en 1923. A esta primera versión le siguieron tres modelos comerciales. El modelo Enigma-C vio la luz en 1926, siendo su principal característica su liviano peso de 11,8 kg frente a los 49,9 kg de sus antecesoras. El modelo Enigma-D se convirtió en el más relevante, y el que tuvo verdadero éxito comercial. A pesar del origen comercial de Enigma, la armada alemana en Febrero de 1926, y posteriormente el ejército el 15 de junio de 1928, adquirieron su propia máquina Enigma, adaptándola y cambiando su fisonomía acorde a sus necesidades, como la inclusión del clavijero en 1930, o la modificación

[8] http://en.wikipedia.org/wiki/Arthur_Scherbius

de las conexiones del cableado de los rotores con el fin de aumentar el número de posibilidades de cifrado y complicar más aún si cabe su criptoanálisis. Sin duda éste era un síntoma claro de que ambos estaban contraviniendo todas las directrices especificadas en el Tratado de Versalles ya que la intención principal de estas adquisiciones era la protección de sus comunicaciones en primera instancia y el rearme como fin último. El ejército alemán comenzó a utilizar el diseño básico de la máquina en 1929, cuyo uso se generalizó prácticamente a la totalidad de los estamentos militares alemanes y la cúpula Nazi. En la marina alemana (*Kriegmarine*) se la denominó con el nombre de máquina "M". Hasta la llegada al poder de Adolf Hitler en 1933 se habían fabricado en el mundo más de 100.000 unidades, llegando a ser utilizadas en países como Suecia, Holanda, Japón, Italia, España, EE.UU o Reino Unido entre otros.

La tercera máquina de cifrado de rotores fue desarrollada por el inventor holandés Hugo Alexander Koch. Dicha invención fue patentada el 7 de octubre de 1919 en Holanda. En vista del escaso éxito comercial que tuvo Koch (parece ser que no vendió ninguno de sus dispositivos de cifrado), éste le vendió algunos de los derechos de su máquina a Scherbius en 1927, por un valor de 600 florines holandeses. Algunos consideran que Scherbius le compró estos derechos a Koch con el fin de proteger su propia invención, ya que el alemán conocía a Koch ya que ambos habían colaborado estrechamente cuando Scherbius estaba desarrollando la Enigma.

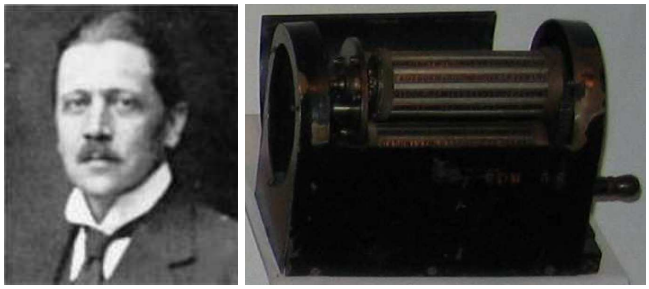


Figura 11. Arvid Gerhard Damm (izq.) y Prototipo Damm (drcha.).[9]

La invención de la última máquina de cifrado de rotores se le atribuye al sueco Arvid Gerhard Damm, que la patentó tan sólo tres días después que Koch, el 10 de octubre de 1919. Su invención utilizaba un rotor doble cuya cadencia era irregular. En 1920, Damm fundó la empresa *Aktiebolaget Cryptograph* con el fin de comercializar su invención, sin embargo, se trataban de máquinas tremendamente erráticas, lo que hizo que Damm no pudiera tener el éxito comercial esperado, ya que sólo vendió unas pocas unidades. Dos de sus inversores eran Karl Wilhelm Hagelin y Emanuel Nobel (sobrino de Alfred). El hijo de Hagelin, Boris, que se habíia graduado en ingeniería mecánica en el Instituto Tecnológico de Estocolmo en 1919, se unió a la empresa en 1922 con el fin de proteger la inversión realizada. El ejército sueco encargó un gran pedido en 1926, sin embargo Damm no pudo disfrutar de su relativo éxito ya que moriría un año después. Un año antes, Boris Hagelin había tomado el control de la empresa (rebautizándola después con el nombre de *Aktiebolaget Cryptoteknik* en 1932), desarrollando de forma exitosa máquinas de cifrado con capacidad de imprimir (B-211) y una máquina totalmente portable (C-35). Un posterior diseño de Hagelin, la C-38, fue adquirida por el gobierno estadounidense y modificada bajo el permiso del propio Hagelin, siendo rebautizada como la M-209. Se vendieron más de 140.000 unidades de dicho modelo durante la 2ª Guerra Mundial, convirtiendo a Hagelin en el primero y posiblemente único millonario de este tipo de tecnología de máquinas de cifrado.

En el año 2003, se descubrió que la máquina de cifrado de rotores fue realmente inventada antes de los cuatro protagonistas mencionados anteriormente. Parece ser que en 1915, dos oficiales navales holandeses, Theo A. van Hengel y R.P.C. Spengler, tuvieron la idea de construir un dispositivo de estas características mientras residían en las colonias holandesas del Este. Construyeron un prototipo en el verano de 1915, pero la armada holandesa no consideró que fuera una invención necesaria como para adoptarla en sus comunicaciones, además de disuadir a Hengel y Spengler que intentaron patentar el dispositivo. Casualidades de la vida, uno de los abogados que inició el proceso de dicha patente era Huybrecht Verhagen, hermanastro de

[9] http://ciphermachines.com/types.html

Hugo Alexander Koch. Esta coincidencia filial permitió con mucha probabilidad conocer dicha invención a Koch, dándole la idea definitiva para desarrollar su dispositivo de cifrado.

2.2. El funcionamiento de Enigma

Enigma era muy similar a una máquina de escribir, salvo porque se alimentaba de una batería y no empleaba papel. Sus mensajes codificados se transmitían en código morse para ser descifrados por otra máquina Enigma al otro extremo de la línea. La máquina estaba formada por varias partes; un teclado de 26 caracteres, un clavijero interno o panel Stecker[10] con 6 pares de conexiones cableadas que podían conmutarse[11], un panel luminoso con 26 caracteres, varios rotores o modificadores (dependiendo de la versión de la Enigma), cada uno de los cuales contenía 26 ranuras dentadas perimetrales con las 26 letras de alfabeto, y el reflector que devolvía el impulso eléctrico hacia los rotores una vez la señal había sido codificada. Cuando el operador pulsaba una tecla, enviaba un impulso eléctrico que recorría el interior de la máquina. Dicho impulso pasaba por el clavijero, donde era redirigido hasta el cilindro de entrada al conjunto de rotores que contenían el alfabeto. En estos rotores era donde el operador llevaba a cabo los ajustes de la máquina. Unas ventanillas mostraban las letras en los rotores. Cada vez que el operador pulsaba una tecla, avanzaba una letra el rotor derecho o rápido. Una vez el rotor rápido diera toda una vuelta (que dependía de donde se situaba su muesca) entonces giraba una posición el rotor central, es decir avanzaba una letra, y del mismo modo lo hacía el de la izquierda o lento con respecto al rotor central, con la salvedad de que éstos dos últimos además de la rotación ya descrita, rotaban también cuando llegaban hasta la posición de su propia muesca. El impulso eléctrico pasaba de derecha a izquierda a través de los cables de cada rotor, y era devuelto por un reflector de izquierda a derecha. En su viaje de vuelta el impulso pasaba por el clavijero nuevamente, y su destino final era el tablero luminoso, donde se iluminaba la letra transpuesta. La letra que se iluminaba se encendía dependiendo de los ajustes de la máquina, y esto se podía hacer en la cantidad de 150 millones de millones de millones de modos. El mensaje codificado era transmitido en código morse para ser descodificado por una máquina enigma receptora ajustada en la misma clave diaria. En tiempos de guerra, estos ajustes se llegaron a realizar hasta tres veces al día.

Sin duda el gran número de permutaciones posibles que la máquina era capaz de barajar, hicieron de ella que fuera considerada prácticamente inviolable. Éste fue uno de los motivos por el que pasó a formar parte del equipamiento de la armada alemana, no sin antes realizar varios cambios significativos como la introducción de un mayor número de rotores, con el fin de aumentar el número de posibilidades de cifrado. Este cambio la haría prácticamente inexpugnable a los ataques criptográficos, sin embargo, la historia probaría que los nazis estaban totalmente equivocados.

2.3. La operatividad de Enigma

El parámetro de configuración fundamental para operar con Enigma era la clave que tanto emisor como receptor debían conocer. Dicha clave estaba compuesta por:

[10] Abreviatura de *Steckerbrett* que en alemán significa "panel de conexiones de clavija". La versión comercial de Enigma no estaba dotada con este dispositivo que fue incluído en la versión militar con la intención de aumentar la seguridad.

[11] Este número aumentó hasta 10 pares en sucesivas modificaciones con el fin de aumentar la seguridad de la máquina.

[12] El diagrama representa el recorrido del impulso eléctrico desde que, una vez ajustada la configuración de los rotores (5), el operador pulsa la tecla A en el teclado (2), entonces el impulso eléctrico generado pasa por el clavijero o panel Stecker (3), de ahí pasa al cilindro de entrada (4), y entonces pasa por los rotores (5), y el reflector (6) que envía dicho impulso nuevamente a los rotores (5), cilindro de entrada (4), hasta que llega nuevamente al Stecker donde el impulso se direcciona con la conexión correspondiente (7 y 8), hasta que finalmente aparece iluminada la tecla codificada D (9) del tablero luminoso. Fuente: http://en.wikipedia.org/wiki/Enigma_machine

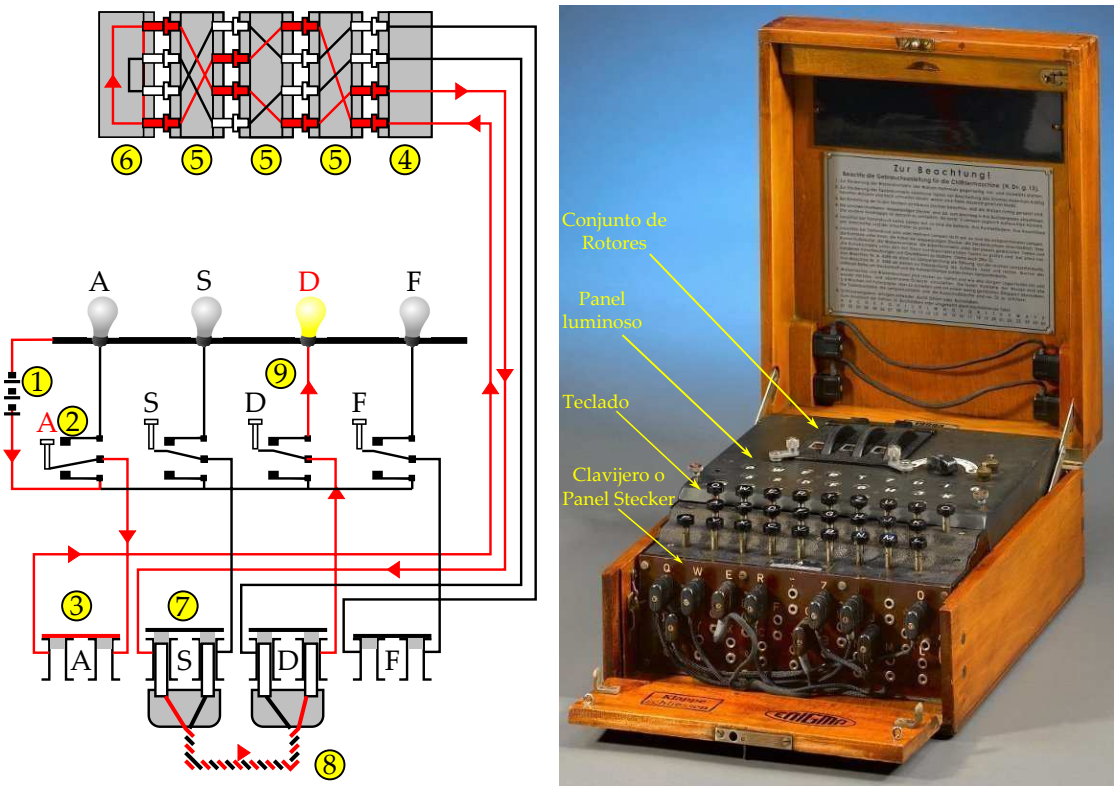


Figura 12. Diagrama de funcionamiento de Enigma y partes de la misma.[12]

- ✓ El orden de los rotores en los huecos de la máquina (*Walzenlage*).
- ✓ La posición inicial de éstos, que se configuraba colocando con la ruleta de la A a la Z (*Grundstellung*).
- ✓ Las conexiones del clavijero o panel Stecker.

Aunque no influía en la configuración de la clave, la distribución inicial de los anillos de los rotores (*Ringstellung*), que servía para variar la estructura del cableado interno de los mismos, también era un factor que podía modificarse.

Cada mes, los operadores de Enigma recibían un libro del alto mando con las claves diarias (*"tageschlüssel"* en alemán) a utilizar en dicho mes[13], de modo que un operador podía leer en el libro algo así como:

- Walzenlage: II-III-I.
- Ringstellung: H-J-R.
- Grundstellung: Y-B-J.
- Stecker: A/G, F/H, J/L, M/O, R/T, U/X.

La configuración anterior le indicaba al operador que debía poner el segundo rotor en el hueco 1 y girarlo hasta la posición Y, el tercer rotor en el hueco 2 y girarlo hasta la B y el primer rotor en el hueco 3 y girarlo hasta la posición J. Así mismo debía conectar los cables en el panel

[13] A medida que avanzó la guerra, el número de claves pasó a ser de hasta tres diarias.

Stecker con los pares de letras indicados. Una vez configurada la máquina, el operador podía comenzar a cifrar los mensajes que eran enviados mediante código morse. El receptor debía asimismo colocar la máquina en la misma disposición según el libro de códigos, y aquí es donde juega su papel el reflector. Simplemente tecletaría el mensaje cifrado recibido, y el mensaje original aparecería en el panel luminoso.

Figura 13. De izq. a drcha. y de arriba a abajo: 1. Rotores de la Enigma. La parte posterior del rotor izqdo. muestra una muesca en la letra H (cada rotor tenía la suya) causante del giro de una posición del siguiente rotor situado inmediatamente a la izquierda. Por ejemplo los rotores I, II y III, tenían estas muescas en las letras Y, M y D, que provocaban el giro del rotor situado inmediatamente a su izquierda en las letras Q, E y V respectivamente. Inclusive la Kriegsmarine introduciría dos nuevos rotores (el IV y el V) que tenían doble muesca (los rotores de la 1ª imagen son de este tipo), y causaban un aumento del número de giros de los mismos. 2. Disposición del anillo que se podía modificar para cambiar la configuración del cableado interno y la muesca del rotor. 3. Cableado interno de un rotor (diferente en cada rotor). 4. Reflector. 5. Interior del reflector. 6. Clavija interna del reflector modificable.[14]

Los alemanes se dieron cuenta que operando de este modo, generaban un sinfín de mensajes con la misma clave durante todo un día (ya adelantaban que en periodos de operaciones bélicas, el tráfico de comunicaciones iba a ser inmenso), y esto resultaba un filón para los criptoanalistas. Conscientes de ello, emitieron una serie de órdenes sobre cómo se debía utilizar Enigma. De lo que no fueron conscientes es que al señalar una serie de normas estrictas, aunque al principio pudieran parecer sensatas, estaban proporcionando pistas para los criptoanalistas que significaron el principio del ataque a Enigma. Dichas normas eran fundamentalmente:

1. No se podía conectar una letra con su inmediatamente anterior o posterior en el panel Stecker.
2. Un rotor no podía permanecer en el mismo hueco durante más de un día.

Sin embargo la norma más importante resultó ser el concepto de "clave de mensaje" (en alemán *"spruchschlüssel"*). Con el fin de evitar un intenso tráfico de mensajes cifrados con la misma clave, lo que en sí mismo constituiría un filón para los criptoanalistas, los alemanes consideraron que cada mensaje enviado debía tener su propia clave. Pero, ¿cómo sabría el receptor la clave que había utilizado el emisor? Para ello el emisor configuraba la Enigma con la clave del día según el libro de códigos. Con dicha configuración, escribía tres letras elegidas al azar, por ejemplo FKM, obteniendo en el panel luminoso ZBH. Después, giraba los rotores desde su posición inicial (la indicada para ese día por el libro) a la posición de esas tres letras, en este caso F-K-M, dejando el orden de rotores y el panel Stecker sin cambios, y entonces procedía a codificar el mensaje a enviar. De este modo el mensaje transmitido comenzaba ZBH, que era la

[14] http://www.cryptomuseum.com/crypto/enigma/m4/index.htm y http://naukas.com/2012/12/24/.

codificación de FKM según la clave del día y el mensaje codificado según la disposición F-K-M de los rotores. El receptor, que tenía la máquina configurada con la clave del día, recibía la transmisión, y se fijaba en las primeras tres letras. Las tecleaba (ZBH en el ejemplo) y veía FKM. Entonces giraba los rotores a esa disposición, F-K-M, y tecleaba el resto del mensaje, obteniendo el original. Este hecho era característico de la Enigma como consecuencia de la propiedad recíproca que veremos más adelante.

Pero con el fin de evitar errores por interferencias en la transmisión o de los operadores, los alemanes obligaban a teclear dos veces seguidas las tres letras de la clave de mensaje. Así que realmente el emisor, con la clave del día, tecleaba FKMFKM, obteniendo en el panel luminoso ZBHGJI, y luego orientaba los rotores en la posición F-K-M y codificaba el mensaje. El receptor recibía el mensaje, tecleaba las seis primeras letras, ZBHGJI, y veía FKMFKM, con lo que ya reconocía la clave de mensaje. Sin embargo lejos de reforzar la seguridad de Enigma, esta norma ofrecía a los criptoanalistas un punto de partida para comenzar a romper el código. Enigma, incumplía algunos de los principios de Kerckhoffs.

Principios de Kerckhoffs

En 1883, el lingüista y criptógrafo holandés Auguste Kerckhoffs (1835-1903) enunció en sus ensayos sobre criptografía militar los seis principios fundamentales que debían cumplirse para diseñar cualquier sistema criptográfico eficiente. Sus trabajos, más que una revisión del estado del arte de esta disciplina, significaron una auténtica renovación para las técnicas criptográficas del momento. Básicamente estos principios eran:

- ✓ Si el sistema no es teóricamente irrompible, al menos debe serlo en la práctica.
- ✓ La efectividad del sistema no debe depender de que su diseño permanezca en secreto.
- ✓ La clave debe ser fácilmente memorizable de manera que sea necesario recurrir a notas escritas.
- ✓ Los criptogramas deberán mostrar resultados alfanuméricos.
- ✓ El sistema debe ser operable por una única persona.
- ✓ El sistema debe resultar fácilmente utilizable.

.

3. El origen del ataque a Enigma. El BS4.

3.1. 1ª Etapa. De Poznań a Varsovia

Tras la 1ª Guerra Mundial, los aliados se encargaron de vigilar las comunicaciones germanas. Sin embargo a partir de 1926, comenzaron a interceptar mensajes cifrados mediante un nuevo método que desconocían hasta el momento. En medio de este desconcierto se encontraba el recientemente formado estado soberano de Polonia, el cual tenía al este a la Unión Soviética, un estado hambriento por expansionar su doctrina comunista fuera de sus fronteras, y al oeste Alemania, un estado que ansiaba recuperar los territorios cedidos a Polonia tras la guerra. En este clima de desconfianza, los polacos crearon su Oficina de Cifras, el *Biuro Szyfrów*, a mediados de 1931, surgido de la unión de la Oficina de Radio-Inteligencia (*Referat Radiowywiadu*) y la Oficina Criptográfica Polaca (*Referat Szyfrów Wlasnych*), e integrada en la 2ª Sección del ejército polaco, siendo su máximo responsable el teniente coronel Gwido Langer (1894-1948), y el mayor Maksymilian Ciężki (1894-1948) el jefe de la sección encargada de desencriptar los mensajes cifrados alemanes. Ciężki conocía la Enigma comercial, sin embargo, no tenía acceso a la Enigma

militar, claramente distinta debido a los cambios introducidos en ella, por lo que al desconocer su cableado interno, fue incapaz de iniciar un ataque efectivo a su cifrado.

En enero de 1929, el director de la Universidad de Poznań (actualmente Universidad Adam Mickiewicz) Zdzislaw Krygowski preparó una lista de 20 estudiantes de matemáticas de últimos cursos que recibieron un llamamiento del ejército para participar en un curso de criptología. Bajo el juramento por parte de estos alumnos de mantener toda la operación en secreto, el curso se impartiría durante dos noches a la semana en dicha Universidad por el ya nombrado mayor Maksymilian Ciężki, Antoni Palluth (1900-1944), un ingeniero empleado civil del Biuro Szyfrów, y el mayor Franciszek Pokorny, por entonces jefe del mismo, emparentado con el famoso criptólogo del ejército austríaco durante la 1ª Guerra Mundial, el capitán Herman Pokorny. El curso tenía como principal propósito servir de apoyo al Servicio de Inteligencia Polaco de Radio con el fin de descifrar los mensajes alemanes interceptados. La razón de la elección de la Universidad de Poznań fue fundamentalmente debido a que la región de Pomerania, situada al oeste de Polonia, formó parte de la Prusia oriental, desde 1793 hasta 1918, por lo que sus habitantes hablaban perfectamente el alemán, de hecho a finales del siglo XIX, la escuela era obligatoriamente impartida en lengua germana. La otra razón de esta elección fue que, aunque no era demasiado conocido, la universidad contaba con un Instituto de Matemáticas.

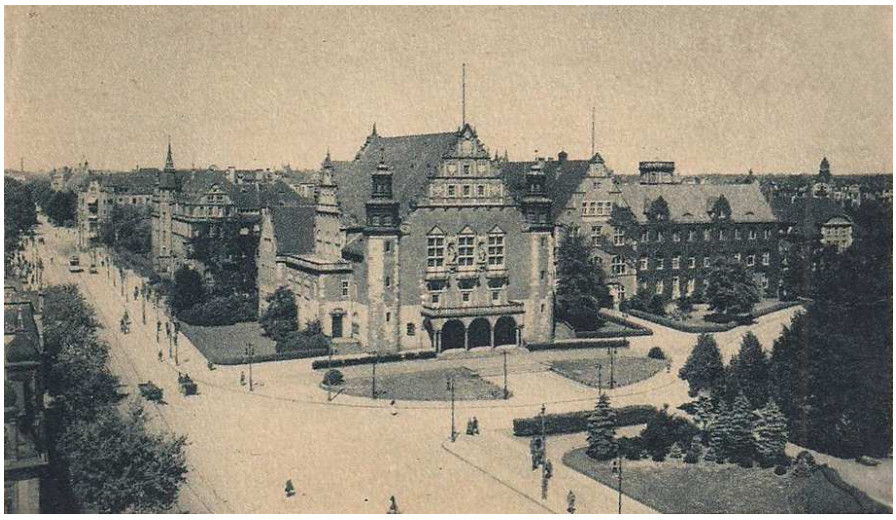


Figura 14. Universidad de Poznań (1929).

Tras varias semanas, los estudiantes que asistieron a dicho curso fueron puestos a prueba para descifrar varios mensajes alemanes reales anteriores al uso de la Enigma que ya habían sido descifrados previamente. Con el fin de acotar su vocabulario se les daba una idea sobre el tema que trataba cada mensaje. Tras un par de horas, algunos estudiantes entre los que se encontraban Marian Rejewski (1905-1980), Jerzy Różycki (1909-1942) y Henryk Zygalski (1908-1978), fueron capaces de descifrar los mensajes. A medida que el curso avanzaba, estos mensajes se fueron complicando paulatinamente, de modo que muchos estudiantes fueron abandonando el curso bien porque preferían dedicarse enteramente a sus estudios, o bien porque consideraban que no tenían suficientes habilidades para la criptología. Únicamente los tres estudiantes antes nombrados fueron capaces de compaginar sus estudios con el curso. Uno de los exámenes a los que fueron sometidos era una comunicación militar alemana entonces actual cifrada mediante el código denominado "Cifrado de Doble Transposición". Los tres estudiantes, cada uno de manera independiente, fueron capaces de romper dicho código, poniendo de manifiesto que estaban dotados de ciertas habilidades criptológicas. Muy a su pesar, Rejewski tuvo que abandonar el curso antes de su finalización, puesto que recibió una beca para estudiar en la Universidad de Gotinga, sueño de cualquier estudiante de matemáticas, puesto que allí habían impartido clases eminencias como Gauss, Riemann, Dirichlet, Poincaré o Hilbert entre otros.

Método de Doble Transposición

Se trata de un código utilizado por el ejército de los EE.UU en la 1ª Guerra Mundial, prácticamente idéntico al código UBCHI alemán. Consiste fundamentalmente en realizar una primera transposición del texto plano según las letras de una o dos claves, así por ejemplo, la palabra clave ENIGMA, equivaldría a la clave 264351 (los números representan el orden de las letras de la palabra clave en el alfabeto). Se coloca el texto plano en una matriz de tantas columnas como letras posea la palabra clave, escribiendo por filas, y se realiza una primera transposición por columnas. Una vez hecha esta operación se vuelven a coger las columnas transpuestas y se escriben nuevamente por filas, y se realiza la segunda transposición por columnas, en este paso se podría hacer uso de una segunda palabra clave. Veamos como se cifraría el mensaje "REPLEGAR TROPAS EN TORNO A LA POSICION INICIAL", con la única palabra clave ENIGMA.

1	2	3	4	5	6
R	E	P	L	E	G
A	R	T	R	O	P
A	S	E	N	T	O
R	N	O	A	L	A
P	O	S	I	C	I
O	N	I	N	I	C
I	A	L			

$\Rightarrow$

2	6	4	3	5	1
E	G	L	P	E	R
R	P	R	T	O	A
S	O	N	E	T	A
N	A	A	O	L	R
O	I	I	S	C	P
N	C	N	I	I	O
A			L		I

$\Rightarrow$

1	2	3	4	5	6
E	R	S	N	O	N
A	G	P	O	A	I
C	L	R	N	A	I
N	P	T	E	O	S
I	L	E	O	T	L
C	I	R	A	A	R
P	O	I			

$\Rightarrow$

2	6	4	3	5	1
R	N	N	S	O	E
G	I	O	P	A	A
L	I	N	R	A	C
P	S	E	T	O	N
L	L	O	E	T	I
I	R	A	R	A	C
O			I		P

Finalmente se agrupaban en grupos de cinco letras para su transmisión posterior en código Morse, resultando:

RGLPL IONII SLRNO PRTER IOAAO TAEAC NICP

En el verano de 1930, Rejewski regresó a Poznań. Al finalizar el curso, los mejores estudiantes del mismo fueron invitados para colaborar con el Biuro Szyfrów cuyas oficinas estaban en los sótanos de la comandancia militar polaca equipadas con todo lo necesario para descifrar los mensajes alemanes. De forma general se permitía a los estudiantes compaginar sus tareas criptológicas con sus estudios, de manera que su trabajo en el Biuro Szyfrów se distribuía generalmente en doce horas semanales en el turno que ellos prefirieran, ya fuera diurno o incluso nocturno. La "cámara oscura" (como llamaban los estudiantes a los oficinas del Biuro) estaba en el puesto de la comandancia militar, tan sólo a unos pasos del Instituto de Matemáticas para que los estudiantes no tuvieran que perder demasiado tiempo en el trayecto y aprovechar así sus tiempos muertos. Rejewski comenzó a trabajar allí en el otoño de 1930.

Se formó de este modo un grupo de trabajo de jóvenes matemáticos, cuya principal tarea consistía en el descifrado de todo tipo de códigos alemanes. Los estudiantes recibían constantemente información de varias estaciones de radio dedicadas a interceptar mensajes cifrados de los alemanes quienes regularmente cambiaban sus claves, y rápidamente aprendieron incluso a aprovechar los errores cometidos por los operadores alemanes, como por ejemplo el hecho de que necesitaran mensajes de al menos 50 caracteres de longitud. Los estudiantes descubrieron que los alemanes caracterizaban estos mensajes más cortos con la letra "X" y a continuación codificaban el mismo. Sin embargo, a pesar de sus más que notables habilidades criptológicas, aparecieron unos cifrados que no podían romper independientemente de las técnicas utilizadas. El uso de la Enigma se había instaurado de forma total en el ejército alemán y era el momento de "profesionalizar" las tareas criptológicas de los estudiantes polacos. En el verano de 1932, el puesto de Poznań fue cerrado y Rejewski primero, y Ròżycki y Zygalski un poco después, comenzaron a trabajar como empleados del Biuro Szyfrów en Varsovia. Nacía así el BS4 y co-

menzaba la guerra contra Enigma.

3.2. 2ª Etapa. La aparición de *Asché*

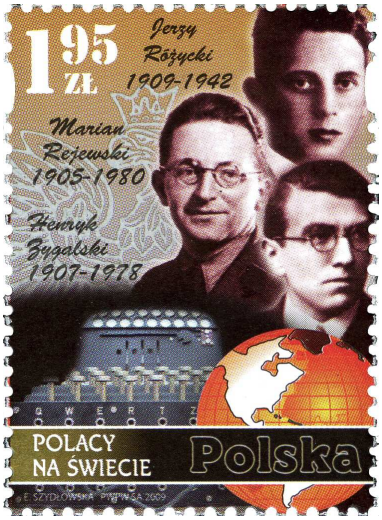


Figura 15. Miembros del BS4.[15]

El trabajo del BS4 se basó fundamentalmente en el estudio de la repetición de patrones. El patrón más obvio de la encriptación de la Enigma era la clave de mensaje, que se codificada dos veces al principio de cada mensaje. Los alemanes habían exigido dicha repetición para prevenir posibles errores causados por las intermitencias de radio o fallos del operador, sin embargo no previeron que esto pondría en peligro la seguridad de la máquina. A pesar de que los polacos del BS4 realizarían un gran avance en el descubrimiento del funcionamiento de Enigma mediante el análisis de los patrones de repetición, consiguiendo identificar que las cadenas de caracteres cifrados tenían una relación dependiente exclusivamente de la posición de los rotores de la máquina, al principio su principal limitación era su desconocimiento sobre la distribución del cableado interior de la máquina, ya que no contaban con ninguna máquina física del ejército alemán. Este hecho añadido a que los alemanes modificaban el cableado interior de las máquinas que adquirían con el fin de evitar posibles espionajes que comprometieran la integridad de sus comunicaciones, impidieron en primera instancia que los polacos del BS4, del que formaba parte el joven Rejewski entre otros, fueran capaces de descifrar los mensajes interceptados.

Existe un punto de vista erróneo que se repite sistemáticamente en multitud de publicaciones, y que no es otro que considerar que la ruptura del código de Enigma se produjo de una manera puntual, cosa que no fue así puesto que los polacos llevaron a cabo pequeños logros que se tradujeron finalmente en comprender el funcionamiento de la Enigma y consecuentemente establecer una estrategia eficaz para desentrañar el código de encriptación que la máquina escondía. El primer intento de búsqueda de la desencriptación del código Enigma llevaría en torno a cuatro meses, proceso que debía considerar dos cuestiones bien diferenciadas:

1. Por un lado la reconstrucción teórica de la Enigma militar. Los criptólogos polacos descubrirían primero la función del reflector (*Umkehrwalze*), tras lo cual reconstruyeron poco a poco todas conexiones existentes en la máquina, cuyos principales componentes eran el sistema de rotores (*Chiffrierwalzen*) que giraban sobre un eje común, y el panel de conexiones o clavijero. Esto supuso que los polacos fueran capaces de construir una réplicas de la Enigma que hacían posible la lectura de los mensajes cifrados alemanes una vez se encontraran las claves de configuración de los rotores.

2. Por otro lado estaba el proceso de elaboración de los métodos para la reconstrucción de las claves de la Enigma basándose únicamente en los mensajes interceptados por las estaciones polacas de radiomonitoreo.

Es en este momento en el que hace su aparición la figura de Hans Thilo Schmidt, un corrupto y resentido funcionario de la *Chiffrierstelle* en Berlín, la oficina responsable de administrar las comunicaciones cifradas de Alemania. Schmidt, que sirvió en la 1ª Guerra Mundial y fue expulsado del ejército después de los recortes producidos en el mismo tras la firma del armisticio en Versalles, había entrado en la oficina de cifras a través de la intervención de su hermano Rudolf, un reputado oficial alemán con una trayectoria en ascenso al que parece ser que

[15] Sello polaco (2009). http://www.wnsstamps.ch/en/stamps/PL039.09

se le atribuye la idea de sugerir al alto mando del ejército alemán que se considerara la Enigma con el objetivo de salvaguardar la seguridad de las comunicaciones. Schmidt tenía fama de mujeriego y parece que le gustaba vivir por encima de las posibilidades que un puesto como el suyo le podía proporcionar. Fue entonces cuando a través de la embajada de Francia en Berlín, accedió a intercambiar información valiosa sobre el funcionamiento de Enigma a cambio de cuantiosas prebendas. Así fue como el servicio secreto francés, a través de la intermediación del entonces capitán Gustav Bertrand (1896-1976) y el agente secreto cuyo pseudónimo era *Rex*, obtuvo copia de varios documentos sobre el funcionamiento de Enigma de manos de Schmidt el 8 de noviembre de 1931 en el Grand Hotel de Verviers, Bélgica. Se establecieron varias reuniones entre septiembre y octubre de 1932, en las que Schmidt, cuyo nombre en clave era *Asché* (pronunciación francesa de *H*), proporcionó los libros de códigos con todas las claves del día completas para 38 meses firmados por el teniente coronel Erich Fellgiebel (más tarde nombrado general y jefe de la sección de comunicaciones de la Wehrmacht), así como fotos de la máquina, aunque en ningún caso ninguna documentación sobre el cableado interno de los rotores. Sin embargo, muy a su pesar, los criptoanalistas franceses fueron incapaces de sacar partido a dicha información. Por ello, en virtud del tratado de colaboración que franceses y polacos habían firmado tras la 1ª Guerra Mundial, y dado que el Biuro Szyfrów estaba muy interesado en todos los asuntos relacionados con Enigma, la inteligencia francesa decidió compartir esta información con sus homónimos polacos, lo que significó un punto de inflexión en el ataque al código de Enigma. Schmidt trabajó en la *Chiffrierstelle* hasta 1938. El 23 de marzo de 1943 sería arrestado y supuestamente reconoció su espionaje en julio de ese año. Finalmente se suicidaría el 19 de septiembre de 1943.

Figura 16. Hans Thilo Schmidt.[16]

El jefe del Biuro Szyfrów, Gwido Langer, tomó una desconcertante pero astuta decisión. No entregó en primera instancia los libros de claves a Rejewski hasta finales de 1932, consciente de que éstas no estarían disponibles en tiempos de guerra. De este modo obligó al propio Rejewski a entrenar sus capacidades criptoanalíticas en tiempo de paz en previsión del inminente conflicto bélico que inevitablemente estaba a punto de estallar. En este punto, Rejewski y sus colegas no tuvieron más remedio que agudizar su ingenio para buscar una manera de romper el código de la Enigma. Rejewski que contaba con alguna Enigma comercial buscó refugio en las matemáticas puras y abstractas, en particular en el estudio de las permutaciones dentro de la rama denominada como teoría de grupos. Uno de los pilares fundamentales para el análisis criptológico en general son el estudio de las repeticiones, en el caso de Enigma, Rejewski comenzó por estudiar los únicos patrones de repetición que conocía, la clave de los mensajes que se repetía al inicio de cada uno de ellos.

Figura 17. Karol Gwido Langer.[17]

3.3. El Método de las Permutaciones. Fundamentación Teórica

A pesar de que la tesis de Marian Rejewski titulada *Teoría de funciones periódicas dobles de segunda y tercera especie y sus aplicaciones*, estaba más cerca del análisis que del álgebra, estaba muy familiarizado con la teoría de grupos, y conocía bastante bien las permutaciones. Desde un punto de vista formal, una permutación puede considerarse como una reordenación de elementos. Por ejemplo cuando ordenamos las lista de nuestros alumnos por orden alfabético de

[16] http://pippick.com/reviews/worldfaceoff/worldtimer_faceoff.htm
[17] http://enigma.umww.pl/index.php?page=gwido-langer

sus apellidos, o cuando barajamos un mazo de cartas, estamos realizando un cambio del orden de estos conjuntos que puede ser representado mediante una permutación.

Imaginemos por un instante que tenemos un conjunto de seis elementos: "a", "b", "c", "d", "e", y "f"[18]. Una permutación podría ser la siguiente:

- ✓ "a" se convierte en "c", ("a" → "c")
- ✓ "b" se convierte en "a", ("b" → "a")
- ✓ "c" se convierte en "b", ("c" → "b")
- ✓ "d" se convierte en "f", ("d" → "f")
- ✓ "e" se convierte en "d", ("e" → "d")
- ✓ "f" se convierte en "e", ("f" → "e")

De esta manera, la permutación que denominaremos P, transforma el conjunto ordenado (abcdef) en el conjunto ordenado (cabfde). Una manera de indicar la permutación es haciendo cadenas cíclicas, esto es, por un lado "a" → "c", "c" → "b", "b" → "a", y por otro "d" → "f", "f" → "e", "e" → "d", de forma que tenemos dos ciclos cerrados de tres elementos cada uno de ellos. Podremos por lo tanto expresar la permutación P como:

$$P = (acb)(dfe)$$

Rejewski supo vislumbrar la conexión entre la matemática abstracta y teórica con el mecanismo de funcionamiento de la máquina Enigma a través de las permutaciones, esperando que la teoría de grupos fuera capaz de extraer alguna propiedad sencillamente asociable a la configuración de los rotores, reduciendo en gran medida el enorme número de posibilidades combinatorias de rotores, reflector y clavijero.

La Enigma era una máquina construida para llevar a cabo permutaciones de letras. Si el operario pulsaba una tecla, la señal eléctrica pasaba a través de diferentes elementos de la máquina, representando cada uno de ellos una permutación (ver Figura 12). Primero lo hacía por el clavijero, en el que algunas letras eran intercambiadas. La señal eléctrica seguía su camino hasta el cilindro de entrada que es como un rotor fijo, donde se producía una segunda permutación. A continuación, la señal eléctrica entraba en el sistema de rotores, primero en el derecho (o rápido), después en el central y por último en el izquierdo (o lento). Después la señal rebotaba en el reflector e iniciaba su camino de vuelta en orden inverso hasta encender la bombilla correspondiente a la letra cifrada. Desde un punto de vista meramente formal, podemos representar el camino de la señal eléctrica como el producto de las siguientes permutaciones:

- ✓ S: permutación causada por el clavijero o panel Stecker.
- ✓ H: permutación causada por el cilindro de entrada.
- ✓ N: permutación causada por el rotor derecho.
- ✓ M: permutación causada por el rotor central.
- ✓ L: permutación causada por el rotor izquierdo.
- ✓ R: permutación causada por el reflector.

[18] Con la intención de seguir un esquema de exposición formal, notaremos en mayúsculas a las permutaciones y en minúsculas las letras del alfabeto.

Teoría de Permutaciones

El grupo de las permutaciones de S, siendo $S = \{x_1, x_2, \ldots, x_n\}$ un conjunto finito de n elementos, resulta ser el ejemplo de grupo finito más utilizado en la rama matemática denominada *teoría de grupos*. En 1854, Arthur Cayley demostró que todo grupo es isomorfo a un subgrupo de un grupo simétrico, y si el grupo es finito y tiene orden n, entonces es isomorfo a un subgrupo de S, resultado que pone de manifiesto el poder de unificación característico de la teoría de grupos, al ser capaz de condensar en un único grupo abstracto, todos los grupos provenientes de las distintas áreas de las matemáticas. Por ejemplo, el nacimiento de la teoría de grupos permitió asociar a cada polinomio un grupo de permutaciones de sus raíces, lo que posibilitó establecer los criterios fundamentales para la solubilidad por radicales de dicho polinomio, resultado que se conoce como *teoría de Galois*.

Denominada originalmente *Teoría de Sustituciones*, históricamente fueron muchos los matemáticos que se dedicaron a su estudio, como Euler, Lagrange, Ruffini, Abel, Gauss, Galois, Cayley o Sylow entre otros.

Si X es un conjunto no vacío, decimos que una *permutación* de X es una aplicación biyectiva $\alpha : X \to X$. Denotamos el conjunto de todas las permutaciones de X por S_X.

Si θ es una *permutación* de S, podemos representarla mediante una matriz de correspondencias de la forma

$$\theta = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_{i1} & x_{i2} & \ldots & x_{in} \end{pmatrix}$$

donde $\theta\, x_1 = x_{i1}$, $\theta\, x_2 = x_{i2}$, $\ldots$, $\theta\, x_n = x_{in}$, es decir el elemento x_1 se convierte en el x_{i1}, $\ldots$ De este modo, una permutación del conjunto S puede ser representada sin ambigüedad por una permutación del conjunto $\{1, 2, \ldots, n\}$. El conjunto de estas permutaciones se denota por S_n y se denomina *Grupo simétrico de grado n*. Se demuestra que para $n \geq 3$, S_n no es abeliano. La correspondencia descrita es claramente una aplicación biyectiva, ya que podemos encontrar una aplicación inversa θ^{-1} de modo que su composición genera la aplicación identidad ($\theta \circ \theta^{-1} = I$). Veamos un ejemplo:

$$\theta = \begin{pmatrix} a & b & c & d & e & f \\ c & a & b & d & e & f \end{pmatrix};\ \theta^{-1} = \begin{pmatrix} c & a & b & d & e & f \\ a & b & c & d & e & f \end{pmatrix} = \begin{pmatrix} a & b & c & d & e & f \\ b & c & a & d & e & f \end{pmatrix}$$

Cuando se tienen dos permutaciones σ y θ en S_n, el producto $\sigma\theta$ se interpreta como composición de aplicaciones, es decir $\sigma\theta(m) = \sigma(\theta(m))$, para todo $m \in \{1, 2, \ldots, n\}$. Es fácilmente demostrable ver que dicha operación en general no es conmutativa, es decir $\sigma\theta \neq \theta\sigma$. Veamos un ejemplo:

$$\sigma = \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix};\ \theta = \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix}$$

$$\sigma\theta = \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix} \cdot \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ a & d & c & b \end{pmatrix}$$

$$\theta\sigma = \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix} \cdot \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ c & b & a & d \end{pmatrix}$$

El conjunto de elementos $\{1, 2, \ldots, n\}$ que son movidos por una permutación θ, se denota A_θ y se denomina el *soporte de la permutación*.

Teoría de Permutaciones (cont.)

Dos permutaciones σ y θ se dicen que son *disjuntas*, si $A_\sigma \cap A_\theta = \varnothing$. Veamos un ejemplo:

$$\theta = \begin{pmatrix} a & b & c & d & e & f \\ b & c & a & d & e & f \end{pmatrix};\ \sigma = \begin{pmatrix} a & b & c & d & e & f \\ a & b & c & e & f & d \end{pmatrix} \Rightarrow$$

$$\Rightarrow A_\theta = \{a,b,c\} \text{ y } A_\sigma = \{d,e,f\}, \text{ claramente } \sigma \text{ y } \theta \text{ son disjuntas.}$$

TEOREMA.- *Si σ y θ son permutaciones disjuntas en S_n, entonces conmutan, es decir $\sigma\theta = \theta\sigma$.*

Una permutación $\theta \in S_n$ se denomina *ciclo*, si existen elementos $s_1, s_2, \ldots, s_k$ en el conjunto $\{1,2,\ldots,n\}$ tales que:

1. Se tienen las relaciones $\theta(s_1) = s_2$, $\theta(s_2) = s_3$, $\ldots$, $\theta(s_{k-1}) = s_k$, y $\theta(s_k) = s_1$.
2. La permutación θ deja fijo a todos los elementos de $\{1,2,\ldots,n\}$ distintos de los s_i.

Con la finalidad de expresar la permutación anterior, se usa la notación cíclica $\theta = (s_1, s_2, \ldots, s_k)$. Al entero k se le denomina *orden* o *longitud del ciclo*.

TEOREMA.- *Toda permutación es o bien un ciclo, o se puede descomponer como un producto de ciclos disjuntos. Esta descomposición o factorización es única salvo por el orden de los factores.*

Sea $\sigma = \sigma_1\sigma_2\cdots\sigma_t$ un producto de ciclos disjuntos de longitudes respectivas $m_1, m_2, \ldots, m_t$. El orden de la permutación σ es el $m.c.m(m_1, m_2, \ldots, m_t)$.

Sea $\sigma = (i_1, i_2, \ldots, i_m)$ un ciclo de longitud m. Entonces $\sigma^{-1} = (i_m, \ldots, i_2, i_1)$ también es un ciclo de longitud m.

Sea $\sigma = \sigma_1\sigma_2\cdots\sigma_t$ un producto de ciclos disjuntos de longitudes respectivas $m_1, m_2, \ldots, m_t$. Entonces $\sigma^{-1} = \sigma_1^{-1}\sigma_2^{-1}\cdots\sigma_t^{-1}$.

Un ciclo de longitud 2 se denomina *transposición*.

TEOREMA.- *Toda permutación se puede descomponer como un producto de transposiciones. Dicha descomposición no es única.*

TEOREMA.- *Sea la permutación $\theta \in S_n$. Entonces θ no puede ser descompuesta como un producto de un número par e impar de transposiciones simultáneamente.*

Dos permutaciones σ y θ en S_n se consideran *conjugadas*, si existe otra permutación $\varphi \in S_n$ tal que

$$\theta = \varphi\sigma\varphi^{-1}$$

Sea σ una permutación cuya descomposición en producto de ciclos disjuntos tiene m_1 ciclos de longitud 1, m_2 ciclos de longitud 2, y en general m_k ciclos de longitud k, se denomina *tipo* o *estructura de ciclos* de la permutación σ al producto formal $1^{m_1}2^{m_2}\cdots k^{m_k}$.

TEOREMA.- *Dos permutaciones son conjugadas si y sólo sí son del mismo tipo.*

Veamos un ejemplo. Consideremos las permutaciones expresadas en su notación cíclica $\sigma = (bf)(ac)(deg)$ y $\theta = (af)(bd)(ceh)$ de S_8. Como vemos ambas poseen una estructura cíclica idéntica. Para definir φ basta poner ambas permutaciones una encima de otra, obteniendo ("h" no aparece en σ, ni "g" en θ, por lo que $\varphi(h) = g$):

$$\begin{matrix} \sigma = (bf)(ac)(deg) \\ \theta = (af)(bd)(ceh) \end{matrix} \Rightarrow \varphi = \begin{pmatrix} a & b & c & d & e & f & g & h \\ b & a & d & c & e & f & h & g \end{pmatrix} \Rightarrow \varphi\sigma\varphi^{-1} = \theta$$

De la misma manera, la señal eléctrica en su camino de vuelta, volvía a sufrir nuevas permutaciones, de forma que si por ejemplo el rotor lento (o izquierdo) provocaba una permutación L cuando la señal iba de derecha a izquierda hasta llegar al reflector, dicho rotor introduciría una permutación inversa a L, que denominaremos L^{-1}, en el camino de vuelta de dicha señal cuando va de izquierda a derecha. Del mismo modo, ocurre con el resto de elementos, teniéndo así las permutaciones M^{-1}, N^{-1}, H^{-1}, S^{-1}, que resultan ser las permutaciones inversas de M, N, H y S respectivamente.

Si llamamos I al camino de ida de la señal eléctrica, y V al camino de vuelta de la misma, podremos expresar se recorrido tal y como representa la Tabla 8.

Tabla 8. Permutación total producida.

Sentido	Elemento que atraviesa	Permutación Total
I	Clavijero	S
I	Cilindro de entrada	SH
I	Rotor drcho.	SHN
I	Rotor central	SHNM
I	Rotor izq.	SHNML
	Reflector	SHNMLR
V	Rotor izq.	$SHNMLRL^{-1}$
V	Rotor central	$SHNMLRL^{-1}M^{-1}$
V	Rotor drcho.	$SHNMLRL^{-1}M^{-1}N^{-1}$
V	Cilindro de entrada	$SHNMLRL^{-1}M^{-1}N^{-1}H^{-1}$
V	Clavijero	$SHNMLRL^{-1}M^{-1}N^{-1}H^{-1}S^{-1}$

Por lo tanto, el efecto neto de pulsar una tecla viene representado por la permutación compuesta $SHNMLRL^{-1}M^{-1}N^{-1}H^{-1}S^{-1}$, o lo que es lo mismo, $(SHNML)\,R\,(SHNML)^{-1}$, es decir cualquier permutación global de Enigma se traduce en una permutación conjugada del reflector.

El reflector era un "medio rotor". Tenía únicamente 26 contactos en su lado derecho. Internamente, los 26 contactos estaban conectados con cables por parejas, de tal manera que la permutación resultante del reflector consistía en 13 transposiciones disjuntas. Los alemanes utilizaron el mismo tipo de reflector para todos los modelos de la Enigma, el cual era completamente desconocido para los polacos. La permutación provocada por el reflector era la siguiente:

$$R = (ae)(bj)(cm)(dz)(fl)(gy)(hx)(iv)(kw)(nr)(op)(pu)(st)$$

De esta manera, como la permutación global de Enigma debe ser del mismo tipo que la provocada por el reflector ya que son conjugadas (ver pág. 82), dicha permutación global puede descomponerse siempre en el producto de 13 transposiciones disjuntas. Sin embargo, se ha de enfatizar el hecho de que cuando el operario pulsaba una tecla, el rotor derecho (o rápido) giraba, y únicamente tras el giro se cerraba el circuito eléctrico. Este hecho llevó a Rejewski a tomar en consideración una nueva permutación que transforma cualquier letra en la siguiente, es decir $a \to b$, $b \to c$, etc. Rejewski denominó a esta permutación P, y es igual a:

$$P = (abcdefghijklmnopqrstuvwxyz)$$

que utilizando la notación de ciclos representada anteriormente, significa que "a" se convierte en "b", "b" se convierte en "c", y así sucesivamente. Por lo tanto cuando el rotor derecho gira, se tiene que se aplica la permutación P, luego la N y después la inversa de P, es decir PNP^{-1}. Cuando la señal realiza el camino de vuelta, la permutación será justo la inversa, es decir $P^{-1}N^{-1}P$.

En segundo lugar, a medida que el operario pulsaba por segunda vez una tecla cualquiera,

el rotor derecho giraba otra vez, sufriendo la señal entrante la permutación $PPNP^{-1}P^{-1}$, o lo que es lo mismo P^2NP^{-2}, y la saliente la inversa de ésta, es decir $P^{-2}N^{-1}P^2$.

También habrá que considerar que cada vez que finalice un ciclo completo el rotor derecho, el central girará una posición, y completado el rotor central su ciclo, entonces girará el rotor izquierdo una posición. Este hecho obliga a considerar dichos movimientos a la hora de formalizar la permutación global. Llegado a este punto, Rejewski se encargó de analizar las relaciones matemáticas de las seis primeras letras cifradas. Si imaginamos los rotores y el clavijero en una disposición concreta, es muy probable que tras pulsar seis teclas, ni el rotor central ni el izquierdo giraran, ya que la probabilidad de que la pulsación de seis teclas hiciera girar el rotor central era de $6/26$, mientras que la de que gire el izquierdo es aún muchísimo menor. Por lo tanto no es descabellado considerar esta hipótesis de partida.

Cualquiera que sea la tecla que se pulsara, la señal eléctrica que generaba daba lugar a la siguiente permutación, que denominaremos A:

$$A = SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1} = (SHPNP^{-1}ML)\,R\,(SHPNP^{-1}ML)^{-1} \quad (1)$$

En una segunda pulsación, el nuevo movimiento del rotor derecho, provocaba que la permutación de A fuera alterada. Por lo tanto, la pulsación de una segunda tecla haría que la señal sufriera la permutación B:

$$B = SHP^2NP^{-2}MLRL^{-1}M^{-1}P^2N^{-1}P^{-2}H^{-1}S^{-1} = (SHP^2NP^{-2}ML)\,R\,(SHP^2NP^{-2}ML)^{-1} \quad (2)$$

Del mismo modo expresaríamos una tercera, cuarta, quinta y sexta pulsaciones, que llamaremos C, D, E y F respectivamente, resultando:

$$C = SHP^3NP^{-3}MLRL^{-1}M^{-1}P^3N^{-1}P^{-3}H^{-1}S^{-1} = (SHP^3NP^{-3}ML)\,R\,(SHP^3NP^{-3}ML)^{-1} \quad (3)$$

$$D = SHP^4NP^{-4}MLRL^{-1}M^{-1}P^4N^{-1}P^{-4}H^{-1}S^{-1} = (SHP^4NP^{-4}ML)\,R\,(SHP^4NP^{-4}ML)^{-1} \quad (4)$$

$$E = SHP^5NP^{-5}MLRL^{-1}M^{-1}P^5N^{-1}P^{-5}H^{-1}S^{-1} = (SHP^5NP^{-5}ML)\,R\,(SHP^5NP^{-5}ML)^{-1} \quad (5)$$

$$F = SHP^6NP^{-6}MLRL^{-1}M^{-1}P^6N^{-1}P^{-6}H^{-1}S^{-1} = (SHP^6NP^{-6}ML)\,R\,(SHP^6NP^{-6}ML)^{-1} \quad (6)$$

Para poder resolver el sistema de ecuaciones representado por las seis ecuaciones que equivalen a las seis pulsaciones de teclas en Enigma, Rejewski necesitaba conocer N, M, L y R, ya que de este modo podría averiguar la configuración del cableado de los rotores y el reflector. De manera adicional necesitaba conocer S y H, es decir, las permutaciones del clavijero y del cilindro de entrada, ya que estos eran desconocidos. Sin embargo lejos de resultar un sistema compatible determinado, Rejewski partía con el gran handicap de desconocer las permutaciones A, B, C, D, E y F. Para que éstas fueran conocidas, sería necesario conocer el texto llano junto con el cifrado, y las estaciones de radioescucha únicamente proporcionaban el segundo.

Aparentemente las investigaciones de Rejewski se situaban en un callejón sin salida, sin embargo, no estamos ante un personaje común, de ahí la genialidad de sus resultados. En conocimiento de la Enigma comercial, Rejewski basó sus investigaciones en tres resultados fundamentales a la hora de obtener la configuración interna del cableado de los rotores, esto es equivalente a determinar N, M, L y R.

El primer resultado proviene de una propiedad de la Máquina Enigma denominada *reciprocidad*, de tal forma que se puede demostrar que $A^{-1} = A$, $B^{-1} = B$, etc. Esto significa que para una configuración concreta de los diferentes elementos de la máquina Enigma, si pulsamos "s" y obtenemos "r", también podemos pulsar "r" y obtenemos "s".

El segundo resultado crucial consistió en aprovechar una de las debilidades ocasionadas por la repetición de las claves. En primer lugar el operador que iba a emitir un mensaje cifrado debía

consultar el libro de claves con el fin de obtener la clave maestra (la que iban a utilizar todos los operadores ese día) que representaban la configuración inicial de partida de los rotores. Imaginemos que "sol" es dicha clave maestra. A continuación el operador elegía una "clave de sesión"[19] para cifrar el mensaje. Imaginemos que dicha clave es "oro". El proceso entonces era el siguiente:

1. El operador cifraba las letras "oro" con la clave "sol" (es decir, ponía los rotores de forma que en la ventana superior de la máquina apareciera "s-o-l"), obteniendo en el panel luminoso "buu".
2. Entonces el operador colocaba los rotores en la posición representada por las letras "o-r-o", y procedía a cifrar el mensaje.
3. El operador enviaba "buu" junto con el mensaje cifrado.

El operador que recibía el mensaje realizaba la operación inversa. Tomaba el libro de claves, colocaba su máquina con los rotores en la posición "s-o-l", tecleaba "buu" y obtenía en el panel luminoso la clave del mensaje "o-r-o". Una vez hecho eso, colocaba los rotores en la posición "o-r-o" y tecleaba el mensaje cifrado obteniendo en el panel luminoso el texto plano.

Sin embargo, debido a que los mensajes se transmitían, entre otros medios, por radio, existía la posibilidad de que se produjeran errores de transmisión ocasionados por perturbaciones atmosféricas, además de considerar que en ocasiones se producían errores de transcripción de los operadores. Con el fin de evitar estos posibles fallos, los alemanes establecieron la norma de que la clave del mensaje debía ser cifrada dos veces. Esto es, en el caso que hemos visto, la máquina se ponía en la posición "s-o-l", y se tecleaba "o-r-o-o-r-o", obteniéndose "buurqr". De este modo el receptor del mensaje cifrado recuperaría la clave del mensaje repetida, o de lo contrario, tendría así dos posibilidades para ensayar y obtener el mensaje descrifrado.

El hecho de repetir la clave del mensaje dos veces, significó encontrar un punto de partida para comenzar el ataque a Enigma. Las repeticiones son un filón para los criptoanalistas y Rejewski no dejó pasar inadvertida la sutil relación que existía en el cifrado de la clave del mensaje. Imaginemos que alguien interceptase el mensaje con la clave de mensaje cifrada "buurqr". Está claro que existe una relación entre las letras primera y cuarta, esto es "b" y "r". Nosotros sabemos que equivalen a la letra "o", pero el criptoanalista sabe que tras pulsar una tecla desconocida (llamémosla "x") obtiene "b", y que cuando pulsa en cuarta posición, obtiene "r". Haciendo uso del lenguaje de permutaciones explicado al principio de esta sección, la permutación A nos indica de qué manera cambian las letras cuando se pulsa una tecla por primera vez, y D lo mismo pero cuando se pulsa una letra por cuarta vez. Esto es equivalente a considerar:

$$A(x) = b;\ D(x) = r$$

El criptoanalista desconoce "x", pero en virtud de la propiedad recíproca de Enigma, sabe que A(b) = x. Puesto que A transforma "b" en "x", y D transforma "x" en "r", la permutación compuesta AD (es decir, la que se obtiene de aplicar A, y después D) nos transforma "b" en "r":

$$AD(b) = r$$

Por lo tanto el criptoanalista desconocía las permutaciones A y D, pero sí que conocía parte de la permutación AD, únicamente considerando el resultado de cifrar la clave del mensaje dos veces ("buurqr") y establecer la relación entre la primera letra y la cuarta. A lo largo del día se interceptaría una cantidad suficiente de mensajes para establecer más indicativos. Si consideramos los siguientes indicativos de un día dado:

[19] También llamada clave del mensaje.

1: (gtaasw)	2: (edjwmv)	3: (ngevjt)	4: (rdjdmv)
5: (cdjqmv)	6: (ntwvso)	7: (dldjbn)	8: (qlaxbw)
9: (zlapbw)	10 (udekmt)	11: (pgjejv)	12: (qtsxsx)

donde se puede ver las siguientes relaciones "g" $\to$ "a", "e" $\to$ "w", "n" $\to$ "v", "r" $\to$ "d", ... En general interceptando unos ochenta mensajes diarios, el criptoanalista podía construirse la siguiente tabla de relaciones:

1ª letra:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
4ª letra:	i	r	q	j	w	c	a	y	o	z	f	b	t	v	u	e	x	d	g	h	k	s	m	n	l	p

obteniendo así la permutación completa AD, ordenada por la longitud de sus ciclos:

$$AD = (aioukfcqxnvsg)(brdjzpewmthyl)^{20}$$

De igual forma, el criptoanalista podría realizar un análisis idéntico con la segunda y quinta letras de la clave del mensaje cifrado y con la tercera y la sexta, conociendo así las permutaciones compuestas BE y CF respectivamente. No olvide el lector que el fin último de todo este "engendro" es lograr conocer el cableado de los rotores y del reflector, o lo que es lo mismo conocer las permutaciones N, M, L y R.

Veamos cómo llevó a cabo Rejewski esta proeza matemática. Para llegar al fin último antes descrito, tuvo que probar innumerables combinaciones, propiedades, teoremas y leyes. En primer lugar, se construía, gracias a los mensajes interceptados, las permutaciones compuestas AD, BE y CF.

Rejewski centró su atención en el hecho de que la permutación S cambiaba únicamente seis pares de letras, mientras que las restantes catorce letras permanecían invariables. Con el fin de aligerar la notación matemática, denominaremos Q a la permutación producida por el reflector y los rotores central y derecho, es decir $Q = MLRL^{-1}M^{-1}$. De este modo las permutaciones resultan:

$$A = SHPNP^{-1}QPN^{-1}P^{-1}H^{-1}S^{-1}$$

$$B = SHP^2NP^{-2}QP^2N^{-1}P^{-2}H^{-1}S^{-1}$$

$$C = SHP^3NP^{-3}QP^3N^{-1}P^{-3}H^{-1}S^{-1}$$

$$D = SHP^4NP^{-4}QP^4N^{-1}P^{-4}H^{-1}S^{-1}$$

$$E = SHP^5NP^{-5}QP^5N^{-1}P^{-5}H^{-1}S^{-1}$$

$$F = SHP^6NP^{-6}QP^6N^{-1}P^{-6}H^{-1}S^{-1}$$

$$AD = SHPNP^{-1}QPN^{-1}P^3NP^{-4}QP^4N^{-1}P^{-4}H^{-1}S^{-1}$$

$$BE = SHP^2NP^{-2}QP^2N^{-1}P^3NP^{-5}QP^5N^{-1}P^{-5}H^{-1}S^{-1}$$

$$CF = SHP^3NP^{-3}QP^3N^{-1}P^3NP^{-6}QP^6N^{-1}P^{-6}H^{-1}S^{-1}$$

Con la representación anterior, Rejewski conocía las permutaciones compuestas AD, BE y CF, y desconocía las permutaciones H, S, N y Q. En un primer intento, consideró que H, es decir la permutación que representa el cilindro de entrada, debiera ser la misma para el modelo militar que para el modelo comercial. Aunque esta suposición resultó ser totalmente errónea, consideremos como punto de partida que la suponemos conocida.

[20] Obsérvese que la permutación resultante se puede descomponer en un número par de ciclos de idéntica longitud cada pareja. Este hecho no pasó desapercibido para Rejewski, que lo denominó *característica*.

El siguiente paso consistía en determinar A, B, C, D, E y F, considerando únicamente como punto de partida las permutaciones compuestas AD, BE y CF, para lo cual Rejewski utilizó varios teoremas.

TEOREMA. (SOBRE EL PRODUCTO DE TRANSPOSICIONES) *Si dos permutaciones del mismo tipo están factorizadas únicamente como producto de transposiciones disjuntas, entonces su producto contiene un número par de ciclos disjuntos de la misma longitud.*

Rejewski argumentó su demostración así:

Si $X = (a_1\, a_2)\,(a_3\, a_4)\,(a_5\, a_6)\,\ldots\,(a_{2k-3}\, a_{2k-2})\,(a_{2k-1}\, a_{2k})$,

e $Y = (a_2\, a_3)\,(a_4\, a_5)\,(a_6\, a_7)\,\ldots\,(a_{2k-2}\, a_{2k-1})\,(a_{2k}\, a_1)$,

entonces $XY = (a_1\, a_3\, a_5\,\ldots\, a_{2k-3}\, a_{2k-1})\,(a_{2k}\, a_{2k-2}\,\ldots\, a_6\, a_4\, a_2)$.

y continuaba [5, p. 262]:

> *"Si, de este modo, no hemos agotado todas las letras de la permutación, continuaremos nuestro procedimiento hasta que lo hayamos hecho."*

La composición de permutaciones es una actividad muy común en álgebra abstracta, pero lo que realmente necesitaba Rejewski era factorizar las permutaciones AD, BE y CF.

TEOREMA. (OPUESTO AL TEOREMA SOBRE EL PRODUCTO DE TRANSPOSICIONES) *Si en cualquier permutación de grado par aparecen un número par de ciclos disjuntos de la misma longitud, entonces la permutación puede ser considerada como un producto de dos permutaciones consistentes en transposiciones disjuntas.*

Hay que poner de manifiesto que las permutaciones AD, BE y CF satisfacen las condiciones de este teorema. Su demostración es inmediata a partir de lo indicado anteriormente.

Dada $XY = (a_1\, a_3\, a_5\,\ldots\, a_{2k-3}\, a_{2k-1})\,(a_{2k}\, a_{2k-2}\, a_5\,\ldots\, a_6\, a_4\, a_2)$,

entonces podemos expresar: $X = (a_1\, a_2)\,(a_3\, a_4)\,(a_5\, a_6)\,\ldots\,(a_{2k-3}\, a_{2k-2})\,(a_{2k-1}\, a_{2k})$,

e $Y = (a_2\, a_3)\,(a_4\, a_5)\,(a_6\, a_7)\,\ldots\,(a_{2k-2}\, a_{2k-1})\,(a_{2k}\, a_1)$

TEOREMA. *Los elementos que forman parte de una única transposición, bien sea de la permutación* X*, o bien sea de la permutación* Y*, forman parte siempre de dos ciclos distintos de la permutación compuesta* XY*.*

TEOREMA. *Si dos elementos que se encuentran en dos ciclos diferentes de igual longitud de la permutación* XY*, pertenecen a la misma transposición, entonces las letras adyacentes a ellas (una por la derecha y la otra por la izquierda) también pertenecen a la misma transposición.*

TEOREMA. (SOBRE LAS PERMUTACIONES CONJUGADAS) *Si* $K(i) = j$*; esto es,* $K = (\ldots\, i\, j\,\ldots)$*; entonces* $T^{-1}KT = (\ldots\, T(i)\, T(j)\,\ldots)$ *Nótese que esto implica que* $K = (\ldots\, i\, j\,\ldots)$ *y* $T^{-1}KT = (\ldots\, T(i)\, T(j)\,\ldots)$ *tiene idéntica descomposición en ciclos disjuntos.*

Para la demostración, Rejewski consideró que $T\,(T^{-1}KT)\,(i) = KT\,(i) = T(K(i)) = T(j)$. En particular, esto significa que la introducción de las permutaciones puede ser ordenada de forma que

$$K = (\ldots\ldots\, i\, j\,\ldots\ldots)$$

$$T^{-1}KT = (\ldots\, T(i)\, T(j)\,\ldots)$$

que describe la permutación T.

Con respecto a las permutaciones A, B y C, se podían obtener unas cuantas soluciones (hasta una docena), de las cuales sólo una era la correcta. En este punto, no se podría saber a priori cuál debiera ser la solución correcta. Sin embargo, en ocasiones se interceptaban mensajes transmitidos por operarios no demasiado "cuidadosos" que habían cifrado dichos comunicados con claves de mensaje relativamente sencillas del tipo "j-j-j", "z-z-z", u otras como "q-w-e", "b-n-m" que indicaban teclas dispuestas consecutivamente en el teclado de la Enigma. Este hecho podía resultar un punto de apoyo para poder determinar cuál de las soluciones para A, B, y C era la correcta.

En este punto del proceso criptoanalítico, Rejewski no conocía aún siquiera si las ecuaciones que dan A, B, C, D, E, y F resultaban ser despejables para obtener S, N y Q. Podían resolverse en el caso de que el criptoanalista tuviera a su disposición los mensajes de dos días diferentes (en los cuales las conexiones del clavijero fueran diferentes pero los rotores estuvieran en las mismas posiciones), pero el enorme número de distintas posiciones y orientaciones de los rotores hacían de este un problema inviable en la práctica.

Es aquí cuando Rejewski se apoyo en los documentos proporcionados por el espía alemán Hans Thilo Schmidt, que llegaron a sus manos de manera inesperada el 9 de diciembre de 1932. Además de las permutaciones AD, BE, CF (obtenidas mediante radioescucha) y las A, B, C, D, E y F (deducidas por los criptoanalistas polacos), ahora se conocía también la permutación S, y dejaba de ser por lo tanto una incógnita, y consecuentemente resultaba despejable, junto con H (recuerde el lector que hemos partido de la hipótesis de que H es conocida, aunque después se demuestre que no es cierto), resultando:

$$H^{-1}S^{-1}ASH = PNP^{-1}QPN^{-1}P^{-1}$$

$$H^{-1}S^{-1}BSH = P^{2}NP^{-2}QP^{2}N^{-1}P^{-2}$$

$$H^{-1}S^{-1}CSH = P^{3}NP^{-3}QP^{3}N^{-1}P^{-3}$$

$$H^{-1}S^{-1}DSH = P^{4}NP^{-4}QP^{4}N^{-1}P^{-4}$$

$$H^{-1}S^{-1}ESH = P^{5}NP^{-5}QP^{5}N^{-1}P^{-5}$$

$$H^{-1}S^{-1}FSH = P^{6}NP^{-6}QP^{6}N^{-1}P^{-6}$$

donde únicamente se tienen las incógnitas N y Q. Rejewski definió las permutaciones U, V, W, X, Y y Z del siguiente modo:

$$U = P^{-1}H^{-1}S^{-1}ASHP = NP^{-1}QPN^{-1}$$

$$V = P^{-1}H^{-1}S^{-1}BSHP = NP^{-2}QP^{2}N^{-1}$$

$$W = P^{-1}H^{-1}S^{-1}CSHP = NP^{-3}QP^{3}N^{-1}$$

$$X = P^{-1}H^{-1}S^{-1}DSHP = NP^{-4}QP^{4}N^{-1}$$

$$Y = P^{-1}H^{-1}S^{-1}ESHP = NP^{-5}QP^{5}N^{-1}$$

$$Z = P^{-1}H^{-1}S^{-1}FSHP = NP^{-6}QP^{6}N^{-1}$$

A continuación, Rejewski calculó las permutaciones compuestas UV, VW, WX, XY e YZ, resultando:

$$UV = NP^{-1}[QP^{-1}QP]PN^{-1}$$

$$VW = NP^{-2}[QP^{-1}QP]P^2N^{-1}$$

$$WX = NP^{-3}[QP^{-1}QP]P^3N^{-1}$$

$$XY = NP^{-4}[QP^{-1}QP]P^4N^{-1}$$

$$YZ = NP^{-5}[QP^{-1}QP]P^5N^{-1}$$

Despejó el factor $[QP^{-1}QP]$ de una de las anteriores ecuaciones y lo introdujo en las otras cuatro, obteniendo:

$$VW = NP^{-1}N^{-1}UVNPN^{-1}$$

$$WX = NP^{-1}N^{-1}VWNPN^{-1}$$

$$XY = NP^{-1}N^{-1}WXNPN^{-1}$$

$$YZ = NP^{-1}N^{-1}XYNPN^{-1}$$

donde la única incógnita resulta ser la permutación NPN^{-1}. En un día normal, se puede estimar que había del orden de varias decenas de soluciones para VW, WX, XY e YZ, pero lo más importante de todo ello es que estas permutaciones mantenían una estructura común. De no ser así, esto únicamente podía significar dos cosas, bien que se había cometido un error ese día, o bien que ese día en particular el movimiento del rotor lento (situado más a la izquierda) inducía movimiento en el rotor medio para alguna de las posiciones, por lo que era necesario en este caso volver a empezar con otro día. Utilizando el mismo método empleado para obtener A, B, C, D, E y F partiendo de AB, CD, y EF, puede determinarse NPN^{-1} partiendo de XW, obteniendo varias posibles soluciones. También se pueden obtener distintas soluciones a partir de la ecuación WX, y únicamente existe solución idéntica para las ecuaciones VW y WX. De igual forma, se puede obtener N a partir de NPN^{-1}, para lo cual bastaba aplicar una cualquiera de las 26 posibles permutaciones P que existen para obtener la N, que resultaba ser la permutación inducida por el cableado del rotor que estaba en la posición lenta de ese día.

Sin embargo el lector no debe olvidar que Rejewski supuso erróneamente una hipótesis que luego resultó ser falsa. Consideró que la permutación H era la misma que la de la Enigma comercial: los cables iban de las teclas al cilindro de entrada en el orden del teclado qwert … Sin embargo, al probarlo con la Enigma militar, el método no funcionaba. La permutación H era otra. De hecho, los alemanes podían haber incluido en H cualquier permutación que les hubiese dado la gana, y el número de permutaciones distintas con 26 elementos es inmensa. Pero Rejewski logró dar con la clave de este problema a finales de 1932 o principios de 1933, considerando que los alemanes, tan ordenados y metódicos, tal vez hubieran considerado H como la permutación alfabética. Es decir, las teclas se unirían mediante cables al cilindro de entrada siguiendo un orden abcdef … Rejewski probó dicha hipótesis, experimentando a buen seguro un sentimiento de triunfo al observar que resultaba ser correcta. De hecho, se comenta que cuando en verano de 1939 los polacos compartieron sus descubrimientos con franceses y británicos en una reunión a las afueras de Varsovia de la que posteriormente hablaremos, la primera pregunta del reputado criptólogo británico Dillwyn Knox a Rejewski fue: "*¿cuál es la permutación del cilindro de entrada?*". Al escuchar la trivialidad de la respuesta, parece que Knox montó en cólera por no haber considerado una posibilidad tan obvia.

3.4. 3ª Etapa. La amenaza de la invasión y la búsqueda de aliados

Rejewski repitió el mismo proceso con las relaciones que existían entre los caracteres 2º y 5º, y los 3º y 6º de la clave de los mensajes. En este punto, llegó a la conclusión que estas cadenas

de caracteres eran una consecuencia directa de la configuración y disposición de los rotores y que el clavijero influía únicamente en que las letras cambiaban, es decir variaban las permutaciones, pero la estructura cíclica de éstas permanecía invariable aún cuando la configuración del clavijero cambiara. Por lo tanto el número de ciclos y sus longitudes dependía única y exclusivamente del orden en el que estaban dispuestos los rotores y de su configuración inicial de partida. Rejewski denominó *característica* a este número de ciclos y longitudes. El número de características que los polacos tenían que estudiar se reducía por lo tanto drásticamente de 10^{16} a 105.456, o lo que es lo mismo $6 \times 26 \times 26 \times 26$, que siendo aún un número grande, sí que permitía abordar manualmente el ataque al código de Enigma. Con respecto a las *características*, Rejewski comentaba [19, p. 217]:

> *"Esta estructura es la más característica, y aunque su representación difiere cada día, su rasgo es siempre el mismo: en cada línea los ciclos de idéntica longitud aparecen siempre por parejas. Observando el papel que dicha estructura jugaba, la denominé estructura característica, o simplemente la característica de un día determinado."*

Figura 18. Palacio Sajón en Varsovia (entre 1930 y 1935).[21]

Rejewski pasó algo más de un año recopilando lo que denominó *catálogo de características*, y gracias a sus descubrimientos, los polacos fueron capaces de construir un catálogo para cada configuración de rotores. Con la ayuda del libro de claves proporcionado por Schmidt, se pudo llevar a cabo con éxito la tarea de desencriptación. Schmidt había proporcionado los libros con las claves de septiembre y octubre (es decir de dos trimestres diferentes), lo que permitió deducir la configuración de dos rotores. Bastaba esperar hasta el comienzo del año 1933, para que los polacos pudieran obtener la configuración del tercer rotor y deducir así la del reflector. A últimos de enero de 1933, el código de la Enigma había sido descubierto.

Tras el incendio del Reichstag a últimos de febrero de 1933, y con la subida al poder de lo que después se convertiría en el régimen nazi, los polacos del BS4, a petición de Rejeski,

[21] El Palacio Sajón sirvió de cuartel general de la comandancia polaca, donde en 1932 los polacos consiguieron romper el código Enigma por primera vez. En la imagen se puede ver la estatua ecuestre del Príncipe Józef Poniatowski. La galería contiene la Tumba del Soldado Desconocido en memoria a los soldados polacos caídos en combate durante la 1ª Guerra Mundial (1914-1918) y la guerra contra la Unión Soviética (1918-1920). Durante la 2ª Guerra Mundial gran parte del edificio y alrededores (la Plaza Jósef Pilsudski o el Palacio Brühl) fueron totalmente destruidos. http://www.herder-institut.de/warschau/ausschnitt_04/ausschnitt-04_01.html

consideraron oportuno reforzar las tareas criptológicas, por lo que la plantilla se aumentó a 6 operarios de descifrado, entre ellos Jerzy Ròżycki y Henry Zygalski, los cuales habían sido minuciosamente entrenados con anterioridad.

Con el fin de mecanizar la tarea de encontrar el catálogo adecuado para una configuración determinada, los polacos construyeron unas réplicas de la Enigma militar. Antoni Palluth, Edward Fockczyński, y los hermanos Ludomir y Leonard Danilewicz, ingenieros y directores de la compañia de Radiomanufactura AVA, encargada de surtir al Biuro Szyfrów todo tipo de material tecnológico para comunicaciones, acometieron la fabricación de dichas réplicas de Enigma que se construyeron casi artesanalmente durante la noche para mantener el asunto en completo secreto. Un operario de total confianza llevaba a cabo el ensamblaje mecánico de dicha máquina. AVA que había sido fundada en 1929 y tenía sus oficinas centrales en el número 34 de la calle Nowy Swiat en Varsovia, recibió el encargo de la comandancia general polaca para llevar a cabo la construcción de 15 de estas réplicas a principios de febrero de 1933, y concluyó la entrega de dicho encargo a mediados de 1934.

Durante los primeros meses de la primera victoria polaca sobre Enigma, los operarios tenían que obtener la configuración inicial de manera prácticamente manual, de forma que giraban los rotores metálicos con 17.576 posibilidades, habiendo 263 posibles configuraciones. Esta tarea resultaba, además de tediosa, profundamente dolorosa puesto que los dedos de los criptólogos llegaban a sangrar, ya que no era posible que éstos delegaran dicha actividad en el personal técnico. Fue entonces cuando Rejewski, con ayuda de Antoni Palluth, inventó el "ciclómetro", un mecanismo que permitió manejar a los criptólogos polacos un catálogo de 105.456 características. El ciclómetro era una máquina Enigma doble (con seis ruedas y dos reflectores) pero en la que el segundo juego de ruedas se ajustaba automáticamente tres posiciones con respecto al primero. El efecto que se conseguía es el mismo que si se pulsase una tecla en una máquina convencional, es decir, se teclean otras dos y luego se teclea la misma otra vez, únicamente que con el ciclómetro sólo era necesario teclear una vez, en lugar de cuatro. Durante tres años las comunicaciones encriptadas con Enigma resultaron ser un libro abierto para los polacos. Sin embargo, para su desgracia, el 1 de noviembre de 1937, los alemanes cambiaron el reflector de las máquinas, lo que significó tener que reconstruir nuevamente el catálogo.

En enero de 1938, la comandancia general polaca llevó a cabo una investigación interna con el fin de cuantificar la eficacia del trabajo del BS4. Los resultados del estudio realizado durante dos semanas fueron bastante concluyentes, ya que ponían de manifiesto que el equipo formado por diez individuos (entre criptólogos y operadores) era capaz de descifrar alrededor del 75 % de todos los mensajes interceptados, lo que daba una idea del éxito de los polacos, considerando que parte de los mensajes interceptados resultaban en ocasiones ilegibles o incompletos debido a las interferencias.

El 27 de Mayo de 1938, los polacos invitaron a Gustave Bertrand, el comandante de la inteligencia francesa que ya les había proporcionado los documentos de H. T. Schmidt, para que éste conociera el nuevo centro en Pyry, en los bosques de Kabackie, unos diez kilómetros al sur de Varsovia, cuyo nombre en clave era "Wicher" (Vendaval), donde además le mostrarían los logros conseguidos por el BS4.

Para desdicha de los polacos, el 15 de septiembre de 1938 los alemanes volvieron a dar una vuelta de tuerca con el fin de buscar la optimización de la Enigma. Esta vez los cambios introducidos dejaron inservibles por completo todos los métodos de desencriptación llevados a cabo hasta el momento. Dichos cambios consistían básicamente en que tanto la configuración de los rotores, como las claves de cada mensaje eran elegidas libremente por el operador en cuestión. Las tres letras de la clave se transmitían de forma abierta en la cabecera del mensaje y éstas precedían a las seis letras que resultaban del doble cifrado de la clave del mensaje. Por ejemplo, la cabecera "FDA GHRMER" indicaba que la configuración de los rotores era FDA (con el orden de los rotores establecido previamente en los libros por el alto mando nazi, y que en aquel momento cambiaba todos los días), y las otras seis letras correspondían al cifrado

El Ciclómetro

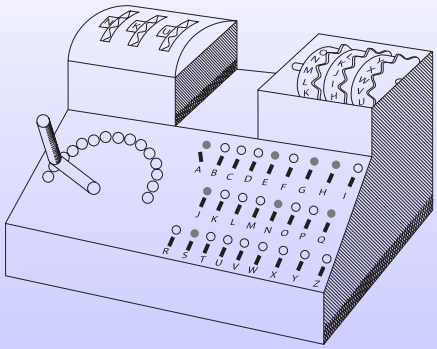


Figura 19. Diseño del Ciclómetro.

Con el fin de automatizar la tarea de confeccionar el catálogo de características, Rejewski y los polacos del BS4 construyeron el ciclómetro. La Figura 19 muestra una reproducción de dicho aparato realizada a partir de un diseño original del propio Rejewski. Este aparato estaba formado por dos bancos de rotores interconectados entre sí, de forma que el de la derecha iba desplazado tres posiciones con respecto al de la izquierda. Bajo dichos bancos de rotores estaban el panel de lámparas y las palancas, una por cada letra del alfabeto. Cuando una de estas palancas era accionada, una corriente eléctrica atravesaba varias veces ambos bancos de rotores y entonces se encendía un número par de lámparas, que eran las correspondientes a los dos ciclos asociados a la permutación AD. Entonces, accionando otra palanca de una letra no iluminada, se deducían dos ciclos asociados. De este modo se determinaba la descomposición en ciclos disjuntos de AD. Si se variaban entonces el orden de los rotores y sus posiciones iniciales, se calculaban todas las permutaciones AD existentes. Con todo esto, los polacos del BS4 elaboraban el catálogo, ya que las permutaciones BE y CF asociadas a una posición determinada de los rotores coincidían con la AD, sólo que bastaba adelantar los rotores de la derecha del ciclómetro una o dos posiciones respectivamente.

doble de la clave del mensaje. Todo el resto del proceso no sufrió ningún cambio significativo adicional, aunque cabe destacar que por entonces, el número de conexiones del Stecker estaba entre cinco y ocho, y que la configuración del Ringtellung se cambiaba todos los días.

Los cambios introducidos se traducían en una modificación de la configuración de los rotores en cada uno de los mensajes, lo cual a su vez provocaba la modificación de los productos AD, BE y CF, sin embargo, los alemanes continuaban cometiendo el mismo error, que consistía en repetir la clave del mensaje al inicio de cada comunicación. Los polacos aprovecharon esta pequeña debilidad. Con el fin de elaborar el catálogo de características, calcularon 105.456 productos posibles de AD. Pudieron comprobar que el 40 % de estas permutaciones contenían ciclos de longitud 1, y del mismo modo ocurría con los productos BE y CF. Pongamos un ejemplo, supongamos que tenemos tres mensajes interceptados con las siguientes cabeceras:

FDE BWHBXT QSC GJVBJM ZDR WSXTGX

Como podemos observar subrayado se produce la repetición en idénticas posiciones de algunos caracteres. Los británicos acuñarían el término *female* para referirse a dichas repeticiones. El mensaje con la cabecera FDE BWHBXT, indica que la permutación AD correspondiente contiene el ciclo (B). Utilizando la terminología introducida por los británicos, dicha cabecera se expresaba como una 1,4-female. Del mismo modo, en el segundo mensaje con la cabecera QSC GJVBJM, tendríamos una 2,5-female y (J) es un ciclo de la permutación BE, y en el tercer mensaje con la cabecera ZDR WSXTGX tendríamos una 3,6-female y (X) es un ciclo de CF.

Recordemos que las conexiones del Stecker no tenían ninguna influencia en las longitudes de las permutaciones AD, BE y CF, ya que dichas longitudes dependían única y directamente

del orden de los rotores y de sus posiciones iniciales, viniendo determinadas por las diferencias entre las letras del Grundstellung y las del Ringstellung (ver 2.3). Por un lado, el Grundstellung era distinto en cada uno de los mensajes, aunque conocido, sin embargo, el Ringstellung era el mismo en todos los mensajes de un mismo día, aunque desconocido. El objetivo fundamental del trabajo criptológico consistía fundamentalmente en identificar correctamente el orden de cada uno de los rotores y la configuración del anillo de entre las 105.456 posibles configuraciones. Sorprendentemente, este enorme número de posibilidades se reducía en un factor de 0,4 cada vez que aparecía un ciclo de longitud 1, ya que únicamente el 40 % de las permutaciones AD (o bien las BE, o las CF) presentaban este tipo de ciclos unitarios. Si las permutaciones AD, BE y CF eran elegidas de manera aleatoria, la teoría de probabilidades arrojaba un resultado sorprendente, y es que el 11,5 % de las cabeceras de los mensajes presentaban females. De este modo, se necesitaban únicamente doce o trece females entre un centenar de mensajes interceptados para determinar de manera unívoca el orden de los rotores y el Ringstellung.

De forma adicional al trabajo desarrollado por Rejewski, en septiembre de 1938 Zygalski inventó un ingenioso método que proporcionaría a los polacos la posibilidad de descifrar de manera masiva los mensajes cifrados interceptados, ya que determinaba el orden de los rotores y el Ringstellung. El método de las *hojas de Zygalski* o *Netz* (del alemán *Netzverfahren*, "método neto"), rudimentario aunque bastante efectivo, basaba su fundamentación en la aparición de females. Zygalski preparó 6 paquetes de 26 hojas cada uno, donde cada paquete representaba una posible configuración de los rotores (cada uno de los 6 órdenes posibles de los rotores y cada una de las 26 posiciones del rotor izquierdo). En cada una de las hojas se escribía una letra y a continuación se dibujaba una cuadrícula de 51×51 (60×60 cms aprox.) en la que se rotulaban tanto las abscisas como las ordenadas con todas las letras, comenzando por la esquina superior izquierda. Las letras horizontales representan las posiciones del rotor central y las verticales las del derecho, de modo que cada pequeño cuadrado, representaba una permutación con ciclos de una letra correspondiente a esa posición de los rotores, es decir una female. Los cuadrados correspondientes a las 1,4-females se perforaban directamente. Sin embargo las 2,5 y 3,6-females, necesitaban un proceso de "normalización" que consistía básicamente en adelantar su Grundstellung derecho una o dos posiciones respectivamente. Utilizando el ejemplo presentado en la página 92:

$$\text{QSC GJVBJM} \Rightarrow \text{QTC GJVBJM} \qquad \text{ZDR WSXTGX} \Rightarrow \text{ZDT WSXTGX}$$

Realizada la nombrada normalización, se procedía a repetir el proceso para cada orden de los rotores y cada posición del Ringstellung del rotor izquierdo. Fijado el orden de los rotores, se normalizaban de nuevo aquellas females cuyo Grundstellung se tradujera en un avance del rotor central. Pongamos un ejemplo, imaginemos que el orden de los rotores era II-I-III, y que el Grundstellung era SGV. Dicho Grundstellung debía ser normalizado a SHV, ya que la V es la letra que provoca en el rotor III un avance del rotor situado inmediatamente a su izquierda, en este caso el rotor central en el que se encuentra el I. Acto seguido, se seleccionaban el juego de 26 hojas asociadas al orden de rotores establecido, y fijada una letra del Ringstellung del rotor izquierdo, pongamos por ejemplo la letra F, se consideraba el Grundstellung de una primera female. Supongamos que una 1,4-female era RDW. Como $R - F = M$, se escogía la hoja correspondiente a la letra M que servía de patrón básico con el que comenzar a trabajar, y se colocaba sobre una mesa transparente iluminada por debajo. A continuación se tomaba otra 1,4-female, pongamos por ejemplo MYS. Como $M - F = H$, se seleccionaba la hoja correspondiente a H y se colocaba sobre el patrón básico representado por la letra M, pero desplazada 5 pequeños recuadros hacia la derecha (ya que de la Y a la D van 5 letras), y 4 pequeños recuadros hacia abajo (porque de la S a la W van 4 letras). Se repetía la operación con el resto de females, y una vez colocadas todas las hojas se observaba si la luz de la iluminación que había debajo de la mesa transparente traspasaba algún agujero común a todas ellas. Si se habían conseguido una cantidad suficiente de females, el haz de luz atravesaba un único agujero, el cual proporcionaba de manera inmediata el orden de los rotores y el Ringstellung del rotor izquierdo. Con el fin

de obtener el de los otros dos rotores, es necesario observar que, fijada una de las females (normalizada si ha sido necesario), las letras del agujero de la hoja correspondiente determinaban la posición de los rotores que la había producido. Dicha posición era precisamente la diferencia entre el Grundstellung de la female y el Ringstellung que se pretendía obtener. Por consiguiente, el Ringstellung de los rotores central y derecho se obtenía restando al Grundstellung de una female las letras del agujero. Como última operación quedaba obtener las conexiones del Stecker. Recordemos que el Stecker no cambiaba la estructura de ciclos, sino que únicamente alteraba las letras de los mismos, en este caso los de longitud 1 del catálogo de características por las letras repetidas de las females, entonces la letra repetida de una female estaba conectaba con una de las letras de los ciclos de longitud 1 de la correspondiente permutación AD del catálogo. Contemplando todas las females a un tiempo, no era difícil averiguar cual.

Pero, ¿qué ocurría si el haz de luz atravesaba más de un agujero? En ese caso se procedía a realizar las anteriores operaciones con cada uno de ellos, y las contradicciones descartaban casi todos los casos, permitiendo considerar la solución correcta como aquella que permitía descifrar los mensajes.

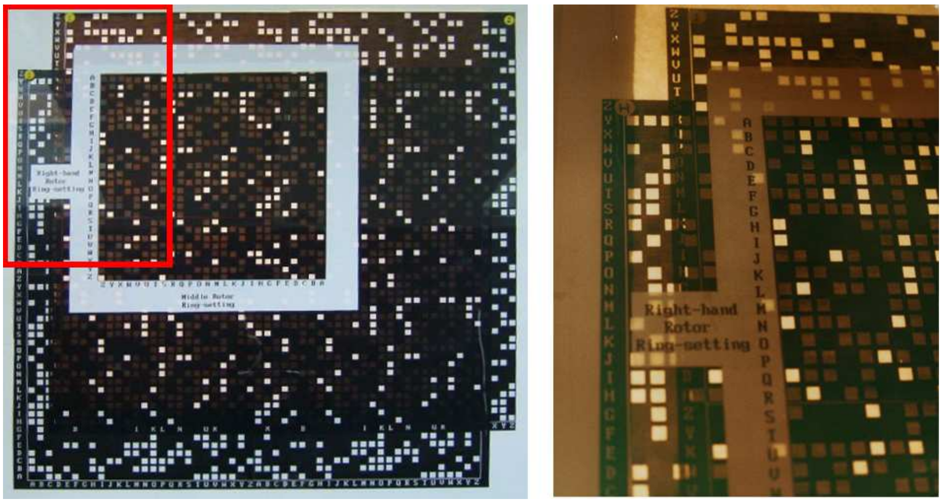


Figura 20. Hojas de Zygalski en el Museo de Bletchley Park.[22]

Por otro lado, también Jerzy Ròżycki contribuyó en gran medida a la lucha contra Enigma desarrollando el denominado *método del reloj*, que hacía posible determinar en ocasiones cuál de los rotores estaba en la posición del rotor derecho o rápido. Su método fue más tarde perfeccionado en Bletchley Park por Alan Turing, desarrollando la técnica denominada *bamburismo*. Hasta finales de 1935, los alemanes cambiaban el orden de los rotores sólo una vez cada tres meses, por lo que hasta entonces obtener la disposición del rotor rápido no resultaba de tan vital importancia. Sin embargo, a partir del 1 de febrero de 1936, dicho cambio se empezó hacer cada mes, y el 1 de noviembre de ese año comenzó a hacerse cada día, de ahí la importancia de obtener la disposición del rotor rápido. Veamos un ejemplo para ver en qué consistía dicho ingenioso método. Imaginemos que tenemos dos textos en alemán y los ponemos uno debajo del otro letra a letra como muestra la Tabla 9.

Tabla 9. Ejemplo de textos en alemán.

W E M G O T T W I L L R E C H T E G U N S T . . .
D E R A L T E L A N D M A N N A N S E I N E N . . .

[22] http://en.wikipedia.org/wiki/Zygalski_sheets

Se puede observar que de media existirá una probabilidad de coincidencia de letras en ambos textos de 2/23. Debemos esperar que esta característica se repita con textos cifrados mediante una clave idéntica. Sin embargo si se encripta cada texto utilizando una clave distinta (en este caso se utilizaron las claves O-G-P y J-N-C, con las conexiones E/G, J/Y, S/O, en el Stecker) resultan los mensajes cifrados que se muestran en la Tabla 10.

Tabla 10. Textos cifrados con Enigma.

V D Z T H D B G H X S P V Y E C G F I A D H ...
F B X G G P A X H W X U O F M Q H U U B Z K O ...

La Tabla 10 muestra que en este caso, la probabilidad de que coincidan letras en la misma posición en los dos textos cifrados con claves diferentes es de 1/23. Este hecho se debe a la distinta frecuencia de aparición de las letras en idioma alemán. En un lapso de 23 letras este hecho no ocurrirá demasiadas veces. Si por el contrario se tuvieran dos mensajes de 260 letras de longitud, con este método se podría generalmente diferenciar si los dos mensajes se cifraron con idéntica clave o con diferentes. Para ello teniendo disponible una cantidad suficiente de material cifrado, normalmente se podía encontrar una docena de pares de mensajes tales que en cada pareja las primeras dos letras de las claves eran idénticas, mientras que las terceras letras eran diferentes. Entonces, se escribían ambos mensajes uno encima de otro. Existían dos posibles formas de escribir un mensaje encima de otro, dependiendo de en qué posición de partida se encontrara el rotor rápido una vez que se producía el desplazamiento del rotor medio. Estas posiciones eran conocidas y diferentes para cada uno de los tres rotores. Por ejemplo, si el rotor I estaba colocado en la posición del rotor rápido, entonces el desplazamiento del rotor medio ocurría cuando el rotor rápido se desplazaba de la letra Q a la R. Si el rotor II estaba situado en la posición del rotor rápido, el desplazamiento sucedía cuando se desplazaba de la letra E a la F, y si el rotor III se situaba en la posición del rotor rápido, el desplazamiento sucedía cuando se desplazaba de la V a la W. Para cada una de las dos formas de escribir los mensajes, era suficiente contar el número de columnas con idénticas letras para determinar cuál era el modo correcto de escribir los mensajes y por lo tanto determinar cuál de los tres rotores estaba localizado en la posición del rotor rápido. De todos los métodos criptológicos desarrollados por el BS4, el método del reloj era el único que tomaba en consideración las características propias del lenguaje alemán, esto es, la frecuencia de aparición de las letras de su alfabeto.

La lucha constante entre la optimización de los recursos polacos y los cambios sucesivos realizados en la Enigma militar por parte de los alemanes, significó desarrollar no una única técnica, sino varios métodos que permitieran desentrañar el código de Enigma de la mejor manera posible. Además de las hojas de Zygalski o el método del reloj de Ròżycki, hubo otros como el *método ANX*. Los polacos utilizaron un hecho bastante llamativo, y es que el texto en claro de muchos mensajes alemanes interceptados comenzaban por "ANX" ("AN" significa PARA en alemán y la "X" se empleaba como separador de palabras). Una vez que era determinada la posición inicial del rotor derecho en un mensaje que comenzara por "ANX", la de los otros dos rotores se podía obtener mediante la utilización del catálogo de características construido por Rejewski.

Con la ayuda de unas invenciones basadas en las réplicas de Enigma, Rejewski fue capaz de encontrar la clave del día de las comunicaciones alemanas antes de que acabara el día. Dichas invenciones, denominadas *bombas*, resultaron ser unos aparatos electro-mecánicos basados en la combinación de 6 réplicas de la Enigma polaca construida previamente, y tenían como principal objetivo mecanizar su sistema de catalogación de modo que pudieran encontrar las posiciones correctas de los rotores. La máquina era capaz de probar 17.576 combinaciones diferentes en un tiempo aproximado de dos horas. Debido a las seis disposiciones posibles de rotores, era necesario tener seis de las máquinas de Rejewski trabajando en paralelo: cada una de ellas represen-

taba una de las posibles disposiciones. Ahora, con cada mensaje interceptado, se desarrollaba una tabla de relaciones para encontrar las cadenas resultantes, y con éstas se acudía al catálogo, encontrando la disposición de los rotores de la clave del día. Quedaba por resolver el problema del clavijero, así que Rejewski ingenió un método para obtener la configuración de éste: una vez conocida la disposición de los rotores, quitaba todos los cables y comenzaba a teclear el texto del mensaje. Al operar de este modo se obtenían frases sin sentido, puesto que se desconocía las conexiones del clavijero, pero de vez en cuando se obtenía un texto parecido a: "VULAR A MURICH". Se deducía fácilmente que esto querría decir "VOLAR A MUNICH", con lo que se veía que la U y la O estaban intercambiadas así como la R y la N. Con un número considerable de mensajes cifrados interceptados, era perfectamente posible deducir todas las posiciones del clavijero. Enigma había sido vencida nuevamente.

Veamos un ejemplo de la operatividad de las bombas. A veces entre las females interceptadas, había tres de ellas que presentaban la repetición de una misma letra.

TGB FGTFAC VHJ DFMNFX ZGP FMSFNQ

La primera de estas females pone de manifiesto que el ciclo (F) se encuentra presente en la permutación AD. Imaginemos que la letra F no se viera alterada por el Stecker, es decir la F no está conectada a ninguna otra letra a través de una conexión de clavija. Entonces el ciclo (R) también aparece en la sustitución AD que se obtendría sin ninguna conexión en el Stecker. Tenemos ya conocimiento de que el número de tales productos AD es 105.456, tantos como posibles configuraciones de los rotores (orden y posiciones iniciales). De todos estos productos, desconocemos cuantos contienen al ciclo (F), sin embargo teniendo como aliado a la Teoría de Probabilidades, sabemos que fijado un ciclo de longitud 1, si A y D se eligen aleatoriamente entre las de su clase, entonces el 4 % de los productos AD contienen dicho ciclo, lo cual reduce drásticamente el anterior número de 105.456 en un factor de 0,04 cada vez que se observe una female con la letra F repetida. Como en nuestro ejemplo, $105.456 \cdot (0,04)^3 = 6,75$, existirán seis o siete configuraciones de rotores que ocasionen las tres females representadas en el ejemplo. Las máquinas ingeniadas por Rejewski eran las encargadas de automatizar la identificación de dichas configuraciones.

Desde el punto de vista de su diseño, la bomba consistía en tres ciclómetros conectados convenientemente. Un motor eléctrico permitía a los seis bancos de rotores girar de forma sincronizada recorriendo las 17.576 posiciones posibles. En el momento en el que se alcanzaba una posición en la que los tres ciclómetros reconocían el ciclo programado, (F) en el ejemplo expuesto, el mecanismo se detenía mostrando dicha posición.

Los polacos construyeron seis bombas, una por cada orden de los rotores. Previamente a su utilización, era preciso ajustar adecuadamente las posiciones de los rotores de los ciclómetros. Para ello, en primer lugar se normalizaban las females del mismo modo que se realizaba en las hojas de Zygalski. Entonces, se asociaba cada uno de los tres ciclómetros a una female y se colocaban sus rotores en la posición indicada en el Grundstellung, con el rotor derecho del segundo banco desplazado tres posiciones respecto a su homónimo del primer banco. En el ejemplo expuesto, el primer banco se colocaría en la posición "TGB", el segundo en la posición "TGE". Después de colocar los rotores se activaba la palanca de la letra F y el mecanismo de la bomba se accionaba. Las seis bombas encontraban las seis o siete posiciones que ocasionaban las tres females en unas dos horas. Entre esas posiciones se encontraba la que proporcionaba la clave, que para conocerla se seguía el mismo procedimiento que con los agujeros de las hojas de Zygalski.

Las bombas mecanizaron enormemente el proceso criptoanalítico, eliminando en gran parte los posibles errores debidos al factor humano. Sin embargo, su principal inconveniente era que se necesitaban al menos tres females con la misma letra repetida y que además dicha letra

permaneciera invariante por el Stecker, algo que no ocurría todos los días.

Una vez que tenía la clave del día poseía la misma información que el receptor a quien iba dirigido el mensaje y, por tanto, podía descifrar los mensajes con la misma facilidad. Los polacos interceptaron multitud de mensajes alemanes, con lo cual si no evitaban el peligro de invasión por parte de éstos, sí que podían ofrecer una idea de las pretensiones que el Tercer Reich tenía con respecto a Polonia.

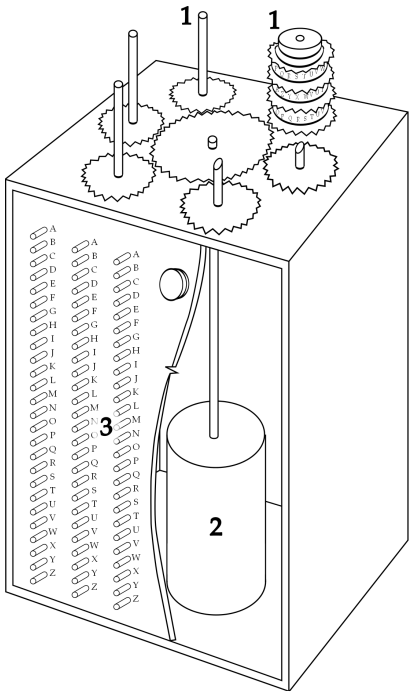


Figura 21. Bomba criptológica.[23]

La inteligencia polaca, mantuvo constantemente informado a su gobierno a través del trabajo realizado por el BS4, lo que les hizo poner sobre aviso a la opinión internacional de las pretensiones invasoras de Hitler para con Polonia. Muy a su pesar, los aliados no tomaron en demasiada consideración estos avisos. Además los acontecimientos no hacían más que empeorar la maltrecha situación de los polacos ya que el 15 diciembre de 1938, los militares nazis, conscientes del origen comercial de Enigma, consideraron oportuno suministrar a los operadores de comunicaciones dos nuevos rotores además de los 3 rotores con los que ya contaba la máquina, lo cual aumentaba enormemente el rango de disposiciones de los mismos, exactamente a la enorme cantidad de $1,59 \times 10^{20}$. En lugar de tener 6 disposiciones distintas de los rotores, ahora se tenían 60, lo cual significaba para los polacos tener que construir 54 máquinas nuevas para poder hacer frente a este nuevo reto, que de tenerlas (opción esta ni remotamente probable ya que no tenían presupuesto para ello) aumentaría el tiempo de obtención de las claves en gran medida. Del mismo modo, ahora eran necesarias $26 \cdot 54 = 1404$ nuevas hojas de Zygalski. Además, el 1 de enero de 1939, los alemanes aumentaron el número de cableado del Stecker hasta 10, provocando un efecto devastador en las labores criptoanalíticas polacas. El método criptológico de Rejewski quedaba prácticamente anulado, de forma que tan sólo uno de cada diez días eran capaces de descifrar los mensajes alemanes. Sin embargo, los polacos contaron esta vez con la accidental "ayuda" del servicio de inteligencia del partido nazi para ser capaces de obtener el cableado interno de los nuevos rotores. Parece ser que la red de comunicaciones nazi incorporó los dos nuevos rotores, pero continuaba cifrando sus mensajes con el sistema previo al 15 de septiembre. Gracias a este desliz, pudieron obtenerse las conexiones de los nuevos rotores sin más que manipulando el antiguo sistema de ecuaciones fundamentado por Rejewski.

A pesar de obtener el cableado interno de los nuevos rotores, la capacidad de cálculo de la pequeña oficina polaca se veía completamente desbordada, y encima el 1 de enero de 1939 el método de las bombas de Rejewski quedaba totalmente inoperante ya que los alemanes incrementaron hasta diez el número de conexiones del Stecker. Todo este cúmulo de acontecimientos dejó a los polacos en una situación de aislamiento ciertamente preocupante lo cual les condujo inexorablemente a buscar ayuda. Sin demasiadas alternativas, la inteligencia polaca no tuvo más remedio que recurrir a sus aliados franceses, con la esperanza de que sus mayores recursos les permitieran aprovechar los avances polacos y sacar un mayor partido al concepto de la

[23] Diseño original de Rejewski. 1. Rotores, 2. Motor eléctrico, 3. Interruptores (Cortesía de Janina Sylwestrzak, hija de Rejewski). Este concepto fue posteriormente desarrollado por los miembros del Servicio de Inteligencia Británica (SIS) en Bletchley Park. Se trataba de una invención más desarrollada que el ciclómetro. Según parece su nombre fue acuñado debido al sonido *"tic-tac"* que éstas emitían cuando probaban las distintas posiciones de los rotores. Otra versión afirma que a Rejewski le vino la inspiración de las máquinas cuando estaba en una cafetería comiendo una bomba, un helado con forma de hemisferio. Las bombas mecanizaron eficazmente el proceso de descifrado. Significaba una respuesta natural a la Enigma, que era una mecanización de la codificación.

bomba. Enigma recuperaba virtualmente su inviolabilidad.

4. Bletchley Park

4.1. La herencia polaca

Figura 22. Puesto de radio a bordo de un Sd.KFz 251 del general de la 2ª División Panzer Heinz Guderian. Invasión de Francia (Mayo - 1940).[24]

La nueva invulnerabilidad de la Enigma resultó ser devastadora para los designios de Polonia, ya que Enigma no era exclusivamente un medio de comunicación, sino un instrumento fundamental en lo que Hitler acuñó como *blitzkrieg* («guerra relámpago»), que implicaba un ataque de la Wehrmacht rápido, intenso y coordinado. Por ello, la comunicación rápida y segura entre las diferentes tropas debía estar protegida, y Enigma significaba un inmejorable aval para garantizar gran parte del éxito de las acciones bélicas consideradas. Si los polacos no podían descifrar la Enigma, no tenían ninguna esperanza de detener una violenta invasión que obviamente tenía todos los visos de producirse de manera inminente tal y como avanzaban los acontecimientos.

Bajo esta amenaza, los polacos decidieron que era necesario informar de sus avances criptoanalíticos, con el fin de que éstos no se perdieran. Si Polonia no podía beneficiarse del trabajo de Rejewski, al menos los aliados deberían tener la oportunidad de tratar de usarlos para seguir avanzando. Quizá Inglaterra o Francia, que contaban con más medios, fueran capaces de sacar el mayor partido al concepto de la bomba.

El 9 de enero de 1939, Gustave Bertrand organizó una infructuosa reunión de dos días en París entre criptólogos polacos, franceses y británicos. Los polacos, representados por el teniente coronel Gwido Langer, deseaban estrechar lazos de cooperación con los británicos visto que la amenaza de la guerra se cernía sobre ellos. Sin embargo no estaban dispuestos a revelar sus logros aún. A mediados de julio de 1939, cuando la invasión alemana de Polonia parecía inminente, el general jefe del ejército polaco, Waclaw Stachiewicz, autorizó al Biuro Szyfrów a compartir con los aliados todos los conocimientos técnicos sobre el descifrado de Enigma. El 24 de julio, Alfred Dillwyn Knox, jefe de los criptoanalistas británicos en la Oficina Exterior (Foreing Office), organizó una reunión a la que asistieron británicos y franceses. Viajaron a Pyry en los bosques de Kabackie, cerca de Varsovia, para reunirse en un viejo búnker, que resultaba ser el centro neurálgico del ataque polaco al código enigma. En el equipo británico figuraba el comandante Alastair Denniston, jefe de las operaciones criptográficas en Bletchley Park (cuyo nombre en clave era "Station X" - Estación X-), una mansión campestre a unos 70 kms al noroeste de Londres, y el comandante Humphrey Sandwich. A. Denniston era un reconocido defensor de la importancia de las matemáticas en la lucha criptoanalítica, de hecho gran parte del posterior éxito en Bletchley Park se debe a que fue uno de los que apostó por enrolar en esta lucha a las mejores mentes matemáticas y lógicas del momento en Gran Bretaña. Los franceses estaban representados por el comandante Gustave Bertrand, y el capitán Henri Braquenié. Finalmente los polacos estaban representados por el capitán Maksymilian Ciężki, el teniente coronel Gwido Langer y el coronel jefe Stefan Mayer. Estas conversaciones sirvieron para que los aliados se

[24] Foto: Erich Borchert, Deutches Bundesarchive (Archivo Federal Alemán). Signatura: Bild+101I-769-0229-10A. http://www.bild.bundesarchiv.de/

pusieran al día de todos los avances logrados por el BS4. El 16 de agosto de 1939, mientras los jóvenes de Reino Unido respondían masivamente a la llamada de alistamiento, el comandante G. Bertrand llegaba a la Estación de Victoria acompañado del comandante Wilfred Dunderdale de la inteligencia británica en París. Bertrand portaba un maletín con información fundamental en la guerra contra Enigma, además de una réplica de la misma (una *bomba* ya prometida por los polacos en su reunión en Pyry) que entregó al general Stewart Menzies, 2º jefe del Servicio de Inteligencia Británico. Dos semanas después, Hitler invadía Polonia y estallaba la 2ª Guerra Mundial.

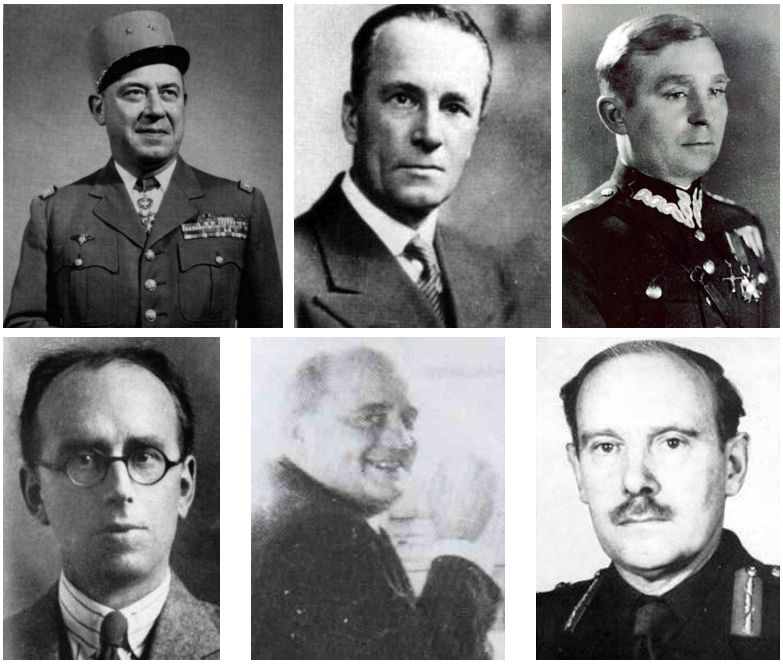


Figura 23. De izq. a drcha y de arriba a abajo: 1. Gustave Bertrand, 2. Alastair Denniston, 3. Maksymilian Ciężki, 4. Alfred Dillwyn Knox, 5. Wilfred Dunderdale y 6. Stewart Menzies.[25]

Durante años, los aliados habían considerado que Enigma era indescifrable, pero los logros conseguidos por los polacos puso de manifiesto la importancia de emplear a matemáticos en las técnicas de criptoanálisis. Bletchley Park, era la sede del Government Code & Cypher School (GC&CS, Escuela Gubernamental de Códigos y Cifras), una organización de descodificación recién fundada en Buckinghamshire, que tras el estallido de la guerra, se convirtió en la sede clandestina y secreta del ataque a Enigma. Bletchley Park era un edificio de arquitectura gótico Tudor, situado a las afueras de la pequeña localidad rural de Milton Keynes, sin duda un lugar insólito para uno de los mayores triunfos tecnológicos de la guerra.

Tras haber recibido la información sobre los logros del BS4, los criptólogos, científicos y matemáticos británicos de Bletchley dedicaron el otoño de 1939 a familiarizarse, comprender y dominar las técnicas polacas. A medida que los ingleses fueron asimilando conceptos y afinando esfuerzos, la actividad de Bletchley Park se fue incrementando más y más. De hecho al inicio de la guerra trabajaban en sus instalaciones en torno a 200 personas, pero al final de la misma esta cantidad aumentó hasta 10.000, lo que significó tener que realizar ampliaciones en el complejo, construyendo un gran número de cobertizos adicionales. Una vez pudieron entender y dominar las técnicas polacas, los criptoanalistas de Bletchley comenzaron a utilizar sus propios

[25] 1. [13], 2. http://enigma.umww.pl/index.php?page=Denniston, 3. http://wyborcza.pl/51,75248,5980398.html, 4. http://enigma.umww.pl/index.php?page=dillwyn-knox, 5. http://bondambitions.com/2011/01/origins-of-bond, 6. http://www.reformation.org/spies-are-despicable.html.

[26] http://es.wikipedia.org/wiki/Bletchley_Park

Figura 24. Fachada principal de Bletchley Park en la actualidad.[26]

atajos para descubrir las claves de la Enigma.

Figura 25. John R. F. Jeffreys.[27]

El primer método criptológico polaco utilizado por los británicos fue el de las hojas de Zygalski. A pesar de los cambios llevados a cabo por los alemanes en la operatividad de la Enigma, ahora los ingleses contaban con recursos humanos prácticamente ilimitados, por lo que este método era viable. La tarea de organizar todo el operativo le fue encargada a John R. F. Jeffreys (1918-1944), un matemático del Downing College de Cambridge reclutado por Alfred Dillwyn Knox junto a otros compañeros como Alan Turing, Goldon Welchman o Peter Twinn. Hacia finales de diciembre de 1939, los británicos tendrían preparadas las 1.560 hojas que eran necesarias. Dichas hojas eran una adaptación de las hojas de Zygalski, por lo que en Bletchley se las denominaron hojas de Jeffreys. Al mismo tiempo que se preparaban las hojas, un equipo se encargó de analizar el tráfico de mensajes, con el fin de identificar distintas redes de comunicaciones del ejército alemán, las emisoras que operaban dentro de cada red, aquella que gestionaba el tráfico dentro de la red, qué emisora transmitía cada mensaje y a cuál otra iba dirigido. Este análisis se convirtió en fundamental para descifrar los mensajes, ya que cada una de las redes funcionaba con una clave diferente.

El método de Zygalski necesitaba una gran cantidad de recursos, por lo que los británicos comenzaron a reclutar a una amplia variedad de personal, entre los que se encontraban matemáticos de Cambridge y sus alumnos de últimos cursos, ingenieros, lintgüistas, jugadores de ajedrez, secretarias, administrativos de apoyo … En total se estima que a lo largo de la guerra, unas 12.000 personas trabajaron en Bletchley Park de forma fija o temporal. Curiosamente un alto porcentaje de estas personas fueron mujeres.

Los británicos se percataron del hecho de que los operadores alemanes utilizaban claves relativamente obvias de descubrir. Para cada mensaje se suponía que el operador elegía una clave de mensaje diferente, tres letras escogidas al azar. Sin embargo, en el fragor de la batalla,

[27] http://enigma.wikispaces.com/John+Jeffreys

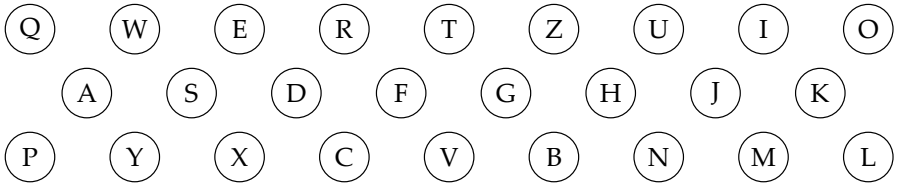


Figura 26. Disposición del teclado de la Enigma.

en vez de forzar su imaginación para elegir una clave al azar, los agotados operadores a veces tomaban tres letras consecutivas del teclado de la Enigma, como, por ejemplo, QWE o BNM. Este tipo de debilidades "de uso" más que fragilidad provocado por el propio diseño de la máquina, se denominaron *cillis*. Además de las cillis, existían otro tipo de errores humanos producidos por los propios responsables de la elaboración de los libros de códigos. La norma de prohibir que un mismo rotor permaneciera en el mismo hueco durante más de un día podría parecer una estrategia sensata, sin embargo, el efecto para el criptoanalista era que su trabajo se veía tremendamente simplificado por este hecho, ya que se reducía el número de posibles configuraciones de rotores que había que considerar para el estudio y análisis. Por supuesto, este hecho no pasó desapercibido a los criptoanalistas de Bletchley ya que descubrieron así una pequeña debilidad en la Enigma que no podían desaprovechar.

4.2. El genio de Turing

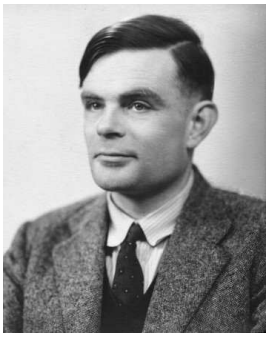


Figura 27. Alan Mathison Turing.[28]

El encargado de recoger el testigo de los logros criptográficos conseguidos por los polacos fue el genio matemático del King's College de Cambridge, Alan Turing (1912-1954). Turing ya había trabajado anteriormente en el desarrollo del concepto de máquina computacional. Son célebres sus trabajos de 1938 en la que define la *máquina-a* o *máquina de Turing*, una máquina virtual o física en el que era posible definir el concepto de *algoritmo* que resulta fundamental en computación. En Bletchley, Turing se convertiría en una de las cuatro figuras al mando de la organización de los trabajos de desencriptado junto a Gordon Welchman, Philip Stuart Milner-Barry y Conel Hugh O'Donel Alexander. Estaba al cargo del barracón 8, responsable de descifrar los códigos de la Enigma de la marina alemana (una de las más complicadas dado que contaba con un rotor adicional y sus operadores eran extremadamente escrupulosos a la hora de su utilización, lo que la hacía prácticamente impenetrable), con el fin de romper el bloqueo naval con el que los submarinos nazis tenían sometido al Reino Unido.

Parece ser que Turing se encargó personalmente de hacer llegar varios juegos de hojas de Jeffreys al equipo de criptólogos bajo el mando de Bertrand en Francia en enero de 1940. Debido a que los alemanes no tardarían en darse cuenta que su técnica de repetición de la clave del mensaje comprometía seriamente la seguridad de Enigma, el 10 de mayo de 1940, coincidiendo con la invasión de Francia, éstos modificaron nuevamente su sistema de cifrado, evitando la repetición de la clave de cada mensaje, hecho que resultó dramático para los aliados, puesto que de este modo se eliminaban así las females de las cabeceras de los mensajes y por lo tanto las hojas de Jeffreys quedaban inutilizables.

Turing se encargó de encontrar una manera alternativa de atacar la Enigma, una forma que no dependiera de la repetición de la clave del mensaje. Su técnica consistió en buscar lo que en

[28] Foto: Elliot&Fry (29 Mar. 1951), National Portrait Gallery (Galería Nacional de Retratos), Londres. http://www.npg.org.uk/collections/search/portrait/mw165875

criptología se denominan *puntales* (*cribs* en inglés) que no es otra cosa que cuando un fragmento de texto llano se puede asociar con un fragmento de texto cifrado. Después de unas pocas semanas estudiando mensajes cifrados interceptados, Turing podía adivinar (más bien predecir) partes de mensajes sabiendo sólo cuándo y desde dónde habían sido emitidos. Los alemanes tenían la costumbre de emitir mensajes cifrados a primera hora de la mañana, sobre las 6, en los que informaban del estado meteorológico a lo largo de todo el frente de guerra. Parecía razonablemente evidente que muchos de los mensajes interceptados en torno a las 6 de la mañana seguramente contendrían la palabra "wetter" (tiempo en alemán), lo cual suponía una fuente inmejorable para la obtención de puntales. Aunque en cierto modo eran suposiciones más que otra cosa, Turing estaba seguro de que por ahí podía desarrollar un método nuevo para atacar a Enigma. Pero considerar el ataque de un modo directo resultaba ser una tarea prácticamente inabordable. Por ello Turing adoptó una estrategia de ataque parecida a la de Rejewski, separando los efectos de las distintas configuraciones de los diferentes componentes de la máquina. Turing intentó separar por un lado el problema asociado a conocer la disposición de los rotores (en qué ranura estaban cada uno de ellos y cuáles eran sus orientaciones respectivas), y por otro el problema asociado al cableado utilizado en el clavijero o panel Stecker. De este modo si podía descubrir algo en un puntal que no tenía nada que ver con los cableados del clavijero, entonces no le resultaría imposible probar cada una de las restantes 1.054.560 combinaciones posibles de los rotores (60 disposiciones $\times$ 17.576 orientaciones). Si descubría las posiciones correctas de los rotores, entonces podía deducir las conexiones del Stecker. La diferencia sustancial con respecto a la estrategia de Rejewski es que Turing no estudió las repeticiones de las claves de los mensajes, sino la codificación de los puntales, que recordemos no dejaban de ser suposiciones. Si por ejemplo se estimaba que la palabra "wetter" era cifrada mediante el código ETJWPX, se estudiaban lo que se denominó *rizos internos*.

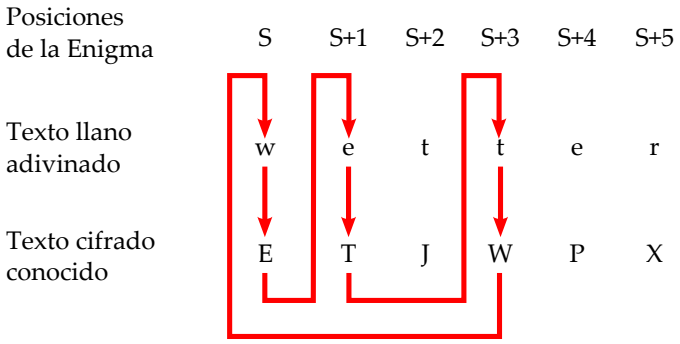


Figura 28. Rizos internos del puntal "wetter".

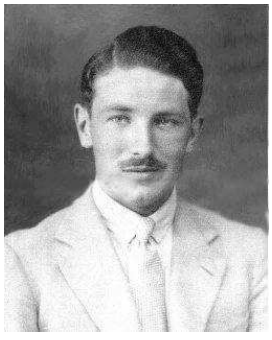


Figura 29. William Gordon Welchman.[29]

Como puede observarse en la Figura 28, en la posición S de la Enigma, la letra w es codificada como E, en la posición S+1, la e es codificada como T, y en la posición S+3, la t es codificada como W. Con la ayuda de los logros polacos, Turing fue capaz de construir un modelo mejorado de la bomba polaca, al que denominó *bombe* cuya finalidad consistía en ir probando multitud de posibilidades mediante la configuración inicial de los rizos establecidos por los puntales. La combinación de puntal, rizos y máquinas conectadas eléctricamente resultó ser finalmente una estrategia extraordinaria de criptoanálisis, capaz únicamente de ser planificada por una mente privilegiada como la de Turing. El primer modelo de *bombe*, denominado *Victory*, fue instalado en Bletchley en marzo de 1940 gracias a la obtención de 100.000 libras para la financiación del proyecto de Turing. Más tarde siguieron otros diseños mejorados por el también matemático Gordon Welch-

[29] http://www.specialforcesroh.com/image-4035.html

man (1906-1985), como el *Spider* en agosto de 1940, cuya principal implementación consistía en la inclusión del denominado *panel diagonal de Welchman* que tenía como función incrementar la efectividad de las máquinas diseñadas por Turing mediante el aprovechamiento de la reciprocidad de caracteres en el panel Stecker, de forma que si un caracter L_1 es permutado por otro L_2 mediante dicho panel, inevitablemente L_2 estará permutado por L_1 a través del Stecker. En la primavera de 1941 vería la luz el *Jumbo*. Las *bombe* eran capaces de identificar palabras en los textos cifrados con una gran probabilidad mediante la técnica denominada *crib*. Mecánicamente, los rotores de las bombe tenían el mismo cableado interno que la Enigma, y el reflector era simulado gracias a un sistema tan sencillo como que las conexiones y cables estaban presentes por duplicado. Para cada posible posición de los rotores se hacía una prueba, y si el resultado era una contradicción entonces esas posiciones de los rotores eran descartadas; en caso contrario, se seleccionaban esas posiciones como solución candidata.

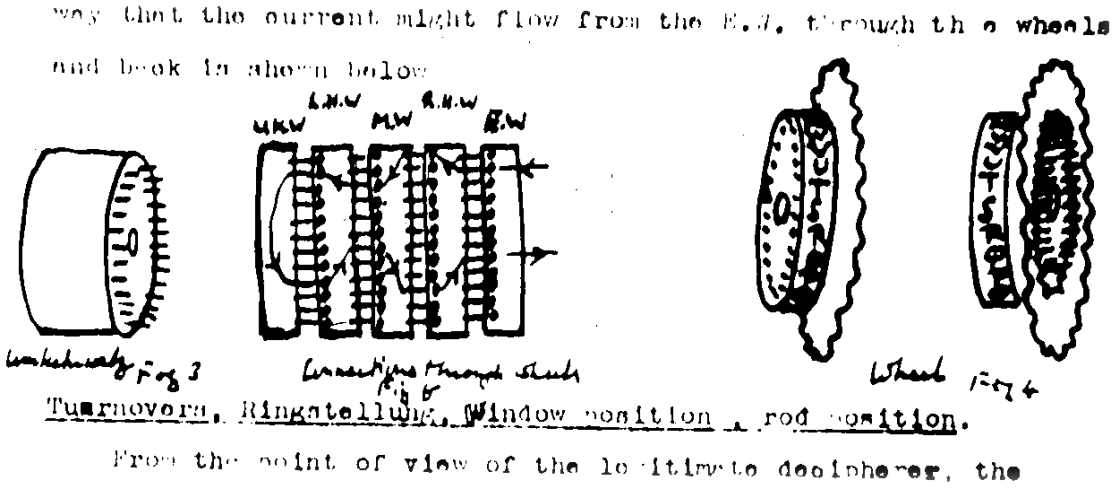


Figura 30. Notas del "Tratado sobre Enigma", manuscrito original de Alan Turing (1939-42).[30]

A finales de 1941, los alemanes sospecharon que los aliados habían conseguido desencriptar el código de la Enigma, por lo que añadieron un cuarto rotor, cuyo cableado interno era totalmente desconocido para los criptólogos de Bletchley. Sin embargo, en las navidades de ese mismo año sucedió un hecho inesperado. Uno de los submarinos emitió un mensaje, pero inexplicablemente el operador utilizó una Enigma de tres rotores, lo que ofreció a los aliados la posibilidad de poder establecer una reciprocidad entre los dos sistemas y deducir el cableado interno del cuarto rotor, y por lo tanto la posibilidad de seguir trabajando en la desencriptación del código. Aunque hubo un periodo de "apagón" que duró casi nueve meses, a finales de octubre de 1942 los criptoanalistas británicos lograron desentrañar el nuevo código.

Cuando la guerra llegaba a su fin, Bletchley Park estaba dotada con 211 máquinas *bombe*, que necesitaban mas de 2.000 personas para su mantenimiento y utilización. El trabajo de Alan Turing y sus *bombe* ayudaron enormemente a que los aliados ganaran la guerra. Hechos importantes que así lo demuestran son el papel que la desencriptación del código Enigma significó en la Batalla del Atlántico en la defensa de los convoyes navales aliados contra los submarinos alemanes, la derrota del Afrikakorps de Rommel, o el desembarco de Normandía. Con la victoria aliada, el primer ministro británico Wiston Churchill consideró oportuno que era necesario destruir todas las *bombe* y toda la documentación relacionada con su diseño y construcción, a pesar del valiosísimo servicio que habían proporcionado durante la guerra. Además todos los participantes en las labores de descodificación de Enigma tuvieron que prestar juramento de que en ningún caso revelarían dato alguno sobre las actividades llevadas a cabo en Bletchley Park du-

[30] http://www.turingarchive.org/browse.php/C/30

rante la contienda. A partir de 1976 la información sobre Enigma comenzó a ser desclasificada y dada a conocer al público en general, fue entonces cuando todos aquellos que colaboraron en la lucha contra Enigma y que tan injustamente habían sido tratados debido a las circunstancias de la guerra fría, comenzaron a gozar del reconocimiento público que merecían.

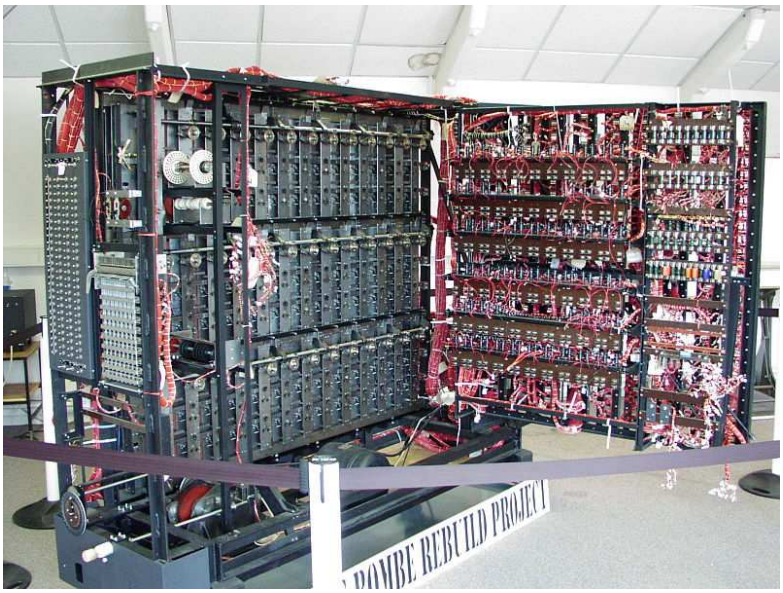


Figura 31. Réplica de la bombe, reconstruida gracias al trabajo de técnicos veteranos voluntarios de Bletchley Park.[31]

5. El final de los protagonistas de Enigma

Tras la invasión de Polonia por los nazis, una gran cantidad de miembros del BS4 fueron capturados, torturados y asesinados. Afortunadamente, Rejewski, Ròżycki y Zygalski pudieron abandonar el país y poner rumbo a Rumanía antes de ser capturados. Cuando llegaron a la capital dacia intentaron sin éxito solicitar asistencia en la Embajada Británica. Sin embargo la Embajada Francesa sí que se la proporcionó, evacuándolos a París a finales de septiembre de 1939.

Por otro lado la Unión Soviética también invadió Polonia el 17 de septiembre de 1939, por lo que el Biuro Szyfrów decidió destruir de forma inmediata toda la documentación acerca de Enigma.

El centro de inteligencia franco-polaca se estableció en octubre de 1939 en el Château de Vignolles, en Gretz-Armainvillers, a 40 kms al noreste de París, recibiendo el nombre secreto de "Bruno"[32]. El centro se dedicó a interceptar transmisiones de radio alemanas en coordinación con el GC&CS británico. De manera adicional, siete criptólogos españoles republicanos fueron empleados en Bruno con el fin de poder descifrar códigos de la Italia fascista y la España franquista.

El principal trabajo del centro era alertar a los Aliados acerca de la inminente invasión de Francia por las tropas germanas. En mayo de 1940, Alemania comenzó su invasión, y a mediados de junio había llegado a París. El 10 de junio de ese año, la unidad Bruno recibió ordenes de evacuar, y en 48 horas Rejewski y sus colegas, además de los criptólogos españoles liderados por Faustino Antonio Camazón Valentín, ponían rumbo en un viaje que duraría 10 días

[31] http://en.wikipedia.org/wiki/File:Bombe-rebuild.jpg
[32] Es posible encontrar que algunos autores lo denominan "PC Bruno", donde PC significa "Puesto de Mando".

que les llevaría a Toulouse, a Orán en el norte de África y finalmente al centro de operaciones denominado Villa Kouba que los franceses tenían cerca de Argel. París cayó el 14 de junio, y el 22, Francia firmaba su rendición parcial (parte del país, que más tarde acuñría el nombre de la Francia de Vichy, no era ocupada y se le permitía cierta autonomía).

Sin embargo, lejos de arrugarse, los criptólogos polacos y españoles, denominados "Equipo Z" y "Equipo D" respectivamente, decidieron continuar con su peligrosa tarea. El mayor Gustave Bertrand regresó en septiembre a Francia y fue entonces cuando los integrantes de Bruno decidieron crear una nueva unidad encubierta denominada "Cadix", en el Château des Fouzes, en Uzès, cerca de Nimes, al sur de la Francia de Vichy, entre Montpellier y Avignon. Para evitar cualquier sospecha Rejewski se empleó como profesor de matemáticas en Nantes.

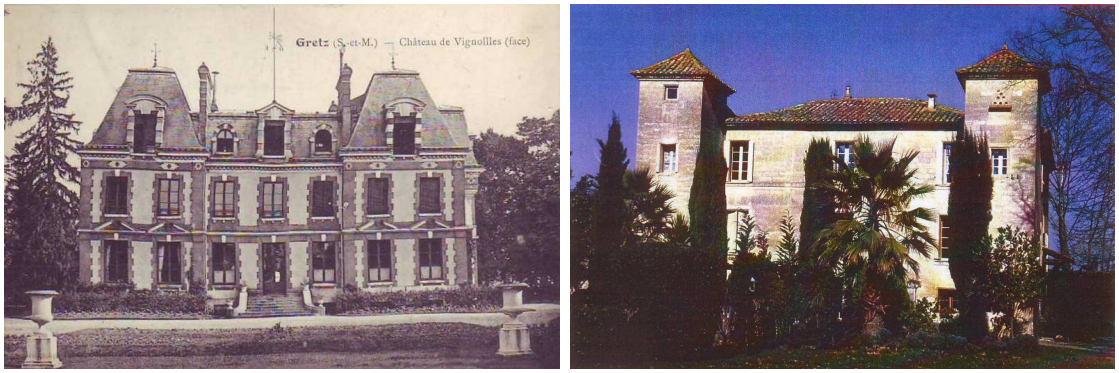


Figura 32. Château de Vignolles (izq.) y Château des Fouzes (drcha.) [13].

Figura 33. Trabajadores del centro polaco-hispano-francés de radioespionaje "Cadix" (1940-1942).[33]

La madrugada del 9 de junio de 1942, mientras regresaba al centro de Cadix de un viaje a la oficina de Château Couba en Argel que estaba dirigida por Maksymilian Ciężki, el barco de

[33] De izq. a drcha: 1. Henri Braquenié, 2. Piotr Smoleński, 3. Edward Fokczyński, 5. Maksymilian Ciężki, 7. Gwido Langer, 8. Mary Bertrand, 9. Gustave Bertrand, 13. Henryk Zygalski (detrás, con gafas), 14. Jan Graliński, 18. Jerzy Ròżycki. 20. Marian Rejewski. http://www.ww2.pl/ww2/zdjecia/153.jpg

[34] (a) De izq. a drcha.: 1. Henryk Zydalski, 2. Jercy Ròżycki, 3. Marian Rejewski. (b) Junto a criptógrafos españoles. De izq. a drcha: 1. Marian Rejewski, 2. Edward Fokczyński, 3. español no identificado, 4. Henryk Zygalski, 5. español no identificado, 6. Jerzy Ròżycki; 7. Faustino Antonio Camazón Valentín, 8. Antoni Palluth, 9. español no identificado. http://en.wikipedia.org/wiki/File:Zygalski-rozycki-rejewski.jpg, http://www.ugr.es/ aquiran/cripto/museo.htm

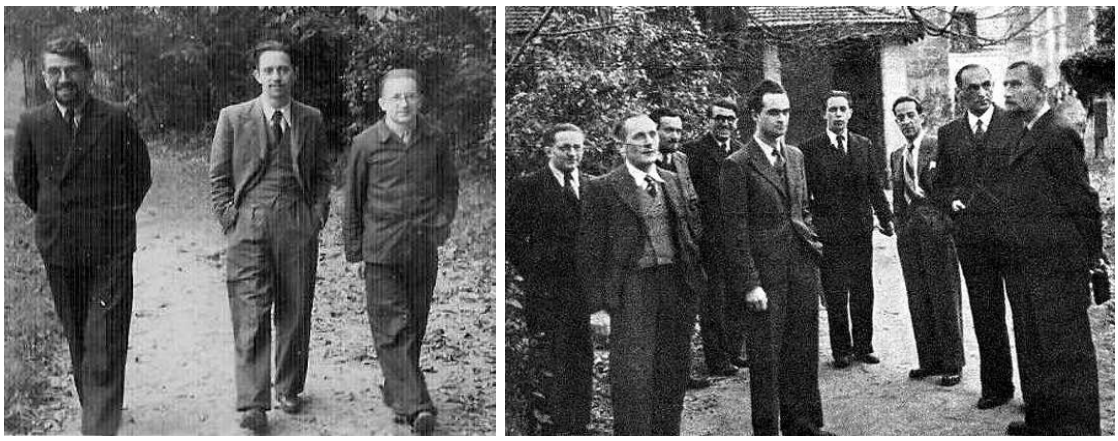


Figura 34. Imágenes en los jardines del Château des Fouzes en algún momento entre septiembre de 1940 y junio de 1941.[34]

Jercy Ròżycki de nombre Lamoricière, se vio sorprendido por un fuerte temporal cuando estaba a 30 millas al norte de la isla de Menorca. Cuando remontaba hacia Marsella por el Canal de Menorca, el buque ya llevaba ocho horas de retraso y se enfrentaba a un temporal con olas de hasta once metros. Aún así, el capitán decidió virar hacia el sur de Menorca con el fin de socorrer al carguero Jumiéges. Al llegar a las coordenadas del carguero, sobre las 3 de la madrugada, la tripulación comprobó que el Jumiéges ya se había hundido. Atrapados en el temporal, el capitán del Lamoriciére ordenó recuperar el rumbo pero al parecer había entrado agua por las compuertas de cubierta que provocó la parada de dos motores del buque. Cuando el capitán consideró que sería imposible llegar a su destino en el puerto de Marsella, decidió buscar refugio. Sin embargo, no tuvo éxito en su maniobra, y el barco fue engullido literalmente por las olas y naufragó. No obstante algunos investigadores ponen de manifiesto que este hecho pudiera no haber sido únicamente un trágico accidente. Su argumentación es que las circunstancias en torno a este naufragio no son demasiado claras. Parece ser que en medio del temporal el capitán intentó girar el barco de 112 metros de eslora para buscar refugio en la costa sur de la isla de Menorca. En esta maniobra la tramontana golpeó violentamente el costado y la carga de naranjas que llevaba en sus bodegas se soltó y golpeó fuertemente contra el casco que resultó gravemente dañado, además de desplazar el centro de gravedad del buque provocando que éste se escorara hacia un costado. Desafortunadamente parece ser que el agua que entraba apagó los motores restantes y el generador eléctrico, con lo que las bombas de achique no funcionaron. Este cúmulo de desafortunados hechos sugiere la sospecha de que se pudiera haber producido un sabotaje. Ante esta situación, el capitán ordenó que tripulantes y pasajeros recolocaran la carga desplazada para que el barco se estabilizara pero todo fue inútil. No parece una casualidad tampoco que entre los 301 pasajeros que perdieron la vida en el suceso (únicamente hubo 93 supervivientes), se encontraran varios criptólogos fundamentales en el trabajo contra el código Enigma, como los polacos Piotr Smolesński, y el capitán Jan Graliński, de la Sección Rusa del Biuro Szyfrów, además del propio Jercy Ròżycki y el oficial francés que acompañaba a los tres polacos, el capitán François Lane.

En noviembre de 1942, mientras los aliados preparaban la invasión del norte de África, las tropas alemanas ocuparon la Francia de Vichy. La unidad secreta en el Château des Fouzes corría un grave peligro de ser descubierta y desmantelada, por lo que sus miembros debieron ser evacuados de manera fulminante. Todo el personal escapó el 9 de noviembre justo a tiempo, ya que tres días después los alemanes descubrían la operación secreta de Cadix. Rejewski y Zygalski no tuvieron más remedio que abandonar el país vía España, pero al cruzar los Pirineos fueron arrestados y encarcelados primero en la prisión de La Seu d'Urgell y después en la de Lleida. El 4 de mayo serían liberados gracias a la intermediación de la Cruz Roja polaca y enviados a

[35] http://en.wikipedia.org/wiki/File:Gralinski,_Rozycki_and_Smolenski.jpg

Figura 35. De izqda. a drcha.: Jan Graliński, 2. Jercy Ròżycki, 3. Piotr Smolesński, en Cadix.[35]

Madrid. El 21 de julio salían de Madrid con rumbo a Portugal. Finalmente llegaron a Londres vía Gibraltar el 3 de agosto de 1943. Allí, paradojas de la vida, no fueron invitados a colaborar con el proyecto que lideraba entre otros el genio matemático de Alan Turing en Bletchley Park, que era el centro neurálgico de la lucha aliada contra el código Enigma, sino que ocuparon puestos menores en oficinas de cifra y código secundarias, digamos de 2ª división, en Boxmoor, cerca de Hemel Hempstead, lo cual no deja de resultar sorprendente, dado que realmente los aliados habían necesitado antes de sus avances para comenzar a desarrollar las máquinas bombe. Sin embargo no todos los polacos corrieron la misma suerte que Rejewski y Zygalski. Un grupo de polacos miembros del equipo Cadix, entre ellos Gwido Langer, Maksymilian Ciężki, Antoni Palluth, Edward Fokczyński y Kazimierz Gaca intentaron escapar cruzando la frontera con España, pero fueron arrestados en Prats de Mollo en un control policial. Tras un mes fueron liberados e intentaron nuevamente entrar en España varias veces sin éxito. Sin noticias de Bertrand, decidieron arriesgarse a cruzar los Pirineos en un último intento guiados por un contrabandista. Fueron traicionados por éste que colaboraba con la Gestapo, y capturados por los alemanes cuando intentaban cruzar la frontera la noche del 10 al 11 de marzo de 1943. A pesar de ser interrogados y torturados con gran brutalidad por la policía alemana de Perpiñán, ninguno de ellos reveló información alguna sobre Cadix. Langer y Ciężki fueron enviados al campo de prisioneros 122 en Compiégne, Francia, y el 9 de septiembre al campo de concentración alemán de las SS *Sonderkommando Schloss Eisenberg* en Checoslovaquia, donde sobrevivieron en condiciones deplorables. Palluth, Fokczyński y Gaca fueron enviados a Alemania a campos de prisioneros de guerra y trabajos forzados. Palluth murió al estallar una bomba durante un ataque aéreo aliado y Fokczyński finalmente no pudo aguantar y murió de agotamiento. Ambos murieron en el campo de concentración de Sachsenhausen, cerca de Berlín. En mayo de 1945, Langer, Ciężki y Gaca fueron liberados por las tropas estadounidenses. Los últimos años de Langer no fueron nada fáciles. Bertrand y gran parte de oficiales polacos le dieron la espalda a pesar de la interpelación a su favor de Ciężki. Herido en su orgullo siempre defendió que siguieron las vías de escape establecidas por la inteligencia francesa para evitar ser capturados por los alemanes, sin embargo

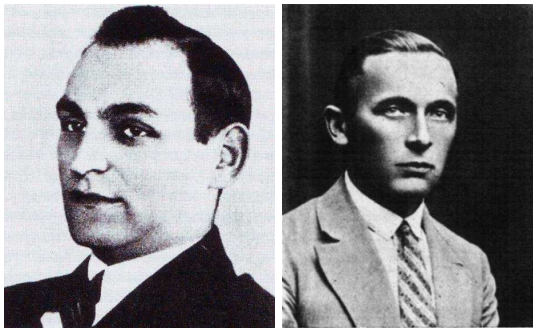


Figura 36. Antoni Palluth (izq.) y Edward Fokczyński (drcha.).[13]

Bertrand siempre le responsabilizó directamente del desacierto de la operación de evacuación. Según posteriores testimonios de oficiales de la inteligencia francesa durante la guerra, parece evidente que no se siguieron los mejores procedimientos en la evacuación, ya que en aquel momento existían vías para cruzar a España completamente seguras que no fueron utilizadas. Con estas revelaciones parece evidente deducir que los polacos fueron en cierto modo abandonados a su suerte. Langer murió en el campo del ejército polaco en Kinross, Escocia, el 30 de marzo de 1948. Ciężki permaneció hasta su muerte en Gran Bretaña, donde al contrario que Langer, obtuvo muchas condecoraciones militares. Murió el 9 de noviembre de 1951.

En noviembre de 1946 Rejewski retornó a Polonia donde la esperaban su mujer y sus dos hijos. Una vez allí le fue muy complicado encontrar un puesto de docente por lo que finalmente aceptó una oferta como contable en Bydgoszcz, su ciudad natal, al norte de Polonia. Mantuvo bajo juramento su promesa de no revelar a nadie ninguna de sus actividades contra los códigos alemanes, manteniendo en estricto secreto todos sus avances con respecto a la máquina Enigma. El 12 de agosto de 1978, en reconocimiento a su labor criptoanalítica, el Gobierno polaco le concedió la Cruz de los Oficiales de la Orden de la Refundación de Polonia. Murió de un ataque al corazón el 13 de febrero de 1980 tras sufrir una larga enfermedad coronaria. Hoy día es considerado como un auténtico héroe nacional y se le han dedicado varios monumentos en su recuerdo.

Figura 37. Estatua de bronce de Rejewski en Bydgoszcz, en conmemoración del centenario de su nacimiento (2005).[36]

Por su parte, tras la guerra, Zygalski permaneció exiliado en el Reino Unido donde trabajó como profesor de estadística matemática en la Universidad de Surrey hasta su retiro, y al igual que Rejewski tuvo que mantener en secreto todos sus trabajos sobre criptografía. Murió el 30 de agosto de 1978 en Liss, donde fue incinerado y sus cenizas fueron llevadas a Londres. Poco antes de su muerte recibió el doctorado honorario de la Universidad Polaca en el Exilio por sus logros conseguidos contra el código Enigma.

Resulta paradójico que la inestimable prestación que significaron los logros de Turing para los Aliados fueran recompensados de la manera en la que las instituciones británicas consideraron. En febrero de 1952, Turing dejó solo en su casa a su amante Arnold Murray. Al regresar, Turing se encontró con la sorpresa de que varios objetos de gran valor sentimental habían des-

[36] http://commons.wikimedia.org/wiki/File:Bydgoszcz_Rejewski_3.jpg?uselang=pl
[37] http://www.geograph.org.uk/photo/2261564

Figura 38. Monumento conmemorativo a los criptoanalistas polacos en Bletchley Park (2002).[37]

aparecido de su casa, por lo que se dispuso a denunciar dicho robo. En su declaración, Turing mencionó con total naturalidad su relación con Murray, por lo que la policía consideró oportuno investigar su homosexualidad en lugar del verdadero hecho importante que era el robo en sí mismo. En marzo de 1952, Turing era enviado a juicio, ya que en aquella época la conducta homosexual estaba penada por las autoridades británicas. Turing perdió el juicio aunque dado su prestigio, tuvo que someterse a un tratamiento de castración química mediante hormonas en lugar de su ingreso en prisión. Parece ser que este hecho provocó cambios fisiológicos en Turing que sufrió como su cuerpo cambiaba hasta el punto de experimentar el crecimiento de sus pechos. Harto de esta situación decidió quitarse la vida comiéndose una manzana a la que previamente había inyectado cianuro potásico.

Figura 39. Estatuas conmemorativas de Alan Turing en Bletchley Park (2008) y en Sackville Park, Manchester (2009).[38]

[38] http://es.wikipedia.org/wiki/Alan_Turing

En septiembre de 2009, el Primer Ministro Gordon Brown, solicitaba disculpas públicas por el trato que Turing había recibido, y manifestaba:

> *"Turing fue un destacado y brillante matemático, cuya labor más famosa fue descifrar los códigos Enigma del ejército alemán. No resulta exagerado señalar que, sin su extraordinaria contribución, la historia de la 2ª Guerra Mundial habría sido bien diferente. Él fue una de esas personas de las que verdaderamente podemos decir que contribuyó a modificar el rumbo de la guerra. La deuda de gratitud que tenemos con él hace mucho más horripilante que fuera tratado de forma tan inhumana.*
>
> *Miles de personas se han unido para solicitar justicia para Alan Turing y el reconocimiento del modo atroz en el que fue tratado . . . el trato que recibió fue completamente injusto, y me complace poder expresar lo consternado que me siento, que nos sentimos todos, por lo que ocurrió.*
>
> *. . . Más allá incluso, Alan merece reconocimiento por su contribución a la humanidad. Para aquellos de nosotros que nacimos después de 1945, en una Europa unida, democrática y en paz, es duro imaginar que nuestro continente fue una vez escenario del momento más oscuro de la humanidad.*
>
> *. . . Por lo tanto, en nombre del Gobierno británico, y de todos aquellos que vivimos en libertad gracias al trabajo de Alan, me siento orgulloso de decir: lo sentimos, mereciste algo mucho mejor."*

6. Las máquinas Lorenz

6.1. Características y particularidades

Muy a pesar del ingenio que supuso la ruptura del código de la Enigma, no fue ésta la máquina que inspiró el nacimiento de lo que hoy día podemos considerar (aunque con algunas restricciones) como el primer ordenador de la historia. Durante el curso de la 2ª Guerra Mundial, Alan Turing fue el encargado de romper el difícil código naval alemán (llamado *Shark*), lo que sirvió para que los aliados se hicieran finalmente con la victoria. Sin embargo, Enigma sólo significó la mitad de la historia de la lucha criptológica contra los alemanes.

En 1940, a principios de la guerra, los británicos interceptaron unas señales de teletipo en las que no se utilizaba el código Morse. Su "música" era completamente distinta al sonido característico proveniente de las Enigma. Se trataban de señales cifradas con las llamadas máquinas *Lorenz SZ40* y *SZ42* (*Schlüsselzusatz*, que significa "cifrado adjunto") que estaban conectadas a un teletipo. Mientras que la Enigma se usaba generalmente por unidades de combate, las Lorenz fueron utilizadas para las comunicaciones cifradas entre el propio Hitler y su alto mando. Esto es debido a que la cúpula del ejército nazi consideraban que las Lorenz ofrecían si cabe una mayor seguridad que las Enigma ya que utilizaban 12 rotores. En cierto modo las Lorenz sirvieron para "dictar" el curso

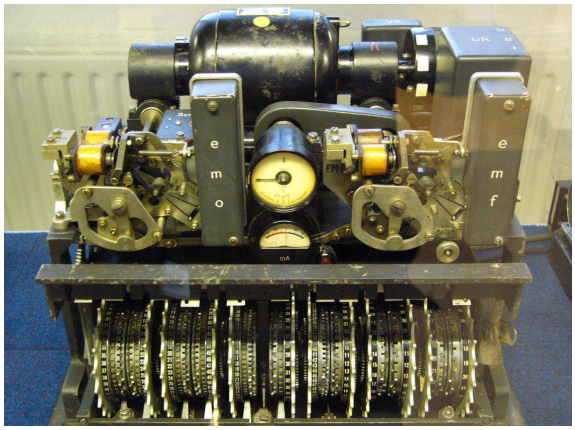


Figura 40. Máquina Lorenz SZ42.[39]

[39] http://es.wikipedia.org/wiki/Código_Lorenz

de la guerra. En Bletchley Park, los criptoanalistas organizaban su trabajo clasificándolo dependiendo de los códigos o claves con los que se referían a las distintas redes de comunicación utilizadas por los alemanes. El tráfico de las señales alemanas que circulaban a través de teletipo eran etiquetadas con la clave *Fish* (pez), y a su vez las que provenían de las máquinas Lorenz, se etiquetaron como *Tunny* (atún). La Figura 41 muestra las lineas de teletipo interceptadas y rotas por los aliados.

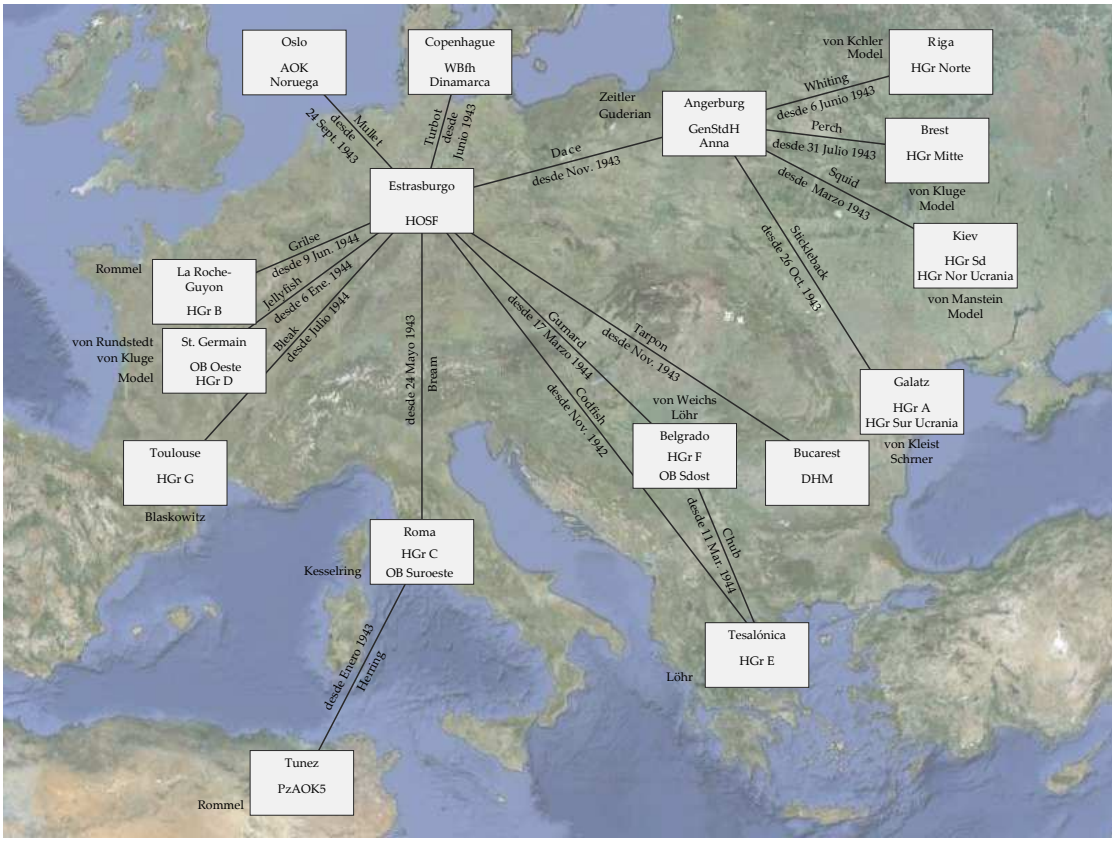


Figura 41. Lineas de teletipo interceptadas durante la 2ª Guerra Mundial. Los cuadros representan el destino de la linea de teletipo con el código de identificación alemán y el/los general/es al mando del destacamento nazi situado en ese destino. Se puede observar el nombre clave de las lineas como se conocían en Bletchley (todas con nombres de peces), y la fecha en la que se consiguió romper el código de encriptación por primera vez.

Figura 42. Equipos de operarios de Enigma.[40]

Si hiciéramos una comparativa con respecto a las Enigma, además de su mayor potencia de encriptación, las Lorenz tenían una ventaja muy clara con respecto a éstas. Mientras Enigma

[40] Imágenes cedidas por Helge Fykse (http://fykse.dnsalias.com/bilder/enigma/)

necesitaba en su operativa un mínimo de tres individuos tanto en el lugar de emisión como en el de recepción, esto es, un operador que tecleaba el mensaje con un ayudante que anotaba las letras a medida que éstas se encendían en la máquina, que finalmente proporcionaba a un operador de radio que emitía en código morse el mensaje cifrado. Del mismo modo se repetía un proceso similar pero al revés en el lugar de recepción del mensaje. Las Lorenz únicamente necesitaban un operador en el lugar de emisión y otro en el de recepción con el consiguiente ahorro de personal y por lo tanto un mayor aprovechamiento y optimización de los recursos humanos.

6.2. El algoritmo de codificación

Cada vez que se escribía un carácter desde el teclado éste era transformado mediante el Código Baudot[41]. Un carácter es representado por una secuencia de 5 bits, esto es, por una secuencia en binario compuesta de 5 dígitos, que en Bletchley Park se representaba mediante puntos y cruces (o 0 y 1 en binario). El método utilizado por la máquina Lorenz para encriptar un mensaje consistía en generar una secuencia aleatoria de 5 números binarios o bits y operar por parejas de bits, uno procedente de la letra a codificar y el otro de la secuencia aleatoria, de acuerdo con el operador booleano *XOR* al que también se conoce como *exclusivo OR*. La máquina en cuestión disponía de un total de 12 ruedas denominadas *pinwheels* con las que se generaba la secuencia aleatoria de 5 bits. De estas ruedas, cinco recibían el nombre de "chi" o χ y giraban paso a paso de modo regular, otras cinco llamadas "psi" o ψ giraban paso a paso de modo irregular, y finalmente había dos ruedas motoras, denominadas μ_1 y μ_2.

Imaginemos que se quiere codificar la letra M que en código Baudot resulta $\cdot\cdot\times\times\times$ (en binario: 00111) [23]. Los pasos a seguir son los siguientes:

1. El operador configura las ruedas χ con la posición inicial de los pines que equivalen a *off-on-on-off-on*, lo que significa que se invierten los valores de la codificación (puntos por cruces y cruces por puntos -en binario 0 por 1 y 1 por 0-) en aquellos dígitos correspondientes a la posición *on*. De esta manera $\cdot\cdot\times\times\times$ (00111) se convierte en $\cdot\times\cdot\times\cdot$ (01010).

2. En segunda instancia se aplica la suma aritmética en módulo 2 (similar a la aplicación del operador booleano *XOR*) a las parejas de bits procedentes de las secuencias que representan la letra M y la letra M modificada por las ruedas χ. Esta operación es de tal forma que si los dos bits son iguales el resultado es $\cdot$ (esto es $\times+\times=\cdot$, o bien $\cdot+\cdot=\cdot$), y si son distintos, el resultado es $\times$ (esto es $\times+\cdot=\times$, o bien $\cdot+\times=\times$)[42]. En este caso, tenemos

$$\cdot\cdot\times\times\times+\cdot\times\cdot\times\cdot=\cdot\times\times\cdot\times$$

   cuyo resultado es equivalente a 01101 en binario.

3. En tercer lugar el operador configura las ruedas ψ con la posición inicial de los pines que equivalen a *on-off-on-off-on* de modo que

$$\cdot\times\times\cdot\times\Rightarrow\times\times\cdot\cdot\cdot$$

[41] Un código inventado en 1874 parecido al ASCII de los ordenadores actuales, pero utilizado en telegrafía. El código original, conocido como Alfabeto Internacional de Telégrafía Número 1, dejó de utilizarse en 1901, ya que en su lugar apareció un código modificado por Donald Murray, donde se reordenaban algunos caracteres, propiciado por el desarrollo de un teclado parecido al de una máquina de escribir. Entonces la disposición de los bits fue disociada de las teclas del operador. Murray arregló su código de modo que los caracteres más usados produzcan la menor cantidad de cambios de estado, lo que reducía al mínimo el desgaste en el equipo. La Western Union desarrolló una nueva modificación del código de Murray. Esta modificación final supuso la supresión de algunos caracteres, y es la que se conoce generalmente como el Código Baudot, también conocido como Alfabeto Internacional de Telegrafía Nº2 (ITA2). El ITA2 todavía se utiliza en teléfonos para sordos, en radioaficionados, y en RTTY (radioteletipo).

[42] Esta operación "aritmética" fue inventada por un empleado de la división de desarrollo de la ATT llamado Gilbert S. Vernam, para permitir la aplicación intensiva en el teletipo del cifrado descrito durante la 1ª Guerra Mundial. Esta suma no era una suma convencional, sino la aplicación de una de las aritméticas binarias descritas por Boole, en particular la del operador *XOR*.

equivalente a 11000 en binario.

4. Por último se suman los dos últimos caracteres obtenidos, esto es

$$\cdot\times\times\cdot\times + \times\times\cdot\cdot\cdot = \cdot\times\cdot\times\cdot$$

equivalente a 01010 en binario, secuencia que en el código Baudot corresponde a la letra R, es decir resumiendo, la letra M se ha codificado como la letra R.

6.3. Criptoanálisis y desencriptado

La historia de la desencriptación del código de las máquinas Lorenz, resulta cuanto menos un tanto rocambolesca. Según parece el 30 de agosto de 1941, un operador alemán encargado de realizar comunicaciones a través de las Lorenz envió un mensaje cifrado de un tamaño bastante considerable, unos 4.000 caracteres tecleados directamente sin utilizar las tiras de papel, desde la ciudad de Atenas con destino Viena. El caso es que una vez enviado pacientemente el mensaje carácter a carácter, parece ser que el operador recibió otro de respuesta en alemán, solicitándole que por favor volviera a enviarlo de nuevo ya que no había sido recibido correctamente. Fue entonces cuando el operador cometió el error táctico de enviar nuevamente el mensaje con un idéntico indicador[43] (HQIBPEXEZMUG) de la máquina Lorenz a como lo había hecho la vez anterior, excepto que esta vez abrevió algunas de las palabras eliminando algunas letras de la terminación de las mismas. Este hecho constituyó un error gravísimo, ya que no respetó una de las normas básicas de la criptología, lo que puso de manifiesto una debilidad en las Lorenz, permitiendo que el equipo de criptoanalistas de Bletchley Park liderados por John Tiltman (1894-1982) comenzaran a analizar el código *Tunny*.

Tiltman, que gozaba de una reputada posición debido a sus trabajos contra las cifras militares japonesas, y algunas cifras alemanas entre otras, comenzó su análisis mediante una ingeniosa técnica. Si por ejemplo sumamos los caracteres J y P, obtenemos L; si a L le sumamos nuevamente P, obtenemos J, que era el carácter de partida.

Figura 43. John Hessel Tiltman.[44]

$$\times\times\cdot\times\cdot + \cdot\times\times\cdot\times = \times\cdot\times\times\times \Rightarrow \times\cdot\times\times\times + \cdot\times\times\cdot\times = \times\times\cdot\times\cdot$$

Una vez sumados los dos textos cifrados, obtuvo una cadena de caracteres que resultaba ser la suma de dos textos planos, esto es si tenemos P_1 y P_2, textos planos, y les sumamos la secuencia K para obtener los textos cifrados C_1 y C_2 ($P_i + K = C_i$, $i = 1, 2$), entonces al sumar los dos textos cifrados, obtendremos la suma de los dos textos planos, ya que en virtud de la propiedad anterior $C_1 + C_2 = (P_1 + K) + (P_2 + K)$, pero como hemos visto antes $K + K = 0$ (considerando por 0 el elemento neutro de esta aritmética). En este punto es necesario observar que si realizamos la suma de dos textos cifrados idénticamente iguales con la misma clave, el resultado es una secuencia de elementos neutros, por lo que los cambios pequeños introducidos por el operador del mensaje fueron lo suficientemente significativos para poder realizar el ataque criptológico. Una vez realizó la eliminación de la secuencia de cifrado, Tiltman sabía que cada carácter del texto resultante era la suma de otros dos que en el mensaje original distaban unas pocas posiciones. Comenzó entonces la tarea que requería una

[43] Con anterioridad a octubre de 1942, los operadores alemanes, conforme al libro de códigos que les era entregado mensualmente, establecían en el preámbulo del mensaje cifrado con un código Tunny una secuencia de 12 caracteres que se denominaba *indicador*, relacionado directamente con la configuración inicial de cada una de las 12 ruedas de las Lorenz. En ocasiones escribían 12 nombres, por ejemplo Martha, Gustav, Otto, Ludwig, ..., que se correspondía con el indicador "MGOL ...". Si el emisor escribía el anterior indicador, el receptor sabía que la primera rueda ψ debía configurarse en la posición X de acuerdo al libro de códigos, siendo X la configuración de la letra M en el libro de códigos para el día de emisión del mensaje.

[44] http://www.rutherfordjournal.org/article030109.html

mayor inspiración, que consistía en adivinar qué palabras combinadas (o sumadas) con el texto obtenido, podían revelar el mensaje original. Tiltman ya había demostrado sus cualidades "adivinatorias" en anteriores ocasiones, una cualidad adquirida y entrenada a lo largo de sus años de servicio. Tiltman, entre muchos de sus logros, había descrifrado un mensaje cifrado mediante el código de Vernam en el verano de 1941. Un resultado directo de la estrategia seguida por Tiltman, que le había llevado 10 días, significaba que sumando el texto plano a cualquiera de los dos mensajes cifrados interceptados, se obtenía la secuencia de caracteres de la clave utilizada para cifrar los mensajes. Fue en ese instante cuando todo el equipo de Tiltman aunó esfuerzos con la esperanza de intentar hallar alguna lógica que explicara la aparente aleatoriedad de los caracteres obtenidos.

Figura 44. William Thomas Tutte.[45]

¿Era posible que los alemanes hubieran inventado un sistema que generara secuencias aleatorias de manera sincronizada? Si fuera así, no cabría menor esperanza de éxito en la empresa en la que los británicos se acababan de enrolar. Por el contrario, mantenían el deseo de encontrar algún tipo de sistematización similar al que habían sido capaces de obtener con la Enigma. Sin embargo, el gran inconveniente con el que contaban era que nadie había llegado a ver nunca ninguna máquina similar, y la poca información que tenían sobre ella era muy pobre. Con este desamparado panorama, y tras muchos intentos infructuosos de descubrir algún tipo de sistematización que explicara aquella aparente aleatoriedad, en las navidades de 1941, Gerry Morgan, director de investigación del departamento de Tiltman, se acercó a la mesa de Bill Tutte (1917-2002), un estudiante de química de la Universidad de Cambridge, y le dijo *"Mira a ver que puedes hacer con esto ..."*. Tutte, que había sido rechazado en Bletchley Park para la desencriptación de Enigma, fue reclutado por el propio Tiltman para su equipo de criptoanalistas. Tutte ya tenía experiencia en tareas criptoanalíticas con el código Hagelin y la máquina sueca C-36. De inmediato se puso a trabajar para averiguar el funcionamiento de las Lorenz. Paradójicamente, a diferencia de las Enigma, la ruptura del código de las Lorenz fue relativamente más sencilla. Tutte, que estaba muy familiarizado con el método de Kasiski ya que había sido instruido en él durante su fase de reclutamiento, comenzó estudiando patrones de repetición de dicho mensaje. Recordemos que aunque el método de Kasiski estuviera diseñado para romper la cifra Vigènere, podía resultar muy útil en general a la hora de encontrar comportamientos periódicos sistemáticos de la clave en multitud de cifrados. Tutte colocó al principio los caracteres cifrados en código Baudot en vertical en siete filas de 575 caracteres cada una. El porqué utilizó esta cantidad es debido a que al colocar todos los caracteres del mensaje cifrado en un rectángulo, observó ciertas repeticiones primero cada 23 posiciones y después cada 25. Tras multiplicar estos números ($23 \times 25 = 575$), consideró oportuno realizar esta suposición. Al principio no parecía haber demasiadas coincidencias, pero para su sorpresa observó que existían algunas repeticiones en una diagonal, y que parecía que obtendría mejores resultados si configuraba el mensaje con un periodo de 574 caracteres. Así lo hizo y observó con gran satisfacción que se producían un gran número de repeticiones de patrones de longitud 5 o 6. Entonces realizó un nuevo intento con un periodo de 41, ya que éste es un factor primo de 574, y los resultados fueron asombrosamente aún mejores. Poco a poco fue descubriendo la configuración de funcionamiento de las Lorenz, lo cual era sorprendente ya que nunca tuvo delante ninguna de estas máquinas.

La máquina Lorenz contaba con lo que hoy día conocemos como generador de *números aleatorios*, que no es otra cosa que una clase de algoritmo que se utiliza en la programación de los modernos ordenadores para la obtención de números pseudoaleatorios. Desde un punto de vista mecánico cada una de estas ruedas o *pinwheels* poseía un cierto número de posiciones sobre su periferia con un perno o pin que admitía dos posiciones, *on* u *off* (encendido o apagado), que durante el giro de la rueda afectaban o no a otras partes de la máquina generándose secuencias

[45] http://www.newmarketlhs.org.uk/personalities5.htm

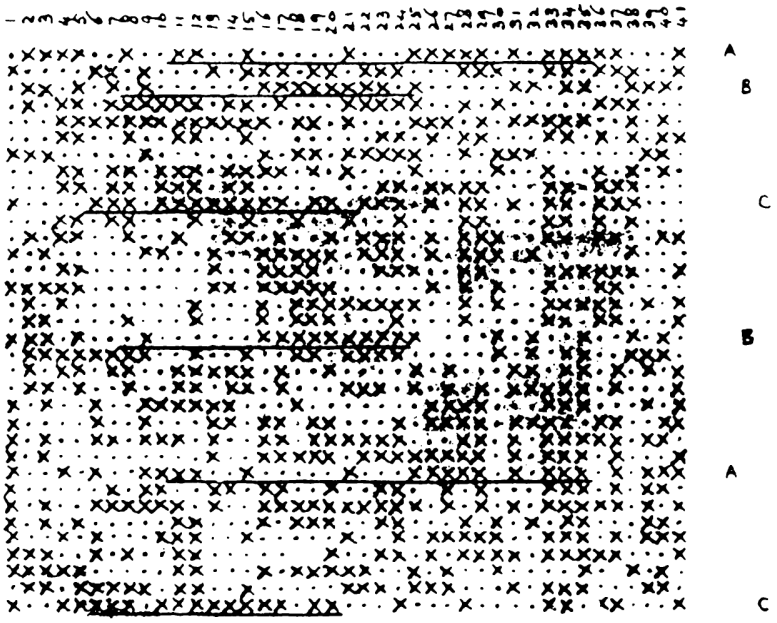


Figura 45. Exámen de periocidad de la rueda χ_1, repeticiones de Kasiski: A, B, C. Secuencias escritas en filas de 41 caracteres de longitud. Manuscrito de Tutte. [1]

de pulsos *on/off* o si se prefiere secuencias de bits $1/0$. El número de pernos o *pins* era variable en cada rueda, de modo que χ_1, χ_2, χ_3, χ_4 y χ_5 tenían 41, 31, 29, 26 y 23 respectivamente, mientras que ψ_1, ψ_2, ψ_3, ψ_4 y ψ_5 presentaban 43, 47, 51, 53 y 59 cada una de ellas, y finalmente las dos ruedas motoras μ_1 y μ_2 contaban con 37 y 61 respectivamente. Las ruedas χ giraban todas una posición para cada carácter. Las ruedas ψ también giraban todas a la vez, pero no con cada carácter. Su movimiento estaba controlado por las dos ruedas motoras μ. En las SZ40 la rueda μ_1 giraba una posición con cada carácter, pero la rueda μ_2 únicamente giraba cuando el *pin* de la periferia estaba en la posición de encendido *on*. Si el *pin* de la rueda μ_2 estaba encendido, entonces todas las ruedas ψ giraban. El orden de las ruedas era (de izquierda a derecha): χ_1, χ_2, χ_3, χ_4, χ_5, μ_2, μ_1, ψ_1, ψ_2, ψ_3, ψ_4, ψ_5. Los modelos SZ42A y SZ42B estaban dotados de un mecanismo aún más complejo. Como puede observarse el número de *pins* de una rueda era un número primo relativo al de otras ruedas, ya que de esta forma se hacía máximo el periodo combinado de todas las ruedas, y de este modo el patrón de repetición. Con un total de 501 *pines*, esto suponía 2^{501} que es aproximadamente 10^{151} posibilidades de cifrado con $1,6 \times 10^{15}$ posiciones iniciales de las ruedas posibles. Sin embargo, si los cinco impulsos se consideraban de manera independiente, los números resultantes eran más manejables. El producto del periodo de rotación de cualquier par de ruedas χ supone entre $41 \times 31 = 1271$ y $26 \times 23 = 598$. Esta clase de ingenio mecánico se considera hoy en día como uno los predecesores de lo que en electrónica y en criptografía se conoce con el nombre de *registros de desplazamiento alimentados linealmente* (en inglés *Linear Feedback Shift Registers*, abreviadamente *LFSK*). Cuatro meses después de haberle sido encomendada la tarea a Tutte, y una vez el código Lorenz había sido descifrado, en Bletchley Park se mandó construir una máquina electro-mecánica, a la que se le bautizó con el nombre de *máquina Tunny*, cuya finalidad era precisamente sistematizar las tareas de descodificación de las Lorenz.

En una primera instancia, Tutte había desarrollado un método para establecer la configuración inicial de las Lorenz "a mano". Sin embargo este método no resultaba operativo, ya que el descifrado de un simple mensaje podía llegar a alargarse varias semanas en el tiempo, por lo que en la mayoría de las ocasiones el mensaje había perdido ya todo el interés, pues hacía referencia a órdenes ya obsoletas, de las cuales era imposible sacar ninguna ventaja desde el punto

de vista estratégico. Por ello, era necesario desarrollar un nuevo método capaz de obtener rápidamente si no el mensaje plano íntegro, sí una gran mayoría de caracteres que ayudaran a la inteligencia británica a adelantarse a los acontecimientos.

En noviembre de 1942, Tutte desarrolló un ingenioso método con el que si bien no se obtenía la traducción exacta de los mensajes, sí que lo hacía en una gran proporción. Este método fue bautizado con el nombre de *Método Estadístico*. Los cálculos necesarios se llevaban a cabo mediante la comparativa de dos secuencias de caracteres en código Baudot, puntos y cruces (similar a 1 y 0 como anteriormente se hizo referencia), y llevando a cabo un recuento del número de veces que cada uno de ellos tenía un punto o una cruz en la misma posición. Tutte puso en conocimiento de Max Newman, jefe de la sección de desarrollo mecánico en Bletchley Park, y éste le sugirió utilizar contadores electrónicos de alta velocidad con el fin de automatizar el proceso.

7. Colossus. El primer ordenador electrónico

Una vez Bill Tutte había formalizado el trabajo de desencriptación del código de las Lorenz, surgía nuevamente la necesidad de sistematizar todas las tareas de desencriptado. Del mismo modo que las *bombe* habían surgido para mejorar la eficacia de las tareas de descifrado de las Enigma, *Colossus* fue construido para lograr una optimización de estas mismas tareas en las máquinas Lorenz. Colossus puede ser considerado en cierto modo, la primera máquina programable, electrónica y digital, y por sus características, aunque con ciertas reservas, se ganó el derecho de ostentar el título de primer ordenador de la historia de la computación.

La idea original para la construcción de Colossus fue desarrollada por el matemático Max Newman (1897-1984) y todo un equipo de técnicos de Bletchley Park, que previamente se habían encargado del desarrollo de la *Heath Robinson* y posteriormente la *Old Robinson*, y la *Super Robinson*, todas ellas máquinas optomecánicas que supusieron un primer intento de sistematizar el método desarrollado por Tutte. Sin embargo las *Robinson* resultaron ser máquinas poco eficientes desde el punto de vista operativo, ya que necesitaban dos cintas, una con el mensaje cifrado y otra con una secuencia de números aleatorios obtenidos a partir de ruedas similares a las de las máquinas Lorenz. Desafortunadamente cuando se intentaba aumentar la velocidad de lectura de datos por encima de los 1.000 caracteres por segundo, esta última cinta se estiraba más de la cuenta, produciendo graves errores. Tommy Flowers (1905-1998), un ingeniero de la *British Post Office Research Station* en Dollis Hill, al noroeste de Londres, fue el encargado de desarrollar el primer prototipo de Colossus. Flowers ya había colaborado previamente en el desarrollo de varios proyectos en Bletchley Park, incluido la invención de algunos componentes de las *bombe* de Turing como los dispositivos rotatorios de alta velocidad. La verdadera genialidad de Flowers en la construcción de Colossus radica fundamentalmente en la utilización de unos nuevos circuitos electrónicos a base de *válvulas* en lugar de los relés tradicionales en la segunda cinta que contenía los números aleatorios, lo cual aumentaba la velocidad de lectura de datos a la vez que la fiabilidad mejoraba ostensiblemente, llegando a conseguir velocidades de lectura de 5.000 caracteres por segundo, lo que suponía unos doce metros de cinta.

El ordenador Colossus llegó a tener unas 1.500 *válvulas*, *tiratrones* y *fotomultiplicadores*. Una *válvula* o tubo de vacío es un componente electrónico que es el antecesor de los actuales diodos y transistores, que en general sirve para incrementar el voltaje dentro de un circuito. El *tiratrón*, otra clase de válvula utilizada en los circuitos de Colossus, era un tubo relleno de gas, por ejemplo neón o xenón. Su comportamiento era el de un rectificador que funcionaba como un interruptor eléctrico. Este dispositivo se utilizaba con el fin de grabar 1 bit. Conectando varios de estos dispositivos entre sí se lograba un circuito, una *memoria*, conocida hoy día como *registro de desplazamiento*, o más comúnmente denominado *tiristor*. Los *fotomultiplicadores* eran un tipo de

[46] http://www.colossus-computer.com/colossus1.html

Figura 46. De izq. a drcha. Max Newman, Tommy Flowers, W. W. Chandler y Donald Mitchie.[46]

válvulas cuya finalidad principal era la detección de luz. Aplicando estos dos últimos componentes, tiratrones y fotomultiplicadores, Colossus era capaz de leer los caracteres de una cinta de papel aplicando una función lógica previamente programada a cada carácter. Si el resultado de aplicar la función lógica era verdadero la lectura de la cinta y el análisis posterior seguían su curso.

En enero de 1944, y tras algo más de un año en construirse, apareció la primera versión de Colossus, denominada Mark I. Rápidamente le siguió la Mark II en junio de ese mismo año. A finales de la 2ª Guerra Mundial, había un total de 10 máquinas Mark II en Bletchley Park. El volumen de dichas máquinas era considerable ya que cada una de ellas ocupaba una gran habitación en los sectores F y H. Al igual que ocurrió con las Bombe, Churchill ordenó su destrucción una vez finalizada la guerra por motivos de seguridad, quemándose todos los planos con el diseño y circuitos. Sin embargo dos de ellas sobrevivieron, trasladándose a Cheltenham, donde fueron utilizadas durante la Guerra Fría hasta que finalmente se ordenó su destrucción en la década de 1960. Debido al secretismo impuesto por las autoridades británicas, tanto Colossus, como sus creadores nunca gozaron del mérito que merecieron en la historia de la computación, ya que la máquina norteamericana ENIAC construida en 1946 y sus creadores fueron los que se llevaron los méritos y el reconocimiento público.

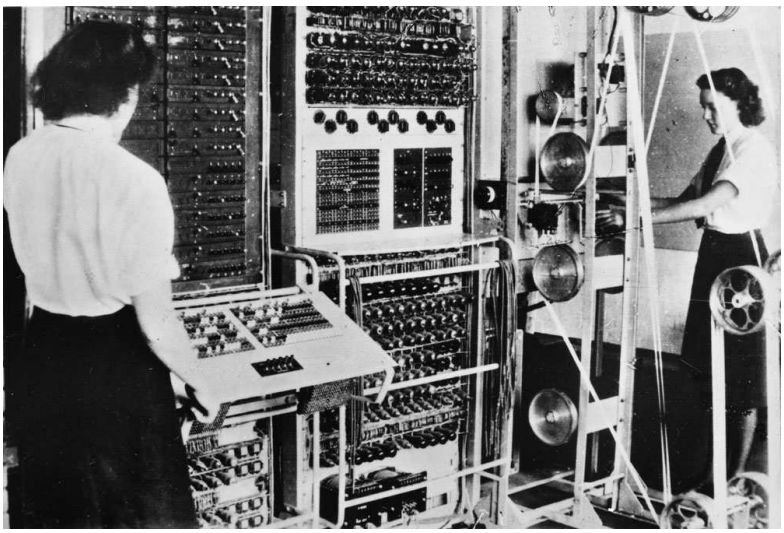


Figura 47. Colossus y dos operadoras del Servicio Naval Real (Royal Naval Service). Dorothy Boisson (izq.) y Elsie Booker (drcha.) (Bletchley Park, 1943).[47]

[47] The National Archives, http://blog.nationalarchives.gov.uk/blog/innovating-at-the-national-archives/

Tony Sale (1931-2011), un antiguo trabajador del servicio británico, fue nombrado conservador del Museo de Bletchley Park al inicio de la década de los 90. Hasta 1993 se dedicó a recopilar cuanta información pudo sobre la máquina Colossus con el fin de comenzar su reconstrucción. En 1994, comenzaban las primeras tareas de reensamblaje eligiéndose además la misma ubicación que una de las máquinas (la número 9) había tenido durante la guerra. Finalmente en 1996, era presentada una primera versión que trabajaba a 2 bits en lugar de los 5 con los que trabajaba la máquina original.

Referencias

[1] BAUER, F. L., *Decrypted Secretsthods and Maxims of Cryotology*, 4th Ed., Springer Verlag, Berlin, 2007.

[2] CEANO, R., *La Máquina Enigma*, http://www.kriptopolis.com/enigma, 2012. (Última consulta 20-11-2012)

[3] COOMBS, A. W. H., *The Making of Colossus*, Annals of the History of Computing, Volume 5, Number 3, july 1983.

[4] COPELAND, J., *Colossus: Its Origins and Originators*, Annals of the History of Computing, pp. 38–44, Computer Society, UK, 2004.

[5] CHRISTENSEN, C., *Polish Mathematicians Finding Patterns in Enigma Messages*, Mathematics Magazine, Nº. 80, pp. 247–273, october 2007.

[6] FERNÁNDEZ, S., *La Criptografía Clásica*, Revista SIGMA, Nº. 24, pp. 119–141, abril 2004.

[7] FLOWERS, T. H., *The Design of Colossus*, Annals of the History of Computing, Volume 5, Number 3, july 1983.

[8] GAJ, K., ORLOWSKI, A. *Facts and myths of Enigma: breaking stereotypes*, EUROCRYPT'03 Proceedings of the 22nd international conference on Theory and applications of cryptographic techniques, Springer-Verlag, Berlin, Heidelberg, pp. 106–122, 2003.

[9] HODGES, A., *The Military Use of Alan Turing*, Mathematics and War, pp. 312–325, Bernhelm Booss Bavnbek and Jens Høyrup Editors, Birkhäuser, 2003.

[10] KERCKHOFFS, A., *La cryptographie militaire*, Journal des sciences militaires, vol. IX, pp. 5—83, jan. 1883, pp. 161—191, fév. 1883.

[11] KOZACZUK, W., *ENIGMA: The Key to the Secrets of the Third Reich 1933-45*, Interpress, june 1984.

[12] LAHOZ-BELTRA, R., *Turing: Del primer ordenador a la inteligencia artificial*, Colección: La matemática y sus personajes, Nº. 24, 1ª Edición. Nívola, Madrid, 2005.

[13] MEDRALA, J., *L'Enigma polonaise en Résistance á Uzés 1940-1942. Une aventure humaine prestigieuse et dramatique*, Conférence Enigma: S'il te plait dessine-moi la Pologne, Paris, 2008.

[14] MILLER, A. R., *The Criptographic Mathematics of Enigma*, Center for Cryptologic History, 1996.

[15] ORTEGA TRIGUERO, J.J., LÓPEZ GUERRERO, M.A. y GARCÍA DEL CASTILLO CRESPO, E.C., *Introducción a la Criptografía. Historia y Actualidad*, Servicio de Publicaciones de la Universidad de Castilla La Mancha, Colección Monografías, Nº. 50, 2006.

[16] QUIRANTES SIERRA, A., *Enigma: la solución polaca (I) y (II)*, Boletín del Taller de Criptología, Nº. 18, diciembre 2003.

[17] RANDEL, B., *The Colossus*, International Research Conference on the History of Computing, Los Alamos Scientific Laboratory, University of California, June 10-15th, 1976.

[18] REJEWSKI, M., *An Application of the Theory of Permutations in Breaking the Enigma Cipher*, Applicaciones Mathematicae. 16, Nº. 4, Warsaw 1980.

[19] REJEWSKI, M., *How Polish Mathematicians Deciphered the Enigma*, Annals of the History of Computing. Volume 3. Number 3, July 1981.

[20] SÁNCHEZ MUÑOZ, J. M., *Nazis y Matemáticas*, 2ª Jornada Internacional "Matemáticas Everywhere", Castro Urdiales, 20–21 junio, 2012.

[21] SINGH, S., *Los Códigos Secretos: El arte y la ciencia de la criptografía, desde el antiguo Egipto a la era Internet*, Editorial Debate, 2000.

[22] TUTTE, W. T., *Fish and I*, Transcripcción de Conferencia en la Universidad de Waterloo (19 de junio de 1998), Ontario, Canadá, 2012.

[23] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, *Reglamento Telegráfico, Revisión de Ginebra, 1958*, Anexo al Convenio Internacional de Telecomunicaciones, Buenos Aires, 1952, Protocolo Final, Ginebra, 1959.

[24] VV.AA, *The History of Information Security: A Comprehensive Handbook*, Karl de Leeuw y Jan Bergstra (Editores), Elsevier B.V., 2007.

[25] WESOLKOWSKI, S., *The Invention of Enigma and How the Polish Broke It Before the Start of WWII*. IEEE Conference on the History of Telecommunications, University of Waterloo, Canada, 2001.

Sobre el autor:
Nombre: José Manuel Sánchez Muñoz
Correo electrónico: jmanuel.sanchez@gmx.es
Institución: Ingeniero de Caminos, Canales y Puertos. Grupo de Innovación Educativa "Pensamiento Matemático", Universidad Politécnica de Madrid, España.

Historias de Matemáticas

Las "Lecciones Académicas" de Evangelista Torricelli

Evangelista Torricelli's "Academic Lectures"

Rosa María Herrera

Revista de Investigación

Volumen III, Número 3, pp. 121–134, ISSN 2174-0410
Recepción: 19 Dic'12; Aceptación: 25 Mar'13

1 de abril de 2013

Resumen

En las Lecciones Académicas ("Lezioni accademiche"), Torricelli a la manera divulgativa dibujó un boceto de bastantes de sus ideas científicas, algunas novedosas, como la circulación general de la atmósfera. El estilo culto e irónico, pero informal, que utilizó le permitió exponer conceptos que de otra manera, dadas las circunstancias, hubiera sido casi imposible. En estas notas muestro algunos ejemplos.

Palabras Clave: Ligereza, Gravedad, Fuerza del golpe, Academia.

Abstract

The "Lezioni accademiche" by Torricelli are a set of divulgative lessons in which the Italian mathematician drew a sketch of several of his scientific ideas, some of them innovative, for instance: the general circulation of the atmosphere. His ironic and informal style allowed him to express ideas, which otherwise under the circumstances, would have been almost impossible. These notes provide some examples. Also I shall try here to sketch its value as scientific tool.

Keywords: Lightness, Gravity, Force of the Blow, Academy.

1. Introducción

En el siglo XVII florecieron por toda Europa instituciones científicas de carácter privado que se dedicaban fundamentalmente al estudio, la experimentación científica y la discusión de temas y problemas en los que los intelectuales científicos andaban empeñados. Estos centros de reunión cultural operaban en paralelo con la Universidad, y si bien en cada país tenían sus propias características e idiosincrasia, el propósito que perseguían la mayoría de ellas guardaba cierta similitud y el espíritu subyacente era común a todas o, al menos, bastante similar.

En este trabajo muestro un ejemplo de esta forma de trabajo científico, tal como se llevaba a cabo en la ciudad de Florencia, en los años que siguieron al fallecimiento de Galileo quien había

dejado sólidamente asentadas las líneas maestras de su manera de trabajar y contaba con un nutrido grupo de continuadores.

2. Contexto y ambiente

Figura 1. Portada de las "Lezioni accademiche" publicadas póstumamente en 1715

Las "Lezioni Accademiche" de Evangelista Torricelli (1608-1647) son un conjunto de textos que fueron publicados por vez primera casi un siglo después del fallecimiento del científico. Están escritas en italiano, idioma en el que fueron dictadas, y no en latín que era el idioma oficial de la ciencia, lo que es un indicio de su carácter divulgativo aunque quizá no el sentido más leve de banalización o vulgarización, sino en el más elevado de proporcionar información científica a un auditorio culto, con el propósito de crear debate y polémica y promover opiniones críticas. Hay un hecho muy interesante, en absoluto menor, introducir ideas científicas novedosas de un modo suave en un ambiente distendido.

Esta manera de proceder le permitía soslayar la rígida mentalidad oficial poco proclive a aceptar novedades ideológicas que no encajaran bien con los pilares básicos de su sistema de pensamiento o no fueran acordes con él. A pesar de estas trabas, algunas ideas lograron de una u otra manera abrirse paso y circulaban con cierta fluidez pero con discreción en la Florencia del XVII.

2.1. La actividad en las sociedades científicas

Las universidades en el seiscientos eran fundamentalmente centros de enseñanza y de preservación de la cultura de los maestros clásicos; en ese sentido, en las asociaciones intelectuales y científicas de origen privado se realizaban los trabajos experimentales más avanzados y otros eventos afines quizá menos ortodoxos.

Torricelli impartió la primera serie de lecciones en el seno de la "Accademia della Crusca"[1],

[1] Permanece en activo en la actualidad, con la naturales transformaciones.

sociedad florentina para la preservación de la lengua, de la cual formaba parte como miembro destacado y respetado; en esta institución desplegó su máxima actividad y su artillería dialéctica. De las otras cuatro conferencias dos tuvieron lugar en la "Accademia fiorentina del Disegno", la penúltima se celebró en la "Accademia dei Percossi" y la última en la Universidad de Florencia. Se convirtieron en material impreso, lecciones escritas, un siglo más tarde.

Impartió las ocho primeras lecciones entre 1642 y 1643, lo que hace pensar en que en esta época estaba plenamente integrado en la vida cultural florentina y que además era muy activo en este ámbito.

Pero aún así, quizá cuesta un poco imaginar a este clérigo circunspecto de los escasos retratos, presentando suntuosamente, con ingenio y gracia temas casi siempre de suyo sobrios. Así de una manera casi poética, mas sin perder ni un ápice de rigurosidad, convertía las sesiones en una invitación a la reflexión en la cual los asistentes se hallaban instalados en una situación cómoda.

En cuanto al formato, solo destacar que se trata de piezas de diferente longitud, que algunas fueron dictadas en varias sesiones, y que en casi todas se descubre un Torricelli fantasioso, literario, con cierto gusto por las imágenes bellas, conocedor de la mitología; un hombre erudito, culto y dotado de una fluidez verbal sorprendente y hasta graciosa. Seguramente es en estos textos donde se permitió más licencias, mayor comicidad, y quizá también, por su naturaleza de textos pensados para un intercambio vivo y directo, mayor ligereza.

2.2. Temática

Lezioni Accademiche d' Evangelista Torricelli Mattematico e Filosofo del Serenissimo Ferdinando II. Gran Duca di Toscana Lettore delle Mattematiche nello studio di Firenze e Accademico della Crusca. Firenze, per Iacopo Guiducci e Santi Franchi, 1715, *in* 4.°, *di pag.* L - 96, *col ritratto dell' Autore.*

Dopo la Prefazione, *che si sa essere di* Tommaso Bonaventuri, *stanno le* Lezioni *col seguente ordine:*

Lezione I. Ringraziamento agli Accademici della Crusca, quando da essi fu ammesso nella loro Accademia.
" II. III. e IV. Della forza della Percossa.
" V. e VI. Della leggerezza.
" VII. Del vento.
" VIII. Della fama.
" IX. In lode delle Matematiche
" X. e XI. Dell' Architettura militare.
" XII. Encomio del secol d' oro.

Furono ristampate in Milano dal Silvestri l' anno 1823 *in* 8.° *picc. con ritratto.*

Figura 2. Índice de una edición de las "Lezioni accademiche" publicadas por primera vez en 1715

Tras una primera lección de apertura, cortesía y agradecimiento a los académicos, el misceláneo índice de las Lecciones Académicas se desglosa según los siguientes puntos: La fuerza del golpe (impacto de un objeto móvil sobre uno fijo) (lecciones 2ª, 3ª y 4ª). La ligereza (lecciones 5ª y 6ª). El viento (lección 7ª). La fama (lección 8ª). Elogio de las Matemáticas (lección 9ª). La arquitectura militar (lecciones 10ª y 11ª). Alabanza del siglo de oro (lección 12ª).

La temática de estas doce charlas está bastante próxima a los tópicos que estudiaba junto a

Galileo, pero también hay cuestiones de otra índole; así, entre algunos asuntos científicamente "serios" intercaló sesiones variopintas de cierta frivolidad, curiosidades algo más mundanas.

De esta forma, entretenía, formaba y creaba una atmósfera receptiva y propicia a las inquietudes científicas que estaban de actualidad en su mundo científico.Nos encontramos, pues, gratamente con una sociedad intelectualmente activa en la que había controversia.

A su auditorio póstumo, los lectores tardíos del siglo XXI, se nos presenta este listado como un catálogo de los temas de conversación distendida que ocupaban a la sociedad florentina acomodada de la primera mitad del siglo XVII.

En el abanico de contenidos y en la forma en que son tratados queda patente la manera de mirar la naturaleza del científico y los problemas asociados a la misma. Además están los temas más leves: culturales, mundanos pero todos compartiendo el mismo tono reflexivo con adornos de tintes éticos.

3. "Lezione accademiche"

En esta sección, que está dividida en cinco apartados, voy a referir solo algunos puntos notables. Como varias de estas lecciones tuvieron cierta repercusión y provocaron controversias (creo que de eso se trataba . . .), comenzaré por ellas y me extenderé un poco más, de las otras el relato lo haré más breve, así es que esta exposición altera el orden cronológico.

Comenzaré por las lecciones quinta y sexta dedicadas a la gravedad y la ligereza, que se desarrollan en un marco aristotélico, el resultado presenta algunas ideas interesantes. Asimismo, por su relación con los estudios barométricos también tiene relevancia la lección séptima que se refiere al viento.

3.1. Grave y ligero

Las disertaciones sobre la ligereza se presentan en clave de relato mitológico, en ellas combina, poesía, con conceptos científicos y estéticos. Las protagonistas, ninfas marinas llamadas Nereidas, son tan cultas y eruditas como encantadoras. Y así en una alegoría bastante fina y humorística, estos espíritus femeninos y "leves" tratan con mucha inteligencia, elegancia y gracia temas científicos "graves" [5].

> *[. . .] Le Nereide stabilorono un giorno di voler comporre una somma di Filosofia. Aprirono la loro Accademia colà ne i profondissimi fondi dell'Oceano Sur. Cominciarono poi a scrivere i dogmi della física, conforme facciamo ancor noi abitatori dell'aria nelle scuole nostre. Vedevano queste Ninfe curiose che parte delle materia praticate descendevano nell'acqua abitata da loro, e parte ascendevano. Però súbito senza star a pensare ciò che potesse seguire negli altri elementi conclusero, che delle cose, alcune son gravi, cioè terra, pietre, metalli, e simili, poi che ne maree discendono; ma alcune son legger, come aria, suveri, cera, olio, e una gran parte dei legnami, perché salgono dentro l'acqua. Se elle procedessero temerariamente, o no, seguitando la semplice scorta del senso, senza corregerla con l'uso della ragiones, io non lo so: so bene, che potrebbero difendere la causa loro, con l'esempio reverito di Filosofi venerabili. Io fabbricando poi chimere fra me stesso mi accorsi, che era comportabile l'errore di inconsiderazione commesso da quelle fanciulle marine, le quali pronunziarono per leggere molte cose da noi tenute per gravi. Fantasticavo con l'immaginazione, e mi dipingevo sopra la testa un altissimo pelago di argento vivo. Ecco che io sono nato e allevato nel fondo di questo fluido metallo. Convienmi ora scrivere un trattato sopra la leggerezza e la gravità. Subito fatta un tantino di reflessione, discorro così. Sono tanti anni che io pratico in questo gorgo dove per esperienza continua ho veduto sempre, che bisogna tenere legate tutte le sorti di roba, fuor*

30 LEZIONI

DELLA LEGGEREZZA

LEZIONE QUINTA.

SE alcuno giammai si ritrovò, che giustamente meritasse il titolo di leggierezza, nessuno per mio credere può mostrarsi più degno di quest' attributo, che colui, il quale ardisca di pronunziare, che tutte le cose create sieno leggieri. Che l' incudini, le colonne, le montagne sieno corpi non solamente privi di gravità, ma anco tali, che abbiano dentro di se principio di leggerezza positiva, e assoluta, sembra proposizione piuttosto di temerità, che di filosofia. Nondimeno Serenis. Principe, Degnissimo Arciconsolo, Virtuosissimi Accademici, nondimeno avrò io ardimento in questo giorno, costituirmi reo di tanta temerità; supplicando però l' esquisitezza de' vostri giudizi a non fulminare contro di me la sentenza, prima che sieno state esposte le mie ragioni. Esamineremo con questo discorso le opinioni antiche circa la gravità, e la leggerezza. Con un

Figura 3. Reproducción del inicio de la lección quinta: "Della leggerezza"

> *che l'oro, acciò elle non sormontino, e se ne fugghino verso l'alto. Dunque senza dubbio tutte le cose son leggere, e hanno inclinazione per natura di andare all'insù, tanto l'acqua, quanto la terra, come anco le pietre, i metalli, e in somma ogni altra cosa corporea fuor che l'oro, il quale solo si trova descendente nell'argento vivo. Al contrario poi penserei che la filosofia delle Salamandre (supposto che elle abitino nel fuoco) fusse per stabilir ogni cosa per grave, compresavi ancor l'aria». [...]*

Esta simpática historia de las Nereidas filósofas, a la ingeniosa manera de un cuento de hadas, el conferenciante esboza conceptos no intrascendentes.

Así, estas criaturas ponen en marcha en el fondo del océano una academia en la cual, con armonía y perspicacia, piensan y conversan sobre física a semejanza de los seres humanos, preparando sesudas y gráciles lecciones en las que hacen recuento de los cuerpos que ascienden y de los que se depositan en el fondo. Al comprobar estas diferencias deciden usarlas para establecer una clasificación de los objetos que resultan así agrupados en "graves" y en "ligeros".

Torricelli reflexiona con este argumento sobre la distinta percepción de estos dos tipos de objetos, y así discierne que las Nereidas tienen por graves cosas que los hombres en la superficie de la tierra consideramos ligeras. Pertrechado con esta reflexión, da paso un hacia delante y fantasea sobre la posibilidad de vivir sumergido en un mar de mercurio para analizar cómo se escribiría en este medio ambiente un tratado sobre la ligereza y la gravedad. En él, naturalmente, cambiaría el listado de las cosas que pesan y flotan ..., y piedras, metales y toda clase de objetos similares pasarían a engrosar el gran grupo de los cuerpos ligeros, todas las cosas excepto el oro, y por tanto para que las cosas permanecieran en lugar conveniente habrían de estar siempre sujetas ...

El párrafo continúa con la filosofía de la salamandra (supuesto este animal habitante del fuego) para el cual todas las cosas serían graves, incluso el aire.

Esta envoltura suaviza pero no enmascara la enjundia del tema. El lector actual debe recordar el ambiente intelectual en el que se efectuaban los razonamientos forjado en la noción aristotélica de "lugar natural", según la cual los cuatro elementos primordiales (tierra, agua, aire y fuego) se encuentran dispuestos en esferas concéntricas en las cuales el aire ocupa su sitio, tiene su lugar natural, y en esta situación no ejerce ningún tipo de presión.

Dicho de otro modo, el aire, sustancia ligera, carecería de peso (la idea aristotélica de ligereza no tiene apenas nada que ver con la densidad).

El objeto que perseguiría Torricelli en esta lección sería conducir a su auditorio por un camino diferente para generar cuando menos a la duda, demostrando mediante paradojas que la disposición de los elementos en la esfera terrestre está regulada por la hidrostática de Arquímedes y no por el concepto más o menos metafísico de lugar natural.

3.2. Una lección sobre el viento

ACCADEMICHE. 45

DEL VENTO.

LEZIONE SETTIMA.

LA Natura, Sereniſs. Principe, Degniſſimo Arciconſolo, Virtuoſiſſimi Accademici, fra le coſe ſue più naſcoſe, e più impenetrabili, non mi par, che alcuna ve n'abbia, occultata con maggior ſegretezza, che quell' accidente dell' aria, il quale con nome di Vento comunemente ſi appella. Le piogge, e le grandini, l'iridi, e le comete, le nevi, i fulmini, i baleni, i parelj, e altre impreſſioni, che ne' campi dell' aria, o ſi generano, o compariſcono, hanno per mio credere, poco nota l'origine, e molto malagevole la con-

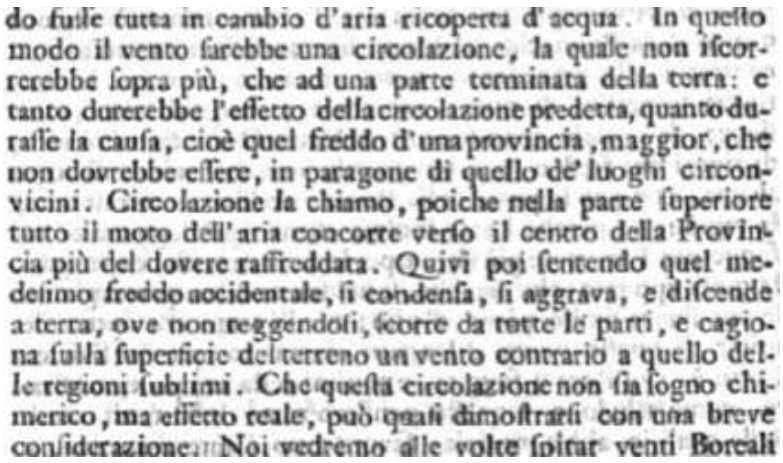
Figura 4. Reproducción del inicio de la lección séptima: "Del vento"

La conferencia séptima no tiene el carácter poético ni alcanza el nivel de lirismo de las lecciones quinta y sexta, sin embargo, el cambio de tono no va en detrimento del interés del contenido. Versa sobre el viento, y la podemos vincular con sus estudios barométricos, sobre la presión atmosférica, el peso del aire y el vacío.

Torricelli en un discurso erudito más inclinado hacia lo dialéctico que a científico, pero con una gran coherencia interna, explica las innumerables contradicciones de las opiniones sostenidas tradicionalmente sobre el viento. En esta lección, recuerda que el estudio del viento, la lluvia ... (en lenguaje actual la meteorología) para Aristóteles era un asunto de la cosmología de los cuatro elementos y posiblemente en su opinión había de ser tratado desde otra perspectiva.

Así explicaba que el viento es invisible por sí mismo aunque lo conocemos por la gran cantidad de efectos que produce, velas que se hinchan, banderas que ondean, plantas que se agitan, el polvo que se mueve y otros accidentes similares. Efectos que son indicio de un aspecto invisible de la naturaleza tanto para los ojos del cuerpo como para los ojos del intelecto. Parece como si la naturaleza quisiera ocultar el viento tanto a los sentidos como a la razón, y el científico se presenta con "cierta modestia" manifestando algo así como que "comparece a comunicar públicamente esa ignorancia".

Por estas razones algunos autores consideran a Torricelli no ya como uno de los precursores más o menos lejanos de la meteorología, sino incluso casi como uno de los fundadores de dicha rama. Y quizá no sea un desatino, pues de hecho al final de esta lección presenta el concepto de circulación general del aire. (Véase el documento de la Figura 5)



do fuile tutta in cambio d'aria ricoperta d'acqua. In quello modo il vento farebbe una circolazione, la quale non iscorrerebbe sopra più, che ad una parte terminata della terra: e tanto durerebbe l'effetto della circolazione predetta, quanto durasse la causa, cioè quel freddo d'una provincia, maggior, che non dovrebbe essere, in paragone di quello de' luoghi circonvicini. Circolazione la chiamo, poiche nella parte superiore tutto il moto dell'aria concorre verso il centro della Provincia più del dovere raffreddata. Quivi poi sentendo quel medesimo freddo occidentale, si condensa, si aggrava, e discende a terra, ove non reggendoli, scorre da tutte le parti, e cagiona sulla superficie del terreno un vento contrario a quello delle regioni sublimi. Che questa circolazione non sia sogno chimerico, ma effetto reale, può quasi dimostrarsi con una breve considerazione. Noi vedremo alle volte spirar venti Boreali

Figura 5. Fragmento de la lección séptima. Torricelli se refiere explícitamente a la circulación del aire

Knowles Middleton, en su libro sobre la historia del barómetro [4], compara la importancia de este instrumento con la del telescopio y la de la pila de Volta en cuanto al valor que conllevan para sus respectivas ramas de la física. Si bien el barómetro o tubo de Torricelli (este es su nombre originariamente) no fue utilizado para medir la presión atmosférica hasta algún tiempo después de fallecido el científico.

3.3. Las ideas de Torricelli sobre la gravedad

La concepción torricelliana de la gravedad se capta muy bien en las disertaciones segunda, tercera y cuarta que pronunció en la Academia della Crusca, que corresponde a la lección sobre la "fuerza del golpe". Se trata de un estudio acerca de los cuerpos que caen sobre objetos inmóviles, para llamar la atención sobre los asistentes en los efectos de la fuerza de los impactos. Conviene recordar que estos trabajos mecánicos ya figuraban entre los problemas sobre los que con cierta profusión y confusión había trabajado Galileo. Y que la gravedad era considerada en la visión galileana como un atributo intrínseco del objeto.

Si bien desde una mirada actual cabría considerar que en la primera mitad del XVII no se había madurado este concepto y otros conceptos mecánicos afines (o que surgen en este contexto) y tampoco las herramientas necesarias para desarrollarlos.

No obstante, la lección tiene la virtud de la claridad, la pulcritud de la presentación de algunas buenas intuiciones y la fluidez expositiva que iría mejorando y perfeccionando y que posiblemente alcanzó su mejor fortuna en las sucesivas conferencias.

En un lenguaje cargado de metáforas muy buenas, ingeniosas y algunas muy líricas, y con expresiones y reflexiones en torno a algunos temas que sorprenden a la mirada actual, y que desvelan algunas concepciones próximas a nuestra visión de la mecánica clásica, sin embargo, otras que se hallan severamente distanciadas. La riqueza lingüística que en estos textos despliega, de haber sido desarrollada sobre unos conceptos madurados y desarrollados más ampliamente, o si se hubiera llevado a efecto sobre algunas ideas mejor construidas, habría producido un resultado brillante.

Proponía a su auditorio experimentos mentales que consistían en producir impactos sobre

bloques de mármol golpeándolos con distinta contundencia, para lo cual aplicaba fuerzas de diferente intensidad.

Note el lector que este matemático consideraba la gravedad como una fuerza que en los cuerpos naturales genera "momento", un impulso de magnitud similar al peso del cuerpo [7].

> *"La gravità en i corpi naturali è una fontana dalla quale continuamente scaturinosco momenti."*

DELLA FORZA
DELLA PERCOSSA

LEZIONE SECONDA.

Egli è vero il detto del Filoſofo, che quelle operazioni della natura, delle quali non ſappiamo le cauſe, ſi ſtimano miracoli, miracoli più maravigliosi d'ogni altro dovranno ſtimarſi gli effetti di quella facoltà, che univerſalmente ſi chiama Meccanica. Maravigliosi dico, Sereniſſimo Principe, Degniſſimo Arciconſolo, Uirtuoſiſſimi Accademici, non ſolo per l' operazioni ſtupende che fanno, ma anco per l' occultazioni delle cauſe onde derivano. La Libra, la Leva, e l' Argano ſono macchine già note al Mondo, e divulgate nel teatro della fama colle dimoſtrazioni del ſapiente di Siracuſa. Ma la Vite, il Cuneo,

Figura 6. Fragmento de la lección segunda. La gravedad como la concebía Torricelli

En un ejemplo "lanza" un grave de 100 libras sobre una losa de mármol (que es capaz de soportar 1000 libras) y como la reacción de la losa al peso del cuerpo es de 1000 y no de 100 libras tendrá capacidad para sostenerlo [7].

> *"[…] il marmo sottoposto in ciascuno istante del tempo che corre, va continuamente corrispondendo al grave premente con un momento di resistenza non come cento ma come mille […]"*

La resistencia del mármol neutraliza a la componente pasiva o estática de la gravedad del cuerpo.

> *"[…] Il nostro grave produce in ogni istante di tempo una forza di cento libre […]"*

Así en 10 instantes de tiempo brevísimo producirá diez veces la fuerza de cien libras. Pero no podremos contemplar la suma de estas fuerzas, porque cuando la segunda fuerza (o "momento") nace, la primera se ha desvanecido …

Pero, ¿qué sucederá si el cuerpo golpea violentamente la losa? [7].

La respuesta de Torricelli, apoyándose en razonamientos y concepciones de Galileo sobre el movimiento, conlleva en ocasiones expresiones del tipo "naturalmente acelerado",

> *"[…] la definizione medesima che el Galileo adduce del moto naturalmente accelerato […]"*

y explica que en el descenso la "gravedad" del cuerpo genera un impulso siempre parecido al peso del cuerpo que en esta ocasión no puede ser neutralizado por la resistencia de la losa, porque los "impulsos" se van sumando y cuando el cuerpo impacta en la losa, esta se rompe.

La última disertación sobre la "fuerza del golpe" que pronunció Torricelli en 1643 suscitó bastantes controversias y discusiones, e incluso aparece registrado en el diario del secretario de la Accademia de la Crusca una anotación sobre el desconcierto y la polémica que esta charla suscitó[2].

"una dotta lezione paradossica del grave e leggeri, sopra la quale si fecero lunghi discorsi."

En ella, al gusto de Galileo, criticó el concepto aristotélico de "ligereza positiva" considerada como una cualidad intrínseca de los cuerpos; la distinción absoluta entre cuerpos pesados y cuerpos ligeros debida a Aristóteles no era del agrado torricelliano que seguramente encontraba muchas inconsistencias en ellas, prueba de ella fueron las lecciones sobre la ligereza que impartió posteriormente (véase 3.1). Sin embargo, se pone de manifiesto la confusión que se encuentra en sus concepciones. Hay que situarse en la posición intelectual de los científicos galileanos del XVII para entrar con convicción en esta polémica y poder captar algunos de sus matices.

Desde un punto de vista post-newtoniano no cabe la disociación de la idea de ligereza absoluta con la de gravedad como cualidad intrínseca de los cuerpos ya que van indisolublemente asociadas, con Newton cambió la mirada sobre la gravedad que pasó a la categoría de una forma de relación entre dos objetos masivos.

3.4. Final de la etapa en "la Crusca"

En 1643, el 13 de agosto dictó la última lección en la sede de la Accademia della Crusca, fue una conferencia no científica, pero es muy útil para el dibujo del perfil del científico y de los gustos de la época. La temática seguramente la eligió él, no he encontrado información en contra, y esto nos da un retrato de las preocupaciones de una sociedad culta, rica y acomodada, construida sobre los cimientos que pusieron los habitantes que forjaron su personalidad,

DELLA FAMA

LEZIONE OTTAVA.

Bacco l'inventor delle Corone, e come vogliono Plinio, e Diodoro, ritrovator della Medicina, e dell' arte mercantile, Capitano prudentiſſimo, e inſaziabile di gloria; Bacco il primo trionfatore del Mondo vinto, che traſcorſa con paſſaggio trionfale l'Europa in parte, e l'Aſia tutta, non finiva le glorie, ſe non gli mancava la terra; l'uccisore de' Tiranni, il domatore dell'Oriente, il ſeveriſſimo Legiſlatore, e punitore dell'ebrietà, vien tradito oggi, e aſſaſſinato dalla Fama.

E per qual cauſa un Eroe così valoroſo non ſa dipingerſi

Figura 7. Fragmento inicial de la lección octava, dedicada a la "Fama"

[2] Benedetto Buonmattei en "Evangelista Torricelli Accademico della Crusca" Amerindo Camelli p.18

comerciantes aventureros y viajeros que surcaron el mundo en busca de nuevos productos y que además de enriquecerse trajeron prosperidad a la ciudad, personas de otras regiones de la Tierra, que establecieron como empleados o servidores y una visión más amplia y abierta de la vida que la de los campesinos toscanos. La dedicó a la Fama.

El enfoque que dio a esta disertación fue el de la distinción entre fama y gloria, considerando la fama como de rango menor, la fama sinónimo del aplauso del pueblo mientras la persona está presente. La gloria otra cosa, según el científico, puede presentarse en vida, sin embargo perdura e incluso crece en la muerte.

Se trata de una preocupación quizá no tan frívola como pudiera parecer a primera vista, sino de una reflexión moral y ética interesante en torno al valor de la vida humana según su desempeño. La persona que alcanza la gloria, en opinión de Torricelli, ha cultivado unos méritos, ha realizado una obra merecedora de alcanzar la posteridad, atributo que no va asociado a la fama, algo más liviana y efímera.

3.5. Las otras lecciones

En la versión impresa de 1715, que es a la que está referida este trabajo, las otras lecciones aparecen un poco más separadas de la temática física principal de las anteriores. Corresponden a otra etapa o periodo. Las dos que dedicó a la arquitectura militar fueron pronunciadas en la Accademia del Disegno, en ellas no aparece ni un solo dibujo, es la transcripción de disertaciones, cabría preguntarse: ¿en la presentación real haría algún tipo de dibujo auxiliar? La última es un elogio al siglo de oro realizada en la Accademia dei Percossi, ambas en Florencia.

DELL' ARCHITETTURA MILITARE.

LEZIONE DECIMA.

Ra tutte l'arti, che dall' induſtria umana, o per eſercizio dell' ingegno, o per ornamento delle Città, ſieno giammai ſtate ritrovate, io per me credo, che le più degne, e le più nobili, ſenza contradizione alcuna, debbano giudicarſi la Pittura, e la Scultura. Arti che quaſi emule dell' onnipotenza creatrice, o cavano da rozzi ſaſſi figure poco men, che ſpiranti, o producono ſulle tele immagini colorite,

Figura 8. Fragmento inicial de la lección décima

Esta dispersión de temas y de sedes, frente a la unidad temática que se corresponden con la actividad en la misma institución (Accademia della Crusca), posiblemente son indicadores de un cambio de situación, o de obligaciones e intereses. La actividad académica posiblemente dejara de ser primordial y tal vez fuera el resultado de los compromisos derivados de la posición que ocupaba. No obstante, el despliegue de brillantez y riqueza expresivos no fueron menores, seguramente le servía para cultivar una faceta de su personalidad que le agradaba y quizá debido a su formación eclesiástica conociese y controlase bien. Sabía hablar en público convenciendo, apostando con firmeza en sus creencias y poniendo pasión en aquello que deseaba transmitir.

Pronunció la lección novena, la dedicada al "Elogio de la Matemática", en la Universidad de Florencia, no nos es dado el tono de su voz, que seguramente sería encendido, o así se puede

ACCADEMICHE. 81

DELL' ARCHITETTURA MILITARE.

LEZIONE UNDECIMA

Giudicano alcuni, che quell'antico valore delle cui maraviglie, ſon piene l' iſtorie, nel Mondo odierno ſia diminuito, o per così dire, quaſi eſtinto : o ciò naſca dall' effeminatezza del ſecolo, o dalla mutazione delle macchine da guerreggiare, penſano, che la fortezza noſtra, in comparazione di quella degli antichi, ſia come di fanciulli, ri-

Figura 9. Fragmento inicial de la lección undécima

ENCOMIO DEL SECOL D' ORO.

LEZIONE DUODECIMA.

SE la lode, e gli applauſi degnamente ſi convengono alla virtù, non è dubbio alcuno Amici, che al vizio con ogni ragione i biaſimi, e le maledicenze ſi converranno. Pare, che non poſſano nominarſi ſenza i meritati encomi, la Giuſtizia, e la Temperanza, la Manſuetudine, e la Liberalità, la Prudenza, la Tolleranza, e l' altre virtù, alle quali per debito ſi convengono le benedizioni della fama, e le corone della gloria. Rallegratevi però fortunati compagni; quel ſecol d' oro, di cui celebriamo le lodi, e rinnoviamo l' uſanza, in queſto rozzo, ma delizioſo apparato, non può biaſi-

Figura 10. Fragmento inicial de la lección duodécima

imaginar. La palabra escrita que ha quedado de los hechos representa una demostraciones elocuente de su pasión por la matemática, el punto de vista que adopta es el galileano y defiende firmemente y con rotundidad que la naturaleza está escrita en caracteres matemáticos. En su concepción, la Matemática por su propia naturaleza excluye todas las contradicciones y es una materia más elevada que el propio hombre, la Matemática significa casi la perfección.

4. Conclusiones

En mi opinión, un aspecto innovador de estas conferencias reside en la presentación de temas para la formación de opinión y el debate público. En ese sentido, muy posiblemente se trata de una forma interactiva de discurso, en la que los asistentes se convierten en interlocutores del conferenciante y en las que se crea opinión. No se trata pues de mera comunicación científica, en

62 LEZIONI

IN LODE
DELLE MATTEMATICHE

LEZIONE NONA.

IO non credo, che le discipline Mattematiche avessero giammai minor bisogno di lode, che in questo giorno, e in questo luogo, alla presenza di voi virtuosissimi Uditori. Imperocchè sono a mio giudizio totalmente superflue le lodi, e inopportuni gli encomj della Mattematica, in questo felicissimo Stato, dove la Nobiltà la professa, e i Principi la proteggono. Mal consiglio sarebbe per certo, legger la Geometria dove ella avesse bisogno di lodatore. So, che sono già persuasi gli animi de' Signori Fio-

Figura 11. Fragmento inicial de la última lección, fervoroso encomio de la matemática galileana

la que un experto relata de manera más o menos simplificada o asequible algo que el auditorio de manera poco crítica escucha en silencio, sino más de un trabajo colectivo, en el que pueden surgir ideas nuevas e innovadoras.

Referencias

[1] BOYER, Carl Benjamin. *Historia de la Matemática*, pp. 241, 146, 485, Alianza Editorial, Madrid, 2010.

[2] HERRERA, Rosa María. *El sólido hiperbólico agudo*, Revista Pensamiento Matemático, Grupo de Innovación Educativa "Pensamiento Matemático", Universidad Politécnica de Madrid, España, Nº 2, abril 2012.

[3] HERRERA, Rosa María. *Historia del pensamiento barométrico*, Revista Pensamiento Matemático, Grupo de Innovación Educativa "Pensamiento Matemático", Universidad Politécnica de Madrid, España, Nº 2, abril 2012.

[4] MIDDLETON, Knowles W.E. *The Story of the Barometer*, Johns Hopkins, University Press, Baltimore, 1953.

[5] TORRICELLI, Evangelista. *"Lezione quinta. Della leggerezza"* en *Opere scelte di Evangelista Torricelli*, pp. 583–584, "Lezione seconda. Della percossa" pp. 557–559 edición de Lanfranco Belloni, UTET, Turín, 1975.

[6] TORRICELLI, Evangelista. *Lezione Academiche*, Nella Stamp. Di S.A.R. Per Jacopo Guiduzi e Santi Franchi, Florencia, 1715.

[7] TORRICELLI, Evangelista. *"Lezione seconda. Della forza de la Percossa"*, *"Lezione terza. Della forza de la Percossa"*, *"Lezione seconda. Della forza de la Percossa"*. *Lezione Academiche*, pp. 3–12.

[8] TORRICELLI, Evangelista. *"Lezione sesta. Della leggerezza"*, *Lezione Academiche*, pp. 37–44

Sobre la autora:
Nombre: Rosa María Herrera
Correo electrónico: herrera.rm@gmail.com
Institución: APYCE.

Cuentos Matemáticos

De clavos y otros seres

About nails and other beings

José Miguel Bel Martínez

Revista de Investigación

Volumen III, Número 1, pp. 135–148, ISSN 2174-0410

Recepción: 4 Feb'13; Aceptación: 20 Mar'13

1 de abril de 2013

Resumen

A través de este relato el lector se pone en contacto con el mundo de la Topografía y más concretamente con La Red Española de Nivelación de Alta Precisión (REDNAP). Se trata de un cuento fantástico en el que autor, lector y elementos topográficos dialogan.

Palabras Clave: Topografía, Clavos de Nivelación , Redes geodésicas.

Abstract

The reader contacts with topics related to Topography as the REDNAP through this tale. It is a fantastic story in which the author, the reader and topographic elements converse.

Keywords: Topography, Levelling Nails, Geodetic Networks.

A Pedro. Te recordamos con cariño
Tus clavos

La Red Española de Nivelación de Alta Precisión (REDNAP) nació en 1870, al tiempo que el Instituto Geográfico y Estadístico. Empezó por llevar a través de los accidentados caminos de la época, la altitud del nivel medio del mar en Alicante al Observatorio Astronómico del Retiro, en Madrid, para completar la coordenada que les faltaba a la longitud y latitud que allí habían obtenido los Astrónomos y Cosmógrafos, a lo largo de años de observaciones a estrellas y planetas.

A partir de aquí, los hombres del recién creado Cuerpo Nacional de Topógrafos -nuestros venerables antepasados- se encargaron de, con miras y niveles, llevar las altitudes de precisión a través de Líneas formadas por clavos de distintas categorías, y que confluían a su vez en otras Líneas que, entrelazadas en puntos fundamentales llamados Nodos, llegaron hasta el último rincón de nuestro país, para ser el sustento de la Geodesia y la Cartografía y que sirvieron a su vez para construir canales, carreteras, ferrocarriles, ciudades ... En definitiva, hacer llegar el Progreso a todos los rincones del país.

Pero ¡ay!, ese mismo progreso al que colaboraba tan activamente la Red, era ingrato y se convirtió en su mayor enemigo. Las mismas vías de comunicación que nacieron gracias a ella,

se encargaban de destruirla. Las carreteras se hacían más anchas. Se reformaban, crecían ... y también arrasaban sin piedad esos abnegados clavos que silenciosamente desde sus márgenes, les habían dado el ser. Mas por fortuna el hombre, que seguía precisando de altitudes, reponía y nivelaba tantas veces como eran destruidos los nuevos clavos de nivelación. Y así ha sido hasta nuestros días, con épocas en las que el genocidio de clavos se agudizaba, como el Plan REDIA, y más recientemente el de la construcción desaforada de autovías y rotondas.

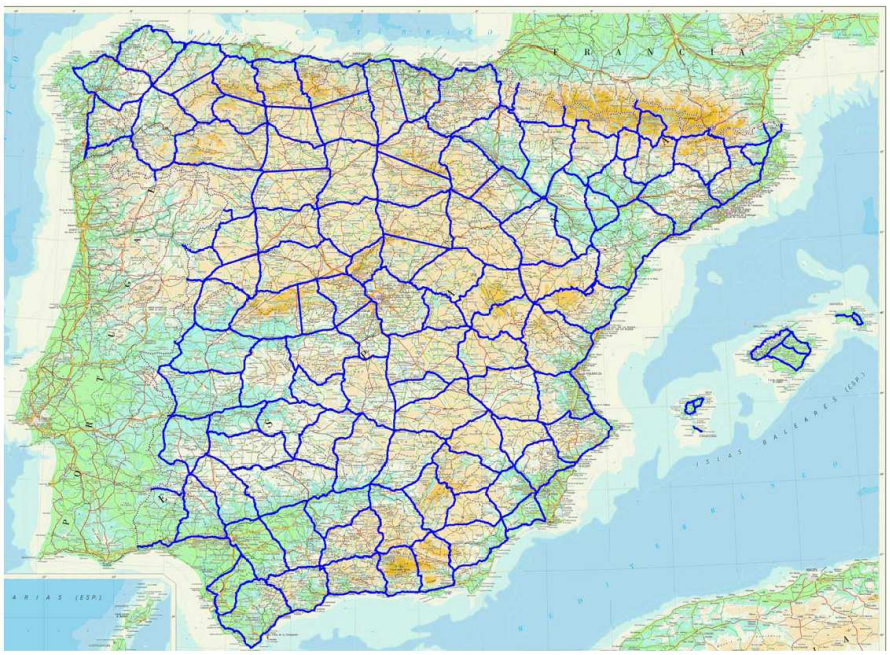


Figura 1. Detalle de REDNAP[1].

Y por fin hoy, en el año del Señor de 2008, después de 10 años de intenso trabajo de muchos cientos de topógrafos, conductores, portamiras y peones del Instituto Geográfico Nacional y de empresas privadas, se da por finalizada definitivamente la señalización y nivelación de la Red Nacional de Alta Precisión. Una obra titánica que aproximadamente comprende 18.200 kilómetros, con 250 Líneas compuestas por 150 Nodos, 4000 clavos principales numerados y 17.500 señales secundarias, en su mayor parte nuevos, aunque se han conservado aquellos valiosos supervivientes de épocas pasadas. Normalmente, cada cinco señales secundarias se intercala un grupo de dos clavos principales, más grandes y numerados. Estas señales distan más o menos un kilómetro entre una y otra y ...

–¡¡UN MOMENTO!! Pero, ¿tú de qué vas tío? ¿Qué me estás contando?

–Pero ... no entiendo. ¿Quién anda ahí? ¡Qué susto me has dado!

–Soy el Lector. Y vigilo la idoneidad de lo que se publica aquí.

–¡Ah!, pues encantado ¿eh? Yo soy el Autor, y lo que pretendo es que tú, Lector ...

–No, si no hace falta que me lo digas. Ya te veo venir. Tú lo que intentas es aburrirnos metiéndonos un ladrillo histórico - técnico - estadístico y abrumarnos con cifras y datos que no hacen al caso. Porque por si no te has enterado, y es obvio que no, en el encabezamiento, "esto", nos lo presentas como RELATO o "cuento". Así que uno espera algo literario y ameno, ¿entiendes? Para colocar tu rollo hay otras secciones más apropiadas en esta misma revista o en otras parecidas. Yo, el Lector, lo que esperaba con tu historia era sólo pasar un rato entreteni ...

[1] Imagen cortesía del Instituto Geográfico Nacional (IGN). http://www.ign.es

–¡¡BASTA!! ¡Ahora escúchame tú! Aún estoy en las primeras líneas y ya estás protestando. ¿Pero tú quién te crees que eres por muy Lector que seas para venirme con esas premuras y exigencias, y encima tratar de imponer al Autor la forma de escribir su relato?

–Bueno hombre, no te lo tomes así. Yo sólo pretendía hacerte ver, que tu escrito lleva toda la pinta de ser un auténtico "latazo". Pero vale, tienes razón. Reconozco que me he precipitado, así que disculpa y continúa con tu narración, o lo que sea aquello en lo que acabe parando esto.

–Disculpado quedas. Realmente ya había terminado el preámbulo que tanto te ha molestado. No vayas a creerte, a mí tampoco me gusta soltar éste ladrillo histórico - técnico - estadístico como dices, pero es que sin él, quizá no comprendas la parte humana, y al igual que se precisa de un pinchazo anestesiante antes de un empaste, o los fórceps antes de un parto complicado, creo que hacía falta éste preámbulo tedioso para llegar a conocer mi parto, que en éste caso es un relato. Ahora, si me das una oportunidad y tienes la paciencia de seguir unas líneas más, te prometo que no te arrepentirás y que te maravillará la apasionante y emotiva historia que viene a continuación, que si bien no tiene visos de ser verídica, tampoco nadie puede asegurar que no lo sea.

Nuestra historia empieza un día cualquiera de fínales de junio de 2008. El campo toledano luce un florido verdor más propio de tierras más norteñas, debido a que la primavera ha sido extraordinariamente lluviosa. Hace una hora que ha amanecido y el suelo aún está húmedo. Sólo el canto de los pájaros rompe el silencio, y únicamente una intersección de carreteras y las grandes torres de alta tensión de la Cumbre Alta, la sierra que cobija en su falda al pueblo de Sevilleja de la Jara, situado unos diez kilómetros al norte de la intersección, delatan la mano del hombre.

Un diminuto punto blanco en la lejanía acompañado del leve rumor de la rodadura de los neumáticos y el motor, se va convirtiendo poco a poco en un Nissan Terrano blanco que se aproxima por la N-502, la carretera más ancha de las dos. Viene rápido y sobre su techo gira sin cesar una luz anaranjada. Lleva una matrícula con unas siglas muy poco corrientes. MF: Ministerio de Fomento. Disminuye la marcha, y aunque tiene la preferencia de paso y no debería hacerlo, parece que va a detenerse en la intersección. Y efectivamente termina haciéndolo. El conductor, que permanece dentro, conecta el "warning" al tiempo que se abre la puerta derecha y del coche se apea un hombre de mediana edad. Lleva dos folios, un cuaderno, un mapa y una cámara de fotos.

Tras ponerse las pequeñas gafas para ver de cerca propias de su edad, se dirige a la margen izquierda de la carretera y busca fuera de ella algo que parece no encontrar. Finalmente, tras consultar uno de los folios parece, tras escarbar con el pié entre el musgo y la hierba, hallar lo que buscaba. Está en el suelo, se agacha y lo mira con detenimiento, después lo pisa repetidas veces y torciendo el gesto se levanta. Cambia el folio por el otro y avanza con decisión hacia una alcantarilla de hormigón que hay en la margen opuesta de la carretera. Observa con atención algo en ella y después llama al conductor que, saliendo del coche y sin siquiera preguntar, saca de la parte trasera un jalón rojo y blanco que coloca en el punto de la alcantarilla que tanto había interesado al otro hombre. Este le hace una fotografía, y después de anotar algo en su cuaderno comentan algo en el mismo momento en el que pasa un camión. Por último los dos hombres vuelven a subir al coche y abandonan con presteza el lugar, volviendo sus pasos por la N-502.

–Eran los Jefes, ¿no? ¡Qué extraño!: ésta línea está señalizada y nivelada hace pocos años. ¿Qué querrán?, es raro que se fueran tan pronto. ¿Has oído tú algo? Entre que estoy lejos y el ruido del dichoso camión no he podido escuchar nada. ¡Manda huevos! Pasan diez al día como mucho, los Jefes vienen una vez cada muchos años, y precisamente en el momento en que dicen algo importante, tiene que pasar uno. ¡Hay que j . . . . . !

–Yo sí he oído: lo he oído todo claramente. El Topógrafo ha dicho, ha escrito, que soy, que soy . . .–la voz se ha tornado temblorosa por la emoción.

–¿Que eres qué? ¡Dilo de una vez, demonios, que me estás poniendo nervioso!

–Que soy ... ¡Dios Santo, es que no me lo puedo creer! ... Soy ... ¡¡UN NODO!!

–¿Te has vuelto loco? ¿Tú un Nodo?

–Sí, le he oído perfectamente decirlo, y se lo he visto escribir en el cuaderno: El 000-192. ¡Santo Cielo! ¡Había soñado con esto tantas veces! En el fondo tenía la corazonada de que un día sucedería algo así.

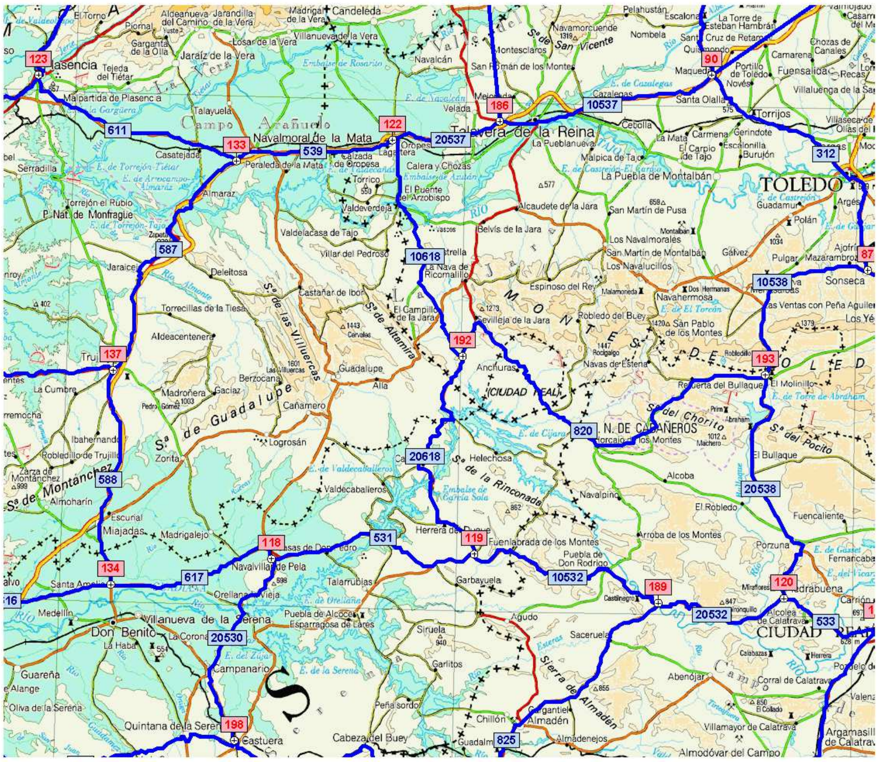


Figura 2. Detalle de REDNAP con Nodo 192 en el centro[2].

–¡Que locura! Sin duda alguien ha debido tirar por la ventanilla un "canuto" encendido en tu alcantarilla y te ha trastornado. ¡Nosotros Nodos!

–Nosotros no: Yo, y sólo yo soy el Nodo. Y no sé porqué te extraña tanto, la verdad. Hace ya más de un año que por las Líneas venía circulando la noticia de que se iban a hacer líneas nuevas, y si hay líneas nuevas, tendrá que haber Nodos nuevos, ¿no? Si además tenemos en cuenta que nuestro grupo está exactamente en la intersección de la carretera CM-4162 con la N-502 que lleva a Horcajo de los Montes y Molinillo, pensándolo bien, no es tan extraño que uno de esos Nodos, esté en nuestro grupo.

Mascullando para sí, la voz se hace casi inaudible, y se torna calculadora haciendo cábalas que sólo él parece comprender.

–A ver, pensemos. Lo más lógico sería que la Línea nueva parta de mí y llegue hasta la Línea 538, en Molinillo. Más de 110 kilómetros, que sumados a los 125 de la nuestra harán un total así por encima de 300 clavos, y en medio de esos 300 clavos, un único Nodo. ¡YO! –termina por decir triunfalmente la voz.

–Tu imaginación se ha desbocado y creo que te estás precipitando, pero aún en el caso de que

[2] Imagen cortesía del Instituto Geográfico Nacional (IGN). http://www.ign.es

todas esas elucubraciones fueran ciertas, cosa que dudo, qué más da ser Nodo o señal principal. No vas a cambiar ni de aspecto ni de numeración.

–¿Que no da dices? ¡Pues claro que da! Ser Nodo es la más alta distinción que puede alcanzar una señal principal. Para mí será un orgullo poder figurar en la base de datos junto a otros Nodos tan ilustres como los de Salamanca, Santiago de Compostela, Sevilla, Córdoba, Cuenca, Ciudad Rodrigo, Mérida, Zafra y tantos otros –afirma con engolada solemnidad la voz.

–Tú lo has dicho. Todas son grandes ciudades y muchos de esos Nodos están incrustados desde hace muchos años en Monumentos y Catedrales conocidos en el mundo entero, algunos de ellos Patrimonios de la Humanidad. ¿Cuál serías tú, cretino?: "Nodo alcantarilla oeste del cruce de la N-502, dirección Sevilleja y Horcajo, con la carretera local CM-4162,". ¡Oh, cuanto Honor! ¡Je!, ni siquiera estamos en ningún pueblo por mísero que sea del que pudieras usar el nombre.

–Pues mira por donde mi nombré será, mejor dicho ya lo es, porque como te dije le he visto escribirlo, Nodo 000-192, conocido también cómo CM-4162, y a mucha honra. Y por cierto, que me parece que en tus palabras se nota un ligero tufillo a envidia, ¿No te parece, "compañero"?

–Pues ya que lo dices, puede que sí. Si este cruce va a ser un Nodo como afirmas, ¿por qué no soy yo? Hay muchas razones para que así sea.

–¿Ah sí? ¿Y cuáles son, si puede saberse?

–Para empezar, soy de los poquísimos supervivientes de la Línea antigua, y por lo tanto soy mucho más experto y veterano que tú. Además estoy diez metros más próximo a la CM-4162, de donde según tú partirá la Línea nueva. A lo mejor ha impresionado al Topógrafo el brillo de tu cabeza de chorlito, más que mi experiencia, buen hacer y estabilidad.

–¿Estabilidad tú? ¡Ja, Ja! Mira, no me hagas hablar, que no quiero herir los sentimientos de nadie, y menos los de un compañero de grupo. Aunque visto lo visto, eso de compañero … Anda calla, que mejor será que dejemos estar las cosas como están.

–¡Ah, no! Dejemos aquí y ahora las cosas claras. ¿Herir, dices? ¿Se puede saber de qué forma podrías hacerlo tú, un advenedizo de alcantarilla que lleva aquí cuatro días como quien dice? Para que te enteres, yo he visto entre otros hechos históricos, pasar a las tropas del mismísimo General Franco camino del Alcázar de Toledo. Llevo más de setenta años en el lugar más estable en el que puede estar un clavo. Lo dice mi reseña: Clavo de "dural" incrustado en afloramiento de roca nativa a 7,58 metros de la carretera. Roca nativa, ¿entiendes lo que significa eso? Roca firme que se formó hace millones de años, y que nace de las mismas entrañas de la Tierra. He visto ya demasiadas reformas de la carretera, y desparecer en un santiamén sucias alcantarillas con clavos mejores que tú. Estoy seguro de que si ese Topógrafo tiene dos dedos de frente, cambiará de opinión cuando esta noche en el hotel lea completas las reseñas de los dos.

–Vale, está bien: tú lo has querido. Sabe Dios que no quería hacerlo, pero ya que vienes con esas, no me dejas otra alternativa que ponerte un espejo delante de los ojos para que al fin te enteres de algo que hace años yo, toda la Línea, y … ¡qué demonios, seguramente tú mismo también sabes, aunque tu estúpido orgullo no te lo haya dejado ver! El Topógrafo no te ha elegido a ti porque no eres de fiar, y ¿sabes por qué?: ¡TE MUEVES! ¿Lo oyes bien? Te balanceas como una mecedora. ¡Ea!, ya era hora de que alguien te lo dijera. ¿Roca nativa, dices? ¡Ja! Puede que así lo pareciera cuando alguien te puso hace tantos años, pero la lluvia, el viento, y sobre todo el tiempo se han encargado de desnudar tu "roca nativa" como a una vulgar "stripper" y descubrir a todos dónde estás incrustado realmente.

–¿Ah si? ¿Y dónde lo estoy entonces, botarate?

–Estás incrustado en una piedra. ¡Una piedra suelta!, ¿lo oyes? Y tu base descarnada se ha ido quedando cada vez más y más visible. Sólo basta con pisarte un poco para hacer que te bambolees como un flan. ¡Un Nodo que se mueve! ¡Cuánto Honor! –dijo remedando el tono

burlón empleado antes por la otra voz.

Sólo el silencio, roto por el cri - cri que emite un grillo despistado cantando a deshora y un leve sollozo contenido, responde. Un silencio que se hace interminable y que rompe finalmente la voz del nuevo Nodo aunque, eso sí, ahora mucho más apaciguada y conciliadora.

–Escucha ... yo no quería ... Me he dejado llevar por la ira. Lo siento, hombre, no me hagas caso. Cuando pierdo la cabeza, no digo más que tonterías.

Los sollozos se hacen ahora claramente audibles.

–NGC365, ¿me oyes? No te pongas así hombre, que ya te he dicho que no sabía lo que decía. Siempre has sido un buen compañero de grupo, de veras, y no te mereces que te haya hablado de esta manera. Es que tengo un carácter, que cuando me caliento no sé lo que me pasa. Anda tío, perdóname.

–Si no hay nada que perdonar, NGX101 –responde al fin NGC365, hipando y tragándose las lágrimas. No has hecho más que decirme la verdad. Hace tiempo, años ya, que noto cómo una y otra vez todos rechazan estacionar en mí. Siempre la misma historia: unas pataditas, un gesto torcido y luego a estacionar en ti. Sólo algún peón despistado o algún topógrafo chapucero lo han hecho en todo este tiempo. No he querido ver lo que era evidente, ni escuchar lo que era ya un secreto a voces en la Línea. Ya no sirvo para nada.

–Hombre tampoco hay que exagerar. Total sólo te mueves uno o dos milímetros, como mucho. Eso no es nada. Sigues siendo perfectamente útil para la mayor parte de las necesidades de la topografía.

–¡Uno o dos milímetros! Escucha, soy una Señal Principal de REDNAP y ambos sabemos que nuestra tolerancia es de 1,5 mm. $\times\sqrt{k}$ ¿Uno o dos milímetro dices? Eso significa que entre tú y yo, que estamos a diez metros, excedo la tolerancia en unas cien o doscientas veces. Eso podría estar bien para un triste clavo de una obra, pero para mí ... Estoy acabado, y mucho más ahora.

–Te repito que exageras. En realidad, nada ha cambiado. Seguirás siendo mi compañero, igual que siempre, y si quieren altitud precisa, aquí estoy yo para dársela, mientras la salud, los planes de carreteras y sobre todo las rotondas quieran. Algo que por el tráfico de esta carretera, creo que será por mucho tiempo.

–Gracias por querer animarme, pero creo que no te haces una idea exacta de la situación. Quizá podría haber seguido siendo parte de un grupo normal sin que pasara nada como hasta ahora, pero un Nodo no puede tener un compañero como yo, ¿no comprendes? El mismo topógrafo que te ha convertido en Nodo, vendrá otra vez no tardando mucho a ponerte otro compañero, no te quepa duda. La alcantarilla que tienes enfrente lo está pidiendo a gritos y yo amigo mío, seré pasto del martillo, nuestro ancestral verdugo. Me machacarán la cabeza hasta que mi "dural", la más resistente aleación de metales de mi época, sea un amasijo informe y no quede ni rastro de mi numeración. Pero aún con ser malo todo eso, lo peor vendrá después. Arrancarán mi piedra del suelo y la volcarán para que no pueda dar una altitud errónea a nadie, y así perderé todo. Perderé nuestra razón de existir: LA ALTITUD. Y con ella el Alma.

–Bueno, pero aunque sea un poco machacado, seguirás ahí.

–No lo entiendes, o no quieres entenderlo. Un clavo movido un milímetro como hasta ahora, sólo está enfermo, pero un clavo arrancado y volcado, es un clavo sin altitud, y por tanto muerto. Mi página del viejo libro de reseñas de piel de nuestra Línea, será arrancada. Mi nombre será borrado con deshonor para siempre de la Base de Datos, y harán muy bien, ambos lo sabemos. Entre nosotros no hay lugar para los débiles.

–Bueno, pensándolo bien, puede que lleves algo de razón -dice NGX101, quedándose ya sin argumentos de consuelo-, pero aunque pasara todo eso que dices, probablemente no será tan

terrible. Los clavos somos materia inerte. No sufrimos.

–¿Que no sufrimos? ¡Cómo se ve que eres joven y tú no lo viviste! Mira, nuestra antigua Línea era muy tranquila. Pocas poblaciones, poco tráfico y poco trabajo. Después de tantos años juntos nos llevábamos todos muy bien y nuestras bajas eran prácticamente inexistentes. SSK230,0, que estaba en un hito kilométrico que fue embestido por el coche de un niñato al volver borracho a su casa una noche. Una alcantarilla hundida por un tractor, muy lejos de aquí, y poco más en tantos años. Y respecto a las tan temidas obras: ni el más pesimista habría pensado nunca que esta carretera se pudiera modificar algún día.

–¿Cómo fue?

–Un malhadado día aparecieron sombrías por el horizonte unas máquinas enormes y ruidosas, que clavaban sus horribles bocas erizadas de dientes de hierro en las cunetas, arrancando sin piedad todo lo que encontraban; alcantarillas, hitos kilométricos, señales de tráfico, y hasta puentes de piedra que parecían indestructibles sucumbían como si fueran de mantequilla. Con ellos desaparecimos también casi todos nosotros. ¿Y todo para qué? Sólo para ensanchar una carretera que no lo necesitaba. Apenas sí pasaban 30 o 40 coches al día. Pero supongo que a algún malnacido se le ocurrió que había que gastar dinero, y a fe que lo hizo.

Si alguno se salvó por estar alejado de la carretera, ya se encargaron cuadrillas de hombres sin corazón armados con picos y mazos, de acabar con ellos. Alguno creyó que éramos valiosos y trató de arrancarnos, separándonos a martillazos la cabeza del cuerpo. ¡Ignorantes salvajes! Y si por descuido dejaron alguno, aún fue mucho peor para ellos. Unas máquinas grandes como trenes, humeantes y malolientes, se encargaron de enterrarlos vivos bajo una gruesa capa de alquitrán ardiente, negra y siniestra como el mismísimo infierno, que les negaba la luz para siempre y los cubrió eternamente de un sudario pegajoso.

NGX101 continuaba escuchando la revelación de su amigo, sobrecogido y en silencio.

–¿Dices que no sufrimos? Sí, es cierto que somos sólo un trozo de metal, y puede que no sintamos dolor del mismo modo que lo sienten los seres llamados "vivos", pero sí sentimos miedo. Nunca he podido olvidar la cara de terror de mi antiguo compañero, NGC366 en el instante mismo en que los dientes de la excavadora iban a hacer presa en su vieja alcantarilla.

Los seises de su cara, se le abrieron tanto que parecían ceros. Ni tampoco he podido olvidar su triste lamento que, ni el ruido del motor ni el chirrido estridente de las cadenas, pudieron acallar.

–Pero tú te salvaste.

–Estaba lejos de la carretera, y sobre todo escondido entre el musgo de mi roca nati …, bueno, de mi piedra móvil como una mecedora, ¿no?

–Hombre, no seas tan duro conmigo, ya me siento bastante mal para que encima ironices de esa forma y me hagas sentir aún peor.

–Lo siento, no era mi intención. Sólo pretendía poner un poco de humor.

–Está bien. Pero dime: ¿por qué nunca me habías hablado de esto?

–Me juré a mi mismo borrarlo de mi memoria para siempre, pero ahora que está tan próximo mi fin creo que debes saber cómo son en realidad los hombres, aunque supongo que no te servirá de mucho. Tenemos el gran inconveniente de que no podemos huir.

–Claro … incrustados, para bien y para mal. Y cuéntame, ¿quién más sobrevivió?

–Casi nadie. Cerca de aquí, solamente SSK222.2, una Señal Secundaria que está a un kilómetro.

–Nunca he oído hablar de ella. ¿La enterró el asfalto?

–No, que va: en realidad lo suyo no tuvo nada que ver con la Masacre de la obra. Estaba en la esquina de una casa a más de cien metros de la carretera. Era una gran casa solariega de gente adinerada. En los más de sesenta años que duró su felicidad, conoció a los abuelos, después a los hijos, a los nietos y hasta incluso al primer biznieto. Estaba muy bien considerada por todos. Cuando el topógrafo del Instituto Geográfico pidió permiso para poner la señal al dueño, el abuelo, allá por los años treinta, le explicó lo que significaba aquel clavo. Llevarle el nivel del mar a su casa de Toledo, nada menos. Él, que se consideraba un marino frustrado a pesar de que nunca había visto el mar, o quizá por eso, no sólo accedió de buen grado, sino que además se ilusionó sobremanera y siempre se sintió orgulloso de conocer con exactitud milimétrica a qué altitud sobre el nivel del mar en Alicante dormía. Algo de lo que se jactaba con sus amigos y los demás socios del Casino.

–¿No me digas? ¿Tenía la cama junto a la señal? –preguntó sorprendido NGX101.

–No, no llegó a tanto, pero mandó medir a los dos trabajadores más despabilados que tenía –los únicos que sabían leer una cinta métrica–la distancia por la fachada hasta donde consideró que estaban las patas de su cama, para después él mismo, medir con sumo cuidado el desnivel desde el suelo hasta la cara superior del colchón. Además, cuando de Pascuas a Ramos iba algún Topógrafo a estacionar en el clavo –algo que no le gustaba nada–, pretendía protegerlo con un grueso felpudo, algo que lógicamente, el topógrafo rechazaba. Entonces accedía de mala gana, pero le obligaba a poner la mira con una suavidad exquisita, no fuera a ser que le rayara la cabeza con esas miras tan duras y pesadas. La devoción por "su" SSK222.2 fue tal, que hasta colgó una copia de la reseña enmarcada, en una pared preeminente del salón.

–Pues francamente, aunque sea un halago para nuestro ego el que alguien considere tan importante la altitud que proporcionamos, lo cierto es que encuentro algo extravagante y hasta ridícula la afición de ese hombre por un clavo de nivelación, y más aún por una simple señal secundaria. Si al menos, hubiera sido uno de nosotros. Pocas preocupaciones debía tener el hombre.

–Puede ser, pero de cualquier forma así fue. Además, trató de inculcar a su hijo la devoción por el clavo, y aunque no lo consiguió en la misma medida ni mucho menos, éste también respetó a SSK222.2. Ella, como es lógico, se sentía muy dichosa. Tan considerada por todos, vio además crecer y jugar a muchos niños de varias generaciones a su alrededor, algo que le encantaba. Incluso hubo un tiempo en que les dio por jugar directamente con ella. El juego consistía en tirarle desde lejos chapas de coca-cola, y ganaba el que conseguía dejarla más cerca. Una especie de petanca de críos.

–Bueno y entonces, ¿qué pudo pasar para que todo acabara tan mal?

–El nieto. Era un crápula y se aficionó a todos los vicios, especialmente al del juego. Era hombre débil y de poca voluntad así que en poco tiempo dilapidó la fortuna que sus antepasados habían amasado durante muchas generaciones. Finalmente, una noche, perdió la finca en el Casino.

–¿La que llaman el Dos de Espadas?

–En efecto. Te contaré la historia completa. Al mozo se le calentó la boca apostando, como siempre, de tal forma que perdió hasta el último céntimo, también como siempre. El contrincante, se ofreció a prestarle cuarenta mil duros a cambio de un pagaré, y él aceptó. Jugaban a la carta más alta y en una de las manos, el otro sacó un dos de espadas. Sólo podría ganar si el nieto sacaba el dos de bastos. Era muy difícil: una carta entre treinta y nueve. Le dijo que ya de perdidos al río: que a pesar de lo mal que lo tenía le apostaba los cien mil duros que le había ganado esa noche, más el pagaré de los cuarenta mil, contra la finca, que por aquel entonces se llamaba La Calderona. El nieto en principio se acojonó y rehusó. Pero el otro, que tenía muchas tablas, pronunció la frase mágica:

¿Ni teniendo treinta y ocho probabilidades contra una tienes huevos de ir? Creía que estaba jugando

con un hombre –le dijo delante de todos los socios.

Eso le picó en su amor propio, se envalentonó y aceptó el envite. Sudoroso y pálido, levanto la carta que le dieron, entre la expectación de todos los principales del pueblo.

–¿Y me vas a decir que era el . . . ?

–Dos de bastos, exactamente. Se dijo después que el ganador era un fullero compinchado con el que dio las cartas, y que ya se había hecho con alguna otra propiedad por el mismo procedimiento en otros Casinos. Pero nadie pudo probar nada, así que el nieto se quedó con una mano delante y otra atrás, y encima debiendo dinero. Un dinero que no tenía y que no era capaz de conseguir. El tío era un señorito que no había dado un palo al agua en su vida.

–Y ¿qué pasó después?

–No tuvo valor para confesar a la familia lo que había hecho y al llegar a la casa, se bebió una botella de coñac, escribió la consabida carta exculpatoria de su muerte al juez, y después se colgó del gancho de la lámpara, de tal forma que los pies le quedaron justamente rozando la cara superior del colchón. Cuando el abuelo, que ya era muy viejo y estaba medio loco en una residencia conoció ese detalle, en su mente enferma se le despertó la antigua obsesión por el clavo y la altitud y eufórico, pretendió emocionado que en su tumba se pusiera el siguiente epitafio: *"Murió ahorcado a 647,245 metros sobre el nivel medio del mar en Alicante"*.

–¡Qué horror!

–Por fortuna su hijo, es decir el padre del ludópata, no hizo semejante barbaridad aunque por no desilusionarle, le hizo creer que se haría su voluntad. Después el nuevo dueño perdió el interés por el caserón. Su familia se negó a vivir en una casa en la que había ocurrido semejante desgracia. En el pueblo la llamaron la Casa del Ahorcado. Se decía que por las noches se aparecía el fantasma del ludópata barajando unos naipes enormes y apostando su alma a todo el que estaba en la casa, así que nadie la quiso ni regalada. El dueño acabó por derribarla unos pocos años antes de la Masacre. No dejó nada en pie y por no quedar, no quedó ni el nombre. El pueblo poco a poco, borró el nombre de "la Calderona", y rebautizó definitivamente la finca con el de "el Dos de Espadas". Se retiraron los escombros de la casa y se sembró de cereal toda la finca, inclusive hasta el lugar que ocupaba aquella.

–Entonces ella, SSK222.2, desaparecería junto con la casa, ¿no?

–Más hubiera valido que hubiese sido así, pero el trozo de solera de cemento en el que estaba quedó intacto. Así que para su desgracia allí sigue, en el único medio metro cuadrado que quedó de "la Calderona".

–Pero no entiendo. ¿Cómo es que nunca se ha comunicado con nadie en todos estos años?

–Antes de que llegarais vosotros lo hizo, pero sólo conmigo. Por un tiempo, mantuvimos largas conversaciones por las noches. Pero un buen día dejó de comunicarse. Tan acostumbrada como estaba al contacto humano, no pudo soportar la soledad y el aislamiento, amén del complejo de culpabilidad, que adquirió al creer que el suicidio del ludópata, al que quería mucho ya que le había conocido desde que nació, tenía que ver con la altitud que ella había llevado hasta la cama que el Destino quiso que fuese su cadalso. El trigo y la maleza crecieron ocultándola a todos. Además, al no quedar ninguna referencia, nadie la pudo encontrar para estacionar en ella, algo que seguramente le hubiera reconfortado. Así que debió enloquecer y finalmente calló para siempre. Muchos la buscaron con ahínco. Ten en cuenta que en los años que transcurrieron entre la Masacre y vuestra llegada, los poquísimos supervivientes que quedamos éramos muy buscados. No es porque yo lo diga pero fui en esa época la estrella de la línea. Entonces, aún estaba en roca nativa y era una garantía para todos. Un día hubo tres topógrafos haciendo cola para estacionar en mí . . . –por unos instantes, NGC365 después de un hondo suspiro, queda en silencio añorando aquellos tiempos felices.

–Bueno eso está muy bien pero sigue hombre, no me dejes así.

–Años después, cuando se reconstruyó la Línea, el topógrafo que la proyectó y te puso a ti y al resto de los nuevos, la estuvo buscando con mucho interés bastante tiempo. De hecho, debió pasar a pocos centímetros de ella pero … no la vio, y en su reseña puso una cruz y la fatídica palabra que tanto tememos: "Desaparecida".

–Pero si no ha dado señales de vida en tanto tiempo, puede que realmente haya desaparecido.

–No: estoy seguro de que vive. No habla, pero alguna noche la he oído sollozar casi imperceptiblemente, y cuando lo hace, me rompe el corazón … Y ahora, perdona, pero no deseo seguir hablando de esto.

–Te comprendo, además, creo que por hoy ya basta. Ha sido un día de muchas emociones. Hasta mañana.

–Sí, mañana … –se despide NGC365 con un hilo de voz.

El manto de la noche se extiende por el campo y la Línea queda en silencio. Todos permanecen en reposo y a su manera, descansan.

Figura 3. Los "protagonistas": el clavo viejo, el nodo, el nuevo y la "chica" (señal secundaria).

El sol sale como siempre y los clavos se preparan a pasar un día más. Pero hay un gran silencio, porque hoy no es un día cualquiera. Toda la Línea, en realidad todas las Líneas, incluso las de Francia y Portugal, unidas por nodos fronterizos a las nuestras, a pesar de hablar diferentes lenguas, saben ya que va a pasar algo trascendental. Un nuevo Nodo será coronado, y un viejo clavo, uno de los más antiguos y respetados de la Red, va a desaparecer después de ser machacado por el martillo. Desde la Gran Masacre no se había visto nada parecido. Por eso, el silencio es absoluto. Los pájaros parecen haber enmudecido, y hasta el grillo despistado parece que también intuye algo y permanece callado en su grillera.

–Ya vienen. No han esperado mucho –rompe el silencio NGC365.

–Yo no oigo nada, pero aunque se acerque alguien, puede ser cualquier otro. Esta es la hora a la que pasa el lechero, y seguramente será él.

–No, son ellos, lo sé: son muy diligentes. Tienen un trabajo que hacer y lo van a hacer deprisa. No han tardado ni veinticuatro horas en regresar.

Al cabo de dos minutos, el Terrano blanco se orilla en el arcén deteniéndose cerca de la alcantarilla que hay enfrente de NGX101. Pedro, el Conductor y Joaquín, el Topógrafo, bajan del coche cada uno por su lado y sin hablar. Los dos saben exactamente qué es lo que tienen que hacer. Joaquín, escribe notas en el cuaderno y además dibuja un croquis de situación del lugar. Pedro abre el portón trasero y de una caja de cartón, extrae un clavo principal reluciente que deja caer sobre de la alcantarilla con un sonido metálico.

–¿Dónde estoy? –balbucea el nuevo clavo, aún algo aturdido por el golpe.

–En un cruce de carreteras. Ya tendrás tiempo para saber dónde. Soy NGX101, el nuevo Nodo, y parece que tú vas a ser mi compañero.

–Encantado. No es mal destino para un novato como yo. Entonces, si por casualidad te pasara algo yo pasaría a ser el Nodo, ¿no?

–Caray con los nuevos. Venís pisando fuerte ¿eh?

–Hombre no me juzgues mal, que sólo era un suponer: aún pareces joven y no te deseo ningún mal. Oye, ¿cómo es que no tienes un compañero?

–Lo tengo. Está a tu espalda, a unos 7,50 metros. En roca nativa. Se llama NGC365, lleva aquí más de setenta años y es el mejor compañero que se puede tener.

–¡Ah, encantado también!, pero entonces, no entiendo. Por tu edad, debes ser toda una institución y además tienes pinta de estar sano. Te conservas muy bien para tus años.

–Estoy en una piedra suelta y me muevo –dice con voz temblorosa NGC365–. Vas a ocupar mi lugar y yo voy a "desaparecer" dentro de unos minutos.

–¡No está en una piedra, j … …! ¡Está en roca nativa!, ¡lo dice la reseña antigua, y eso es lo que cuenta! –afirma tajantemente NGX101, con la voz transida de rabia y emoción.

–Oíd chicos, yo no quiero ser motivo de disgustos y siento de veras esta situación. –dice el nuevo, compungido.

–No tienes culpa de nada. Es que me altero con facilidad. Ya tendrás mucho tiempo para comprobarlo –replica NGX101 ya más calmado–. Por cierto, que pareces algo más pequeño que nosotros. ¿Cómo te llamas?

–Es que lo soy. Han decidido disminuir nuestro tamaño por reducción de costes. Cosas del "marketing". Me llamo NGAB.

–NGAB, qué.

–NGAB a secas.

–¿Y los otros compañeros que van en la caja?

–Igual; todos somos NGAB. Este año se acabaron las letras del abecedario, y desde entonces ya no hay números porque no cabían tantos caracteres en una cabeza más pequeña. Pero bueno, ¿que pasa? ¿Es tan importante tener número?

–¿Para un clavo principal? ¡Por supuesto! Imprescindible. Es lo que hace que seamos únicos e irrepetibles. ¿Cómo hacen entonces para distinguiros?

–Por el punto kilométrico, o por el paraje, ¡Yo que sé!, ¡qué más da!

–¡Qué juventud! Y ¿tú pretendías ser Nodo? Si casi eres una señal secundaria.

–Y qué. Las Señales secundarias ahora también son Nodos en las nuevas Líneas. Da lo mismo.

–¡¡Nooo!! ¡¡No puede ser!! ¿Oyes eso, NGC365? Esto lo cambia todo. Aún no soy oficialmente Nodo, y ya he perdido la ilusión por serlo. ¡Señales Secundarias que son Nodos! ¿Dónde iremos a parar, Dios mío?, además …

–Además qué –tercia un muy triste NGC365.

–Que ojalá todo hubiera seguido siendo igual. He sido un necio arrogante con toda esta historia del Nodo. Por su culpa voy a perderte a cambio de un niñato atolondrado y estúpido que ni siquiera tiene nombre.

–Hombre, tampoco hay que faltar, digo yo, que no tengo culpa en todo este embrollo –se defiende tímidamente NGAB.

NGX101 parece ignorarle y continúa a lo suyo.

–Viejo amigo, daría lo que fuera, mi nombramiento de nodo, y todo lo que tengo … ¿Me creerías si te digo que daría hasta … hasta mi existencia porque siguieras viviendo? Tú te lo mereces mucho más que yo.

–¡Basta! Te creo, pero calla, o me vas a hacer todavía más duro este trance. –dice emocionado NGC365.

El fuerte ruido del percutor y el motor de gasolina del martillo haciendo el taladro en la alcantarilla, acaba con la conversación. Después de incrustar y coger con cemento a NGAB en su alojamiento de la alcantarilla, viene la foto de rigor del recién nacido clavo principal sin nombre. Pedro va a la trasera del Nissan, y se da la vuelta empuñando un mazo. Se dirige resuelto a NGC365, y le mira a él y a su piedra, seguramente sopesando cómo va a hacer su trabajo, mientras enciende un "Fortuna" del que aspira con delectación un par de caladas.

Después de unos instantes, levanta con resolución la mano blandiendo el mazo por encima de su cabeza.

–Tengo miedo, mucho miedo … Ahora amigos, no me miréis u os pesará toda vuestra vida. ¡Adiós! –se despide para siempre NGC365.

–¡¡Espera un momento!! –la voz de Joaquín desvía "in extremis" el mazo, que ya impulsado, acaba golpeando el suelo, que retumba haciendo estremecer a los tres clavos.

–¿Qué pasa?

–Es que estaba pensando … que esa piedra es bonita, ¿no?

–Hombre, es una piedra. Yo la veo igual que todas.

–Pues es bonita, te lo digo yo. ¿Sabes cuánto te cobran en un vivero por una buena piedra para decorar el jardín? Un pastón. Anda, ayúdame a ver.

Joaquín observa la piedra, y ayudado por Pedro la mueve hasta que consigue sacarla del suelo, algo que hace sentir un escalofrío a los tres clavos, especialmente a NGC365, que siente como tras setenta años pierde definitivamente la Altitud.

–Tiene un buen tamaño, y limpiándola sin quitarle el musgo, yo creo que quedará preciosa semienterrada en el césped de la piscina del chalé. Además tiene un clavo, un clavo muy antiguo y en muy buen estado. Lo puliré y quedará reluciente: Le voy a dar una sorpresa a Nieves: le va a encantar. Menos mal que me he dado cuenta a tiempo. Venga, vamos a echarla al coche. Con cuidado ¿eh?

Los dos hombres van transportando con dificultad la piedra hasta el maletero del Nissan,

–¿Sabes lo que se me está ocurriendo también? ¡Qué idea!

–No sé, cualquier cosa. Estás como una cabra.

–A un kilómetro de casa hay un clavo de nivelación en la Estación, y ahora que tengo un

nivel y unas miras, le vamos a dar altitud buena a éste. Voy a hacer un ramal de ida y vuelta hasta éste clavo. ¿Qué te parece? La superficie del agua de mi piscina referida al nivel del Mar en Alicante con precisión milimétrica. La única en el mundo, seguro.

–¡Vaya gilipollez! Pues si quieres que sea yo el que te lleve la mira, vete pensando en invitarme a un "cubata" o mejor a cenar.

–Eso está hecho. Te tomo la palabra. Y ahora vámonos que tenemos muchos clavos que poner hoy –dice Joaquín, mirando un buen rato con complacencia a su clavo, antes de subir al coche.

Un momento antes de que Pedro cierre la puerta del maletero, la C de la cara de NGC365 se abre, dedicando una amplia sonrisa a sus compañeros que le ven irse con alegría. Al fin, va a recuperar la Altitud y con ella su Alma y tendrá un merecido retiro. El mejor que nunca podría tener un Clavo de Nivelación. NGX101 cree escuchar claramente una suave voz femenina que no había oído nunca, y que proviene de la finca "Dos de Espadas", a un kilómetro de distancia diciendo: "Adiós querido amigo, hasta siempre. Sé feliz por los dos".

Mientras, por la Línea 618 y extendiéndose al unísono por los 20.000 kilómetros del resto de Líneas de la REDNAP, y las más próximas de los países vecinos, se escucha una prolongada, emocionada y cerrada … OVACIÓN.

Sobre el autor:
Nombre: José Miguel Bel Martínez
Correo Electrónico: jmbelm@gmail.com
Institución: Ingeniero Técnico en Topografía (Colegiado Nº 492), Instituto Geográfico Nacional , España.

Investigación

NNtex: A toolbox to use the Neural Networks in an easy way

NNtex: Una toolbox para utilizar las Redes Neuronales de un modo sencillo

Xuefei Li, Alberto Camarero Orive, Francisco Soler Flores

y Nicoletta González Cancelas

Revista de Investigación

Volumen III, Número 1, pp. 149–154, ISSN 2174-0410
Recepción: 26 Oct'12; Aceptación: 10 Feb'13

1 de octubre de 2012

Abstract

An optimal toolbox: NNtex, which is based on Matlab software is developed in this paper. With the NNtex, the users can process and calculate the data through the simple operations. Through the built-in neural network toolbox in the NNtex, the users can optimize and calculate the input data and get the visual output and analysis results, including tables and figures. At the same time, by adopting the optimization algorithm, the models uses less memory space and has a fast operation, and for large-scale data it can also get the operation result in short time. The NNtex toolbox is applicable to be used in every field of science, and is convenient used for scientific and technological personnel, and it will have a good social value.

Keywords: Matlab, Neural Network, NNtex, Labbtex.

Resumen

En este trabajo se presenta NNtex, una toolbox para Matlab desarrollada para trabajar con redes neuronales de una manera sencilla y óptima. Con NNtex, los usuarios pueden procesar y calcular resultados a través de operaciones simples además de obtener salidas que incluyen tablas y figuras. Al mismo tiempo, mediante la elección automática del algoritmo, los modelos utilizan menos memoria y tiene un funcionamiento rápido, computacionalmente hablando, esto permite el trabajo con bases de datos grandes. NNtex puede ser usada en cualquier disciplina científica y ser utilizado por personal científico o técnico de forma sencilla.

Palabras clave: Matlab, Redes Neuronales, NNtex, Labbtex.

1. Introduction

Artificial Neural Networks (ANNs) is also referred to as Neural Networks (NNs) or called Connection Model. Neural networks are composed of simple elements operating in parallel. These elements are inspired by biological nervous systems. [1] It is an algorithm mathematical model that imitate the neural networks behavior characteristic of animals, and process the distributed parallel information. This network relies on the complexity of the system, through the adjustment of the internal connected relations of the nodes, in order to achieve the purpose of processing information[2].

In recent years, the researches about the neural networks are very popular, till now, a variety of neural network models have been developed and applied in different areas, such as the Back Propagation Neural Network(BP Neural Network), the Radical Basis Function Neural Network(RBF Neural Network), the Linear Neural Networks .etc[3][4][5]. The neural network is used to forecast, classification and identification, optimization and other typical fields, and plays an important role in all the fields. Especially for classification problem, the neural network is widely used because of its short operation time characteristic and the high operation efficiency.

Matlab is a well-known mathematical optimization software, the software is widely accepted and used by the science researchers in many different research fields. The friendly interface and simple operation of Matlab can make it easy to be used by the non-professionals. Matlab software has a toolbox specialized in neural networks: Neural Network Toolbox, which has multiple functions and models for creating and dealing with neural networks, and we can use them to assist the writing of the programs which are created by us.

However, the neural network theory is esoteric and the parameters setting process is relatively complex, and the quality of the parameters setting has great influence for the operation time and the accuracy of the operation result. Although Matlab software has a Neural Network Toolbox, how to use the neural network and how to set the related parameters will be a big difficult question for the normal users, such as engineers and beginners. In the Neural Network Toolbox, it only offers the basic functions of Neural Networks, not includes the ways to choose the parameters values and compare different neural networks. Therefore, we develop the new toolbox: NNtex which is based on the Neural Network Toolbox and NNtex can choose the related parameters and compare different neural networks results in an automatic way. By using NNtex, it will be much more easier to use neural networks for the engineers and beginners. After the running, NNtex uses Labbtex to generate report in an automatic way.

At the same time, through many years of experience and research, we often meet optimization and forecast problems in the transport and logistics research process. Therefore, in order to facilitate the repeated use, simplify the use process, and improve efficiency, we have developed NNtex toolbox. Through the use of NNtex toolbox, the users only by entering the data can get the optimization results and analysis results through the automatic operation of the program. In this way, it will reduce the difficulty and the workload for the users.

In order to ensure the accuracy of the NNtex toolbox operation results, we embedded three different kinds of neural network models in the development process, including the BP neural network, the RBF neural network and the linear neural network. After the user input

the data, the three kinds of neural network will be operated in order, and then get three different operation results. After this, we choose the best result by comparing the results with the receiver operating characteristic curve (ROC Curve)[6]. By using the NNtex toolbox, not only can let the users use the neural network toolbox through more simple ways, but also can choose the best answer from the different networks, and output tables and figures for users to adopt.

2. Description of NNtex

We develop the NNtex toolbox by using the Matlab R2009a software. The NNtex toolbox consists of seven parts, as following:

(1)data input module: provide the data input window for users

(2)data normalization module: normalize the input data, and get the data which is suitable for the model operation.

(3)BP neural network module: construct the BP neural network, this network could select the corresponding parameter and compare the results of different parameters according to the characteristics of the input data, and get the better the BP neural network and results.

(4)RBF neural network module: set up the RBF neural network, this network could choose the corresponding parameter and could obtain the good optimization operation result.

(5)linear neural network module: establish the linear neural network, this network could select the corresponding parameter, and get the good result.

(6)ROC analysis: compare the operation results of the BP neural network, RBF neural network and linear network, obtain the ROC curves and the area under concentration-time curve(AUC) values, and then select the maximum AUC value of the results for best result.

(7)data output: export the running results and acquire the analysis report by using the Labbtex.

The calculate flow chart of NNtex is shown in Figure 1.

3. A real-world example

By using the NNtex toolbox, we can get the research result in the form shown in Figures 2 and 3.

We can see from Figure 2 and Figure 3 that there is an intuitive calculate result which could show the computing process clearly and has a strong persuasion. After we get the research results and figures, we can generate the research report by using Labbtex[7] in the right forms.

4. Conclusion

NNtex is an important and precious toolbox which can solve the practice problems based on the Matlab software. The calculation process of this toolbox is stable, fast and

comprehensive. At the same time, NNtex requires less memory and could solve the large-scale problems in the limited conditions.

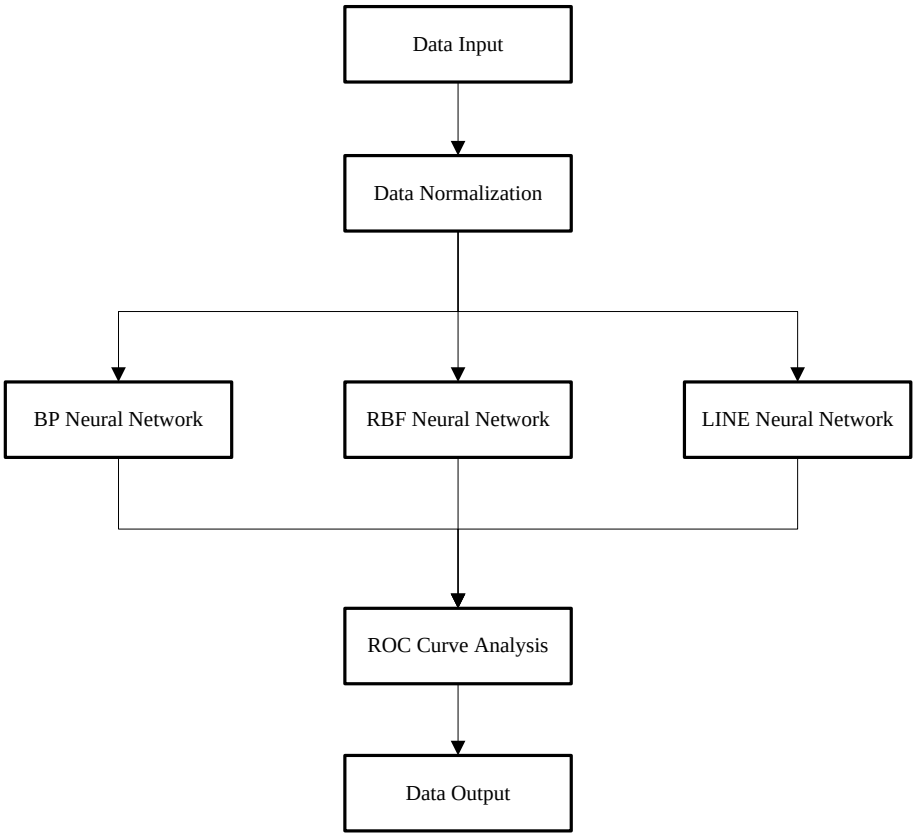


Figure 1. Calculate flow chart of NNtex.

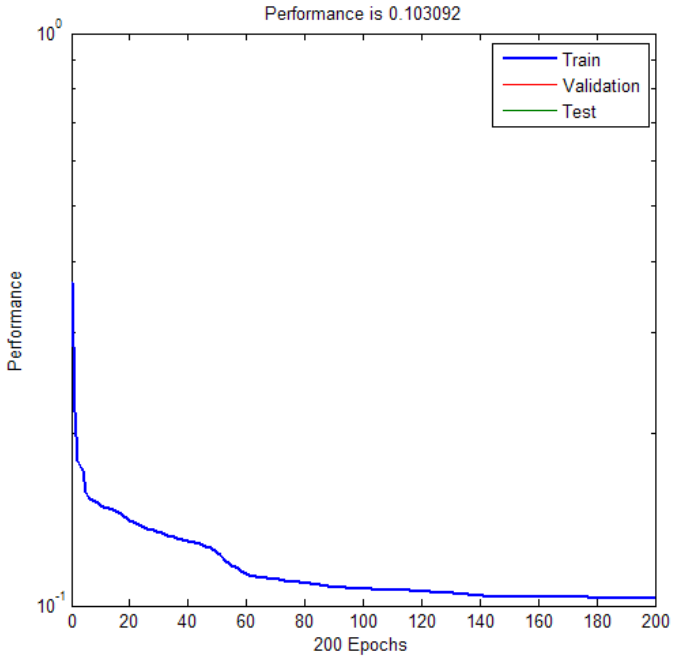


Figure 2. Calculate result of Neural Network

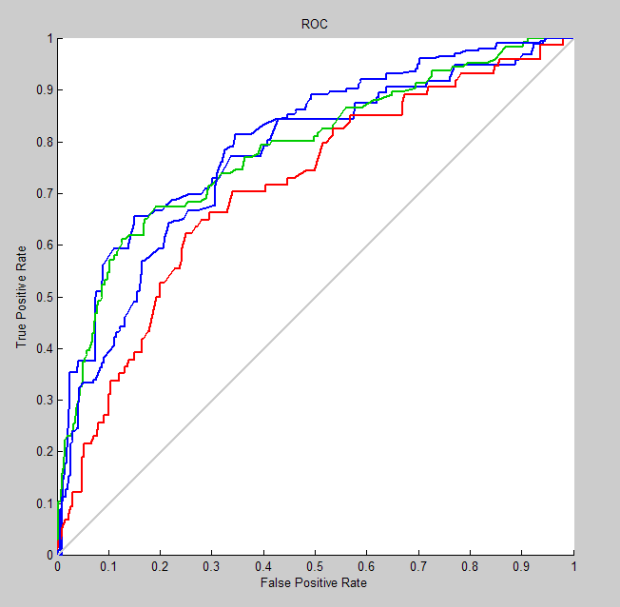


Figure 3. ROC analysis result

In the future, our research group will develop the toolbox which has more powerful functions, such as adding more different kinds of neural networks as contrast and improve the algorithm to improve the operation efficiency.

Acknowledgements

We gratefully acknowledge the valuable support of Departamento de Ingeniería Civil. Transportes, Escuela Técnica Superior de Ingenieros de Caminos, Universidad Politécnica de Madrid (Spain) and School of Traffic and Transportation, Beijing Jiaotong University (China) in preparing this paper. It is a project supported by the Fundamental Research Funds for the Central Universities (2012YJS054).

References

[1] HOWARD DEMUTH, Mark Beale. Neural Network Toolbox User's Guide, http://www.mathworks.com.

[2] FEISI Science and Technology Research Center. Matlab Application. Publishing House of Electronics Industry, Beijing, 2005.

[3] Robert Hecht-Nielsen. Theory of the Backpropagation Neural Network, pp. 593-605, International Joint Conference on, 1989.

[4] SAN HE, Yongli Zou, Desheng Quan and Hanyi Wang. Recent Advances in Computer Science and Information Engineering, pp. 639-644, Lecture Notes in Electrical Engineering, 2012.

[5] Terence D. Sanger. Neural Networks, pp. 459-473, Pergamon Press Plc, USA, 1989.

[6] Alberto Jiménez-Valverde. Global Ecology and Biogeography, pp. 498-507, Blackwell Publishing Ltd, 2012.

[7] F. Soler, N. González, A. Camarero, M.C. Palomino and J.L. Almazán. Segunda Jornada Internacional"Matemáticas Everywhere", pp. 313-319, Grupo de Investigación de la Universidad Politécnica de Madrid: "Matemática Aplicada a la Ingeniería Civil" (MAIC) and Grupo de Innovación Educativa de la Universidad Politécnica de Madrid: "Pensamiento Matemático", Spain, 2012.

Sobre los autores:

Nombre: Xuefei Li
Correo Electrónico: hopeandfuture2010@gmail.com
Institución: School of Traffic and Transportation, Beijing Jiaotong University, China.

Nombre: Alberto Camarero Orive
Correo Electrónico: alberto.camarero@upm.es
Institución: Universidad Politécnica de Madrid, España.

Nombre: Francisco Soler Flores
Correo Electrónico: f.soler@upm.es
Institución: Universidad Politécnica de Madrid, España.

Nombre: Nicoletta González Cancelas
Correo Electrónico: nicoleta.gcancelas@upm.es
Institución: Universidad Politécnica de Madrid, España.

Investigación

Creación de esculturas inspiradas en el análisis matemático de la obra de Jaume Espí

Creating sculptures inspired by mathematical analysis of Jaume Espí's work

M. Carmen Gómez-Collado, Jaume Puchalt, Joel Sarrió y Macarena Trujillo

Revista de Investigación

Volumen III, Número 1, pp. 155–166, ISSN 2174-0410
Recepción: 31 Ene'13; Aceptación: 25 Mar'13

1 de abril de 2013

Resumen

En este trabajo se hace un estudio matemático de alguna de las obras del escultor Jaume Espí donde se pone de manifiesto la relación tan estrecha que existe en algunos casos entre matemáticas y escultura. Presentamos además dos obras escultóricas creadas por nosotros, en cuya concepción y diseño ha sido fundamental el uso de matemáticas.

Palabras Clave: Matemáticas, Escultura, Jaume Espí, Mathematica.

Abstract

In this work is made a mathematical study of some works of Jaume Espí sculptor. We note that there exists a close relationship between mathematics and sculpture in some cases. We also present two sculptures created by us, in whose conception and design was essential to use of the mathematics.

Keywords: Mathematics, Sculpture, Jaume Espí, Mathematica.

1. Introducción

Para empezar desde el inicio, un inicio, elegiremos éste de una manera voluntaria. De esta manera fijaremos en el tiempo aquello de lo que queremos tratar, en concreto este trabajo se centra en un tiempo, nuestro tiempo, para desde el análisis contemporáneo intentar extraer cuál es la esencia de la escultura y la relación de las matemáticas con ésta. Respecto a la escultura queremos saber qué recursos matemáticos se han utilizado en sus procesos creativos.

Para nosotros es importante remarcar que el tema principal de toda escultura, ya que no podemos centrar nuestro trabajo en hacer un recorrido histórico, es fundamentalmente la repetición continua de elementos naturales: elementos existentes en el crecimiento de una flor, en la forma geométrica de una col,…

La formación académica de las antiguas escuelas de arquitectura y arte, hasta bien recientemente, sólo incluyó un aprendizaje geométrico; de ahí que los artistas que a lo largo de la historia trabajaron con fundamentos matemáticos más allá de la geometría siempre tuvieron cerca otros técnicos expertos en la materia, como es el caso de Le Corbusier con el músico matemático Xenakis. Otros escultores que incluyeron en su obra, pese a no tener ningún tipo de formación académica, aspectos geométricos y matemáticos, fue debido a que siempre partieron de un análisis, observación y repetición de formas naturales como cuerpos, paisajes, formas de crecimiento y desarrollo animal y vegetal … Esta forma no innata (porque surge de una formación previa), podríamos llamar casi intuitiva, de obtener unos resultados "matemáticos" es la que más nos interesa. Esta representación técnica (arquitectura y escultura) de las formas naturales cobrará un especial interés en el movimiento moderno, con la escultura abstracta…

La escultura abstracta no se ha entendido, y creemos que es un problema de la época, un problema de que no ha sido explicada. Esta incomprensión podría venir dada por la sobresaturación informativa en un momento histórico determinado. Ante tanta información (las dos guerras mundiales, las distintas crisis sociales, revoluciones…) no se supo explicar el qué se hacía, el porqué se hacía, pero es evidente la importancia histórica en la producción artística de esta época.

Figura 1. Peine del viento XV. E. Chillida

La escultura moderna intentó representar el espacio con los mínimos planos posibles (Neoplasticismo, Chillida, Oteiza), trató de representar la torsión de un cuerpo con un giro mínimo…, en definitiva trató de sintetizar la naturaleza. En la figura 3, se muestra la obra *Peine del viento XV* de Eduardo Chillida situada en la bahía de La Concha, San Sebastián.

A veces escuchamos "este cuadro lo podría haber hecho un niño de 3 años", y esta afirmación que se hace desde la ignorancia no sólo no es cierta sino que también es imposible.

No es cierto que cualquiera de los que estamos aquí ahora pueda dibujar como Picasso, uno de los artistas más valorados del movimiento moderno, ni tan siquiera entre todos

podríamos hacerlo. Es imposible porque ninguno de nosotros es influido por la luz que influyó a Picasso, ninguno de nosotros ha tenido una experiencia vital como la de Picasso, nuestras memorias son distintas, nuestras vivencias, y por tanto nuestros actos, pensamientos y reflexiones.

Pondremos un ejemplo. Si le proponemos a un adulto que dibuje la luz, no sabrá qué modelo de lámpara representar, cómo es el haz de luz que emite su bombilla, el neón o el tubo incandescente. Picasso, y un niño saben cuál es la esencia de la luz, qué cosas implica o no. La luz nos permite ver, muy sencillo. Así es cómo seguramente un niño representaría la luz, como un gran ojo que abierto (encendido) permite iluminar, reivindicar la vista (sentido). Como Picasso en el *Guernika*.

Figura 2. Guernica, P. Picasso, Museo Reina Sofía de Madrid

Cada uno de nosotros como sabréis, hablamos de una forma, sentimos de unas maneras, nos relacionamos entre nosotros de forma distinta…estas cosas nos hacen únicos e irrepetibles. Como también único ha de ser nuestro dibujo, al final una manera más de comunicarse, de exteriorizar aquello que somos, aquello que hacemos y hacia dónde queremos ir.

Para iniciar nuestro camino de analizar la esencia de la escultura e indagar en la relación de las matemáticas con ésta conviene reseñar, sin detenernos en hacer un recorrido por la evolución de las matemáticas a través de los tiempos, que en las últimas décadas el avance en las nuevas tecnologías y también en lo que respecta al software matemático desarrollado ha involucrado una apertura de miras en lo que al desarrollo del quehacer matemático. Como ejemplo nombraremos el *Teorema de Cuatro Colores* cuya demostración llevó más de 100 años de intensas investigaciones y fue el primer teorema de Matemáticas que se demostró por medio de una computadora.

Este universo de posibilidades que ofrece el uso del ordenador ha hecho que aparezcan numerosas manifestaciones escultóricas en cuya concepción, diseño, desarrollo o ejecución resulta fundamental la utilización de matemáticas. En este campo destacan autores como H. Ferguson (figura 3 izquierda), B. Grossman (figura 3 derecha), G. W. Hart, R. Roolofs o C. Sequin entre otros.

J. Barrallo y R. Zalaya en [1] hacen un estudio de esculturas definidas con la tipología descrita anteriormente que ellos definen como *Escultura matemática* y proponen una clasificación de las mismas desde un punto de vista puramente matemático en función de la propiedad/es matemática/s que la/s definen. Además fueron comisarios de la exposición que se llevó a cabo en la Universidad Politécnica de Valencia sobre este tema donde se expusieron algunas obras de los autores referenciados anteriormente. La asistencia a dicha exposición nos hizo plantearnos la posibilidad de abrir un campo de estudio sobre la influencia de las matemáticas en la escultura y el mundo de posibilidades que este tándem escultura-matemáticas podía tener. Nuestra intención no era construir con ayuda del ordenador nuevas impresiones en tres dimensiones que respondieran a ecuaciones matemáticas sino que pretendíamos ir más allá, contactar con algún escultor en cuyo trabajo no contara con la ayuda de ordenador y que en alguna de sus obras emanara un fondo matemático, estudiarlo, y poder entablar una cooperación con el propio escultor con el fin de darle una vuelta de tuerca a esas matemáticas subyacentes, que el propio autor no se había planteado ni que pudiera tener, para que nuestro trabajo le sirviera de fuente de ideas a él y a nosotros mismos para dar origen a nuevas formas de expresión que obedecieran a razones matemáticas. El autor elegido es el escultor Jaume Espí.

Nuestro objetivo, matemáticamente hablando es doble, por una parte estudio matemático de obras ya hechas y obtención de una modelización de éstas para compararlas con la original y por otra parte, experimentar con la ayuda del programa Mathematica 8.0 (Wolfram Research, Champaign, Illinois, EEUU), 3DStudioMax (Autodesk Inc., San Rafael, CA, EEUU) la creación de obras escultóricas que estén descritas por conceptos matemáticos.

2. Modelización de esculturas de Jaume Espí

Nuestro punto de arranque en la modelización de esculturas fue estudiar algunas obras del escultor valenciano Jaume Espí cuyo taller se encuentra en Carlet (Valencia). Para la realización de nuestro estudio contactamos con él, que nos proporcionó información muy valiosa respecto a su forma de trabajo y su método creativo. J. Espí nunca trabaja con medios informáticos, ni sistemas de representación externos a aquello que no hagan sus propias manos.

2.1. Jaume Espí escultor

Lo Para describir la obra de Jaume Espí empezaremos refiriéndonos a su formación personal, a su experiencia. Cuando Jaume trabaja siempre intenta encontrar el camino más sencillo, la solución a aquellos imprevistos que le surgen, y esto define su trabajo. Para él no es importante llegar a un punto determinado con su escultura, sino el misterio de poder trabajar cada día en aquello que le gusta y mejor hace, la escultura.

Por ejemplo, tras conseguir una partida de piedra extraída de los antiguos bordillos del casco antiguo de la ciudad de Carlet, necesitaba una manera de ensayar las formas que quería realizar. Las proporciones de estas piezas eran parecidas a las de las tizas cuadradas, utilizadas en nuestras escuelas, y respondían a su necesidad. De esta manera realiza ahora muchos de sus trabajos previos en este material. Debido a la escala y fragilidad de estas piezas, J. Espí se ve obligado a reflexionar sobre cuáles serán los problemas al realizar las

reproducciones en otro material, el proceso ejecutivo de las mismas y el tamaño ideal de las ampliaciones.

Figura 4. Foto de J. Espí trabajando la tiza.

Al verlo trabajar (figura 4) transmite siempre cuáles son sus intenciones, a veces en forma de dibujo sobre las piezas en bruto, otras mediante gestos con las manos o mediante la realización de otras maquetas en otros materiales que expresen aquello que quiere comunicar. Esta esencia escultórica es muy importante a la hora de parametrizar sus esculturas.

2.2 Modelización matemática de la escultura ``Alexandria''

Nosotros, cómo el artista, intentaremos extraer esta esencia, y de esta manera realizaremos el análisis matemático. Para no complicar el análisis, ni tampoco extendernos demasiado, explicaremos principalmente el trabajo desarrollado sólo con la obra ``*Alexandria*'' de la serie ``*Fars*'' reflejada en la Figura 5.

Figura 5. Alexandria. Medidas b 110 x 110 x h 660 mm. Piedra calcárea de la Mola

La idea (boceto) de esta obra se inscribe dentro de una de las tizas con las que trabaja habitualmente J. Espí (Figura 6). En concreto podríamos describirla como el resultado escultórico de coger el prisma de yeso y torsionarlo.

Figura 6. Tiza esculpida

Su descripción matemática sería la siguiente: Se consideran dos cuadrados en el espacio, de iguales dimensiones, separados una distancia h (altura de la torre) y con la particularidad de que el cuadrado superior es el resultado de efectuar un giro de 90° (en sentido de las agujas del reloj) en el cuadrado inferior. La escultura viene determinada como el resultado de unir por medio de rectas cada punto de los lados del cuadrado inferior con el correspondiente punto del cuadrado superior una vez efectuado el giro. La Figura 7 representa esta idea.

Figura 7. Dibujo que representa la torsión implícita en la obra Alexandria

Para modelizar matemáticamente la torre, poder implantar las ecuaciones en el programa Mathematica y obtener con posterioridad una representación en tres dimensiones de la obra, una de las opciones posibles es seguir los siguientes pasos:

- Parametrización del cuadrado que forma la base

- Parametrización del cuadrado que forma la tapa

- Parametrización da cada uno de los lados de la torre que se reduce a parametrizar los segmentos que unen los puntos de un lado con los puntos del otro lado.

El proceso anterior se puede simplificar parametrizando sólo un lado del cuadrado inferior, el correspondiente lado en el cuadrado superior una vez efectuado el giro y la parametrización del lado de la torre que se obtendría uniendo los puntos de los dos lados por medio de rectas. El resto de lados que componen la torre se obtendrían haciendo giros de 90°, 180° y 270° en el ya construido.

La representación obtenida con el programa Mathematica es la mostrada en la Figura 8.

Figura 8. Representación obtenida con Mathematica

La torre también puede ser descrita, de forma más simplificada, por medio de una ecuación implícita pero hemos recurrido al uso de su descripción paramétrica principalmente por los dos motivos siguientes: el primero es la simplicidad de este método ya que todo se reduce a la parametricación de un segmento y al uso de la matriz de rotación en el espacio. El segundo radica en que esta metodología de trabajo también nos permite una generalización fácil de la deformación de este volumen con tan solo alterar las fórmulas usadas en la parametricación y poder considerar diferentes curvas de unión entre los ocho vértices que conforman la torre. Algunas de estas deformaciones pueden visualizarse en la figura 13.

Una vez realizado este trabajo matemático, las posibilidades para experimentar con nuevas formas a partir de la idea inicial de torsión son infinitas. Las primeras modificaciones sencillas que vamos a realizar son las correspondientes a eliminar en la torre *Alexandria* dos de sus caras y quedarnos con las otras dos. Cada uno de estos procesos se corresponde a otras esculturas ya realizadas por el escultor:

- Si eliminamos en la escultura Alexandria dos caras contiguas obtenemos la escultura *Pedra de toc 2* de la serie *Clau de volta* representada en la Figura 9.

Figura 9. Pedra de toc 2. Medidas b20 x20 x h 50 mm. Piedra calcárea de la Mola

- Si eliminamos en la escultura dos caras paralelas obtenemos la obra *Pedra de toc 3* también de la serie *Clau de volta* que vemos en la Figura 10.

Figura 10. Pedra de toc 3. Medidas b 20 x20 x h 50 mm. Piedra calcárea de la Mola

De esta manera, si miramos con ojos matemáticos algunas de las obras de J. Espí, podemos decir que el escultor sólo ha realizado una escultura, como el arquitecto sólo un edificio, o el pintor un cuadro. Recuerden que estamos hablando de la esencia de las cosas. Por si les estamos confundiendo les pondremos un ejemplo. A Chillida le preguntaron una vez si se había dado cuenta que uno de sus collages (*Gravitaciones*), La escultura *Consejo al espacio* ubicada en Chillida-LeKu, y el *Elogio del agua* ubicada en el parque Creueta de Coll de Barcelona, eran la misma. Él se sorprendió.

En las Figuras 11 y 12, vemos algunas obras de J. Espí que reflejan esta idea.

Figura 11. Izquierda: Clarobscur I. Medidas b 170 x 170 x h 480 mm. Central: Babel. Medidas b 170 x 170 x h 680 mm. Derecha: Pedra de toc 4. Medidas b 20 x 20 x h 50 mm

Figura 12. Izquierda: Porta stelae petrum. Medidas b 1.5 x 1 x h 2 m. Piedra calcárea de la Mola. Derecha: Canyamel. Medidas b 0.5 x 0. 5 x h 2.4 m. Bronce pavonado negro

Como ejemplos de otras posibles obras que pueden ser obtenidas a partir de la obra Alejandria y de la idea de torsión pero considerando que las funciones que definen el giro sean por ejemplo hélices de diferente paso (lineal, cuadrático, logarítmico,...), con diferentes ángulos de giro, etc. son las que presentamos en la Figura 13.

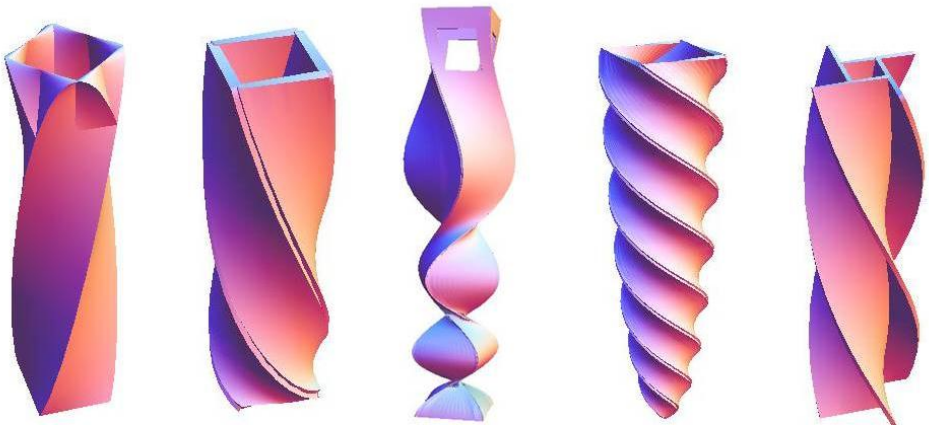


Figura 13. Dibujos obtenidos con Mathematica

Esto es un pequeño descubrimiento que si se incorporase al procedimiento creativo del escultor podría ser una herramienta rápida que permitiría visualizar distintas posibles esculturas de una manera económica. Contamos con que el trabajo escultórico no es el matemático, sino aquel que realizaría J. Espí a partir del proceso que hemos seguido. De esta manera la unión entre las matemáticas y la escultura ha de venir de la mano de aportar conocimientos de una a la otra, de intentar sacar la esencia de los procedimientos creativos matemáticos para utilizarlos en la escultura y viceversa.

3. Nuestras nuevas esculturas

Para aquellos que están familiarizados con las matemáticas habrán oído alguna vez la frase ``curiosidad matemática" que define la inquietud de aquellos que trabajan con ellas en saber qué pasará si en vez de considerar una cosa considero otra, si en vez de suponer esto supongo aquello, si esta condición la cambio por aquella, etc. Pues bien si a la hora de escribir en Mathematica las sentencias que definen la parametrización de la escultura inicial (Alexandria) se recurre al uso de parámetros en las expresiones genéricas de las funciones que definen la torsión, el ángulo de giro, las dimensiones del cuadrado, etc., no requiere gran esfuerzo la obtención de un amplio abanico de variantes de la torre (algunos de ellos ya están mostradas en la figura 13) y queda sembrada la semilla para experimentar con nuevas superficies donde las secciones transversales ya no tienen por qué ser un cuadrado y en cuya parametrización se pueden combinar, jugando, funciones de diferentes familias que proporcionan resultados que escultóricamente nos han gustado y en cuya esencia también radica la torsión (Figuras 14 y 15). En la escultura renderizada en la Figura 15 queda patente además la influencia de las columnas salomónicas en la descripción matemática de la misma.

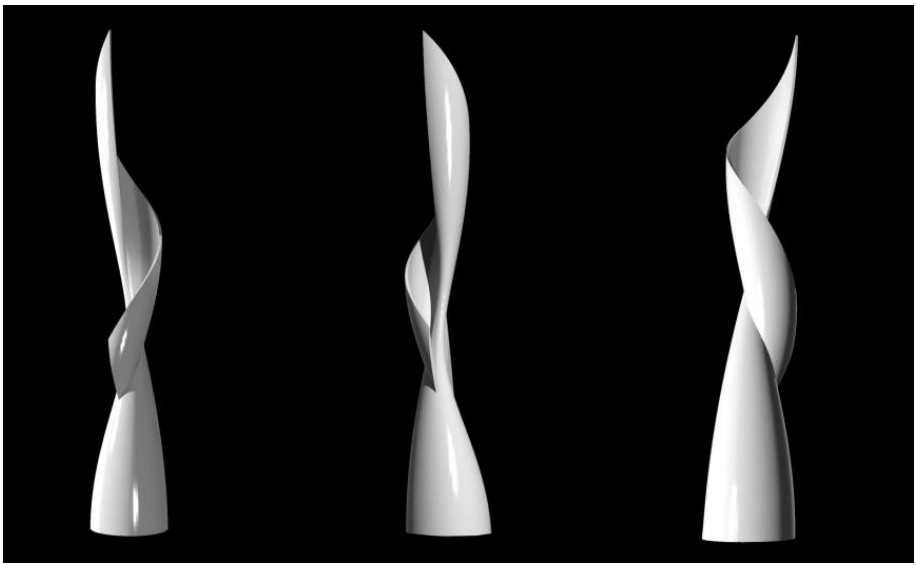


Figura 14. Renderizado de la nueva escultura "Iness"

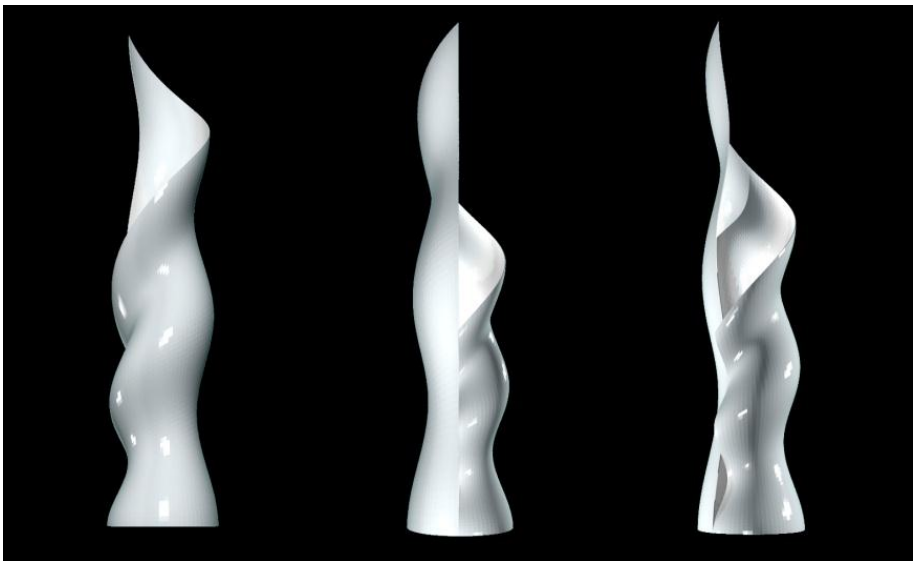


Figura 15. Renderizado de la nueva escultura "Adrigón"

Por último, decir que según J. Barrallo y R. Zalaya [1] estas obras serían catalogadas como Escultura Matemática pero dejamos a criterio del lector el juzgar si les trasmite emociones o no.

Agradecimientos

Este trabajo ha sido financiado parcialmente con la Ayuda de Innovación Docente del Dpto. de Matemática Aplicada de la UPV (PID-DMA2012).

Referencias

[1] BARRALLO, Javier y ZALAYA, Ricardo. *La escultura matemática y su clasificación*, Editorial UPV, Valencia, 2006

[2] ESPI, Jaume . *Clau de volta*. Editado por Fundació Caixa Carlet. ISBN 84-933366-7-7.

[3] ESPI, Jaume *Jaume Espí Escultura*, http://www.jaumeespi.com

Sobre los autores:

Nombre: María del Carmen Gómez Collado
Correo Electrónico: cgomezc@mat.upv.es
Institución: Instituto Universitario de Matemática Pura y aplicada (IUMPA), Universidad Politécnica de Valencia, España.

Nombre: Jaume Puchalt Lacal
Correo Electrónico: jaume.jpl@gmail.com
Institución: ETS de Arquitectura, Universidad Politécnica de Valencia, España. Jaume Espí escultura.

Nombre: Joel Sarrió
Correo Electrónico: sarriopuig@gmail.com
Institución: ETS de Arquitectura, Universidad Politécnica de Valencia, España.

Nombre: Macarena Trujillo Guillén
Correo Electrónico: matrugui@mat.upv.es
Institución: Instituto Universitario de Matemática Pura y Aplicada (IUMPA), Universidad Politécnica de Valencia, España.

Investigación

Matemáticas de Sociedad y Síndromes Sociales

Societal Mathematics and Social Syndromes

José–Manuel Rey

Revista de Investigación

Volumen III, Número 1, pp. 167–176, ISSN 2174-0410

Recepción: 1 Feb'13; Aceptación: 26 Mar'13

1 de abril de 2013

Resumen

En una situación de interacción social en que cada individuo está afectado por las decisiones de los demás hay dos cuestiones fundamentales: qué es lo previsible que suceda, y qué es lo deseable. Cuando la conducta de los individuos responde a sus propios incentivos y el resultado previsible es indeseable socialmente se produce un síndrome social. La teoría de juegos –las matemáticas de sociedad– ha proporcionado el armazón teórico para esas cuestiones. Aquí se presentan algunos sencillos ejemplos que se producen en situaciones cotidianas y sirven de paradigma de otras patologías sociales.

Palabras Clave: Interacción social, Dilema del prisionero, Gallina, Teoría de juegos, Trampas sociales.

Abstract

In any situation of social interaction in which every individual is affected by the actions of the others, two fundamental issues arise: what is foreseeable and what is desirable, that is, what must be expected to occur and what is the preferable outcome from a social perspective. A situation in which individuals obey their own incentives and the expected outcome is socially undesirable may be called a social syndrome. Game theory provides the theoretical framework to analyze formally these questions. In this paper we considered several situations that are part of the everyday and serve as basic models for many other social pathologies.

Keywords: Social interaction, Prisoner's dilemma, Chicken, Game theory, Social Traps.

Este artículo está dedicado a Pedro de Alzaga.

1. Los prisioneros

Dos estudiantes han obtenido un notable en el examen de junio, que se copiaron. El profesor les reúne y les explica que tiene suficiente evidencia como para bajarles la nota a un aprobado, pero les propone una forma de conservar su nota. Les pide que escriban en un papel por separado si copiaron o no. Si uno reconoce la trampa y el otro no, le mantendrá el notable al primero

pero suspenderá al mentiroso en junio y en septiembre. Si los dos admiten que copiaron, les suspenderá a ambos sólo en junio, mientras que si ambos lo niegan les dejará en aprobado.

Los dos estudiantes se plantean independientemente la difícil disyuntiva de si confesar o no la culpa. La dificultad reside en que el resultado más ventajoso para cada uno, mantener el notable, depende de que el otro no confiese y se gane así un suspenso total en el curso. Así que cada uno debe contar que el otro confesará. Pero, haciéndolo ambos, se arrepentirán de no haber callado, con mejor resultado para los dos. Sin embargo, eso no puede esperarse, porque cada uno estará tentado a confesar si el otro no lo va a hacer. La lógica les devuelve a la confesión doble y el malestar de saber que hay una solución mejor pero que está fuera de alcance.

Probablemente sin saberlo, los estudiantes están atrapados en uno de los embrollos más famosos de las ciencias sociales: el dilema del prisionero. El problema fue originalmente ideado en 1950 por dos matemáticos, Flood y Dresher, en la corporación RAND en California (EEUU) [3]. Se trataba de un experimento para contrastar la predicción sobre la conducta de los individuos de la entonces reciente teoría de juegos –las matemáticas de las relaciones sociales. La puesta en escena más conocida del dilema –y que le da nombre– se debe al matemático norteamericano Albert Tucker, que inventó la historia de dos delincuentes, sospechosos de un crimen, que han sido capturados por un delito menor. Al ser interrogados por la policía, deben elegir entre confesar o no el crimen que han cometido juntos. Serán condenados a un año si ninguno confiesa el crimen, pero a 5 años si los dos lo confiesan. Si sólo confiesa uno, saldrá libre –por colaborar con la justicia–, mientras al otro le caerán 10 años. El problema que afrontan los estudiantes es una versión *mutatis mutandis* del dilema del prisionero.

Hay un modo muy sencillo de representar la situación de los estudiantes usando una tabla:

	sí	no
sí	S, S	N, SS
no	SS, N	A, A

En las entradas de la primera columna se representan las posibles estrategias (sí o no confesar) de un estudiante –jugador, como se llama en la teoría de juegos– y en la primera fila las estrategias del otro. En cada una de las cuatro casillas se escriben los posibles resultados del juego, expresados con las notas obtenidas por los estudiantes: notable (N), aprobado (A), suspenso en junio (S), y suspenso en junio y septiembre (SS) –ése es el orden en que las prefieren los estudiantes. En cada casilla, la primera nota es la del estudiante que juega por filas y la segunda la del que juega por columnas.

La teoría de juegos permite analizar las situaciones sociales –"juegos"– en que los individuos toman sus decisiones independientemente obedeciendo sus propios intereses. Estos suelen ser egoístas en un sentido moral. Por ejemplo, a cada estudiante sólo le preocupa sacar la máxima nota posible, sin tener en cuenta el coste para el otro. Pero la teoría de juegos no se preocupa por la naturaleza de los incentivos de los individuos. Sólo asume que cada individuo se comportará *racionalmente*, es decir, que será coherente con sus propios incentivos, eligiendo la opción que más le satisface entre las que tiene disponibles. Bajo esa hipótesis, la lógica de la teoría da una solución precisa para el dilema de los estudiantes: ambos deben confesar. Es fácil convencerse de que esa es la solución: si uno estudia su mejor estrategia en función de la que podría adoptar el otro, concluye que confesar es más ventajoso *en cualquier caso*. En efecto, si el otro confiesa, uno debe hacerlo y conseguir un suspenso sólo en junio; y si el otro no confiesa, también debe hacerlo para mantener su notable en lugar de aprobar. Es sencillo representar en la tabla ese análisis señalando las mejores estrategias de cada jugador para cada una del otro. Debajo se ha destacado en negrita, para cada columna la mejor estrategia fila, y para cada fila la mejor estrategia columna. La mejor estrategia en ambos casos es la misma: confesar. La casilla (S, S) en rojo es, por tanto, la predicción de la teoría para el dilema.

	sí	no
sí	**S, S**	**N**, SS
no	SS, **N**	A, A

La solución que se obtiene es muy poderosa: confesar es mejor siempre, en cualquier contingencia, sin importar qué hará el otro, ni siquiera cuáles son sus preferencias , es decir, su mejor estrategia, entendida como función de las estrategias del otro, es constante. En teoría de juegos, esa solución se llama equilibrio en estrategias *dominantes*, porque cada estrategia de equilibrio *domina* a las demás en cualquier escenario.

No existe dificultad lógica alguna para resolver el dilema del prisionero. Sin embargo, se han escrito bibliotecas completas sobre el asunto. La razón es que la conclusión resulta del todo insatisfactoria. El verdadero dilema de los prisioneros reside en que hay un resultado mejor para ambos –la casilla (A, A) en verde en la tabla– que el que les impone la lógica –la roja– y, sin embargo, no se producirá. Para ello deberían coordinarse independientemente y no confesar, lo que no será posible si siguen sus propios intereses. Podrían intentarlo, razonando en el lugar del otro para llegar a la conclusión que dos individuos "razonables" escogerán la misma opción y que, entre las soluciones simétricas, la mejor es no confesar. Pero eso sólo servirá para que cada uno, creyendo al otro convencido de que no debe confesar, le traicione y confiese para sacar la máxima ventaja del silencio del otro. El dilema se convierte así en una tensa cuestión de confianza en el otro, que a su vez no es más que un trasunto de uno mismo.

En cada nuevo dilema del prisionero, los dos protagonistas sufrirán el síndrome que produce la cuestión de confianza. En el momento de hacer su elección sentirán su tensión, incluso si conocen el análisis del dilema de antemano. Los acuerdos o juramentos previos para coordinarse si no son vinculantes no sirven para evitar el estrés del dilema y su peor desenlace. En efecto, los estudiantes podrían acordar previamente que lo deseable es callar y prometerse hacerlo, pero en el instante de tomar la decisión lo previsible es que ambos confiesen –racionalidad obliga. Tan cierto es que el dilema tiene una nítida solución lógica como que el combate sobre la realidad y el deseo es inevitable. Y que, finalmente, lo previsible quedará lejos de lo deseable.

Descubrir el dilema del prisionero es como caer en la cuenta de que el aire existe, como afirma William Poundstone, que escribió alrededor del dilema todo un libro [6]. En mayor o menor medida siempre hemos sentido actuar su mecanismo, que es parte indisoluble de nuestra dimensión social. Cada vez que aparece, el dilema inocula en los prisioneros el mismo veneno: coordinarse o ir por libre. Lejos de ser un artefacto teórico, el dilema está muy presente en la vida real. Es fácil crear un dilema del prisionero. Basta con que exista, de partida, una solución de compromiso que cada parte mejorará si sigue sus incentivos unilateralmente, pero que conduce a una situación peor que la inicial si las dos partes lo hacen. Las guerras de precios entre empresas, la proliferación nuclear entre países enemistados, las guerras de bandas organizadas, la competencia por el share en los medios de comunicación, ... todas exhiben a menudo la desastrosa solución de un dilema del prisionero.

Los dilemas similares con muchos "prisioneros" también abundan, y su desenlace suele ser tan agrio como en el dilema de dos (ver por ejemplo [1], [6]). Estas situaciones sociales patológicas –síndromes o trampas, en psicología– aparecen fácilmente, puesto que la sensación de traición al romper la solución coordinada se diluye más entre muchos individuos, que además son anónimos. Sin una conciencia social de los individuos adquirida o impuesta, esas patologías sociales son difíciles de neutralizar. Muchos fenómenos que observamos cotidianamente se pueden explicar como síndromes del prisionero: la contaminación excesiva en algunas ciudades debida al tráfico, la sobreexplotación de la pesca en aguas internacionales, la inacción de los países frente al cambio climático, el estado degradado de áreas y zonas públicas, ...

A continuación se muestran dos situaciones cotidianas en que se produce un síndrome so-

cial. Responden a mecanismos diferentes. En la primera, un dilema del prisionero con muchos participantes, las matemáticas permiten demostrar que hay una solución previsible –roja, como arriba– que es indeseable: existe otra mejor –verde– que no se producirá. En la segunda situación, sí existen a priori resultados deseables que son previsibles, pero esas soluciones –rojas y verdes a la vez– son muchas, de modo que si los individuos no son capaces de coordinarse existe riesgo severo de que se produzca un resultado pésimo.

2. El escote

El episodio es bien conocido y suele suceder, por ejemplo, a menudo por navidad. En la cena con los colegas de trabajo o en las cañas con los compañeros del gimnasio, el procedimiento se repite una y otra vez. El numeroso grupo se acomoda en el restaurante o en el bar, y entre ruidos y risas, cada uno por su cuenta pide al camarero su cena o sus bebidas. Después de más ruidos y risas llega el momento de pedir la cuenta. Alguien saca el móvil, divide el total entre el número de presentes y anuncia la noticia: "redondeando con la propina ... ¡tocamos a tropecientas!" Cada uno paga su parte, mientras va rumiando la sensación de que la cena ha sido mala o el bar muy caro. El año que viene habrá que cambiar.

Y el año que viene se cambia: para repetir la misma escena final en distinto escenario. Porque la molesta sensación tras la cena se debe a un mecanismo de interacción de grupo que nada tiene que ver con el restaurante o el bar. Si a los comensales les gusta comer bien a buen precio, piden consecuentemente por separado y la cuenta se paga a escote, no hay forma de evitar el malestar del desenlace. A pesar de las razonables condiciones de partida o, mejor, a causa de ellas el grupo es víctima de una trampa social, el síndrome del pago a escote.

Las matemáticas permiten convencerse de que, en efecto, el síndrome se produce. Se trata de deducir la conducta de los individuos del grupo cuando piden su cena por libre y la cuenta se reparte entre todos por igual. Para simplificar, se supone que el placer que proporciona la cena es sólo función de su precio y que todos los comensales disfrutan por igual de la comida. En concreto, se supone que el placer de una comida de un precio $p \geq 0$ está dado por una función $V(p)$ derivable, y tal que $V' > 0$ y $V'' < 0$. Esa es una hipótesis natural para la satisfacción que proporciona disfrutar de algo bueno: es un principio general en psicología que "las cosas buenas sacian" [2]. Así, al aumentar el precio lo hace la calidad de la comida, y por tanto el disfrute –porque V es creciente–, pero aumenta cada vez menos con cada euro adicional gastado –porque V es cóncava. Se supone que hay N personas en la cena que disfrutan por igual con la comida –todos la valoran con V–, y que su satisfacción con la cena es el balance entre el placer de degustar su propia comida y el precio que pagan por ella. Como pagan a escote, si se pagan precios p_i, $i = 1, 2, \ldots, N$, la satisfacción de cada uno con la cena esta dada por

$$U_i(p_1, p_2, \ldots, p_N) = V(p_i) - \frac{p_1 + p_2 + \ldots + p_N}{N},$$

con $i = 1, 2, \ldots, N$. La interacción del grupo es aparente en cada función U_i: la satisfacción de cada uno depende de todas las decisiones, no sólo de la suya. Para simplificar el análisis se puede suponer que $V(P) = p^\alpha$, con $0 < \alpha < 1$. Se trata entonces de determinar la solución previsible si los individuos son racionales. Cada individuo decidirá el menú de su cena –su precio p_i^*– estratégicamente en función del resto de precios, como el precio que le da mayor satisfacción. Por lo tanto, debe ser $p_i^* = (\alpha N)^{\frac{1}{1-\alpha}}$, el mismo precio para todos[1], como se podía anticipar por la simetría del problema. Como en el dilema del prisionero, el precio de cada cena es constante –no depende del resto de precios. El dilema de la cena a escote también tiene una solución de estrategias dominantes: todos pedirán el mismo menú, de precio $p^*(N) = (\alpha N)^{\frac{1}{1-\alpha}}$.

[1] Como U_i es cóncava en cada variable, p_i^* se obtiene de $\frac{\partial U_i}{\partial p_i} = 0$.

Ese menú es la solución "roja" del dilema de la cena, equivalente a la solución "confesar" del dilema del prisionero. Es interesante analizar cómo cambia el menú rojo con N. En primer lugar, se observa que a medida que aumenta el número de comensales el precio de los menús aumenta. Así que cuantas más personas haya cenando más cara saldrá la cena por barba. En fin, merecerá la pena si la sensación con la cena también mejora con N. Sin embargo, resulta que la satisfacción de cada individuo en el equilibrio $U_i^*(N) \equiv U_i^*(p_1^*(N), p_2^*(N), \ldots, p_N^*(N))$ es decreciente estrictamente para $N \geq 1$[2], de modo que la sensación prevista con la cena disminuye con el tamaño de la mesa: a medida que aumenta el grupo, empeora la sensación tras pagar la cuenta. Irónicamente, la satisfacción de la cena en grupo es máxima cuando se cena sólo $(N = 1)$[3].

Parece haber sólo malas noticias para la cena a escote, que además empeoran si el tamaño del grupo aumenta. Quizá existe, sin embargo, otra forma de pedir el menú que sea más satisfactoria para todos –una solución coordinada como en el dilema del prisionero. Por ejemplo, se pueden decidir los menús "socialmente", eligiendo los precios p_i^S, $i = 1, 2, \ldots, N$, que consiguen que sea máxima la satisfacción agregada –la suma de las de todos , i.e.

$$\sum_{i=1}^{N} U_i(p_1, p_2, \ldots, p_N) = \sum_{i=1}^{N} V(p_i) - (p_1 + p_2 + \ldots + p_N).$$

Con ese criterio, se obtiene el menú de precio $p_i^S = p^S \equiv \alpha^{\frac{1}{1-\alpha}}$[4]. Así que el precio del menú social igual para todos es constante y no aumenta con el tamaño del grupo. Es más, ya a partir de dos comensales, es claro que el precio del menú social es siempre más barato que el menú de equilibrio. Parecen buenas noticias. Y desde luego lo serán si la satisfacción de cada persona con el menú social $U_i^S \equiv U_i(p_1^S, p_2^S, \ldots, p_N^S)$ es mayor que con el menú rojo $U_i^*(N)$. Resulta que, en efecto, se verifica que $U_i^S \equiv U_i(p_1^S, p_2^S, \ldots, p_N^S) > U_i^*(N)$ para todo $N > 1$[5]. Por tanto, el menú social no sólo es más barato que el menú rojo, sino que deja más satisfechos a todos con la cena y además eso mejora cuando el grupo aumenta. El menú social hace de solución "verde" de la cena, como "no confesar" en el dilema del prisionero.

Se diría que el problema de la cena se soluciona si todos piden el menú social: cenan barato y bien, sin importar el tamaño del grupo. Pero no, porque opera el mismo síndrome del dilema del prisionero: si cada uno considera a priori pedir el menú verde, al pedir su cena por separado, finalmente estará tentado a pedir el precio del menú rojo –su mejor opción pidan lo que pidan los demás. Todos acabarán pidiendo el menú rojo, cenando caro y mal. De nuevo aparece la brecha entre el deseable menú verde y el previsible menú rojo.

El síndrome no es producto de la maldad o de la ignorancia de los individuos a la hora de elegir su cena. Al contrario, cada uno resuelve su problema individual correctamente, pero no pueden evitar el mal resultado para todos, incluso si conocen el engranaje de las piezas de la trampa. En la práctica existen formas para implementar la solución social y evitar el síndrome, como contratar el menú verde de antemano de modo que nadie tenga que pedir su cena. No es casual que esa sea práctica usual en muchas cenas de empresa o de navidad.

El síndrome del escote aparece a menudo en la vida social. Ocurre cuando, al no ser ob-

[2] Puesto que $U_i^*(N) = (\alpha N)^{\frac{\alpha}{1-\alpha}} - (\alpha N)^{\frac{1}{1-\alpha}}$, resulta que

$$\frac{\partial U_i^*}{\partial N} = -\frac{1}{1-\alpha}\alpha^{\frac{1}{1-\alpha}} N^{\frac{\alpha}{1-\alpha}}(1 - N^{-1}) < 0 \text{ para } N > 1.$$

[3] De la nota 2 y que la derivada $\dfrac{\partial U_i^*}{\partial N}$ se anula para $N = 1$.

[4] El menú $(p_1^S, p_2^S, \ldots, p_N^S)$ es la solución de un problema de optimización cóncava multivariante. Del sistema $\dfrac{\partial}{\partial p_i}\left(\sum_{i=1}^{N} U_i\right) = 0$, $i = 1, 2, \ldots, N$, se obtiene $p_i^N(N) = p^S \equiv \alpha^{\frac{1}{1-\alpha}}$ para cada i.

[5] Puesto que $\min_N\{U_i^S - U_i^*(N)\} = U_i^S - U_i^*(1) = 0$ y $U_i^N(N)$ decrece estrictamente con N (ver notas 2 y 3).

servado, uno está tentado a saltar la barrera del metro y viajar gratis. O cuando uno quiere disfrutar de una Wikipedia libre de anunciantes pero no aporta un euro para sostenerla así –periódicamente, la enciclopedia virtual solicita recaudación para mantenerse libre de publicidad[6]. El fenómeno se suele conocer como el *problema del polizón*.

3. El gallinero

La siguiente escena es un estereotipo que se repite a menudo en innumerables bares y sábados. Un grupo de chicos que se halla en el local está considerando cómo interaccionar con otro grupo de chicas que ha llamado su atención. Entre ellas destaca una rubia que todos encuentran poderosamente atractiva. Cada chico está valorando si acercarse a hablar a la rubia o irse a charlar con una de las otras chicas –todas morenas. Si se aproxima a la rubia podría encontrarse compitiendo con otros y, como resultado, terminar solo –puesto que si, tras la rubia se acerca a una morena, ninguna le hará caso al verse como "segundo plato". Por otra parte, si de entrada elige una morena, no habrá competencia y tendrá charla y compañía asegurada[7].

De nuevo, la situación presenta un dilema de interacción psicológica entre los chicos, puesto que la decisión de cada uno –acercarse a la rubia o a una morena– está condicionada por las de los otros. Si cada uno va por una chica diferente, todos consiguen charlar con una, aunque estará más contento el que consigue charlar con la rubia. Si más de uno se arrima a la rubia, entre el bloqueo entre ellos con la rubia y el rechazo posterior de las morenas ninguno de ellos se empareja.

Cómo no, los chicos caerán en la cuenta de que se trata de coordinarse. Pero sin negociación previa entre los chicos, no es fácil. De entrada, los resultados favoritos de cada uno –"yo con la rubia"– están en conflicto entre sí. Si cada chico piensa entonces en ir por una morena para evitar lo peor –acabar sólo en la barra–, la rubia se quedará sola. Si por eso considera ir con la rubia, ocurre lo peor, porque todos habrán pensado lo mismo y estará rodeada. Para evitarlo, contempla acercarse a una morena,… ¡pero de nuevo la rubia se queda sola! A diferencia del dilema del prisionero, los jugadores del bar no tienen una estrategia dominante, que prefieren en cualquier escenario, sino que se encuentran con que sus mejores opciones son contingentes, lo que les atrapa en el razonamiento circular de arriba. Ese tipo de circularidad es característica de las situaciones sociales como la del bar. De hecho, fue un serio obstáculo para el avance de la teoría de juegos en sus inicios.

Sin solución de estrategias dominantes, el análisis de la situación del bar requiere de nuevas ideas. Fue un logro de la teoría de juegos establecer una previsión de equilibrio para asuntos como el del bar, cuya solución se puede intuir observando lo que sucede cada fin de semana en muchos locales: uno de los chicos va por la rubia y el resto va por morenas. La lógica de la solución es más sutil que la prominente de las estrategias dominantes. Ese equilibrio acopla simultáneamente la conducta racional de todos los participantes, en el sentido de que nadie querrá cambiar su estrategia unilateralmente porque empeorarán su situación si lo hacen. Es decir, todos los jugadores están lo mejor que pueden –resolviendo a la vez correctamente su problema de elección óptima– dado lo que hacen los demás. Es difícil argumentar que jugadores racionales en situaciones sociales complejas, como la del bar, muevan de otra manera. Ese concepto de solución –acompañado del teorema que garantiza que siempre tiene sentido en situaciones como la del bar le consiguió a Nash el Premio Nobel de Economía en 1994 [5].

[6] Si, gracias a los fondos recaudados, la Wikipedia no se inunda de anunciantes no es necesariamente porque los muchos donantes no razonen eficientemente, sino porque –de momento– sus decisiones no toman sólo en cuenta el dinero gastado, sino además otros valores.

[7] La discusión de esta sección sigue en buena parte el modelo en [7]. La descripción de la situación en el bar y de sus posibles desenlaces corresponden específicamente a los que se explican a una escena de la película "Una mente maravillosa" (Ron Howard, 2001) protagonizada por Russell Crowe en el papel del matemático norteamericano John Nash.

El premio al trabajo de Nash –menos de una página en la prestigiosa revista que lo publicó [4] fue el primero concedido a un resultado puramente matemático en noventa y tres años de historia del Nobel. Una breve introducción a la trascendencia de la idea de Nash y los problemas iniciales de la teoría de juegos se puede ver en [8].

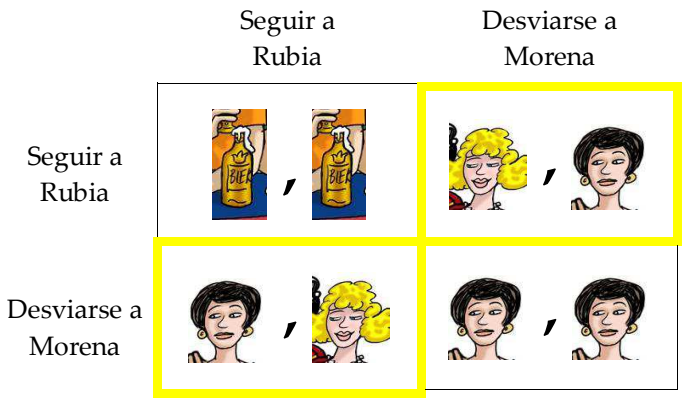
La solución previsible -"roja"– que proporciona el equilibrio de Nash para los chicos del bar también es de color verde, como la solución coordinada en el dilema del prisionero. La eficiencia social consiste aquí en que, en el *statu quo* del equilibrio, no se puede mejorar la situación de ninguno de los chicos si no es a costa de empeorar la de otro. En el dilema del prisionero, la solución verde cumple esa propiedad. Esa es la noción de eficiencia en el sentido de Pareto, que se usa como test básico de bienestar social en economía (ver e.g. [10]).

La situación del bar no plantea la tensión entre lo previsto y lo deseado del dilema del prisionero. La solución "uno va por la rubia y los demás por morenas" es roja y verde a la vez –amarilla, entonces. La situación no parece producir ningún síndrome, al menos similar al de los prisioneros del dilema. Sin embargo, hay una cuestión… ¿quién va entonces por la rubia? Existen demasiadas soluciones amarillas, tantas como chicos en el grupo. El dilema asoma porque los chicos deben coordinarse para seleccionar una. Esto es muy fácil si hay un gallo que destaca en el gallinero, un "George Clooney" entre los chicos de la pandilla. Espontáneamente, sin acuerdo expreso, todos se moverán sabiendo que será George quien se empareje con la rubia. Esos equilibrios que emergen espontáneamente se llaman *puntos focales* o de Schelling (ver e.g. [1]). En esas situaciones, en efecto, no hay síndrome:

Pero cuando no sobresale ningún gallo en el gallinero, se produce una situación delicada. Si sólo hay "pollos" en el bar –o si todos son gallos– , no hay modo de seleccionar una de las soluciones amarillas. Si todos los pollos de la pandilla se ven iguales, es difícil coordinar un equilibrio. El arreglo razonable es acordar la mejor solución simétrica: "todos por morenas". Pero esa solución no es equilibrio de Nash: cada uno, que va a lo suyo, intentará mejorar yendo a por la rubia.

Como todos razonarán así, acabarán solos en la situación pésima. Los chicos entonces desearían una solución amarilla –mejoran todos en cualquiera de ellas– pero parecerá inalcanzable.

La referencia al gallinero es más que metafórica: la situación del bar se puede ver como una versión para N jugadores de otro famoso juego social: el "gallina", que Bertrand Russell usó a mediados del siglo XX como metáfora de la tensión de los dos bloques en la guerra fría [9]. La versión popular del juego consiste en que dos conductores se dirigen en sus coches a la colisión frontal y deben optar por seguir o desviar su vehículo. El que se desvíe será el gallina mientras el otro ríe quedando por encima. Si ambos se desvían, hay tablas; y si ninguno lo hace sucede el desastre –¡crash!– que es el peor resultado para ambos. La situación del bar con dos jugadores puede representarse con la tabla de un gallina[8]:



[8] Los dibujos de la tabla son del autor italiano Gianni Peg.

En esta interpretación, los jugadores se dirigen –figuradamente– a colisionar en la rubia y deben decidir si siguen hacia la rubia o se desvían por una morena. Cada casilla muestra los acompañantes de los dos jugadores en los correspondientes desenlaces del juego. Las soluciones previsibles son los dos equilibrios de Nash asimétricos y eficientes en que uno va por la rubia y el otro por una morena, que evitan el resultado malo –tomar la bebida sólo en la barra. Corresponden a las casillas amarillas en la tabla. Sin Clooneys, existe riesgo importante de que el síndrome lleve al resultado malo, a pesar de que cualquier otro es mejor. Usando el gallina como parábola de la tensión nuclear, Russell alertaba de que es un juego "increíblemente peligroso" y culpaba a los líderes de países o bloques por participar en él para resolver sus diferencias: "Llegará un momento en que ninguno de los bandos podrá soportar que le griten con burla ¡Gallina! desde el otro. Entonces los dirigentes de los dos lados sumirán al mundo en la destrucción" [9].

En un gallina de muchos, en que ninguno destaca, la asimetría de las soluciones amarillas es insatisfactoria: se debe esperar que jugadores que no se distinguen actúen del mismo modo en equilibrio. El mecanismo que causa el síndrome del gallina es precisamente la necesidad de establecer una solución simétrica[9]. Cuando individuos similares juegan al gallina, es previsible que se produzca el peor resultado para todos.

Como el dilema del prisionero, el juego del gallina con muchos participantes similares sirve de paradigma de diversas situaciones sociales cotidianas que suelen presentan los síntomas del síndrome del gallinero. Por ejemplo, sucede a menudo en situaciones en que nadie se presta, entre un numeroso grupo, a una tarea que quedará finalmente sin hacer. Ese es el caso de que la rubia del bar se acabe quedando sola. O de que algunos correos electrónicos con una pregunta dirigida a todo un grupo se quede sin responder. O que nadie se detenga al ver un coche averiado en una carretera principal. Tales fenómenos ocurren sin que los implicados sean unos indolentes. Sucede entre personas preocupadas por el otro y dispuestas a prestarle ayuda, pero que preferirían que lo hiciera otro o están esperando que llegue el Clooney de turno. Sucede que sufren un síndrome social.

Referencias

[1] BINMORE, Kenneth, *Playing for Real*, Oxford University Press, 2007.

[2] COOMBS, Clide H. y AVRUNIN, George S., *Single peaked functions and the theory of preference*, Psychological Review **84**, pp. 216–230, 1977.

[3] FLOOD, Merril, *Some experimental games*, Research Memorandum RM-789,RAND Corporation, Santa Monica, CA, 1952.

[4] NASH, John F., *Equilibrium Points in N–Person Games*, Proceedings of the Nacional Academy of Sciences, USA, 36, pp. 48–49, 1950.

[5] NOBELPRIZE.ORG, *The Price in Economics 1994 – Press release*. http://nobelprize.org/nobel_prizes/economics/laureates/1994/press.html

[9] Otra posibilidad para determinar un equilibrio simétrico es considerar estrategias mixtas (ver e.g. [1]), en que los jugadores aleatorizan su decisión de ir o no por la rubia. Para ello es necesario cuantificar los resultados del juego. Por ejemplo, si en el flirteo del bar con dos jugadores, éstos valoran hablar con la rubia con 4 puntos, hablar con una morena con 1, y quedar solo en la barra con 0, la tabla del juego es

	Rubia	Morena
Rubia	0, 0	4, 1
Morena	1, 4	1, 1

En ese caso se demuestra que existe una solución simétrica que consiste en que cada jugador irá a por la rubia con probabilidad 0,75 y el resultado más probable es que los dos acaben solos en la barra.

[6] POUNDSTONE, William, *El dilema del prisionero*, Alianza Editorial, 1995.

[7] REY, José-Manuel, *If we all go for the blonde*, +Plus Magazine **47**, 2008. http://plus.maths.org/issue47/features/rey/index.html

[8] REY, José-Manuel, *La doble hélice de las ciencias sociales*, Matematicalia **7**(2), 2011.

[9] RUSSELL, Bertrand, *Common Sense and Nuclear Warfare*, George Allen & Unwin Ltd., 1959.

[10] SAMUELSON, Paul A. y NORDHAUS, William D., *Economía*, 10ª ed. McGraw Hill, 2002.

Sobre el autor:
Nombre: José Manuel Rey
Correo electrónico: j-man@ccee.ucm.es
Institución: Departamento de Análisis Económico, Universidad Complutense de Madrid.

Investigación

Matemáticas en la construcción de escalas musicales

Mathematics in the construction of musical scales

Marco Castrillón López

Revista de Investigación

Volumen III, Número 1, pp. 177–188, ISSN 2174-0410

Recepción: 1 Feb'13; Aceptación: 26 Mar'13

1 de abril de 2013

Resumen

En este trabajo se dan algunas notas matemáticas sobre la determinación de las notas de la escala y la noción de consonancia de notas simultáneas.

Palabras Clave: Consonancia, escalas musicales, suma de armónicos.

Abstract

This work presents some indications about the construction of the notes in the scale as well as some notions on the consonance of two notes played simultaneously.

Keywords: Consonance, musical scales, sum of harmonics.

1. Introducción

Un interesante experimento que puede realizar el lector en caso de poder contar con un piano (o un instrumento musical electrónico que emule un piano) y un nutrido grupo de oyentes voluntarios es el siguiente. Se pulsan simultáneamente las nota Do y Do# (de una misma escala, si puede ser la central del teclado) y a continuación se pulsan simultáneamente las notas Do y Sol (de nuevo, en la escala central). En ningún momento se dice qué notas se han tocado. La idea es realizar una sencilla votación en el público sobre la "consonancia" o "disonancia" de estos dos pares de notas. Si no se cuenta con un público de avanzada formación musical, cuyos conocimientos pueden influir a priori en su elección, el resultado suele ser el siguiente: la mayoría considera que el segundo par (el formado por Do+Sol) suena mejor que el primero (el Do+Do#). Hemos puesto anteriormente la palabra consonancia o disonancia entre comillas no porque no sean correctas (véase, por ejemplo, la definición de las mismas en un diccionario cualquiera) sino porque ellas son precisamente el objetivo de este pequeño trabajo. Más concretamente, en estas hojas se pretende dar una posible explicación matemática a la cualidad consonante de notas tocadas simultáneamente.

Las Matemáticas han sido, desde la Grecia antigua, lugar de paso indiscutible en la formalización de la Música. En particular, la escuela de Pitágoras de Samos fue el germen primordial en el que surgió la música occidental y cuya herencia sigue hoy en día de indudable relevancia.

Es cierto que el ser consonante o disonante comporta un indudable sentido subjetivo por parte del oyente. La Música, como buen arte, toca en lo profundo al espíritu humano y hace surgir de él sentimientos únicos e irrepetibles en cada uno de nosotros. Sin embargo, es cierto que la composición musical ha contado a lo largo de la historia con marcadas reglas de construcción, de las que las ideas de la escuela pitagórica contribuyó enormemente. Surge de forma natural las siguientes preguntas: ¿son las reglas meras convenciones? ¿qué nos pueden decir las Matemáticas al respecto? ¿hubiera sido nuestra música occidental diferente si nuestras raíces hubieran sido otras? No pretendemos dar respuestas a estas cuestiones. Eso sería demasiado ambicioso. Sin embargo, esperamos que el lector encuentre en las siguientes secciones algunas ideas que le sirvan para poder contemplarlas, al menos, desde otra perspectiva.

Figura 1. "Teorica Musice", cap. 8, Libro I, de Franchinus Gaffurius (Milán, 1492). La imagen mostrada es muy representativa del fuerte dogmatismo aritmético pitagórico presente aún en la música del siglo XV.

2. Nociones fundamentales

2.1. Las escalas musicales

Un sonido es una variación de la presión del aire perceptible por nuestro sentido auditivo. Atendiendo a la naturaleza de la ecuación de ondas que modeliza el comportamiento del fluido aéreo, esta función presión es localmente (tanto en sentido espacial como temporal) en buena medida periódica. En un desarrollo de Fourier, podemos por tanto realizar una descomposición de dicha onda en sus frecuencias elementales. De las cuatro características fundamentales del sonido, a saber, la intensidad, el timbre (asociado a los coeficientes de Fourier de la onda), la duración y la altura (frecuencia de la contribución de Fourier dominante), vamos a atender fundamentalmente a la última, es decir, vamos a trabajar con tonos. Los sonidos producidos

por los instrumentos musicales tiene una frecuencia fundamental (su timbre) muy definida. Más aun, algunos instrumentos y especialmente si trabajamos con instrumentos electrónicos, pueden producir sonidos sinusoidales prácticamente puros. Pensemos por un momento que trabajamos con estos sonidos puros.

Son pocos oídos afortunados los que pueden describir de forma exacta una frecuencia determinada. Sin embargo, sí es normal el poder distinguir, una vez que se tiene dos sonidos, cuál es más agudo (tiene un tono mayor) que el otro. Por ello, al hablarse de los tonos de un sonido, se suele hacer partiendo de una referencia. En la música occidental se suele escoger la frecuencia de 440 Hz (La) como frecuencia fundamental, aunque cualquier otra f_0 es igualmente válida. Igualmente, como se puede comprobar experimentalmente, a partir de una frecuencia aproximada de unos 500 Hz el oído aprecia las distancias entre dos tonos no por la diferencia de frecuencias sino por la razón entre las mismas (Ley de Weber-Fechner para el oído). Eso quiere decir que dentro del espectro auditivo humano (20 Hz - 20.000 Hz), la percepción de los tonos menores de 500 Hz es lineal, pero a partir de ahí es logarítmica. Así se habla de razones (o intervalos) de frecuencia como una aplicación del conjunto de frecuencias $\mathcal{F}$ del cual podemos olvidar en qué unidades se mide, a la semirecta real como

$$\begin{aligned} \mathcal{F} &\longrightarrow \mathbb{R}^+ \\ f &\mapsto \frac{f}{f_0}. \end{aligned} \tag{1}$$

Se dice que dos tonos f_1 y f_2 están separados una *octava* si $f_2 = 2f_1$. Los sonidos separados por una o varias octavas son percibidos por el oído humano como prácticamente indistinguibles si son escuchados simultáneamente. Por esta razón, la aplicación (1) se puede describir de forma más ajustada al oído humano como

$$\begin{aligned} \mathcal{F} &\longrightarrow \mathbb{R} \\ f &\mapsto \log_2 \frac{f}{f_0} \end{aligned}$$

que además podemos simplificar si consideramos la relación de equivalencia $\mathcal{R}$ "estar separado por una octava" de forma que la proyección al conjunto cociente es

$$\begin{aligned} \mathcal{F} &\longrightarrow \mathbb{R}/\mathbb{Z} \\ f &\mapsto \left(\log_2 \frac{f}{f_0} \right)_{\mathcal{R}} \end{aligned} \tag{2}$$

donde $(x)_{\mathcal{R}}$ es la clase de x. Si identificamos $\mathbb{R}/\mathbb{Z}$ con el intervalo $[0,1)$, entonces $(x)_{\mathcal{R}}$ no es más que $\{x\}$, es decir, tomar la parte fraccionaria de x. Si en cambio identificamos $\mathbb{R}/\mathbb{Z}$ con la circunferencia unidad S^1 de complejos unitarios, la aplicación queda por tanto definida como

$$\begin{aligned} \mathcal{F} &\longrightarrow S^1 \\ f &\mapsto \exp\left(i2\pi \left\{ \log_2 \frac{f}{f_0} \right\} \right), \end{aligned} \tag{3}$$

es decir, el análisis de tonos puede analizarse de forma geométrica como puntos de la circunferencia.

De los infinitos elementos de S^1 con las que un compositor puede trabajar a la hora de elegir los tonos que formen parte de su obra, se suele tomar tonos que formen parte de un subconjunto discreto (y por tanto finito) de S^1 elegido de antemano. Estos subconjuntos se denominan *escalas*, y el cómo elegirlos constituye toda una disciplina musical que ha vivido a lo largo de los siglos múltiples interpretaciones y teorías. Vamos, sin embargo, a centrarnos en la construcción de la escala de la escuela de Pitágoras. Si, como hemos dicho antes, las potencias de dos (las octavas)

definen sonidos de naturaleza similar, parece natural estudiar que sucede cuando se toman potencias del siguiente número natural, es decir, el tres. Así, partiendo de la nota fundamental f_0 que hayamos escogido, se toma el conjunto $(3^k f_0)_{k\in\mathbb{Z}}$. La imagen de estos puntos por medio de las aplicaciones (2) o (3) representan un conjunto denso de $[0,1)$ o S^1. Si consideramos las K primeras notas $\{\log_2 3^k\}$, $k=0,\dots,K-1$, partiendo de 0, dado que 2 y 3 son primos entre sí, nunca podremos volver a ese valor inicial. Sin embargo hay valores concretos de K para los que nos acercamos mucho a 0. Este es el caso de 3^7. En efecto, tenemos

$$\begin{array}{lll} \{\log_2(3^0)\}=0, & \{\log_2(3^1)\}=0'5949\dots, & \{\log_2(3^2)\}=0'1699\dots, \\ \{\log_2(3^3)\}=0'7649\dots, & \{\log_2(3^4)\}=0'3398\dots, & \{\log_2(3^5)\}=0'9248\dots, \\ \{\log_2(3^6)\}=0'5098\dots, & \{\log_2(3^7)\}=0'0947\dots, & \end{array}$$

en el que el último elemento dista menos de una décima del 0. Si ahora consideramos las primeras 7 notas y los ordenados de menor a mayor obtenemos los números

$$0 \quad 0'1699\dots \quad 0'3398\dots \quad 0'5098\dots \quad 0'5949\dots \quad 0'7649\dots \quad 0'9248\dots \tag{4}$$

que son las 7 notas de la escala pitagórica, inicialmente etiquetadas con letras del alfabeto griego. Nótese que el valor $\{\log_2(3^1)\}=0'5849\dots$ ocupa el quinto puesto en el reordenamiento dado en (4). Es por esta razón que la frecuencia asociada al número 3 con el que se ha construido esta escala es denominada *quinta* (o *quinta pitagórica*). Igualmente, el octavo valor de la escala corresponde (salvo la pequeña desviación comentada anteriormente y que se conoce como *coma pitagórica*) al 1 o 0 de $\mathbb{R}/\mathbb{Z}$ y que justifica que la potencia 2 se conozca como octava. Como nota histórica, hay que esperar hasta el siglo XI cuando, a partir de la música añadida por Guido de Arezzo a unos versos dedicados a San Juan Bautista, se asignó a las correspondientes notas la primera sílaba de dichos versos, a saber: *Ut, Re, Mi, Fa, Sol, La* y *Si*. La primera nota fue posteriormente cambiada a *Do*, apócope del *Dominus* latino.

2.2. El teorema de los tres pasos

Si inspeccionamos los valores de frecuencias ajustadas por los logaritmos dados en (4) podemos ver que las diferencias entre notas consecutivas (considerando la última diferencia con el valor 1) toman los valores

$$0 \quad 0'1699\dots \quad 0'1699\dots \quad 0'1699\dots \quad 0'0850\dots \quad 0'1699\dots \quad 0'1699\dots \quad 0'0850\dots$$

es decir, recordando que tomamos el tono inicial f_0 como el La (440 Hz), el intervalo entre dos notas consecutivas de la escala pitagórica toma un valor constante (un tono) salvo entre Si-Do y Mi-Fa en donde se tiene un valor distinto aproximadamente la mitad de un tono (y llamado hemitono). La existencia de dos tipos distintos de intervalos en la escala pitagórica es una propiedad esencial de la misma y es piedra angular de su riqueza musical. Sin embargo, al hilo de esta propiedad, cabe preguntarse si la elección de la quinta pitagórica ha sido determinante en la existencia de exactamente dos intervalos distintos. Esta cuestión está estrechamente relacionada con una conocida conjetura de Steinhaus (demostrada simultáneamente por Sós y Świerczkowski en 1958) que enunciamos a continuación (véase [7]).

Teorema 1 (de los tres pasos)**.** *Para cualquier $\theta\in\mathbb{R}^+$ y cualquier entero positivo K, la sucesión de puntos* $\exp(2\pi k\theta i)$, $k=0,\dots,K-1$, *divide la circunferencia unidad en subintervalos de, a lo sumo, tres longitudes distintas.*

En concreto, si $\theta=p/q$ es un número racional (escrito de forma irreducible) y $K\geq q$, tenemos exactamente un polígono regular y por tanto un único paso. Si θ es irracional, siempre habrá dos o más pasos. Ése es el caso de la escala pitagórica en donde $\theta=\log_2 3$. Para distinguir

cuándo se tienen dos o tres pasos distintos hay que recurrir a la teoría de números de la mano de las fracciones simples. Recordemos que todo número real (positivo) θ se puede escribir como

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

en donde los a_i, $i \geq 1$ son enteros positivos. La secuencia $[a_0; a_1 a_2 a_3 \ldots]$ acaba con una división exacta únicamente si θ es racional. En caso contraro, la secuencia de θ es infinita y única. Se denomina *convergente* de θ al número racional que se obtiene truncando su desarrollo en fracciones contínuas simples $[a_0; a_1 a_2 \ldots a_r]$ en cualquier orden r. Se denomina *semiconvergente* a la fracción $[a_0; a_1 a_2 \ldots n]$, $0 < n < a_r$ (si $a_r \geq 2$). Los convergentes y semiconvergentes gozan de propiedades muy interesantes. Referimos al clásico manual [3] para estas y otras muchas propiedades.

En relación con las escalas, tenemos el siguiente resultado.

Teorema 2. *Dado un número θ irracional positivo, la sucesión de puntos de la circunferencia* $\exp(2\pi k\theta i)$, $k = 0, \ldots, K-1$, *divide a la misma en arcos de exactamente dos longitudes distintas si y sólo si K es el denominador de un convergente o de un semiconvergente de θ.*

Por ejemplo, para $\theta = \log_2 3 = [1; 1, 1, 2, 2 \ldots]$, el denominador del semiconvergente $[1; 1, 1, 2, 1]$ es precisamente 7, lo que nos da la escala pitagórica construida anteriormente.

2.3. Los instrumentos musicales

Consideremos una cuerda tensa de longitud L, densidad lineal λ y tensión (es decir, la fuerza que tira de la cuerda en cualquiera de sus extremos fijos) de valor T. Supongamos que la cuerda es considerada infinitesimalmente delgada, de tal manera que pueda ser modelizada como un segmento al cual se le aplica la ecuación de ondas unidimensional. Se puede probar entonces que la cuerda en vibración tiene una frecuencia fundamental de valor

$$f_1 = \frac{1}{2L}\sqrt{\frac{T}{\lambda}} \tag{5}$$

que es acompañada por todos sus múltiplos $f_n = nf_1$, $n \in \mathbb{N}$. Estos valores f_n son conocidos como *armónicos* de la vibración de la cuerda y simplemente quieren decir que cualquier estado vibracional de la misma se puede escribir como suma infinita de vibraciones sinusoidales de frecuencia f_n, $n \in \mathbb{N}$. Aunque con la técnica adecuada puede conseguirse que, cuando se pulsa una cuerda de un instrumento, la misma vibre predominantemente con una frecuencia f_2 o f_3, lo general es que al tocar un instrumento de cuerda, el sonido predominante de cada cuerda sea el asociado a la vibración fundamental f_1. Sin embargo, dicho sonido contendrá contribuciones de los armónicos superiores f_n, $n > 1$, cuya aportación determina el timbre del instrumento. Como primera aproximación, se puede considerar que la intensidad de cada aportación f_n, $n > 1$, decrece geométricamente por un factor 0'7 a medida que crece n.

En el caso de una columna hueca de longitud L con un gas (ideal) en su interior, el sonido producido por la vibración de dicho gas tiene un comportamiento muy parecido. Se cuenta con una frecuencia fundamental

$$f_1 = \frac{c}{2L}, \tag{6}$$

siendo c la velocidad del sonido en ese gas, que es acompañada por sus múltiplos $f_n = nf_1$, $n > 1$, presentes en la descomposición de cualquier sonido.

Como se ve, el comportamiento de los instrumentos de cuerda y viento es a grandes rasgos bastante similar. Sin embargo la familia de percusión tiene características diferentes. Se puede

acudir a monografías de organología o de acústica musical para analizar más detalladamente el complejo análisis del tambor, la campana o el xilófono. Por ejemplo, la vibración de un paralelepípedo sólido (en particular, las láminas de un xilófono sencillo) contiene una frecuencia fundamental f_1 y los siguientes primeros armónicos

$$f_2 \simeq 2,75 f_1, \quad f_3 \simeq 5,40 f_1, \quad f_4 \simeq 8,93 f_1, \quad f_5 \simeq 13,34 f_1, \dots \tag{7}$$

El lector interesado puede encontrará un excelente manual sobre la física de los instrumentos musicales en [5].

2.4. El oído humano

La audición, aunque fue uno de los primeros sentidos en ser entendido en profundidad, no es en absoluto sencillo. No se pretende entrar aquí en detalles especializados, aunque sí es interesante ver cómo opera el oído interno al enfrentarse con un estímulo complejo compuesto de varios sonidos de frecuencias distintas.

Las vibraciones moduladas por los huesecillos del oído interno, llegan por medio de estribo a la hacer vibrar el líquido que baña el interior del caracol. Podemos ver el caracol como un tubo de tres pisos enrollado sobre sí mismo. En el piso central se encuentra el llamado órgano de Corti, verdadero aparato sensor auditivo, formado células ciliadas sensibles al movimiento del líquido que les rodea. La perturbación producida por el estribo viaja por el conducto superior y se ve forzado, debido a la forma curvada del caracol a traspasar el piso central y llegar así al piso inferior. Este "cambio de piso" estimula a algunas células ciliadas que, a su vez, están comunicadas con el cerebro. Sin embargo, cada frecuencia realiza este estímulo en un sitio determinado de la longitud del caracol. Es decir, el oído interno realiza una descomposición en frecuencias elementales dentro del espectro auditivo del mismo. A "grosso modo", el caracol es capaz de realizar una análisis de Fourier del estímulo auditivo que recibe. Por tanto, nuestra percepción auditiva es sensible al espectro de frecuencias de los sonidos que recibe como, por ejemplo, el espectro de un sonido musical de los estudiados en el epígrafe anterior.

3. Algunas pinceladas históricas de la consonancia musical

Es ingente la cantidad de trabajos y teorías alrededor de la armonía y la consonancia musical. Damos a continuación tres brevísimas pinceladas de algunos momentos de relevancia en dicho desarrollo desde un punto de vista matemático.

La construcción de la escala de 7 notas a partir de la tercera pitagórica forma parte de una entera concepción musical basada en los números naturales. La escuela de Pitágoras concedía al *número* un valor de marcado carácter ontológico en el cosmos. El número, como origen de toda explicación del mundo, era también la pieza fundamental de la perfecta composición musical y de las reglas que determinan el carácter consonante y disonante de varios sonidos coincidentes. Si bien se exploraban todas las familias de instrumentos, la tradición pitagórica escribía sus conclusiones generalmente por medio de experimentos de instrumentos de cuerda y de viento. Así, con dos cuerdas tensas de la misma tensión, la ley pitagórica de los números sencillos afirma que el sonido simultáneo de ambas resulta agradable (consonante) si las longitudes de las cuerdas están relacionadas por números naturales pequeños. Por ejemplo, una cuerda de longitud L y otra de longitud $L' = L/2$ suenan perfectamente consonantes. En efecto, las frecuencias fundamentales (véase (5)) son una el doble de la otra, es decir, el intervalo definido por ambas frecuencias es exactamente una octava. Si $L' = 2L/3$ o $L' = L/3$ estamos tratando con sonidos separados por una quinta o por una quinta más una octava. En el caso $L' = 3L/4$ tenemos la llamada *cuarta* (un intervalo de cuatro notas). Heredera de la cultura helénica, en la

música occidental medieval (en particular, en la polifonía inicial, aproximadamente entre el 900 y el 1.300 d.C.) se consideraban consonantes únicamente los intervalos octava (2:1), quinta (3:2), cuarta (4:3), octava más quinta (3:1), octava más cuarta (8:3) y doble octava (4:1). Este conjunto de consonancias es aumentado con las terceras (4:5) y las sextas (3:5) en el contrapunto.

Galileo y Mersenne dan un primer avance matemático a la relación entre frecuencias, consonancia y la ley de los números pequeños de Pitágoras. En concreto Galileo afirma, dentro de su concepción matematizante de la Naturaleza, que si dos notas tienen sus frecuencias relacionadas por un entero pequeño, la onda resultante presentará una regularidad o simetría no presente para otras razones más complejas y tendrá, por tanto, más armonía. Es sin embargo Rameau quien primero pensó en la escala musical a partir de consideraciones vibracionales.

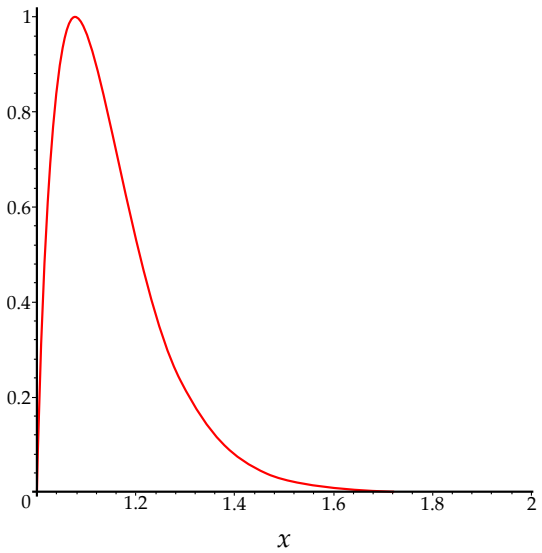
De cualquier manera hay que esperar al descubrimiento de la estructura de los armónicos (5) y (6) para poder elaborar teorías más elaboradas. En el siglo XIX, Helmholtz explota esa idea en dos direcciones. Primeramente, partiendo de la identidad trigonométrica

$$\operatorname{sen} f_1 + \operatorname{sen} f_2 = 2 \operatorname{sen} \left(\frac{f_1 + f_2}{2} \right) \cos \left(\frac{f_1 - f_2}{2} \right),$$

tenemos que el sonido resultante de la suma de dos frecuencias f_1 y f_2 tiene dos comportamientos periódicos acoplados, con frecuencias respecticas la semisuma y la semidiferencia de f_1 y f_2. Si nos centramos en la segunda, y atendiendo a la sensación del oído humano, ésta provoca unos pulsos lentos cuando f_1 o f_2 son próximos. Helmoltz afirmaba que alrededor de una diferencia de 30 ó 40 Hz se tenía la máxima sensación de desasosiego. A partir de ahí, esta sensación desaparece y se recupera la consonancia. En segundo lugar, Helmholtz aplicaba esta idea a las relaciones entre los distintos armónicos del instrumento con el que se tocase las correspondientes notas. De esta manera Helmholtz trazó unas curvas de "aspereza" que presenta unos mínimos precisamente en las notas construídas de la forma pitagórica.

4. La teoría de Plomp y Levelt

Parece ser que fueron los americanos Plomp y Levelt (véase [4]) quienes elaboraron el primer análisis experimental de consonancia y disonancia de ondas sinusoidales puras. A los sujetos del experimento se les hacía oir sonidos puros a distintas relaciones de frecuencias quienes tenían que además valorar el grado de consonancia y disonancia. Los datos así obtenidos promediados proporcionaron una curva similar a la siguiente



en donde el eje de ordenadas va de 0 (consonancia total) a 1 (disonancia total) y el de abscisas parametriza la razón entre las frecuencias f y f' confrontadas, es decir $f' = xf$. Esta aportación está relacionada con la idea de *banda crítica*, es decir la mínima banda de frecuencias alrededor de una frecuencia determinada que activan la misma zona de la membrana basilar en el caracol del oído. Podemos dar varias funciones que definan una gráfica con un perfil similar al anterior. Por ejemplo, en [1] se opta por la función

$$d(x) = a\,|x|\,e^{1-b|x|}, \tag{8}$$

en donde a, b son constantes a ajustar y además asumimos un rango de frecuencias superior a 500 Hz para poder aplicar las relaciones de frecuencias por razones y no por diferencias. En el caso de trabajarse en un rango de frecuencias bajo, la función sería similar, pero la variable x asumiría el papel de diferencia de notas confrontadas. En el caso de Sethares (véase [6])) la función es

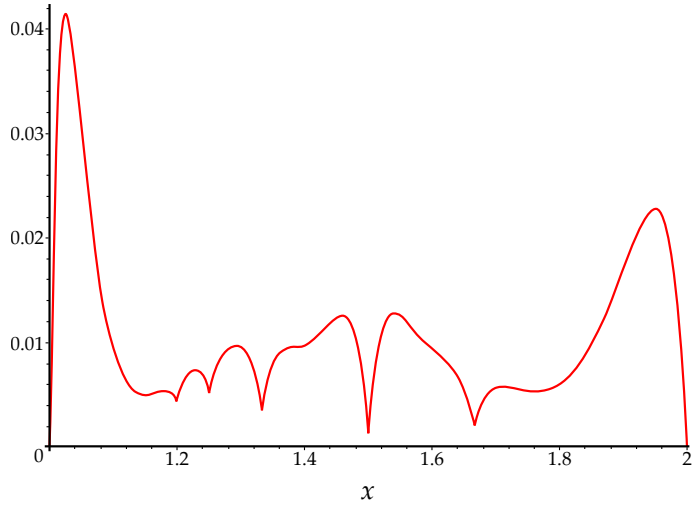
$$d(x) = e^{-ax} - e^{-bx},$$

de nuevo a, b son constantes a ajustar empíricamente.

De cualquier manera, como se puede ver, en esta curva no hay vestigio de las consonancias o disonancias de la construcción pitagórica. Parece que el oído humano (principalmente por el tipo de análisis de Fourier que elabora el órgano de Corti en el caracol), experimenta una sensación desagradable a cierto rango de frecuencias cercanas, mientras que fuera de ese rango (fuera ya de la banda crítica), cualquier par de frecuencias suena "bien". Sin embargo, los instrumentos emiten sonidos compuestos por armónicos, tal y como vimos en §2.3. En la línea sugerida por Hemlholtz, el trabajo de Plomp y Levelt analizó además el grado de consonancia o disonancia total de dos notas de un instrumento de viento o de cuerda sumando el valor de la función $D(x)$ en distintos armónicos de los sonidos confrontados. Es decir, se considera la función

$$D(x) = \sum_{n,n'=1}^{\infty} \nu_n \nu_{n'} d\left(\frac{n}{n'}x\right)$$

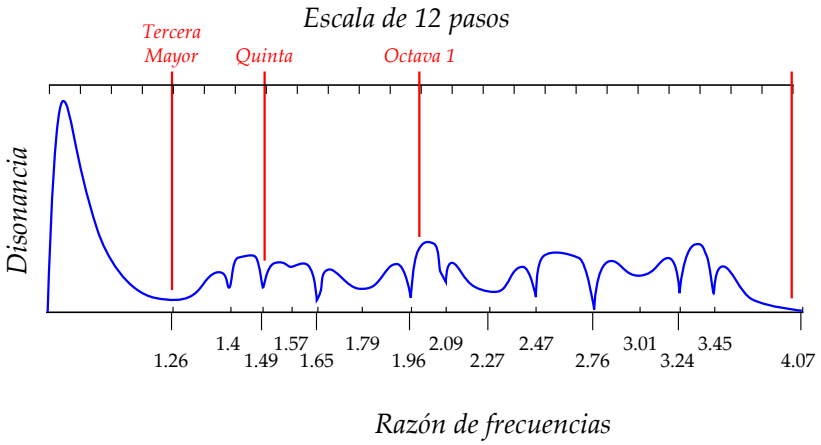
que estudia la disonancia de dos notas de frecuencias f_0 y $f = xf_0$, junto con todos sus armónicos, en donde ν_n es la amplitud (relativa) del n-ésimo armónico. Por simplicidad se puede limitar la suma a los primeros 6 armónicos y considerar, como se comentó en §2.3, que la intensidad relativa es $\rho_n = 0'7^n$, por lo que aproximadamente $\nu_n = 0'84^n$, para todo n. En ese caso se obtiene la gráfica



En ella observamos: que la consonancia es máxima (la gráfica tiene mínimo absoluto) para $x = 2$, es decir, notas separadas una octava. El siguiente valor de consonancia máxima (el

siguiente mínimo de la gráfica) se da para $x = 3/2$, es decir, para una quinta pitagórica. Los siguientes mínimos locales (ordenados de mayor a menor consosnancia) están ubicados en los valores $x = 4/3$ (una cuarta), $x = 5/4$ (una tercera mayor), $x = 6/5$ (tercera menor) y $x = 5/3$ (una sexta). Se recuperan los valores clásicos de la consonancia polifónica.

Imaginemos ahora, por ejemplo, que se trabaja con un xilófono simple. Si repetimos el mismo proceso, pero con las frecuencias dadas en (7), entonces la curva presenta una distribución de mínimos distinta a la de Plomp y Levelt como se ve a continuación (en una imagen de [6] cedida por el autor).



En este punto es interesante preguntarse como sería la musica occidental hoy en día si Pitágoras hubiera estado sumergido en una cultura de percusión en vez del sustrato de mediterráneo de cuerda y viento en el que vivió.

El espectacular desarrollo de la música electrónica en el segundo tercio del siglo XX permitió realizar interesantes construcciones a partir de estas ideas. En particular, con un sintetizador, se puede emitir sonidos formados por una frecuencia fundamental y una distribución de armónicos f_n de valores arbitrarios. De esa manera, el compositor puede tener control de los valores para los que se tiene los intervalos de máxima consonancia. Por ejemplo, si se construye un sonido de armónicos

$$f_2 = 2^{5/4} f_1, \quad f_3 = 2^{8/4} f_1, \quad f_4 = 2^{10/4} f_1, \quad f_5 = 2^{11/4} f_1, \quad f_6 = 2^{12/4} f_1,$$

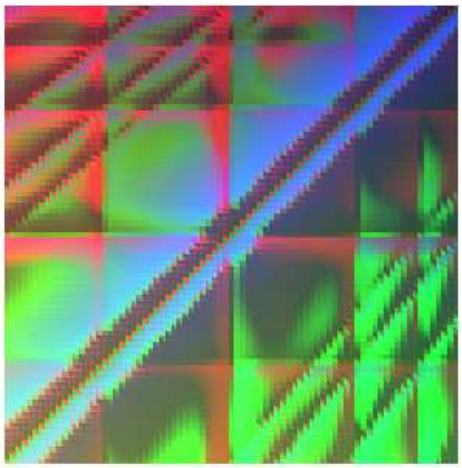
(construcción de Pierce, 1966) se tiene una gráfica de consonancia de tal manera que cualquier par de notas de la escala de temperamento igual (equiespaciadas en la circunferencia) suenen consonantes. En efecto, cuando dos notas de esta escala suenan con los anteriores armónicos, lo que sucede es que estos armónicos o bien coinciden o bien están separados lo suficientemente en la banda crítica. Ésta y otras mucha otras construcciones han permitido crear una nueva concepción de la composición musical dotada de un notable peso matemático (*xentonalidad*, *xenomúsica* y muchas otras). Para algunas reflexiones, véase [2] y [6].

5. Consonancia de tres notas

Para terminar, vamos a generalizar la construcción de Plomp y Levelt para el caso en el que se confrontan tres notas de instrumento de cuerda (o de viento) simultáneamente. Utilizando de nuevo la función $d(x)$ dada en (8) se considera la función de dos variables

$$D(x,y) = \sum_{n_1,n_2,n_3=1}^{\infty} \left(\nu_{n_1}\nu_{n_2} d\left(\frac{n_2 x}{n_1}\right) + \nu_{n_1}\nu_{n_3} d\left(\frac{n_3 y}{n_1}\right) + \nu_{n_2}\nu_{n_3} d\left(\frac{n_2 x}{n_3 y}\right) \right),$$

en donde se confronta una nota fija f_1 con las notas $f_2 = xf_1$ y $f_3 = yf_1$, con $x > 0$, $y > 0$. De nuevo ν_{n_i} es la amplitud relativa del n_i-armónico de f_i y que por comodidad consideramos igual a $0'84^{n_i}$. Con un programa de cálculo científico se puede obtener la gráfica de dicha función, en donde la perspectiva se ha elegido de forma vertical, es decir, se observa la gráfica desde el eje Z en proyección ortogonal sobre la región $[1,2] \times [1,2]$ del plano XY. Los efectos de sobra ayudan además a percibir mejor los mínimos de la misma:



Se observa lo siguiente. Por una parte la gráfica es obviamente simétrica respecto de la recta $x = y$ por lo que podemos restringirnos al caso $x > y$. Además, la información de la gráfica sobre los bordes no es relevante, pues en los mismos dos de las tres notas son iguales por lo que no se estudia una verdadera confrontación de tres tonalidades diferentes. La gráfica tiene líneas de mínimos uniendo valores de la escala pitagórica ubicados en el segmento $[1,2]$ de la X y de la Y. En particular, son especialmente notables los siguientes mínimos: El obtenido al cruzar las líneas $x = 3/2$, $y = 5/4$, es decir, el punto que corresponde con la relación $(1 : 5/4 : 3/2)$ que es exactamente el acorde mayor pitagórico (por ejemplo, el acorde de Do mayor Do+Mi+Sol). Y el obtenido al cruzar las líneas $x = 5/3$, $y = 5/4$, es decir, el punto que corresponde con la relación $(1 : 5/4 : 5/3)$ que es exactamente el acorde menor pitagórico (por ejemplo, el acorde de La menor La+Do+Mi).

Referencias

[1] BENSON, D.J., *Music: A Mathematical Offering*, Cambridge University Press, 2006.

[2] HUTCHINSON, W., KNOPOFF, L., *The acoustic component of western consonance*, Interface **7** (1978), 1–29.

[3] KHINCHIN A.Y., *Contiuned Franctions*, Phoenix Books. University of Chicago Press, 1964.

[4] PLOMP, R., LEVELT, W., *Tonal consonance and critical bandwith*, J. Acoustic Soc. Amer. **38**, 1965.

[5] ROSSING, T.D., MOORE, R.F., WHEELER, P.A., *The scienc of sound*, Addison-Wesly, 2002.

[6] SETHARES, W., *Tuning, Timbre, Spectrum, Scale*, Springer Verlag, 2004.

[7] SLATER, N.B., *Gaps and steps for the sequence Nr* mod 1, Proc. Camb. Phil Soc. **63**, 1967, 1115–1123.

Sobre el autor:
Nombre: Marco Castrillón López
Correo Electrónico: mcastri@mat.ucm.es
Institución: ICMAT(CSIC-UAM-UC3M-UCM). Departamento de Geometría y Topología. Facultad de CC. Matemáticas. Universidad Complutense de Madrid, 28040, Madrid, España.

Juegos Matemáticos

Un juego competitivo basado en un problema matemático

A competitive game based in a mathematical problem

Javier Rodrigo Hitos

Revista de Investigación

Volumen III, Número 1, pp. 189–194, ISSN 2174-0410
Recepción: 28 Feb'13; Aceptación: 20 Mar'13

1 de abril de 2013

Resumen

En este artículo se presenta un problema propuesto en la competición matemática IMC como ejemplo de reto matemático combinado con un juego competitivo entre dos agentes.

Palabras Clave: Olimpiada matemática, teoría de Juegos, estrategias ganadoras.

Abstract

In this paper a proposed problem for the mathematical competition IMC is presented. This problem can be seen as a mathematical challenge but also as an example of a two player game.

Keywords: Mathematic competition, game theory, winning strategies.

1. Introducción

Los juegos matemáticos suelen ser retos que se proponen para que cada persona demuestre su pericia resolviéndolos de forma individual. Pero también se puede considerar como un juego matemático aquél en el que una persona tiene que derrotar a otra utilizando sus conocimientos matemáticos y su capacidad deductiva, en lo que sería un juego competitivo.

En este artículo se presenta un ejemplo de este segundo tipo de juego, que se propuso precisamente en otro tipo de competición: una olimpiada internacional de matemáticas, que puede ser considerada como una mezcla de los dos tipos de juegos planteados anteriormente: cada participante se enfrenta de forma individual con los problemas que se le proponen, pero

compite a su vez con los otros participantes por medio de un ranking según la puntuación que obtenga en dichos problemas.

La estructura del artículo es la siguiente: en la sección 2 se hace una breve introducción a la teoría de juegos (ver [1] y [2] para más información), en la sección 3 se introduce la competición matemática IMC, de la que se tomó el juego, y en la sección 4 se da el enunciado de dicho juego y su solución.

2. La teoría de juegos

La teoría de juegos estudia los procesos que se dan cuando dos ó más agentes compiten entre sí buscando maximizar su ganancia ó derrotar a los otros jugadores. Analiza entonces las estrategias de cada jugador para ganar y las situaciones de estabilidad, como las posiciones de equilibrio de Nash.

En definitiva, la teoría de juegos tiene como finalidad el modelar matemáticamente el proceso de decidir, la estrategia en la toma de decisiones.

Existen diferentes clasificaciones de los tipos de juegos que estudia esta disciplina. Algunas de ellas son:

- Juegos no cooperativos y cooperativos.

En los juegos no cooperativos, los jugadores compiten individualmente buscando

optimizar su beneficio, en los cooperativos los jugadores establecen alianzas buscando optimizar el bien común.

En el caso de la competición política, que se puede interpretar como un juego en el que los

agentes buscan la máxima ganancia en votos, se puede decir que los partidos políticos cooperan por medio de coaliciones.

- Juegos simultáneos y secuenciales.

En los juegos simultáneos, los jugadores hacen sus movimientos a la vez. En los juegos secuenciales, uno de los jugadores mueve primero y el otro después respondiendo a la acción del primer jugador, y así sucesivamente. El concepto de estabilidad que se estudia en este tipo de juegos es el equilibrio de Stackelberg.

Un ejemplo "deportivo" de juego simultáneo sería el fútbol, donde los equipos actúan a la vez en el campo de juego, peleando por una bola. Ejemplos de juegos secuenciales podría ser el tenis ó el ajedrez, donde un jugador inicia el juego, el otro responde, el primero sigue, y así hasta el final.

Aunque en estos dos juegos el empezar da ventaja, ya que se lleva la iniciativa, no en todos los juegos secuenciales tiene ventaja el que empieza: a veces es más provechoso actuar en segundo lugar, ya que tienes información sobre el movimiento del otro jugador, lo que te puede servir para preparar tu estrategia.

El juego que se presenta en este artículo es un ejemplo de juego secuencial en que tiene ventaja el segundo jugador. De hecho, éste tiene siempre una estrategia ganadora,

independientemente de las acciones que tome el primer jugador. Antes de verlo, introduzcamos la competición matemática en que se propuso.

3. La Olimpiada matemática IMC

La IMC (International Mathematics Competition) es un concurso matemático a nivel universitario en el que participan estudiantes de todo el mundo. En el año 2012 se celebró la 19 edición, que congregó a unas 200 instituciones universitarias de 44 países.

Esta 19 edición tuvo lugar en Blagoevgrad (Bulgaria), sede más habitual de las anteriores ediciones. En todo caso, la competición siempre se lleva a cabo en algún país de Europa del Este, siendo los estudiantes de esta zona los habituales dominadores de la competición.

Aunque los estudiantes representan a sus Universidades compiten de manera individual, por medio de dos exámenes de cinco horas y cinco problemas cada uno que tienen lugar los dos primeros días de competición.

Los problemas suelen estar relacionados con temas de Álgebra, Análisis y Combinatoria, aunque en esta edición por primera vez se plantearon problemas que tenían que ver con la Teoría de Juegos: El tercero del primer día (nivel intermedio) y el primero del segundo día (nivel "bajo"), que es el que analizamos en la siguiente sección.

4. El juego y su solución

4.1. Enunciado del problema

El enunciado del primer problema del examen del segundo día es el siguiente.

Considera un polinomio $f(x)=x^{2012}+a_{2011}x^{2011}+\ldots+a_1\,x+a_0$

Albert Einstein y Homer Simpson juegan el siguiente juego: Por turnos eligen uno de los coeficientes $a_{2011},\ldots,a_0$ y le asignan un número real, no pudiendo repetir coeficientes.

Empieza el juego Albert y el juego termina cuando se ha asignado valores a todos los coeficientes.

El objetivo de Homer es hacer que $f(x)$ sea divisible por un polinomio $m(x)$ dado, y el de Albert evitarlo.

a) ¿Cuál de los dos jugadores tiene una estrategia ganadora si $m(x)=x-2012$?

b) ¿Cuál de los dos jugadores tiene una estrategia ganadora si $m(x)=x^2+1$?

Vamos a ver que en los dos casos Homer tiene una estrategia ganadora. Por tanto, si Homer deduce esa estrategia (ó si alguien se la apunta) y la sigue ganará a Albert Einstein, haga lo que haga éste, a pesar de sus diferentes inteligencias.

Antes de ver estas estrategias, comentemos que es una broma habitual en este tipo de competiciones matemáticas el introducir el año en curso como dato. Esto hace que el dato sea lo suficientemente grande para que no se pueda resolver el problema por el método de

ensayo-error, pero hay que notar que en este caso el problema sería esencialmente el mismo si el grado del polinomio fuera un número genérico *n*, con *n* par.

4.2. Solución al problema

Vemos la solución de los dos apartados:

a) En este caso, al ser *m* un polinomio de grado 1, dividirá a *f* si 2012, la raíz de *m*, es raíz también de aquel polinomio. Entonces da igual lo que hagan en los primeros movimientos, lo que tiene que hacer Homer para cerrar el juego es elegir el coeficiente que queda, supongamos sin perdida de generalidad que es a_0, para que se cumpla que 2012 es raíz de *f*, es decir, que $f(2012)=0$. Para ello tiene que resolver una ecuación de primer grado en a_0, lo que determina el valor que tiene que jugar. Hay que notar que Homer termina el juego en los dos apartados, al ser el número de coeficientes par y empezar a jugar Albert.

b) Este caso es más difícil, al ser *m* un polinomio de grado 2, de raíces no reales $\pm i$, siendo *i* la unidad imaginaria. También se cumplirá que *m* divide a *f* si *i* es raíz de *f*.

La dificultad estriba en que al evaluar $f(i)$ da un número no real, por lo que Homer debe procurar que se anulen sus partes real e imaginaria.

Una estrategia a seguir entonces es la siguiente: elegir siempre un coeficiente de distinta paridad a la del coeficiente elegido por Albert. Es decir, si Albert elige un coeficiente de índice par, Homer ha de elegir uno de índice impar. Así se asegura que cuando vaya a hacer su penúltimo movimiento, queda algún coeficiente par (que, al sustituir *x* por *i*, va a estar en la parte real) y alguno impar (que estará en la parte imaginaria). Si, por ejemplo, Albert ha elegido uno con índice impar en su penúltima jugada, quedarán un coeficiente par, digamos que a_0 y dos impares disponibles para Homer en su penúltimo movimiento, por lo que tendrá que elegir a_0 para anular la parte real de $f(i)$ en ese penúltimo movimiento, resolviendo una ecuación de primer grado como en el apartado a. Entonces no importa la última elección de Albert, ya que Homer tendrá que elegir el coeficiente impar que queda, supongamos que a_1, para anular la parte imaginaria de $f(i)$ y ganar la partida.

Observemos finalmente que la estrategia ganadora que se presenta en la solución oficial al apartado b (ver [3]), es curiosamente la opuesta a la planteada aquí: elegir siempre un coeficiente de la misma paridad que el elegido por Albert. Aunque las dos ganan, hay que decir que la elegida en este artículo es más general, ya que vale para cualquier polinomio *f* de grado par, mientras que la estrategia dada en la solución oficial sólo vale para polinomios cuyo grado es múltiplo de cuatro.

Referencias

[1] VON NEUMANN, John, MORGENSTERN, Oskar. *Theory of Games and Economic Behavior*, páginas específicas consultadas, Princeton University Press, New Jersey, 2004.

[2] ROEMER, John. *Political Competition*, Harvard University Press, Boston, 2001.

[3] *Página web de la IMC*, http://www.imc-math.org.uk/

Sobre el autor:
Nombre: Javier Rodrigo Hitos
Correo Electrónico: jrodrigo@upcomillas.es
Institución: Universidad Pontificia Comillas, Madrid, España.

Críticas

πoetas, poesía con matemáticas

πoetas, poetry with mathematics

Jesús Malia

Revista de Investigación

Volumen III, Número 1, pp. 195–198, ISSN 2174-0410

Recepción: 4 Sep'12; Aceptación: 20 Mar'13

1 de abril de 2013

Resumen

En *πoetas* se repasan las relaciones que se han dado en la historia entre matemáticas y poesía y se recoge la obra de autores vivos y en español que siguen y acrecen esa tradición.

Palabras Clave: Poesía, matemáticas.

Abstract

πoetas reviews the relationships that have occurred in the history between mathematics and poetry and collects the works of living authors and in Spanish that follow and grow that tradition.

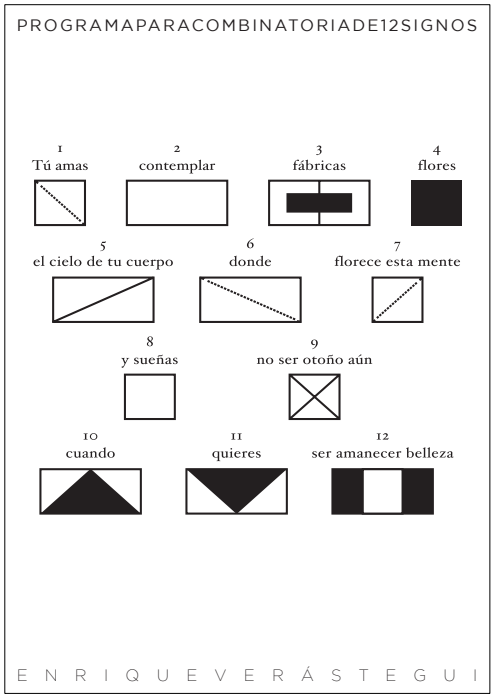
Keywords: Poetry, mathematics.

πoetas, primera antología de poesía con matemáticas

Enfrentar, en un espacio reservado para la crítica, la tarea de hablarles de mi propio libro (*πoetas, primera antología de poesía con matemáticas*, Amargord, 2012), reconozco que me pone en una situación problemática. Pero soy matemático y he de confesarles que agradezco los problemas. En cualquier caso, no sé si soy la persona adecuada para señalar críticamente los logros de mi antología, pues cuando hablo de ella ¿lo hago sobre hechos objetivos por todos observables o sobre los objetos emotivos e intelectuales en los que me recreaba alucinado y que me llevaron a construirla, no sé si realizando aquellas pretensiones primigenias en que tal vez siga?

Por suerte también soy poeta y puedo superar esos escrúpulos intelectuales por el gusto de escribir y compartir mi palabra. Y muy tonto sería llevar esos recelos de que hablo al extremo, pues de poco me aprovecharían, y cuando, además, no podemos escuchar música ni contemplar arte sin conocer previamente los pareceres del autor y, acaso, de los intérpretes.

A lo nuestro. Que las matemáticas poseen un valor instrumental lo saben ingenieros, economistas, sociólogos . . . , que son un valor en sí mismas lo saben matemáticos y filósofos, y que son fuente inagotable de inteligencia, belleza y sensibilidad es algo que ya hace mucho que saben los artistas y que ahora comienzan a descubrir los poetas.



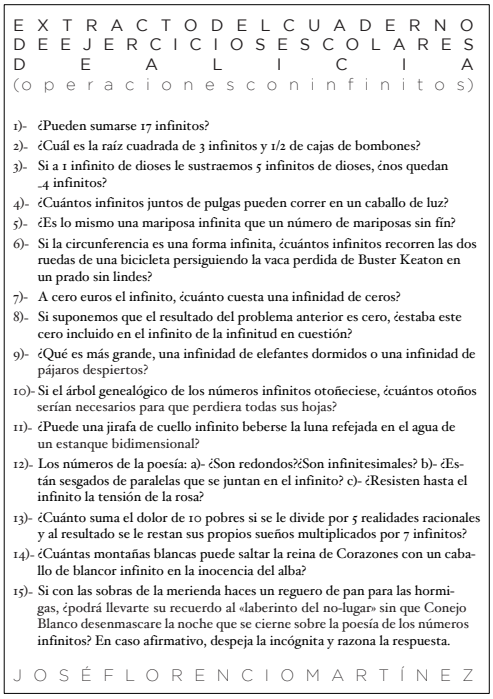


Figura 1. Detalles de páginas del libro (I).

En *ποetas, primera antología de poesía con matemáticas*, Amargord, 2012 se ofrecen varios aportes originales en el ámbito literario:

1. Comenzando en Grecia, se hace un amplio repaso a cómo matemáticas (con carácter más general, la ciencia) y poesía se han servido mutuamente. Se haya y se habla de:

   - Poesía científica (estrictamente, en definición de Aristóteles, de poesía didáctica) , entre la que se incluyen las obras de Hesíodo: *Teogonía y Los trabajos y los días*;
   - Matemáticas en verso, que es lo que encontramos en los enunciados de 40 problemas aritméticos en la Antología Palatina (alguno tan popular como el de las edades de Diofanto);
   - Matemáticas en la forma del verso, cuando Sotades el Obsceno introduce los palíndromos partiendo de la por entonces definición de simetría (igual medida).

   De Grecia se salta a Roma, donde la poesía didáctica sigue teniendo vigencia y se realiza algún aporte en el campo astronómico-astrológico y en el aspecto o forma del verso al recurrir a la numerología.

2. Pero como la obra que les presentamos no es únicamente una obra literaria, sino que además las matemáticas desempeñan un papel esencial, no se limita el prólogo de nuestra antología a bucear en lo escrito en las lenguas que dan esta en la que nos expresamos y nos lee, sino que amplía la tradición a la India, Persia, Al-Ándalus (que normalmente se excluye, sí, de nuestra tradición literaria) y la América precolombina, antes de dar el salto al renacimiento europeo y centrarse en lo que acontece en España en el siglo XIX.

   Como muestra, en la India, al periodo que abarca los siglos V-XII se lo llama "época de la poesía" porque en esta forma se dieron sus obras matemáticas. Traigamos el ejemplo de *Lilavati*, de Bhaskara, al final de ese tiempo, y de la que les puedo anticipar que muy pronto se editará, al fin, en español. Y en Persia, el bello Omar Khayyam, matemático y

poeta recordado por ambas facetas; y en Al-Ándalus, Abbas ibn Firnas; y en América, Nezahualcóyotl. No agotemos aquí el contenido del libro.

3. Tras presentar las diferentes formas en que históricamente se han utilizado matemáticas y poesía y habiendo ampliado el concepto de tradición de nuestra lengua a nuestra cultura, se presenta y razona la novedad que ofrecen los autores antologados, y es que son poetas, de formaciones muy diversas (muchos exclusivamente humanista), y haciendo versos (ya sea en su forma tradicional o con poesía visual) recurren a las matemáticas como parte de su bagaje emocional y expresivo.

4. No es frecuente encontrar una antología tan bien fundamentada, atenta a poner de relieve las sensibilidades y objetivos y no de congraciarse con algunas personas o defender otro tipo de intereses, y con unas perspectivas amplias y valientes que han permitido reunir a grandes poetas de ambas orillas del atlántico. Y esto último no por el prestigio del antólogo ni por su influencia, que entonces casi no tenía obra poética ni tenía edición que defender, sino por la propia identificación de los autores con el proyecto: todos se han reconocido en las ideas que inspiraban esta obra, todos echaban en falta su existencia y todos anhelaban formar parte de un trabajo así, por eso han colaborado a pesar de estar al frente un poeta que no gozaba de su prestigio y una editorial mucho menor de las que editan sus obras.

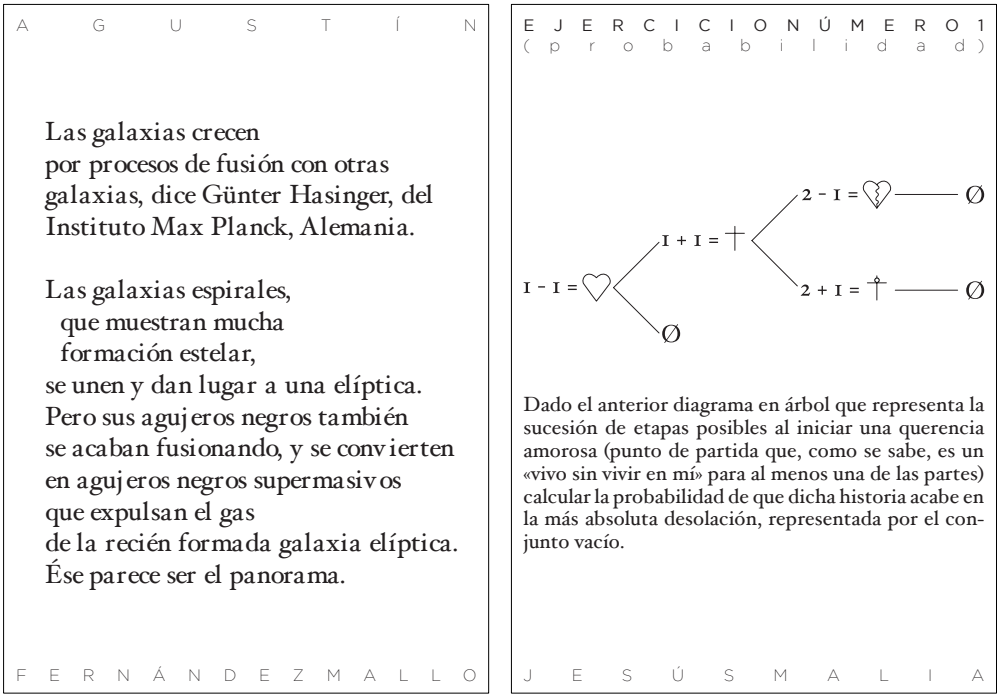


Figura 2. Detalles de páginas del libro (II).

En cuánto a matemáticas, ¿qué encontrarán en *πoetas*? Aritmética, geometría, álgebra, astronomía …, conceptos, fórmulas, simbología … Las matemáticas como las han sentido y compartido Rodolfo Hinostroza, Enrique Verástegui, José Florencio Martínez, David Jou, Ramon Dachs, Daniel Ruiz, Agustín Fernández Mallo, Javier Moreno y Jesús Malia, diez autores sobresalientes representados por una breve reflexión personal de la acercanza entre matemáticas y poesía y por su obra poética. 48 páginas iniciales de prólogo y estudio preliminar y hasta la 239 de poesía con matemáticas. Y atiendan bien al nexo, no vale otro para la obra recogida en *πoetas* ni hablamos de otra cosa: es poesía, poesía lírica, y parte del bagaje intelectual y emocional, y

por tanto del verso, de sus autores son las matemáticas. Poesía matemática o matemáticas en verso son otra cosa, de lo segundo les hablará Lilavati, estén atentos.

No creo necesario hacer aquí más apreciaciones sobre *ποetas* (que por cierto, se lee "poetas"), pero sí lo es hablarles del proyecto editorial que representa la "Colección pi de poesía" que se inició con dicha antología. Esta colección nace en el seno de la poesía desde el entusiasmo por las matemáticas y sus manifestaciones culturales. Principalmente serán poetas los que se recojan en ella, pero no es descartable que registremos matemáticas en verso, arte, fotografía … llevados por el amor a las matemáticas y la consideración que les tenemos y queremos que se les tengan como elemento de cultura. ¿Aspiración? Que igual que quien no ha leído el Quijote lo reconoce no sin vergüenza, quien no se acerque a los Elementos de Euclides no lo haga sin bochorno. Y aún menos, que al igual que en el restaurante todos queremos nuestra propia carta para leer por nosotros mismos lo que se nos ofrece, no seamos menos animosos al hacer el cálculo mental para pagar a escote.

Sobre el autor:
Nombre: Jesús Malia
Correo Electrónico: jesusmalia@yahoo.es
Institución: Director de la "Colección pi de poesía" de la editorial Amargord.

Entrevista

Carlos Óscar Sorzano: entre la investigación y la docencia

Carlos Óscar Sorzano: research and teaching

Equipo Editorial

Revista de Investigación

Volumen III, Número 1, pp. 199–204, ISSN 2174-0410
Recepción: 5 Mar'13; Aceptación: 20 Mar'13

1 de abril de 2013

Resumen

Carlos Óscar Sorzano es investigador del CSIC (Consejo Superior de Investigaciones Científicas), donde coordina el centro de procesamiento de imágenes y es profesor de la Escuela Politécnica Superior de la Universidad San Pablo CEU donde coordina el nuevo grado de Ingeniería Biomédica. Dedica así su vida profesional a la investigación más puntera y a la docencia universitaria. Hablamos con él para cambiar impresiones sobre estos dos aspectos.

Palabras Clave: Investigación y docencia, Ingeniería biomédica, Procesamiento digital de imágenes.

Abstract

Carlos Óscar Sorzano is a researcher at CSIC (Consejo Superior de Investigaciones Científicas), where he coordinates the Instruct image processing center and he is an associate professor at the Polytechnic School of San Pablo CEU University where he coordinates the new degree on Biomedical Engineering. In this way, he dedicates his professional life to the high investigation and to the University. We speak to him to discuss about these two aspects.

Keywords: Teaching and research, Biomedical Engineering, Digital image processing.

1. Entrevista

- Carlos Óscar, lo primero que sorprende al ver tu currículo es tu extensa y variada formación: eres Ingeniero de Telecomunicaciones, Ingeniero Informático, Matemático y Doctor en Ingeniería Biomédica. Actualmente estudias Farmacia. ¿Responde esto a una inquietud intelectual, o te has visto impelido a esa formación para mejorar tu investigación?

Carlos O. Sorzano

Yo diría que es una mezcla de las dos cosas. Por un lado, siempre he tenido esa inquietud por saber más, sobre todo atraído por cualquier aspecto relacionado con la teoría de la señal, los algoritmos, el análisis de datos, la matemática aplicada, etc. y utilizar todas estas herramientas para resolver

problemas de la vida real. En este marco entrarían las tres primeras titulaciones. Lo de estudiar Farmacia sí que está relacionado con complementar mi formación en el área en el que trabajo. Si estás desarrollando algoritmos para procesar imágenes en Biología Estructural y estás todo el día tratando con biólogos, es importante que tengas la formación adecuada que te permita entender el problema que estás tratando de resolver. En mi opinión, el éxito de los grupos científicos actuales es la interdisciplinariedad, juntar a un grupo de personas, con diferentes perspectivas y conocimientos de forma que todos colaboren para resolver un problema complejo. El carácter interdisciplinar de los grupos requiere que los integrantes del grupo tengan una mente abierta y estén dispuestos a entender un poco del "otro lado". El que haya personas "bisagra" que comprenden en cierta profundidad ambos lados es un enorme facilitador de esta tarea.

- Desde el principio has estado vinculado al CSIC, pero realizaste una estancia posdoctoral en Suiza. ¿Qué tal fue tu experiencia allí? ¿Encauzó tu carrera investigadora? ¿Recomendarías estancias en el extranjero a los jóvenes investigadores?

Efectivamente, desde que me vine a Madrid hace 16 años siempre he estado vinculado al CSIC de una forma u otra, y posteriormente a la Universidad. El poderme ir a Suiza fue gracias a que pude reorganizar mis clases en la Universidad sacando un año completo de estancia post-doctoral en el extranjero. El grupo en el que me integré es uno de los mejores del mundo en el análisis de imágenes biomédicas, y desde luego, fue una experiencia única: tanto por las técnicas que conocí y los problemas a los que me expuse, como por el hecho de ver cómo se desarrolla la investigación en una universidad en la que más de un tercio del personal del campus se dedicaba a la investigación. La visión de Suiza, como país, sobre la importancia de la investigación y la posterior transferencia del conocimiento a un tejido industrial muy desarrollado no es comparable a la visión que tenemos en España. También ves cómo los estudiantes de grado se integran en el trabajo de investigación y cómo gustan de él durante su periodo de formación; algo que tampoco se suele ver en España. Además, al ser un país alpino, es un paraje estupendo para pasar un año de tu vida. No podría decir que mi estancia en el extranjero haya tenido un impacto directo y medible en mi carrera investigadora en el sentido de que me haya servido para alcanzar alguna plaza o para acceder a proyectos o trabajos que no hubiera podido acceder de otra forma. Quizás es por ello que los estudiantes de doctorado que terminan ahora intentan evitar salir al extranjero. Por un lado, porque les supone un paréntesis en su vida personal y porque tampoco ven muy claro de qué les va a servir a su vuelta a España. Quizás, esto sea un error porque a nivel personal y científico es una experiencia de lo más enriquecedora y, aunque la situación laboral de los científicos en España está pasando por unos momentos muy críticos, está claro que las pocas plazas que haya serán para aquellos con mejor currículo, y entre otras cosas cuenta las estancias en el extranjero y la productividad durante las mismas.

- Resúmenos, en pocas palabras si es posible, de qué trata tu investigación.

En la Unidad de Biocomputación del Centro Nac. De Biotecnología del CSIC desarrollamos algoritmos y software para el análisis de imagen en microscopía electrónica y de rayos X. El objetivo es resolver la estructura tridimensional de complejos macroleculares. Son como pequeñas piezas con las que las células realizan todas sus funciones. Para conocer su forma, se prepara una solución concentrada de estas piececitas, se visualizan en el microscopio y posteriormente se combinan miles de estas imágenes en el ordenador. El problema de las imágenes adquiridas es que están emborronadas (como si nos pusiéramos unas gafas con muchas dioptrías), tienen mucho ruido y poco contraste (la imagen de cada una de las piececitas es como una pequeña mancha "enterrada" en nieve de la tele), y además es posible que tengamos varios tipos de piececitas en una misma micrografía por lo que hay que separar computacionalmente qué foto va con qué pieza (¡sin conocer de antemano las piezas!). Resolvemos todos estos problemas desarrollando algoritmos con una fuerte base matemática y de tratamiento de señal que nos ayudan a solucionar pequeñas cuestiones. La aplicación sucesiva de varios de estos algoritmos es la que nos lleva desde las imágenes del microscopio hasta una reconstrucción tridimensional del com-

plejo macromolecular que permite a los biólogos entender cómo esa piececita realiza la función fisiológica de la que se encarga, qué modificaciones pueden dar lugar a patologías, e incluso, cómo podría un fármaco interaccionar con ella para alterar su funcionamiento.

- Desde el punto de vista académico, llevas años como profesor en la Universidad San Pablo CEU. Actualmente estás coordinando el nuevo grado de Ingeniería Biomédica de dicha Universidad. ¿Qué tal está funcionando? ¿Te está ayudando tu experiencia investigadora en dicho campo en el planteamiento docente de este grado?

La Ingeniería Biomédica es una interesante rama de la ingeniería que ha cristalizado en un Grado en los últimos años en varias universidades, y es una de las titulaciones más demandadas de las universidades en las que se imparte con una nota de corte, en general, superior al 11.5. Nuestra universidad cuenta con un Laboratorio de Bioingeniería desde el año 2007 que agrupa a varios profesores que trabajan en aplicaciones de las tecnologías de la información y las comunicaciones (TIC) a la medicina, la biología y la farmacia. Por ello, decidimos hace dos años comenzar a impartir esta titulación. Hasta ahora hemos estado en la fase de preparación de la documentación acreditativa del grado, su aprobación por la ANECA y la organización a nivel de universidad para comenzar a impartir este título oficial a partir del curso 2013/2014. Quizás uno no se da cuenta de la cantidad de trabajo que supone el impartir un nuevo grado hasta que le toca hacerlo. Sin embargo, este trabajo se ve compensado porque las expresiones de interés por parte de los alumnos sobre esta titulación nos muestran que previsiblemente ésta sea muy bien recibida cuando la empecemos a impartir en el próximo curso.

- Existe siempre una polémica sobre las prioridades que un profesor universitario debe tener investigación o docencia. ¿Es posible un equilibrio que compagine las dos vertientes? ¿Cómo enfocas tú estas dos facetas?

Es triste que en la práctica tengamos que hablar de investigación o docencia en vez de investigación y docencia. Recordemos que la universidad no sólo debe transmitir el conocimiento (docencia), sino también crearlo (investigación). En España, es difícil armonizar estos dos aspectos debido a la amplísima carga docente que tenemos. Comentando con un colega del Imperial College London sobre su carga docente me decía que era de unas 16 horas ¡al año!, su perfil era evidentemente investigador y las clases eran para alumnos de postgrado. La carga media en una universidad privada está entorno a las 11 horas por semana y en una universidad pública es algo menor, aunque en los últimos años está subiendo considerablemente. Visto lo que hay en otras universidades del mundo, creo que en España debería distinguirse entre el profesor con un perfil eminentemente investigador (y del que los alumnos obtienen un enorme beneficio por estar en contacto con la ciencia más puntera) y el profesor con un perfil eminentemente docente (y del que los alumnos obtienen un enorme beneficio por la claridad que consigue transmitir en sus clases). En la práctica, por mucho que quieran hacernos ver desde los Vicerrectorados de Investigación y Profesorado, la opción en España es "café para todos": todos los profesores tienen la misma carga (con pequeñas modulaciones). A la vista de nuestros resultados en los rankings mundiales, está claro que algo hay que cambiar en nuestras universidades y posiblemente éste sea uno de los aspectos que más repercusión tenga.

En mi caso particular, yo he resuelto esta dicotomía entre investigación y docencia reduciendo mi participación en la universidad a una cantidad de horas de clase con la que puedo investigar cómodamente. Como suelo responder cuando me preguntan "me gusta mucho dar clase, pero no sólo dar clase". Creo que en esta situación actual yo me encuentro cómodo y los alumnos también.

- En tu opinión, ¿se hace buena investigación en las universidades españolas, o crees que donde de verdad se avanza es en centros específicos de investigación y desarrollo como el CSIC?

Scimago es un organismo de elaboración de rankings en temas de producción científica. Para 2011 identificó 71.155 artículos científicos provenientes de España, de los cuales 46.048 provenían del CSIC, casi 2 de cada 3. Sin embargo, el número de investigadores de plantilla

del CSIC es de 3000, mientras que el de profesores universitarios es de 130.000, según el INE. La productividad del CSIC sería de casi 80 veces la productividad de la universidad. Esto no es realmente así porque habría que contar que muchos de los profesores universitarios lo son a tiempo parcial y, por tanto, normalmente no contribuyen con investigación, que hay trabajos conjuntos entre la universidad y el CSIC (que han sido contados en el lado del CSIC en esta estadística), que por cada investigador del CSIC hay una media de 3 ó 4 estudiantes predoctorales, postdoctorales o técnicos de laboratorio y que esta proporción es menor en las universidades, etc. En cualquier caso, es indudable de que la producción científica media por investigador del CSIC es mayor que la de por profesor de universidad. Esto tiene, sin duda, que ver con las tareas docentes y también con la cultura que se instaura en cada institución. De hecho, el CSIC no sería quizás el paradigma de buen hacer científico en España, sino que hay centros de reciente creación, no vinculados administrativamente ni al CSIC, ni a las universidades, ni a las Comunidades Autónomas que están liderando la excelencia científica en España como así lo acredita el Programa Severo Ochoa del ministerio. Luego, a nivel particular, en todas partes hay grupos buenos, malos y regulares, y me he referido a valores medios. Las universidades podrían jugar un papel fundamental en investigación, como así ocurre en otros países, pero tendríamos que cambiar mucho de las mismas para que así fuera: carga y distribución docente, estructura de la financiación, promoción laboral por criterios docentes e investigadores, cultura de selección y permanencia del personal, participación de los alumnos en la investigación, etc.

- ¿A qué nivel crees que está España en el aspecto investigador y en el docente con respecto a otros países europeos como Suiza, país que tú conoces?

De acuerdo con Scimago, España sería el 9º país del mundo con mayor producción científica (http://www.scimagojr.com/countryrank.php), por delante de países como Suiza. Pero este indicador puede conducir a errores porque depende del tamaño del país. Si ordenamos los países por el número de citas que reciben sus trabajos, una mejor medida de la calidad de la investigación, resulta que Suiza es el país del mundo con mayor número medio de citas por artículos (22,5), casi el doble que España (13,7). Detrás de Suiza están los países que todos tenemos en la cabeza cuando hablamos de investigación de calidad: Dinamarca, Holanda, Estados Unidos, Suecia, Finlandia, … hasta llegar a España en el puesto 19. Hay países como Estados Unidos, Reino Unido, Alemania, Francia, Canadá e Italia que están por delante de España tanto en cantidad de trabajos como en calidad de los mismos. España no es, por desgracia, un país en el que la investigación ocupe un lugar importante en las prioridades sociales ni políticas. Esto ha sido así culturalmente desde hace siglos casi diría. Me gusta un ejemplo futbolístico que todos entenderemos: si resultara que un chico sahariano destacara mucho como futbolista, lo más probable es que emigrara a aquellos países en los que el fútbol es un deporte valorado (España, Francia, Italia, Inglaterra, …); si se queda en el Sáhara para "subir el nivel de la liga de su país", lo más probable es que sufra una terrible frustración continua. Por desgracia, la ciencia en España no es la actividad más valorada a pesar de que nuestros políticos no paran de decir que hay que salir de esta crisis con un cambio de modelo productivo. Además, cambiar las tendencias científicas de un país no es cuestión de dos años, ni de una legislatura, ni de dos, sino que probablemente estemos hablando de procesos que impliquen varias décadas, algo que no sé si veremos en el futuro próximo y que ningún político desee acometer de forma seria.

- Volviendo a tu trayectoria profesional, fuiste galardonado con el Premio Ángel Herrera de Investigación en 2006. ¿Crees que este tipo de premios abren más puertas, o simplemente son un motivo de orgullo?

Hasta ahora no he sentido que este premio haya significado ningún cambio en mi trayectoria profesional, creo que este tipo de cosas son más anecdóticas que reales en el sentido que la concesión de proyectos, el acceso a financiación, puestos laborales, … no dependen de estos premios.

- Has ocupado ya varios cargos relevantes, tanto en la Universidad como en el CSIC. Además de la coordinación del grado ya mencionada, codirigiste el Postgrado en Biotecnología computacional, diriges

el centro INSTRUCT de procesamiento de imágenes, presides la Asociación Nacional de Investigadores, participas en el Comité de Ética de Experimentación Animal del CNB, coordinas el servicio de análisis estadístico del CNB … ¿Llevas bien este tipo de cargos, o su carga de gestión hace que te alejes de los aspectos científicos?

No se puede negar que estos cargos llevan asociada una importante labor de gestión (reuniones, informes, correos electrónicos, …), pero también me han dado acceso a una visión de la ciencia que nunca habría podido adquirir sin las oportunidades de discusión de determinados temas con personajes de cierta relevancia y agradezco mucho este aspecto en la medida que me ha hecho madurar personalmente y tener una mayor visión de conjunto. Sin embargo, no quiero dedicar mi vida a la gestión. Lo mío es estar en el día a día del laboratorio peleando con las ecuaciones, implementándolas en un ordenador y consiguiendo que se alcancen mejores resultados cada vez, haciendo avanzar a la ciencia y la tecnología en la primera línea. Por desgracia, la carga de gestión es algo que saca a los científicos del trabajo de laboratorio diario. De momento, no me ha llegado ese día y no sé cómo será en el futuro porque a la vista de mi trayectoria mi tendencia es a meterme en "líos de organizar cosas".

- Sorprende también el gran número de publicaciones que tienes, sobre todo teniendo en cuenta tu edad (este año cumples los cuarenta). ¿Piensas bajar el pistón a partir de ahora, o mantienes la ilusión? ¿Cuáles son tus proyectos para el futuro?

Como dicen los futbolistas, el mérito no es sólo mío, sino del equipo. Hasta ahora he tenido la suerte de jugar siempre en equipos de 1ª división, con un sesgo muy marcado hacia la productividad. Por un lado, evidentemente tu productividad personal aumenta al estar en un entorno en el que ésa es la cultura imperante; por otro, es cierto que te pone un nivel de trabajo y presión muy alto (como cuando Messi sólo marca 1 gol por partido, y todo el mundo se pregunta cuál es la crisis que le está afectando). Además, esta elevada productividad hay que compararla con la gente que también juega en esa liga, que también tienen una productividad muy alta.

En mi caso concreto, tengo una experiencia en matemática aplicada y estadística muy sólida, y esto me permite colaborar con un abanico muy amplio de diferentes aplicaciones, no sólo de diseño de algoritmos de procesamiento de imagen. En muchos de los trabajos, yo he participado únicamente en el diseño del experimento y el análisis de los datos, una fracción relativamente menor del trabajo.

De momento, pienso seguir con este ritmo de trabajo en la medida que las circunstancias me lo permitan ya que disfruto mucho tanto de los trabajos que lidero yo directamente, como de las oportunidades que te da el ver otros aspectos científicos a través de mi participación secundaria en ellos. En esto coincido con la mayoría de mis colegas científicos: hace un par de años una ETT realizó una encuesta sobre la satisfacción laboral de diferentes colectivos. Los científicos eran el colectivo que más disfrutaba de su trabajo.

Esta revista fue 100% maquetada
con software de código abierto

$$\frac{\pi}{2} = \sum_{k=0}^{\infty} \frac{k!}{(2k+1)!!} = \sum_{k=0}^{\infty} \frac{2^k k!^2}{(2k+1)!}$$
$$= 1 + \frac{1}{3}\left(1 + \frac{2}{5}\left(1 + \frac{3}{7}(1 + \cdots)\right)\right)$$

3,14159265358979323846264338327950288419716939937
51058209749445923078164062862089986280348253421170679821480865 1
32823066470938446095505822317253594081284811174502841027019385211
05559644622948954930381964428810975665933446128475648233786783165 27
12019091456485669234603486104543266482133936072602491412737245870066 0
63155881748815209209628292540917153643678925903600113305305488204665 21
38414695194151160943305727036575959195309218611738193261179310511854807
4462379 962749567 351885752
72489 122793818 330119491
2983 367336244 065664308
602 139494639 522473719
070 217986094 370277053
921717629 317675238
467481846 766940513
200056812 714526356

G.I.E

Pensamient Matemàtic

MAIC

$$\frac{6}{\pi^2} = \sum_{k=1}^{\infty} \frac{1}{k^2}$$

$$\pi = 4\sum_{k=0}^{\infty} \frac{(-1)^k}{2k+1} = 4 - \frac{4}{3} + \frac{4}{5} - \frac{4}{7} + \frac{4}{9} - \cdots$$

$$\frac{\pi}{2} = \prod_{k=1}^{\infty} \frac{(2k)^2}{(2k)^2 - 1} = \frac{2}{1}\cdot\frac{2}{3}\cdot\frac{4}{3}\cdot\frac{4}{5}\cdot\frac{6}{5}\cdot\frac{6}{7}\cdot\frac{8}{7}\cdot\frac{8}{9}\cdots$$
$$= \frac{4}{3}\cdot\frac{16}{15}\cdot\frac{36}{35}\cdot\frac{64}{63}\cdots$$

$$\pi = 6\arcsin\frac{1}{2} = 3\sum_{k=0}^{\infty} \frac{\binom{2k}{k}}{16^k(2k+1)}$$
$$= 6\left(\frac{1}{2^1\cdot 1} + \left(\frac{1}{2}\right)\frac{1}{2^3\cdot 3} + \left(\frac{1\cdot 3}{2\cdot 4}\right)\frac{1}{2^5\cdot 5} + \left(\frac{1\cdot 3\cdot 5}{2\cdot 4\cdot 6}\right)\frac{1}{2^7\cdot 7} + \cdots\right)$$
$$= 3 + \frac{1}{8} + \frac{9}{640} + \frac{15}{7168} + \frac{35}{98304} + \frac{189}{2883584} + \frac{693}{54525952} + \frac{429}{167772169} + \cdots$$