comunicación ::
matematicalia
revista digital de divulgación matemática
Vol. 2, no. 1 (feb. 2006)

Los primeros 50 años de la teoría de códigos (*)

Richard Pinch
Institute of Mathematics and its Applications
Southend-on-Sea, Essex (UK)
e-mail: rgep@chalcedon.demon.co.uk
página web: http://www.chalcedon.demon.co.uk/rgep/rcam.html

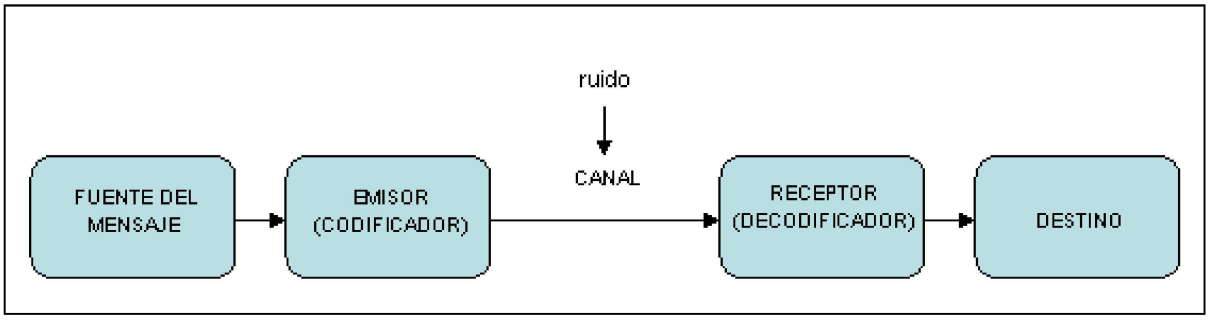
En las últimas semanas gente de todo el planeta ha estado fascinada por las imágenes y datos científicos que han sido retransmitidos desde Marte por la misión Pathfinder de la NASA[1]. Durante décadas, las sondas espaciales han enviado datos similares desde los planetas más lejanos. Sin embargo, la potencia de los transmisores de radio en esas naves es sólo de unos pocos vatios, comparable a la fuerza de una bombilla eléctrica tenue. ¿Cómo puede ser enviada esta información de un modo fiable a través de cientos de millones de kilómetros sin que quede completamente anegada por las interferencias?

El explorador Sojourner (i) y el módulo Mars Pathfinder (d), visto desde el explorador. La antena circular de alta ganancia apunta hacia la Tierra. [Fuente: Jet Propulsion Laboratory, NASA].

En el proceso de recuperar con éxito esas señales intervienen muchas disciplinas: la ingeniería electrónica, la informática y las matemáticas.

La *teoría de códigos* es la rama de las matemáticas que se ocupa de la transmisión y posterior recepción de datos a través de canales ruidosos. Su objetivo es *facilitar* la lectura de mensajes: no debe ser confundida con la *criptografía,* ¡que es el arte de *dificultar* la lectura de mensajes!

Suponemos que nuestro mensaje está en forma de dígitos binarios o *bits*, cadenas de ceros y unos. Tenemos que transmitir esos bits a través de un canal (como, por ejemplo, una línea telefónica) en el que se producen errores aleatoriamente, pero con una tasa global predecible. Para compensar los errores hemos de transmitir más bits que los que tiene el mensaje original.



Un canal.

El método más simple para detectar errores en los datos binarios es el código de *paridad*, que hace que la fuente del mensaje transmita un bit de “paridad” extra cada 7 bits. Sin embargo, este método sólo puede detectar errores; la

única forma de corregirlos es ¡pedir que se retransmitan los datos!

Una forma simple de corregir los errores además de detectarlos es repetir cada bit un número determinado de veces. El receptor examina qué valor, el cero o el uno, ocurre con más frecuencia y presupone que ese es el bit que se pretendía transmitir. Ese esquema admite márgenes de error de hasta 1 error por cada 2 bits transmitidos, a costa de incrementar el número de repeticiones.

Los inicios

La desventaja del esquema de repetición es que multiplica el número de bits transmitidos por un factor que puede resultar inaceptablemente alto. En 1948, Claude Shannon, trabajando en los Laboratorios Bell (Estados Unidos), inauguró la disciplina de la teoría de códigos probando que es posible codificar mensajes de manera que el número de bits extra transmitidos sea lo menor posible. Desafortunadamente, su demostración no incluía ninguna "receta" explícita para obtener estos códigos optimales.

Dos años después, Richard Hamming, también de los Laboratorios Bell, publicó detalles de su trabajo sobre códigos de corrección de errores explícitos, con tasas de transmisión de la información más eficientes que la simple repetición.

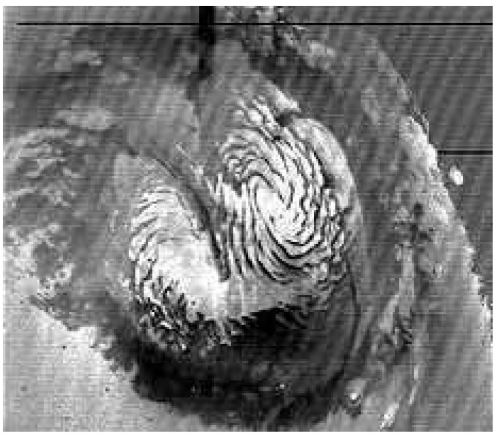
Su primer intento produjo un código en el que 4 bits de datos iban seguidos de 3 bits de comprobación, lo que no sólo permitía la detección sino también la corrección de errores sueltos. (El código de repetición requiere 9 bits de comprobación para lo mismo).

Se dice que Hamming inventó este código después de varios intentos de perforar un mensaje en una cinta de papel usando el código de paridad. "Si puede *detectar* el error", se quejó, "¡por qué no puede *corregirlo*!".

Mientras Shannon y Hamming trabajaban sobre la transmisión de la información en los Estados Unidos, John Leech ideó códigos similares al investigar sobre teoría de grupos en Cambridge (Reino Unido). Esta investigación incluía el problema del empaquetamiento de esferas (véase el *Misterio Matemático*[2] del mismo número de *Plus Magazine* donde aparece el original de este artículo) y culminó en el notable *retículo de Leech*, de 24 dimensiones, cuyo estudio fue una pieza clave en el programa hacia la comprensión y clasificación de los grupos de simetría finitos.

Aplicaciones

El valor de los códigos correctores de errores para la transmisión de la información, tanto en la Tierra como desde el espacio, fue evidente desde un primer momento. Se construyó así una amplia variedad de códigos orientados tanto a la economía en la transmisión como a la capacidad de corrección de errores. Entre 1969 y 1973, la sonda Mariner de la Nasa utilizó un potente código *Reed-Muller* capaz de corregir 7 errores de cada 32 bits transmitidos, consistente ahora en ¡6 bits de datos y 26 bits de comprobación! A la Tierra fueron retransmitidos más de 16.000 bits por segundo.



El casquete polar norte de Marte, fotografiado por el Mariner 9 en 1972. [Fuente: NASA].

Una aplicación no tan obvia de los códigos correctores de errores surgió con el desarrollo de los discos compactos. En un CD, la señal se codifica digitalmente. Para protegerlo contra los arañazos, roturas y daños similares, se usan dos códigos "entrelazados" que pueden corregir hasta 4.000 errores consecutivos (2,5 mm de pista, aproximadamente). Los reproductores de discos de audio pueden recuperar incluso daños mayores, interpolando la señal.

Desarrollos recientes

En los últimos dos años se ha logrado el objetivo de encontrar códigos explícitos que alcancen los límites predichos por el trabajo original de Shannon. Su construcción requiere técnicas de una variedad sorprendentemente amplia de matemáticas puras: el álgebra lineal, la teoría de cuerpos y la geometría algebraica desempeñan un papel primordial. La teoría de códigos no sólo ha ayudado a resolver problemas de importancia vital en el mundo externo a las matemáticas, sino que ha enriquecido otras ramas de las matemáticas con nuevos problemas además de nuevas soluciones.

Referencias

Las matemáticas de los códigos correctores de errores se discuten en:

C. Goldie, R. Pinch: *Communication theory.* Cambridge University Press, 1992.

R. Hill: *A first course in coding theory.* Oxford University Press, 1986.

D. Welsh: *Codes and cryptography.* Oxford University Press, 1988.

Puede encontrarse más información sobre la misión Mars Pathfinder en el sitio web Mars Missions[3].

Las biografías de los matemáticos que se mencionan en el artículo están disponibles en el MacTutor history of mathematics archive:

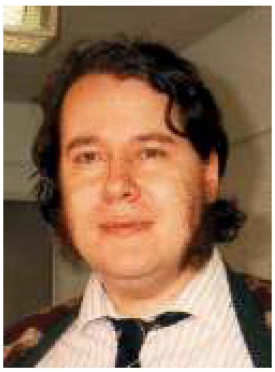
Claude Shannon
Richard Hamming
John Leech

---

[1] El artículo original fue publicado en septiembre de 1997. El Mars Pathfinder descendió en la superficie de Marte el día 4 de julio de 1997, luego de despegar de Cabo Cañaveral (Florida, EE.UU.) y recorrer durante 212 días (7 meses) 497 millones de kilómetros a una velocidad de 21.271 km/h. (N. de la T.).

[2] La demostración de Thomas C. Hales de la conjetura de Kepler que se menciona en esta referencia fue finalmente conseguida gracias a una combinación de herramientas matemáticas y cálculo computacional. La versión abreviada apareció publicada en *Annals of Mathematics* 162, no. 3 (noviembre 2005), 1065-1185, y la extendida puede consultarse en http://annals.math.princeton.edu/keplerconjecture/proof_kepler.pdf. Los recursos computacionales utilizados están disponibles en http://annals.math.princeton.edu/keplerconjecture. Véase también la Noticia aparecida al respecto en *Matematicalia* (N. de la T.).

[3] En castellano en http://mpfwww.jpl.nasa.gov/marte/overview.html (N. de la T.).



Sobre el autor

Richard G.E. Pinch perteneció al Departament of Pure Mathematics and Mathematical Statistics de la Universdad de Cambridge (UK) entre 1984 y 1998. Actualmente es Fellow y Chartered Mathematician del Institute of Mathematics and its Applications, e investiga en números de Carmichael y pseudoprimos. Sus anteriores líneas de investigación incluyen teoría de números computacional, aritmética de curvas elípticas, combinatoria algebraica y criptografía de clave pública. Es miembro de la London Mathematical Society y de la American Mathematical Society.

(*) Este artículo apareció en el número 3 (septiembre 1997) de *Plus Magazine*. *Matematicalia* agradece a los responsables del Millennium Mathematics Project de la Universidad de Cambridge la autorización para publicar su traducción al castellano. [Traductora: Isabel Marrero].

Cerrar ventana