

CÓDIGOS SECRETOS Y TEORÍA DE LA INFORMACIÓN EN LA MAGIA

PEDRO ALEGRIÁ (*)

La teoría de códigos es una disciplina matemática de gran actualidad por su importancia social y su velocidad de desarrollo. En su reciente visita a España, el ilustre matemático **Michael Atiyah** (ganador de una medalla Field, premio Abel de Matemáticas y académico de la Real Academia Española de Ciencias) afirmaba que el siglo XXI será precisamente el siglo de la información.

En nuestra vida diaria, manejamos constantemente información, la cual se transmite ininterrumpidamente, bien de forma codificada, bien sin codificar. También comprendemos fácilmente que los sistemas de codificación son fundamentales en el desarrollo y la fiabilidad de la información transmitida.

Un método original para motivar el estudio de los códigos y comprender algunas de las propiedades en que se basa consiste en plantear algunos trucos de magia y discutir las reglas que se aplican en su funcionamiento.

Ilustraremos lo anterior con algunos juegos, los cuales clasificamos en dos grupos: en la primera parte estudiaremos juegos de adivinación de números mediante un conjunto de preguntas y respuestas. En la segunda parte analizaremos trucos que pueden plantearse como pruebas de comunicación no verbal. En ambos casos, la transmisión de la información se realiza exclusivamente en base a principios matemáticos.

1. LOS CÓDIGOS DE HAMMING

Cualquier aficionado a problemas de ingenio puede resolver fácilmente el siguiente problema:

¿Cuál es el número mínimo de preguntas, cuyas únicas respuestas posibles sean Sí o NO, necesarias para deducir un número pensado?

Una estrategia elemental consiste en separar los números en dos grupos iguales (o que se diferencien en uno) y preguntar si el número pensado está en uno de ellos. Así, por cada pregunta se reduce a la mitad el número de posibilidades. Se deduce así que, si el número pensado está comprendido entre 2^n y 2^{n+1} , son necesarias $n+1$ preguntas para tener la seguridad de adivinar el número.

Aparentemente, para que el método funcione, las preguntas sucesivas dependen de las respuestas a las anteriores. De modo que es natural preguntarse:

¿Cuál es el número mínimo de preguntas, realizadas todas a la vez, necesarias para adivinar el número?

A pesar de la aparente mayor complejidad, la respuesta es la misma. Basta que cada pregunta determine una cifra en la representación binaria del número. Como un número comprendido entre 2^n y 2^{n+1} tiene $n+1$ cifras en su representación binaria y cada cifra sólo tiene dos posibles valores, podemos asignar a cada valor una respuesta Sí o NO.

(*)Departamento de Matemáticas, Universidad del País Vasco.
Correo electrónico: mtpalezp@lg.ehu.es

Son bien conocidos algunos juegos de magia que utilizan esta estrategia. Uno muy común consiste en pedir a un espectador que piense un número y mostrarle un conjunto de tarjetas pidiéndole que determine en cuáles de ellas aparece escrito el número pensado. Si la k -ésima tarjeta contiene los números que tienen un uno en la posición k -ésima de su representación binaria, es fácil determinar de qué número se trata pues el menor número contenido en dicha tarjeta es precisamente 2^{k+1} . La suma de los primeros elementos de las tarjetas que contienen el número pensado permite recuperar la representación decimal del número (otra versión del juego está explicada también en el artículo “La matemagia desvelada”, Revista *Sigma*, Octubre de 2002).

En el diagrama siguiente mostramos el caso de 16 números. A partir de su representación binaria, formamos las tarjetas del modo recién explicado.

Representación decimal	Representación binaria
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111
16	10000

Tarjeta 1 (números que contienen un uno en la última cifra):

1, 3, 5, 7, 9, 11, 13, 15

Tarjeta 2 (números que contienen un uno en la penúltima cifra):

2, 3, 6, 7, 10, 11, 14, 15

Tarjeta 3 (números que contienen un uno en la antepenúltima cifra):

4, 5, 6, 7, 12, 13, 14, 15

Tarjeta 4 (números que contienen un uno en la primera cifra):

8, 9, 10, 11, 12, 13, 14, 15

También se han explotado variantes donde las respuestas no sólo consisten en SÍ o NO. Por ejemplo, si se reparte un conjunto de cartas en tres montones sobre la mesa y se pregunta en qué montón se encuentra una carta pensada, se reduce el número de preguntas necesarias para deducir la carta pensada. En la siguiente sección, nos detendremos un poco en el estudio de este caso.

Queremos considerar a continuación una variante distinta, muy ligada con la teoría de códigos:

¿Cuál es el mínimo número de preguntas necesarias para adivinar un número pensado si se permite que entre las respuestas haya alguna falsa?

Para resolver el problema, una buena estrategia consiste en utilizar los *códigos de Hamming*. A grandes rasgos, se trata de añadir a las cifras significativas de un número otro conjunto de cifras que permita detectar y corregir algún error (equivalente en nuestro problema a alguna respuesta falsa) en la codificación del número.

Para comprender el método, explicaremos su desarrollo con un ejemplo, planteado como juego de magia.

EL DETECTOR DE MENTIRAS

El mago se presenta con las 16 cartas siguientes: As, dos, 9 y 10 de cada palo (denotaremos por "R" a los rombos, "C" a los corazones, "P" a las picas y "T" a los tréboles).

Las muestra a un espectador.

- Aquí tienes un conjunto de cartas. Piensa una de ellas.
- Ya sabes que las cartas tienen diferencias que permiten distinguirlas unas de otras. De modo que si te hago una serie de preguntas, cuya respuesta consista simplemente en decir SÍ o NO, es fácil llegar a adivinar la carta pensada.
- Sin embargo, vamos a complicar un poco el proceso: te voy a hacer una serie de preguntas y te permito que una de las respuestas, como máximo, sea falsa.
- A pesar de todo, al final si me has mentido, sabré en qué pregunta lo has hecho e, incluso, adivinaré tu carta.

1^a pregunta: ¿Tu carta es de CORAZÓN o de PICA?

2^a pregunta: ¿Es roja?

3^a pregunta: ¿Es de valor alto?

4^a pregunta: ¿Es par?

5^a pregunta: ¿Es alguna de éstas?

Conjunto A: {2C, 10C, 1P, 9P, 1R, 9R, 2T, 10T}.

6^a pregunta: ¿Es alguna de éstas?

Conjunto B: {9C, 10C, 1P, 2P, 1R, 2R, 9T, 10T}.

7^a pregunta: ¿Es alguna de éstas?

Conjunto C: {1C, 10C, 1P, 10P, 2R, 9R, 2T, 9T}.

Es todo, después de comprobar las respuestas con la máquina de la verdad, se adivina la carta.

SECRETO:

En primer lugar se asigna un número a cada carta. En la siguiente tabla se muestran las cartas y el valor asignado a cada una.

Carta	Número decimal	número binario	código de Hamming
10C	0	0000	0000000
9C	1	0001	0001101
2C	2	0010	0010011
1C	3	0011	0011110
10P	4	0100	0100110
9P	5	0101	0101011
2P	6	0110	0110101
1P	7	0111	0111000
10R	8	1000	1000111
9R	9	1001	1001010
2R	10	1010	1010100
1R	11	1011	1011001
10T	12	1100	1100001
9T	13	1101	1101100
2T	14	1110	1110010
1T	15	1111	1111111

En la tercera columna escribimos la representación binaria de cada número y en la cuarta columna representamos el código de Hamming de cada número. Para ello se añaden tres cifras de control, según la siguiente regla:

Si llamamos x_1, x_2, x_3, x_4 a las cifras del número, definimos x_5, x_6 y x_7 de modo que se verifique:

$$x_1 + x_2 + x_4 + x_5 = 0 \pmod{2}$$

$$x_1 + x_2 + x_3 + x_6 = 0 \pmod{2}$$

$$x_1 + x_3 + x_4 + x_7 = 0 \pmod{2}$$

(esto equivale a que la suma de dichas cuatro cifras sea par).

Vamos a ver con un ejemplo el método de adivinación de la carta pensada.

El espectador elige el **9P**, que corresponde al 0101, o bien al 0101011.

A cada respuesta se le asigna un dígito, de modo que SÍ corresponde a 0 y NO corresponde a 1. Así pues,

Pregunta	Enunciado	Respuesta	Dígito
1	¿Corazón / pica?	Sí	0
2	¿Roja	No	1
3	¿Alta?	No (mentira)	1
4	¿Par?	No	1
5	¿Conjunto A?	Sí	0
6	¿Conjunto B?	No	1
7	¿Conjunto C?	No	1
			0111011

A continuación se calcula la distancia de Hamming entre el valor obtenido y los valores correspondientes a los 16 números de la tabla inicial. Dicha distancia es simplemente el número de dígitos diferentes. En este caso,

Carta	código de Hamming	Distancia a 0111011
10C	0000000	5
9C	0001101	4
2C	0010011	2
1C	0011110	3
10P	0100110	4
9P	0101011	1
2P	0110101	3
1P	0111000	2
10R	1000111	6
9R	1001010	4
2R	1010100	3
1R	1011001	3
10T	1100001	4
9T	1101100	5
2T	1110010	3
1T	1111111	2

Como el método utilizado para construir el código de Hamming asegura que la distancia entre cualesquiera dos números es mayor o igual a tres, la distancia del número obtenido a partir de las preguntas efectuadas será mayor o igual a dos a todos los números excepto al correspondiente a su valor exacto. Si no han mentido ninguna vez, habrá una distancia igual a cero; si han mentido una vez, habrá una distancia igual a 1. El número (y la carta que representa) situado a dicha distancia será el elegido.

Una sugerencia: no tiene porqué hacerse con cartas. Pueden ser imágenes de otro tipo, animales, gráficas de colores, personajes, ..., siempre que posean cuatro propiedades dicotómicas.

Con las ideas anteriores pueden plantearse variantes del juego con una cantidad mayor de números, si se construyen adecuadamente los códigos de Hamming de números binarios con mayor cantidad de cifras. En la mayoría de textos básicos sobre teoría de códigos se incluyen tablas que especifican el número de dígitos que deben tener los códigos para representar otras cantidades de números. Por ejemplo, para una baraja española de 40 cartas, los códigos han de tener 9 cifras para poder detectar y corregir un error. Un problema interesante consiste en diseñar un programa informático mediante el cual pueda realizarse el juego de forma interactiva.

2. EL PROBLEMA DE GERGONNE (LAS VEINTIÚN CARTAS)

Se atribuye al matemático francés **Joseph Gergonne**, rector de la Universidad de Montpellier en el periodo 1830-1844 y fundador de una publicación matemática conocida como *Annales de Gergonne*, la primera versión de lo que hoy conocemos como el juego de las 21 cartas. Es actualmente muy conocido incluso entre los profanos y consiste en lo siguiente:

1. *El mago separa 21 cartas cualesquiera de una baraja y reparte con ellas sobre la mesa tres filas de 7 cartas cada una.*
2. *Un espectador piensa (sin nombrar) una de las cartas e indica en qué fila se encuentra.*
3. *El mago recoge las cartas, de modo que el montón que contiene la carta elegida quede en medio de los otros dos.*
4. *Se repite el proceso de repartir tres montones sobre la mesa dos veces más, colocando siempre el montón que contiene la carta elegida entre los otros dos.*

El resultado final de esta serie de operaciones es que la carta elegida se encuentra justamente en medio del paquete de cartas, es decir, ocupará el lugar undécimo de la baraja.

Una nueva pregunta surge en este contexto:

¿Podemos encontrar situaciones similares si el experimento se realiza con un número diferente de cartas?

Para resolver este problema, llamaremos “c” al número de montones repartidas y “f” al número de filas (o cartas en cada montón). Si p_k es la posición de la carta elegida (empezando a contar en cero) después de la k-ésima iteración, es fácil comprobar que

$$p_k = [p_{k-1}/c] + (c - 1) \cdot f/2$$

(el símbolo $[::]$ representa la parte entera del número).

Es evidente entonces que el truco funcionará siempre que después de n iteraciones se llegue a $p_n = [c \cdot f/2]$.

Ejemplos:

c=3, f=7

p_0	p_1	p_2	p_3
0,1,2	7	9	
3,4,5	8	9	
6,7,8	9	10	

9,10,11	10	10	10
12,13,14	11	10	
15,16,17	12	11	
18,19,20	13	11	

c=5, f=5

p ₀	p ₁	p ₂
0,1,2,3,4	10	
5,6,7,8,9	11	
10,11,12,13,14	12	12
15,16,17,18,19	13	
20,21,22,23,24	14	

c=3, f=5

p ₀	p ₁	p ₂	p ₃
0,1,2	5	6	
3,4,5	6	7	
6,7,8	7	7	7
9,10,11	8	7	
12,13,14	9	8	

Al observar estos ejemplos, surgen otras cuestiones relacionadas:

¿Deben ser "c" y "f" impares?

¿Cuál es el mayor número de cartas que requieren la misma cantidad de iteraciones?

Si se quiere disimular el resultado final para que la carta pensada no se encuentre en el centro de la baraja, ha de modificarse el procedimiento original. A este respecto, utilizando sistemas de numeración en base distinta de diez, puede demostrarse la siguiente propiedad.

"Es posible llevar la carta elegida a cualquier posición de la baraja".

Nos limitaremos aquí a ilustrar lo anterior mediante un ejemplo.

Ejemplo

Si $c = 3$, $f = 9$, y deseamos que la carta elegida aparezca en la posición 15, escribimos en base tres el número 14:

$$15 - 1 = 14 = 112_{(3)}$$

A continuación, basta aplicar la clave

- 0 = arriba
- 1 = centro
- 2 = abajo

y leer el número $112_{(3)}$ al revés. El proceso a seguir sería entonces:

Después del primer reparto, colocar el montón de la carta elegida abajo (debido al 2); después del segundo reparto, colocar el montón de la carta elegida en el centro (debido al 1); después del tercer reparto, dejar nuevamente el montón de la carta elegida en el centro (otra vez debido al 1).

El propio Gergonne demostró el siguiente resultado general.

Generalización de Gergonne:

“Si se reparten n^n cartas formando n filas de n^{n-1} cartas cada una, siempre se pueden combinar las filas de modo que, después de n repartos, la carta elegida aparece en cualquier posición (no necesariamente en la posición central)”.

3. JUEGOS DE COLABORACIÓN

El denominador común de los juegos que mostraremos en esta sección es el siguiente:

La acción se desarrolla con tres personajes: un espectador (E), un médium (M) y un vidente (V). Mientras el vidente está de espaldas, el espectador selecciona un conjunto de cartas y las mezcla y el médium oculta una o varias de ellas. Cuando el vidente se vuelve de cara, adivina las cartas retiradas por el médium.

Ejemplo 1

El vidente entrega cinco cartas al espectador y éste las mezcla. Manteniendo el orden final, el médium las coloca sobre la mesa en una fila y gira cara abajo tres de ellas. El vidente es capaz de adivinar la posición de las tres cartas cara abajo.

Esta primera versión está explicada por **Colm Mulcahy** en su artículo on-line. Si se quiere repetir el juego, puede hacerse en condiciones más difíciles:

El espectador mezcla diez cartas y las coloca cara arriba sobre la mesa. El médium gira cara abajo cuatro de las cartas. También en este caso el vidente puede adivinar la posición de todas las cartas.

Explicación

El principio matemático de este experimento es una aplicación, debida a **Erdős y Szekeres** en 1935, del famoso principio del palomar. Su enunciado general es el siguiente:

Sean a, b dos números naturales y $n=ab+1$. Toda sucesión x_1, \dots, x_n de n números reales diferentes contiene una subsucesión creciente (decreciente) de $a+1$ términos o una sucesión decreciente (creciente) de $b+1$ términos.

El caso $n=10$ está ilustrado por **Martin Gardner** del modo siguiente:

Si 10 soldados, todos de distinta estatura, se colocan en una fila, siempre habrá al menos 4, no necesariamente juntos, que estarán en orden, bien creciente o bien decreciente.



Paul Erdős

Otro resultado sorprendente, que involucra matrices, es el siguiente:

Si los elementos de cada fila de una matriz rectangular de números reales distintos forman una sucesión creciente, al reordenar las columnas para que formen sucesiones crecientes, las filas

siguen formando sucesiones crecientes.

De este modo, para la realización del truco, el médium buscará la mayor sub-sucesión creciente (o decreciente) de cartas después de la mezcla realizada por el espectador. Basta girar estas cartas cara abajo para que el vidente sepa a qué cartas corresponden. Como no es posible determinar de antemano si la sucesión será creciente o decreciente, el médium colocará las cartas de izquierda a derecha en el primer caso, y de derecha a izquierda en el segundo caso, para evitar dar otro tipo de codificación física.

Ejemplo 2

El espectador selecciona libremente de una baraja francesa cinco cartas, el médium oculta una de ellas y deja sobre la mesa, en una fila y caras arriba, las otras cuatro cartas. El vidente, al observar las cuatro cartas de la mesa, anuncia la carta que ha quedado oculta.

Explicación

Se atribuye al matemático **William Cheney Jr.** (primer estudiante de matemáticas que obtuvo el doctorado del MIT, en 1927) la creación de este juego y al libro de Wallace Lee, publicado en 1950, la primera manifestación escrita. Recientemente se ha despertado el interés de la comunidad educativa por este problema, debido a su potencial pedagógico y la riqueza de aspectos matemáticos involucrados. Un ejemplo que demuestra lo anterior lo proporciona el reciente artículo “Using a card trick to teach Discrete Mathematics” de **Shai Simonson y Tara Holm**.

La estrategia que proponemos a continuación puede ser utilizada por el médium y el vidente para que éste pueda deducir una carta a partir de las otras cuatro:

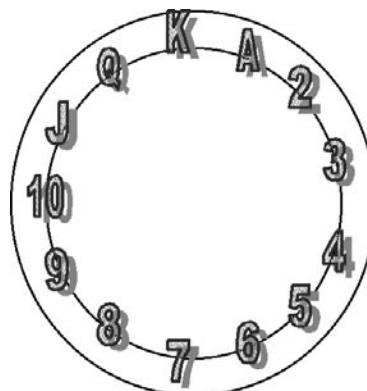
- Una vez que el espectador ha elegido cinco cartas, es seguro que habrá dos del mismo palo (por el principio del palomar). El médium debe retirar una de ellas y colocar la otra en una posición conocida por ambos (por ejemplo la segunda, para no ser demasiado evidente).
- Con las otras tres cartas debe transmitirse el valor de la carta. Sin embargo, quedan doce cartas posibles (pues hay una visible) y sólo $3! = 6$ posibles permutaciones de las tres cartas. Esto quiere decir que no basta retirar una cualquiera de las cartas del mismo palo.
- Si establecemos un orden circular en las cartas (según sus valores)

$$1 < 2 < 3 < \dots < 12 < 13 < 1 < 2 < \dots,$$

es fácil deducir que dos cartas cualesquiera pueden ordenarse de modo que estén a distancia menor o igual a seis.

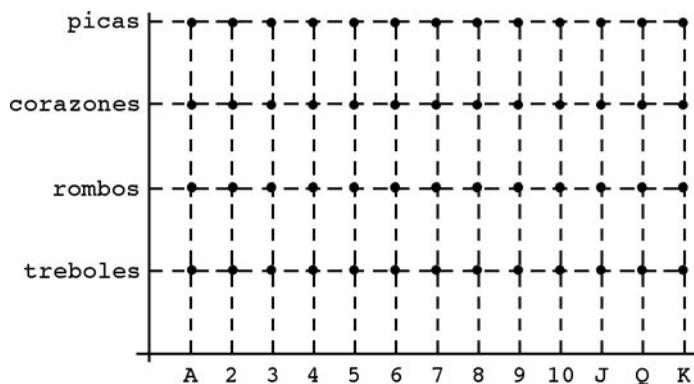
Por ejemplo, $1 < 8$ a distancia 7, pero $8 < 1$ a distancia 6.

- Esto sugiere que, si las cartas del mismo palo son P_1 y P_2 , con $P_1 < P_2$ y $P_2 - P_1 = k$ (k comprendido entre 1 y 6), la carta oculta por el médium debe ser la mayor de las dos con la precaución de que la menor esté a distancia menor o igual a seis, lo que permite conocer la carta oculta sumando a la menor el valor asignado a la permutación construida con las otras tres cartas.
- Por último, debemos ordenar el resto de las cartas según cualquier criterio convenido por el médium y el vidente. Como las cartas se determinan mediante dos coordenadas, una buena idea consiste en adoptar el orden lexicográfico: se dice que $(x, y) < (x', y')$ cuando



- i. o bien $x < x'$
- ii. o bien, $x = x'$ pero $y < y'$.

Si la primera coordenada de una carta se representa por su valor y la segunda coordenada por su palo, la fórmula anterior permite ordenar todas las cartas de la baraja.



Las tres cartas restantes se pueden ahora ordenar. Si representamos por "1" a la carta de menor valor, por "2" a la de valor intermedio y por "3" a la de mayor valor, asignamos un número a cada una de las seis permutaciones de dichas cartas. Por ejemplo:

1 2 3	→	1
1 3 2	→	2
2 1 3	→	3
2 3 1	→	4
3 1 2	→	5
3 2 1	→	6

El vidente sólo tiene que sumar el valor de la carta que representa el palo con el número resultante de la permutación formada por el médium.

La solución propuesta llenaría de satisfacción a cualquiera que la haya obtenido por sí mismo, no sólo por su belleza sino por la optimización de los recursos a nuestro alcance: se necesita conocer el palo y tenemos otra carta de su mismo palo, se necesitan seis permutaciones y contamos con tres cartas que podemos ordenar de seis formas.

A pesar de ello, la solución está muy lejos de ser óptima: en el juego propuesto, el médium envía un mensaje que consiste en un conjunto ordenado de cuatro números; hay un total de $52 \cdot 51 \cdot 50 \cdot 49$ posibles mensajes. Ahora bien, él debe escoger qué mensaje transmitir a partir de un conjunto ordenado de 5 cartas; tiene para ello $C(52, 5)$ posibilidades. Como el cociente entre el número de mensajes posibles y las posibles elecciones es 2.5, podemos aventurar que la estrategia anterior puede mejorarse ostensiblemente.

Esta argumentación permite deducir lo siguiente:

Con un conjunto de "n" cartas, si el espectador selecciona "k" de ellas y el médium oculta una, teóricamente puede transmitir con el resto un máximo de

$$n(n - 1)(n - 2) \dots (n - k + 2)$$

mensajes. Como hay un total de $C(n, k)$ posibles elecciones de las "k" cartas, el truco de transmisión es imposible si

$$C(n, k) > n(n - 1)(n - 2) \dots (n - k + 2),$$

es decir, si

$$n > k! + k - 1.$$

Esto proporciona una cota superior al número de cartas que pueden utilizarse en el juego, en relación con el número de cartas que selecciona el espectador. Por ejemplo, si el espectador elige cinco cartas ($k = 5$), no hay ninguna estrategia que permita realizar el juego con más de 124 cartas.

Queda el problema de saber si la cota superior puede alcanzarse, es decir, si existe una estrategia válida para el caso $n = k! + k - 1$. Teóricamente, una estrategia consiste en establecer una biyección entre el conjunto de mensajes posibles, es decir $V(n, k - 1)$, y el número de posibles selecciones de k cartas, o bien $C(n, k)$, pero de modo que cada mensaje contenga únicamente elementos de su imagen.

La siguiente tabla muestra los valores, tanto de las cotas superiores como del número máximo de estrategias posibles, en algunos casos particulares:

K	N máximo	Número de estrategias
3	8	6^{56}
4	27	24^{17550}
5	124	***
k	$k! + k - 1$	$k!C(k! + k - 1, k)$

Se observa fácilmente que el número de estrategias posible aumenta rápidamente lo que dificulta enormemente encontrar alguna válida.

A pesar de ello, una respuesta positiva a la pregunta de saber si la cota superior puede alcanzarse la ofrece **Michael Kleber** en el artículo que se cita en las referencias. En dicho artículo ofrece dos demostraciones: una no constructiva, basada en el teorema de Birkhoff-von Neumann sobre matrices estocásticas, y una constructiva, que proporciona un método práctico de resolución cuyo éxito depende de la capacidad de cálculo mental del médium a la hora de encontrar la codificación adecuada y del vidente para interpretar el código transmitido.

Tanto en magia como en matemáticas existe el más difícil todavía. Nos reservamos la información como un secreto profesional, pero nos gustaría apuntar que es posible realizar una interesante variante del juego anterior, que contradice lo recién expuesto:

El espectador selecciona cinco cartas cualesquiera de una baraja de 52 cartas. Él mismo elige una de ellas y la retira. Las otras cuatro cartas, en un orden apropiado, son transmitidas por el médium al vidente. A pesar de que sólo es posible realizar $4! = 24$ permutaciones con dichas cuatro cartas, el vidente es capaz de adivinar la carta retirada por el espectador.

Los lectores interesados en encontrar una solución pueden recorrer la amplia y fecunda bibliografía del gran divulgador de las matemáticas y mago de gran calidad, **Martin Gardner**. En su libro *El ahorcamiento inesperado y otros entretenimientos matemáticos* ilustra de manera teatral el juego y su correspondiente secreto.

Ejemplo 3

En esta ocasión, el espectador selecciona de una baraja francesa cuatro cartas, el médium oculta una de ellas y deja sobre la mesa las otras tres cartas. El vidente, al observar las tres cartas de la mesa, anuncia la carta que ha quedado oculta. El médium incluso puede dejar cara abajo alguna de las tres cartas que verá el vidente; aún así, el experimento de transmisión no fallará nunca.

Explicación

Vamos a considerar dos casos:

Primer caso: Entre las elegidas por el espectador hay dos cartas del mismo palo P_1 y P_2 .

Si establecemos entre las cartas el orden cíclico natural,

$$\{\text{As}, 2, 3, \dots, 10, \text{J}, \text{Q}, \text{K}, \text{As}, 2, \dots\}$$

entre P_1 y P_2 necesariamente una de ellas es mayor que la otra (supongamos que es P_2) y se encuentra a una distancia menor o igual que seis.

Entonces el médium oculta la carta P_2 , de modo que, cuando el vidente vea P_1 (que será la primera que vea de cara), sabrá el palo de P_2 y que su valor dista del valor de P_1 una cantidad comprendida entre 1 y 6. La estrategia seguida por el médium para indicar dicho número puede ser la siguiente (llamaremos I a cualquier carta indiferente y por  a la carta mostrada de dorso):

P_1			\rightarrow	$P_1 + 1$
	P_1		\rightarrow	$P_1 + 2$
		P_1	\rightarrow	$P_1 + 3$
P_1	I		\rightarrow	$P_1 + 4$
P_1		I	\rightarrow	$P_1 + 5$
	P_1	I	\rightarrow	$P_1 + 6$

Segundo caso: Todas las cartas C_1, C_2, C_3, C_4 elegidas por el espectador son de distinto palo.

Asignamos a cada palo un valor numérico (por ejemplo en el Bridge se utiliza la equivalencia trébol = 0, rombo = 1, corazón = 2, pica = 3).

Ahora llamamos r al resto de la división por cuatro de la suma $C_1 + C_2 + C_3 + C_4$ y el médium oculta la carta cuyo palo coincide con r (según la equivalencia citada) que supondremos es C_4 .

Cuando el vidente ve las otras tres cartas cara arriba, sabe el palo que falta y, cuando calcula el resto de la división por cuatro de $C_1 + C_2 + C_3$, que llamaremos s , sabe también que el resto de la división de C_4 por 4 es $r - s$. Quedan sólo cuatro posibilidades:

- Si $r - s = 1$, la carta sólo puede ser un As, 5, 9, K;
- si $r - s = 2$, la carta sólo puede ser un 2, 6, 10;
- si $r - s = 3$, la carta sólo puede ser un 3, 7, J;
- si $r - s = 0$, la carta sólo puede ser un 4, 8, Q.

Con las tres cartas mostradas se pueden realizar seis permutaciones, si se ordenan adecuadamente (en primer lugar mediante el orden natural del valor de las cartas y, en caso de haber dos o más cartas con el mismo valor, por el orden de los palos, que puede ser el indicado anteriormente), así que basta ordenar las tres cartas según las permutaciones 123, 132, 213, 231, para codificar la carta oculta.

No deja de ser sorprendente el hecho de que el problema es más difícil que el anterior y, sin embargo, de la solución se desprende que queda margen para deducir más cartas si las hubiera.

4. PROBLEMAS ABIERTOS

(a) Una vez resuelto el problema de adivinar un número pensado a través de una serie de preguntas si se permite alguna respuesta falsa, es natural preguntarse si puede generalizarse al caso donde se permita más de una mentira. En primer lugar es necesario saber si existe algún código que permita detectar y corregir más de un error.

Profundizando un poco más en el estudio de la teoría de códigos, pueden plantearse casos cuya solución es positiva. Ahora bien, no es suficiente saber que existen tales códigos. Nos interesa determinar un método práctico que funcione como en el caso desarrollado en la sección 1.

(b) El problema de las cinco cartas, estudiado en la sección 3, puede generalizarse en otra dirección, como plantea **Eric Farmer**:

De una baraja con “n” cartas, un espectador selecciona “k” de ellas y el médium elige entre ellas “m” cartas, las cuales muestra al vidente. Con esta información, el vidente adivina las $k - m$ cartas restantes.

Con este enunciado, el problema de Cheney corresponde al caso $n = 52$, $k = 5$, $m = 4$. Si razonamos de forma análoga al caso antes desarrollado, sabemos que existen $m! C(k, m)$ posibles mensajes y $C(n - m, k - m)$ posibles selecciones, de modo que sólo puede haber solución cuando

$$m! C(k, m) \geq C(n - m, k - m),$$

es decir cuando

$$k! (n - k)! \geq (n - m)!$$

Desconocemos la existencia de una estrategia óptima para este problema. Dejaremos al lector la búsqueda de una solución para un caso sencillo: $n = 13$ (es decir, donde se utilizan todas las cartas de un mismo palo), $k = 8$, $m = 3$.

AGRADECIMIENTOS

Tanto en el entorno mágico como en la comunidad matemática, hay personas que reconocen el interés educativo que proporcionan estos y otros juegos de magia con gran contenido matemático. En especial, los compañeros del departamento de Matemáticas de la Universidad del País Vasco, **Jesús Gómez y Julián Aguirre**, me han planteado y resuelto problemas de esta índole; el compañero mago **Juan Carlos Ruiz de Arcaute** ha colaborado también elaborando los programas que permiten realizar los juegos anteriores con ayuda de un ordenador (algunos de ellos se encuentran en la página web www.todomagia.com/automagia).

BIBLIOGRAFÍA

Brain Epstein: *All you need is cards*, en “Puzzlers’ Tribute” (David Wolfe y Tom Rodgers, eds.).

Colm Mulcahy, 2000: *Mathematical Card Tricks* en AMS.

Michael Kleber, 2002: *The Best Card Trick*, en “Mathematical Intelligencer” 24.

Wallace Lee, 1950: *Math Miracles*, ed. Mickey Hades.