CODIS DE HAMMING

JOAQUIM ORTEGA CERDÀ

Codis de Hamming. Al codi original de Hamming volem transmetre 4 bits (0 o 1) que diem c_3, c_5, c_6, c_7. A més per cada 4 bits que volem transmetre afegirem 3 bits de control c_1, c_2, c_4. Aquests dígits de control els triarem de manera que

$$c_1 + c_3 + c_5 + c_7 \text{ sigui parell}$$
$$c_2 + c_3 + c_6 + c_7 \text{ sigui parell}$$
$$c_4 + c_5 + c_6 + c_7 \text{ sigui parell}$$

Això sempre ho podem fer. Per exemple si $c_3 = 0$, $c_5 = 1$, $c_6 = 1$ i $c_7 = 0$ aleshores $c_3 + c_5 + c_7 = 1$ i de la primera equació veiem que $c_1 = 1$. De la mateixa manera $c_3 + c_6 + c_7 = 1$ i la segona equació força que $c_2 = 1$. Finalment $c_5 + c_6 + c_7 = 2$, i per la tercera equació $c_4 = 0$.

Transmetem per wifi $c_1, c_2, c_3, c_4, c_5, c_6, c_7$ i rebem $x_1, x_2, x_3, x_4, x_5, x_6, x_7$. Aquest nous bits poden tenir errors de transmissió. Si només ens equivoquem un cop ho veurem de seguida, ja que $x_1 + x_3 + x_5 + x_7$ serà senar, o $x_2 + x_3 + x_6 + x_7$ serà senar, o $x_4 + x_5 + x_6 + x_7$ serà senar.

Com corregir l'error? Suposem que hem fet un error en la transmissió (i només un). Veiem ara com reparar-lo. Definim unes variables auxiliars z_1, z_2, z_4 de la següent manera:

Si la primera equació $x_1 + x_3 + x_5 + x_7$ és senar diem $z_1 = 1$ i si és parell $z_1 = 0$.

De la mateixa manera si $x_2 + x_3 + x_6 + x_7$ és senar diem $z_2 = 1$ i si és parell $z_2 = 0$.

Finalment si $x_4 + x_5 + x_6 + x_7$ és senar diem $z_4 = 1$ i si és parell $z_4 = 0$.

Si no hi ha errors $(z_1, z_2, z_4) = (0, 0, 0)$. Si hi ha un error aleshores aquest es troba en el bit de posició $z_1 + 2z_2 + 4z_4$. Es pot comprovar cas a cas.

Date: Novembre, 2017.

Un exemple. Anem a veure un cas a tall d'exemple. Suposem com abans que $(c_3, c_5, c_6, c_7) = (0, 1, 1, 0)$. Com hem vist això diu que $(c_1, c_2, c_4) = (1, 1, 0)$ i tots junts fan

$$(c_1, c_2, c_3, c_4, c_5, c_6, c_7) = (1, 1, 0, 0, 1, 1, 0).$$

Transmetem i suposem que fem un error en un bit. Per exemple $c_4 = 0$ passa a ser $x_4 = 1$ i els altres bits es transmeten be. Aleshores

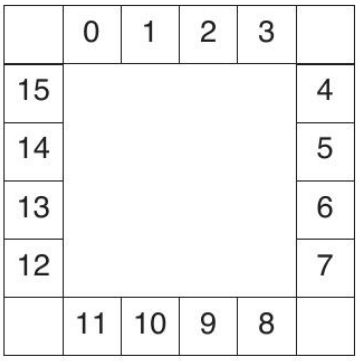
$$(x_1, x_2, x_3, x_4, x_5, x_6, x_7) = (1, 1, 0, 1, 1, 1, 0).$$

Calculem ara (z_1, z_2, z_4). En aquest cas, com que $x_1 + x_3 + x_5 + x_7 = 2$ aleshores $z_1 = 0$. Com que $x_2 + x_3 + x_6 + x_7 = 2$, aleshores $z_2 = 0$ i $x_4 + x_5 + x_6 + x_7 = 3$ i per tant $z_2 = 1$. El bit incorrecte segons el mètode de Hamming és el $z_1 + 2z_2 + 4z_4 = 4$. Això és correcte, ja que havíem canviat el bit $c_4 = 0$ per $x_4 = 1$.

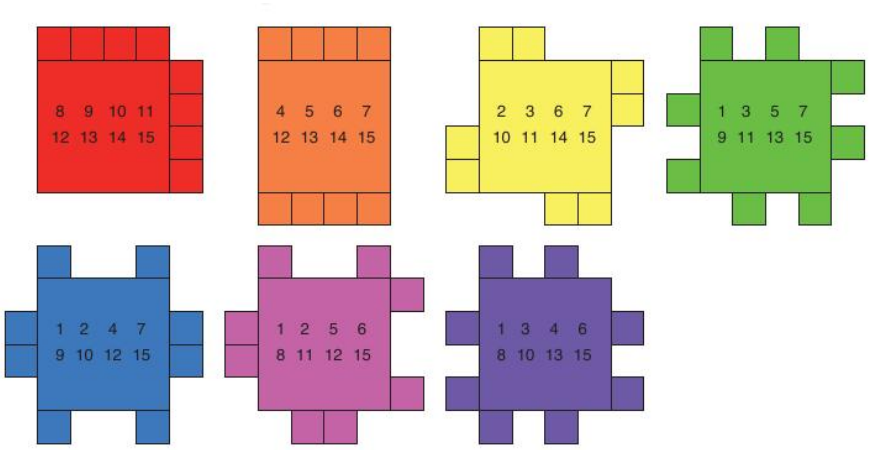
Un joc utilitzant aquest codi

Presentem un joc de màgia introduït per Richard Erenborg en 2006, i millorat per Todd Mateer el 2013, basat en el codi de Hamming anterior.

El joc té una base blanca, com en la figura,

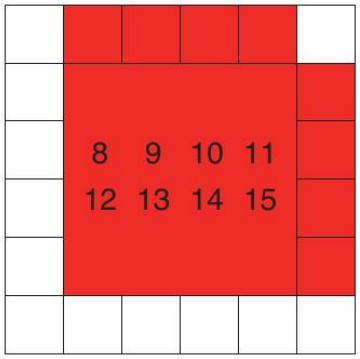


amb nombres del 0 al 15 marcats (alternativament es poden memoritzar les posicions i no escriure els nombres a la base per fer més impressió). També tenim 7 cartes de color, cadascuna amb 8 nombres impresos, com a la segona figura.

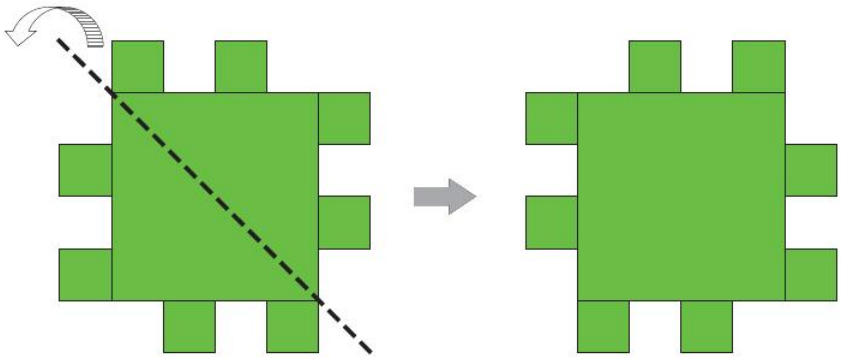


El joc consisteix en el següent. Es demana a un voluntari que esculli un nombre (del 0 al 15). Després se li ensenyen d'una en una les set cartes de colors i a cada carta se li pregunta si el nombre que ha pensat figura o no en la carta de colors. El voluntari ha de contestar sempre la veritat excepte en un dels colors. Un cop donades les respostes el "mag" pot encertar quin és el nombre triat i quina és la carta on ha mentit el voluntari.

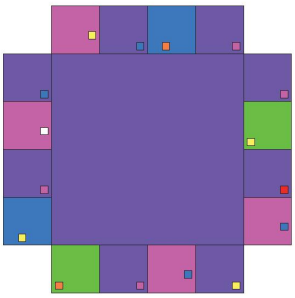
Tal com funciona el truc és el següent. Quan el voluntari diu "Sí" la carta de colors es situa sobre la carta blanca base amb els nombres cap endavant. Per exemple si el nombre triat és el 8 i ensenyem la carta vermella i el voluntari diu que sí aleshores la situem com a la figura:



Si el voluntari en canvi diu que el nombre no és en la carta (perquè realment no hi és o perquè decideix mentir en aquesta ocasió) aleshores abans de situar la carta sobre la base la girem, com a la figura:



Al final de tot tindrem una pila amb la carta base i les set cartes de colors com en la figura:



El nombre escollit és aquell que té només una carta sobre la pestanya i aquesta carta és exactament en la que el voluntari ha mentit. Es pot detectar fàcilment ja a través dels forats (que estan situats en zones diferents de la pestanya) s'ha de veure el fons blanc de la carta base. En el cas del dibuix el nombre triat seria el 14 i fúcsia el color de la carta on el voluntari ha mentit. Hi ha una aplicació per Mathematica en el disc Z dels ordinadors amb nom: HammingMagicTrick.cdf

Si voleu descarregar-vos els fitxer pdfs amb les fitxes, els podeu trobar en: http://maa.org/mathhorizons/supplemental.htm

Com és que funciona. Els nombres del 0 al 15 es poden codificar en 4 bits utilitzant la base 2, com a la taula de sota. Cada carta conté 8 nombres. El fet que el nombre sigui o no a la carta dona una informació sobre el nombre (un bit). Per tant, com que ens donen informació sobre set cartes tenim set bits de informació. En la transmissió de fet es perd un bit (hi ha una carta en la que el voluntari ens menteix). No sabem d'entrada quina carta és (quin bit és). Però justament aquesta és la situació dels codis de Hamming que transmetem 7 bits. Un pot

ser erroni però podem encara recuperar els 4 bits d'informació que codifiquen el nombre desitjat.

Una mica més. Intenteu ara fer una versió més simple de aquest joc. Heu de dissenyar només 4 cartes similars a les del joc anterior que permetin endevinar el nombre escollit (entre 0 i 15). Ara les regles del joc són més simples. El voluntari ha de dir si en cada carta el nombre hi és o no, però no està permès dir cap mentida.

Recordeu que els nombres del 0 al 15 s'escriuen base 2 de la següent manera:

Decimal	Binari	Decimal	Binari
0	0000	8	1000
1	0001	9	1001
2	0010	10	1010
3	0011	11	1011
4	0100	12	1100
5	0101	13	1101
6	0110	14	1110
7	0111	15	1111

Referències

[1] R. Ehrenborg *Decoding the Hamming code* Math Horizons, 13 (2006), 16–17.
[2] R. W. Hamming, *Error detecting and error correcting codes*, Bell System Tech. J. 29 (1950) 147–160.
[3] T. Korner *Coding and Criptography* https://www.dpmms.cam.ac.uk/∼twk/Shan.pdf
[4] T. Matter *A Magic Trick Based on the Hamming Code*, Math Horizons 11, 2013.