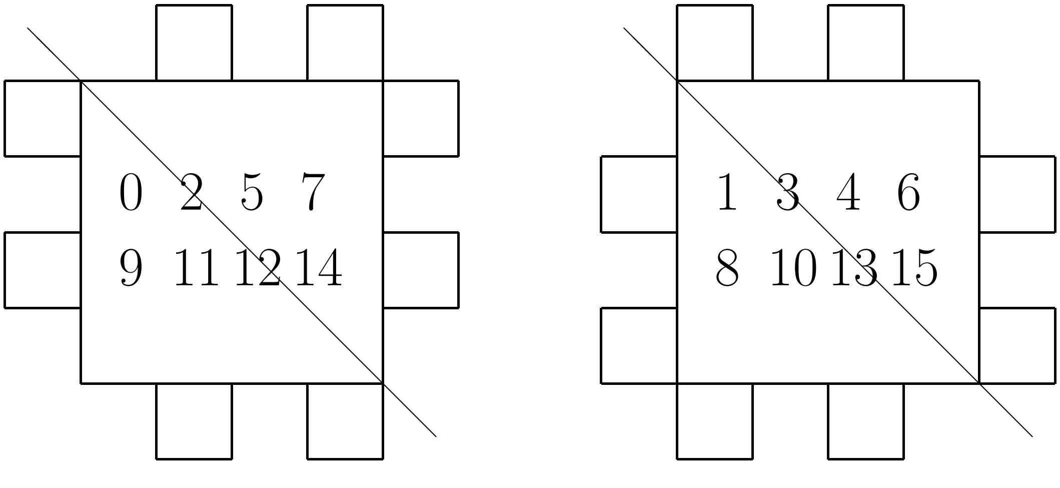
Decoding the Hamming code*

Richard EHRENBORG

A friend thinks of an integer between 0 and 15. You are allowed to ask seven yes/no-questions in order to determine which number your friend has in mind. However, he is allowed to tell at most one lie. Can you do this task?

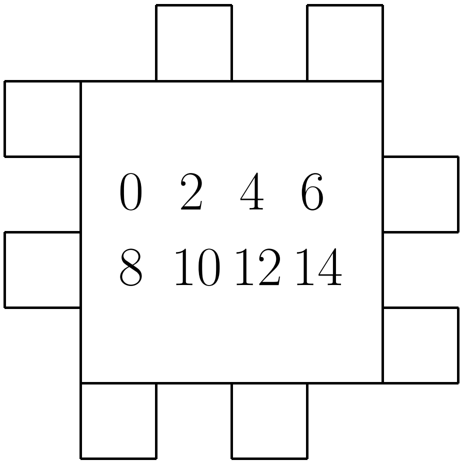
The theory of error correcting codes says that you can do it. In fact, this problem is solved by the Hamming code of length 7, with 4 information bits [2]. However, the practical question remains, can you find the number while standing on your feet together with your friend.

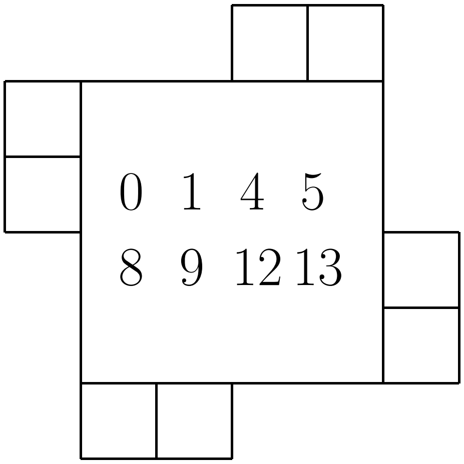
This note presents seven question cards and one base card allowing you to do this feat. Each card encodes one question. Depending on the answer, the card is either placed right-side up or turned upside-down. Below is one of the cards and how it looks when turned over the northwest-southeast axis.

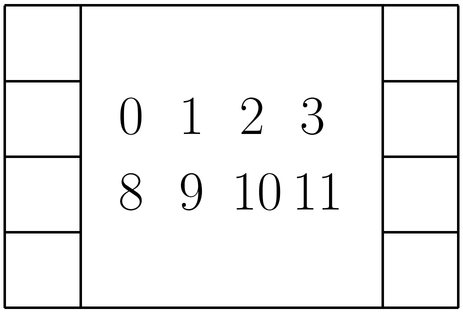


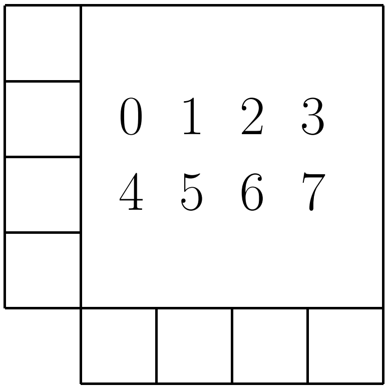
Observe how the set of numbers on each side are complements. Moreover, the teeth of both sides of the card also complement each other. The other six cards of the seven cards are as follows, where we only show one side of each card.

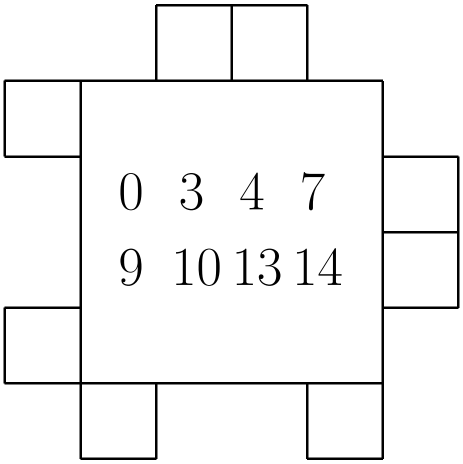
*Appeared in Math Horizons, special issue on Codes, Cryptography and National Security, **13** (2006), 16–17.

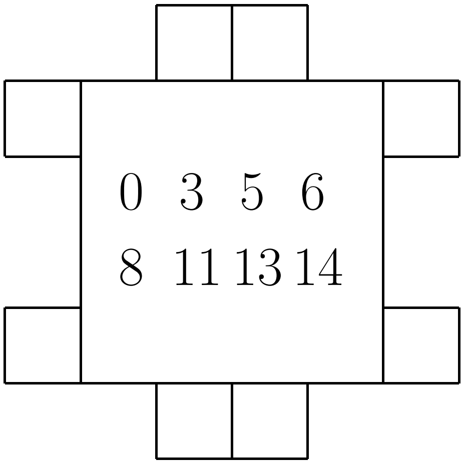

0 2 4 6
8 10 12 14


0 1 4 5
8 9 12 13

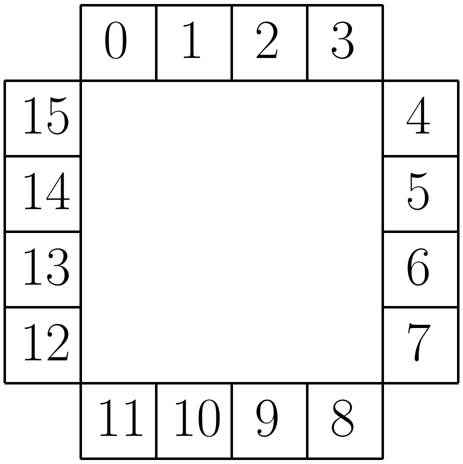

0 1 2 3
8 9 10 11


0 1 2 3
4 5 6 7


0 3 4 7
9 10 13 14


0 3 5 6
8 11 13 14

The base card is as follows.



Proceed as follows: For each question card ask your friend if the chosen number is among the following numbers and read the numbers on one side of the card out loud. If he answers yes, place the card on the base card such that the side you read is showing. If the answer is no, place the other side up. After repeating this procedure for the seven question cards you have two cases: either exactly one number is not covered or all the numbers are covered. In the first case he has been truthful in all seven questions and the sought after integer is showing. In the other case he lied once. Now you have the straightforward task to locate the unique number covered by at most one card. This number is the sought after integer. Moreover, you can tell which question your friend lied.

Observe that you may use the cards in any order and vary which side of the cards you are reading. This is very good thing to do in order to add to the effect of the performance.

Why does this card trick work? Recall that the classical Hamming code is a set of 16 vectors in the vector space $\mathbb{Z}_2^7 = \{0,1\}^7$ called codewords. This collection can be described either as the null space of the matrix

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

or as the polynomials $a_0 + a_1 x + \cdots + a_6 x^6$ in $\mathbb{Z}_2[x]$ that are divisible by $1 + x + x^3$. Two different codewords differ in at least 3 positions. Hence when given a word that differs in one position (the error) from a codeword, the codeword is uniquely determined.

Each number 0 through 15 corresponds to a codewords and each card is associated with one bit. Thus when asking the 7 questions one is determining a codeword or a codeword with one bit error. If your friend is truthful the correct number will be uncovered. If he lies exactly once, we have received one bit with an error, and the correct number will be covered by exactly one card. If he lies more than once, the Hamming code is helpless and will decode incorrectly.

To understand the null space description of the code can be an extra topic in a linear algebra class using matrix multiplication modulo 2. The other description is an application of the field with 8 elements and can be done in an abstract algebra class. See Childs' text [1] for both of these approaches.

References

[1] L. N. Childs, *A Concrete Introduction to Higher Algebra, second edition,* Springer-Verlag, New York, 1997.

[2] R. W. Hamming, Error detecting and error correcting codes, *Bell System Tech. J.* **29** (1950) 147–160.

Richard Ehrenborg, Department of Mathematics, University of Kentucky, Lexington, KY 40506-0027