FROM A PRESENTATION GIVEN AT THE "WHAT IS?" SEMINAR AT
THE OHIO STATE UNIVERSITY

Ulam's Game and Error Correcting Codes

Andrew Krieger
July 10, 2012

1 INTRODUCTION AND CONVENTIONS

Ulam's Game: Guess a number ($0 \le n < N$, say $N = 1,000,000$) by asking a series of yes-or-no questions. The Responder may lie at most once.

Often, we will want to consider the binary expansion of a number $b = \sum_{i=1}^{\infty} 2^{i-1} b_i$. I will write (for example) $13 = 1101_2$ to invoke the binary expansion of a particular integer. In this example, $b = 13$ and $b_1 = 1, b_2 = 0, b_3 = 1, b_4 = 1$, and $b_m = 0$ for $m > 4$. I will refer to the $\{b_i\}$ as the *bits* of b, where b_1 is the first bit, b_2 is the second bit, and so on.

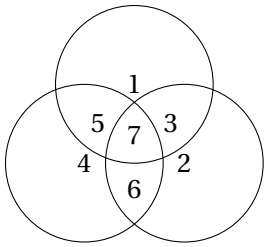
2 A SIMPLER PROBLEM

Following the work of Niven [1]

First solve a simpler game, where $0 \le n < 16$ (with at most one lie).

We will use four data bits to encode the binary expansion of $n = (n_4 n_3 n_2 n_1)_2$. However, we will relabel the bits as $b_3 = n_1, b_5 = n_2, b_6 = n_3, b_7 = n_4$. The remaining bits will satisfy the following relations (illustrated in the diagram on the right):

$$b_1 = b_3 + b_5 + b_7$$
$$b_2 = b_3 + b_6 + b_7$$
$$b_4 = b_5 + b_6 + b_7$$



When decoding, if there are no lies, all of these relations will still hold.

If the Responder lied about bit 0, then all of the equations above will be false.

If the Responder lied about bit 1, then the first two equations will be false, but the last will still be true.

Finally, if the Responder lied about bit 4, then only the first equation will be false, and the other two will hold.

In each case, we can determine when the Responder lied, correct the data (if necessary), and guess the actual number.

3 Extending the Solution

Also as per Niven [1]

To extend this solution to $0 \le n < 1{,}000{,}000$, we will organize the parity bits in a more logical way. Define the following sets, based on the binary expansions of their members:

Set	Members	Description
S_0	$\{1,3,5,7,9,11,13,15,17,19,21,23,25\}$	Bit 1 is 1
S_1	$\{2,3,6,7,10,11,14,15,18,19,22,23\}$	Bit 2 is 1
S_2	$\{4,5,6,7,12,13,14,15,24,25\}$	Bit 3 is 1
S_3	$\{8,9,10,11,12,13,14,15,24,25\}$	Bit 4 is 1
S_4	$\{16,17,18,19,20,21,22,23,24,25\}$	Bit 5 is 1

The bits b_{2^j} will be used as parity bits. The parity bit b_{2^j} will be the sum of all bits b_i where $i \in S_j$, that is, the bits b_i where the binary expansion of i has a one in the $(j+1)^{\text{th}}$ place. Using these parity bits, we can determine which bit is incorrect.

The construction is easily expanded to create arbitrarily long Hamming codes by continuing the patterns for S_j.

4 Hamming Codes

As presented in [2], or any book on coding theory

Hamming distance: A metric on a code $\mathscr{C}$ given by $d(\mathbf{u},\mathbf{v}) = \#\{i \in \mathbb{N} | u_i \neq v_i\}$ for $\mathbf{u} = (u_1,\ldots,u_s), \mathbf{v} = (v_1,\ldots,v_s) \in \mathscr{C}$

Any code can correct (up to) $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ errors, where $d = \min d(\mathbf{u},\mathbf{v})$ over all distinct $u, v \in \mathscr{C}$

Also, any code can detect (but not correct) up to $d-1$ errors

Hamming sphere-packing bound: $M\left(1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{t}(q-1)^t\right) \le q^n$, where:

M is the number of code words — n is the length of the code words
q is the radix (eg $q = 2$ for a binary code) — $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ is the number of errors that $\mathscr{C}$ can correct.

Perfect Code: Equality in the sphere-packing bound. An example is a Hamming code. The significance is that the Hamming code uses all available space, so it is maximally efficient while correcting 1 error.

5 Hamming Codes in Ulam's Game

Niven's solution (above) for the game with $0 \le n < n$ requires the following number of questions:

$$f(N) = m + r = m + 1 + [\log_2(m + 1 + \log_2 m)], \text{ where}$$

$m = 1 + [\log_2(N-1)]$ is the number of bits in the binary expansion of $N-1$
r is the unique positive integer satisfying $2^{r-1} < m + r < 2^r$.

An optimal solution of Ulam's Game with $0 \le n < N$ (with feedback) requires

$$g(N) = \min h \text{ such that } \begin{cases} N(h+1) \le 2^h & \text{if N is even} \\ N(h+1) + (h-1) \le 2^h & \text{if N is odd} \end{cases}$$

So, $g(2^m) = h$ such that $2^m(h+1) \le 2^h \iff h + 1 \le 2^{h-m} \iff h < 2^{h-m}$.

Write $r = h - m$; then $h < 2^{h-m} \iff m + r < 2^r$, so Niven's solution is optimal if N is a power of two.

The result cannot be directly extended to all N; however, for any N, either $f(N) = g(N)$ or $f(N) = g(N) + 1$

REFERENCES

[1] Ivan Niven, *Coding Theory Applied to a Problem of Ulam*. Math. Mag. 61 (1988) 275-281.

[2] Gareth A Jones and J. Mary Jones, *Information and Coding Theory*. Springer-Verlag, London, 2000.

[3] Andrzej Pelc, *Solution of Ulams problem on searching with a lie*. J. Combin. Theory Ser. A 44 (1987) 129-140.