Richard W. Hamming

Learning to Learn

The Art of Doing Science and Engineering

Session 12: Error-Correcting Codes

How Great Things Are Done

I invented error correcting codes.

You know they are important.

What follows is how it happened.

Great Scientists

Feinman, Metropolis, Oppenheimer, Bohr, Teller and Farame

- I met these people at Los Alamos
- There, as a "janitor of science," I just kept the machines going
- What was the difference between them and me?
- Pasteur quote: "Luck favors the prepared mind."
- Study successes not mistakes!

Extreme Interest in Matters

When you're up at bat, you think about hitting the ball. You don't think about how.

- I can tell you what happened at the conscious level and a slight probing of the unconscious
- The great stuff comes from people who care and care passionately
- Many people are content to just do things well
- Some great scientists sterilize themselves by inventing a great idea, but then forever dwell on it

How It Happened

Two out of five code relay computer, circa 1947-48, could detect errors.

If it detected an error, it would try three times before dropping the problem to pick up the next.

Insight: if a machine can find out if there is an error, why can't it find out where it is?

Error Correction

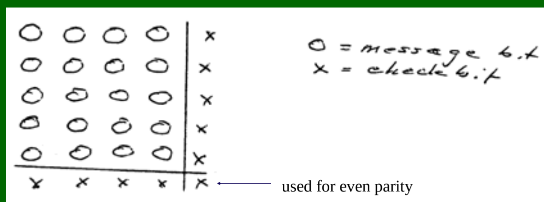
Brute force method:

- Build three machines
- Build inter-comparing circuits
- Take the majority vote
- Not really feasible, too expensive!

A better method: parity checks.

Rectangular Form

Arrange the message bits of any message symbol in a rectangle. A single error will divulge its (row, column) coordinate.



Redundancy Ratio

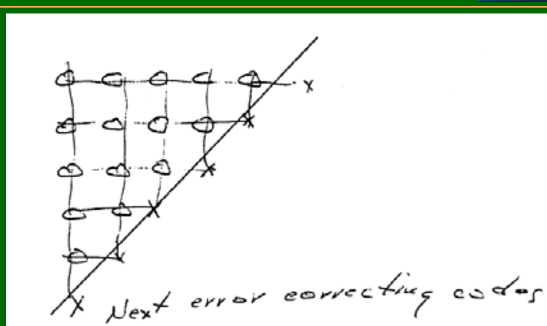
The closer the rectangle is to a square, the lower the redundancy for the same amount of message.

$$R = \frac{mn}{(m-1)(n-1)}$$

$$= 1 + \frac{1}{(m-1)} + \frac{1}{(n-1)} + \frac{1}{(m-1)(n-1)}$$

However, there is a risk of double error! Exercise your engineering judgment.

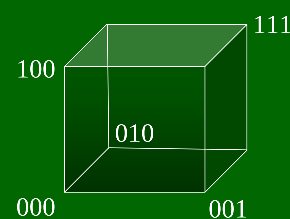
A Better Form - Triangular



A Cube of Bits

Parity checks across entire planes and parity check on all three axes can provide coordinates of error.

Cost: (3n – 2) parity checks for n^3 encoded message.



n Dimensions

Review Lecture 9

- No need to build n dimensions, just wire it that way
- An n-dimensional cube will have (n + 1) parity checks
- (n + 1) parity checks represent 2^{n+1} different things
- Need only 2^n points in a cube plus 1 result that the message is correct
- This will be off by a factor of 2!

Syndrome

Have the syndrome of the error name the place of the error – a binary number.

1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000
9	1001

Parity check #1	1, 3, 5, 7, 9,11,13,15,...
Parity check #2	2, 3, 6, 7,10,11,14,15,...
Parity check #3	4, 5, 6, 7,12,13,14,15,...
Parity check #4	8, 9,10,11,12,13,14,15,...
etc.	

Parity check bits involve ones in the position of the check.

Checking the Syndrome Approach

An even parity example check of 4 message and 3 check positions must satisfy the condition: $2^3 \ge 7+1$

1	2	3	4	5	6	7	position
		1		0	0	1	message
0	0	1	1	0	0	1	encoded message
0	0	1	1	0	1	1	message with error

Apply Parity Checks

0	0	1	1	0	1	1	message with error

1 3 5 7 → 0

2 3 6 7 → 1

4 5 6 7 → 1

Binary number 110 → 6

This result locates the error. Flip 6th bit, strip out check bits, regain original message!

Single Error Correct, Double Detect

Add a single new parity check over the whole message

- Single-error correct (SEC) double-error detect (DED) is a good balance
- For short message, redundancy of 4 message and four check bits, bad
- If message is too long, you risk double uncorrectable error: SEC/DED will mistakenly overcorrect into a third error!

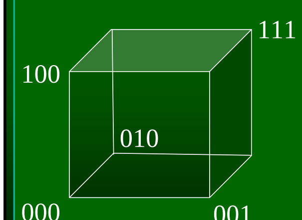
Working in L1 Space

The conventional conditions on a metric D(x,y) between two points x and y are:

1. $D(x,y) \ge 0$ (non negative)
2. $D(x,y) = 0$ if and only if $x = y$ (Identity)
3. $D(x,y) = D(y,x)$ (symmetry)
4. $D(x,y) + D(y,z) \ge D(x,z)$ (triangle inequality)

A Cube of Bits (Revisited)

Vertices are fixed at 1 unit, 2 units and 3 units away from the origin



min. distance	meaning
1	unique decoding
2	single error detecting
3	single error correcting
4	1 error correct and 2 error detect
5	double error correcting
2k + 1	k error correction
2k + 2	k error correction and k-1 error detection

Higher Minimum Distance Codes

$$\frac{2^n}{1+C(n,1)+C(n,2)+...+C(n,k)} \ge \#\,of\,spheres$$

k = sphere radius

C(n, k) = # of points in a sphere of radius k

2^n = whole space

This quotient represents the upper bound on the number of non-overlapping spheres and code points in the corresponding space.

Finding an Error Correcting Code

Same as finding a set of code points in the n-dimensional space that has the required minimum distance between legal messages.

- Minimum distance function is both necessary and sufficient
- Some error correction can be exchanged for more detection, i.e. give up one error correction and get two more in error detection

Why Error Correction?

Space vehicles operating on possibly as low as 5 watts can have hundreds of errors in a single block of message.

When you are not prepared to overcome “noise” or “deliberate jamming” then such codes are the only known answer.