THE BITS BETWEEN THE BITS

1. Error-correcting codes

2. Sphere packings and lattices

3. Sporadic simple groups

1947: Richard W Hamming (Bell Labs)...

> *Two weekends in a row I came in and found that all my stuff had been dumped and nothing was done. I was really aroused and annoyed because I wanted those answers and two weekends had been lost. And so I said 'Damn it, if the machine can detect an error, why can't it locate the position of the error and correct it?'*

The problem:

Reliable transmission of data over a noisy channel

$$\equiv$$

Reliable storage of data on fallible media

Shannon's theorem

As long as the information transfer rate over the channel is within the channel capacity (or **bandwidth**), then it is possible to construct a code such that the error probability can be made arbitrarily small.

Costs of increased reliability:

- transfer rate decreased
- code becomes more complex

Error-detecting codes

We want to be able to tell, upon receiving a message, whether the message has been corrupted in transit.

Repetition codes

SSeenndd eeaacchh ccooddeewwoorrdd ttwwiiccee.

For example, encode ‘1100’ (12) as ‘11001100’

The first four bits are the message, and the next four are the **check bits** or **check digits**.

This code detects any one error in transmission and is the (8,4) **block repetition code**.

Generalise to:

- (rs, r) block repetition code
- (n, r) block code

Define the **information rate** of an (n, r) binary code with w codewords to be:

$$R = \frac{\log_2 w}{n}$$

If $w = 2^r$, for example, then $R = \frac{r}{n}$.

So, the higher the number of check bits (and hence the more reliable the code), the lower the information rate.

The problem is now to devise a code which maximises reliability and information rate, while still allowing detection of transmission errors.

PARITY CHECK CODES

Append to each 4-bit block (‘*nybble*’) another bit (the **parity bit**) making the sum of the bits even ($\equiv 0 \mod 2$).

Information rate: $R = \frac{4}{5}$ – much better than the (8,4) block repetition code.

In general, the $(r+1, r)$ **parity check code** has information rate $R = \frac{r}{1+r}$.

Error-correcting codes

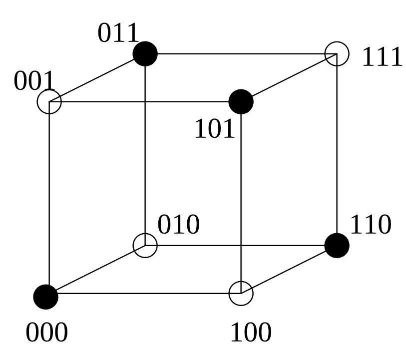
Error-detection is all well and good, but not enough in certain circumstances (like a compact disc, or remote-piloting unmanned space probes). We need to be able to figure out what the message should have been.

[Hamming 1950]: Geometric approach.

Consider the unit cube in $\mathbb{R}^n$ whose vertices are the 2^n n-tuples of 0s and 1s; the binary expansions of $0, \ldots, 2^n - 1$.

The (3,2) parity check code

The codewords of this (single-error-detecting) code are the four 3-bit binary numbers with an even number of 1s:



HAMMING DISTANCE

The **Hamming distance** $D(x, y)$ is the number of bits which differ between the codewords x and y.

This is the number of edges in a shortest path between the two vertices of the unit n-cube corresponding to the codewords.

The **minimum distance** d of a code is the minimal distance between any two non-identical codewords. For the (3,2) parity check code $d = 2$.

The (4,1) repetition code (consisting of codewords 0000 and 1111) has minimum distance 4 – any two errors can be detected. In addition, any single error can be corrected.

In general, a code with minimum distance d will detect up to $\left[\frac{d}{2}\right]$ errors and will correct up to $\left[\frac{d-1}{2}\right]$ errors.

HAMMING SPHERE

The **Hamming sphere** of radius ε centred on a vertex of the unit cube in $\mathbb{R}^n$ is the set of all vertices at a Hamming distance of at most ε from the given vertex.

A code of length n is said to be **perfect** (or **close-packed** or **lossless**) if there is an $\varepsilon \geqslant 0$ such that:

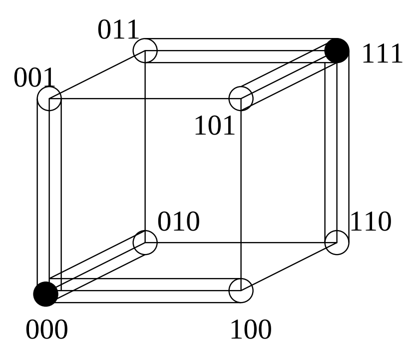
- The ε-spheres centred on the codeword vertices are pairwise disjoint.

- Each vertex of the n-cube is contained in some ε-sphere

The $(n, n-1)$ repetition codes with n odd are all perfect

(take $\varepsilon = \frac{n-1}{2}$).

The Hamming spheres of radius 1 for the (3,1) repetition code are:



THE (7,4) HAMMING CODE $\mathcal{H}_7$

The requirements of this code are that the checking number (three bits) should locate any single error in a codeword. Rather than placing the check bits at the end, Hamming put the ith check bit at the 2^{i-1}th position. This has the result that no two check bits check each other.

The essential idea is that the ith parity bit should check the parity of the positions with a 1 in their ith position.

So, the first check bit checks the parity of bits 1,3,5,7, the second checks bits 2,3,6,7, and the third checks bits 4,5,6,7, with the check bits themselves in positions 1,2 and 4.

The idea is that if no error occurs then the check number should be 000.

This (7,4) code is perfect.

In fact, all the $(2^k - 1, 2^k - 1 - k)$ Hamming codes are perfect.

Suppose we wish to encode the number 0101:

Position	7	6	5	4	3	2	1
Message data	0	1	0		1		
Check data				1		0	1
Codeword	0	1	0	1	1	0	1

If, during transmission, this particular codeword is corrupted:

$$0101101 \mapsto 0001101$$

The parity checks are then:

$$\begin{array}{ll} \text{Bits 4,5,6,7:} & 1+0+0+0 \equiv 1 \pmod 2 \\ \text{Bits 2,3,6,7:} & 0+1+0+0 \equiv 1 \pmod 2 \\ \text{Bits 1,3,5,7:} & 1+1+0+0 \equiv 0 \pmod 2 \end{array}$$

The checking number is thus 110, so the error is in the 6th position.

We can regard the (n, r) Hamming codes as vector subspaces of $\mathbb{F}_2^n$, since the sum of any two codewords is itself a codeword.

Any code which may be thought of in this way is said to be **linear**.

In fact, since only words with check digits 000 are valid codewords, we can regard the (7,4) Hamming code as the kernel of some linear map $\mathbb{F}_2^7 \to \mathbb{F}_2^3$.

A suitable matrix for this map is:

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

In general, if a code can be regarded as the kernel of some linear transformation with matrix H, then H is the **generating matrix** or **parity check matrix** for the code.

GOLAY CODES

1950s: Marcel Golay extended Hamming's ideas to construct perfect single-error-correcting codes on p symbols for any prime p.

A necessary condition for the existence of a perfect binary code which can correct more than one error, is the existence of three or more first numbers of a line of Pascal's triangle which add up to an exact power of two.

A possible candidate is:

$$\binom{90}{0} + \binom{90}{1} + \binom{90}{2} = 2^{12}$$

This suggests the existence of a perfect, double-error-correcting (90,78) code, but it was proved by Golay and Zaremba that no such code exists.

The second candidate that Golay found is:

$$\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2^{11}$$

This suggests the existence of a perfect 3-error-correcting (23,12) binary code.

This code ($\mathcal{C}_{23}$) does exist, and Golay constructed a generating matrix for it.

Golay also constructed an (11,6), double-error-correcting ternary code, $\mathcal{C}_{11}$, whose check matrix may be regarded as a map from $\mathbb{F}_3^{11} \to \mathbb{F}_3^5$.

No other perfect codes are known. In fact, the perfect error-correcting codes have been classified, and are:

1. Trivial codes (such as a code with one codeword, the universe code, or the binary repetition codes of odd length)

2. Hamming/Golay $\left(\frac{p^k-1}{p-1}, \frac{p^k-1}{p-1} - k\right)$ codes over $\mathbb{F}_p$ with minimum distance 3.

3. Nonlinear codes with the same parameters as the Hamming/Golay codes
(these haven't been completely enumerated).

4. The binary and ternary Golay codes $\mathcal{C}_{23}$ and $\mathcal{C}_{11}$

Sphere Packings and Lattices in $\mathbb{R}^n$

How may we pack disjoint, identical, open n-balls in $\mathbb{R}^n$ so as to maximise the space covered?

Dates back to Gauss (1831): Notes that a problem of Lagrange (1773), concerning the minimum nonzero value assumed by a positive definite quadratic form in n variables, can be restated as a sphere-packing problem.

Lattice packings

If a packing $\mathcal{P} \subset \mathbb{R}^n$ contains spheres centred at $\mathbf{u}$ and $\mathbf{v}$, then there is also a sphere centred at $\mathbf{u} + \mathbf{v}$ and $\mathbf{u} - \mathbf{v}$.

– The set of sphere centres forms an additive group.

A **lattice** is the $\mathbb{Z}$-span of some basis for $\mathbb{R}^n$.

(Or, a finitely-generated free $\mathbb{Z}$-module with an integer-valued symmetric bilinear form.)

Density – the proportion Δ of $\mathbb{R}^n$ which is covered by the spheres.

(Let $V_n = \frac{\pi^{(n/2)}}{(n/2)!}$ be the volume of the n-ball $\mathcal{B}^n$.)

Packing radius – half the minimal distance between lattice points.

Kissing number – The number of n-balls which can be arranged so that they all touch another of the same size.

Voronoi cell – Around each point P in a discrete collection of points $\mathcal{P}$ in $\mathbb{R}^n$, this is the subset of $\mathbb{R}^n$ composed of points which are closer to P than any other point of $\mathcal{P}$.

THE CUBIC LATTICES $\mathbb{Z}^n$

Density	$V_n 2^{-n}$
Packing radius	$\frac{1}{2}$
Kissing number	$2n$

Voronoi cells are n-cubes.

THE A_n ROOT LATTICES

Density	$V_n\sqrt{2^{-n}(n+1)^{-1}}$
Packing radius	$\frac{1}{\sqrt{2}}$
Kissing number	$n(n+1)$

A_2 is the hexagonal lattice in $\mathbb{R}^2$.
Voronoi cells are hexagons.

A_3 is the face-centred-cubic lattice in $\mathbb{R}^3$.
Voronoi cells are rhombic dodecahedra.

The E_6 root lattice

Density	$\frac{\pi^3}{48\sqrt{3}} \approx 0.373$
Packing radius	$\frac{1}{\sqrt{2}}$
Kissing number	72

The E_7 root lattice

Density	$\frac{\pi^3}{105} \approx 0.295$
Packing radius	$\frac{1}{\sqrt{2}}$
Kissing number	126

The E_8 root lattice

Density	$\frac{\pi^4}{384} \approx 0.254$
Packing radius	$\frac{1}{\sqrt{2}}$
Kissing number	240

THE D_n ROOT LATTICES

The ‘chessboard’ lattices in $\mathbb{R}^n$.

Density	$V_n\sqrt{2^{-(n+2)}}$
Packing radius	$\frac{1}{\sqrt{2}}$
Kissing number	$2n(n-1)$

Voronoi cell of D_4 is a regular self-dual 4-polytope called the **24-cell**, composed of 24 regular octahedra glued together along their faces.

Take D_n and fit another copy in the gaps, centred at $(\frac{1}{2},\ldots,\frac{1}{2})$, to get D_n^+.

This is a lattice iff n is even.

D_3^+ is the molecular structure of diamond.

D_4^+ is congruent to $\mathbb{Z}^4$.

D_8^+ is E_8.

WHAT THIS HAS TO DO WITH CODES

It turns out that (as suggested by Hamming's geometric approach) we can construct sphere packings from codes in a variety of ways.

First, define the **coordinate array** of a point $\mathbf{x} \in \mathbb{R}^n$: Write the binary expansions of the coordinates of x_i in columns beginning with the least-significant digit.

So $(2, 7, 11, 9, 8)$ is:

$$\begin{array}{ll} \begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix} & \begin{array}{l} \text{1s row} \\ \text{2s row} \\ \text{4s row} \\ \text{8s row} \\ \end{array} \end{array}$$

CONSTRUCTION A

Given a binary (n, r) code $\mathcal{C}$, we can construct a sphere packing in $\mathbb{R}^n$ where $\mathbf{x} = (x_1, \ldots, x_n)$ is a centre iff $\mathbf{x}$ is congruent (mod 2) to a codeword of $\mathcal{C}$.

Or. . . a point of $\mathbb{R}^n$ with integer coordinates is a centre iff the 1s row of its coordinate array is a codeword of $\mathcal{C}$.

A lattice packing is obtained iff $\mathcal{C}$ is linear.

Applying this construction to the $(n, n-1)$ parity check code we get the D_n lattice.

Applying this construction to the (3,2) parity check code gives the face-centred cubic lattice.

Applying this construction to the (7,4) Hamming code $\mathcal{H}_7$ we obtain the E_7 lattice.

Extend $\mathcal{H}_7$ by appending a parity check bit to each codeword, to get the **extended Hamming code** $\mathcal{H}_8$. Then apply construction A to get the E_8 lattice.

Construction B

Let $\mathcal{C}$ be a binary code whose codewords have even parity.

Then $\mathbf{x}$ is a sphere centre iff $\mathbf{x}$ is congruent (mod 2) to a codeword of $\mathcal{C}$ and $\sum_{i=1}^{n} x_i$ is divisible by 4.

Or... $\mathbf{x}$ is a centre iff its 1s row is a codeword $c \in \mathcal{C}$ and its 2s row has even parity if c has weight divisible by 4, or odd parity if c has weight divisible by 2 but not 4.

Again, this gives a lattice packing iff $\mathcal{C}$ is linear.

Apply this construction to the (8,1) repetition code to get the E_8 lattice.

Apply to the **extended Golay code** $\mathcal{C}_{24}$ ($\mathcal{C}_{23}$ with an extra parity bit) to get a lattice in $\mathbb{R}^{24}$.

We can mesh two copies of this lattice together to get an unexpectedly good (dense) lattice packing in $\mathbb{R}^{24}$...

THE LEECH LATTICE Λ_{24}

Consists of vectors of the form

$$\frac{1}{\sqrt{8}}(\mathbf{0} + 2\mathbf{c} + 4\mathbf{x}) \text{ and } \frac{1}{\sqrt{8}}(\mathbf{1} + 2\mathbf{c} + 4\mathbf{y})$$

Where $c \in \mathcal{C}_{24}, \mathbf{0} = (0, \ldots, 0), \mathbf{1} = (1, \ldots, 1)$, and $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^{24}$ such that $\sum_{i=1}^{24} x_i \equiv 0 \mod 2$ and $\sum_{i=1}^{24} y_i \equiv 1 \mod 2$.

This is one of many different descriptions of Λ_{24}.

Density	$\frac{\pi^{12}}{12!} \approx 0.00193$
Packing radius	1
Kissing number	196560

Voronoi cell is a 24-polytope with 16 969 680 faces.

Discovered by John Leech in 1964.

Simple groups

A **simple group** is one with no proper nontrivial normal subgroups.

Finite simple groups classified between 1950 and 1980 by hundreds of mathematicians, in thousands of pages of journal articles. Classification finished in 1980 by Griess and Aschbacher.

Any finite simple group is one of:

1. A cyclic group of prime order
2. An alternating group of degree $\geqslant 5$
3. A finite group of Lie type
4. 26 others (the '**sporadic simple groups**')

Leech suspected that the automorphism group of Λ_{24} might contain some interesting simple groups, but wasn't able to solve the problem.

Told McKay – then (1968) at work proving the existence of a sporadic group J_3 of order $50\,232\,960$ predicted by Z. Janko.

Told Coxeter – who had no students capable of solving the problem.

Meanwhile, McKay told Conway, who was intrigued, and tried to interest John Thompson, who challenged him to calculate the order of the group.

Conway sets aside twelve hours every saturday afternoon and evening and six hours every wednesday evening, for as long as it takes to solve the problem.

By just after midnight on the first saturday, the problem was solved.

This group Co_0 isn't simple, but it contained three new sporadic groups, Co_1, Co_2 and Co_3.

Group	Discovered	Order
Co_0	1968	8 315 553 613 086 720 000
Co_1	1968	4 157 771 806 543 360 000
Co_2	1968	42 305 421 312 000
Co_3	1968	495 766 656 000

It also contains the oldest known sporadic groups (the Mathieu groups M_{11}, M_{12}, M_{22}, M_{23} and M_{24}, discovered between 1861 and 1873).

Group	Discovered	Order
M_{11}	1861	7 920
M_{12}	1861	95 040
M_{22}	1873	443 520
M_{23}	1873	10 200 960
M_{24}	1873	244 823 040

In addition, it contains four other previously known sporadic groups, bringing the total to twelve.

So, nearly *half* of the 26 sporadic simple groups are contained in the automorphism group of the Leech lattice Λ_{24}.