A "case study": the Hamming code

Lecture 36
4/25/2007

Goal:

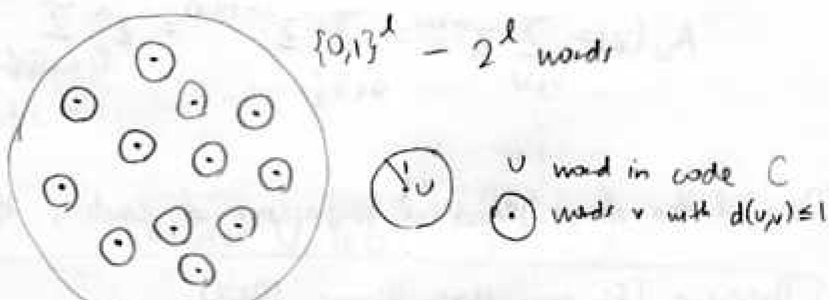
To build a (large) code of words in $\{0,1\}^{\ell}$ which can detect and correct one error.

(History: Hamming's punch card computer at Bell Labs (1940s) could detect errors, but could not correct them. So he had to work on weekends to operate the computer.)

Recall:

Using a code of distance 3 I can detect and correct one error.

A rough estimate:



Note:
- There are $|C|$ balls
- Each ball has $\ell+1$ words $\Rightarrow |C|(\ell+1) \le 2^{\ell}$
- The balls are disjoint.

$$\boxed{|C| \le \frac{2^{\ell}}{\ell+1}}$$

A 1-error correcting code on $\{0,1\}^\ell$ has $\leq \frac{2^\ell}{\ell+1}$ words.

Is this size actually possible?

Say $\ell+1 = 2^n$ for simplicity. (Note: 1 KB = 1,024 B; 1 MB = 1'048,576 B)

kibi $\uparrow$ 2^{10} ; 2^{20}

Q. Is there a code of
- length 2^n-1
- 2^{2^n-n-1} words
- distance 3 ?

Maybe a linear code $H \subseteq \mathbb{F}_2^{2^n-1}$ with $\dim H = 2^n-n-1$?

The dual would be G of $\dim G = n$

$$A_n = \begin{array}{cc} \boxed{\begin{matrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{matrix}} & 2^n-1 \\ n & \end{array}$$

G = rowspace of an $n \times (2^n-1)$ matrix over $\mathbb{F}_2$ of full rank.

- no 0 column
- no equal columns

$\rightarrow$ only one possibility: all 2^n-1 nonzero vectors in $\mathbb{F}_2^n$

G = rowspace A_n

H = nullspace $A_n = G^\perp$

$\boxed{\text{\underline{Prop}. The \underline{Hamming code} } H \text{ is a code of } 2^{2^n-n-1} \text{ words of length } 2^n-1 \text{ and distance } 3}$

Note. I can think of a vector $v \in \{0,1\}^{2^n-1}$ as

$$v = (v_{100}, v_{010}, v_{001}, v_{110}, v_{101}, v_{011}, v_{111})$$

Now, $v \in H$ means $A_n v = 0$

means $\begin{cases} v_{100} + v_{110} + v_{101} + v_{111} = 0 \\ v_{010} + v_{011} + v_{110} + v_{111} = 0 \\ v_{001} + v_{011} + v_{101} + v_{111} = 0 \end{cases}$ $\quad$ $\sum v_{1**} = 0$, $\quad \sum v_{*1*} = 0$, $\quad \sum v_{**1} = 0$

Claim: $w(v) \neq 1$

Pf: If $v_{\_1\_} = 1$ is the only nonzero entry, then $\sum v_{\_1\_} = 1$

Claim: $w(v) \neq 2$

Pf: Say $v_{\_\_1\_} = 1$, $v_{\_\_0\_} = 1$ are the only ones $\rightarrow \sum v_{\_\_1\_} = 1$

Note: $w(v) = 3$ is possible: $v_{\_1\_1\_0\_} = 1$, $v_{\_1\_0\_1\_} = 1$, $v_{\_0\_1\_1\_} = 1$

<u>Q</u> How about G?

A word $v \in G$ is
$$\begin{array}{r} a \\ +b \\ +c \end{array}\boxed{\begin{matrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{matrix}}$$
a b c a+c a+b+c
a+b b+c

$$v_{11010} = v_{10000} + v_{01000} + v_{00010}$$

v word in $G \longleftrightarrow f_v$ linear functional on $\mathbb{F}_2^n$

$$w(v) = \#\text{ nonzero values of } f_v$$
$$= 2^n - |\ker f_v| \in \{2^n - 2^n, 2^n - 2^{n-1}, 2^n - 2^{n-2}, \ldots, 2^n - 2, 2^n - 1\}$$

$\Rightarrow$ G has distance 2^{n-1}.

(91) <u>Exercise.</u> Find weight enumerator of G, H.