Relations between Check matrices and Generating matrices of Error Correcting Codes

For (n,κ) code V $\quad v=(v_1,\dots,v_n)\in V$ iff:

$H\,\theta=0$ $\quad$ H check matrix

G is a generating matrix of V
iff all linear combinations of rows of G
with coefficients $\{0,1\}$ are codewords of G

Let

$$G=\left[\, I_\kappa \,!\, P \,\right]$$

where I_κ is the $(\kappa\times\kappa)$ identity matrix
P some $\kappa\times(n-\kappa)$ matrix

Then H can be chosen as

$$H=\left[\, P^{TR} \,!\, I_{n-\kappa} \,\right]$$

where P^{TR} is the transposed matrix of
$I_{n-\kappa}$ is the $(n-\kappa)\times(n-\kappa)$ identity matrix

Example (7,4,3) HAMMING CODE

$$H = \begin{bmatrix} 1&0&1&1&1&0&0 \\ 1&1&0&1&0&1&0 \\ 1&1&1&0&0&0&1 \end{bmatrix} \Rightarrow P^{TR} = \begin{bmatrix} 1&0&1&1 \\ 1&1&0&1 \\ 1&1&1&0 \end{bmatrix}, \quad H = \left[P^{TR} \,|\, I_3 \right]$$

Since $Hv = 0$ we have

$$v_1 \oplus v_3 \oplus v_4 = v_5$$
$$v_1 \oplus v_2 \oplus v_4 = v_6$$
$$v_1 \oplus v_2 \oplus v_3 = v_7.$$

Thus
$$G = \left[\begin{array}{cccc|ccc} 1&0&0&0&1&1&1 \\ 0&1&0&0&0&1&1 \\ 0&0&1&0&1&0&1 \\ 0&0&0&1&1&1&0 \end{array}\right] = \left[I_4 \,|\, P \right]$$

Let $R(v)$ are check bits of $v = (v_1, \ldots, v_k, v_{k+1}, \ldots, v_n) \in V$

$$R(v) = (v_{k+1}, v_{k+2}, \ldots, v_n)$$

Then
$$R(v) = (v_1, \ldots, v_k)\, P.$$

Extended codes

Let V is an $(n, k, 2t+1)$ code

Then $V' \subset V$ containing all vectors from V with even weight is $(n, k-1, 2t+2)$ code

Check matrix matrix for V' can be obtained by adding a row of all ones to the check matrix for V.

To construct $(n+1, k, 2t+2)$ from $(n, k, 2t+1)$ code V it is sufficient to add one bit to every codeword in such a way that number of ones in codewords of a new code will be even.

Shortened codes

Let $\mathcal{V}$ is an (n, k, d) code

One can construct $(n-i, k-i, d)$ codes for any $i < k$ by deleting i columns from the check matrix of the (n, k, d) code

Example: From $(31, 21, 5)$ double-error correcting [redacted] code one can construct $(24, 14, 5)$ code by deleting $i=7$ columns in the check matrix of $(31, 21, 5)$ code.

§6753

Weight distributions of ERROR CORRECTING CODES

Let V is an (n, K, d) code

and $A(i)$ is a number of codewords in V with HAMMING norm (number of ones) equal to i

$0 \leq i \leq n$

$A(0) = 1$, $A(1) = A(2) = \ldots = A(d-1) = 0$.

$\{A(i)\}$ is a weight distribution for V

PROBLEM of computing a weight distribution of a given code is very difficult

Relations between weight distributions and a probability of error detection.

Let p is a probability of a distortion of one bit in an output vector (codeword)

(For different outputs these events are independent)

An error $e \neq 0$ is <u>not</u> detected by code V iff $e \in V$

Let $\{A(i)\}$ is a weight distribution of V and R is a probability of error detection by code V.

$$R = 1 - \sum_{i=1}^{n} A(i)\, p^i (1-p)^{n-i}$$

For (n, K, d) codes

$$R = 1 - \sum_{i=d}^{n} A(i)\, p^i (1-p)^{n-i}$$

PROBABILITY OF ERROR DETECTION DEPENDS ON weight distributions only

Example Let

$$G = \begin{pmatrix} 0000\ 1111 \\ 0011\ 0011 \\ 0101\ 0101 \end{pmatrix}$$ - generating matrix of V

$n=8$, $K=3$, $d=4$

Codewords :

0000 0000
0001 1111
0010 0011
0011 1100
0100 0101
0101 1010
0110 0110
0111 1001

$A(0) = 1$

$A(1) = A(2) = A(3) = 0$

$A(4) = 7$

$A(5) = A(6) = A(7) = A(8) = 0$

$$R = 1 - 7p^4(1-p)^{8-4}$$
$$= 1 - 7p^4(1-p)^4$$

SC753

Estimations on a minimal number of check bits

Hamming Bound:

For any (n,k)-code with distance $d=2\ell+1$

$$2^k \le \frac{2^n}{V(\ell)}$$

$V(\ell) = \sum_{i=0}^{\ell} \binom{n}{i}$ - volume of a ball with radius ℓ

Lower bound

$$r = n-k \ge \lceil \log_2 \sum_{i=0}^{\ell} \binom{n}{i} \rceil$$

A code is <u>perfect</u> if

$n-k = \log_2 \sum_{i=0}^{l} \binom{n}{i}$ ⇒ Perfect packing of the space by balls of radius l

<u>Perfect codes:</u>

1. <u>Hamming codes</u>

$l=1$, $d=3$, $n=2^m-1$, $k=2^m-m-1$

for any m

Example: $\alpha=4 \Rightarrow n=15$, $k=11$, $d=3$

2. <u>Golay code</u>

$l=3$, $d=7$, $n=23$, $k=12$

There are no other nontrivial <u>linear</u> perfect codes. (For the binary case.)

3. <u>Repetition Codes</u>

$n=2s+1$, $k=1$, $d=2s+1$, $l=s$

Gilbert - Varshamov Bound. (G - V Bound)

There exists a code with distance d and r parity check bits if

$$r = \lceil \log_2(1 + \binom{n-1}{1} + \binom{n-1}{2} + \ldots + \binom{n-1}{d-2}) \rceil$$

Example : **n = 31, d = 5, (ℓ = 2)**

By the *Hamming bound*

$$r_{min} \geq 9 \ ;$$

By the *Gilbert - Varshamov bound*

$$r_{min} \leq 13 \ .$$

It is not known how to construct codes satisfying *G -V Bound* for any n, k.

Number of Check bits for best Error-Correcting codes.

n \ d	2	3	4	5	6
8	1	4	4	6	7
16	1	5	5	8	9
24	1	5	6	10	11
32	1	6	6	10	11
48	1	6	7	11	12
64	1	7	7	12	13

All codes are linear

Correction of Burst Errors (for magnetic discs)

∴ Burst of length "b" is an error which distorts at most "b" consequitive bits:

$$e = \underbrace{0\ldots0\overbrace{1\ldots1}^{b}0\ldots0}_{n}$$

∴ Code V detect bursts if for any $v_1, v_2 \in V$ and any burst e

$$\boxed{v_1 \oplus e \neq v_2}$$

∴ Code V correct bursts if for any $v_1, v_2 \in V$ and any two bursts e_1, e_2

$$\boxed{v_1 \oplus e_1 \neq v_2 \oplus e_2}$$

∴ For <u>detection</u> of bursts of length "b"

$r = b$ check Symbols are sufficient.

∴ For <u>correction</u> of bursts of length "b"

$$2b \le r \le 2(b-1) + \lceil \log_2 (n-2b+2) \rceil$$

<u>Example</u> $n = 32$, $b = 6$

<u>Detection</u> : (32, 26) linear code

$r = 6$

<u>Correction</u> :

$12 \le r \le 15$