

Reference Pages

The Hamming Bound

If C is a code of length n and distance $\delta = 2t + 1$ or $\delta = 2t + 2$ then

$$|C| \leq \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{t}}.$$

The Gilbert-Varshamov Bound

Let n , k and δ be integers. If

$$\binom{n-1}{0} + \binom{n-1}{1} + \dots + \binom{n-1}{\delta-2} < 2^{n-k},$$

then there exists a linear code of length n , dimension k and distance at least δ .

Corollary to the Gilbert-Varshamov Bound

If $n \neq 1$ and $\delta \neq 1$ then there exists a linear code C with length n and distance at least δ with

$$|C| \geq \frac{2^{n-1}}{\binom{n-1}{0} + \binom{n-1}{1} + \dots + \binom{n-1}{\delta-2}}.$$

Factorisations of $1 + x^n$ into irreducible polynomials

$$\begin{aligned} 1 + x &= 1 + x \\ 1 + x^3 &= (1 + x)(1 + x + x^2) \\ 1 + x^5 &= (1 + x)(1 + x + x^2 + x^3 + x^4) \\ 1 + x^7 &= (1 + x)(1 + x + x^3)(1 + x^2 + x^3) \\ 1 + x^9 &= (1 + x)(1 + x + x^2)(1 + x^3 + x^6) \\ 1 + x^{15} &= (1 + x)(1 + x + x^2)(1 + x + x^4)(1 + x^3 + x^4)(1 + x + x^2 + x^3 + x^4) \\ 1 + x^{23} &= (1 + x)(1 + x + x^5 + x^6 + x^7 + x^9 + x^{11})(1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11}) \end{aligned}$$

IMLD for cyclic linear codes correcting cyclic burst errors

To correct a cyclic burst error of length at most t using the parity-check matrix \mathbf{H} :

1. Calculate the syndrome of w with corresponding polynomial $s_0(x)$.
2. Calculate $s_i(x) = xs_{i-1}(x) \bmod g(x)$ until an s_i is found with a burst error of length at most t .
3. Let $e_i = (0, s_i)$ and back shift to find the most likely error pattern e .

$$\mathbf{H} = \begin{pmatrix} r_{n-k} \\ r_{n-k+1} \\ r_{n-k+2} \\ \vdots \\ r_{n-1} \\ \mathbf{I}_{n-k} \end{pmatrix}$$

The Extended Golay Code C_{24} and the Golay code C_{23}

$$\mathbf{B} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

IMLD for the Extended Golay Code C_{24}

1. Compute the syndrome $s = w\mathbf{H} = w \begin{pmatrix} \mathbf{I}_{12} \\ \mathbf{B} \end{pmatrix}$.
2. If $wt(s) \leq 3$ then $u = [s, 0]$.
3. If $wt(s + b_i) \leq 2$ for some row b_i of \mathbf{B} then $u = [s + b_i, e_i]$.
4. Compute the second syndrome $s\mathbf{B}$.
5. If $wt(s\mathbf{B}) \leq 3$ then $u = [0, s\mathbf{B}]$.
6. If $wt(s\mathbf{B} + b_i) \leq 2$ for some row b_i of \mathbf{B} then $u = [e_i, s\mathbf{B} + b_i]$.
7. If u is not yet determined, then more than 3 errors have occurred so request retransmission.

IMLD for the Golay Code C_{23}

1. Form $w^* = w0$ or $w^* = w1$ so that w^* has odd weight.
2. Decode w^* to a codeword $c^* \in C_{24}$ using the Algorithm for IMLD of C_{24} .
3. Remove the last digit from c^* to obtain a codeword $c \in C_{23}$.