Math 422 Review

1. General (n, M, d) Codes

Detect t errors $\Leftrightarrow$ $d \geq t+1$

Correct t errors $\Leftrightarrow$ $d \geq 2t+1$

$(n, M, d)\ \exists \Rightarrow (n-1, M, d-1)\ \exists$

$\Leftarrow$ d even, $q=2$ (extend by adding parity check)

w.l.o.g. $0 \in C' \equiv C$

$$M \sum_{k=0}^{t} \binom{n}{k} (q-1)^k \leq q^n \quad \text{(Sphere-Packing Bound)}$$

↑ perfect if $=$

ISBN code

2. Linear $[n, k, d]$ Codes $M = q^k$

$d(C) = w(C)$

$F_q^n = \bigcup_{i=0}^{q^r-1} C_i$, (Lagrange's Theorem)

the union of $q^r = q^{n-k}$ distinct cosets C_i, each with q^k vectors. $C_0 \equiv C$

cosets $\overset{1-1}{\longleftrightarrow}$ syndromes

$$G = k\left[\underset{=}{1} \;\middle|\; \underset{=}{A}^{\,n}\right] \Leftrightarrow H = {}^{n-k}\left[-\underset{=}{A}^{t} \;\middle|\; \underset{=}{1}\right]$$

Syndrome $Hy^t \equiv$ linear combination of columns of H corresponding to error positions

$C = \{vG : v \in F_q^k\} = \{v : Hv^t = 0\}$ (k)

$C^\perp = \{vH : v \in F_q^{n-k}\} = \{v : Gv^t = 0\}$ $(n-k)$

$$P_{corr}(C) = \sum_{i=0}^{n} \alpha_i \, p^i (1-p)^{n-i}$$

p: bit error rate; α_i: number of coset leaders of weight i.

3. Hamming Codes $Ham(r, q)$

$H =$ n distinct nonzero columns that begin with 1.

$n = \frac{q^r-1}{q-1}$, $d = 3$, perfect

$(\equiv$ cyclic for $q=2)$

4. Golay Binary $[23, 12, 7]$ and Ternary $[11, 6, 5]$ Codes

5. Cyclic $[n, k]$ Codes

all cyclic shifts $\in C$

$C \subset R_n = F_q[x]/(x^n-1) =$ polynomials of degree $< n$.

C cyclic $\Leftrightarrow C = \langle g(x) \rangle = a(x)\,g(x)$, where $g(x) \mid x^n-1$ ($\deg k$, $\deg r = n-k$, $\deg < n$)

$g(x) = g_r x^r + \dots + g_0$

$$G = \begin{bmatrix} g_0 & g_1 & \dots & g_r & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_r & & \\ \vdots & & & & & & \\ 0 & \dots & & g_0 & g_1 & \dots & g_r \end{bmatrix}$$

$$H = \begin{bmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & \dots & 0 \\ 0 & h_k & \dots & & h_0 & \dots & 0 \\ & & & & & & \\ 0 & \dots & & 0 & h_k & \dots & h_0 \end{bmatrix} ?$$

where $h(x) = h_k x^k + \dots + h_0$

$g(x)\,h(x) = x^n - 1$

$C_\perp = \langle \bar{h}(x) \rangle$, where $\bar{h} = h_0 x^k + \dots + h_k$

$\alpha \in F_{2^r}$ primitive with min poly $m_1(x) \Rightarrow \langle m_1(x) \rangle =$ Ham $(r, 2)$

6. BCH $[n, k]$ Codes

$\alpha \in F_q$ s with order n $(\alpha^n = 1)$

$\langle g(x) \rangle$, where $g(x) \in F_q[x]$ has roots $\alpha, \alpha^2, \dots \alpha^{d-1}$

e.g. $g(x) = \underbrace{m_1(\alpha)\; m_3(\alpha) \dots}_{\text{distinct irreducible factors of } (x^{q^s} - x)}$ ← deg $r = n-k$

can correct $\frac{d-1}{2}$ errors!

Syndromes $S_i = v(\alpha^i)$, $i = 1, \dots d-1$

Decoding: $\begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} \begin{bmatrix} b_2 \\ b_1 \end{bmatrix} = \begin{bmatrix} S_3 \\ S_4 \end{bmatrix}$?, where

b_i are coeff of $\sigma(x) = (e_1 x - 1)(e_2 x - 1) \dots (e_t x - 1)$
$= b_t x^t + \dots b_1 x + 1$

$\therefore$ inverses of roots of $\sigma \Rightarrow$ error positions

Make use of $b_t = e_1 e_2 \dots e_t$

7. Cryptographic Codes

p prime

$$a^{p-1} = 1 \mod p \quad \text{if } p \nmid a$$

$$\varphi(n) = \{ m \in \mathbb{N} : 1 \le m \le n,\ (m,n) = 1 \}$$

$$\varphi(p^r) = p^r - p^{r-1}$$

$$\varphi(mn) = \varphi(m)\varphi(n) \quad \text{if } (m,n) = 1$$

RSA: $n = pq$, where p, q distinct primes

$1 < e < \varphi(n) = (p-1)(q-1)$

$d = e^{-1} \mod \varphi(n)$: $de = 1 + r\varphi(n)$ $\leftarrow$ $1 = \gcd(e, \varphi(n))$ (Euclid)

public (n, e)

private (p, q, d)

$$c = m^e \mod n$$

$$m = c^d \mod n = ayq + bxp \mod n,$$

where $\begin{cases} 1 = xp + yq \\ a = c^d \mod p = c^{d \bmod (p-1)} \mod p \\ b = c^d \mod q = c^{d \bmod (q-1)} \mod q \end{cases}$