Nonbinary Hamming codes

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

q - prime

Take $P(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_{r-1} x^{r-1} + x^r$ - primitive

$a_i \in \{0, 1, \dots, q-1\} = \mathbb{Z}_q$

Construct $\mathbb{Z}_q^r = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{q^r-2}\}$

where $P(\alpha) = 0$ $\quad \alpha = 00\dots 010.$

Take $H = [1 \; \alpha \; \alpha^2 \; \alpha^3 \dots \alpha^{n-1}]$

$n = \frac{q^r-1}{q-1}.$ all columns are different

and $\alpha^i \neq a\alpha^j$ $\quad a \in \mathbb{Z}_q$

PROOF:

Let $\alpha^i = a\alpha^j \quad a \in Z_q$

$0 \le i, j \le n-1 \quad , n = \frac{q^r - 1}{q-1}$

Let $j > i$

Then $\alpha^{j-i} = a$

Let $s = j - i$ then $s < n$

$\alpha^s = a \quad$ (α - primitive)

$\alpha^{s(q-1)} = a^{q-1} = 1$ but

by Ferma Theorem

$s(q-1) < n \cdot (q-1) = q^r - 1$

Contradiction $\begin{cases} \alpha^{s(q-1)} = 1 \\ s(q-1) < q^r - 1 \end{cases}$

Example $\quad q=3 \quad r=2$

$$n = \frac{q^2-1}{q-1} = q+1 = 4. \qquad d=3$$

$$P(x) = x^2 + x + 2$$

$$\mathbb{Z}_3^2 = \mathbb{Z}_q^r \qquad \mathbb{Z}_q = \{0,1,2\}$$

0	0	0
0	1	1
0	2	α^4
1	0	α
1	1	α^7
1	2	α^6
2	0	α^5
2	1	α^2
2	2	α^3
α	1	$\alpha^8=1$

$$\alpha^2+\alpha+2=0$$

$$\alpha^2 = 2\alpha+1$$

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 2 & 2 \\ 1 & 0 & 1 & 2 \end{bmatrix}$$

Consider $v = (2\,1\,1\,0)$

Then $Hv = [1\ \alpha\ \alpha^2\ \alpha^3] \begin{bmatrix} 2 \\ 1 \\ 1 \\ 0 \end{bmatrix} =$

$= 2 + \alpha + \alpha^2 = 0 \iff P(\alpha) = 0$

$(2\,1\,1\,0)$ is a codeword.

Let $v = (v_1\ v_2\ v_3\ v_4)$

then $v(x) = v_1 + x\,v_2 + x^2 v_3 + x^3 v_4$

$Hv = v_1 + \alpha\, v_2 + \alpha^2 v_3 + \alpha^3 v_4 = 0 \Rightarrow$

v is a codeword iff

$v(\alpha) = 0$ $\quad$ α is a root of $v(x)$

If $v \in C \Rightarrow v(\alpha)=0$

$w(x)=v(x)\,Q(x)$ For any $Q(x)$

$w(\alpha)=v(\alpha)\,Q(\alpha)=0 \Rightarrow w \in C$

code consists of all multiples of $v(x)$ if $v \in C$

$x^n = 1$

Multiplication by x is equivalent to rotation (cyclic shift)

example $v = (2110)$

$v(x) = 2 + x + x^2$

$w(x) = \text{Rot } v(x) = 2x + x^2 + x^3$

$w = 0211$

$y = \text{Rot } w = 1021$

$y(x) = 1 + 2x^2 + x^3 = w(x) \cdot x =$

$$= (2x + x^2 + x^3)\, x = 2x^2 + x^3 + x^4 \underset{\substack{\uparrow \\ x^4 = 1}}{=}$$

$$= 1 + 2x^2 + x^3 \Rightarrow$$

$$y = 1021.$$

Since $P(\alpha) = 0$ $\quad P \in \mathbb{C}$

For our example

$$p(x) = x^2 + x + 2 \Rightarrow$$

$$p = (2\,1\,1\,0) \in C$$

$$w = \text{Rot}\, p = (0\,2\,1\,1) \in C$$

$\text{Rot}\,w = (1\,0\,2\,1) \in C$ to verify

$$\begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 2 \\ 1 \end{bmatrix} = 1 + 2\alpha^2 + \alpha^3$$

$\alpha^2 = 2\alpha + 1$

$\alpha^3 = 2\alpha + 2$

Thus

$$1 + 2\alpha^2 + \alpha^3 =$$

$$= 1 + 2(2\alpha + 1) + 2\alpha + 2 =$$

$$= 1 + 6\alpha + 5 = 0$$ Thus

$$1021 = \mathrm{Rot}(0211) \in C$$

Thus we constucted

(4, 3, 3) ternary cyclic Hamming code with

the check matrix

$$H = [1\ \alpha\ \alpha^2\ \alpha^3] = \begin{bmatrix} 0 & 1 & 2 & 2 \\ 1 & 0 & 1 & 2 \end{bmatrix} \quad r = 2$$

the generating matrix for this code is

$$G = P(x) = [2\ 1\ 1\ 0]$$

EXAMPLE: $q=3 \quad r=3$

$$n = \frac{q^3-1}{q-1} = 13 \qquad K = 13-3 = 10$$

$$H = [1\ \alpha\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6\ \alpha^7\ \alpha^8\ \alpha^9\ \alpha^{10}\ \alpha^{11}\ \alpha^{12}]$$

$$G = \begin{bmatrix} P(x) \\ x P(x) \\ x^2 P(x) \\ x^3 P(x) \\ x^4 P(x) \\ x^5 P(x) \\ x^6 P(x) \\ x^7 P(x) \\ x^8 P(x) \end{bmatrix}$$