

Definition

For $r \geq 2$, $n = \frac{q^r - 1}{q - 1}$, \mathbb{F}_q a finite field.

Partition non-zero vectors of \mathbb{F}_q^n into the n different L_v as previous.

Take one vector from each L_v to be columns of $H \in M_{r, n}(\mathbb{F}_q)$.

Then $Ham_q(r) = \{x \in \mathbb{F}_q^n \mid xH^t = 0\}$

Note:

Different choices of vectors from L_v 's or different order produces equivalent codes.

One can always choose $\lambda v \in L_v$, so that it's last non-zero entry is 1.

Proposition 5.6

$Ham_q(r)$ is a perfect $[n, n - r, 3]$ code, with check matrix H .

Proof

Similar to binary case. (Prop 5.3)

$d(C)$: We avoided all zero cols or one col = $\lambda \times$ another

So d

But cols picked from L_{e_i} , L_{e_j} and $L_{e_i + e_j}$ must be linearly dependent.

Example

For $Ham_3(2)$, H could be

$$\begin{bmatrix} 0 & 1 & 2 & 2 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

$$\text{Here } \begin{bmatrix} 0 \\ 1 \end{bmatrix} + 2 \begin{bmatrix} 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

Algorithm

(Error-correction)

For $y \in \mathbb{F}_q^n$ received, compute $S(y) = yH^t$.

1) If $S(y) = 0$, decode y as y

2) Otherwise, $S(y) = \lambda \cdot j^{\text{th}}$ row of H^t . Decode y as $y - \lambda e_j$

Example

Consider $Ham_3(2)$ with $H = \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{bmatrix}$

If $y = (2101)$ received,

$$S(y) = \begin{bmatrix} 2 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \end{bmatrix} = 2 \begin{bmatrix} 2 & 1 \end{bmatrix} \text{ [[Row 4]]}$$

\therefore decode to

$$y - 2e_4 = \begin{bmatrix} 2 & 1 & 0 & 1 \end{bmatrix} - 2 \begin{bmatrix} 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 & 0 & 2 \end{bmatrix} \in C$$

Definition 5.9

For p prime, and d, n st $2d - 1 < np - 1$

$$\text{Let } H \in M_{d-1, n}(\mathbb{F}_p) \text{ be } \begin{bmatrix} 1 & 2 & 3 & \dots & n \\ 1^2 & 2^2 & 3^2 & \dots & n^2 \\ \dots & \dots & \dots & \dots & \dots \\ 1^{d-1} & 2^{d-1} & 3^{d-1} & \dots & n^{d-1} \end{bmatrix}$$

$$\text{Then } bch_p(n, d) = \left\{ x \in \mathbb{F}_p^n \mid xH^t = 0 \right\}$$

Proposition 5.10

$bch_p(n, d)$ is a $[n, n - d + 1, d]$ code, with check matrix H

Proof: Let $C = bch_p(n, d)$

(n): Clearly block length is n .

(H is check): By corollary 5.6 (see handout)

$$\left\| \begin{bmatrix} 1 & 2 & \dots & d-1 \\ \dots & \dots & \dots & \dots \\ 1 & 2^{d-1} & \dots & (d-1)^{d-1} \end{bmatrix} \right\|$$

So these (truncated) rows are linearly independent. It follows that the rows of H are lin. ind.

So by proposition 4.8 H is a check matrix for C

(k): and so $\dim(C)$ is $n - (d - 1)$

(d): Any $d - 1$ columns are linearly independent. Since they make a matrix with $\det \neq 0$ by Cor to 5.8.

Buy any d columns must be linearly dep. Then by Thm 3.7, $d(C) = d$

Example

$bch_7(5, 5)$ has check matrix:

$$H = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 \\ 1^3 & 2^3 & 3^2 & 4^3 & 5^3 \\ 1^4 & 2^4 & 3^4 & 4^4 & 5^4 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 2 & 4 \\ 1 & 1 & 6 & 1 & 6 \\ 1 & 2 & 4 & 4 & 2 \end{bmatrix}$$

and is a $[5, 5 - 5 + 1, 5] = [5, 1, 5]$ code