# Linear codes (13.4)

Recall a block code of length $n$ over alphabet $A$ is a subset $C \subseteq A^n$. Have

- Hamming distance $\Delta(\vec{a},\vec{b})$ = # coordinates differing in $\vec{a}$ & $\vec{b}$ $\quad \vec{a},\vec{b} \in A^n$
- $d(C) = \min_{\vec{a}\neq\vec{b}\in C} \Delta(\vec{a},\vec{b})$
- $C$ is $t$-error correcting if $d(C) \geq 2t+1$.

Let now $q$ be a prime power $q = p^n$ (e.g. $q=2$), let $A = K = GF(q)$, the field of $q$ elements.

Def A linear code is a linear subspace $C \subseteq K^n$.

Recall linear subspace means $C \subseteq K^n$ and

1. $\vec{0} \in C$
2. $\alpha \in K,\ \vec{a} \in C \Rightarrow \alpha\vec{a} \in C$
3. $\vec{a},\vec{b} \in C \Rightarrow \vec{a}+\vec{b} \in C$.

If $K = GF(p) = \mathbb{Z}_p$, then 1 + 3 $\Rightarrow$ 2.

Ex $K = \mathbb{Z}_2$, parity code $C \subseteq K^n$, $C = \{\vec{a} \mid \sum_{i=1}^{n} a_i = 0 \pmod 2\}$ is linear.

1. Obvious
2. $\alpha = 0 \rightsquigarrow \alpha\vec{a} = 0 \in C$, $\alpha = 1 \Rightarrow \alpha\vec{a} = \vec{a} \in C$
3. $\vec{a},\vec{b} \in C$, $\vec{c} = \vec{a}+\vec{b} \Rightarrow$ if $a_i = b_i$ then $c_i = 0$, if $a_i \neq b_i$ then $c_i = 1$, $c_i = a_i + b_i \pmod 2$

$$\Rightarrow \sum_{i=1}^{n} c_i = \sum_{i=1}^{n} a_i + b_i \equiv 0 + 0 \pmod 2.$$

$(1,0,1) + (1,1,1) = (0,1,0)$ (XOR)

Ex Double repetition code, $n = 3k$, $C \subseteq K^n$ is

$$C = \{ w\,w\,w \mid w \in K^k \}.$$

Then $0 = 000 \in C$, $\alpha(w\,w\,w) = \alpha w\,\alpha w\,\alpha w$,

$w_1 w_1 w_1 + w_2 w_2 w_2 = (w_1+w_2)(w_1+w_2)(w_1+w_2)$, so $C$ is linear.

Def Fano code

Ex Fano code $C \subseteq K^7$ $K = \mathbb{Z}_2$, defined by bijection

$S = \{1, 2, \ldots, 7\}$ $\quad K^7 \longleftrightarrow 2^S$

$\vec{a} \longmapsto \{ i \mid a_i = 1 \}$

$C = \{\emptyset\} \cup \{S\} \cup \{ l \mid l \text{ a line in Fano plane} \} \cup \{ S \setminus l \mid l \text{ a line in F. plane} \}$

$= \{0\ldots0, 1\ldots1, 1110000, \ldots, 0001111, \ldots \}.$

$C$ is linear!

Def For $\vec{a} \in K^n$, the weight of $\vec{a}$ is $w(\vec{a}) = |\{ i \mid a_i \neq 0 \}|$.

Ex $w(1111) = 4$ $\quad w(0000) = 0$, $\quad w(1010) = 2$.

Proposition Let $C \subseteq K^n$ be a linear code. Then $d(C) = \min_{\vec{a} \in C \setminus \{0\}} w(\vec{a})$.

Proof $C$ is linear $\Rightarrow \forall \vec{a}, \vec{b} \in C$, $\vec{a} - \vec{b} \in C$.

$\vec{a} - \vec{b} = (a_1 - b_1, a_2 - b_2, \ldots, a_n - b_n)$, $i$th coordinate $0 \Leftrightarrow a_i - b_i = 0 \Leftrightarrow a_i = b_i$.

$w(\vec{a} - \vec{b})$ = # non-zero coordinates $= \#i$ s.t. $a_i \neq b_i = \Delta(\vec{a}, \vec{b})$.

$d(C) = d \Rightarrow \exists \vec{a} \neq \vec{b} \in C$, $\Delta(\vec{a}, \vec{b}) = d \Rightarrow w(\vec{a} - \vec{b}) = d$

$\min_{\vec{a} \in C \setminus \{0\}} w(\vec{a}) = e \Rightarrow \exists \vec{a} \in C \setminus \{0\}$ $w(\vec{a}) = e \Rightarrow \Delta(0, \vec{a}) = e$.

So $w$ & $\Delta$ take same values, hence have same minimal value

---

Ex Parity code has $w(\vec{a})$ even for all $\vec{a} \neq 0$ $w(100\ 01) = 2$

$\Rightarrow d(C) = 2$

Repetion code has $w(\vec{a}) \geq 3$ for all $\vec{a} \neq 0$, $w(1000\ 1000\ 1000) = 3$

$\Rightarrow d(C) = 3$.

Fano code has $d(C) = 3$.

Recall a linear subspace $C \subseteq K^n$ has a basis, a sequence $\{\vec{a}_1, \vec{a}_2, \dots, \vec{a}_k\} \in C$ such that

① $\vec{a}_1, \dots, \vec{a}_k$ are linearly independent: $\sum_{i=1}^{k} \alpha_i \vec{a}_i = 0 \iff \alpha_1 = \dots = \alpha_k = 0$ $\quad \alpha_i \in K$

② $\vec{a}_1, \dots, \vec{a}_k$ span $C$: $\forall \vec{b} \in C$ can find $\alpha_1, \dots, \alpha_k \in K$ s.t. $\vec{b} = \sum_{i=1}^{k} \alpha_i \vec{a}_i$.

Equivalently, ①+② means every $\vec{b} \in C$ can be written as $\vec{b} = \sum_{i=1}^{k} \alpha_i \vec{a}_i$ for exactly one choice of $\alpha_1, \dots, \alpha_k \in K$.

Def dimension of $C$ is $k$

Note bijection $K^k \longleftrightarrow C$

$$(\alpha_1, \dots, \alpha_k) \longmapsto \sum_{i=1}^{k} \alpha_i \vec{a}_i$$

$\rightsquigarrow |C| = |K^k| = q^k$.

A linear code $C \subseteq K^n$ of dimension $k$ is called $(n,k)$-code.

Ex Parity code $C \subseteq \mathbb{Z}_2^n$ has $|C| = 2^{n-1}$ & basis

$(1,0,0,0,\dots,0,1), (0,1,0,\dots,0,1), \dots (0,0,\dots,1,1)$,

an $(n, n-1)$-code.

Def Given a linear code $C \subseteq K^n$, the dual code is $C^\perp \subseteq K^n$ given by

$$C^\perp = \{\vec{a} \in K^n \mid \vec{a} \cdot \vec{c} = 0 \quad \forall \vec{c} \in C\}.$$

Note: • $\vec{a} \cdot \vec{c} \overset{\text{def}}{=} a_1 c_1 + \dots + a_n c_n \in K$ scalar product

• $C^\perp$ has dimension $n-k$ if $C$ has dimension $k$.

• If $\vec{g}_1, \dots, \vec{g}_k$ is basis for $C$, then

$$\vec{a} \in C^\perp \iff \vec{a} \cdot \vec{g}_1 = \vec{a} \cdot \vec{g}_2 = \dots = \vec{a} \cdot \vec{g}_k = 0$$

• Warning: Can have $\vec{a} \cdot \vec{a} = 0$, e.g. $(1,1) \cdot (1,1) = 1 + 1 = 0$ in $\mathbb{Z}_2^2$

- $(C^\perp)^\perp = C$, so knowing $C^\perp$ determines $C$.

~~The two matrices Let $C$ be of~~ $\vec{g}_1 \quad \dots \quad \vec{g}_{n-1}$

Ex Parity code $C \subseteq \mathbb{Z}_2^n$ has basis $(1,0,\dots,0,1), \dots, (0,0,\dots,1,1)$

$\vec{a} \in \mathbb{Z}_2^n$ lies in $C^\perp \iff \vec{a} \cdot \vec{g}_i = 0 \quad i = 1, \dots, n-1$

$$\iff \begin{matrix} a_1 + a_n = 0 \\ a_2 + a_n = 0 \\ \vdots \\ a_{n-1} + a_n = 0 \end{matrix} \iff a_1 = a_2 = \dots = a_n$$

$C^\perp = \{(0,\dots,0), (1,\dots,1)\}$.

Two matrices: Let $C \subseteq K^n$ be an $(n,k)$-code, with basis $\vec{g}_1, \dots, \vec{g}_k$. Let $\vec{h}_1, \dots, \vec{h}_{n-k}$ be a basis for $C^\perp$.

Then the ~~(k x k)~~ $(k \times n)$ matrix $G = \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{bmatrix}$ is a generator matrix for $C$.

The $(n-k) \times n$-matrix $H = \begin{bmatrix} h_1 \\ \vdots \\ h_{n-k} \end{bmatrix}$ is a parity check matrix for $C$.

Ex: Parity code:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 1 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 1 \\ \vdots & & & & \ddots & 0 & 1 \\ & & & & & 1 & 1 \end{pmatrix} \qquad H = (1\ 1 \cdots 1)$$

Note: $G$ & $H$ not uniquely determined by $C$ (basis not unique!)

G & H determine C

**Prop** For $\vec{a} \in K^n$, the following are equivalent.

1. $\vec{a} \in C$
2. $\exists w_1, \ldots, w_k \in K$ s.t. $\vec{a} = (w_1, \ldots, w_k)\, G$
3. $H\vec{a} = \vec{0}$.

**Ex** Parity code, $H = (1, 1, \ldots, 1)$, $H\vec{a} = a_1 + \cdots + a_n = 0 \iff \vec{a} \in C$.

**Thm** Let $C$ be a linear code with parity check matrix $H$, let $d \geq 0$.
Then $d(C) \geq d \iff$ every set of $d-1$ columns in $H$ is linearly independent.

Pf of $\Leftarrow$: Let $\vec{a} = (a_1, \ldots, a_n)^T \in C \setminus \{0\}$ & let $H = [\vec{c}_1, \ldots, \vec{c}_n]$ with $\vec{c}_i \in K^{n-k}$. Then $H\vec{a} = 0$
$\iff \sum_{i=1}^{n} a_i \vec{c}_i = 0$. At least $d$ of the coordinates of $\vec{a}$ are then $\neq 0$, else get a linear dependence relation between $\leq d-1$ of the $\vec{c}_i$. Hence $w(\vec{a}) \geq d$
$\Rightarrow d(C) \geq d$.

**Ex** Parity code: Column vectors are all $(1)$.
1 of these linearly independent $\Rightarrow d(C) \geq 2 \Rightarrow d(C) = 2$.
2 of these not linearly indep $\Rightarrow d(C) < 3$

**Ex** (Hamming codes) Want 1-error correcting codes
$\rightsquigarrow d(C) \geq 3 \iff$ any 2 columns of $H$ should be linearly independent.

Say H is $(n-k)\times n$ - matrix

$n-k=1 \rightsquigarrow H=(1)$ trivial case

$n-k \geq 2$: 2 vectors $\vec{v}_1, \vec{v}_2$ are linearly independent unless $\vec{v}_1$ is a rescaling of $\vec{v}_2$.

Since $\vec{v} \in K^{n-k}$ can be rescaled to $q-1$ other vectors, can find $\frac{|K^{n-k}-\{0\}|}{q-1} = \frac{q^{n-k}-1}{q-1}$ vectors which differ up to scaling.*

E.g. $n-k=3$, $q=3$

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

* Explicitly, can take all $(a_1, _, a_n) \in K^n$ s.t. first non-zero $a_i$ is 1

This gives a 1-error correcting code of length $q^{n-k}-1$ & dimension $q^{n-k}-1-(n-k)$.