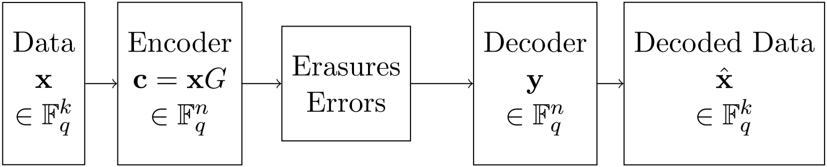
Coding Theory: Decoding Algorithms

A Generic Communication Channel

Transmitter Channel Receiver



Data $\mathbf{x}$ $\in \mathbb{F}_q^k$

Encoder $\mathbf{c} = \mathbf{x}G$ $\in \mathbb{F}_q^n$

Erasures Errors

Decoder $\mathbf{y}$ $\in \mathbb{F}_q^n$

Decoded Data $\hat{\mathbf{x}}$ $\in \mathbb{F}_q^k$

$d_H(\mathcal{C}) = d$ means $\mathcal{C}$ can recover from $d-1$ erasures and $\lfloor \frac{d-1}{2} \rfloor$ errors (BSC).

Packing radius

The largest radius of spheres centered at codewords so that the spheres are pairwise disjoint.

For $t = \lfloor \frac{d_H(\mathcal{C})-1}{2} \rfloor$, $\mathcal{C}$ is a t-error-correcting code, but not a $(t+1)$-error correcting code.

The packing radius of $\mathcal{C}$ is $t = \lfloor \frac{d_H(\mathcal{C})-1}{2} \rfloor$.

It is such that nearest neighbour decoding always decodes correctly a codeword with at most t errors, but may fail for $t+1$ errors.

Decoding

■ Algorithms

Given n and k, we wish to find a code $\mathcal{C}$ with $d_H(\mathcal{C})$ as high as possible.

Need for an efficient algorithm that will correct up to t errors.

Option 1: Examine all codewords until one is found with distance t or less from the received vector. ⇒ only for a small number of codewords.

Option 2: Make a table consisting of a nearest codeword for each of the q^n vectors in $\mathbb{F}_q^n$, and look up a received vector in the table ⇒ only for small values of q^n.

Coset

For an (n, k) linear code $\mathcal{C}$, a set of the form $\mathbf{x} + \mathcal{C}$, $\mathbf{x} \in \mathbb{F}_q^n$.

$\mathcal{C} = \{(0,0,0),(1,1,1)\}$ over $\mathbb{F}_2$.

$\mathbf{x} = (1,0,0)$, then $\mathbf{x} + \mathcal{C} = \{(1,0,0) + (0,0,0),\ (1,0,0) + (1,1,1)\} = \{(1,0,0),\ (0,1,1)\}$.

Decoding

Cosets

Exercise. Consider the repetition code of length 3 over $\mathbb{F}_2$. Compute all its cosets.

Exercise. Consider the repetition code of length 3 over $\mathbb{F}_2$. Compute all its cosets.

The repetition code $\mathcal{C}$ of length 3 over $\mathbb{F}_2$ is

$$\mathcal{C} = \{(0,0,0),\ (1,1,1)\}.$$

Exercise. Consider the repetition code of length 3 over $\mathbb{F}_2$. Compute all its cosets.

The repetition code $\mathcal{C}$ of length 3 over $\mathbb{F}_2$ is

$$\mathcal{C} = \{(0,0,0),\ (1,1,1)\}.$$

$\mathbf{x} \in \mathbb{F}_2^3$	$\mathbf{x} + \mathcal{C}$
$(0,0,0)$	$\{(0,0,0),\ (1,1,1)\}$
$(1,0,0)$	$\{(1,0,0),\ (0,1,1)\}$
$(0,1,0)$	$\{(0,1,0),\ (1,0,1)\}$
$(1,1,0)$	$\{(1,1,0),\ (0,0,1)\}$
$(0,0,1)$	$\{(0,0,1),\ (1,1,0)\}$
$(1,0,1)$	$\{(1,0,1),\ (0,1,0)\}$
$(0,1,1)$	$\{(0,1,1),\ (1,0,0)\}$
$(1,1,1)$	$\{(1,1,1),\ (0,0,0)\}$

Decoding

Cosets

$\mathcal{C} = \{(0,0,0),\ (1,1,1)\}$ over $\mathbb{F}_2$.

$\mathbf{x} \in \mathbb{F}_2^3$	$\mathbf{x} + \mathcal{C}$
$(0,0,0)$	$\{(0,0,0),\ (1,1,1)\}$
$(1,0,0)$	$\{(1,0,0),\ (0,1,1)\}$
$(0,1,0)$	$\{(0,1,0),\ (1,0,1)\}$
$(1,1,0)$	$\{(1,1,0),\ (0,0,1)\}$
$(0,0,1)$	$\{(0,0,1),\ (1,1,0)\}$
$(1,0,1)$	$\{(1,0,1),\ (0,1,0)\}$
$(0,1,1)$	$\{(0,1,1),\ (1,0,0)\}$
$(1,1,1)$	$\{(1,1,1),\ (0,0,0)\}$

- Cosets may appear several times, they are not all distinct.

Decoding

■ Cosets

$\mathcal{C} = \{(0,0,0),\ (1,1,1)\}$ over $\mathbb{F}_2$.

$\mathbf{x} \in \mathbb{F}_2^3$	$\mathbf{x} + \mathcal{C}$
$(0,0,0)$	$\{(0,0,0),\ (1,1,1)\}$
$(1,0,0)$	$\{(1,0,0),\ (0,1,1)\}$
$(0,1,0)$	$\{(0,1,0),\ (1,0,1)\}$
$(1,1,0)$	$\{(1,1,0),\ (0,0,1)\}$
$(0,0,1)$	$\{(0,0,1),\ (1,1,0)\}$
$(1,0,1)$	$\{(1,0,1),\ (0,1,0)\}$
$(0,1,1)$	$\{(0,1,1),\ (1,0,0)\}$
$(1,1,1)$	$\{(1,1,1),\ (0,0,0)\}$

- Every vector in $\mathbb{F}_2^3$ is contained in the union of cosets.

Decoding

■ Cosets

$\mathcal{C} = \{(0,0,0),\ (1,1,1)\}$ over $\mathbb{F}_2$.

$\mathbf{x} \in \mathbb{F}_2^3$	$\mathbf{x} + \mathcal{C}$
$(0,0,0)$,$(1,1,1)$	$\{(0,0,0),\ (1,1,1)\}$
$(1,0,0)$,$(0,1,1)$	$\{(1,0,0),\ (0,1,1)\}$
$(0,1,0)$,$(1,0,1)$	$\{(0,1,0),\ (1,0,1)\}$
$(1,1,0)$,$(0,0,1)$	$\{(1,1,0),\ (0,0,1)\}$

- Cosets do not intersect.
- Every coset contains the same number $|\mathcal{C}|$ of vectors.
- $|\mathbb{F}_2^3| = |\mathcal{C}|\cdot$(number of cosets).

$\mathcal{C} = \{(0,0,0),\ (1,1,1)\}$ over $\mathbb{F}_2$.

$\mathbf{x} \in \mathbb{F}_2^3$	$\mathbf{x} + \mathcal{C}$
$(0,0,0)$,$(1,1,1)$	$\{(0,0,0),\ (1,1,1)\}$
$(1,0,0)$,$(0,1,1)$	$\{(1,0,0),\ (0,1,1)\}$
$(0,1,0)$,$(1,0,1)$	$\{(0,1,0),\ (1,0,1)\}$
$(1,1,0)$,$(0,0,1)$	$\{(1,1,0),\ (0,0,1)\}$

- Cosets of $\mathcal{C}$ partition $\mathbb{F}_2^3$.

(0,0,0) (1,1,1)	(1,0,0) (0,1,1)	(0,1,0) (1,0,1)	(1,1,0) (0,0,1)

- Cosets do not intersect.
- Every coset contains the same number $|\mathcal{C}|$ of vectors.
- $|\mathbb{F}_2^3| = |\mathcal{C}|\cdot$(number of cosets).

For a linear (n, k) code $\mathcal{C}$:

(P_1) Every vector in $\mathbb{F}_q^n$ is contained in the union of cosets: the vector $\mathbf{0}$ always belongs to a linear code.

For a linear (n,k) code $\mathcal{C}$:

(P_1) Every vector in $\mathbb{F}_q^n$ is contained in the union of cosets: the vector $\mathbf{0}$ always belongs to a linear code.

(P_2) Cosets do not intersect: suppose $\mathbf{v} \in (\mathbf{x}+\mathcal{C}) \cap (\mathbf{y}+\mathcal{C})$. Then $\mathbf{v} = \mathbf{x}+\mathbf{c} = \mathbf{y}+\mathbf{c}'$ which implies $\mathbf{x} = \mathbf{y} + (\mathbf{c}'-\mathbf{c}) \in \mathbf{y}+\mathcal{C}$ and $\mathbf{x}+\mathcal{C} \subseteq \mathbf{y}+\mathcal{C}$. Conversely $\mathbf{y} = \mathbf{x} - (\mathbf{c}'-\mathbf{c}) \in \mathbf{x}+\mathcal{C}$ and $\mathbf{y}+\mathcal{C} \subseteq \mathbf{x}+\mathcal{C}$. Note the use of linearity.

For a linear (n, k) code $\mathcal{C}$:

(P_1) Every vector in $\mathbb{F}_q^n$ is contained in the union of cosets: the vector $\mathbf{0}$ always belongs to a linear code.

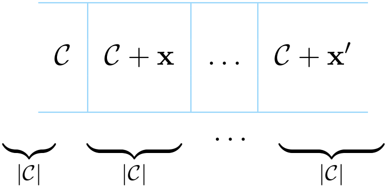
(P_2) Cosets do not intersect: suppose $\mathbf{v} \in (\mathbf{x} + \mathcal{C}) \cap (\mathbf{y} + \mathcal{C})$. Then $\mathbf{v} = \mathbf{x} + \mathbf{c} = \mathbf{y} + \mathbf{c}'$ which implies $\mathbf{x} = \mathbf{y} + (\mathbf{c}' - \mathbf{c}) \in \mathbf{y} + \mathcal{C}$ and $\mathbf{x} + \mathcal{C} \subseteq \mathbf{y} + \mathcal{C}$. Conversely $\mathbf{y} = \mathbf{x} - (\mathbf{c}' - \mathbf{c}) \in \mathbf{x} + \mathcal{C}$ and $\mathbf{y} + \mathcal{C} \subseteq \mathbf{x} + \mathcal{C}$. Note the use of linearity.

(P_3) Every coset contains the same number of vectors, in fact $|\mathbf{x} + \mathcal{C}| = |\mathcal{C}|$: $|\mathbf{x} + \mathcal{C}| \leq |\mathcal{C}|$, since adding $\mathbf{x}$ to every codeword in $\mathcal{C}$ cannot increase the number of vectors we have. To have $|\mathbf{x} + \mathcal{C}| < |\mathcal{C}|$, we would need $\mathbf{x} + \mathbf{c} = \mathbf{x} + \mathbf{c}'$, but this happens only when $\mathbf{c} = \mathbf{c}'$.

For a linear (n, k) code $\mathcal{C}$:

(P_4) Cosets of $\mathcal{C}$ partition $\mathbb{F}_q^n$: the term partition means that $\mathbb{F}_q^n$ is a disjoint union of cosets, then use (P_1) and (P_2).

(P_5) $|\mathbb{F}_q^n| = q^n = |\mathcal{C}|\cdot$(number of cosets)$=q^k \cdot q^{n-k}$ using (P_3).



(P_6) The vectors $\mathbf{x}, \mathbf{y}$ belong to the same coset if and only if $\mathbf{y} - \mathbf{x} \in \mathcal{C}$: $\mathbf{x}, \mathbf{y} \in \mathbf{v} + \mathcal{C}$ is equivalent to $\mathbf{x} = \mathbf{v} + \mathbf{c}$, $\mathbf{y} = \mathbf{v} + \mathbf{c}'$ then $\mathbf{y} - \mathbf{x} = \mathbf{c}' - \mathbf{c} \in \mathcal{C}$. Conversely, if $\mathbf{y} - \mathbf{x} = \mathbf{c} \in \mathcal{C}$, then $\mathbf{y} = \mathbf{c} + \mathbf{x} \in \mathbf{x} + \mathcal{C}$ and $\mathbf{y}$ belongs to the same coset as $\mathbf{x}$.

Decoding

Cosets

Exercise. Consider the code $\mathcal{C}$ over $\mathbb{F}_4$ given by:
$(x_1, x_2) \mapsto (x_1, x_2, x_1 + wx_2)$.

1. How many codewords are contained in $\mathcal{C}$?
2. How many cosets of $\mathcal{C}$ are there?
3. List all distinct cosets (no need to give the actual list of elements within each coset).
4. In which coset does the vector $(w, 1, 0)$ belong to?

Exercise. Consider the code $\mathcal{C}$ over $\mathbb{F}_4$ given by:
$(x_1, x_2) \mapsto (x_1, x_2, x_1 + wx_2)$.

1. How many codewords are contained in $\mathcal{C}$?
2. How many cosets of $\mathcal{C}$ are there?
3. List all distinct cosets (no need to give the actual list of elements within each coset).
4. In which coset does the vector $(w, 1, 0)$ belong to?

1. There are $|\mathcal{C}| = q^2 = 4^2$ codewords.
2. There are $|\mathbb{F}_4^3| = 4^3$ vectors, each coset contains $|\mathcal{C}| = 4^2$ vectors. Thus $4^3 = 4^2 \cdot 4$ and there are thus 4 cosets.

Decoding

Cosets

4. Recall $\mathcal{C}$ over $\mathbb{F}_4$ is given by: $(x_1, x_2) \mapsto (x_1, x_2, x_1 + wx_2)$.

   The first coset is $\mathcal{C}$ itself.

   The next coset is $(1, 0, 0) + \mathcal{C}$ which is different since $(1, 0, 0)$ is not in $\mathcal{C}$.

   The 3rd coset is $(0, 1, 0) + \mathcal{C}$, since $(0, 1, 0)$ is not in $\mathcal{C}$, and it is not in $(1, 0, 0) + \mathcal{C}$ either, otherwise we would need $(0, 1, 0) = (1, 0, 0) + \mathbf{c}$ for $\mathbf{c} \in \mathcal{C}$, that is $(1, 1, 0) \in \mathcal{C}$ which is not the case.

   Finally the 4rth coset is $(1, 1, 0) + \mathcal{C}$, because $(1, 1, 0)$ is not in $\mathcal{C}$, it is not of the form $(1, 1, 0) = (1, 0, 0) + \mathbf{c} \iff \mathbf{c} = (0, 1, 0)$, and it is not of the form $(1, 1, 0) = (0, 1, 0) + \mathbf{c} \iff \mathbf{c} = (1, 0, 0)$.

Decoding

Cosets

4. Recall $\mathcal{C}$ over $\mathbb{F}_4$ is given by: $(x_1, x_2) \mapsto (x_1, x_2, x_1 + wx_2)$.

   $(w, 1, 0) \in \mathbf{x} + \mathcal{C}$

   $(w, 1, 0) = (1, 0, 0) + \mathbf{c} \iff (w + 1, 1, 0) \in \mathcal{C}$. But $w + 1 + w \neq 0$.

   $(w, 1, 0) = (0, 1, 0) + \mathbf{c} \iff (w, 0, 0) \in \mathcal{C}$. But $w \neq 0$.

   $(w, 1, 0) = (1, 1, 0) + \mathbf{c} \iff (w + 1, 0, 0) \in \mathcal{C}$. But $w + 1 \neq 0$.

   $(w, 1, 0) = (0, 0, 0) + \mathbf{c}$ and $w + w = 0$. So $(w, 1, 0) \in \mathcal{C}$.

Weight of a coset and coset leader

Smallest weight of a vector in the coset. Any vector of this smallest weight in the coset is called coset leader.

$\mathcal{C} = \{(0,0,0),\ (1,1,1)\}$ over $\mathbb{F}_2$.

$\mathbf{x} + \mathcal{C}$	weight
$\{(0,0,0),\ (1,1,1)\}$	0
$\{(1,0,0),\ (0,1,1)\}$	1
$\{(0,1,0),\ (1,0,1)\}$	1
$\{(1,1,0),\ (0,0,1)\}$	1

A coset of weight at most $t = \lfloor \frac{d_H(\mathcal{C})-1}{2} \rfloor$ has a unique coset leader.

Suppose we have two coset leaders, $\mathbf{x}$ and $\mathbf{y}$, then $\mathbf{y} - \mathbf{x} \in \mathcal{C}$ (by (P_6)).

Yet by the triangle inequality

$$\begin{aligned} & wt(\mathbf{y}-\mathbf{x}) = d_H(\mathbf{x},\mathbf{y}) \\ \leq \quad & d_H(\mathbf{x},\mathbf{0}) + d_H(\mathbf{0},\mathbf{y}) \\ = \quad & wt(\mathbf{x}) + wt(\mathbf{y}) \\ \leq \quad & 2\frac{d_H(\mathcal{C})-1}{2} \leq d_H(\mathcal{C}) - 1. \end{aligned}$$

for $\mathbf{y} - \mathbf{x} \in \mathcal{C}$.

- The converse is not true.
- If the coset leader is not unique, then the coset has weight more than t.

Syndrome

For a linear (n, k) code $\mathcal{C}$ with parity check matrix H, the syndrome $syn(\mathbf{x})$ of a vector $\mathbf{x} \in \mathbb{F}_q^n$ is

$$syn(\mathbf{x}) = H\mathbf{x}^T.$$

H has rank $n - k$, thus every vector in $\mathbb{F}_q^{n-k}$ is a syndrome.

Decoding
■ Syndrome

$\mathcal{C}$ over $\mathbb{F}_4$ is given by the generator matrix $G = [1, 1, w]$.

$$H\mathbf{x}^T = \begin{bmatrix} 1 & 1 & 0 \\ w & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_1 + x_2 \\ wx_1 + x_3 \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ w \end{bmatrix} + \underbrace{x_2 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + x_3 \begin{bmatrix} 0 \\ 1 \end{bmatrix}}_{\text{generates } \mathbb{F}_4^2}$$

Decoding

■ Syndrome

$\mathcal{C}$ over $\mathbb{F}_4$ is given by the generator matrix $G = [1, 1, w]$.

$$H\mathbf{x}^T = \begin{bmatrix} 1 & 1 & 0 \\ w & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_1 + x_2 \\ wx_1 + x_3 \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ w \end{bmatrix} + \underbrace{x_2 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + x_3 \begin{bmatrix} 0 \\ 1 \end{bmatrix}}_{\text{generates } \mathbb{F}_4^2}$$

The vector $(w, 1)$ is a syndrome.

Decoding

Syndrome

$\mathcal{C}$ over $\mathbb{F}_4$ is given by the generator matrix $G = [1, 1, w]$.

$$H\mathbf{x}^T = \begin{bmatrix} 1 & 1 & 0 \\ w & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_1 + x_2 \\ wx_1 + x_3 \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ w \end{bmatrix} + \underbrace{x_2 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + x_3 \begin{bmatrix} 0 \\ 1 \end{bmatrix}}_{\text{generates } \mathbb{F}_4^2}$$

The vector $(w, 1)$ is a syndrome. Take $x_1 = 0$, $x_2 = w$, $x_3 = 1$ and $(w, 1)^T = syn(\mathbf{x})$.

Two vectors belong to the same coset if and only if they have the same syndrome.

For $\mathbf{x}, \mathbf{x}'$ in the same coset, $\mathbf{x} - \mathbf{x}' = \mathbf{c} \in \mathcal{C}$. Then $syn(\mathbf{x}) = H(\mathbf{x}' + \mathbf{c})^T = H(\mathbf{x}')^T = syn(\mathbf{x}')$. If $syn(\mathbf{x}) = syn(\mathbf{x}')$, then $H(\mathbf{x} - \mathbf{x}')^T = \mathbf{0}$ and $\mathbf{x} - \mathbf{x}' \in \mathcal{C}$. □

There is a one-to-one correspondence ψ between cosets of $\mathcal{C}$ and syndromes: $\psi(\mathbf{x} + \mathcal{C}) = H\mathbf{x}^T$.
(1) Both sets contain q^{n-k} elements. (2) If $\mathbf{y} \in \mathbf{x} + \mathcal{C}$, then $H\mathbf{y}^T = H\mathbf{x}^T$ (ψ well-defined). (3) Injectivity: if $\psi(\mathbf{x} + \mathcal{C}) = \psi(\mathbf{x}' + \mathcal{C})$, then $H\mathbf{x}^T = H(\mathbf{x}')^T$ which is equivalent to having both $\mathbf{x}, \mathbf{x}'$ in the same coset and thus $\mathbf{x} + \mathcal{C} = \mathbf{x}' + \mathcal{C}$.

$\mathcal{C}$ over $\mathbb{F}_4$ is given by: $(x_1) \mapsto (x_1, x_1, x_1 w)$.

$$H\mathbf{x}^T = \begin{bmatrix} 1 & 1 & 0 \\ w & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_1 + x_2 \\ wx_1 + x_3 \end{bmatrix}$$

Examples of $\psi(\mathbf{x} + \mathcal{C}) = H\mathbf{x}^T$ (4 out of the 16 cosets are illustrated):

$\mathbf{x} + \mathcal{C}$	$H\mathbf{x}^T$
$\mathcal{C}$	$(0,0)^T$
$(1,0,0) + \mathcal{C}$	$(1,w)^T$
$(0,1,0) + \mathcal{C}$	$(1,0)^T$
$(1,1,0) + \mathcal{C}$	$(0,w)^T$

ML Decoding.

Maximum likelihood ⇒Nearest neighbour decoding: decode the codeword $\hat{\mathbf{c}}$ closest to the received vector $\mathbf{y} = \mathbf{c} + \mathbf{e}$ ($\hat{\mathbf{c}}$ minimizes $d_H(\mathbf{y}, \mathbf{c})$).

ML Decoding.

Maximum likelihood ⇒Nearest neighbour decoding: decode the codeword $\hat{\mathbf{c}}$ closest to the received vector $\mathbf{y} = \mathbf{c} + \mathbf{e}$ ($\hat{\mathbf{c}}$ minimizes $d_H(\mathbf{y}, \mathbf{c})$).

- $d_H(\mathbf{y}, \mathbf{c}) = wt(\mathbf{y} - \mathbf{c}) = wt(\mathbf{e})$ so given $\mathbf{y}$, we are looking for a vector $\mathbf{e}$ of smallest weight such that $\mathbf{y} - \mathbf{e} \in \mathcal{C}$.

ML Decoding.

Maximum likelihood ⇒Nearest neighbour decoding: decode the codeword $\hat{\mathbf{c}}$ closest to the received vector $\mathbf{y} = \mathbf{c} + \mathbf{e}$ ($\hat{\mathbf{c}}$ minimizes $d_H(\mathbf{y}, \mathbf{c})$).

- $d_H(\mathbf{y}, \mathbf{c}) = wt(\mathbf{y} - \mathbf{c}) = wt(\mathbf{e})$ so given $\mathbf{y}$, we are looking for a vector $\mathbf{e}$ of smallest weight such that $\mathbf{y} - \mathbf{e} \in \mathcal{C}$.

ML Decoding and cosets.

$\mathbf{y} - \mathbf{e} \in \mathcal{C}$ if and only if $\mathbf{y}$ and $\mathbf{e}$ are in the same coset ⇒ we are looking for a vector $\mathbf{e}$ of smallest weight in the coset containing $\mathbf{y}$.

- We are looking for a coset leader of the coset containing $\mathbf{y}$.

Syndrome Decoding

$\mathcal{C}_s$ = coset consisting of vectors in $\mathbb{F}_q^n$ with syndrome $\mathbf{s}$.

Step 1. For each syndrome $\mathbf{s} \in \mathbb{F}_q^{n-k}$, choose a coset leader $\mathbf{e}_s$ of the coset $\mathcal{C}_s$. Create a table pairing the syndrome with the coset leader.

Step 2. After receiving $\mathbf{y}$, compute its syndrome.

Step 3. $\mathbf{y}$ is decoded as the codeword $\mathbf{y} - \mathbf{e}_s$.

This needs a table with q^{n-k} elements instead of q^n.

The (4,2) self-dual tetracode $\mathcal{C}$ over $\mathbb{F}_3$

The (4,2) self-dual tetracode $\mathcal{C}$ over $\mathbb{F}_3$

$$\underbrace{H\mathbf{x}^T}_{\text{syndrome}} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} x_1 + x_3 + x_4 \\ x_2 + x_3 - x_4 \end{bmatrix} = \underbrace{\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}}_{x_3=x_4=0}$$

$\mathbb{F}_3^{4-2}$	$H\mathbf{x}^T$	$\mathbf{x}+\mathcal{C}$	coset leader
$(0,0)$	$H(0,0,0,0)^T$	$\mathcal{C}$	(0,0,0,0)
$(0,1)$	$H(0,1,0,0)^T$	$(0,1,0,0)+\mathcal{C}$	(0,1,0,0)
$(0,2)$	$H(0,2,0,0)^T$	$(0,2,0,0)+\mathcal{C}$	(0,2,0,0)
$(1,0)$	$H(1,0,0,0)^T$	$(1,0,0,0)+\mathcal{C}$	(1,0,0,0)
$(1,1)$	$H(1,1,0,0)^T$	$(1,1,0,0)+\mathcal{C}$	$(1,1,0,0)$?
$(1,2)$	$H(1,2,0,0)^T$	$(1,2,0,0)+\mathcal{C}$	$(1,2,0,0)$?
$(2,0)$	$H(2,0,0,0)^T$	$(2,0,0,0)+\mathcal{C}$	(2,0,0,0)
$(2,1)$	$H(2,1,0,0)^T$	$(2,1,0,0)+\mathcal{C}$	$(2,1,0,0)$?
$(2,2)$	$H(2,2,0,0)^T$	$(2,2,0,0)+\mathcal{C}$	$(2,2,0,0)$?

The (4,2) self-dual tetracode $\mathcal{C}$ over $\mathbb{F}_3$

$(x_1, x_2) \mapsto (x_1, x_2, x_1 + x_2, x_1 - x_2)$.

$(1,1,0,0)$: $(x_1 + 1, x_2 + 1, x_1 + x_2, x_1 - x_2)$, we know we cannot have $x_1 + x_2 = 0 = x_1 - x_2$, take $x_1 = x_2 \Rightarrow$ $(x_1 + 1, x_1 + 1, 2x_1, 0)$, take $x_1 = 2 \Rightarrow$ $\boxed{wt(0,0,1,0) = 1}$.

$(1,2,0,0)$: $(x_1 + 1, x_2 + 2, x_1 + x_2, x_1 - x_2)$, take $x_2 = -x_1$, $(x_1 + 1, -x_1 + 2, 0, 2x_1)$, take $x_1 = 2$ and $\boxed{wt(0,0,0,1) = 1}$.

$(2,1,0,0)$: $wt(x_1 + 2, x_2 + 1, x_1 + x_2, x_1 - x_2) =$ $\boxed{wt(0,0,0,2) = 1}$ with $x_2 = -1$ and $x_1 = 1$

$(2,2,0,0)$: $wt(x_1 + 2, x_2 + 2, x_1 + x_2, x_1 - x_2) =$ $\boxed{wt(0,0,2,0) = 1}$ with $x_1 = x_2 = 1$.

The (4,2) self-dual tetracode $\mathcal{C}$ over $\mathbb{F}_3$

Step 1. For each syndrome $\mathbf{s} \in \mathbb{F}_q^{n-k}$, choose a coset leader $\mathbf{e}_s$ of the coset $\mathcal{C}_s$. Create a table pairing syndrome/coset leader.

$\mathbb{F}_3^{4-2}$	$H\mathbf{x}^T$	$\mathbf{x}+\mathcal{C}$	coset leader
$(0,0)$	$H(0,0,0,0)^T$	$\mathcal{C}$	(0,0,0,0)
$(0,1)$	$H(0,1,0,0)^T$	$(0,1,0,0)+\mathcal{C}$	(0,1,0,0)
$(0,2)$	$H(0,2,0,0)^T$	$(0,2,0,0)+\mathcal{C}$	(0,2,0,0)
$(1,0)$	$H(1,0,0,0)^T$	$(1,0,0,0)+\mathcal{C}$	(1,0,0,0)
$(1,1)$	$H(1,1,0,0)^T$	$(1,1,0,0)+\mathcal{C}$	(0,0,1,0)
$(1,2)$	$H(1,2,0,0)^T$	$(1,2,0,0)+\mathcal{C}$	(0,0,0,1)
$(2,0)$	$H(2,0,0,0)^T$	$(2,0,0,0)+\mathcal{C}$	(2,0,0,0)
$(2,1)$	$H(2,1,0,0)^T$	$(2,1,0,0)+\mathcal{C}$	(0,0,0,2)
$(2,2)$	$H(2,2,0,0)^T$	$(2,2,0,0)+\mathcal{C}$	(0,0,2,0)

Since every coset weight is at most $\lfloor \frac{3-1}{2} \rfloor$, there is a unique coset leader in each coset.

Syndrome Decoding

Step 1. Create a table pairing the syndrome $\mathbf{s} \in \mathbb{F}_q^{n-k}$ with the coset leader $\mathbf{e}_s$ of the coset $\mathcal{C}_s$.

Step 2. After receiving $\mathbf{y}$, compute its syndrome.

Step 3. $\mathbf{y}$ is decoded as the codeword $\hat{\mathbf{c}} = \mathbf{y} - \mathbf{e}_s$.

$\mathbf{s} \in \mathbb{F}_3^2$	$\mathbf{e}_s$
$(0,0)$	$(0,0,0,0)$
$(0,1)$	$(0,1,0,0)$
$(0,2)$	$(0,2,0,0)$
$(1,0)$	$(1,0,0,0)$
$(1,1)$	$(0,0,1,0)$
$(1,2)$	$(0,0,0,1)$
$(2,0)$	$(2,0,0,0)$
$(2,1)$	$(0,0,0,2)$
$(2,2)$	$(0,0,2,0)$

Syndrome Decoding

Step 1. Create a table pairing the syndrome $\mathbf{s} \in \mathbb{F}_q^{n-k}$ with the coset leader $\mathbf{e}_s$ of the coset $\mathcal{C}_s$.
Step 2. After receiving $\mathbf{y}$, compute its syndrome.
Step 3. $\mathbf{y}$ is decoded as the codeword $\hat{\mathbf{c}} = \mathbf{y} - \mathbf{e}_s$.

$\mathbf{s} \in \mathbb{F}_3^2$	$\mathbf{e}_s$
$(0,0)$	$(0,0,0,0)$
$(0,1)$	$(0,1,0,0)$
$(0,2)$	$(0,2,0,0)$
$(1,0)$	$(1,0,0,0)$
$(1,1)$	$(0,0,1,0)$
$(1,2)$	$(0,0,0,1)$
$(2,0)$	$(2,0,0,0)$
$(2,1)$	$(0,0,0,2)$
$(2,2)$	$(0,0,2,0)$

$(1,2) \mapsto \mathbf{c} = (1,2,0,2) \mapsto \mathbf{y} = (1,0,0,2)$, $\mathbf{s} = H\mathbf{y}^T = (0,1)$, $\hat{\mathbf{c}} =$

Syndrome Decoding

Step 1. Create a table pairing the syndrome $\mathbf{s} \in \mathbb{F}_q^{n-k}$ with the coset leader $\mathbf{e}_s$ of the coset $\mathcal{C}_s$.

Step 2. After receiving $\mathbf{y}$, compute its syndrome.

Step 3. $\mathbf{y}$ is decoded as the codeword $\hat{\mathbf{c}} = \mathbf{y} - \mathbf{e}_s$.

$\mathbf{s} \in \mathbb{F}_3^2$	$\mathbf{e}_s$
$(0,0)$	$(0,0,0,0)$
$(0,1)$	$(0,1,0,0)$
$(0,2)$	$(0,2,0,0)$
$(1,0)$	$(1,0,0,0)$
$(1,1)$	$(0,0,1,0)$
$(1,2)$	$(0,0,0,1)$
$(2,0)$	$(2,0,0,0)$
$(2,1)$	$(0,0,0,2)$
$(2,2)$	$(0,0,2,0)$

$(1,2) \mapsto \mathbf{c} = (1,2,0,2) \mapsto \mathbf{y} = (1,0,0,2)$, $H\mathbf{y}^T = (0,1)$, $\hat{\mathbf{c}} = (1,0,0,2) - (0,1,0,0) = (1,2,0,2) = \mathbf{c}$.

Syndrome Decoding

Remarks

- The tetracode has minimum distance 3, it can correct up to $\lfloor \frac{3-1}{2} \rfloor = 1$ error. Syndrome decoding achieves this: for one error (1) $\mathbf{y} = \mathbf{c} + \mathbf{e}$ where $\mathbf{e}$ has weight 1, (2) $\mathbf{e}$ is in the same coset as $\mathbf{y}$, (3) every coset (and thus the one in which $\mathbf{y}$ belongs) contains a unique coset leader, namely $\mathbf{e}$.
- If more than one error occurs, $\mathbf{y}$ will belong to one of the cosets but will not be not decoded, since it will have weight 2, and there is coset leader of weight 1 that will be decoded.

In general, for an (n, k) linear code $\mathcal{C}$ of minimum Hamming distance $d_H(\mathcal{C})$:

- It can correct up to $t = \lfloor \frac{d_H(\mathcal{C})-1}{2} \rfloor$ errors. Syndrome decoding achieves this: for up to t errors (1) $\mathbf{y} = \mathbf{c} + \mathbf{e}$ where $\mathbf{e}$ has weight at most t, (2) $\mathbf{e}$ is in the same coset as $\mathbf{y}$, thus this coset cannot have weight more than t (3) this coset contains a unique coset leader, namely $\mathbf{e}$.
- If more than t errors occur, $\mathbf{y}$ will belong to one of the cosets but will not be not decoded, since it will have weight more than t, and there is coset leader of weight at most t that will be decoded.

Syndrome Decoding

■ Remarks

In general, for an (n, k) linear code $\mathcal{C}$ of minimum Hamming distance $d_H(\mathcal{C})$:

- It can correct up to $t = \lfloor \frac{d_H(\mathcal{C})-1}{2} \rfloor$ errors. Syndrome decoding achieves this: for up to t errors (1) $\mathbf{y} = \mathbf{c} + \mathbf{e}$ where $\mathbf{e}$ has weight at most t, (2) $\mathbf{e}$ is in the same coset as $\mathbf{y}$, thus this coset cannot have weight more than t (3) this coset contains a unique coset leader, namely $\mathbf{e}$.
- If more than t errors occur, $\mathbf{y}$ will belong to one of the cosets but will not be not decoded, since it will have weight more than t, and there is coset leader of weight at most t that will be decoded.

Syndrome Decoding

Remarks

In this table, cosets are computed to emphasize the one-to-one correspondance with $\mathbb{F}_3^2$.

$\mathbb{F}_3^2$	$H\mathbf{x}^T$	$\mathbf{x}+\mathcal{C}$	coset leader
$(0,0)$	$H(0,0,0,0)^T$	$\mathcal{C}$	(0,0,0,0)
$(0,1)$	$H(0,1,0,0)^T$	$(0,1,0,0)+\mathcal{C}$	(0,1,0,0)
$(0,2)$	$H(0,2,0,0)^T$	$(0,2,0,0)+\mathcal{C}$	(0,2,0,0)
$(1,0)$	$H(1,0,0,0)^T$	$(1,0,0,0)+\mathcal{C}$	(1,0,0,0)
$(1,1)$	$H(1,1,0,0)^T$	$(1,1,0,0)+\mathcal{C}$	(0,0,1,0)
$(1,2)$	$H(1,2,0,0)^T$	$(1,2,0,0)+\mathcal{C}$	(0,0,0,1)
$(2,0)$	$H(2,0,0,0)^T$	$(2,0,0,0)+\mathcal{C}$	(2,0,0,0)
$(2,1)$	$H(2,1,0,0)^T$	$(2,1,0,0)+\mathcal{C}$	(0,0,0,2)
$(2,2)$	$H(2,2,0,0)^T$	$(2,2,0,0)+\mathcal{C}$	(0,0,2,0)

This could be done differently.

Consider instead cosets of weight at most 1 ($2n + 1$ of them).

$\mathbf{x} + \mathcal{C}$	coset leader
$\mathcal{C}$	$(0, 0, 0, 0)$
$(1, 0, 0, 0) + \mathcal{C}$	$(1, 0, 0, 0)$
$(2, 0, 0, 0) + \mathcal{C}$	$(2, 0, 0, 0)$
$(0, 1, 0, 0) + \mathcal{C}$	$(0, 1, 0, 0)$
$(0, 2, 0, 0) + \mathcal{C}$	$(0, 2, 0, 0)$
$(0, 0, 1, 0) + \mathcal{C}$	$(0, 0, 1, 0)$
$(0, 0, 2, 0) + \mathcal{C}$	$(0, 0, 2, 0)$
$(0, 0, 0, 1) + \mathcal{C}$	$(0, 0, 0, 1)$
$(0, 0, 0, 2) + \mathcal{C}$	$(0, 0, 0, 2)$

Syndrome Decoding

Remarks

More generally, one can compute cosets of weight 1 first ($(q-1)n$ of them), then cosets of weight 2 ($(q-1)\binom{n}{2}$ of them), then cosets of weight $3, \ldots, t$, this allows to decode up to t errors.

If the received vector has more than t errors, it will be either incorrectly decoded, or not decoded at all (if the syndrome is not in the table).

maximum likelihood decoding

Hamming spheres

Connection to error correction

Cosets and syndrome decoding