

Coding Theory: Equivalent Codes

Fundamental Problem

■ Equivalent codes

Given n and k , when are two (n, k) codes “essentially the same”?

Equivalent Codes

■ Example

Given the following two generator matrices G_1 and G_2 over \mathbb{F}_2

$$G_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \quad G_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix},$$

are the corresponding codes $\mathcal{C}_1, \mathcal{C}_2$ “the same”?

Equivalent Codes

■ Example

Given the following two generator matrices G_1 and G_2 over \mathbb{F}_2

$$G_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \quad G_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix},$$

are the corresponding codes $\mathcal{C}_1, \mathcal{C}_2$ “the same”?

Yes they are, since permuting the rows of G_2 (putting G_2 in a systematic form) gives G_1 .

Equivalent Codes

■ Example

Given the following two generator matrices G_1 and G_2 over \mathbb{F}_3

$$G_1 = \begin{bmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 \end{bmatrix}, \quad G_2 = \begin{bmatrix} 1 & 2 & 2 & 0 \\ 0 & 1 & 2 & 1 \end{bmatrix},$$

are the corresponding codes $\mathcal{C}_1, \mathcal{C}_2$ “the same”?

Equivalent Codes

■ Example

Given the following two generator matrices G_1 and G_2 over \mathbb{F}_3

$$G_1 = \begin{bmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 \end{bmatrix}, \quad G_2 = \begin{bmatrix} 1 & 2 & 2 & 0 \\ 0 & 1 & 2 & 1 \end{bmatrix},$$

are the corresponding codes $\mathcal{C}_1, \mathcal{C}_2$ “the same”?

In G_2 , add the second row to the first one to get:

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

Equivalent Codes

■ Example

Given the following two generator matrices G_1 and G_2 over \mathbb{F}_3

$$(x_1, x_2)G_1 = (x_1, x_2) \begin{bmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 \end{bmatrix} = (x_1, x_2, 2x_1 + x_2, 2x_1 + 2x_2),$$

$$(x_1, x_2)G_2 = (x_1, x_2) \begin{bmatrix} 1 & 2 & 2 & 0 \\ 0 & 1 & 2 & 1 \end{bmatrix} = (x_1, 2x_1 + x_2, 2x_1 + 2x_2, x_2),$$

Equivalent Codes

■ Example

Given the following two generator matrices G_1 and G_2 over \mathbb{F}_3

$$(x_1, x_2)G_1 = (x_1, x_2) \begin{bmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 \end{bmatrix} = (x_1, x_2, 2x_1 + x_2, 2x_1 + 2x_2),$$

$$(x_1, x_2)G_2 = (x_1, x_2) \begin{bmatrix} 1 & 2 & 2 & 0 \\ 0 & 1 & 2 & 1 \end{bmatrix} = (x_1, 2x_1 + x_2, 2x_1 + 2x_2, x_2),$$

Yes they are essentially the same codes, since we have the same codewords up to permuting coordinates.

Equivalent Codes

■ Example

$$(x_1, x_2)G_1 = (x_1, x_2, 2x_1 + x_2, 2x_1 + 2x_2),$$

$$(x_1, x_2)G_2 = (x_1, 2x_1 + x_2, 2x_1 + 2x_2, x_2)$$

$$(x_1, 2x_1+x_2, 2x_1+2x_2, x_2) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} = (x_1, x_2, 2x_1+x_2, 2x_1+2x_2)$$

Equivalent Codes

■ Example

Given the following two generator matrices G_1 and G_2 over \mathbb{F}_3

$$(x_1, x_2)G_1 = (x_1, x_2) \begin{bmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 \end{bmatrix} = (x_1, x_2, 2x_1 + x_2, 2x_1 + 2x_2),$$

$$(x_1, x_2)G_2 \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}}_{G_1} = (x_1, x_2) \begin{bmatrix} 1 & 2 & 2 & 0 \\ 0 & 1 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$= (x_1, 2x_1 + x_2, 2x_1 + 2x_2, x_2) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} = (x_1, x_2)G_1.$$

Permutation equivalent

Two linear codes \mathcal{C}_1 and \mathcal{C}_2 are permutation equivalent provided there is a permutation matrix P such that G_1 is a generator matrix of \mathcal{C}_1 if and only if $G_1 P$ is a generator matrix of \mathcal{C}_2 .

Applying P to a generator matrix rearrange the columns of the generator matrix.

A linear (n, k) code \mathcal{C} is permutation equivalent to a code which has generator matrix in systematic form.

Apply elementary row operations to any $k \times n$ generator matrix of \mathcal{C} to transform it into row echelon form: every row will be nonzero (it has rank k).

Each row contains a pivot, a 1st nonzero number from the left, always strictly to the right of the pivot of the row above.

Multiply every row so that the pivot is 1, repeat row operations so that zeroes are introduced above pivots. Because of the pivot positions, all the columns of \mathbf{I}_k are present, **permute** then.

A linear (n, k) code \mathcal{C} is permutation equivalent to a code which has generator matrix in standard form.

Consider the following generator matrix ($k = 3$ over \mathbb{F}_2):

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

Row echelon form (pivots are 1):

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

All the columns of \mathbf{I}_k are present, permute then.

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

(here best to permute rather than removing 0 above pivots.)

Monomial matrix

A square matrix with exactly one nonzero entry in each row and column.

$$M = \begin{bmatrix} 0 & a & 0 \\ 0 & 0 & b \\ c & 0 & 0 \end{bmatrix}$$

Over \mathbb{F}_2 , every monomial matrix is a permutation matrix:

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

Every monomial matrix can be written either as DP or PD' , D, D' are diagonal matrices, P is a permutation matrix.

$$M = \begin{bmatrix} 0 & a & 0 \\ 0 & 0 & b \\ c & 0 & 0 \end{bmatrix}$$

$$DP = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

$$PD' = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} c & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & b \end{bmatrix}$$

Monomial matrix:
convention

We usually choose
 $M = DP$ and apply it
on the right of row
vectors.

$$\mathbf{x}M = (x_1, x_2, x_3) \begin{bmatrix} 0 & a & 0 \\ 0 & 0 & b \\ c & 0 & 0 \end{bmatrix}$$

$$\underbrace{(x_1, x_2, x_3) \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix}}_{\text{scaling}} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

$$= (ax_1, bx_2, cx_3) \underbrace{\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}}_{\text{permutation}}$$

Monomially equivalent

Two linear codes \mathcal{C}_1 (with generator matrix G_1) and \mathcal{C}_2 are monomially equivalent provided there is a monomial matrix M such that G_1M is a generator matrix of \mathcal{C}_2 .

We can also say that $\mathcal{C}_2 = \mathcal{C}_1M$.

Monomial equivalence and permutation equivalence are the same for binary codes.

Monomially Equivalent Codes

■ Example

Given the following two generator matrices G_1 and G_2 over \mathbb{F}_3

$$G_1 = \begin{bmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 \end{bmatrix},$$

$$G_2 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix},$$

there is a monomial matrix M such that $G_1 M = G_2$, so $\mathcal{C}_2 = \mathcal{C}_1 M$.

Code Equivalences

■ One more equivalence

Suppose there exists an element ω which is a zero of $X^2 + X + 1 \pmod{2}$. Then $\omega \neq 0, 1$,

$$\omega^2 = \omega + 1 \pmod{2}, \quad \omega^3 = \omega(\omega + 1) = \omega^2 + \omega = 1 \pmod{2}.$$

\mathbb{F}_4

$+$	0	1	ω	ω^2	\cdot	0	1	ω	ω^2
0	0	1	ω	ω^2	0	0	0	0	0
1	1	0	ω^2	ω	1	0	1	ω	ω^2
ω	ω	ω^2	0	1	ω	0	ω	ω^2	1
ω^2	ω^2	ω	1	0	ω^2	0	ω^2	1	ω

Automorphisms of \mathbb{F}_q

A map σ from \mathbb{F}_q to itself, such that

$$\sigma(x + y) = \sigma(x) + \sigma(y),$$

$$\sigma(xy) = \sigma(x)\sigma(y),$$

$$\sigma(0) = 0 \text{ and } \sigma(1) = 1.$$

Automorphisms of \mathbb{F}_q

A map σ from \mathbb{F}_q to itself, such that

$$\sigma(x + y) = \sigma(x) + \sigma(y),$$

$$\sigma(xy) = \sigma(x)\sigma(y),$$

$$\sigma(0) = 0 \text{ and } \sigma(1) = 1.$$

Consider $\mathbb{F}_4 = \{0, 1, w, w^2 = w + 1\}$.

Automorphisms of \mathbb{F}_q

A map σ from \mathbb{F}_q to itself, such that

$$\sigma(x + y) = \sigma(x) + \sigma(y),$$

$$\sigma(xy) = \sigma(x)\sigma(y),$$

$$\sigma(0) = 0 \text{ and } \sigma(1) = 1.$$

Consider $\mathbb{F}_4 = \{0, 1, w, w^2 = w + 1\}$.

- $\sigma(0) = 0, \sigma(1) = 1.$

Automorphisms of \mathbb{F}_q

A map σ from \mathbb{F}_q to itself, such that

$$\begin{aligned}\sigma(x+y) &= \sigma(x) + \sigma(y), \\ \sigma(xy) &= \sigma(x)\sigma(y), \\ \sigma(0) &= 0 \text{ and } \sigma(1) = 1.\end{aligned}$$

Consider $\mathbb{F}_4 = \{0, 1, w, w^2 = w + 1\}$.

- $\sigma(0) = 0, \sigma(1) = 1.$
- $\sigma(w^2) = \sigma(w)\sigma(w)$
 $= \sigma(w) + \sigma(1) = \sigma(w) + 1.$ So
 $x = \sigma(w)$ satisfies $x^2 = x + 1.$
So $\sigma(w)$ can be either w or $w^2.$

Automorphisms of \mathbb{F}_q

A map σ from \mathbb{F}_q to itself, such that
 $\sigma(x + y) = \sigma(x) + \sigma(y)$,
 $\sigma(xy) = \sigma(x)\sigma(y)$,
 $\sigma(0) = 0$ and $\sigma(1) = 1$.

Consider $\mathbb{F}_4 = \{0, 1, w, w^2 = w + 1\}$.

- $\sigma(0) = 0, \sigma(1) = 1$.
- $\sigma(w^2) = \sigma(w)\sigma(w)$
 $= \sigma(w) + \sigma(1) = \sigma(w) + 1$. So
 $x = \sigma(w)$ satisfies $x^2 = x + 1$.
So $\sigma(w)$ can be either w or w^2 .
- Thus $\sigma : a + bw \mapsto a + bw$ or
 $\sigma : a + bw \mapsto a + bw^2, a, b \in \mathbb{F}_2$.

Equivalent

Two linear codes \mathcal{C}_1 and \mathcal{C}_2 are equivalent provided there is a monomial matrix M and an automorphism σ of \mathbb{F}_q such that $\mathcal{C}_1 M \sigma = \mathcal{C}_2$.

For a vector

$$\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_q^n, \\ \mathbf{x}\sigma = (\sigma(x_1), \dots, \sigma(x_n)).$$

For a codeword

$$\mathbf{c} = (c_1, \dots, c_n) \in \mathbb{F}_q^n \text{ and} \\ M = DP \text{ a monomial} \\ \text{matrix:}$$

$$\mathbf{c}M\sigma = \mathbf{c}DP\sigma$$

so

$$\mathcal{C}_1 M \sigma = \{\mathbf{c}DP\sigma, \mathbf{c} \in \mathcal{C}_1\}.$$

Code Equivalences

■ Example

Consider the code \mathcal{C}_1 over \mathbb{F}_4 with generator matrix

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & w \end{bmatrix}, \quad (x_1, x_2) \mapsto (x_1, x_2, x_1 + wx_2).$$

c	cσ	c	cσ
(0, 0, 0)	(0, 0, 0)	(0, w, w ²)	(0, w ² , w)
(1, 0, 1)	(1, 0, 1)	(1, w, w)	(1, w ² , w ²)
(w, 0, w)	(w ² , 0, w ²)	(w, w, 1)	(w ² , w ² , 1)
(w ² , 0, w ²)	(w, 0, w)	(w ² , w, 0)	(w, w ² , 0)
(0, 1, w)	(0, 1, w ²)	(0, w ² , 1)	(0, w, 1)
(1, 1, w ²)	(1, 1, w)	(1, w ² , 0)	(1, w, 0)
(w, 1, 0)	(w ² , 1, 0)	(w, w ² , w ²)	(w ² , w, w)
(w ² , 1, 1)	(w, 1, 1)	(w ² , w ² , w)	(w, w, w ²)

Equivalent

Two linear codes \mathcal{C}_1 and \mathcal{C}_2 are equivalent provided there is a monomial matrix M and an automorphism σ of \mathbb{F}_q such that $\mathcal{C}_1 M \sigma = \mathcal{C}_2$.

- Most general form of equivalence we will consider.
- For binary codes, permutation equivalence, monomial equivalence and equivalence are the same.
- For p -ary codes, monomial equivalence and equivalence are the same.

Equivalent

Two linear codes \mathcal{C}_1 and \mathcal{C}_2 are equivalent provided there is a monomial matrix M and an automorphism σ of \mathbb{F}_q such that $\mathcal{C}_1 M \sigma = \mathcal{C}_2$.

- Hamming distances are preserved by code equivalences (permutating, scaling, applying an automorphism, none changes the number of zero coordinates).
- Self-duality is preserved by permutation equivalence, but not by other equivalences.

For $r \geq 2$, any
 $(2^r - 1, 2^r - 1 - r, 3)$
binary code is equivalent
to the binary Hamming
code with these
parameters.

Consider a code \mathcal{C} with
 $n = 2^r - 1$, and $k = n - r$,
that is $n - k = r$. It has
a parity check matrix H
with $n - k = r$ rows, and
 n columns.

For $r \geq 2$, any $(2^r - 1, 2^r - 1 - r, 3)$ binary code is equivalent to the binary Hamming code with these parameters.

Consider a code \mathcal{C} with $n = 2^r - 1$, and $k = n - r$, that is $n - k = r$. It has a parity check matrix H with $n - k = r$ rows, and n columns.

- To create columns of length r over \mathbb{F}_2 , we have 2^r choices, and $2^r - 1$ distinct choices excluding the whole zero vector.
- If we try to repeat one column, the minimum distance drops since we have two columns which are multiples of each other. Therefore we can only obtain a Hamming code.

The $(4, 2)$ tetracode over \mathbb{F}_3 is equivalent to a Hamming code.

A generator matrix is

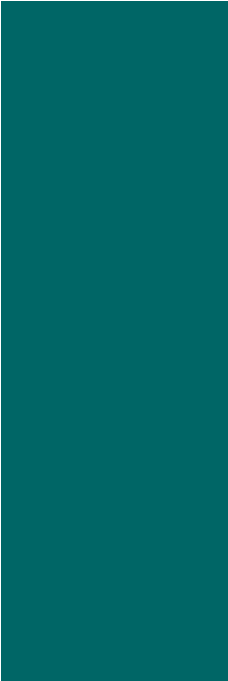
$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix}$$

which is also a parity check matrix since the code is self-dual.

- Over \mathbb{F}_3 , it is

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

- The columns contain all 1-dimensional subspaces of \mathbb{F}_3^2 , the $\frac{3^2-1}{3-1} = 4$ of them. So this is a ternary Hamming code.
- Finally the only perfect codes we know are Hamming codes.



Permutation equivalence

Monomial equivalence

Code equivalence