Coding Theory: Revision

A Generic Communication Channel

Transmitter | Channel | Receiver

$$\boxed{\text{Data } \mathbf{x}} \to \boxed{\text{Encoder}} \to \boxed{\text{Noise } \mathbf{e}} \to \boxed{\text{Decoder}} \to \boxed{\text{Decoded Data } \hat{\mathbf{x}}}$$

$$\mathbf{x} = (x_1, \ldots, x_k) \in \mathbb{F}_q^k \mapsto \mathbf{c} = \underbrace{(c_1, \ldots, c_n)}_{\text{codeword, } n \geq k} = (x_1, \ldots, x_k)G \mapsto \mathbf{c}+\mathbf{e} \mapsto \hat{\mathbf{x}}$$

Code Parameters

1. Length: n
2. Number of codewords, or dimension: k
3. alphabet: $\mathbb{F}_q$

Alphabet $\mathbb{F}_q$

1. $\mathbb{F}_p$, p a prime
2. $\mathbb{F}_q$, q a prime power

1. p a prime: working modulo p
2. $q = p^r$: working in $\mathbb{F}_p[X]/(p(X))$ for $p(X)$ a monic irreducible polynomial

Exercise. (a) What is the multiplicative inverse of 3 modulo 7?
(b) Provide a description of $\mathbb{F}_{25}$.

Exercise. (a) What is the multiplicative inverse of 3 modulo 7? (b) Provide a description of $\mathbb{F}_{25}$.

(a) The inverse x of 3 modulo 7 satisfies $3x \equiv 1 \pmod 7$, it is 5 because $15 \equiv 1 \pmod 7$.

Exercise. (a) What is the multiplicative inverse of 3 modulo 7? (b) Provide a description of $\mathbb{F}_{25}$.

(a) The inverse x of 3 modulo 7 satisfies $3x \equiv 1 \pmod 7$, it is 5 because $15 \equiv 1 \pmod 7$.
(b) To construct $\mathbb{F}_{25}$, since $25 = 5^2$, we need an irreducible polynomial of degree 2 modulo 5. Take for example $p(X) = X^2 + 2$. Then for $X = 0, 1, 2, 3, 4$, $p(X)$ is not zero, so the polynomial is irreducible. Then

$$\mathbb{F}_{25} = \{a_0 + a_1 w,\ a_0, a_1 \in \mathbb{F}_5\}$$

where $w^2 = -2$.

Alphabet $\mathbb{F}_q$

1. $\mathbb{F}_p$, p a prime
2. $\mathbb{F}_q$, q a prime power

1. Always pay attention to the alphabet, answers to questions usually depend on the choice of the alphabet.
2. Be cautious with multiplicative inverses, we do not use $1/x$ in modular arithmetic.

Length n

A codeword is an element of $\mathbb{F}_q^n$, that is a vector of length n.

1. $(0, 1, 0, 0) \in \mathbb{F}_2^4$, so $n = 4$,
2. $(0, \omega, \omega + 1, 0, 1) \in \mathbb{F}_4^5$, so $n = 5$.

Number of codewords

A code $\mathcal{C}$ is a family of codewords. We count the number of codewords $|\mathcal{C}|$.

If $\mathcal{C}$ is linear, then it is a subspace of $\mathbb{F}_q^n$, which has a dimension k.

1. The number of codewords is then $|\mathcal{C}| = q^k$ where k is the dimension of $\mathcal{C}$.
2. It also means that there are k codewords which generate all the possible codewords.

Exercise. (a) Is $\mathcal{C} = \{(0,0,0,0),(0,1,0,1),(1,1,0,0),(1,1,1,0),(0,0,0,1)\}$ over $\mathbb{F}_2$ linear? Compute $|\mathcal{C}|$. (b) Does there exist a code $\mathcal{C}$ of dimension 2 in $\mathbb{F}_{25}^4$? If yes, compute $|\mathcal{C}|$.

Exercise. (a) Is
$\mathcal{C} = \{(0,0,0,0),(0,1,0,1),(1,1,0,0),(1,1,1,0),(0,0,0,1)\}$ over $\mathbb{F}_2$ linear? Compute $|\mathcal{C}|$. (b) Does there exist a code $\mathcal{C}$ of dimension 2 in $\mathbb{F}_{25}^4$? If yes, compute $|\mathcal{C}|$.

(a) It cannot be linear because it contains 5 elements, 5 is not a power of 2. We cannot speak of dimension but $|\mathcal{C}| = 5$.

Exercise. (a) Is $\mathcal{C} = \{(0,0,0,0),(0,1,0,1),(1,1,0,0),(1,1,1,0),(0,0,0,1)\}$ over $\mathbb{F}_2$ linear? Compute $|\mathcal{C}|$. (b) Does there exist a code $\mathcal{C}$ of dimension 2 in $\mathbb{F}_{25}^4$? If yes, compute $|\mathcal{C}|$.

(a) It cannot be linear because it contains 5 elements, 5 is not a power of 2. We cannot speak of dimension but $|\mathcal{C}| = 5$.
(b) Yes, take for example $\mathcal{C} = \{a_0(1,0,0,1) + a_1(0,1,1,0),\ a_0, a_1 \in \mathbb{F}_{25}\}$, we have $|\mathcal{C}| = (25)^2$.

Matrices

When the code is linear, it has:

1. a generator matrix G
2. a parity check matrix H

1. A generator matrix G contains as rows a basis of $\mathcal{C}$: thus G is $k \times n$, it is often considered in systematic form: $G = [\mathbf{I}_k | A]$.
2. a parity check matrix H, of dimension $(n-k) \times n$, we have $H\mathbf{x}^T = 0 \iff \mathbf{x} \in \mathcal{C}$. Also if $G = [\mathbf{I}_k | A]$, $H = [-A^T | \mathbf{I}_{n-k}]$.

Exercise. Let $\mathcal{C}_1$ be an (n_1, k_1) linear code with generator matrix G_1, and $\mathcal{C}_2$ be an (n_2, k_2) linear code with generator matrix G_2. Let $\mathcal{C}$ be a code with generator matrix G given by

$$G = \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix}.$$

What are the parameters (n, k) of this code?

Exercise. Let $\mathcal{C}_1$ be an (n_1, k_1) linear code with generator matrix G_1, and $\mathcal{C}_2$ be an (n_2, k_2) linear code with generator matrix G_2. Let $\mathcal{C}$ be a code with generator matrix G given by

$$G = \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix}.$$

What are the parameters (n, k) of this code?

The length is $n = n_1 + n_2$. The dimension k is $k = k_1 + k_2$ because of the block structure of G that makes its $k_1 + k_2$ rows linearly independent.

Matrices

When the code is linear, it has:

1. a generator matrix G
2. a parity check matrix H

1. To compute a systematic form, pay attention to the alphabet.
2. To compute the dimension from G, make sure the rows are linearly independent.
3. When computing $H = [-A^T|\mathbf{I}]$, pay attention to the alphabet.

Code Performance

1. reliability: minimum Hamming distance d_H
2. efficiency: rate k/n

1. Compute d_H by trying to set information symbols to 0.
2. $d_H = d$ if and only if its parity check matrix H has a set of d linearly dependent columns but no set of $d-1$ linearly dependent columns.

   Use the parity check matrix, not the generator matrix.

Code Duality

$\mathcal{C}^\perp$ is the $(n, n-k)$ code generated by the rows of the parity check matrix H of $\mathcal{C}$, an (n, k) code. Also $\mathcal{C}^\perp = \{\mathbf{v} \in \mathbb{F}_q^n,\ \mathbf{c} \cdot \mathbf{v}^T = \mathbf{0} \text{ for all } \mathbf{c} \in \mathcal{C}\}$.

1. self-orthogonal: $\mathcal{C} \subseteq \mathcal{C}^\perp$
2. self-dual: $\mathcal{C} = \mathcal{C}^\perp$

1. for a code to be self-dual, we need $n = 2k$.
2. self-orthogonality is checked using the rows of G
3. self-dual = self-orthogonal + dimension argument
4. self-duality can be checked by computing H and showing it is equivalent to G

Bounds

$B_q(n,d)$ = number of codewords in a linear code over $\mathbb{F}_q$ of length n and minimum distance $\geq d$ ($A_q(n,d)$ for arbitrary codes)

1. the Sphere Packing Bound (SPB)
2. Gilbert Bound
3. Singleton Bound

SPB ($t = \lfloor \frac{d-1}{2} \rfloor$):

$$A_q(n,d) \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i}$$

Gilbert Bound:

$$B_q(n,d) \geq \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i}.$$

Singleton Bound:

$$B_q(n,d) \leq q^{n-d+1}$$

or $d \leq n-(k-1)$.

Code Families

1. Perfect codes
2. MDS codes
3. Hamming Codes
4. Reed-Mueller Codes
5. Golay Codes
6. Reed-Solomon Codes
7. Cyclic codes

Perfect codes

Codes meeting the sphere packing bound:

$$A_q(n,d) \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i}$$

$t = \lfloor \frac{d-1}{2} \rfloor$.

The $(4,2,3)_3$ tetracode is perfect. The code contains $3^2 = 9$ codewords and

$$SPB = \frac{3^4}{\sum_{i=0}^{1} \binom{4}{i} 2^i} = \frac{3^4}{1+8} = 3^2.$$

MDS codes

Codes reaching the Singleton bound:

$$B_q(n,d) \leq q^{n-d+1}$$

or $d \leq n-(k-1)$. MDS = maximum distance separable.

The $(4,1)_2$ repetition code is MDS.

$$d = 4 = n-(k-1) = 4.$$

Reed-Solomon codes are MDS.

Hamming Codes

For $n = 2^r - 1$, $r \geq 2$, and q a prime power, codes whose parity check matrix is having as columns a nonzero vector from each 1-dimensional subspace of $\mathbb{F}_q^r$. Their Hamming distance is 3.

For $r = 2$ and $q = 3$,

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

For $r = 3$ and $q = 2$:

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

Reed-Mueller Codes

Binary codes of length 2^m. $\mathcal{R}(0,m) =$ repetition code, $\mathcal{R}(m,m) = \mathbb{F}_2^{2^m}$ For $1 \leq r < m$, $\mathcal{R}(r,m) = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}),\ \mathbf{u} \in \mathcal{R}(r,m-1),\ \mathbf{v} \in \mathcal{R}(r-1,m-1)\}$ is the rth order binary Reed-Muller code.

Generator matrix $G(r,m)$:

$$\begin{bmatrix} G(r,m-1) & G(r,m-1) \\ \mathbf{0} & G(r-1,m-1) \end{bmatrix}.$$

For $m = 3$ and $1 \leq r = 1 < 3$

$$G(1,3) = \begin{bmatrix} G(1,2) & G(1,2) \\ \mathbf{0} & G(0,2) \end{bmatrix}$$

$$G(1,2) = \begin{bmatrix} G(1,1) & G(1,1) \\ \mathbf{0} & G(0,1) \end{bmatrix} =$$

$$\left[\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 1 & 1 \end{array}\right]$$

Reed-Mueller Codes

Binary codes of length 2^m. $\mathcal{R}(0,m) =$ repetition code, $\mathcal{R}(m,m) = \mathbb{F}_2^{2^m}$ For $1 \leq r < m$, $\mathcal{R}(r,m) = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}),\ \mathbf{u} \in \mathcal{R}(r,m-1),\ \mathbf{v} \in \mathcal{R}(r-1,m-1)\}$ is the rth order binary Reed-Muller code.

Dimension

$$\binom{m}{0} + \binom{m}{1} + \ldots + \binom{m}{r}.$$

Minimum Hamming distance:

$$d_H(\mathcal{R}(r,m)) = 2^{m-r}.$$

Golay Codes

4 codes: $\mathcal{G}_{24}$, $\mathcal{G}_{23}$ (binary) and $\mathcal{G}_{12}$, $\mathcal{G}_{11}$ (ternary).

Reed-Solomon Codes

Choose nonzero $v_1, \ldots, v_n$ and distinct $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$. Set $\mathbf{v} = (v_1, \ldots, v_n)$ and $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$. For $k \leq n$: $GRS_{n,k}(\boldsymbol{\alpha}, \mathbf{v}) =$ $\{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)), f(X$ $\mathbb{F}_q[X],\ \deg f(X) \leq$ $k-1\}$. They are MDS.

Take $\mathbb{F}_q = \mathbb{F}_4$, and choose $k = 2$, so $f(X) = f_0 + f_1 X$.

Choose $\alpha_1 = 1$, $\alpha_2 = w$, $\alpha_3 = w^2$ (thus $n = 3$).

$GRS_{3,2}((1, w, w^2), \mathbf{1}) = \{(f_0 + f_1, f_0 + f_1 w, f_0 + f_1 w^2),\ f_0, f_1 \in \mathbb{F}_4\}$.

Please pay attention to the size of $\mathbb{F}_q$ with respect to the length n.

Cyclic codes

A linear code $\mathcal{C}$ of length n such that for each vector $\mathbf{c} = (c_0, \ldots, c_{n-1})$ in $\mathcal{C}$, the vector $(c_{n-1}, c_0, \ldots, c_{n-2})$ in $\mathcal{C}$.

1. Working in $\mathbb{F}_q[X]/(X^n - 1)$ $\mathcal{C} = \{q(X)g(X),\ q(X) \in \mathbb{F}_q[X], \deg(q(X)) < n - r\}$, for a generator polynomial $g(X)$ (a nonzero polynomial $g(X)$ of lowest degree r in $\mathcal{C}$).
2. If $\deg g(X) = r$, the dimension of $\mathcal{C}$ is $k = n - r$.

3. For a generator polynomial $g(X) = \sum_{i=0}^{r} g_i X^i$ of degree r:

$$G = \begin{bmatrix} g_0 & g_1 & \dots & g_{r-1} & g_r & 0 & \dots & 0 & \\ 0 & g_0 & g_1 & \dots & g_{r-1} & g_r & 0 & \dots & 0 \\ \vdots & & \ddots & \ddots & & & & & \\ 0 & & 0 & g_0 & g_1 & & g_{r-1} & g_r & \end{bmatrix}$$

4. To construct a generator matrix in systematic form, encode the message polynomials $m(X) = X^i$ for $i = 0, \dots, k-1$.
5. There is a correspondance between divisors $g(X)$ of $X^n - 1$ and cyclic codes of length n.

5. The check polynomial $h(X)$ satisfies

$$g(X)h(X) = X^n - 1.$$

6. $\mathcal{C} = \{c(X),\ \deg c(X) \leq n-1,\ c(X)h(X) \equiv 0 \pmod{X^n - 1}\}$
7. If $h(X) = \sum_{i=0}^{k} h_i X^i$ of degree k, a parity-check matrix H is:

$$H = \begin{bmatrix} h_k & h_{k-1} & \dots & h_1 & h_0 & 0 & \dots & 0 & \\ 0 & h_k & h_{k-1} & \dots & h_1 & h_0 & 0 & \dots & 0 \\ \vdots & & \ddots & \ddots & & & & & \\ 0 & & 0 & h_k & h_{k-1} & & h_1 & h_0 & \end{bmatrix}$$

and $\mathcal{C}^{\perp}$ is the cyclic code generated by the polynomial $h^{[-1]}(X)$.

BCH Bound

Let $\mathcal{C}$ be an (n, k, d) cyclic code over $\mathbb{F}_q$ with defining set $T = \cup_s C_s$,

$$C_s = \{s, sq, \ldots, sq^{u-1}\} \pmod{n}.$$

If T contains $\delta - 1$ consecutive elements for some integer δ, then

$$d \geq \delta.$$

Consider the binary code generated by

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

It is cyclic since $(1,0,1,1,1,0,0) \xrightarrow{shift} (0,1,0,1,1,1,0) \xrightarrow{shift}$ $(0,0,1,0,1,1,1) \xrightarrow{shift} (1,0,0,1,0,1,1) \xrightarrow{shift}$ $(1,1,0,0,1,0,1) \xrightarrow{shift} (1,1,1,0,0,1,0) \xrightarrow{shift} (0,1,1,1,0,0,1)$. It has generator polynomial $g(X) = 1 + X^2 + X^3 + X^4$ and check polynomial $h(X) = 1 + X^2 + X^3$.

Since $h(X) = 1 + X^2 + X^3$, its parity check matrix is

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Since $g(X) = 1 + X^2 + X^3 + X^4 = (X+1)(X^3 + X + 1) = (X+1)(X-\alpha)(X-\alpha^2)(X-\alpha^4)$ over $\mathbb{F}_2$, with defining set $T = C_0 \cup C_1 = \{0, 1, 2, 4\}$ which contains a set $\{0, 1, 2\}$ of $v = 3 = \delta - 1$ consecutive elements. Thus

$$d \geq 4.$$

Modifying Codes

1. Puncturing
2. Extending
3. Equivalence

Puncturing

For a linear $(n, k, d)_q$ code $\mathcal{C}$, puncturing means deleting the same coordinate i in each codeword. The resulting code is denoted by $\mathcal{C}^*$.

(1) if $d > 1$, $\mathcal{C}^*$ is an $(n-1, k, d^*)$ code where $d^* = d - 1$ if $\mathcal{C}$ has a minimum weight codeword with a nonzero ith coordinate and $d^* = d$ otherwise.
(2) if $d = 1$, $\mathcal{C}^*$ is an $(n-1, k, 1)$ code if $\mathcal{C}$ has no codeword of weight 1 whose nonzero entry is in coordinate i, otherwise, if $k > 1$, $\mathcal{C}^*$ is an $(n-1, k-1, d^*)$ code with $d^* \geq 1$.

Extending

If $\mathcal{C}$ is an $(n,k,d)_q$ code, the extended code $\hat{\mathcal{C}}$ is the code $\{(x_1,\ldots,x_n,x_{n+1}) \in \mathbb{F}_q^{n+1},\ (x_1,\ldots,x_n) \in \mathcal{C},\ x_1+\cdots+x_{n+1}=0\}$

- $\hat{G}$ is obtained by adding an extra column to G, so that the sum of the coordinates of each row of $\hat{G}$ is 0.
- $\hat{H} = \left[\begin{array}{ccc|c} 1 & \ldots & 1 & 1 \\ \hline & & & 0 \\ & H & & \vdots \\ & & & 0 \end{array}\right]$
- Minimum distance: $d_H(\hat{\mathcal{C}}) = d_H(\mathcal{C})$ or $d_H(\mathcal{C})+1$.

Equivalence

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

1. $P \Rightarrow$ permutation equivalence
2. $M = DP \Rightarrow$ monomial equivalence
3. $M\sigma \Rightarrow$ equivalence