Coding and Information Theory
Chapter 7:
Linear Codes

Xuejun Liang

2019 Fall

Chapter 7: Linear Codes

1. Matrix Description of Linear Codes
2. Equivalence of Linear Codes
3. Minimum Distance of Linear Codes
4. The Hamming Codes
5. The Golay Codes
6. The Standard Array
7. Syndrome Decoding

Key content in this chapter

- Will study linear codes in greater detail by applying elementary linear algebra and matrix theory
  - including an even simpler method for calculating the minimum distance.
- Theoretical background required includes
  - Topics such as linear independence, dimension, and row and column operations
  - Linear space on a finite field

7.1 Matrix Description of Linear Codes

- Given a linear code $C \subseteq V = F^n$ and let dim(C) = k. A **generator matrix *G*** for C is defined as a $k \times n$ matrix, in which the row vectors are a basis of C.
- Example 7.1
  - The repetition code R_n over F has a single basis vector u_1 = 11 . . . 1, so it has a generator matrix G = (11 … 1)
- Example 7.2

The parity-check code P_n over F has basis u_1, …, u_{n-1} where each $u_i = e_i - e_n$ in terms of the standard basis vectors e_1, ..., e_n of V, so it has a generator matrix G

$$G = \begin{pmatrix} 1 & & & & -1 \\ & 1 & & & -1 \\ & & \ddots & & \vdots \\ & & & 1 & -1 \end{pmatrix}$$

Matrix Description of Linear Codes

- Example 7.3

  A basis u_1 = 1110000, u_2 = 1001100, u_3 = 0101010, u_4 = 1101001 for the binary Hamming code H_7 was given in Example 6.5. So this code has a generator matrix G.

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

- Given a linear code $C \subseteq V = F^n$ and let dim(C) = k. Encoding of source $A = F^k$ is a linear isomorphism $A \to C$ ($\boldsymbol{a} \in A \mapsto \boldsymbol{u} \in C$) given by the matrix G

$$\boldsymbol{u} = \boldsymbol{a}G$$

- **Thus encoding is multiplication by a fixed matrix**

Matrix Description of Linear Codes

- Example 7.4
  - The repetition code R_n has k = 1, so A = F^1 = F. Each **a** = $a \in A$ is encoded as $\boldsymbol{u}$ = $\boldsymbol{a}G$ = $a \ldots a \in R_n$.
- Example 7.5
  - If C = P_n then $k = n - 1$, so A = F^{n-1}. Each **a** = $a_l \ldots a_{n-l}$ $\in A$ is encoded as **u** = **a**G = $a_l \ldots a_{n-l}a_n$, where $a_n = -(a_l + \ldots + a_{n-1})$, so $\sum_i a_i = 0$
- Example 7.6
  - If $C = H_7$ then n = 7 and k = 4, so A = F_2^4. Each **a** = $a_1 \ldots a_4 \in$ A is encoded as **u** = **a**$G \in H_7$. For example, a = 0110

Matrix Description of Linear Codes

- Recall: How to construct the code for **a** = $a_1a_2a_3a_4$
  - Let the code word **u** = $u_1u_2u_3u_4u_5u_6u_7$
  - Bits $u_3 = a_1$, $u_5 = a_2$, $u_6 = a_3$, and $u_7 = a_4$
  - Bits u_1, u_2, u_4 for checking, determined by

$$\begin{aligned} u_4 + u_5 + u_6 + u_7 &= 0 \\ u_2 + u_3 + u_6 + u_7 &= 0 \\ u_1 + u_3 + u_5 + u_7 &= 0 \end{aligned}$$

$$\begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \\ u_6 \\ u_7 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 + a_4 \\ a_1 + a_3 + a_4 \\ a_1 \\ a_2 + a_3 + a_4 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = a_1 \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + a_2 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + a_3 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + a_4 \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Matrix Description of Linear Codes

- Given a linear code $C \subseteq V = F^n$ and let dim(C) = k. C consists of all solutions of **a set of $\boldsymbol{n}$ - $\boldsymbol{k}$ simultaneous linear equations**.
- Example 7.7
  - The repetition code R_n consists of the vectors $v = v_1 \ldots v_n \in V$ satisfying $v_1 = \cdots = v_n$, which can be regarded as a set of n - k = n - 1 simultaneous linear equations $\boldsymbol{v_i} - \boldsymbol{v_n} = \boldsymbol{0}$ (i =1, .. . , n - 1).
- Example 7.8
  - The parity-check code P_n (which has n - k = 1) is the subspace of V defined by the single linear equation $\boldsymbol{v_1} + \cdots + \boldsymbol{v_n} = \boldsymbol{0}$.

Matrix Description of Linear Codes

- Example 7.9
  - The Hamming code H_7 consists of the vectors $v = v_1 \dots v_7 \in V = F_2^7$ satisfying

$$v_4 + v_5 + v_6 + v_7 = 0,$$

$$v_2 + v_3 + v_6 + v_7 = 0,$$

$$v_1 + v_3 + v_5 + v_7 = 0.$$

- These equations are called **parity-check equations**
- Their matrix H of coefficients is called a **parity-check matrix** for C

Matrix Description of Linear Codes

- Lemma 7.10
  - Let C be a linear code, contained in V, with parity-check matrix H, and let $v \in V$. Then $v \in C$ if and only if $vH^T = 0$, where H^T denotes the transpose of the matrix H.
- Examples: Compute **parity-check matrix** H for C
  - 7.11: The repetition code R_n.
  - 7.12: The parity-check code P_n.
  - 7.13: The Hamming code H_7.

Matrix Description of Linear Codes

- H can be viewed as the matrix of a linear transformation $h: V \to W = F^{n-k}$
  - $\boldsymbol{v} \mapsto h(\boldsymbol{v}) = \boldsymbol{v}H^T$
- We have
  - $C = \ker(h) = \{\boldsymbol{v}: h(\boldsymbol{v}) = 0\}$
  - $im(h) = \{h(\boldsymbol{v}): v \in V\}$
  - $\dim(V) = \dim(\ker(h)) + \dim(im(h))$
  - H has rank $n-k$.
- So, n-k rows of H forms a basis of a linear space $D \subseteq V$ of dimension n-k. This linear code, with generator matrix H, called the **dual code** of C.

Matrix Description of Linear Codes

- A scalar product on $V = F^n$ is defined as
  - $u \cdot v = (u_1 \ldots u_n) \cdot (v_1 \ldots v_n) = u_1 v_1 + \cdots + u_n v_n \in F$
- ***u*** and **v** are orthogonal if ***u·v*** = 0
- We have

$$\mathcal{D} = \mathcal{C}^{\perp} = \{\, \mathbf{w} \in \mathcal{V} \mid \mathbf{v}.\mathbf{w} = 0 \ \text{ for all } \ \mathbf{v} \in \mathcal{C} \,\}$$

- Example 7.14
  - Let q = 2, let n = 2m, and let C be the linear code with basis vectors $u_i = e_{2i-1} + e_{2i}$ for i = 1, ..., m. we have $C = C^{\perp}$.

Matrix Description of Linear Codes

- Example 7.15
  - The repetition code R_n is spanned by **1** = 1 ... 1, so

    $$\mathcal{R}_n^{\perp} = \{\mathbf{w} \in \mathcal{V} \mid \mathbf{1}.\mathbf{w} = 0\} = \{\mathbf{w} \in \mathcal{V} \mid w_1 + \cdots + w_n = 0\} = \mathcal{P}_n$$
  - and similarly, $P_n^{\perp} = R_n$
- Example 7.16
  - The code $H_7^{\perp}$ is a linear [7, 3]-code over F_2
- Lemma 7.17
  - Let C be a linear $[n, k]$-code over F with generator matrix G, and let H be a matrix over F with n columns and n - k rows. Then H is a parity-check matrix for C if and only if H has rank n - k and satisfies GH^{T} = 0.

7.2 Equivalence of Linear Codes

- The elementary row operations of matrix consist of
  - permuting rows,
  - multiplying a row by a non-zero constant, and
  - replacing a row r_i with $r_i + ar_j$ where $j \neq i$ and $a \neq 0$.
- Two linear codes C_1 and C_2 are **equivalent** if they have generator matrices G_1 and G_2 which differ only by elementary row operations and permutations of columns.
  - Elementary row operations on generator G may change the basis for C, but they do not change the subspace C.
  - Permutations of columns of G may change C, but the new code will differ from C only in the order of symbols within code-words.

Equivalence of Linear Codes

- By systematically using elementary row operations and column permutations, one can convert any generator matrix into the form

$$G = (I_k \mid P) = \begin{pmatrix} 1 & & & & * & * & \dots & * \\ & 1 & & & * & * & \dots & * \\ & & \ddots & & \vdots & \vdots & & \vdots \\ & & & 1 & * & * & \dots & * \end{pmatrix} \qquad (7.2)$$

- We then say that G (or C) is in systematic form.
  - In this case, each $\boldsymbol{a} = a_1 \dots a_k \in F^k$ is encoded as

$$\mathbf{u} = \mathbf{a}G = a_1 \dots a_k a_{k+1} \dots a_n$$

  - where $a_1 \dots a_k$ are information digits and $a_{k+1} \dots a_n = \boldsymbol{a}P$ is a block of n - k check digits.

Equivalence of Linear Codes

- Example 7.18
  - The generator matrices G for the codes R_n and P_n are in systematic form.
- Example 7.19.
  - The generator matrix G for H_7, is not in systematic form.
  - But, it can be transformed into systematic form.
- If we have a generator matrix $G = (I_k|P)$ in systematic form for a linear code C, then we can find a parity-check matrix for C.

$$H = (-P^{\mathrm{T}} \mid I_{n-k}) \qquad (7.3)$$

  - This is the systematic form for a parity-check matrix

Equivalence of Linear Codes

- Example 7.20
  - Parity-check matrix in systematic form for the code R_n
- Example 7.21
  - Parity-check matrix in systematic form for the code P_n
- Example 7.22
  - Parity-check matrix in systematic form for the code H_7
- Theorem 7.23 (the Singleton bound (Exercise 6.18) for linear codes)
  - If C is a linear code of length n, dimension k, and minimum distance d, then

$$d \leq 1 + n - k.$$

Equivalence of Linear Codes

- Example 7.24
  - The Singleton bound is attained by R_n, with k = 1 and d = n, and by P_n, with k = n - 1 and d = 2;
  - But, not by H_7, with d = 3 and 1 + n - k = 4,
- Corollary 7.25
  - A t-error-correcting linear [n, k]-code requires at least $2t$ check digits.
- Example 7.26
  - The linear codes R_3 and H_7 both have t = 1; the number of check digits is n - k = 2 or 3 respectively.

7.3 Minimum Distance of Linear Codes

- Theorem 7.27
  - Let C be a linear code of minimum distance d, and let H be a parity-check matrix for C. Then d is the minimum number of linearly dependent columns of H.
- Meaning of linearly dependent of columns of H
  - One column $\boldsymbol{c_i}$ linearly dependent, then $\boldsymbol{c_i} = \mathbf{0}$
  - Two columns $\boldsymbol{c_i}$ and $\boldsymbol{c_j}$ linearly dependent, then $\boldsymbol{c_i}$ is multiple of $\boldsymbol{c_j}$ (or $\boldsymbol{c_j}$ is multiple of $\boldsymbol{c_i}$).
  - So, $d \geq 3$ if and only if the columns of H are non-zero and none is a multiple of any other.
- Example 7.28
  - The parity-check matrix H = (1 1 … 1) for P_n has its columns non-zero and equal , so P_n has minimum distance d = 2.

Minimum Distance of Linear Codes

- Example 7.29
  - In the parity-check matrix H for R_n, any set of n - 1 columns are linearly independent, while $c_1 + \cdots + c_n = 0$. So d = n.
- Example 7.30
  - Now, look at the parity-check matrix H for H_7

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

- Corollary 7.31
  - There is a t-error-correcting linear $[n, k]$-code over F if and only if there is an $(n - k) \times n$ matrix H over F, of rank n - k, with every set of $2t$ columns linearly independent.

7.4 The Hamming Codes

- For a 1-error-correcting binary linear code, put t = 1 and q = 2 in the sphere-packing bound (Corollary 6.17), so the condition for a perfect code becomes

$$2^{n-k} = 1 + \binom{n}{1} = 1 + n$$

- Let c = n - k (the number of check digits), then this condition is equivalent to

$$n = 2^c - 1. \tag{7.4}$$

- So

$c =$	1	2	3	4	5	...
$n =$	1	3	7	15	31	...
$k =$	0	1	4	11	26	...

The Hamming Codes

Construct codes with these parameters on $F_2 = \{0,1\}$

- By Corollary 7.31, need to construct a c x n matrix H over F_2, of rank c, with every pair of columns linearly independent (non-zero and distinct).
- Columns of H must consist of all 2^c - 1 non-zero binary vectors of length c, in some order.
- This matrix H has rank of c. Use it as the parity-check matrix, we have a code C with these parameters. This code is called the **binary Hamming code $\boldsymbol{H_n}$** of length n = $2^c - 1$.

The Hamming Codes

- Example 7.32
  - H_3 has the parity checking matrix $H = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$
  - H_3 is R_3 !!!
- Note: The rate of H_n will approaches to 1.

$$R = \frac{k}{n} = \frac{2^c - 1 - c}{2^c - 1} \to 1$$

- Nearest neighbor decoding with H_n
  - The receiver computes $s = vH^T$, called the syndrome of v. If s = 0, the receiver decodes v as $\Delta(v) = v$, and if s = ${c_i}^T$ (the i-th column of H) then $\Delta(v) = v - e_i$.

The Hamming Codes

- Example 7.33
  - Let us use H_7, with parity-check matrix

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

  - Suppose that u = 1101001 is sent, and v = 1101101 is received, so the error-pattern is e = e_5.
  - The syndrome is $s = vH^T$ =100, which is the transpose ${c_5}^T$ of the fifth column of H.
  - This indicates an error in the fifth position, so changing this entry of v we get $\Delta(v)$ = 1101001 = u

The Hamming Codes

- Using the parity checking matrix as below, then a non-zero syndrome is the binary representation of the position i where a single error e, has appeared

$$H = \begin{array}{c} \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \\ \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{matrix} \end{array}$$

- Example 7.34
  - Verify this using example 7.33
  - Note: need to perform a column permutation (1362547) to change between the two representations.

Construction of perfect 1-error-correcting linear codes for prime-powers q > 2

- We take the columns of H to be

$$n = \frac{q^c - 1}{q - 1} = 1 + q + q^2 + \cdots + q^{c-1}$$

  pairwise linearly independent vectors of length c over F_q.
- The resulting linear code has length n, dimension k = n - c, and minimum distance d = 3, so t = 1.
- As in the binary case, $R \to 1$ as $c \to \infty$, but $\mathrm{Pr}_E \nrightarrow 0$.
- Example 7.35
  - If q = 3 and c = 2, then n = 4 and k =2. Then a perfect 1-error-correcting linear [4, 2]-code over F_3 can be given by H. H = ?

7.5 The Golay Codes

- Skip this section

7.6 The Standard Array

- Suppose $C \subseteq V$ is a linear code. The standard array of C is essentially a table in which the elements of V are arranged into cosets of the subspace C.
- Suppose that $C = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_M\}$ is a linear code with $M = q^k$ elements. Assume $\boldsymbol{u_1} = \mathbf{0}$.
- For i = 1,2,3, ..., let the i-th row consist of the elements of the coset of C.

$$\mathbf{v}_i + C = \{\mathbf{v}_i + \mathbf{u}_1 \ (= \mathbf{v}_i),\ \mathbf{v}_i + \mathbf{u}_2,\ \ldots,\ \mathbf{v}_i + \mathbf{u}_M\}$$

  where $wt(v_i) \leq wt(v_{i+1}), i = 1, \ldots, q^{n-k} - 1$ and v_i is not in the previous (< i) rows.

- A horizontal line across the array, immediately under the last row to satisfy $wt(v_i) \leq t$, where $t = \lfloor (d-1)/2 \rfloor$.

The Standard Array

- Example 7.39
  - Let C be the binary repetition code R$_4$ of length n = 4, so q = 2, k = 1 and the code-words are $\boldsymbol{u_1}$ = **0** = 0000 and $\boldsymbol{u_2}$ = **1** = 1111
  - There are $q^{n-k} = 8$ cosets of C in V, each with two vectors
  - So, standard array has 8 rows:

$$v_1 + C, v_2 + C, \dots, v_8 + C$$

$v_1 = has\ weight\ 0$
$v_2\ to\ v_5\ has\ weight\ 1$
$v_6, v_7, v_8\ has\ weight\ 2$

$v_1 + C$	0000	1111
$v_2 + C$	1000	0111
$v_3 + C$	0100	1011
$v_4 + C$	0010	1101
$v_5 + C$	0001	1110
$v_6 + C$	1100	0011
$v_7 + C$	1010	0101
$v_8 + C$	1001	0110

The Standard Array

- Lemma 7.40
  a) If v is in the j-th column of the standard array (that is, $v = v_i + u_j$ for some i), then $u_j$is a nearest code-word to v.
  b) If, in addition, v is above the line in the standard array (that is, $wt(v_i) \leq t$),then u_j is the unique nearest code-word to v.
- Thus C is perfect if and only if the entire standard array is above the line
  - The sphere $S_t(u_j)$ of radius t about u_j is the part of the j-th column above the line.

The Standard Array

- Decoding rule
  - Suppose that a code-word $u \in C$ is transmitted, and $v = u + e \in V$ is received, where e is the error-pattern.
  - The receiver finds $v = v_i + u_j$ in the standard array, and decides that $\Delta(v) = u_j$ (u_j is header of a column)
- Note this rule gives correct decoding if and only if the error-pattern is a coset leader ($e = v_i$).
- Example 7.41
  - Let $C = R_4$. Suppose that $\boldsymbol{u}$ = 1111 is sent, and the error-pattern is e = 0100, $v =$? And $u_j =$?
  - How when e = 0110?

7.7 Syndrome Decoding

- If H is a parity-check matrix for a linear code $C \subseteq V$ then the syndrome of a vector $v \in V$ is the vector

$$\mathbf{s} = \mathbf{v}H^{\mathrm{T}} \in F^{n-k} \qquad (7.8)$$

- Lemma 7.42
  - Let C be a linear code, with parity-check matrix H, and let $v, v' \in V$ have syndromes s, s'. Then v and v' lie in the same coset of C if and only if $s = s'$.
- This shows that
  - A vector $\boldsymbol{v} \in V$ lies in the i-th row of the standard array if and only if it has the same syndrome as $\boldsymbol{v_i}$, that is, $\boldsymbol{v}H^T = \boldsymbol{v_i}H^T$.
- A syndrome table can be created with each row having a coset leader $\boldsymbol{v_i}$ and its syndrome $\boldsymbol{s_i}$ $(= \boldsymbol{v_i}H^T)$.

Syndrome Decoding

- Example 7.43
  - Let C be the binary repetition code R_4, with standard array as given in Example 7.39, so the coset leaders $\boldsymbol{v_i}$ are the words in its first column.
  - Apply the parity-check matrix given in Example 7.11.

$$H = \begin{pmatrix} 1 & & & -1 \\ & 1 & & -1 \\ & & 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & & & 1 \\ & 1 & & 1 \\ & & 1 & 1 \end{pmatrix}$$

  - Compute syndrome $\boldsymbol{s_i}$ for each $\boldsymbol{v_i}$.

$\mathbf{v}_i$	$\mathbf{s}_i$
0000	000
1000	100
0100	010
0010	001
0001	111
1100	110
1010	101
1001	011

Syndrome Decoding

- The syndrome decoding proceeds as follows
  - Given any received $\boldsymbol{v}$, compute its syndrome $\boldsymbol{s} = \boldsymbol{v}H^T$.
  - Find $\boldsymbol{s}$ in the second column of the syndrome table, say $\boldsymbol{s} = \boldsymbol{s_i}$, the i-th entry.
  - If $\boldsymbol{v_i}$ is the coset leader corresponding to $\boldsymbol{s_i}$ in the table, Then decode v as $u_i = v - v_i$. I.e.

$$\Delta(\mathbf{v}) = \mathbf{u}_j = \mathbf{v} - \mathbf{v}_i\,, \quad \text{where} \quad \mathbf{v}H^{\mathrm{T}} = \mathbf{s}_i$$

- Example 7.44
  - As in Example 7.43. v = 1101 is received. its syndrome $\boldsymbol{s} = \boldsymbol{v}H^T$ = 001. This is s_4 in the syndrome table, so we decode v as $\Delta(\mathbf{v}) = \mathbf{v} - \mathbf{v}_4 = 1101 - 0010 = 1111$