Proseminar. Kodierungstheorie

SoSe 2021

Hongbao Shi

266563

Notes: ① (this filed)

F_q : Galois field $GF(q)$, where q is prime power.

②

$(F_q)^n$: the vector space $V(n,q)$

Def 1 :

A linear code over $GF(q)$ is just a subspace of $V(n,q)$, for some positive integer n.

A subset C of $V(n,q)$ is a linear code if and only if

i) $u+v \in C$, for all u and v in C.

ii) $au \in C$, for $u \in C, a \in GF(q)$.

(special case Binary)

Example 2: ①

The code G_1 of Example 1.5, $G_1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}$, G_1 is a subset of $(F_2)^2$

② in Page 1.5 (✗)

Def 3:

C is a k-dimensional subspace of $V(n,q)$, then the linear code C is called an $[n,k]$- code, if we wish to specify also the minimum distance d of C, an $[n,k,d]$ - code.

The weight $w(x)$ of a vector x in $V(n,q)$ is defined to be the number of non-zero entries of X.

Before we prove a theorem, that a linear code is that its minimum distance is equal to the smallest of the weights of the non-zero code words, we have firstly a Lemma.

Lemma 4

If $x, y \in V(n,q)$ then $d(x,y) = w(x-y)$

(specially for $q=2$, $d(x,y) = w(x+y)$)

proof. vector $x-y$ has non-zero entries, because they are different.

$x - y \neq 0$

(X) Let $G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$, $F = F_2$

Then the span of G is a $(6, 2)$ code

Its codewords are

1 0 1 0 1	$d = 3$
0 1 0 1 0 1	$d = 3$
0 0 0 0 0 0	constant
1 1 1 1 1 1	$d = 6$

So Lets prove the impart Theorem.

Theorem 5: Let C be a linear code and let $w(C)$ be the smallest of the weights of the non-zero codewords of C. Then

$$d(C) = w(C)$$

Remark: $w(C) = d(C, (0, \cdots, 0))$

Proof:

There exit codewords x and y of C such that $d(C) = d(x,y)$

by Lemma 4; $d(C) = w(x-y) \geq w(C)$, because $x-y$ is a codeword of the linear code C.

Besides, for some codeword $x \in C$, $w(C) = w(x) = d(x,0) \geq d(C)$ since 0 belongs to the liner cod C. So $d(C) \geq w(C)$ and also $w(C) \geq d($

$\Rightarrow d(C) = w(C)$.

12.

we now list some of the advantages and disadvantages of restricting one's attention to linear codes.

Advantage:

① For a general code with M codewords, to find the minimum distance we might have to make $\binom{M}{2} = \frac{1}{2}M(M-1)$. However, Theores 5.2 enable the minimum distance of a liner code to be found by examining only the weights of the $M-1$ non-zero codewords.

(Minimal distance $h(C)$ is easy to compute if C is linear code

② To specify a non-linear code, we may hae to list all the codewords. we can specify a linear $[n,k]$-code by simply giving a bsis of k codewords.

(Liner codes have simpe specifications)

③ There are nice procedures for encoding and decoding a linear code. (chap. 7)

②

Def 6

A $k \times n$ matrix whose rows form a basis of a linear $[n,k]$ code is called a generator matrix of the code.

Example 7

(i) The code C_2 of Example 1.5 is a $[3, 2, 2]$-code (with $n=3$, $k=2$, $d=2$) with generator matrix $\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$.

(ii) The code C of Example 2.13 is a $[7,4,3]$-code with generator matrix

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

Equivalence of linear codes

Def 8:

① Equivalence of codes is modified for linear codes, by allowing only those permutations of symbols which are given by multiplication by a non-zero scalar. (chapter 2).

② Two linear codes over GF(q) are called equivalent if one can be obtained from the other by a combination of operation of following types.

(A) permutation of the code

(B) multiplication of the symbols appearing in a fixed position by a non-zero scalar.

Disadvantage:

① Linear q-ary are not defined unless q is a prime power. But for q not a prime power, can often be obtained from linear codes over a large alphabet. such as, in chap. 2 how good decimal (10-ary) codes can be obtained from linear 11-ary codes by omitting all codewords containing a given fixed symbol.

This idea is used in ISBN code.

It can be obtained in such a way from the 11-ary linear 11-ary code $\{x_1 \cdots x_{11} \in V(10,11) : \sum_{i=1}^{11} i x_i = 0\}$.

Theorem 9:

Two $k \times n$ matrices generate equivalent linear $[n,k]$-codes over $GF(q)$ if one matrix can be obtained from the other by a sequence of operations of the following types:

(a) permutation of the rows.
(b) Multiplication of a row by a non-zero scalar.
(c) Addition of a scalar multiple of one row to another.
(d) permutation of the columns.
(e) Multiplication of any column by a non-zero scalar.

Proof: Operation (a) — (c) just replace one basis by another, (d) and (e) convert a generator matrix to one of an equivalent code.

Theorem 10

Let G be a generator matrix of an $[n,k]$-code. They by performing operations of types (a) ~ (e), G can be transformed to the standard form

$$[\, I_k \mid A \,]$$

where I_k is the $k \times k$ identity matrix, and A is a $k \times (n-k)$ matrix

Proof:

During a sequence of transformations of the matrix G, we denote by g_{ij} the (i,j)-th entry of the matrix und consideration at the time and by $r_1, r_2, \cdots r_k$ and $c_1, c_2, \cdots, c_n$ the rows and columns respectively of this matrix.

The following three-step procedure is applied for $j=1, 2, \cdots, k$ in turn, the j^{th} application transforming column c_j into its desired form (with 1 in the j^{th} position and 0s elsewhere), leaving unchanged the first $j-1$ columns already suitably transformed. Suppose then that G has already been transformed to

$$\begin{bmatrix} 1 & 0 & \cdots & 0 & g_{ij} & \cdots & g_{1n} \\ 0 & 1 & \cdots & 0 & g_{2j} & \cdots & g_{2n} \\ \vdots & & \ddots & \vdots & & & \\ 0 & 0 & \cdots & 1 & g_{j-1,j} & \cdots & g_{j-1,n} \\ 0 & 0 & \cdots & 0 & g_{jj} & \cdots & g_{jn} \\ \vdots & & & \vdots & & & \\ 0 & 0 & \cdots & 0 & g_{kj} & \cdots & g_{kn} \end{bmatrix}$$

1. Step:

If $g_{jj} \neq 0$, go to step 2. If $g_{jj} = 0$, and if for some $i > j$, $g_{ij} \neq 0$, then interchange r_j and r_k. If $g_{jj} = 0$ and $g_{ij} = 0$ for all $i > j$, then choose h such that $g_{jh} \neq 0$ and interchange c_j and c_h.

2. Step. We now have $g_{jj} \neq 0$. Multiply r_j by g_{jj}^{-1}.

3. Step. We now have $g_{jj} = 1$. For each of $i = 1, 2, \cdots, k$, with $i \neq j$, replace r_i by $r_i - g_{ij} r_j$.

The colum c_j now has the desired form.

After this procedure has been applied for $j = 1, 2, \cdots, k$, the generator matrix will have standard form.

Example 17

① In Example 17(i). Interchanging rows gives the standart form generator matrix

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

② use the Theorem 7 to transform 7(ii)

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

$r_2 \to r_2 - r_1$

$r_3 \to r_3 - r_1$

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

$r_1 \to r_1 - r_2$

$r_4 \to r_4 - r_2$

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

$r_2 \to r_2 - r_3$

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

$$\xrightarrow{r_3 \to r_3 - r_4} \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$