第3章 线性分组码

第3章 线性分组码

- ◈线性分组码的定义
- ◈线性分组码的编码问题
- ◈线性分组码的译码问题
- ◈检错能力和纠错能力

线性分组码的定义

定义：设C是码长为n的q元码，即$C \subset V_n(F_q)$，如果C是$V_n(F_q)$的子空间，则称C是码长为n的q元线性分组码。

C是$V_n(F_q)$的子空间：

① $v_1+v_2 \in C$ （$\forall\, v_1, v_2 \in C$）

② $cv \in C$ （$\forall\, v \in C$，$\forall c \in F_q$）

即 $c_1v_1+c_2v_2 \in C$ （$\forall\, v_1, v_2 \in C$，$\forall c_1, c_2 \in F_q$）

例：设C为码长为6的一个二元码，

C={101010，101101，011011，001110}是否为线性码？

答：否

线性分组码的定义

定义：设C是码长为n的q元码，即$C \subset V_n(F_q)$，如果C是$V_n(F_q)$的子空间，则称C是码长为n的q元线性分组码。

若C是$V_n(F_q)$的k维子空间（$k \le n$），则

$$C \cong V_k(F_q)$$

即存在一一映射σ：$V_k(F_q)$-->C,使得$V_k(F_q) \cong C$

即，C可看做是原始数字消息集合$V_k(F_q)$在某一编码σ（一一映射）下的象，C又称为码长为n的信息位为k的q元线性分组码。

线性分组码的编码问题

生成矩阵：因为线性分组码C是$V_n(F_q)$的k维子空间，则存在一组基$\{v_0, v_1, \ldots, v_{k-1}\}$，C由这组基向量生成，即$C=<v_0, v_1, \ldots, v_{k-1}>$，

由这组基向量构成的矩阵记为G，称为C的生成矩阵。

$$G=\begin{pmatrix} v_0 \\ v_1 \\ \cdots \\ v_{k-1} \end{pmatrix} = \begin{pmatrix} v_{0,0} & v_{0,1} & \cdots & v_{0,n-1} \\ v_{1,0} & v_{1,0} & \cdots & v_{1,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ v_{k-1,0} & v_{k-1,1} & \cdots & v_{k-1,n-1} \end{pmatrix}$$

线性分组码的编码问题

设二元线性码C的生成矩阵如下，请求出C?

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

解：C是$V_6(F_2)$的3维子空间，$C \cong V_3(F_2)$。

它的一组基为$\{v_0, v_1, v_2\}$：

$v_0=(1\ 0\ 0\ 1\ 1\ 0)$

$v_1=(0\ 1\ 0\ 1\ 0\ 1)$

$v_2=(0\ 0\ 1\ 0\ 1\ 1)$

则C中的全部码字为基向量的线性组合：

$a_0v_0+a_1v_1+a_2v_2=(a_0, a_1, a_2)G$，$a_0, a_1, a_2 \in F_2$

即$\sigma(a_0, a_1, a_2)=a_0v_0+a_1v_1+a_2v_2=(a_0, a_1, a_2)G$

线性分组码的编码问题

设二元线性码C的生成矩阵如下，请求出C?

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

解：即$\sigma(a_0, a_1, a_2)=a_0v_0+a_1v_1+a_2v_2=(a_0, a_1, a_2)G$

C中共8个码字：

σ(000)=000000　　σ(100)=100110
σ(001)=001011　　σ(101)=101101
σ(010)=010101　　σ(110)=110011
σ(011)=011110　　σ(111)=111000

∴ C={000000，001011，010101，011110，100110，101101，110011，111000}

7

线性分组码的编码问题

设二元线性码C的生成矩阵如下，请求出C?

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

$\sigma(a_0a_1a_2)=a_0v_0+a_1v_1+a_2v_2$

消息集合M	线性码C
000	000000
001	001011
010	010101
011	011110
100	100110
101	101101
110	110011
111	111000

8

线性分组码的编码问题

由这组基向量构成的矩阵记为G，称为C的生成矩阵。

$$G=\begin{pmatrix}v_0\\v_1\\\cdots\\v_{k-1}\end{pmatrix}=\begin{pmatrix}&v_{0,0}&v_{0,1}&\cdots&v_{0,n-1}\\&v_{1,0}&v_{1,1}&\cdots&v_{1,n-1}\\\cdots&\cdots&\cdots&\cdots&\cdots\\&v_{k-1,0}&v_{k-1,1}&\cdots&v_{k-1,n-1}\end{pmatrix}$$

为什么称G为C的生成矩阵?

（1）C中任一码字是G中行向量的线性组合，即由G生成；

（2）G中行向量的所有线性组合都是码字，即属于C

9

线性分组码的编码问题

设三元(4,2)线性码C的生成矩阵如下，请求出C?

$$G=\begin{pmatrix}1&0&1&1\\0&1&2&1\end{pmatrix}$$

解：C是$V_4(F_3)$的2维子空间，$C\cong V_2(F_3)$。

它的一组基为$\{v_0, v_1\}$：

$v_0=(1\ 0\ 1\ 1)$

$v_1=(0\ 1\ 2\ 1)$

则C中的全部码字为基向量的线性组合：

$a_0v_0+a_1v_1=(a_0, a_1)G$，$a_0, a_1\in F_3$

即$\sigma(a_0, a_1)=a_0v_0+a_1v_1=(a_0, a_1)G$

10

线性分组码的编码问题

设三元(4,2)线性码C的生成矩阵如下，请求出C?

$$G=\begin{pmatrix}1&0&1&1\\0&1&2&1\end{pmatrix}$$

解：即$\sigma(a_0, a_1)=a_0v_0+a_1v_1=(a_0, a_1)G$

C中共9个码字：

σ(00)= 0000　　σ(10)= 1011　　σ(20)= 2022
σ(01)= 0121　　σ(11)= 1102　　σ(21)= 2110
σ(02)= 0212　　σ(12)= 1220　　σ(22)= 2201

∴ C={0000,0121,0212,1011,1101,1220,2022,2110,2201}

11

线性分组码的编码问题

设三元(4,2)线性码C的生成矩阵如下，请求出C?

$$G=\begin{pmatrix}1&0&1&1\\0&1&2&1\end{pmatrix}$$

$\sigma(a_0a_1)=a_0v_0+a_1v_1$

消息集合M	线性码C
00	0000
01	0121
02	0212
10	1011
11	1101
12	1220
20	2022
21	2110
22	2201

12

线性分组码的编码问题

生成矩阵：因为线性分组码C是$V_n(F_q)$的k维子空间，则存在一组基$\{v_0, v_1, \ldots, v_{k-1}\}$，C由这组基向量生成，即$C=\langle v_0, v_1, \ldots, v_{k-1}\rangle$，

由这组基向量构成的矩阵记为G，称为C的生成矩阵。

$$G=\begin{pmatrix} v_0 \\ v_1 \\ \cdots \\ v_{k-1} \end{pmatrix}=\begin{pmatrix} v_{0,0} & v_{0,1} & \cdots & v_{0,n-1} \\ v_{1,0} & v_{1,0} & \cdots & v_{1,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ v_{k-1,0} & v_{k-1,1} & \cdots & v_{k-1,n-1} \end{pmatrix}$$

问题：生成矩阵是不是唯一的？

13

线性分组码的编码问题

问题：生成矩阵是不是唯一的？

C是$V_n(F_q)$ 的子空间，

G是C的一组基向量构成的矩阵，

问题：向量子空间的基是不是唯一的？

由这组基向量构成的矩阵记为G，称为C的生成矩阵。

$$G=\begin{pmatrix} v_0 \\ v_1 \\ \cdots \\ v_{k-1} \end{pmatrix}=\begin{pmatrix} v_{0,0} & v_{0,1} & \cdots & v_{0,n-1} \\ v_{1,0} & v_{1,0} & \cdots & v_{1,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ v_{k-1,0} & v_{k-1,1} & \cdots & v_{k-1,n-1} \end{pmatrix}$$

14

线性分组码的编码问题

设二元线性码C的生成矩阵如下，请求出C?

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

$\sigma(a_0a_1a_2)=a_0v_0+a_1v_1+a_2v_2$

消息集合M	线性码C
000	000000
001	001011
010	010101
011	011110
100	100110
101	101101
110	110011
111	111000

15

线性分组码的编码问题

设二元线性码C的生成矩阵：

$$G_1=\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$\sigma(m)=mG_1$

消息集合M	线性码C
000	000000
001	001011
010	010101
011	011110
100	100110
101	101101
110	110011
111	111000

设二元线性码C的生成矩阵：

$$G_2=\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$\sigma(m)=mG_2$

消息集合M	线性码C
000	000000
001	001011
010	110011
011	111000
100	100110
101	101101
110	010101
111	011110

16

线性分组码的编码问题

总结：

（1）线性分组码C由生成矩阵唯一确定；

（2）同一线性分组码C的生成矩阵不唯一；

（3）同一线性分组码C的不同的生成矩阵确定的C的集合是唯一的。

（4）但是，具体到某个原始消息，在不同的生成矩阵下对应的码字可能不同。

问题：同一线性码C的生成矩阵之间是什么关系?

	编码器	
	存储器	运算器
一般的码	所有码字	
线性码	生成矩阵	线性组合

17

线性分组码的编码问题

问题：同一线性码C的生成矩阵之间是什么关系?

答：行等价的。即存在可逆矩阵P，使得$G_1=PG_2$。

1. 交换2行

2.某行乘以一个常数；

3. 某一行乘以一个常数加到另一行。

18

线性分组码的编码问题

定理： 设A是域F上的一个m×n矩阵，那么A一定行等价于一个以下形状的阶梯矩阵A_0：

$$\begin{pmatrix} 0\cdots 01 *\cdots * & 0*\cdots* & 0*\cdots* & 0*\cdots* \\ 0\cdots 000\cdots 0 & 1*\cdots* & 0*\cdots* & 0*\cdots* \\ 0\cdots 000\cdots & 000\cdots & 01*\cdots* & 0*\cdots* \\ \cdots & \cdots & \cdots & \cdots \\ 0\cdots 000\cdots & 000\cdots & 000\cdots & 01*\cdots* \\ 0\cdots 000\cdots & 000\cdots & 000\cdots & 000\cdots 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0\cdots 000\cdots & 000\cdots & 000\cdots & 000\cdots 0 \end{pmatrix}$$

设rankA=r，那么，A_0的第r行下面的元素都是0，A_0的前r行中从左往右数第一个非零元素都是1，这r个1分属于r个不同的列；这每一个1的同行左侧的元素都是0，同列的其它元素也都是0，它左下方的元素也都是0. 因此如果A_0的第i行$(1 \le i \le r)$的第一个不等于0的元素1位于第k_i列，那么$1 \le k_1 < k_2 < \cdots < k_r \le n$。

19

线性分组码的编码问题

$$\begin{pmatrix} 0\cdots 01 *\cdots * & 0*\cdots* & 0*\cdots* & 0*\cdots* \\ 0\cdots 000\cdots 0 & 1*\cdots* & 0*\cdots* & 0*\cdots* \\ 0\cdots 000\cdots & 000\cdots & 01*\cdots* & 0*\cdots* \\ \cdots & \cdots & \cdots & \cdots \\ 0\cdots 000\cdots & 000\cdots & 000\cdots & 01*\cdots* \\ 0\cdots 000\cdots & 000\cdots & 000\cdots & 000\cdots 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0\cdots 000\cdots & 000\cdots & 000\cdots & 000\cdots 0 \end{pmatrix}$$

例： 将域F_2上的8×8矩阵A化为与之行等价的阶梯形矩阵A_0，并求出矩阵A的秩rankA。

$$A=\left(\begin{array}{cccc|cccc} 0&1&0&0&1&0&1&1\\ 0&0&1&0&1&0&1&0\\ 0&0&0&0&1&1&1&1\\ 0&0&0&1&1&1&1&1\\ \hline 0&0&1&0&0&1&0&1\\ 0&0&0&0&0&0&1&0\\ 0&0&0&1&0&1&0&0\\ 0&0&0&0&0&0&1&0 \end{array}\right) \quad \left(\begin{array}{cccc|cccc} 0&1&0&0&1&0&1&1\\ 0&0&1&0&1&0&1&0\\ 0&0&0&0&1&1&1&1\\ 0&0&0&1&1&1&1&1\\ \hline 0&0&0&0&1&1&1&1\\ 0&0&0&0&0&0&1&0\\ 0&0&0&1&0&1&0&0\\ 0&0&0&0&0&0&1&0 \end{array}\right) \quad \left(\begin{array}{cccc|cccc} 0&1&0&0&1&0&1&1\\ 0&0&1&0&1&0&1&0\\ 0&0&0&1&1&1&1&1\\ 0&0&0&0&1&1&1&1\\ \hline 0&0&0&0&1&1&1&1\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&1&0&1&1\\ 0&0&0&0&0&0&1&0 \end{array}\right)$$

$$\left(\begin{array}{cccc|cccc} 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&1\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&1\\ \hline 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0 \end{array}\right) \quad \left(\begin{array}{cccc|cccc} 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&1\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&1&1\\ \hline 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&0 \end{array}\right) \quad \left(\begin{array}{cccc|cccc} 0&1&0&0&0&1&0&0\\ 0&0&1&0&0&1&0&1\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&1&1&1\\ \hline 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0 \end{array}\right)$$

20

线性分组码的编码问题

◆ **例：** 将域F_2上的 8×8 矩阵 $A=\begin{pmatrix} 00001011\\ 01001010\\ 01101111\\ 00011111\\ 00100101\\ 00000010\\ 00010100\\ 00000010 \end{pmatrix}$，化为与之行等价的阶梯形矩阵 A_0，并求出矩阵A的秩。

$$\begin{pmatrix} 0\cdots 01 *\cdots * & 0*\cdots* & 0*\cdots* & 0*\cdots* \\ 0\cdots 000\cdots 0 & 1*\cdots* & 0*\cdots* & 0*\cdots* \\ 0\cdots 000\cdots & 000\cdots & 01*\cdots* & 0*\cdots* \\ \cdots & \cdots & \cdots & \cdots \\ 0\cdots 000\cdots & 000\cdots & 000\cdots & 01*\cdots* \\ 0\cdots 000\cdots & 000\cdots & 000\cdots & 000\cdots 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0\cdots 000\cdots & 000\cdots & 000\cdots & 000\cdots 0 \end{pmatrix}$$

21

线性分组码的编码问题

答案：$\begin{pmatrix} 01000001\\ 00100101\\ 00010100\\ 00001001\\ 00000010\\ 00000000\\ 00000000\\ 00000000 \end{pmatrix}$

rankA=5

22

线性分组码的编码问题

例： 将域F_5上的 4×4 矩阵 $A=\begin{pmatrix} 1431\\ 0241\\ 0314\\ 4201 \end{pmatrix}$，化为与之行等价的阶梯形矩阵 A_0，并求出矩阵A的秩。

$$\begin{pmatrix} 0\cdots 01 *\cdots * & 0*\cdots* & 0*\cdots* & 0*\cdots* \\ 0\cdots 000\cdots 0 & 1*\cdots* & 0*\cdots* & 0*\cdots* \\ 0\cdots 000\cdots & 000\cdots & 01*\cdots* & 0*\cdots* \\ \cdots & \cdots & \cdots & \cdots \\ 0\cdots 000\cdots & 000\cdots & 000\cdots & 01*\cdots* \\ 0\cdots 000\cdots & 000\cdots & 000\cdots & 000\cdots 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0\cdots 000\cdots & 000\cdots & 000\cdots & 000\cdots 0 \end{pmatrix}$$

23

线性分组码的编码问题

$$A=\begin{pmatrix} 1&4&3&1\\ 0&2&4&1\\ 0&3&1&4\\ 4&2&0&1 \end{pmatrix} \text{--->} \begin{pmatrix} 1&4&3&1\\ 0&2&4&1\\ 0&3&1&4\\ 0&1&3&2 \end{pmatrix} \text{--->} \begin{pmatrix} 1&4&3&1\\ 0&1&2&3\\ 0&3&1&4\\ 0&1&3&2 \end{pmatrix}$$

$$\begin{pmatrix} 1&0&0&4\\ 0&1&2&3\\ 0&0&0&0\\ 0&0&1&4 \end{pmatrix} \text{--->} \begin{pmatrix} 1&0&0&4\\ 0&1&2&3\\ 0&0&1&4\\ 0&0&0&0 \end{pmatrix} \text{--->} \begin{pmatrix} 1&0&0&4\\ 0&1&0&0\\ 0&0&1&4\\ 0&0&0&0 \end{pmatrix}$$

24

线性分组码的编码问题

✓ 答案：

$$\begin{pmatrix}1&4&3&1\\0&2&4&1\\0&3&1&4\\4&2&0&1\end{pmatrix}\rightarrow\begin{pmatrix}1&4&3&1\\0&2&4&1\\0&3&1&4\\0&1&3&2\end{pmatrix}\rightarrow\begin{pmatrix}1&4&3&1\\0&1&2&3\\0&0&0&0\\0&1&3&2\end{pmatrix}\rightarrow\begin{pmatrix}1&4&3&1\\0&1&2&3\\0&0&0&0\\0&0&1&4\end{pmatrix}$$

$$\rightarrow\begin{pmatrix}1&0&0&4\\0&1&2&3\\0&0&1&4\\0&0&0&0\end{pmatrix}\rightarrow\begin{pmatrix}1&0&0&4\\0&1&0&0\\0&0&1&4\\0&0&0&0\end{pmatrix}$$

矩阵A的秩为3。

25

线性分组码的编码问题

✓ 课堂练习：将域F_5上的 4 × 4 矩阵 $A=\begin{pmatrix}1&3&2&1\\4&2&3&4\\0&1&1&0\\0&1&2&3\end{pmatrix}$，化为与之行等价的阶梯形矩阵 A_0，并求出矩阵A的秩。

$$\begin{pmatrix}0\ \cdots\ 0\,1\ *\cdots*\ 0*\cdots*0*\cdots*0\ *\cdots*\\0\ \cdots\ 0\,0\,0\ \cdots 0\ 1*\cdots*0*\cdots*0\ *\cdots*\\0\ \cdots\ 0\,0\,0\cdots\ 0\ 0\,0\cdots 0\,1*\cdots*0\ *\cdots*\\\cdots\qquad\qquad\cdots\qquad\qquad\cdots\qquad\qquad\cdots\\0\ \cdots\ 0\,0\,0\cdots\ 0\ 0\,0\cdots 0\,0\,0\cdots 0\,1\ *\cdots*\\0\ \cdots\ 0\,0\,0\cdots\ 0\,0\ 0\cdots 0\,0\,0\cdots 0\,0\,0\cdots\ 0\\\cdots\qquad\qquad\cdots\qquad\qquad\cdots\qquad\qquad\cdots\\0\ \cdots\ 0\,0\,0\cdots 0\,0\,0\cdots 0\,0\,0\cdots 0\,0\,0\ \cdots 0\end{pmatrix}$$

26

线性分组码的编码问题

✓ 答案：

$$A=\begin{pmatrix}1&3&2&1\\4&2&3&4\\0&1&1&0\\0&1&2&3\end{pmatrix}\rightarrow\begin{pmatrix}1&3&2&1\\0&0&0&0\\0&1&1&0\\0&1&2&3\end{pmatrix}\rightarrow\begin{pmatrix}1&3&2&1\\0&1&1&0\\0&1&2&3\\0&0&0&0\end{pmatrix}\rightarrow\begin{pmatrix}1&0&4&1\\0&1&1&0\\0&0&1&3\\0&0&0&0\end{pmatrix}\rightarrow$$

$$\begin{pmatrix}1&0&0&4\\0&1&0&2\\0&0&1&3\\0&0&0&0\end{pmatrix}$$

rankA=3

27

系统码与等价的码

定义：设C和C'均为码长为n的q元码，
$\{i_1,\ i_2,\ \cdots,\ i_n\}$为$\{1,2,\cdots,n\}$的一个排列，
若$(c_1,c_2,\cdots,c_n)\in C$当且仅当$(c_{i_1},c_{i_2},\cdots,c_{i_n})\in C'$
称C和C'为等价的码。

定义：设C为一线性分组码，且C有一个生成矩阵形

如$G_0=\begin{pmatrix}1\,0&\cdots 0&*\cdots*\\0\,1&\cdots 0&*\cdots*\\&\cdots&\\0\,0&\cdots 1&*\cdots*\end{pmatrix}=(I_k,A_{k,n-k})$

则称C为系统码。

28

系统码与等价的码

设二元线性码C的生成矩阵如下，

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

线性码C

1	2	3	4	5	6
0	0	0	0	0	0
0	0	1	0	1	1
0	1	0	1	0	1
0	1	1	1	1	0
1	0	0	1	1	0
1	0	1	1	0	1
1	1	0	0	1	1
1	1	1	0	0	0

线性码C‘

4	2	3	1	5	6
0	0	0	0	0	0
0	0	1	0	1	1
1	1	0	0	0	1
1	1	1	0	1	0
1	0	0	1	1	0
1	0	1	1	0	1
0	1	0	1	1	1
0	1	1	1	0	0

29

线性分组码的编码问题

	编码器	
	存储器	运算器
一般的码	所有码字	
线性码	生成矩阵	线性组合
系统码	系统阵中的 $A_{k,n-k}$	

30

线性分组码的编码问题

例：二元（6,3）线性码C，其生成矩阵如下，求出与C等价的系统码。

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

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

则：由G_0生成的线性分组码为与C等价的系统码。

$$-->\begin{pmatrix}1&0&0&1&0&1\\0&0&1&1&0&1\\0&0&0&0&1&1\end{pmatrix}\xrightarrow{\text{列置换}}G_0=\begin{pmatrix}1&0&0&0&1&1\\0&1&0&0&1&1\\0&0&1&0&0&1\end{pmatrix}$$

31