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

线性分组码的编码问题（回顾）

定义：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。

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

线性分组码的编码问题（回顾）

编码：$\sigma(a_0a_1\ldots a_{k-1}) = (a_0a_1\ldots a_{k-1})G$

$$=(a_0a_1\ldots a_{k-1})\begin{pmatrix} v_0 \\ v_1 \\ \cdots \\ v_{k-1} \end{pmatrix}=a_0v_0+a_1v_1+\ldots+a_{k-1}v_{k-1}$$

编码：$\sigma(m)=mG$

C=MG

消息集合M

00…0
00…1
…
…
…
…
11…1

$$\xrightarrow{\sigma(a_0a_1\ldots a_{k-1})=a_0v_0+a_1v_1+\ldots+a_{k-1}v_{k-1}}$$

线性码C

σ(00…0)
σ(00…1)
…
…
…
…
σ(11…1)

线性分组码的译码问题（回顾）

问题：如何判断一个字是否为码字？

定义：设W是$V_n(F_q)$的一个子空间，令

$W^*=\{v|v\in V_n(F_q)$，而$v\cdot w'=0$，对一切$w\in W\}$，则W^*也是$V_n(F_q)$的一个子空间，称为W的对偶子空间。

定义：设C是(n,k)线性分组码，C^*是C的对偶子空间，C^*的生成矩阵称为C的一致校验矩阵。

$$H=\begin{pmatrix} h_0 \\ h_1 \\ \cdots \\ h_{n-k-1} \end{pmatrix}=\begin{pmatrix} h_{0,0} & h_{0,1} & \cdots & h_{0,n-1} \\ h_{1,0} & h_{1,0} & \cdots & h_{1,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ h_{n-k-1,0} & h_{n-k-1,1} & \cdots & h_{n-k-1,n-1} \end{pmatrix}$$

线性分组码的译码问题（回顾）

问题：如何求出一致校验矩阵H？（由生成矩阵G）

答：由生成矩阵G求一致校验矩阵H，即求$Gx'=0$的解空间的一组基。

定理：$Ax'=0$和$(PA)x'=0$的解空间一致(其中P为一个可逆矩阵)。

因为$PA=A_0$，所以$Ax'=0$的解空间和$Ax'=0$的解空间一致。

线性分组码的译码问题（回顾）

例：求域F_2上的齐次线性方程组$Gx'=0$的解空间的秩和解空间的一组基。

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

例：求以G为生成矩阵的二元(6,3)线性分组码C的一致校验矩阵H。

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

7

线性分组码的译码问题（回顾）

例：求域F_2上的齐次线性方程组$Gx'=0$的解空间的秩和解空间的一组基。

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

解：将G通过行初等变换化为阶梯型矩阵G_0，

$Gx'=0$的解空间<==>$G_0x'=0$的解空间

$$G=\begin{pmatrix}1&0&1&0&0&1\\1&1&0&1&1&0\\0&1&0&1&1&0\end{pmatrix}\qquad G_0=\begin{pmatrix}1&0&0&1&0&1\\0&0&1&1&0&1\\0&0&0&0&1&1\end{pmatrix}$$

8

线性分组码的译码问题（回顾）

一致校验矩阵的求法：

定理：设(n,k)系统码C的生成矩阵为G_0，

$$G_0=\begin{pmatrix}1&0&\cdots&0&a_{11}&\cdots&a_{1,n-k}\\0&1&\cdots&0&a_{21}&\cdots&a_{2,n-k}\\\cdots&&\cdots&&&\cdots&\\0&0&\cdots&1&a_{k,1}&\cdots&a_{k,n-k}\end{pmatrix}=(I_k,A_{k,n-k})$$

则C的一致校验矩阵H：

$$H=\begin{pmatrix}-a_{11}&\cdots&-a_{k,1}&1&0&\cdots&0\\-a_{12}&\cdots&-a_{k,2}&0&1&\cdots&0\\&\cdots&&&&\cdots&\\-a_{1,n-k}&\cdots&-a_{k,n-k}&0&0&\cdots&1\end{pmatrix}=(-A'_{k,n-k},I_{n-k})$$

9

线性分组码的译码问题（回顾）

定义：设C是(n,k)线性分组码，H是C的一致校验矩阵，则$\forall x\in V_n(F_q)$，称Hx'为x的校验子。

译码表：

校验子 Hx'	陪集首				
$H0'$	$\mathbf{0}$	c_1	c_2	$\cdots$	c_{q^k-1}
He_1'	e_1	e_1+c_1	e_1+c_2	$\cdots$	$e_1+c_{q^k-1}$
He_2'	e_2	e_2+c_1	e_2+c_2	$\cdots$	$e_2+c_{q^k-1}$
…	…	…	…	…	…
$He_{q^{n-k}-1}'$	$e_{q^{n-k}-1}$	$e_{q^{n-k}-1}+c_1$	$e_{q^{n-k}-1}+c_2$	$\cdots$	$e_{q^{n-k}-1}+c_{q^k-1}$

10

线性分组码的译码问题---译码表

陪集首与校验子的求法：

① 选取重量为1的向量作为陪集首，计算其校验子；

② 若重量为1的向量不够（不够校验子的个数，即q^{n-k}），则选取重量为2的向量计算其校验子，直到获得q^{n-k}个校验子为止。

译码方法：

发a，收r。

① 计算r的校验子Hr'；

② 找到Hr'对应的陪集首e；

③ 将r译为$r-e$.

11

检错、纠错能力

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

12

线性分组码的检错能力和纠错能力

定理1：设C为码长为n的一个码，
(1) 若任意两个码字的距离$\geq t+1$，则C是可检出t个差错的检错码；
(2) 若确有两个码字的距离$= t+1$，则C不能检出$t+1$个差错；
(3) 若任意两个码字的距离$\geq 2t+1$，则C是可纠正t个差错的纠错码；
(4) 若确有两个码字的距离$= 2t+1$，则C不能纠正$t+1$个差错。

定理：设C是q元(n,k)线性码，那么C的极小重量等于C的极小距离。

定理：设C是q元(n,k)线性码，H是它的一个一致校验矩阵，如果H的任意t列都线性无关，而有t+1列线性相关，那么C的极小重量等于t+1，这时C是可检t错的检错码，是可纠$\lfloor t/2 \rfloor$错的纠错码。

13

线性分组码的检错能力和纠错能力

例：二元（6，3）线性码C，其生成矩阵和校验矩阵分别为

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

Min（C）=3，检2错，纠1错。

14

线性分组码的检错能力和纠错能力

推论：设C是一个二元线性码，H是它的一个一致校验矩阵，那么，

C是可以纠正1个错误的纠错码

$$\Leftrightarrow \begin{cases} H\text{无全}0\text{列向量} \\ H\text{中任意两列不相等} \end{cases}$$

15

例：二元(7, 4)线性分组码

例子：设信息空间为$V_4(F_2)$，构造一个信息率为4/7的二元（7，4）线性码。

① 编码
- a) 生成矩阵
- b) 编码
- c) 编译器存储

② 译码
- a) 校验矩阵
- b) 伴随式译码方法
- c) 译码
- d) 检错、纠错能力

16

例：二元(7, 4)线性分组码

一、编码：

1. 首先确定一个秩为4的4×7矩阵，作为该(7,4)线性码C的生成矩阵G：

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

2. 编码：

$\sigma(m)=mG$

C=MG

消息	码字	消息	码字
0000	0000000	1000	1000111
0001	0001001	1001	1001110
0010	0010010	1010	1010101
0011	0011011	1011	
0100	0100101	1100	
0101	0101100	1101	
0110	0110111	1110	
0111	0111111	1111	

例：二元(7, 4)线性分组码

一、编码：

3. 编译器：

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

存储生成矩阵$G=(I_4A_{4\times3})$，或仅存储$A_{4\times3}$

运算器：计算mG。

18

例：二元(7, 4)线性分组码

二、译码：

1. 求出一致校验矩阵H：

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

rank(H)=3

例：二元(7, 4)线性分组码

二、译码：

2. 伴随式译码方法：

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

确定校验子和陪集首：

校验子	陪集首
(0 0 0)'	0 0 0 0 0 0 0
(1 0 0)'	0 0 0 0 1 0 0
(1 0 1)'	0 1 0 0 0 0 0
(1 1 1)'	1 0 0 0 0 0 0
(0 0 1)'	0 0 0 0 0 0 1
(0 1 0)'	0 0 0 0 0 1 0
(0 1 1)'	0 0 0 0 0 1 1
(1 1 0)'	0 0 0 0 1 1 0

例：二元(7, 4)线性分组码

二、译码：

3. 译码：

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

校验子	陪集首
(0 0 0)'	0 0 0 0 0 0 0
(1 0 0)'	0 0 0 0 1 0 0
(1 0 1)'	0 1 0 0 0 0 0
(1 1 1)'	1 0 0 0 0 0 0
(0 0 1)'	0 0 0 0 0 0 1
(0 1 0)'	0 0 0 0 0 1 0
(0 1 1)'	0 0 0 0 0 1 1
(1 1 0)'	0 0 0 0 1 1 0

对下列收到的字进行译码，并判断是否为确定性译码：

r_1=1111001，r_2=1110011, r_3=0001110

Hr'_1=(000)'，译为r_1, 确定译码

Hr'_2=(011)'，译为r_2-e_6=0110000, 不确定译码

Hr'_3=(111)'，译为r_3-e_3=1001110 确定译码

例：二元(7, 4)线性分组码

二、译码：

4. 检错、纠错能力：

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

H任意1列线性无关（t=1），

有2列线性相关，

所以C的极小重量等于2，可以

检1错，

纠0错。

例：三元(5, 3)线性分组码

课堂练习：设信息空间为$V_3(F_3)$，构造一个信息率为3/5的二元（5，3）线性码。

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

① 编码
- a) 生成矩阵
- b) 编码
- c) 编译器存储

② 译码
- a) 校验矩阵
- b) 伴随式译码方法
- c) 译码
- d) 检错、纠错能力

例：三元(5, 3)线性分组码

一、编码：

1. 首先确定一个秩为3的三元的3×5矩阵，作为该(5,3)线性码C的生成矩阵G：

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

2. 编码：

$\sigma(m)=mG$

C=MG

消息	码字	消息	码字	消息	码字
000		100		200	
001		101		201	
002		102		202	
010		110		210	
011		111		211	
012		112		212	
020		120		220	
021		121		221	
022		122		222	

例：三元(5, 3)线性分组码

一、编码：

3. 编译器：

存储生成矩阵$G=(I_3A_{3\times 2})$，或仅存储$A_{3\times 2}$

运算器：计算mG。

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

25

例：三元(5, 3)线性分组码

二、译码：

1. 求出一致校验矩阵H：

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

rank(H)=2

26

例：三元(5, 3)线性分组码

二、译码：

2. 伴随式译码方法：

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

确定校验子和陪集首：

校验子	陪集首
(0 0)'	0 0 0 0 0
(0 1)'	0 0 0 0 1
(0 2)'	0 0 0 0 2
(1 0)'	0 0 1 0 0
(1 1)'	0 0 0 1 1
(1 2)'	2 0 0 0 0
(2 0)'	0 0 2 0 0
(2 1)'	1 0 0 0 0
(2 2)'	0 0 0 2 2

27

例：三元(5, 3)线性分

校验子	陪集首
(0 0)'	0 0 0 0 0
(0 1)'	0 0 0 0 1
(0 2)'	0 0 0 0 2
(1 0)'	0 0 1 0 0
(1 1)'	0 0 0 1 1
(1 2)'	0 0 0 0 2
(2 0)'	0 0 2 0 0
(2 1)'	1 0 0 0 0
(2 2)'	0 0 0 2 2

二、译码：

3. 译码：

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

对下列收到的字进行译码，并判断是否为确定性译码：

$r_1=11021$，$r_2=00111$, $r_3=11110$

$Hr'_1=(11)'$，译为$r_1-e_4=11010$，不确定译码

$Hr'_2=(01)'$，译为$r_2-e_1=00110$，不确定译码

$Hr'_3=(10)'$，译为$r_3-e_3=11010$，不确定译码

28

例：三元(5, 3)线性分组码

二、译码：

4. 检错、纠错能力：

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

H任意1列线性无关（t=1），

有2列线性相关，

所以C的极小重量等于2，可以

检1错，

纠0错。

29