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：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。

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$C=<v_0, v_1, \ldots, v_{k-1}>$，由这组基向量构成的矩阵记为G，称为C的生成矩阵。

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

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		线性码C
00…0		σ(00…0)
00…1		σ(00…1)
…	$\xrightarrow{\sigma(a_0a_1\ldots a_{k-1})=a_0v_0+a_1v_1+\ldots+a_{k-1}v_{k-1}}$	…
…		…
…		…
…		…
11…1		σ(11…1)

线性分组码的译码问题——一致校验矩阵

线性分组码C是$V_n(F_q)$的子空间。$C\subset V_n(F_q)$，

$V_n(F_q)$ → C （$\cong V_k(F_q)$，q^k个n维向量，码字）

$V_n(F_q)$ → $V_n(F_q)-C$ （q^n-q^k个n维向量，非码字）

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。

注：对偶子空间是相互的。

线性分组码的译码问题——一致校验矩阵

线性分组码C
是$V_n(F_q)$的k维子空间，
存在一组基$\{v_0, v_1, \ldots, v_{k-1}\}$，
$C=<v_0, v_1, \ldots, v_{k-1}>$，
由这组基向量构成的矩阵记为G，
是C的生成矩阵。

C的对偶子空间C*
是$V_n(F_q)$的$n-k$维子空间，
存在一组基$\{h_0, h_1, \ldots, h_{n-k-1}\}$，
$C^*=<h_0, h_1, \ldots, h_{n-k-1}>$，
由这组基向量构成的矩阵记为H，
是C*的生成矩阵。

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

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

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。

线性分组码的译码问题——一致校验矩阵

定理：设H是(n,k)线性分组码C的一致校验矩阵，则$\forall x \in V_n(F_q)$，

$$x \in C \Leftrightarrow Hx'=0$$

$$G=\begin{pmatrix} v_0 \\ v_1 \\ \cdots \\ v_{k-1} \end{pmatrix}=\begin{pmatrix} v_{0,0} & v_{0,1} & \cdots & v_{0,n-1} \\ v_{1,0} & v_{1,0} & \cdots & v_{1,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ v_{k-1,0} & v_{k-1,1} & \cdots & v_{k-1,n-1} \end{pmatrix} \quad H=\begin{pmatrix} h_0 \\ h_1 \\ \cdots \\ h_{n-k-1} \end{pmatrix}=\begin{pmatrix} h_{0,0} & h_{0,1} & \cdots & h_{0,n-1} \\ h_{1,0} & h_{1,0} & \cdots & h_{1,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ h_{n-k-1,0} & h_{n-k-1,1} & \cdots & h_{n-k-1,n-1} \end{pmatrix}$$

证明：由对偶子空间的定义，$\forall v \in C$，$\forall w \in C^*$，有

$$v \cdot w'=0，\ w \cdot v'=0$$

(=>)$x \in C \Rightarrow \forall w \in C^*$，有$w \cdot x'=0$，$\Rightarrow h_i \in C^*$，所以，$h_i \cdot x'=0$。

(<=)$Hx'=0 \Rightarrow h_i \cdot x'=0 \Rightarrow \forall w \in C^*$，$w=w_0h_0+w_1h_1+\ldots+w_{n-k-1}h_{n-k-1}$，$w \cdot x'=0 \Rightarrow x \in C$

7

线性分组码的译码问题——一致校验矩阵

问题：如何求出一致校验矩阵H？（由生成矩阵G）

定理：$Ax'=0$的解向量的全体构成的一个子空间（称为解空间），若rankA=r, 则rank($Ax'=0$的解空间)=n-r。

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。

8

线性分组码的译码问题——一致校验矩阵

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。

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

9

线性分组码的译码问题——一致校验矩阵

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。

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

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

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

10

线性分组码的译码问题——一致校验矩阵

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:

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

11

线性分组码的译码问题——一致校验矩阵

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。

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

解：C的一致校验矩阵H:

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

12

线性分组码的译码问题——一致校验矩阵

课堂练习：求以G为生成矩阵的三元(4,2)线性分组码C的一致校验矩阵H。

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

解：C的一致校验矩阵H：

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

13

线性分组码的译码问题——校验子

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。

若收到的字为r，计算Hr'，

$Hr'=0 \Rightarrow r\in C$

$Hr'\neq 0 \Rightarrow r\notin C$

若发x，差错模式为e，收到的字为 $r=x+e$

译为r-e，则e有什么特点？

（1）$Hr'=H(x+e)'=Hx'+He'=He'$(即e与r有相同的校验子)

（2）e的Hamming重量较小。

所以，在与r有相同校验子的字中找到Hamming重量最小的。

14

线性分组码的译码问题——校验子

子群：若群G的非空子集G'对于群G中所定义的代数运算也构成群，则称G'为G的子群。

$V_n(F_q)$关于向量的加法构成交换群。

线性分组码C是$<V_n(F_q), +>$的子群。$C=\{c_1,c_2,\ldots,c_{q^k}\}$

设G'为交换群G的非空子群，取 $h\in G$，则称$h * G'$为G'的陪集，元素h 称作陪集首。

取任取 $a\in V_n(F_q)$，$a+C=\{a+c_1,a+c_2,\ldots,a+c_{q^k}\}$是C的一个陪集。

C本身是一个陪集；

取$a_1\in V_n(F_q)-C$，a_1+C是C的一个陪集；

取$a_2\in V_n(F_q)-C-(a_1+C)$, a_2+C是C的一个陪集；

…

取$a_{q^{(n-k)}-1}\in V_n(F_q)-C-(a_1+C)-\ldots-(a_{q^{(n-k)}-2}+C)$,

$a_{q^{(n-k)}-1}+C$是C的一个陪集；

$|C|=q^k$, $|V_n(F_q)|=q^n$, 所以，共有q^{n-k}个陪集。

15

线性分组码的译码问题——译码表

译码表：

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

16

线性分组码的译码问题——校验子

定理：$\forall x, y\in V_n(F_q)$,

$x, y\in C$的同一个陪集$\Leftrightarrow Hx'=Hy'$

定理的证明：$x, y\in C$的同一个陪集$a+C$(设$x=a+c_1$, $y=a+c_2$)$\Leftrightarrow H(x-y)'=Hx'-Hy'=H(c_1-c_2)'=0 \Leftrightarrow Hx'=Hy'$

e为Hr'对应陪集的陪集首。

译码方法：收到r，计算Hr'

若$Hr'=0$，译为r；

若$Hr'\neq 0$，找到Hr'为标记的陪集，陪集首为e，将r译为 $r-e$

17

线性分组码的译码问题——译码表

① 将C排在首行，0向量排在首位；

② 下面每一个陪集排成一行（共q^{n-k}行）

a) 以校验子作为该行的标记

b) 重量最小的向量排在该行的首位，即0向量的下面（称为陪集首e）

c) c+e排在码字c的下方。

18

线性分组码的译码问题---译码表

译码表：

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

19

线性分组码的译码问题---译码表

注意：

（1）若陪集首不唯一，则任选其一，此时非确定译码，虚线下；

20

线性分组码的译码问题---译码表

注意：

（2）这样的译码表是否符合极大似然译码法则？

Hamming(r,c)<Hamming(r,a)？（∀a∈C，a≠c）

Ham(r,c)=Ham(r−c,0)=Ham(e)

Ham(r,a)=Ham(r−a,0)=Ham(c+e−a)

e与e+c−a在同一个陪集中，e是陪集首，所以

Hamming(r,c)<Hamming(r,a)

（3）这样的译码表何时正确译码？

21

线性分组码的译码问题---译码表

注意：

（3）这样的译码表何时正确译码？

若发c，差错模式为d，收到的字为 r

计算Hr'

找到Hr'为标记的陪集，陪集首为e，将r译为 r-e。

当d=e时，正确译码。

即差错模式正好是r所在陪集的陪集首时。

22

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。

23

线性分组码的译码问题---译码表

这样的译码表的存储量：

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

只需要存储校验子列和陪集首列。

24

线性分组码的译码问题——伴随式译码方法

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$r-e$.

25

线性分组码的译码问题

例：二元(6,3)线性码C，其生成矩阵为：

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

（1）求出C；

（2）求出其一致校验矩阵；

（3）求出其校验子和所对应的陪集首；

（4）对下列收到的字进行译码，并判断是否为确定性译码：

r_1=010101，r_2=100111, r_3=000111

26

线性分组码的译码问题

例：二元(6,3)线性码C，其生成矩阵为：

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

（1）求出C；

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

27

线性分组码的译码问题

例：二元(6,3)线性码C，其生成矩阵为：

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

（2）求出其一致校验矩阵；

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

28

线性分组码的译码问题

例：二元(6,3)线性码C，其生成矩阵为：

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

（3）求出其校验子和所对应的陪集首；

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

29

线性分组码的译码问题

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

生成矩阵为：

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

（4）对下列收到的字进行译码，并判断是否为确定性译码：

r_1=010101，r_2=100111, r_3=000111

Hr'_1=(000)'，译为r_1， 确定译码

Hr'_2=(001)'，译为r_2-e_1=100110， 确定译码

Hr'_3=(111)'，译为r_3-e_7=010101， 不确定译码

30