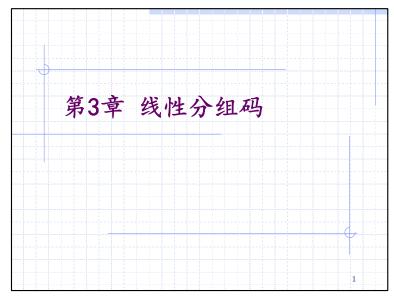
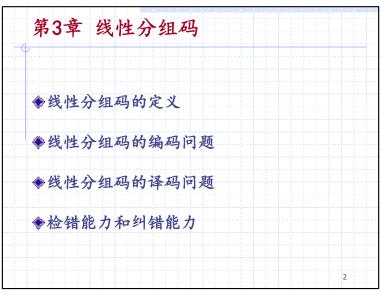
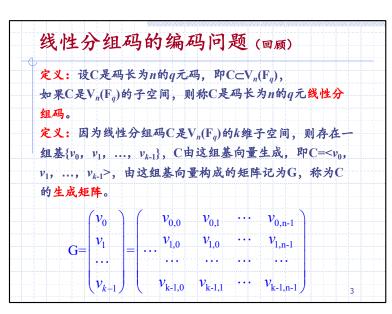
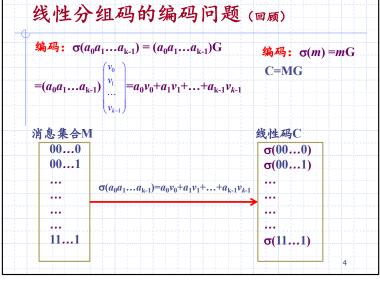
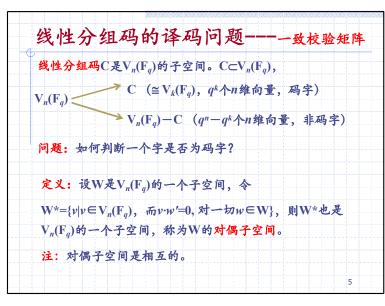
zheng

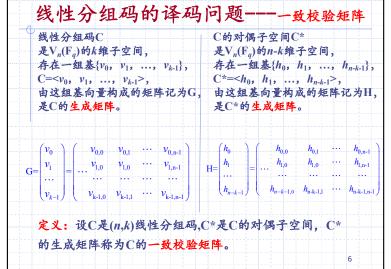












线性分组码的译码问题----致校验矩阵

 $egin{align*} egin{align*} egin{align*}$

证明: 由对偶子空间的定义, ∀v∈C, ∀w∈C*, 有 v·w′=0, w·v′=0

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

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

 $w: x'=0 \Rightarrow x \in C$

线性分组码的译码问题----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----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。

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

线性分组码的译码问题----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G₀,

Gx'=0的解空间<==>G₀x'=0的解空间

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} \qquad \qquad \mathbf{G}_0 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

线性分组码的译码问题----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 ,

$$\mathbf{G}_{0} = \begin{pmatrix} 1 & 0 & \cdots & 0 & a_{11} & \cdots & a_{1,n-k} \\ 0 & 1 & \cdots & 0 & a_{21} & \cdots & a_{2,n-k} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & a_{k,1} & \cdots & a_{k,n-k} \end{pmatrix} = (\mathbf{I}_{k}, \mathbf{A}_{k,n-k})$$

则C的一致校验矩阵H:

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

线性分组码的译码问题----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。

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

解: C的一致校验矩阵H:

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

线性分组码的译码问题----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:

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

13

15

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 $\forall x \in V_n(F_a)$, $\text{$hat} \text{$hat} \text{$

若收到的字为r、计算Hr'、

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

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

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。

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_n)关于向量的加法构成交换群。

线性分组码 \mathbb{C} 是< $\mathbb{V}_n(\mathbb{F}_q)$,+>的子群。 \mathbb{C} = $\{c_1,c_2,...,c_{qk}\}$

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 $a \in V_n(F_a)$, $a+C=\{a+c_1,a+c_2,...,a+c_{ak}\}$ 是C的一个陪集。

C本身是一个陪集:

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

取 $a_{\mathbf{q}^{\wedge}(\mathbf{n}\cdot\mathbf{k})-1}\in V_n(\mathbf{F}_q)-\mathbf{C}-(a_1+\mathbf{C})-\ldots-(a_{\mathbf{q}^{\wedge}(\mathbf{n}\cdot\mathbf{k})-2}+\mathbf{C}),$ $a_{\mathbf{q}^{\wedge}(\mathbf{n}\cdot\mathbf{k})-1}+\mathbf{C}$ 是C的一个陪集;

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

		4	支	性	. 3	分	女	E.	矼	51	约	1	圣.	矼	51	日	是	页	-	 -i	圣延	5.7	ŧ
1	n)																						

校验子 <i>Hx</i> ′	陪集首				
<i>H</i> 0′	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	$e_2 + c_1$	$e_2 + c_2$	 $e_2 + c_{q^k - 1}$	
•••				 	
$He_{q^{n-k}-1}$	$e_{q^{n-k}-1}$	$\begin{array}{c} e_{q^{n-k}-1} \\ +c_1 \end{array}$	$\begin{array}{c} e_{q^{n-k}-1} \\ +c_2 \end{array}$	 $\begin{array}{c} e_{q^{n-k}-1} \\ +c_{q^k-1} \end{array}$	
				16	

线性分组码的译码问题---校验子

定理: $\forall x, y \in V_n(F_a)$,

x, v∈C的同一个陪集<=>Hx'= Hv'

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

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'≠0, 找到Hr'为标记的陪集, 陪集首为e, 将r译为 r-e

线性分组码的译码问题---译码表

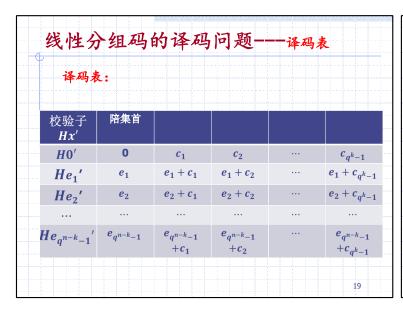
① 将C排在首行, 0向量排在首位;

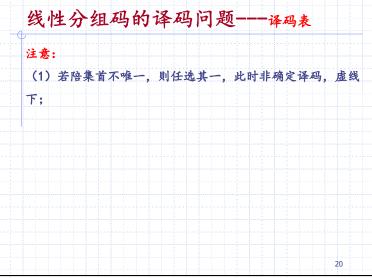
② 下面每一个陪集排成一行(共qn-k行)

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。





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?

