第24卷第2期 数学研究与评论 Vol. 24 No. 2
2004年5月 JOURNAL OF MATHEMATICAL RESEARCH AND EXPOSITION May 2004

中国剩余码*

张爱丽[1], 刘秀峰[2]
(1. 复旦大学计算机科学系, 上海 200433; 2. 西南交通大学应用数学系, 四川 成都 610031)

摘 要: 本文利用弱区组设计和环论中的"中国剩余定理"构造了中国剩余码. 这种新型线性码是将同余类环 $R/I_1\cap I_2\cap\cdots\cap I_n$ 中的同余类作为信息位, 将 R/J_i 嵌入 $R/I_1\cap I_2\cap\cdots\cap I_n$, 视其为 $R/I_1\cap I_2\cap\cdots\cap I_n$ 的子环, R/J_i 在 $R/I_1\cap I_2\cap\cdots\cap I_n$ 中的陪集作为监督维线. 中国剩余码中存在一系列码率较高的码类, 它是孙子码的本质推广.

关键词: 线性码; 同余类; 陪集; 环.
分类号: AMS(2000) 13H/CLC number: O153
文献标识码: A **文章编号**: 1000-341X(2004)02-0347-06

建立在有限域基础上的经典代数编码方法已日臻完善, 而以组合设计为基础的编码理论是现代编码理论的一个重要分支, 组合编码以其超限译码能力, 功能的多样性, 使用的灵活性及编译码器的简单化, 模块化的结构正受到国内外编码界的关注与重视. 组合设计为组合编码奠定了理论基础, 探索新型的组合设计是组合编码的核心研究问题之一, 组合设计的一些新的特性不仅揭示了组合设计与线性码的内在规律, 同时也为构造新型的线性码指出了一条路径. 文献[1]和[2]提出了"孙子码", 它是受我国古代的"孙子定理"的启发, 利用整数环上的理想和同余类而得到的一种新型线性码. 本文就是将这种编码方法推广到一般的带1的交换环, 并利用1998年由本文作者提出的弱区组设计的概念给出了一种新型的编码方法. 为此我们先介绍弱区组设计的概念.

定义1(弱区组设计) 设 b,v,r,k,λ 均为正整数, $X=\{x_1,x_2,\cdots,x_v\}$, 其中 $x_1,x_2,\cdots,x_v$ 是两两互异的元素. $B_1,B_2,\cdots,B_b$ 为 X 的 b 个子集(其中允许出现重复的子集), $\mathscr{B}=\{B_1,B_2,\cdots,B_b\}$, 以下将称 B_j 为区组, $j=1,2,\cdots,b$, 即使 B_i 与 B_j 为重复的子集, 但 $i\neq j$, 我们仍然将 B_i 与 B_j 视为不同的区组. 如果 $(X,\mathscr{B})$ 满足下列条件:

(1) 对于任意的 $j\in\{1,2,\cdots,b\}$, 恒有 $|B_j|\geqslant k$, 并且存在 B_{j_0} 使得 $|B_{j_0}|=k$;

(2) 设 $B^{(i)}=\{B_j|1\leqslant j\leqslant b, x_i\in B_j\}$ $(1\leqslant i\leqslant v)$, 对任意的 $i\in\{1,2,\cdots,v\}$, 恒有 $|B^{(i)}|\geqslant r$, 并且存在 $B^{(i_0)}$ 使得 $|B^{(i_0)}|=r$;

(3) 当 $1\leqslant i\neq j\leqslant v$ 时, 恒有 $|B^{(i)}\cap B^{(j)}|\leqslant\lambda$,

则称 $(X,\mathscr{B})$ 为 X 上的一个弱区组设计, 记为 WBD(b,v,r,k,λ).

* 收稿日期: 2001-03-05
作者简介: 张爱丽(1959-), 女, 博士, 副教授. 现工作单位是西南交通大学数学系.

由定义可以看出：弱区组设计(WBD)是平衡不完全区组设计(BIBD)和异元平衡区组设计(DBBD)的推广，WBD不要求每个区组包含同样多的元素，也不要求每个元素在区组中出现的次数相等或者每两个区组的交集包含同样多的元素.更重要的是，弱区组设计与线性码在同构意义下是一一对应的.任给一个弱区组设计 WBD(b,v,r,k,λ)，存在一个线性码 $C[n,h,d]$ 与之对应，其中 n,h,d 分别表示码长、维数与极小码距，并且诸参数满足：$n=b+v, h=v$，$[r/\lambda]+1\leqslant d\leqslant r+1$，$[r/\lambda]$表示不小于$r/\lambda$的最小整数.反之，任给定一个线性码$C[n,h,d]$，则存在一个弱区组设计 WBD$(b,v,r,k,\lambda)$，使得该弱区组设计对应的线性码 $C_1=C_1[b+v,v,d]$ 与 C 同构.

设 WBD(b,v,r,k,λ) 表示一个弱区组设计，$A=(a_{ij})_{v\times b}$ 是它的关联矩阵，即

$$a_{ij}=\begin{cases}1, & \text{如果 } x_i\in B_j,\\ 0, & \text{如果 } x_i\notin B_j,\end{cases}$$

其中 $X=\{x_1,x_2,\cdots,x_v\}$ 表示 WBD 的顶点集，$\mathscr{B}=\{B_1,B_2,\cdots,B_b\}$ 表示区组族.令 G 表示下面的分块矩阵

$$G=(I_v,A),$$

其中 I_v 表示 v 阶单位矩阵，则以 G 为生成矩阵的线性码就是 WBD 对应的线性码 $C[n,h,d]$.即以 WBD 的顶点为信息位，以区组为监督维线，同时以关联矩阵为监督关系的线性码就是 $C[n,h,d]$.

引理 设 R 是带 1 的交换环，$I_1,I_2,\cdots,I_s$ 是 R 的 s 个两两互素的理想，并且 R/I_i 为有限环，$|R/I_i|=m_i, i=1,2,\cdots,s$，

$$\begin{aligned}J_1&=I_2\cap I_3\cap\cdots\cap I_s,\\ J_2&=I_1\cap I_3\cap\cdots\cap I_s,\\ &\cdots\quad\cdots\\ J_s&=I_1\cap I_2\cap\cdots\cap I_{s-1},\end{aligned}$$

则

(1) $|R/I_1\cap I_2\cap\cdots\cap I_s|=\prod_{i=1}^{s}m_i$;

(2) $|R/J_i|=(m_1m_2\cdots m_s)/m_i$.

证明 (1) 因为 $I_1,I_2,\cdots,I_s$ 是环 R 中两两互素的理想，由“中国剩余定理”[3]，则有环的自然同构

$$R/I_1\cap I_2\cap\cdots\cap I_s\cong R/I_1\oplus R/I_2\oplus\cdots\oplus R/I_s,$$

$$a(\mathrm{mod}\bigcap_{i=1}^{s}I_i)\to(a(\mathrm{mod}I_1),a(\mathrm{mod}I_2),\cdots,a(\mathrm{mod}I_s)).$$

按假设 $|R/I_i|=m_i, 1\leqslant i\leqslant s$，对于任意的 $\bar{a}\in R/I_1\cap I_2\cap\cdots\cap I_s$，$\bar{a}$ 能够一意地表示为

$$\bar{a}=(\bar{a}_1,\bar{a}_2,\cdots,\bar{a}_s),\bar{a}_i\in R/I_i,\quad 1\leqslant i\leqslant s.$$

因此，$|R/I_1\cap I_2\cap\cdots\cap I_s|=m_1m_2\cdots m_s$.

(2) 因为 $R/J_i=R/I_1\cap\cdots\cap I_{i-1}\cap I_{i+1}\cap\cdots\cap I_s$，再根据“中国剩余定理”，可以得到

$$R/J_i\cong R/I_1\oplus\cdots\oplus R/I_{i-1}\oplus R/I_{i+1}\oplus\cdots\oplus R/I_s,$$

$$a(\mathrm{mod}J_i)\to(a(\mathrm{mod}I_1),\cdots,a(\mathrm{mod}I_{i-1}),a(\mathrm{mod}I_{i+1}),\cdots,a(\mathrm{mod}I_s)),$$

所以有 $|R/J_i|=m_1\cdots m_{i-1}m_{i+1}\cdots m_s=(m_1m_2\cdots m_s)/m_i$. □

定理 1 (1) 设 R 是带 1 的交换环，$I_1,I_2,\cdots,I_s$ 是 R 的 s 个两两互素的理想，并且 R/I_i 为有限环，$1\leqslant i\leqslant s$；

(2) 设

$$\begin{aligned}I^*&=I_1\cap I_2\cap\cdots\cap I_s,\\J_1&=I_2\cap I_3\cap\cdots\cap I_s,\\J_2&=I_1\cap I_3\cap\cdots\cap I_s,\\&\cdots\quad\cdots\\J_s&=I_1\cap I_2\cap\cdots\cap I_{s-1}.\end{aligned}$$

(3) 设 $|R/I_i|=m_i,1\leqslant i\leqslant s$；

(4) 设 R/J_i 中含有 n_i 个同余类，每一个同余类选取一个代表元素，得到 $y_1^{(i)},y_2^{(i)},\cdots,y_{n_i}^{(i)}$. 用 R/I^* 中的同余类作信息位[4]，定义监督维线[4]：

$$\begin{aligned}B_{1j}&=\{\bar{x}\mid\bar{x}\in R/I^*,\bar{x}=x+I^*,x\equiv y_j^{(1)}(\mathrm{mod}J_1)\},\ 1\leqslant j\leqslant n_1;\\B_{2j}&=\{\bar{x}\mid\bar{x}\in R/I^*,\bar{x}=x+I^*,x\equiv y_j^{(2)}(\mathrm{mod}J_2)\},\ 1\leqslant j\leqslant n_2;\\&\cdots\quad\cdots\\B_{sj}&=\{\bar{x}\mid\bar{x}\in R/I^*,\bar{x}=x+I^*,x\equiv y_j^{(s)}(\mathrm{mod}J_s)\},\ 1\leqslant j\leqslant n_s.\end{aligned}$$

按照上述信息位和监督维线，可得到一个$[n,h,d]$线性码，这里 n,h,d 分别表示码长、维数和极小码距，并且有

$$n=\prod_{j=1}^{s}m_j+\sum_{i=1}^{s}\left(\frac{1}{m_i}\prod_{j=1}^{s}m_j\right),\ h=\prod_{j=1}^{s}m_j,\ d=s+1.$$

证明 (1) 设 $\bar{x}$ 是 $R/I_1\cap I_2\cap\cdots\cap I_s$ 的任意一个元素，$x\in R$ 是 $\bar{x}$ 的代表元素，即 $\bar{x}=x+I^*$. 因为 R 有如下同余类分解式：

$$R=(y_1^{(i)}+J_i)\cup(y_2^{(i)}+J_i)\cup\cdots\cup(y_{n_i}^{(i)}+J_i)$$

注意到不同的同余类没有公共元素，则 x 必属于分解式中唯一的同余类，则 $\bar{x}$ 被 J_i 对应的监督维线 $B_{i1},B_{i2},\cdots,B_{in_i}$ 恰监督一次. 因此每个信息位恰被监督 s 次.

(2) 每两个不同的信息位至多包含于一条监督维线之中.

事实上，设 $\bar{x}_1,\bar{x}_2$ 包含于两条不同的监督维线 $B_{i_1j_1}$ 和 $B_{i_2j_2}$，即

$$\{\bar{x}_1,\bar{x}_2\}\subseteq(B_{i_1j_1}\cap B_{i_2j_2}),\bar{x}_1,\bar{x}_2\in R/I^*,$$

$$\bar{x}_1\neq\bar{x}_2,\bar{x}_1=x_1+I^*,\bar{x}_2=x_2+I^*,x_1\not\equiv x_2(\mathrm{mod}I^*),$$

$$x_1,x_2\in R,\text{并且}(i_1,j_1)\neq(i_2,j_2),1\leqslant i_1,i_2\leqslant s,1\leqslant j_1\leqslant n_{i_1},1\leqslant j_2\leqslant n_{i_2}$$

则

$$\begin{cases}x_1\equiv y_{j_1}^{(i_1)}(\mathrm{mod}J_{i_1}),\\x_1\equiv y_{j_2}^{(i_2)}(\mathrm{mod}J_{i_2}),\\x_2\equiv y_{j_1}^{(i_1)}(\mathrm{mod}J_{i_1}),\\x_2\equiv y_{j_2}^{(i_2)}(\mathrm{mod}J_{i_2}).\end{cases}\tag{1}$$

首先注意到 $i_1 \neq i_2$. 倘若 $i_1 = i_2$,则 $j_1 \neq j_2$. 则

$$x_1 \equiv y_{j_1}^{(i_1)} (\mathrm{mod} J_{i_1}), 1 \leqslant j_1 \leqslant n_{i_1},\ x_1 \equiv y_{j_2}^{(i_1)} (\mathrm{mod} J_{i_1}), 1 \leqslant j_2 \leqslant n_{i_1},$$

则 $y_{j_1}^{(i_1)} \equiv y_{j_2}^{(i_1)} (\mathrm{mod} J_{i_1})$,与 $j_1 \neq j_2$ 矛盾.

由(1)式可得:

$$\begin{cases} x_1 - x_2 \equiv 0 \ (\mathrm{mod} J_{i_1}), \\ x_1 - x_2 \equiv 0 \ (\mathrm{mod} J_{i_2}). \end{cases} \tag{2}$$

因为 $i_1 \neq i_2, J_{i_1} = \bigcap\limits_{\substack{1 \leqslant i \leqslant s \\ i \neq i_1}} I_i, J_{i_2} = \bigcap\limits_{\substack{1 \leqslant i \leqslant s \\ i \neq i_2}} I_i$,所以 $J_{i_2} \subseteq I_{i_1}$. 则

$$\begin{cases} x_1 - x_2 \equiv 0 \ (\mathrm{mod} J_{i_1}), \\ x_1 - x_2 \equiv 0 \ (\mathrm{mod} I_{i_1}). \end{cases} \tag{3}$$

即

$$x_1 - x_2 \in J_{i_1}, x_1 - x_2 \in I_{i_1}. \tag{4}$$

则 $x_1 - x_2 \in J_{i_1} \cap I_{i_1} = I_1 \cap I_2 \cap \cdots \cap I_s = I^*$. 即 $\bar{x}_1 - \bar{x}_2 = \bar{0}$,这里 $\bar{0}$ 表示 R/I^* 中的零元. 这与 $\bar{x}_1 \neq \bar{x}_2$ 矛盾.

(3) 我们来计算信息位的个数. 因为 R/I^* 中的同余类表示信息位,所以只需计算 $|R/I^*|$. 按照引理,则 $|R/I^*| = |R/I_1 \cap I_2 \cap \cdots \cap I_s| = \prod\limits_{j=1}^{s} m_j$.

(4) 我们来计算监督维线的条数.

因为以理想 J_i 为模的监督维线有 $n_i = |R/J_i|$ 条, $i = 1, 2, \cdots, s$. 再根据引理,有 $|R/J_i| = (m_1 m_2 \cdots m_s / m_i) = \dfrac{1}{m_i} \prod\limits_{j=1}^{s} m_j$. 因此分别以 $J_1, J_2, \cdots, J_s$ 为模的监督维线 $B_{1j}, 1 \leqslant j \leqslant n_1$; $B_{2j}, 1 \leqslant j \leqslant n_2, \cdots, B_{sj}, 1 \leqslant j \leqslant n_s$,合计 $\left(\sum\limits_{i=1}^{s} (1/m_i) \prod\limits_{j=1}^{s} m_j\right)$ 条.

(5) 设该线性码对应的弱区组设计[1,2]是 WBD(b, v, r, k, λ),容易看出

$$b = \sum_{i=1}^{s} \left(\frac{1}{m_i} \prod_{j=1}^{s} m_j\right), v = \prod_{j=1}^{s} m_j, r = s, \lambda = 1.$$

因为

$$R/I_1 \cap \cdots \cap I_s \cong R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_s, \tag{5}$$

$$R/J_i \cong R/I_1 \oplus \cdots \oplus R/I_{i-1} \oplus R/I_{i+1} \oplus \cdots \oplus R/I_s, \tag{6}$$

所以 R/J_i 可以嵌入 $R/I_1 \cap I_2 \cap \cdots \cap I_s$,视为 $R/I_1 \cap I_2 \cap \cdots \cap I_s$ 的一个子环. 注意到 $B_{ij} = \{\bar{x} | \bar{x} \in R/I^*, \bar{x} = x + I^*, x \equiv y_j^{(i)} (\mathrm{mod} J_i)\}, 1 \leqslant j \leqslant n_i, |R/I^*| = \prod\limits_{j=1}^{s} m_j, |R/J_i| = \dfrac{1}{m_i} \prod\limits_{j=1}^{s} m_j$, 则以理想 J_i 为模的监督维线的容量(即容纳信息位的个数)等于 $\left(\prod\limits_{j=1}^{s} m_j\right) / \left(\dfrac{1}{m_i} \prod\limits_{j=1}^{s} m_j\right) = m_i$. 因此,参数 $k = \min\{m_1, m_2, \cdots, m_s\}$.

(6) 从而得到,这个线性码的码长 $n = b + v = \prod\limits_{j=1}^{s} m_j + \sum\limits_{i=1}^{s} \left(\dfrac{1}{m_i} \prod\limits_{j=1}^{s} m_j\right)$,维数 $h = v = \prod\limits_{j=1}^{s} m_j$,极小码距 d 满足不等式: $\left[\dfrac{r}{\lambda}\right] + 1 \leqslant d \leqslant r + 1$. 即 $d = s + 1$. □

定义 2 定理 1 给出的线性码，我们将它命名为中国剩余码.

注 中国剩余码本质上是将同余类环 $R/I_1 \cap I_2 \cap \cdots \cap I_s$ 中的同余类作为信息位，将 R/J_i 嵌入 $R/I_1 \cap I_2 \cap \cdots \cap I_s$，视为 $R/I_1 \cap I_2 \cap \cdots \cap I_s$ 的子环，将 R/J_i 在 $R/I_1 \cap I_2 \cap \cdots \cap I_s$ 中的陪集作为监督维线.

定理 2 设中国剩余码的码率[5]为 η, m_i 的意义与定理 1 中的相同，$1 \leqslant i \leqslant s$，则

$$\eta = M/(M + \sum_{i=1}^{s} M_i),$$

其中 $M = \prod_{j=1}^{s} m_j, M_i = \frac{1}{m_i} \prod_{j=1}^{s} m_j, 1 \leqslant i \leqslant s.$

证明略.

推论 如果 $m_1 \leqslant m_2 \leqslant \cdots \leqslant m_s$，则中国剩余码的码率 η 有下列估计式：

$$\eta \geqslant m_1/(m_1 + s).$$

证明 因为 $m_1 \leqslant m_2 \leqslant \cdots \leqslant m_s$，且 $M_i = (1/m_i) \prod_{j=1}^{s} m_j$，故 $M_1 \geqslant M_2 \geqslant \cdots \geqslant M_s$. 由定理 2 得到：

$$\eta = M/(M + \sum_{i=1}^{s} M_i) \geqslant M/(M + sM_1) = (m_1 m_2 \cdots m_s)/(m_1 m_2 \cdots m_s + s m_2 m_3 \cdots m_s)$$

$$= m_1/(m_1 + s).$$

例 设 $F_p[x]$ 表示有限域 F_p 上的全体多项式构成的环[6]，即

$$F_p[x] = \{f(x) \mid f(x) = \sum_{i=0}^{n} a_i x^i, a_i \in F_p, 0 \leqslant i \leqslant n, 0 \leqslant n < \infty\},$$

其中 p 为一个素数. 则 $F_p[x]$ 是一个带 1 的交换环. 将 $F_p[x]$ 作为定理 1 中的 R.

设 I_1 和 I_2 分别为 x 和 $x+1$ 生成的主理想，即

$$I_1 = (x), \quad I_2 = (x+1).$$

因为 $x + 1 - x = 1$，故 $I_1 + I_2 = R$，I_1 与 I_2 互素.

容易看出，

$$R/I_1 = \{\bar{k} \mid \bar{k} = k + I_1, k = 0,1,\cdots,p-1\},$$

$$R/I_2 = \{\bar{k} \mid \bar{k} = k + I_2, k = 0,1,\cdots,p-1\}.$$

所以，$|R/I_1| = p, |R/I_2| = p$ 按照定理 1 得到一个线性码 $C = C[n,h,d]$，其中

(1) 码长：$n = m_1 m_2 + m_1 + m_2 = p^2 + 2p$；

(2) 维数：$h = m_1 m_2 = p^2$；

(3) 极小码距：$d = s + 1 = 3$；

(4) 码率：$\eta = \frac{h}{n} = \frac{p}{p+2}$.

在定理 1 所给出的“中国剩余码”中，特取 R 为整数环 Z，设 $m_1, m_2, \cdots, m_s$ 是 s 个两两互素的正整数，将 $m_1, m_2, \cdots, m_s$ 各自生成的主理想作为 $I_1, I_2, \cdots, I_s$，即

$$I_i = (m_i), \ i = 1,2,\cdots,s.$$

那么 $I_1, I_2, \cdots, I_s$ 是 R 的 s 个两两互素的理想，并且

$$R/I_1 \cap I_2 \cap \cdots \cap I_s = \{1,2,\cdots,M\} (\mathrm{mod} M),$$

$$M = m_1 m_2 \cdots m_s,$$
$$R/J_i = R/I_1 \cap \cdots \cap I_{i-1} \cap I_{i+1} \cap \cdots \cap I_s = \{1, 2, \cdots, M_i\} (\mathrm{mod} M_i),$$
$$M_i = M/m_i,\ 1 \leqslant i \leqslant s.$$

参考文献：

[1] 刘秀峰，张爱丽. 仿射流形码和射影流形码 [J]. 西南交通大学学报，1998，33(4)：470—474.
LIU Xiu-feng, ZHANG Ai-li. *Affine manifold codes and projective manifold codes* [J]. Journal of Southwest Jiaotong University, 1998, 33(4): 470—474. (in Chinese)

[2] 张爱丽. 弱区组设计与一类新型线性码的研究 [D]. 博士学位论文，西南交通大学，1999.
ZHANG Ai-li. *Study on weak block designs and a new class of linear codes* [D]. Ph. D. Thesis, Southwest Jiaotong University, 1999. (in Chinese)

[3] JACOBSON. *Theory of Rings* [M]. New York, 1943, 68—80.

[4] 靳 蕃. 组合设计与编码 [M]. 成都：西南交通大学出版社，1990，361—395.
JIN Fan. *Combinatorial Designs and Coding* [M]. Chengdu: Publishing House of Southwest Jiaotong University, 1990, 361—395. (in Chinese)

[5] Van Lint J H. *Introduction to Coding Theory* [M]. Berlin: Springer—Verlag, 1982, 15—83.

[6] Van der Waerden B L. 代数学(Ⅰ) [M]. 曹锡华，曾肯成，郝炳新，译. 北京：科学出版社，1976：450—494.
Van der Waerden B L. *Algebra* (Ⅰ) [M]. Translated by Cao Xi-hua, ZENG Ken-cheng, HAO Bing-xin. Beijing: Science Publishing House, 1976, 450—494. (in Chinese)

Chinese Remainder Codes

ZHANG Ai-li[1], LIU Xiu-feng[2]

(1. Dept. of Computer Science, Fudan University, Shanghai 200433, China;
2. Dept. of Appl. Math., Southwest Jiaotong University, Chengdu 610031, China)

Abstract: Chinese remainder codes are constructed by applying the weak block design and Chinese remainder theorem of ring theory. The new type of linear codes are to take the congruence class in the congruence class ring $R/I_1 \cap I_2 \cap \cdots \cap I_n$ for the information bit, to embed R/J_i into $R/I_1 \cap I_2 \cap \cdots \cap I_n$ as a subring of $R/I_1 \cap I_2 \cap \cdots \cap I_n$, and to regard the cosets of R/J_i in $R/I_1 \cap I_2 \cap \cdots \cap I_n$ as check lines. There exist many code classes in Chinese remainder codes, which have higher code rate. Chinese remainder codes are essential generalization of Sun Zhi codes.

Key words: linear code; congruence class; coset; ring.