有限局部环 Z/q^kZ 上对合矩阵标准形的应用*

吴 炎
（琼州大学数学系，海南 五指山市 572200）

摘 要： 设 $\bar{R} = Z/q^kZ$ 是模整数 q^k 的有限局部环，其中 q 是素数，$k > 1$，$q \neq 2$。利用 $\bar{R}$ 上 n 阶对合矩阵的相似标准形，构作了一个 Cartesian 认证码，计算其全部参数。

关键词： 有限局部环；对合矩阵标准形；认证码
中图分类号： O152.8 **文献标识码：** A **文章编号：** 0529-6579（2003）S1-0274-03

设 $\bar{R} = Z/q^kZ$ 是模整数 q^k 的有限局部环[1]，其中 q 是素数 $k > 1$，$q \neq 2$。用 $\bar{R}^*$ 表示 $\bar{R}$ 中可逆元乘群，用 $\bar{a}$ 表示 $\bar{R}$ 中元素，$\langle \bar{q} \rangle$ 表示 $\bar{R}$ 的惟一极大理想。显然 $\bar{2}$ 是 $\bar{R}$ 的单位，$\bar{R}$ 的所有理想都均由 $\bar{q}$ 的某次方幂生成，且对 $\forall \bar{a} \in \bar{R}$，都有 $\bar{a} = \bar{l}\bar{q}^f$，其中 $\bar{l} \in \bar{R}^*$，$0 \leqslant f \leqslant k$。当 $f = 0$ 时，$\bar{a} \in \bar{R}^*$，当 $0 < f \leqslant k$ 时 $\bar{a} \in \langle \bar{q} \rangle$，且 $f = k$ 时 $\bar{a} = \bar{l}\bar{q}^k = \bar{0}$（注意 $\bar{q}^k = \bar{0}$）。易见对 $\forall \bar{l} \in \bar{R}^*$ 和 $\bar{a} \in \langle \bar{q} \rangle$，有 $\bar{l}\bar{a} \in \bar{R}^*$。用 $M_n(\bar{R})$ 表示 $\bar{R}$ 上所有 n 阶矩阵构成的集合，令 $W_n(\bar{R}) = \{A \in M_n(\bar{R}) \mid A^2 = I\}$。

容易证明如下命题

命题 1 若对于 $\bar{a} \in \bar{R}$（$\bar{2}$ 是 $\bar{R}$ 的单位），有 $2\bar{a} = \bar{0}$（注意 $2\bar{a} = \bar{2}\bar{a}$），则 $\bar{a} = \bar{0}$。

引理 1 $W_n(\bar{R})$ 中任意 n 阶对合矩阵 H 都相似于标准形

$$PHP^{-1} = \mathrm{diag}\{-I^{(t)}, I^{(n-t)}\}$$

其中，$P \in GL_n(\bar{R})$，$t = 0,1,\cdots,n$。

此引理利用矩阵代数方法可以证明，由于篇幅原因，在此略去。

关于 Cartesian 认证码的定义及其模仿攻击成功概率的最大值 P_I 和替换攻击成功概率的最大值 P_S 的计算公式请参见文[2,4]。下面利用有限局部环 $\bar{R} = Z/q^kZ$（$q \geqslant 3$，q 为素数）上 n 阶对合矩阵（$\neq \pm I$）标准形，构作了一个 Cartesian 认证码，并计算出其全部参数。

现设

$$W_n^*(\bar{R}) = \{A \in M_n(\bar{R}) \mid A^2 = I, A \neq \pm I\},$$

$$N = \{N_r = \mathrm{diag}(-I^{(r)}, I^{(n-r)}\}$$

其中，$r = 1,2,\cdots,n-1$

令 $M = W_n^*(\bar{R})$，$E = GL_n(\bar{R})$，$S = N$。

对于 $\forall g \in E$，作映射

$$f: S \times E \to M$$
$$(s,g) \to gsg^{-1}$$

由引理 1 知任一不等于 $\pm$ I 的对合矩阵在相似变换下都等价于 N 中某一矩阵标准形，且这种变换下的标准形是唯一确定的；故上面映射是满射，这样就构作了一个 Cartesian 认证码。下面计算其参数。

容易得出

引理 2

$$|S| = n-1,$$
$$|E| = |GL_n(\bar{R})| =$$
$$q^{kn^2}\prod_{i=0}^{n-1}(1-q^{i-n}) = q^{kn^2\frac{n(n+1)}{2}}\prod_{i=1}^{n}(q^i-1)$$

引理 3 设 m 是与信源 $s = N_r = \mathrm{diag}\{-I^{(r)}, I^{(n-r)}\}$ 相应的信息，则属于信息 m 的编码规则的个数等于

$$\omega_r = |GL_r(\bar{R})||GL_{n-r}(\bar{R})| \qquad (1)$$

证明 易见，属于信息 m 的编码规则的个数，就是满足矩阵方程 $XN_rX^{-1} = m$ 的解 X 的个数（$X \in GL_n(\bar{R})$）。此方程 $XN_rX^{-1} = m$ 一定有解，因为由引理 1 知道，至少存在一个 $V \in GL_n(\bar{R})$，使得 $VmV^{-1} = N_r$，即 $V^{-1}N_rV = m$，故 $X = V^{-1}$ 是此方程的解。由此也有 $VXN_rX^{-1}V^{-1} = N_r$。令

$$D_1 = \{X \mid XN_rX^{-1} = m, X \in GL_n(\bar{R})\},$$
$$D_2 = \{VX \mid X \in D_1\} = \{VX \mid VXN_rX^{-1}V^{-1} = N_r, X \in D_1\},$$
$$B_1 = \{Y \mid YN_rY^{-1} = N_r, Y \in GL_n(\bar{R})\},$$

* **收稿日期：** 2003-03-14
基金项目： 海南省教育厅资助项目
作者简介： 吴炎（1964年生），男，副教授；E-mail：wuh1962@eyou.com

$$B_2 = \{V^{-1}Y \mid Y \in B_1\} = \{V^{-1}Y \mid V^{-1}YN_rY^{-1}V = m, Y \in B_1\}$$

则容易看出 $|D_1| = |D_2|$，$|B_1| = |B_2|$，且 $D_2 \subseteq B_1, B_2 \subseteq D_1$；从而有 $|D_1| = |B_1|$。故求矩阵方程 $XN_rX^{-1} = m$ 的解 X(可逆阵) 的个数就是要求出

$$|\{X \in GL_n(\bar{R}) \mid XN_rX^{-1} = N_r\}| = |G_r|$$

由方程 $XN_rX^{-1} = N_r$ 得到

$$XN_r = N_rX \tag{2}$$

取 $X = \begin{bmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{bmatrix} \in GL_n(\bar{R})$，其中 X_{11}, X_{22} 分别是 r 阶和 $n-r$ 阶方阵，而 X_{12}, X_{21} 分别是 $r \times (n-r)$ 矩阵和 $(n-r) \times r$ 矩阵。由(2)式得到 $2X_{12} = 0, 2X_{21} = 0$。于是由命题1得到 $X_{12} = 0, X_{21} = 0$。因此有 $X_{11} \in GL_n(\bar{R}), X_{22} \in GL_{n-r}(\bar{R})$，故属于信息 m 的编码规则个数为(1)所给个数。

引理4

$$|M| = \sum_{r=1}^{n-1} \frac{|GL_n(\bar{R})|}{|GL_r(\bar{R})||GL_{n-r}(\bar{R})|} = \sum_{r=1}^{n-1} \prod_{i=r+1}^{n} \frac{(q^i-1)}{(q^{i-r}-1)} q^{r(n-r)(2k-1)}$$

证明 令 $\Gamma_r = \{A = PN_rP^{-1} \mid P \in GL_n(\bar{R}), A \in W_n^*(\bar{R})\}(r = 1,2,\cdots,n-1)$，易见 $W_n^*(\bar{R}) = \bigcup_{r=1}^{n-1} \Gamma_r$。由于线性群 $GL_n(\bar{R})$ 可迁地作用在 Γ_r 上，令 $G_r = \{P \in GL_n(\bar{R}) \mid PN_rP^{-1} = N_r\}$，由群在集合上作用定理，得到 $|\Gamma_r| = \frac{|GL_n(\bar{R})|}{|G_r|}$；再由引理3的证明有 $|G_r| = |GL_r(\bar{R})||GL_{n-r}(\bar{R})|$。由文[3]中定理1有

$$|GL_n(\bar{R})| = q^{kn^2\frac{n(n+1)}{2}} \prod_{i=1}^{n} (q^i-1),$$

$$|GL_{n-r}(\bar{R})| = q^{k(n-r)^2\frac{(n-r)(n-r+1)}{2}} \prod_{i=1}^{n-r} (q^i-1),$$

$$|GL_r(\bar{R})| = q^{kr^2-\frac{r(r+1)}{2}} \prod_{i=1}^{r} (q^i-1)$$

于是有

$$|M| = |W_n^*(\bar{R})| = \sum_{r=1}^{n-1} |\Gamma_r| = \sum_{r=1}^{n-1} \frac{|GL_n(\bar{R})|}{|G_r|} = \sum_{r=1}^{n-1} \frac{q^{kn^2-\frac{n(n+1)}{2}} \prod_{i=1}^{n} (q^i-1)}{q^{kr^2-\frac{r(r+1)}{2}} q^{k(n-r)^2-\frac{(n-r)(n-r+1)}{2}} \prod_{i=1}^{r} (q^i-1) \prod_{i=1}^{n-r} (q^i-1)}$$

整理便得到引理4所求结果。

引理5 设 m 是与信源 N_{r_2} 相应的信息，m' 是与信源 N_{r_1} 相应的信息 $(1 \leqslant r_1 < r_2 \leqslant n-1)$，且有共同的编码规则属于 m 和 m'，则同属于 m 和 m' 的编码规则的个数为

$$|GL_{r_1}(\bar{R})||GL_{r_2-r_1}(\bar{R})||GL_{n-r_2}(\bar{R})| \tag{3}$$

证明 仿照引理3的证明方法可得到，同属于 m 和 m' 的编码规则的个数就是求满足以下矩阵方程组的可逆矩阵 P 的个数

$$\begin{cases} PN_{r_1}P^{-1} = m' \\ PN_{r_2}P^{-1} = m \end{cases} \text{即} \begin{cases} PN_{r_1} = N_{r_1}P & (4) \\ PN_{r_2} = N_{r_2}P & (5) \end{cases}$$

其中，$N_{r_1} = \mathrm{diag}\{-I_{r_1}, I^{(r_2-r_1}, I^{n-r_2}\}$，

$N_{r_2} = \mathrm{diag}\{-I_{r_2}, I^{n-r_2}\}$。

由于 $1 \leqslant r_1 < r_2 \leqslant n-1$，故取 $P = \begin{bmatrix} P_{11}^{(r_2)} & P_{12}^{r_2\times(n-r_2)} \\ P_{21}^{(n-r_2)\times r_2} & P_{22}^{(n-r_2)} \end{bmatrix}$，将 P 代入(5)式得到 $2P_{12} = 0, 2P_{21} = 0$；由命题1有 $P_{12} = 0, P_{21} = 0$。于是有 $P_{11} \in GL_{r_2}(\bar{R}), P_{22} \in GL_{n-r_2}(\bar{R})$。再设 $P_{11} = \begin{bmatrix} X_{11}^{(r_1)} & X_{12}^{r_1\times(r_2-r_1)} \\ X_{21}^{(r_2-r_1)\times r_1} & X_{22}^{(r_2-r_1)} \end{bmatrix}$，此时 $P = \mathrm{diag}\{P_{11}, P_{22}\}$；将 $P = \mathrm{diag}\{P_{11}, P_{22}\}$ 代入(4)式，同样讨论又得到 $X_{12} = 0, X_{21} = 0, X_{11} \in GL_{r_1}(\bar{R}), X_{22} \in GL_{r_2-r_1}(\bar{R}), P_{22} \in GL_{n-r_2}(\bar{R})$。故得到同属于 m 和 m' 的编码规则个数就是(3)式所给个数。

为方便讨论，引进函数

$$f(r) = |GL_r(\bar{R})||GL_{n-r}(\bar{R})| = q^{\frac{(2k-1)(n^2+2r^2-2nr)-n}{2}} \prod_{i=1}^{r} (q^i-1) \prod_{j=1}^{n-r} (q^j-1)$$

容易看出 $f(r) = f(n-r)$，且直接计算有

$$\frac{f(r+1)}{f(r)} = \frac{q^{r+1}-1}{(q^{n-r}-1)} q^{(2k-1)(2r-n+1)}$$

由于 $k > 1, q \geqslant 3$，所以当 $1 \leqslant r < n/2$ 时，有

$$2r - n + 1 \leqslant 0, r + 1 \leqslant n - r, \frac{f(r+1)}{f(r)} \leqslant 1$$

当 n 是奇数，$r = (n-1)/2$ 时才取等号

此时有

$$f(r+1) < f(r) < \cdots < f(1),$$

$$f(n-r) < f(n-r+1) < \cdots < f(n-1)$$

由引理2和引理3有

$$P_l = \max \frac{|\{e \in E \mid e \in m\}|}{|E|} = \max_{1 \leqslant r \leqslant n-1} \frac{f(r)}{|GL_n(\bar{R})|} = \frac{f(1)}{|GL_n(\bar{R})|} = \frac{q-1}{q^{(n-1)(2k-1)}(q^n-1)}$$

再由引理3和引理5又得到，当 $1 \leqslant r_1 < r_2 \leqslant n-$

1时(当 $r_1 = 1, r_2 = 2$ 时就直接取等号),有

$$\frac{|GL_{r_1}(\bar{R})||GL_{r_2-r_1}(\bar{R})||GL_{n-r_2}(\bar{R})|}{f(r_2)} \leqslant$$

$$\frac{|GL_1(\bar{R})||GL_{r_2-1}(\bar{R})||GL_{n-r_2}(\bar{R})|}{|GL_{r_2}(\bar{R})||GL_{n-r_2}(\bar{R})|} \leqslant$$

$$\frac{|GL_1(\bar{R})||GL_{2-1}(\bar{R})}{GL_2(\bar{R})} =$$

$$\frac{(q^k - q^{k-1})^2}{q^{4k-3}\prod_{i=1}^{2}(q^i - 1)} = \frac{1}{q^{2k-1}(q+1)}$$

故有

$$P_S = \max \frac{|\{e \in E \mid e \in m \text{ 且 } e \in m'\}|}{|\{e \in E \mid e \in m\}|} =$$

$$\max_{1 \leqslant r_1 < r_2 \leqslant n-1} \frac{|GL_{r_1}(\bar{R})||GL_{r_2-r_1}(\bar{R})||GL_{n-r_2}(\bar{R})|}{f(r_2)} =$$

$$\frac{1}{q^{2k-1}(q+1)}$$

综上讨论，得到

定理 利用有限局部环 $\bar{R}$ 上 n 阶对合矩阵 ($\neq \pm I$) 标准形构作的 Cartesian 认证码的参数为

$$|S| = n - 1, \quad |E| = q^{kn^2 - \frac{n(n+1)}{2}}\prod_{i=1}^{n}(q^i - 1),$$

$$|M| = \sum_{r=1}^{n-1}\prod_{i=r+1}^{n}\frac{(q^i - 1)}{(q^{i-r} - 1)}q^{r(n-r)(2k-1)},$$

$$P_I = \frac{q-1}{q^{(n-1)(2k-1)}}(q^n - 1),$$

$$P_S = \frac{1}{q^{2k-1}(q+1)}$$

参考文献：

[1] You H, Nan J Z. Some anzahl theorems in vectorspace over [J]. Acta Math Scientia, 1996, 16(1): 81 - 88.

[2] You H, Nan J Z. Using normal form of matrices over finite fields to construct Cartesian authentication codes[J]. J Math Research & Exposition, 1998, 18(3): 341 - 346.

[3] 游宏，高有. 有限交换环上的典型群阶的计[J]. 科学通报, 1994, 39(14): 1150 - 1154.

[4] Wan Z X. Further constructions of Cartesian authentication code from symplectic Geometry[J]. Northeastern Mathmatical Journal, 1992, 8: 4 - 20.

Normal Form of Involutory Matrices and Its Application over Z/q^kZ

WU Yan

(Department of Mathemathics, Qiongzhou University, Hainan, Wuzhishan 572200, China)

Abstract: Let $\bar{R} = Z/q^kZ$ is finite local ring, where q is prime and $k > 1$ and $q \neq 2$. Using the normal form of involutory matrices over $\bar{R}$, this paper constructs a Cartesian authentication code and compute the parameters of Cartesian authentication code.

Key words: finite local ring; the normal form of involutory matrices; authentication code