Jizhu Nan; Yufang Qin

Structure of unitary groups over finite group rings and its application

Czechoslovak Mathematical Journal, Vol. 60 (2010), No. 2, 495–512

Persistent URL: http://dml.cz/dmlcz/140584

Czechoslovak Mathematical Journal, 60 (135) (2010), 495–512

STRUCTURE OF UNITARY GROUPS OVER FINITE GROUP RINGS AND ITS APPLICATION

Jizhu Nan, Yufang Qin, Dalian

(Received December 5, 2008)

Abstract. In this paper, we determine all the normal forms of Hermitian matrices over finite group rings $R = F_{q^2}G$, where $q = p^\alpha$, G is a commutative p-group with order p^β. Furthermore, using the normal forms of Hermitian matrices, we study the structure of unitary group over R through investigating its BN-pair and order. As an application, we construct a Cartesian authentication code and compute its size parameters.

Keywords: finite group ring, BN-pair, authentication code

MSC 2010: 20E42, 19G24, 94A60

1. Introduction

It is an important topic to investigate classical groups over finite commutative rings. Many results on the structures of the general linear groups, symplectic groups and orthogonal groups over finite commutative rings have been obtained [6], [8], [2]. In [2], the unitary group over a finite group ring was defined by the Hermitian matrix of special form $\left(\begin{smallmatrix} & I^{(n)} \\ I^{(n)} & \end{smallmatrix}\right)$. In the present paper, we determine all the normal forms of Hermitian matrices over finite group rings. Moreover, we study the structures of unitary groups over finite group rings including constructing BN-pairs and computing orders. As an application, we construct a Cartesian authentication code and compute the size parameters.

Let F_{q^2} be a finite field with q^2 elements, where $q = p^\alpha$. Then F_{q^2} has an involutive automorphism $\omega\colon\ x \mapsto x^q$, and the fixed field of this automorphism is F_q. Let G be a commutative p-group with order p^β. From the reference [3], we know that the group ring $R = F_{q^2}G$ is a local ring and its maximal ideal is $M = J(R) = I(G)$, where

Supported by the National Natural Science Foundation of China No. 10771023.

$J(R)$ is Jacobson root of R and $I(G)$ is augmentation ideal of R. Since $I(G)$ is a free F_{q^2}-module with a basis $g-e$, $e \neq g \in G$, it then follows that

$$F_{q^2} \cong R/M \cong R/I(G), \quad |I(G)| = q^{2(p^\beta - 1)} \quad \text{and} \quad |F_{q^2}G| = q^{2p^\beta}.$$

Now the involutive automorphism ω can be extended to an involutive automorphism ω' of R: $\sum\limits_{g\in G} x_g g \mapsto \sum\limits_{g\in G} \omega(x_g)g$. For the convenience of notation, we write $\bar{a}$ for $\omega'(a)$, where $a \in R$. Let $R' = F_qG$. Then R' is a local ring. Denote by M' the maximal ideal of R'.

Throughout this paper, the finite group ring we considered is $R = F_{q^2}G$, where $q = p^\alpha$, G is a commutative p-group with order p^β. Now let us list some definitions that will be used in this paper.

Definition 1.1 ([1])**.** Let $\mathcal{G}$ be a group. A pair of subgroups (B, N) of the group $\mathcal{G}$ is said to be a *BN-pair* if B and N generate $\mathcal{G}$, the intersection $T = B \cap N$ is normal in N and the quotient $W = N/T$ admits a set of generators S such that the following two conditions hold:

(BN1) $\quad BsB \cdot BwB \subset BwB \cup BswB$, where $s \in S$ and $w \in W$;

(BN2) $\quad sBs^{-1} \nsubseteq B$, where $s \in S$.

The group W is called the *Weyl group* associated to the BN-pair. A BN-pair is called *spherical* if the group W is finite.

Definition 1.2. An $m \times m$ matrix H over a finite group ring R is said to be *Hermitian* if ${}^t\overline{H} = H$, where ${}^tH$ denotes the transpose of H and $\overline{H} = (\bar{h}_{ij})$.

Definition 1.3. Let H be an $m \times m$ nonsingular Hermitian matrix over a finite group ring R. The *unitary group* over R with respect to H is defined to be

$$U_m(R, H) = \{T \in GL_m(R) \colon {}^t\overline{T}HT = H\}.$$

2. The normal forms of Hermitian matrices over finite group rings

Before proving the normal forms of Hermitian matrices over R, we first give the following lemmas. Lemmas 2.1 and 2.3 are not going to be proved, see [2], [5].

Lemma 2.1 ([2])**.** *For any $\lambda \in R'$, the equation $x + \bar{x} = \lambda$ has exactly q^{p^β} solutions in R. And for any $\lambda \in M'$, the equation $x + \bar{x} = \lambda$ has exactly $q^{p^\beta - 1}$ solutions in M.*

Lemma 2.2. *Let R^* and R'^* be the sets of all invertible elements of R and R' respectively. Then for any $a \in R'^*$, the equation $x\bar{x} = a$ has exactly $(q+1)q^{p^\beta-1}$ solutions in R^*.*

P r o o f. First we claim that the solution of $x\bar{x} = a$ exists, for any $a \in R'^*$. By [3], $g_1, \dots, g_k \in G$ are a basis of R with $k = p^\beta$, then we can write $x\bar{x} = a$ as follows

$$(x_1, \dots, x_k) \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix} (g_1, \dots, g_k) \begin{pmatrix} \bar{x}_1 \\ \vdots \\ \bar{x}_k \end{pmatrix} = (a_1, \dots, a_k) \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix}.$$

Without loss of generality, we assume that $a_1 \neq 0$. Then we have

$$(x_1, \dots, x_k)T \begin{pmatrix} g'_1 \\ \vdots \\ g'_k \end{pmatrix} (g'_1, \dots, g'_k)^t T \begin{pmatrix} \bar{x}_1 \\ \vdots \\ \bar{x}_k \end{pmatrix} = (1, \dots, 0) \begin{pmatrix} g'_1 \\ \vdots \\ g'_k \end{pmatrix},$$

where

$$T = \begin{pmatrix} a_1^{-1} & -a_1^{-1}a_2 & \dots & -a_1^{-1}a_k \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} g'_1 \\ \vdots \\ g'_k \end{pmatrix} = T^{-1} \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix}.$$

Denote

$$y = (y_1, \dots, y_k) \begin{pmatrix} g'_1 \\ \vdots \\ g'_k \end{pmatrix} = (x_1, \dots, x_k)T \begin{pmatrix} g'_1 \\ \vdots \\ g'_k \end{pmatrix}.$$

Then under the basis $g'_1, \dots, g'_k$ we have $y\overline{y} = 1 \cdot g'_1$. It is clear that this equation has a solution. Thus the claim is proved. □

Consider the map $\varphi\colon\ R^* \to R'^*\colon\ x \mapsto x\bar{x}$. Clearly it is an epimorphism of groups by the claim above. Then we have $|\operatorname{Ker}\varphi| = |R^*|/|R'^*| = (q+1)q^{p^\beta-1}$. Consequently, for any $a \in R'^*$, the equation $x\bar{x} = a$ has exactly $(q+1)q^{p^\beta-1}$ solutions in R^*.

Lemma 2.3 ([6])**.** *Any $m \times m$ nonsingular Hermitian matrix over F_{q^2} is cogredient to*

$$\begin{pmatrix} & I^{(n)} \\ I^{(n)} & \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} & I^{(n)} & \\ I^{(n)} & & \\ & & 1 \end{pmatrix},$$

when $m = 2n$ or $m = 2n+1$, respectively.

Theorem 2.4. *Any $m \times m$ nonsingular Hermitian matrix over R is cogredient to*

$$\begin{pmatrix} & I^{(n)} \\ I^{(n)} & \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} & I^{(n)} & \\ I^{(n)} & & \\ & & 1 \end{pmatrix},$$

when $m = 2n$ or $m = 2n+1$, respectively.

P r o o f. Let H be an $m \times m$ nonsingular Hermitian matrix over R. Consider the group homomorphism $\psi\colon GL_m(R) \to GL_m(F_{q^2})$ induced by the canonical homomorphism $\pi\colon R \to F_{q^2}$. Then $\psi(H) \in GL_m(F_{q^2})$ is a Hermitian matrix over F_{q^2}. By Theorem 5.2 in [5], there exists $Q \in GL_m(F_{q^2})$ such that

$$(1) \qquad {}^t\bar{Q}\psi(H)Q = \begin{pmatrix} h_1 & & \\ & \ddots & \\ & & h_m \end{pmatrix},$$

where $h_1, \ldots, h_m$ are invertible elements of F_{q^2}, i.e., $h_i \neq 0$ $(1 \leqslant i \leqslant m)$. Let $H, Q' \in GL_m(R)$ be coset representatives of $\varphi(H)$ and Q. Then

$$(2) \qquad {}^t\bar{Q}'HQ' = \begin{pmatrix} h_{11} & h_{12} & \ldots & h_{1m} \\ \bar{h}_{12} & h_{22} & \ldots & h_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{h}_{1m} & \bar{h}_{2m} & \ldots & h_{mm} \end{pmatrix} \in GL_m(R).$$

We claim that $h_{11}, \ldots, h_{mm}$ are invertible elements of R and $h_{ij} \in M$, $1 \leqslant i \neq j \leqslant m$. Otherwise, by (2), we have that

$$\psi({}^t\bar{Q}'HQ') = \begin{pmatrix} \pi(h_{11}) & \pi(h_{12}) & \ldots & \pi(h_{1m}) \\ \pi(\bar{h}_{12}) & \pi(h_{22}) & \ldots & \pi(h_{2m}) \\ \vdots & \vdots & \ddots & \vdots \\ \pi(\bar{h}_{1m}) & \pi(\bar{h}_{2m}) & \ldots & \pi(h_{mm}) \end{pmatrix} \in GL_m(F_{q^2}),$$

where $\pi(h_{ii}) = 0$ $(1 \leqslant i \leqslant m)$ and $\pi(h_{ij}) \neq 0$ $(1 \leqslant i \neq j \leqslant m)$. Observe that the fact $\psi({}^t\bar{Q}'HQ') = {}^t\bar{Q}\psi(H)Q$. This is a contradiction with (1).

Denote

$$\begin{pmatrix} h_{11} & h_{12} & \ldots & h_{1m} \\ \bar{h}_{12} & h_{22} & \ldots & h_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{h}_{1m} & \bar{h}_{2m} & \ldots & h_{mm} \end{pmatrix} = T$$

and write T in block form

$$\begin{pmatrix} h_{11} & T_{12} \\ {}^t\overline{T}_{12} & T_{22} \end{pmatrix},$$

where $h_{11} = \bar{h}_{11}$ and T_{22} is an $(m-1)\times(m-1)$ Hermitian matrix. We use induction on m to prove that T is cogredient to a diagonal matrix. When $m = 1$, this is obvious. Now assume that $m \geqslant 2$ and the assertion holds for all $r < m$. Let

$$R = \begin{pmatrix} h_{11} & -h_{11}^{-1}T_{12} \\ & I^{(m-1)} \end{pmatrix}.$$

Then

$${}^t\overline{R}TR = \begin{pmatrix} h_{11} & \\ & -h_{11}^{-1}T_{12}{}^t\overline{T}_{12} + T_{22} \end{pmatrix},$$

where $-h_{11}^{-1}T_{12}{}^t\overline{T}_{12} + T_{22}$ is an $(m-1)\times(m-1)$ nonsingular Hermitian matrix. By induction hypothesis, $-h_{11}^{-1}T_{12}{}^t\overline{T}_{12} + T_{22}$ is cogredient to a diagonal matrix. Consequently, H is cogredient to a diagonal matrix

$$\begin{pmatrix} h_{11} & & & \\ & h'_{22} & & \\ & & \ddots & \\ & & & h'_{mm} \end{pmatrix}.$$

According to Lemma 2.2, there exists $\lambda_i \in R^*$ $(1 \leqslant i \leqslant m)$ such that

$$\begin{pmatrix} \bar{\lambda}_1^{-1} & & \\ & \ddots & \\ & & \bar{\lambda}_m^{-1} \end{pmatrix} \begin{pmatrix} h_{11} & & \\ & \ddots & \\ & & h'_{mm} \end{pmatrix} \begin{pmatrix} \lambda_1^{-1} & & \\ & \ddots & \\ & & \lambda_m^{-1} \end{pmatrix} = I^{(m)}.$$

By Lemma 2.3, $I^{(m)}$ is cogredient to

$$\begin{pmatrix} & I^{(n)} \\ I^{(n)} & \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} & I^{(n)} & \\ I^{(n)} & & \\ & & 1 \end{pmatrix},$$

when $m = 2n$ or $m = 2n+1$ respectively, so does H. □

3. BN-pairs and orders of unitary groups over finite group rings

By Theorem 2.4, when studying the unitary groups over finite group rings R, we only need consider the two special cases $U_m(R, H_1)$ and $U_m(R, H_2)$, where

$$H_1 = \begin{pmatrix} & I^{(n)} \\ I^{(n)} & \end{pmatrix} \quad \text{and} \quad H_2 = \begin{pmatrix} & & I^{(n)} \\ I^{(n)} & & \\ & & 1 \end{pmatrix}.$$

For simplicity we denote them by $U_{2n}(R)$ and $U_{2n+1}(R)$ respectively.

Now we give the definitions of elementary unitary matrices of $U_{2n}(R)$ and $U_{2n+1}(R)$, which play an important role in verifying BN-pairs.

The *elementary unitary matrix* of $U_2(R)$ is the unitary matrix of the following form

$$\begin{pmatrix} a & \\ & \bar{a}^{-1} \end{pmatrix}, \quad \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, \quad \begin{pmatrix} 1 & \\ b & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & c \\ & 1 \end{pmatrix},$$

where a is an invertible element of R, $b + \bar{b} = 0$ and $c + \bar{c} = 0$.

Let R^{2n} be a free module of rank $2n$. Denote the standard basis vectors of R^{2n} by $e_1, e_2, \ldots, e_n, f_1, f_2, \ldots, f_n$. When $n \geqslant 2$, an *elementary unitary matrix* of $U_{2n}(R)$ is defined to be the image of a 2×2 elementary matrix in $U_{2n}(R)$ under one of the embeddings in the following:

(1) For each $i = 1, \ldots, n$, there is an elementary unitary matrix of $U_2(R)$ acting on $[e_i, f_i]$ in $U_{2n}(R)$, which fixes all the basis vectors other than e_i and f_i.
(2) Given $1 \leqslant i < j \leqslant n$, there is an elementary matrix of $GL_2(R)$ acting on $[e_i, e_j]$ in $U_{2n}(R)$, which stabilizes $[e_i, e_j]$ and $[f_i, f_j]$ and fixes all the basis vectors other than these four.
(3) Given $1 \leqslant i < j \leqslant n$, there is an elementary matrix of $GL_2(R)$ acting on $[e_i, f_j]$ in $U_{2n}(R)$, which stabilizes $[e_i, f_j]$ and $[e_j, f_i]$ and fixes all the basis vectors other than these four.

Example. We give some examples of elementary unitary matrices. Take $n = 2$ and $i = 1$ for example in the first embedding. We obtain an elementary unitary matrix $A \in U_4(R)$ which has the following form

$$\begin{pmatrix} * & & * & \\ & 1 & & \\ * & & * & \\ & & & 1 \end{pmatrix}.$$

In the second embedding, for instance, we take $n = 2$, $i = 1$, $j = 2$ and construct an elementary unitary matrix $A \in U_4(R)$ which is given by an elementary matrix

$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ on $[e_1, e_2]$ and which stabilizes $[f_1, f_2]$. Then A must have the form

$$\begin{pmatrix} 1 & a & & \\ 0 & 1 & & \\ & & 1 & 0 \\ & & -\bar{a} & 1 \end{pmatrix}.$$

Similarly, we have the definition of elementary unitary matrix of $U_{2n+1}(R)$.

3.1. BN-pairs of unitary groups $U_{2n}(R)$

Consider the group homomorphism $\theta\colon\ U_{2n}(R) \to U_{2n}(F_{q^2})$ induced by the canonical homomorphism $\pi\colon\ R \to F_{q^2}$. Let $\hat{B}$ be the subgroup of $U_{2n}(F_{q^2})$ consisting of the matrices of the form

$$\begin{pmatrix} C_1 & C_2 \\ & C_3 \end{pmatrix},$$

where C_1 is an $n \times n$ invertible lower triangular matrix, ${}^t\overline{C}_1 C_3 = I$ and ${}^t\bar{C}_2 C_3 + {}^t\bar{C}_3 C_2 = O$. Let $\hat{N}$ be the monomial subgroup of $U_{2n}(F_{q^2})$. We take B and N to be the inverse images of $\hat{B}$ and $\hat{N}$ in $U_{2n}(R)$ respectively and prove that (B, N) is a BN-pair of $U_{2n}(R)$. To show this, we first prove the following lemma.

Lemma 3.1. *The unitary group $U_{2n}(R)$ is generated by its subgroups B and N.*

P r o o f. Through the row and column operations by the elementary unitary matrices and the definition of unitary group, any $A \in U_{2n}(R)$ is reduced to the identity matrix. This proves the assertion. □

Note that $T = B \cap N$ is the inverse image of the diagonal subgroup of $U_{2n}(F_{q^2})$ in $U_{2n}(R)$. Consequently, T is a normal subgroup of N. Then $W = N/T$ has a set of generators $S = \{s_1, s_2, \ldots, s_n\}$, where

$$s_1 = \begin{pmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & I^{(n-2)} & & & & \\ & & & 0 & 1 & & \\ & & & 1 & 0 & & \\ & & & & & I^{(n-2)} \end{pmatrix}, \quad \ldots,$$

$$s_{n-1} = \begin{pmatrix} I^{(n-2)} & & & & & \\ & 0 & 1 & & & \\ & 1 & 0 & & & \\ & & & I^{(n-2)} & & \\ & & & & 0 & 1 \\ & & & & 1 & 0 \end{pmatrix}, \quad s_n = \begin{pmatrix} I^{(n-1)} & & & \\ & 0 & 0 & 1 \\ & 0 & I^{(n-1)} & 0 \\ & 1 & 0 & 0 \end{pmatrix}.$$

Theorem 3.2. *The pair (B, N) is a spherical BN-pair in $U_{2n}(R)$.*

P r o o f. To prove that the axiom (BN1) holds, it is enough to show that for each $s \in S$, $sB \subset BB' \cup BsB'$, where $B' = wBw^{-1}$. We verify only for $s = s_1$, the other elements of S are treated similarly. Any element of sB has the form

$$\begin{pmatrix} c_{21} & a_{22} & \dots & b_{2n} & c_{2,n+1} & c_{2,n+2} & \dots & c_{2,2n} \\ a_{11} & b_{12} & \dots & b_{1n} & c_{1,n+1} & c_{1,n+2} & \dots & c_{1,2n} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ c_{n1} & c_{n2} & \dots & a_{nn} & c_{n,n+1} & c_{n,n+2} & \dots & c_{n,2n} \\ b_{n+2,1} & b_{n+2,2} & \dots & b_{n+2,n} & b_{n+2,n+1} & a_{n+2,n+2} & \dots & c_{n+2,2n} \\ b_{n+1,1} & b_{n+1,2} & \dots & b_{n+1,n} & a_{n+1,n+1} & c_{n+1,n+2} & \dots & c_{n+1,2n} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ b_{2n,1} & b_{2n,2} & \dots & b_{2n,n} & b_{2n,n+1} & b_{2n,n+2} & \dots & a_{2n,2n} \end{pmatrix},$$

where $a_{11}, \dots, a_{2n,2n}$ are invertible elements of R and $b_{ij} \in M$ with $i \neq j$. Through left multiplication by the matrices in B and the definition of unitary group, it is reduced to

$$\begin{pmatrix} c_{21} & a_{22} & b_{23} & \dots & b_{2n} & & & & & \\ a_{11} & 0 & b_{13} & \dots & b_{1n} & & & & & \\ 0 & 0 & & & & & & A_2 & & \\ \vdots & \vdots & & A_1 & & & & & & \\ 0 & 0 & & & & & & & & \\ b_{n+2,1} & b_{n+2,2} & & & & 0 & a_{n+2,n+2} & 0 & \dots & 0 \\ b_{n+1,1} & b_{n+1,2} & & & & a_{n+1,n+1} & c_{n+1,n+2} & 0 & \dots & 0 \\ \vdots & \vdots & & A_3 & & \vdots & \vdots & & A_4 & \\ b_{2n,1} & b_{2n,2} & & & & b_{2n,n+1} & b_{2n,n+2} & & & \end{pmatrix}, \tag{3}$$

where

$$A_1 = \begin{pmatrix} a_{33} & \dots & b_{3n} \\ & \ddots & \vdots \\ & & a_{nn} \end{pmatrix}, \quad A_4 = \begin{pmatrix} a_{n+3,n+3} & & \\ \vdots & \ddots & \\ b_{2n,n+3} & \dots & a_{2n,2n} \end{pmatrix},$$

A_2 is an $n \times n$ zero matrix and A_3 is an $n \times (n-2)$ matrix with entries in the maximal ideal M.

In case that $c_{21} \in M$, the matrix (3) is reduced to s through left multiplication by the matrices in B, i.e., $sB \subset BsB'$. If c_{21} is an invertible element, then using right multiplication by the matrices in B', we reduce the matrix (3) to s or 1, i.e., $sB \subset BB' \cup BsB'$.

Let

$$P = \begin{pmatrix} 1 & & & & & & \\ 1 & 1 & & & & & \\ & & I^{(n-2)} & & & & \\ & & & 1 & -1 & & \\ & & & & 1 & & \\ & & & & & I^{(n-2)} & \end{pmatrix} \in B.$$

Then $s_1 P s_1 \notin B$, which shows that the axiom (BN2) holds. Therefore, (B, N) is a BN-pair and obviously it is spherical. □

3.2. BN-pairs of unitary groups $U_{2n+1}(R)$

Just as in Section 3.1, we consider the group homomorphism $\varphi\colon\ U_{2n+1}(R) \to U_{2n+1}(F_{q^2})$ induced by the canonical homomorphism $\pi\colon\ R \to F_{q^2}$. Let

$$\breve{B} = \left\{ P = \begin{pmatrix} P_1 & & \\ & & a_{2n+1,2n+1} \end{pmatrix} :\ P_1 \in U_{2n}(F_{q^2}),\ P \in U_{2n+1}(F_{q^2}) \right\}$$

and $\breve{N}$ be the monomial subgroup of $U_{2n+1}(F_{q^2})$. Take B' to be the inverse image of $\breve{B}$ and N' the inverse image of $\breve{N}$ in $U_{2n+1}(R)$. Then $T' = B' \cap N'$ is the inverse image of the diagonal subgroup of $U_{2n+1}(F_{q^2})$ in $U_{2n+1}(R)$, whence it is a normal subgroup of N'. Consequently, W' has a set of generators $S' = \{s'_1, s'_2, \dots, s'_n\}$, where

$$s'_1 = \begin{pmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & I^{(n-2)} & & & & \\ & & & 0 & 1 & & \\ & & & 1 & 0 & & \\ & & & & & I^{(n-2)} & \\ & & & & & & 1 \end{pmatrix}, \quad \dots,$$

$$s'_{n-1} = \begin{pmatrix} I^{(n-2)} & & & & & & \\ & 0 & 1 & & & & \\ & 1 & 0 & & & & \\ & & & I^{(n-2)} & & & \\ & & & & 0 & 1 & \\ & & & & 1 & 0 & \\ & & & & & & 1 \end{pmatrix}, \quad s'_n = \begin{pmatrix} I^{(n-1)} & & & \\ & 0 & 0 & 1 \\ & 0 & I^{(n-1)} & 0 \\ & 1 & 0 & 0 \\ & & & & 1 \end{pmatrix}.$$

Theorem 3.3. *The pair (B', N') is a spherical BN-pair in $U_{2n+1}(R)$.*

P r o o f. The proof is analogous to the case of $U_{2n}(R)$. □

3.3. Homological properties of BN-pairs in the unitary groups over group rings

As in Section 1, G is a commutative p-group with order p^β. Suppose that G_i are subgroups of G with order p^i for all $1 \leqslant i \leqslant \beta - 1$. Then $R_i = F_{q^2}G_i$ are a family of group rings. Accordingly, we obtain a family of unitary groups $U_m(R_i)$, where $1 \leqslant i \leqslant \beta - 1$.

Theorem 3.4. *Let (B, N) be the BN-pairs of unitary groups $U_m(R)$ constructed in Sections* 3.1 *and* 3.2. *Assume that $B_i = B \cap U_m(R_i)$ and $N_i = N \cap U_m(R_i)$. Then the pair (B_i, N_i) is a BN-pair of unitary group $U_m(R_i)$.*

P r o o f. The proof is completely similar to the case of $U_m(R)$. □

Let (B_0, N_0) be the BN-pair of the unitary group $U_m(F_{q^2})$. Denote $T_0 = B_0 \cap N_0$ and $W_0 = N_0/T_0$. Then we have the following theorem.

Theorem 3.5. *There exists a commutative diagram with the exact columns:*

$$\begin{array}{ccccccccc}
0 & & 0 & & 0 & & 0 & & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
T_0 & \xrightarrow{i_0} & T_1 & \longrightarrow \cdots \longrightarrow & T_{\beta-1} & \xrightarrow{i_{\beta-1}} & T & & \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
N_0 & \xrightarrow{i'_0} & N_1 & \longrightarrow \cdots \longrightarrow & N_{\beta-1} & \xrightarrow{i'_{\beta-1}} & N & & \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
W_0 & \xrightarrow{\mathrm{id}} & W_1 & \longrightarrow \cdots \longrightarrow & W_{\beta-1} & \xrightarrow{\mathrm{id}} & W & & \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & & 0 & & 0 & & 0 & &
\end{array}$$

where i_j and i'_j $(0 \leqslant j \leqslant \beta - 1)$ are embeddings of groups.

Remark. Although the groups $U_m(R_i)$ $(1 \leqslant i \leqslant \beta)$ and $U_m(F_{q^2})$ are not isomorphic, the associated Weyl groups are completely identical.

3.4. Some Anzahl theorems in unitary groups over finite group rings

Let $\varphi\colon U_{2n+1}(R) \to U_{2n+1}(F_{q^2})$ be as in Section 3.2. Denote $\operatorname{Ker}\varphi = U_{2n+1}M$. Before we prove our main result of this section, we need prove two lemmas.

Lemma 3.6. $|U_3M| = (q+1)q^{9(p^\beta-1)}$.

P r o o f. Assume that

$$P = \begin{pmatrix} 1+c_{11} & c_{12} & c_{13} \\ c_{21} & 1+c_{22} & c_{23} \\ c_{31} & c_{32} & 1+c_{33} \end{pmatrix} \in U_3M,$$

where $c_{ij} \in M$. The definition of unitary group implies that $(1+\bar{c}_{11})c_{21} + \bar{c}_{21}(1+c_{11}) + \bar{c}_{31}c_{31} = 1$, whence c_{11}, c_{21}, c_{31} have $q^{5(p^\beta-1)}$ values by Lemma 2.1. If we choose $c_{11} = c_{21} = c_{31} = 0$, then

$$P = \begin{pmatrix} 1 & c_{12} & c_{13} \\ 0 & 1 & 0 \\ 0 & c_{32} & 1+c_{33} \end{pmatrix}.$$

Since $\bar{c}_{12} + c_{12} + \bar{c}_{32}c_{32} = 1$ by the definition of unitary group, we know c_{12}, c_{32} have $q^{3(p^\beta-1)}$ values. Similarly, we choose $c_{12} = c_{32} = 0$. Then

$$P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1+c_{33} \end{pmatrix},$$

whence $(1+\bar{c}_{33})(1+c_{33}) = 1$ and c_{33} has $(q+1)q^{p^\beta-1}$ values. Therefore, $|U_3M| = (q+1)q^{9(p^\beta-1)}$. □

Lemma 3.7. $|U_{2n+1}M| = (q+1)q^{(4n^2+4n+1)(p^\beta-1)}$.

P r o o f. Assume that

$$P = \begin{pmatrix} 1+c_{11} & \dots & c_{1,n+1} & \dots & c_{1,2n} & c_{1,2n+1} \\ \vdots & & \vdots & & \vdots & \vdots \\ c_{n1} & \dots & c_{n,n+1} & \dots & c_{n,2n} & c_{n,2n+1} \\ c_{n+1,1} & \dots & 1+c_{n+1,n+1} & \dots & c_{n+1,2n} & c_{n+1,2n+1} \\ \vdots & & \vdots & & \vdots & \vdots \\ c_{2n,1} & \dots & c_{2n,n+1} & \dots & 1+c_{2n,2n} & c_{2n,2n+1} \\ c_{2n+1,1} & \dots & c_{2n+1,n+1} & \dots & c_{2n+1,2n} & 1+c_{2n+1,2n+1} \end{pmatrix},$$

where $c_{ij} \in M$. Let

$$P_1 = \begin{pmatrix} I^{(n)} & & \\ S & I^{(n)} & \\ & & 1 \end{pmatrix} \begin{pmatrix} V_1 & & \\ & V_2 & \\ & & 1 \end{pmatrix} \begin{pmatrix} Q_1 & & \\ & Q_2 & \\ & & 1 \end{pmatrix} P,$$

where $Q_1 = \mathrm{diag}[(1+c_{11})^{-1}, 1, \ldots, 1]$, $Q_2 = \mathrm{diag}[1+\bar{c}_{11}, 1, \ldots, 1]$,

$$V_1 = \begin{pmatrix} 1 & & & \\ -c_{21} & 1 & & \\ \vdots & \vdots & \ddots & \\ -c_{n1} & 0 & \ldots & 1 \end{pmatrix}, \quad V_2 = \begin{pmatrix} 1 & \bar{c}_{21} & \ldots & \bar{c}_{n1} \\ & 1 & \ldots & 0 \\ & & \ddots & \vdots \\ & & & 1 \end{pmatrix},$$

$$S = \begin{pmatrix} 0 & \bar{c}_{n+2,1} & \ldots & \bar{c}_{2n,1} \\ -c_{n+2,1} & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -c_{2n,1} & 0 & \ldots & 0 \end{pmatrix}.$$

Then P_1 has the following form

$$\begin{pmatrix} 1 & \ldots & c_{1,n+1} & \ldots & c_{1,2n+1} \\ \vdots & & \vdots & & \vdots \\ 0 & \ldots & c_{n,n+1} & \ldots & c_{n,2n+1} \\ c_{n+1,1}(1+\bar{c}_{11}) + \sum_{j=2}^{n} c_{n+j,1}\bar{c}_{j1} & \ldots & 1+c_{n+1,n+1} & \ldots & c_{n+1,2n+1} \\ \vdots & & \vdots & & \vdots \\ 0 & \ldots & c_{2n,n+1} & \ldots & c_{2n,2n+1} \\ c_{2n+1,1} & \ldots & c_{2n+1,n+1} & \ldots & 1+c_{2n+1,2n+1} \end{pmatrix}.$$

Since P_1 is a unitary matrix, we have that $c_{n+1,1}(1+\bar{c}_{11}) + \bar{c}_{n+1,1}(1+c_{11}) + \sum_{j=2}^{n}(c_{n+j,1}\bar{c}_{j1} + \bar{c}_{n+j,1}c_{j1}) + \bar{c}_{2n+1,1}c_{2n+1,1} = 1$, and hence $c_{11}, \ldots, c_{2n+1,1}$ have $q^{(4n+1)(p^\beta-1)}$ values by Lemma 2.1. If we choose $c_{11} = \ldots = c_{2n+1,1} = 0$, then by the definition of unitary matrix we have

$$P_1 = \begin{pmatrix} 1 & \ldots & c_{1,n+1} & \ldots & c_{1,2n+1} \\ \vdots & & \vdots & & \vdots \\ 0 & \ldots & c_{n,n+1} & \ldots & c_{n,2n+1} \\ 0 & \ldots & 1 & \ldots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \ldots & c_{2n,n+1} & \ldots & c_{2n,2n+1} \\ 0 & \ldots & c_{2n+1,n+1} & \ldots & 1+c_{2n+1,2n+1} \end{pmatrix}.$$

By repetition of the argument, P_1 is reduced to

$$(4)\qquad \begin{pmatrix} 1 & \dots & c_{1,n+1}+\sum_{j=2}^{n} c_{j,n+1}\bar{c}_{n+j,n+1} & \dots & c_{1,2n+1} \\ \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & \dots & c_{n,2n+1} \\ 0 & \dots & 1 & \dots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & \dots & c_{2n,2n+1} \\ 0 & \dots & c_{2n+1,n+1} & \dots & 1+c_{2n+1,2n+1} \end{pmatrix}.$$

Thus $c_{1,n+1}+\bar{c}_{1,n+1}+\sum_{j=2}^{n}(c_{j,n+1}\bar{c}_{n+j,n+1}+\bar{c}_{j,n+1}c_{n+j,n+1})+\bar{c}_{1,2n+1}c_{1,2n+1}=1$ and $c_{1,n+1},\dots,c_{n,n+1},c_{n+2,n+1},\dots,c_{2n+1,n+1}$ have $q^{(4n-1)(p^\beta-1)}$ values. Choose $c_{1,n+1}=\dots=c_{2n+1,n+1}=0$. Then the matrix (4) has the following form

$$(5)\qquad \begin{pmatrix} 1 & 0 & \dots & 0 & \dots & 0 \\ 0 & 1+c_{22} & \dots & 0 & \dots & c_{2,2n+1} \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & c_{n2} & \dots & 0 & \dots & c_{n,2n+1} \\ 0 & 0 & \dots & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & c_{2n,2} & \dots & 0 & \dots & c_{2n,2n+1} \\ 0 & c_{2n+1,2} & \dots & 0 & \dots & 1+c_{2n+1,2n+1} \end{pmatrix}.$$

Clearly, the matrix (5) is the direct sum of

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

and

$$\begin{pmatrix} 1+c_{22} & \dots & c_{2,n+1} & \dots & c_{2,2n} & c_{2,2n+1} \\ \vdots & & \vdots & & \vdots & \vdots \\ c_{n2} & \dots & c_{n,n+1} & \dots & c_{n,2n} & c_{n,2n+1} \\ c_{n+1,2} & \dots & 1+c_{n+1,n+1} & \dots & c_{n+1,2n} & c_{n+1,2n+1} \\ \vdots & & \vdots & & \vdots & \vdots \\ c_{2n,2} & \dots & c_{2n,n+1} & \dots & 1+c_{2n,2n} & c_{2n,2n+1} \\ c_{2n+1,2} & \dots & c_{2n+1,n+1} & \dots & c_{2n+1,2n} & 1+c_{2n+1,2n+1} \end{pmatrix},$$

whence we have $|U_{2n+1}M| = q^{8n(p^\beta-1)}|U_{2n-1}M|$. By Lemma 3.6, we have $|U_{2n+1}M|=(q+1)q^{(4n^2+4n+1)(p^\beta-1)}$.

Theorem 3.8. *Let (B, N) and (B', N') be the BN-pairs of unitary groups $U_{2n}(R)$ and $U_{2n+1}(R)$ constructed above. Then we have*

(1) $|U_{2n}(R)| = q^{4n^2p^\beta-(2n^2+n)} \prod_{i=1}^{2n}(q^i-(-1)^i)$,

$|U_{2n+1}(R)| = (q+1)q^{(4n^2+4n+1)p^\beta-(2n^2+3n+1)} \prod_{i=1}^{2n+1}(q^i-(-1)^i)$;

(2) $|B| = (q^2-1)^n q^{4n^2p^\beta-2n^2}$, $|N| = 2^n n!\,(q^2-1)^n q^{4n^2(p^\beta-1)}$;

(3) $|B^{'}| = (q^2-1)^n(q+1)^2 q^{(4n^2+4n+1)p^\beta-(2n^2+4n+1)}$,

$|N^{'}| = 2^n n!(q^2-1)^n(q+1)q^{(4n^2+4n+1)(p^\beta-1)}$.

P r o o f. The first equation is proved in [2]. Observe that $|U_{2n+1}(F_{q^2})| = q^{n(2n+1)} \prod_{i=1}^{2n+1}(q^i-(-1)^i)$, $\hat{B} = (q^2-1)^n q^{2n^2}$, $\breve{B} = (q+1)(q^2-1)^n q^{2n^2}$, $\hat{N} = 2^n n!(q^2-1)^n$ and $\breve{N} = 2^n n!(q^2-1)^n(q+1)$. By Lemma 3.7, we obtain the results, as required. □

4. Construction of Cartesian authentication codes

In this section, by the normal forms of Hermitian matrices over finite group rings in Theorem 2.4, we construct a Cartesian authentication code and compute its size parameters and the probabilities of successful impersonation and substitution attack. For the definitions of authentication code $(S, E, M; f)$, Cartesian authentication code and the size parameters of code the reader is referred to [4], [7].

Define the source state S to be the set

$$J = \left\{ \begin{pmatrix} I^{(r)} & \\ & 0 \end{pmatrix}_{m\times m} : \ r = 1, 2, \ldots, m \right\},$$

the message M to be the set $N_m(R) = \{A \in M_m^*(R) \colon {}^t\bar{A} = A\}$ and the encoding rules E to be the set $GL_m(R)$. Define

$$f \colon S \times E \to M$$
$$s \times g \to {}^t\overline{g}sg.$$

By Theorem 2.3, we know that every $m \times m$ matrix over R is cogredient to its normal form, so the map f is surjective. Moreover, by the invariance of the rank under cogredient transformation, we show that given any message m there is a unique source state s such that $m = f(s, e)$ for any encoding rule e contained in m. Therefore, $(J, N_m(R), GL_m(R); f)$ is a Cartesian authentication code.

Lemma 4.1. *The number of Hermitian matrices with rank r in $N_m(R)$ is equal to*

$$\begin{cases} \dfrac{q^{2mrp^\beta}\prod\limits_{i=m-r+1}^{m}\left(1-1/q^{2i}\right)}{q^{r^2p^\beta-\frac{1}{2}(r^2+r)}\prod\limits_{i=1}^{r}(q^i-(-1)^i)}, & r=2s, \\ \dfrac{q^{2mrp^\beta}\prod\limits_{i=m-r+1}^{m}\left(1-1/q^{2i}\right)}{(q+1)q^{r^2p^\beta-\frac{1}{2}(r^2+r)}\prod\limits_{i=1}^{r}(q^i-(-1)^i)}, & r=2s+1. \end{cases}$$

P r o o f. Let l be the number of Hermitian matrices with rank r in $N_m(R)$. Consider the action of $GL_m(R)$ on the set $N_m(R)$:

$$\begin{aligned} GL_m(R)\times N_m(R) &\to N_m(R) \\ (P,A) &\mapsto {}^t\overline{P}AP. \end{aligned}$$

Then

$$l=\frac{|GL_m(R)|}{|G_0|},$$

where G_0 is the stabilizer of $\begin{pmatrix} I^{(r)} & \\ & 0 \end{pmatrix}$. Note that $|G_0|$ is equal to the number of the solutions of equation

$${}^t\overline{P}\begin{pmatrix} I^{(r)} & \\ & 0 \end{pmatrix}P=\begin{pmatrix} I^{(r)} & \\ & 0 \end{pmatrix}.$$

Let

$$P=\begin{pmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{pmatrix}.$$

Then ${}^t\overline{P}_{11}I^{(r)}P_{11}=I^{(r)}$, $P_{22}\in GL_{m-r}(R)$ and P_{21} is uniquely determined by P_{12}. Thus

$$l=\frac{|GL_m(R)|}{q^{2p^\beta r(m-r)}|GL_{m-r}(R)||U_r(R)|},$$

as required. □

Lemma 4.2.

$$|S| = m, \quad |E| = q^{2p^\beta m^2} \prod_{i=1}^{m} \Big(1 - \frac{1}{q^{2i}}\Big),$$

$$|M| = \begin{cases} \displaystyle\sum_{s=1}^{n} \left(\frac{q^{4msp^\beta} \prod\limits_{i=m-2s+1}^{m} \big(1 - 1/q^{2i}\big)}{q^{4s^2p^\beta - (2s^2+s)} \prod\limits_{i=1}^{2s} (q^i - (-1)^i)} \right. \\ \qquad \left. + \dfrac{q^{(4ms-2m)p^\beta} \prod\limits_{i=m-2s+2}^{m} \big(1 - 1/q^{2i}\big)}{(q+1) q^{(4s^2-4s+1)p^\beta - (2s^2-s)} \prod\limits_{i=1}^{2s-1} (q^i - (-1)^i)} \right), \\ \qquad m = 2n, \\ \displaystyle\sum_{s=1}^{n} \left(\frac{q^{4msp^\beta} \prod\limits_{i=m-2s+1}^{m} \big(1 - 1/q^{2i}\big)}{q^{4s^2p^\beta - (2s^2+s)} \prod\limits_{i=1}^{2s} (q^i - (-1)^i)} \right. \\ \qquad \left. + \dfrac{q^{(4ms-2m)p^\beta} \prod\limits_{i=m-2s+2}^{m} \big(1 - 1/q^{2i}\big)}{(q+1) q^{(4s^2-4s+1)p^\beta - (2s^2-s)} \prod\limits_{i=1}^{2s-1} (q^i - (-1)^i)} \right) \\ \qquad + \dfrac{q^{2m^2p^\beta} \prod\limits_{i=1}^{m} (1 - 1/q^{2i})}{(q+1) q^{(4n^2+4n+1)p^\beta - (2n^2+3n+1)} \prod\limits_{i=1}^{2n+1} (q^i - (-1)^i)}, \\ \qquad m = 2n+1. \end{cases}$$

P r o o f. The conclusion is obvious by Lemma 4.1. □

Lemma 4.3. *The number of encoding rules contained in a message m is*

$$q^{2(m^2-mr)p^\beta} q^{4s^2p^\beta - (2s^2+s)} \prod_{i=1}^{2s} (q^i - (-1)^i) \prod_{i=1}^{m-2s} \Big(1 - \frac{1}{q^{2i}}\Big)$$

and

$$q^{2(m^2-mr)p^\beta} (q+1) q^{(4s^2+4s+1)p^\beta - (2s^2+3s+1)} \prod_{i=1}^{2s+1} (q^i - (-1)^i) \prod_{i=1}^{m-2s-1} \Big(1 - \frac{1}{q^{2i}}\Big)$$

when $r = 2s$ and $r = 2s+1$, respectively.

P r o o f. Let

$$A = \begin{pmatrix} I^{(r)} & \\ & 0 \end{pmatrix}$$

be the source state corresponding to m. It is easy to see that the number of the encoding rules contained in the message m is equal to the number of the solutions of the equation ${}^t\overline{X}AX = A$. □

Lemma 4.4. *Let m_1 and m_2 be two distinct messages which contain a common encoding rule. Then the number of the encoding rules in both m_1 and m_2 is*

$$q^{2(m^2-r_1m)p^\beta} \prod_{i=1}^{m-r_1} \Big(1 - \frac{1}{q^{2i}}\Big) |U_{r_2}(R)||U_{r_1-r_2}(R)|,$$

where $\operatorname{rank}(m_1) = r_1$, $\operatorname{rank}(m_2) = r_2$ *and* $r_1 \geqslant r_2$.

P r o o f. Let

$$A_1 = \begin{pmatrix} I^{(r_1)} & \\ & 0 \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} I^{(r_2)} & \\ & 0 \end{pmatrix}$$

be the source states corresponding to m_1 and m_2 respectively. Assume that $r_1 > r_2$, for otherwise, $m_1 = m_2$, a contradiction. It suffices to compute the number of the solutions of the matrix equations

$$\text{(6)} \qquad \begin{cases} {}^t\overline{X}A_1X = m_1, \\ {}^t\overline{X}A_2X = m_2, \end{cases} \quad \text{i.e.} \quad \begin{cases} {}^t\overline{X}A_1X = A_1, \\ {}^t\overline{X}A_2X = A_2. \end{cases}$$

By Lemma 4.1, we can assume that

$$X = \begin{pmatrix} X_{11} & X_{12} \\ & X_{22} \end{pmatrix}_{m\times m},$$

where ${}^t\overline{X}_{11}I^{(r_1)}X_{11} = I^{(r_1)}$, $X_{22} \in GL_{m-r_1}(R)$. By (6), we have

$${}^t\overline{X}_{11} \begin{pmatrix} I^{(r_2)} & \\ & 0 \end{pmatrix}_{r_1\times r_1} X_{11} = \begin{pmatrix} I^{(r_2)} & \\ & 0 \end{pmatrix}_{r_1\times r_1}.$$

If we write X_{11} as follows

$$X_{11} = \begin{pmatrix} a & b \\ & d \end{pmatrix},$$

then ${}^t\bar{a}I^{(r_2)}a = I^{(r_2)}$, $d \in GL_{r_1-r_2}(R)$. The fact ${}^t\overline{X}_{11}I^{(r_1)}X_{11} = I^{(r_1)}$ implies that $b = 0$, whence

$$X_{11} = \begin{pmatrix} a & \\ & d \end{pmatrix}_{r_1\times r_1},$$

where ${}^t\bar{a}I^{(r_2)}a = I^{(r_2)}$ and ${}^t\bar{d}I^{(r_1-r_2)}d = I^{(r_1-r_2)}$. □

Theorem 4.5. *If the encoding rules are chosen according to a uniform probability distribution, then the probabilities of a successful impersonation attack P_I and of a successful substitution attack P_S are*

$$P_I = \frac{(q+1)^2}{q^{(2m-1)(p^\beta-1)}(q^{2m}-1)}, \qquad P_S = \frac{(q+1)^3}{(q^m-(-1)^m)q^{(2m-2)p^\beta-(m-1)}}.$$

References

[1] *K. S. Brown*: Buildings. Springer-Verlag, New York, 1989.

[2] *Y. Gao*: Computation of the orders of unitary groups over finite local rings. Acta Math. Scientia *25A* (2005), 564–568. (In Chinese.)

[3] *G. Karpilovsky*: Commutative Group Algebra. Marcel Dekker, New York, 1983.

[4] *Z. X. Wan*: Further construction of Cartesian authentication codes from unitary geometry. Designs, Codes and Cryptology *2* (1992), 333–356.

[5] *Z. X. Wan*: Geometry of Classical Groups over Finite Fields. Studentlitteratur, Lund, 1993.

[6] *H. You*: Sylow subgroups of classical groups over finite commutative rings. Acta Math. Sinica *39* (1996), 33–40. (In Chinese.)

[7] *H. You, J. Z. Nan*: Using normal form of matrices over finite fields to construct Cartesian authentication codes. J. Math. Res. Exposition *18* (1998), 341–346.

[8] *H. You*: Overgroups of symplectic group in linear group over commutative rings. J. Algebra *282* (2004), 23–32.

Authors' address: J. Nan, Y. Qin, Department of Applied Mathematics, Dalian University of Technology, Dalian 116024, P. R. China, e-mail: jznan@163.com.