COGREDIENT STANDARD FORMS OF ORTHOGONAL MATRICES OVER
FINITE LOCAL RINGS OF ODD CHARACTERISTIC

YOTSANAN MEEMARK AND SONGPON SRIWONGSA

Abstract. In this work, we present a cogredient standard form of an orthogonal space over a
finite local ring of odd characteristic.

1. Units and the Square Mapping

A local ring is a commutative ring which has a unique maximal ideal. For a local ring $R$, we
denote its unit group by $R^\times$ and it follows from Proposition 1.2.11 of [1] its unique maximal ideal
$M = R \setminus R^\times$ consists of all non-unit elements. We also call the field $R/M$, the residue field of $R$.

Example 1. If $p$ is a prime, then $\mathbb{Z}_{p^n}$, $n \in \mathbb{N}$, is a local ring with maximal ideal $p\mathbb{Z}_{p^n}$ and residue
field $\mathbb{Z}_{p^n}/p\mathbb{Z}_{p^n}$ isomorphic to $\mathbb{Z}_p$. Moreover, every field is a local ring with maximal ideal $\{0\}$.

Recall a common theorem about local rings that:

Theorem 1.1. Let $R$ be a local ring with unique maximal ideal $M$. Then $1 + m$ is a unit of $R$
for all $m \in M$. Furthermore, $u + m$ a unit in $R$ for all $m \in M$ and $u \in R^\times$.

Proof. Suppose that $1 + m$ is not a unit. Since $R$ is local, $1 + m \in M$. Hence, 1 must be in $M$,
which is a contradiction. Finally, we note that $u + m = u(1 + u^{-1}m)$ is a unit in $R$. □

Let $R$ be a finite local ring of odd characteristic with unique maximal ideal $M$ and residue
field $k$. Then $R$ is of order an odd prime power, and so is $M$. From Theorem XVIII. 2 of [2] we
have that the unit group of $R$, denoted by $R^\times$, is isomorphic to $(1 + M) \times k^\times$. Consider the exact
sequence of groups

$$1 \longrightarrow K_R \longrightarrow R^\times \longrightarrow (R^\times)^2 \longrightarrow 1$$

where $\theta : a \mapsto a^2$ is the square mapping on $R^\times$ with kernel $K_R = \{a \in R^\times : a^2 = 1\}$ and
$(R^\times)^2 = \{a^2 : a \in R^\times\}$. Note that $K_R$ consists of the identity and all elements of order two in $R^\times$. Since
$R$ is of odd characteristic and $k^\times$ is cyclic, $K_R = \{\pm 1\}$. Hence, $[R^\times : (R^\times)^2] = |K_R| = 2$.

Proposition 1.2. Let $R$ be a finite local ring of odd characteristic with unique maximal ideal $M$ and residue field $k$.

1. The image $(R^\times)^2$ is a subgroup of $R^\times$ with index $[R^\times : (R^\times)^2] = 2$.
2. For $z \in R^\times \setminus (R^\times)^2$, we have $R^\times \setminus (R^\times)^2 = z(R^\times)^2$ and $|(R^\times)^2| = |z(R^\times)^2| = (1/2)|R^\times|$.
3. For $u \in R^\times$ and $a \in M$, there exists $c \in R^\times$ such that $c^2(u + a) = u$.
4. If $-1 \notin (R^\times)^2$ and $u \in R^\times$, then $1 + u^2 \in R^\times$.
5. If $-1 \notin (R^\times)^2$ and $z \in R^\times \setminus (R^\times)^2$, then there exist $x, y \in R^\times$ such that $z = (1 + x^2)y^2$.

2000 Mathematics Subject Classification. Primary: 05C25; Secondary: 05C60.
Key words and phrases. Cogredient, Local rings, Orthogonal spaces.
Proof. We have proved (1) in the above discussion and (2) follows from (1). Let \( u \in R^x \) and \( a \in M \). Then \( u^{-1}(u + a) = 1 + u^{-1}a \in 1 + M \), so \((u^{-1}(u + a))^{1+|M|+1} = u^{-1}(u + a) \). Since \(|1 + M| = |M| \) is odd, \( u^{-1}(u + a) = (c^{-1})^2 \) for some \( c \in R^x \). Thus, \( c^2(u + a) = u \) which proves (3).

For (4), assume that \(-1 \notin (R^x)^2 \) and let \( u \in R^x \). Suppose that \( 1 + u^2 = x \in M \). Then \( u^2 = -(1-x) \). Since \(|M| \) is odd and \( 1-x \in 1+M \), \((u|M|)^2 = -((1-x)|M| = -(1)|M|(1-x)|M| = (-1)(1) = -1 \), which contradicts \(-1 \) is non-square. Hence, \( 1 + u^2 \in R^x \).

Finally, we observe that \(|1 + (R^x)^2| = |(R^x)^2| \) is finite. If \( 1 + (R^x)^2 \subseteq (R^x)^2 \), then they must be equal, so there exists \( b \in (R^x)^2 \) such that \( 1 + b = 1 \), which forces \( b = 0 \), a contradiction. Hence, there exists an \( x \in R^x \) such that \( 1 + x^2 \notin (R^x)^2 \). By (4), \( 1 + x^2 \in R^x \). Therefore, for a non-square unit \( z \), we have \( R^x \) is a disjoint union of cosets \((R^x)^2 \) and \( z(R^x)^2 \), so \( 1 + x^2 = z(y^{-1})^2 \) for some \( y \in R^x \) as desired.

In what follows, we shall apply the above proposition to obtain a nice cogredient standard form of an orthogonal space over a finite local ring of odd characteristic. This work generalizes the results over a Galois ring studied in \([2]\).

2. Cogredient standard forms of orthogonal spaces

Throughout this section, we let \( R \) be a finite local ring of odd characteristic.

**Notation.** For any \( l \times n \) matrix \( A \) and \( q \times r \) matrix \( B \) over \( R \), we write

\[
A \oplus B := \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}
\]

which is an \((l+q) \times (n+r)\) matrix over \( R \).

For any matrices \( S_1, S_2 \in M_n(R) \), if there exists an invertible matrix \( P \) such that \( PS_1P^T = S_2 \), we say that \( S_1 \) is cogredient to \( S_2 \) over \( R \) and we write \( S_1 \approx S_2 \). Note that \( S \approx c^2 S \) for all \( c \in R^x \).

The next lemma is a key for our structure theorem.

**Lemma 2.1.** For a positive integer \( \nu \) and \( z \in R^x \setminus (R^x)^2 \), \( zI_{2\nu} \) is cogredient to \( I_{2\nu} \).

**Proof.** If \( -1 = u^2 \) for some \( u \in R^x \), we may choose \( P = 2^{-1} \begin{pmatrix} (1+z) & u^{-1}(1-z) \\ u(1-z) & (1+z) \end{pmatrix} \) whose determinant is \( z \in R^x \). Note that our \( R \) of odd characteristic, so 2 is a unit. Hence, \( P \) is invertible and \( PP^T = zI_2 \). Next, we assume that \(-1 \) is non-square. Then, by Proposition 1\( \nu \) (5), \( z = (1 + x^2) y^2 \) for some units \( x \) and \( y \) in \( R^x \). Choose \( Q = \begin{pmatrix} xy & y \\ -y & xy \end{pmatrix} \). Then \( \det Q = (1 + x^2) y^2 \) and so \( Q \) is invertible and \( QQ^T = \begin{pmatrix} (1 + x^2) y^2 & 0 \\ 0 & 1 + x^2 \end{pmatrix} = zI_2 \). Therefore, \( zI_{2\nu} = \overbrace{zI_2 \oplus \cdots \oplus zI_2}^{\nu \text{ times}} \) is cogredient to \( I_{2\nu} \). \( \square \)

Let \( R \) be a local ring. Let \( V \) be a free \( R \)-module of rank \( n \), where \( n \geq 2 \). Assume that we have a function \( \beta : V \times V \to R \) which is \( R \)-bilinear, symmetric and the \( R \)-module morphism from \( V \) to \( V^* = \text{Hom}_R(V, R) \) given by \( \bar{x} \mapsto \beta(\cdot, \bar{x}) \) is an isomorphism. For \( \bar{x} \in V \), we call \( \beta(\bar{x}, \bar{x}) \) the norm of \( \bar{x} \). The pair \((V, \beta)\) is called an orthogonal space. Moreover, if \( \beta = \{ \bar{b}_1, \ldots, \bar{b}_n \} \) is a basis of \( V \), then the associated matrix \([\beta]_{B} = [\beta(\bar{b}_i, \bar{b}_j)]_{n \times n} \). We say that \( B \) is an orthogonal basis if \( \beta(\bar{b}_i, \bar{b}_j) = u_i \in R^x \) for all \( i \) and \( \bar{b}_i, \bar{b}_j = 0 \) for \( i \neq j \).

McDonald and Hershberger \([4]\) proved the following theorem.
Theorem 2.2 (Theorem 3.2 of [3]). Let \( (V, \beta) \) be an orthogonal space of rank \( n \geq 2 \). Then \( (V, \beta) \) processes an orthogonal basis \( C \) so that \( [\beta]_C \) is a diagonal matrix whose entries on the diagonal are units.

Let \( (V, \beta) \) be an orthogonal space of rank \( n \geq 2 \). Let \( C \) be an orthogonal basis of \( V \) such that \( [\beta]_C \) is a diagonal matrix whose entries on the diagonal are units. From \( [\beta]_C = \text{diag}(u_1, \ldots, u_n) \) and \( u_i \) are units for all \( i \). Assume that \( u_1, \ldots, u_r \) are squares and \( u_{r+1}, \ldots, u_n \) are non-squares. Since \( R^\times \) is a disjoint union of the cosets \( (R^\times)^2 \) and \( z(R^\times)^2 \) for some non-square unit \( z \), we have \( u_i = w_i^2 \) for some \( w_i \in R^\times \), \( i = 1, \ldots, r \) and \( u_j = z w_j^2 \) for some \( w_j \in R^\times \), \( j = r + 1, \ldots, n \). Thus, \( [\beta]_C = \text{diag}(u_1, \ldots, u_r) \oplus z \text{diag}(w_{r+1}, \ldots, w_n) \) which is cogredient to \( I_f \oplus z I_{n-r} \). If \( n - r \) is even, Lemma 2.1 implies that \( [\beta]_C \) is cogredient to \( I_n \). If \( n - r \) is odd, then \( n - r - 1 \) is even and so \( [\beta]_C \) is cogredient to \( I_{n-1} \oplus (z) \) by the same lemma. Note that \( I_n \) and \( I_{n-1} \oplus (z) \) are not cogredient since \( z \) is non-square. We record this result in the next theorem.

Theorem 2.3. Let \( z \) be a non-square unit in \( R \). Then \( [\beta]_C \) is cogredient to either \( I_n \) or \( I_{n-1} \oplus (z) \).

The next lemma follows by a simple calculation.

Lemma 2.4. Let \( z \) be a non-square unit in \( R \) and and \( \nu \) a positive integer. Write \( H_{2\nu} = \begin{pmatrix} 0 & I_{\nu} \\ I_{\nu} & 0 \end{pmatrix} \).

(1) If \(-1 \in (R^\times)^2 \), then \( I_{\nu} \) is cogredient to \( H_{2\nu} \) and \( \begin{pmatrix} 1 & 0 \\ 0 & z \end{pmatrix} \approx \begin{pmatrix} 1 & 0 \\ 0 & -z \end{pmatrix} \).

(2) If \(-1 \notin (R^\times)^2 \), then \( I_{\nu} \oplus z I_{\nu} \) is cogredient to \( H_{2\nu} \) and \( I_2 \approx \begin{pmatrix} 1 & 0 \\ 0 & -z \end{pmatrix} \).

Proof. First we observe that if \(-1 = u^2 \) for some unit \( u \), then

\[
\begin{pmatrix} 1 & 0 \\ 0 & -z \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.
\]

However, if \(-1 \) is non-square, then \(-1 = z c^2 \) for some unit \( c \in R \) and

\[
\begin{pmatrix} 1 & 0 \\ 0 & -z \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -z \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -z c^2 \end{pmatrix} = I_2.
\]

Next, a simple calculation with \( P = \frac{1}{2} \begin{pmatrix} I_{\nu} & -I_{\nu} \\ I_{\nu} & I_{\nu} \end{pmatrix} \) shows that \( L = 2 \begin{pmatrix} I_{\nu} & 0 \\ 0 & -I_{\nu} \end{pmatrix} \) is cogredient to \( H_{2\nu} \). Clearly, if \(-1 \) is square, \( L \) is cogredient to \( I_{2\nu} \). Assume that \(-1 \) is non-square. By Proposition 1.2 (2), \(-1 = z c^2 \) for some unit \( c \) which also implies that \( 2 \) or \(-2 \) must be a square unit. If \( 2 \) is a square unit, then

\[
I_{\nu} \oplus (-I_{\nu}) \approx I_{\nu} \oplus z c^2 I_{\nu} \approx I_{\nu} \oplus z I_{\nu}.
\]

Similarly, if \(-2 \) is a square unit, then

\[
(-I_{\nu}) \oplus I_{\nu} \approx z c^2 I_{\nu} \oplus I_{\nu} \approx I_{\nu} \oplus z I_{\nu}.
\]

Therefore, \( I_{\nu} \oplus z I_{\nu} \) is cogredient to \( H_{2\nu} \). \( \square \)

Next, we apply Lemmas 2.1 and 2.4 in the following calculations. We distinguish three cases. Let \( z \) be a non-square unit and \( \nu \) a positive integer.

1. Assume that \(-1 \) is square. Then

   \( \text{(a) } I_{2\nu} \approx H_{2\nu} \) and \( I_{2\nu+1} \approx H_{2\nu} \oplus (1). \)
(b) $I_{2\nu} \oplus (z) \approx H_{2\nu} \oplus (z)$ and $I_{2(\nu-1)} \oplus (z) \approx I_{2(\nu-1)} \oplus \begin{pmatrix} 1 & 0 \\ 0 & z \end{pmatrix} \approx H_{2\nu-1} \oplus \begin{pmatrix} 1 & 0 \\ 0 & -z \end{pmatrix}$.

(2) Assume that $-1$ is non-square and $\nu$ is even. Then

(a) $I_{2\nu} \approx I_{\nu} \oplus I_{\nu} \approx I_{\nu} \oplus zI_{\nu} \approx H_{2\nu}$ and $I_{2\nu+1} \approx I_{\nu} \oplus I_{\nu} \oplus (1) \approx I_{\nu} \oplus zI_{\nu} \oplus (1) \approx H_{2\nu} \oplus (1)$.

(b) $I_{2\nu} \oplus (z) \approx I_{\nu} \oplus I_{\nu} \oplus (z) \approx I_{\nu} \oplus zI_{\nu} \oplus (z) \approx H_{2\nu} \oplus (z)$ and

$bI_{2\nu-1} \oplus (z) \approx I_{\nu-2} \oplus I_{\nu-2} \oplus I_{3} \oplus (z) \approx I_{\nu-2} \oplus zI_{\nu-2} \oplus I_{3} \oplus (z)$

$\approx I_{\nu-1} \oplus zI_{\nu-1} \oplus I_{2} \approx H_{2(\nu-1)} \oplus \begin{pmatrix} 1 & 0 \\ 0 & -z \end{pmatrix}$.

(3) Assume that $-1$ is non-square and $\nu$ is odd. Then

(a) $I_{2\nu} \approx I_{\nu-1} \oplus I_{\nu-1} \oplus I_{2} \approx I_{\nu-1} \oplus zI_{\nu-1} \oplus I_{2} \approx H_{2(\nu-1)} \oplus \begin{pmatrix} 1 & 0 \\ 0 & -z \end{pmatrix}$ and

$I_{2\nu+1} \approx I_{\nu-1} \oplus I_{\nu-1} \oplus I_{2} \oplus (1) \approx I_{\nu-1} \oplus zI_{\nu-1} \oplus I_{2} \oplus (1) \oplus I_{\nu} \oplus zI_{\nu} \oplus (z) \approx H_{2\nu} \oplus (z)$.

(b) $I_{2\nu} \oplus (z) \approx I_{\nu-1} \oplus I_{\nu-1} \oplus I_{2} \oplus (z) \approx I_{\nu-1} \oplus zI_{\nu-1} \oplus I_{2} \oplus (z) \approx I_{\nu-1} \oplus zI_{\nu-1} \oplus (1) \approx H_{2(\nu-1)} \oplus (1)$ and

$I_{2\nu-1} \oplus (z) \approx I_{\nu-2} \oplus I_{\nu-2} \oplus I_{3} \oplus (z) \approx I_{\nu-2} \oplus zI_{\nu-2} \oplus I_{3} \oplus (z) \approx I_{\nu-1} \oplus zI_{\nu} \approx H_{2\nu}$.

This proves a cogredient standard form of an orthogonal space over a finite local ring of odd characteristic.

**Theorem 2.5.** Let $R$ be a finite local ring of odd characteristic and let $(V, \beta)$ be an orthogonal space where $V$ is a free $R$-module of rank $n \geq 2$. Then there exists a $\delta \in \{0, 1, 2\}$ such that $\nu = \frac{n - \delta}{2} \geq 1$ and the associating matrix of $\beta$ is cogredient to $S_{2\nu+\delta, \Delta}$.

$$S_{2\nu+\delta, \Delta} = \begin{pmatrix} 0 & I_{\nu} \\ I_{\nu} & 0 \end{pmatrix},$$

where

$$\Delta = \begin{cases} \emptyset & \text{if } \delta = 0, \\
(1) & \text{or } (z) & \text{if } \delta = 1, \\
\text{diag}(1, -z) & \text{if } \delta = 2, \end{cases}$$

and $z$ is a fixed non-square unit of $R$.

**Acknowledgments** I would like to thank the Science Achievement Scholarship of Thailand (SAST) for financial support throughout my undergraduate and graduate study.

**References**

[1] G. Bini, F. Flamini, *Finite Commutative Rings and Their Applications*, Spinger, New York, 2002.

[2] Y. Cao, Cogredient standard forms of symmetric matrices over Galois rings of odd characteristic, *ISRN Algebra* (2012). [http://dx.doi.org/10.5402/2012/520148](http://dx.doi.org/10.5402/2012/520148)

[3] B. R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York, 1974.

[4] B. R. McDonald, B. McDonald, The orthogonal group over a full ring, *J. Algebra* 51 (1978) 536-549.

**Yotsanan Meemark**, Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Bangkok, 10330 THAILAND

E-mail address: yotsanan.m@chula.ac.th

**Songpon Sriwongsa**, Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Bangkok, 10330 THAILAND

E-mail address: songpon_sriwongsa@hotmail.com