Bull. Aust. Math. Soc. **96** (2017), 389–397
doi:10.1017/S0004972717000405

CONGRUENCE OF SYMMETRIC INNER PRODUCTS OVER FINITE COMMUTATIVE RINGS OF ODD CHARACTERISTIC

SONGPON SRIWONGSA

(Received 25 February 2017; accepted 2 April 2017; first published online 8 June 2017)

Abstract

Let R be a finite commutative ring of odd characteristic and let V be a free R-module of finite rank. We classify symmetric inner products defined on V up to congruence and find the number of such symmetric inner products. Additionally, if R is a finite local ring, the number of congruent symmetric inner products defined on V in each congruence class is determined.

2010 *Mathematics subject classification*: primary 11E08; secondary 13M99.

Keywords and phrases: congruence, local ring, symmetric inner product.

1. Introduction

Symmetric inner products over finite fields have been widely studied and their classification by congruence is well known [2]. In this paper, we classify the symmetric inner products defined on a free R-module, where R is a finite commutative ring of odd characteristic. Since a finite commutative ring can be decomposed as a finite sum of finite local rings [4, Theorem VI.2], it suffices to classify the symmetric inner products over finite local rings of odd characteristic. Moreover, we determine the number of congruent symmetric inner products in each congruence class.

The paper is organised as follows. In Section 2, we study the general theory of finite local rings. Then, in Section 3, we define a symmetric inner product on a free R-module, where R is a finite commutative ring of odd characteristic. We prove the results over finite local rings and generalise to finite commutative rings in a natural way. Finally, in Section 4, we find the number of congruent symmetric inner products over a finite local ring in each congruence class. More generally, for finite commutative rings, we obtain the number of all symmetric inner products.

2. Finite local rings

A *local ring* is a commutative ring which has a unique maximal ideal. For a local ring R, we denote its unit group by $R^{\times}$. It follows from [1, Proposition 1.2.11] that the

© 2017 Australian Mathematical Publishing Association Inc. 0004-9727/2017 $16.00

https://doi.org/10.1017/S0004972717000405 Published online by Cambridge University Press

unique maximal ideal is $M = R\backslash R^\times$ and consists of all nonunit elements. We call the field R/M, the *residue field of* R. From [4, Theorem V.1]), $1 + m$ is a unit of R for all $m \in M$ and $u + m$ is a unit in R for all $m \in M$ and $u \in R^\times$.

Let R be a finite local ring of odd characteristic with unique maximal ideal M and residue field k. The order of R is a power of an odd prime and so is that of M. From [4, Theorem XVIII. 2], the unit group $R^\times$ is isomorphic to $(1 + M) \times k^\times$. Consider the exact sequence of groups

$$1 \longrightarrow K_R \longrightarrow R^\times \xrightarrow{\theta} (R^\times)^2 \longrightarrow 1,$$

where $\theta : a \longmapsto a^2$ 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 2.1. *Let R be a finite local ring of odd characteristic with unique maximal ideal M.*

(1) *The image of θ is $(R^\times)^2$ and it is a subgroup of $R^\times$ with index $[R^\times : (R^\times)^2] = 2$.*
(2) *For $z \in R^\times\backslash(R^\times)^2$, $R^\times\backslash(R^\times)^2 = z(R^\times)^2$ 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 $z \in R^\times\backslash(R^\times)^2$, then there exist $x, y \in R^\times$ such that $z = (1 + x^2)y^2$.*

Proof. We have proved (1) in the above discussion and (2) follows from (1). Take $u \in R^\times$ 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 $c \in R^\times$. Thus $c^2(u + a) = u$, which proves (3).

For (4), assume that $-1 \notin (R^\times)^2$ and let $u \in R^\times$. 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 the fact that -1 is nonsquare. Hence, $1 + u^2 \in R^\times$.

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

3. Symmetric inner products

Let R be a finite commutative ring of odd characteristic and let V be a free R-module of rank n, where $n \geq 2$. A symmetric bilinear function $\beta : V \times V \to R$ is called a *symmetric inner product* if the R-module morphism from V to $V^* = \mathrm{Hom}_R(V, R)$ given by $\vec{x} \mapsto \beta(\cdot, \vec{x})$ is an isomorphism. Moreover, if $\mathcal{B} = \{\vec{b}_1, \ldots, \vec{b}_n\}$

https://doi.org/10.1017/S0004972717000405 Published online by Cambridge University Press

is a basis of V, then the associated matrix is $[\beta]_{\mathcal{B}} = [\beta(\vec{b}_i, \vec{b}_j)]_{n\times n}$. We say that $\mathcal{B}$ is an *orthogonal basis* if $\beta(\vec{b}_i, \vec{b}_i) = u_i \in R^\times$ for all $i \in \{1, 2, \ldots, n\}$ and $\beta(\vec{b}_i, \vec{b}_j) = 0$ for $i \neq j$.

Two matrices S_1 and $S_2 \in M_n(R)$ are called *congruent*, denoted by $S_1 \approx S_2$, if there exists an invertible matrix $P \in \mathrm{GL}_n(R)$ such that $PS_1P^T = S_2$. Note that $S \approx c^2S$ for all $c \in R^\times$. Clearly, if $S_1 \approx S_2$, then S_1 is symmetric if and only if S_2 is symmetric. This implies that congruence of matrices over R is an equivalence relation on the set of all $n \times n$ symmetric matrices over R. Let β_1 and β_2 be symmetric inner products with the associated matrices S_1 and S_2, respectively. We also say that β_1 and β_2 are *congruent* if $S_1 \approx S_2$.

Notation 3.1. For any $l \times n$ matrix A and $q \times r$ matrix B over R, $A \oplus B$ is the $(l + q) \times (n + r)$ matrix over R defined by

$$A \oplus B := \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}.$$

First, we shall concentrate on a finite local ring of odd characteristic. McDonald and Hershberger [5] proved the following theorem.

Theorem 3.2 [5, Theorem 3.2]. *Let R be a finite local ring of odd characteristic and let V be a free R-module of rank $n \geq 2$ equipped with a symmetric inner product β. Then V possesses an orthogonal basis C, so that $[\beta]_C$ is a diagonal matrix whose diagonal entries are units and hence $[\beta]_C$ is invertible.*

We write $H_{2\nu} = \left(\begin{smallmatrix} 0 & I_\nu \\ I_\nu & 0 \end{smallmatrix}\right)$. The next two lemmas are important tools.

Lemma 3.3. *Let R be a finite local ring of odd characteristic and let $z \in R^\times \backslash (R^\times)^2$. Then $zI_{2\nu}$ and $I_{2\nu}$ are congruent, where $\nu \in \mathbb{N}$.*

Proof. If $-1 = u^2$ for some $u \in R^\times$, we may choose $P = 2^{-1}\left(\begin{smallmatrix} (1+z) & u^{-1}(1-z) \\ u(1-z) & (1+z) \end{smallmatrix}\right)$ whose determinant is $z \in R^\times$. Since R has odd characteristic, 2 is a unit. Hence, P is invertible and $PP^T = zI_2$.

Next, assume that -1 is nonsquare. By Proposition 2.1(5), $z = (1 + x^2)y^2$ for some units x and y in $R^\times$. Choose $Q = \left(\begin{smallmatrix} xy & y \\ -y & xy \end{smallmatrix}\right)$. Then $\det Q = (1 + x^2)y^2 = z \in R^\times$, so Q is invertible and $QQ^T = \left(\begin{smallmatrix} (1+x^2)y^2 & 0 \\ 0 & (1+x^2)y^2 \end{smallmatrix}\right) = zI_2$. Therefore $zI_{2\nu} = \overbrace{zI_2 \oplus \cdots \oplus zI_2}^{\nu \text{ times}}$ is congruent to $I_{2\nu} = \overbrace{I_2 \oplus \cdots \oplus I_2}^{\nu \text{ times}}$. □

Lemma 3.4. *Let R be a finite local ring of odd characteristic and let $z \in R^\times \backslash (R^\times)^2$. For $\nu \in \mathbb{N}$:*

(1) *if $-1 \in (R^\times)^2$, then $I_{2\nu}$ is congruent to $H_{2\nu}$ and* $\mathrm{diag}(1, z) \approx \mathrm{diag}(1, -z)$*; and*
(2) *if $-1 \notin (R^\times)^2$, then $I_\nu \oplus zI_\nu \approx H_{2\nu}$ and $I_2 \approx$* $\mathrm{diag}(1, -z)$.

https://doi.org/10.1017/S0004972717000405 Published online by Cambridge University Press

Proof. First, observe that if $-1 = u^2$ for some unit u, then

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

However, if -1 is nonsquare, then $-1 = zc^2$ for some unit $c \in R$ and

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

A simple calculation with $P = 2^{-1}\left(\begin{smallmatrix}I_\nu & -I_\nu\\ I_\nu & I_\nu\end{smallmatrix}\right)$ shows that $L = 2\left(\begin{smallmatrix}I_\nu & 0\\ 0 & -I_\nu\end{smallmatrix}\right) \approx H_{2\nu}$. Clearly, if -1 is square, $L \approx I_{2\nu}$. Assume that -1 is nonsquare. By Proposition 2.1(2), $-1 = zc^2$ for some unit c which also implies that 2 or -2 must be a square unit. If 2 is a square unit, then

$$L \approx I_\nu \oplus (-I_\nu) \approx I_\nu \oplus zc^2 I_\nu \approx I_\nu \oplus zI_\nu.$$

Similarly, if -2 is a square unit, then

$$L \approx (-I_\nu) \oplus I_\nu \approx zc^2 I_\nu \oplus I_\nu \approx I_\nu \oplus zI_\nu.$$

Therefore, $I_\nu \oplus zI_\nu \approx H_{2\nu}$. □

Let R be a finite local ring of odd characteristic and let V be a free R-module of rank $n \geq 2$ equipped with a symmetric inner product β. By Theorem 3.2, we can choose an orthogonal basis C of V such that $[\beta]_C = \operatorname{diag}(u_1, \ldots, u_n)$ is a diagonal matrix whose diagonal entries are units. We may assume that $u_1, \ldots, u_r$ are squares and that $u_{r+1}, \ldots, u_n$ are nonsquares. Since $R^\times$ is a disjoint union of the cosets $(R^\times)^2$ and $z(R^\times)^2$ for some nonsquare unit z (Proposition 2.1), $u_i = w_i^2$ for some $w_i \in R^\times$, $i = 1, \ldots, r$ and $u_j = zw_j^2$ for some $w_j \in R^\times$, $j = r+1, \ldots, n$. Thus $[\beta]_C = \operatorname{diag}(u_1, \ldots, u_r) \oplus z\operatorname{diag}(w_{r+1}, \ldots, w_n)$, which is congruent to $I_r \oplus zI_{n-r}$. If $n - r$ is even, Lemma 3.3 implies that $[\beta]_C$ is congruent to I_n. If $n - r$ is odd, then $n - r - 1$ is even and so $[\beta]_C$ is congruent to $I_{n-1} \oplus (z)$ by the same lemma. Note that I_n and $I_{n-1} \oplus (z)$ are not congruent since z is nonsquare. We record this result in the following theorem.

Theorem 3.5. *Let R be a finite local ring of odd characteristic and let V be a free R-module of rank $n \geq 2$ equipped with a symmetric inner product β. If C is a basis for V, then $[\beta]_C \approx I_n$ if and only if* $\det[\beta]_C$ *is a square unit and $[\beta]_C \approx I_{n-1} \oplus (z)$ if and only if* $\det[\beta]_C$ *is a nonsquare unit, where z is a nonsquare unit in R.*

Proof. The theorem follows directly from the above discussion and the observations that $\det P[\beta]_C P^T = \det[\beta]_C (\det P)^2$ and $\det P$ is a unit in R. □

Next, we apply Lemmas 3.3 and 3.4, distinguishing three cases. In the calculations, z is a nonsquare unit and ν is a positive integer.

Case 1. Assume that -1 is square. Then:

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

(b) $I_{2\nu} \oplus (z) \approx H_{2\nu} \oplus (z)$ and $I_{2\nu-1} \oplus (z) \approx I_{2(\nu-1)} \oplus \left(\begin{smallmatrix}1 & 0\\ 0 & z\end{smallmatrix}\right) \approx H_{2(\nu-1)} \oplus \left(\begin{smallmatrix}1 & 0\\ 0 & -z\end{smallmatrix}\right)$.

https://doi.org/10.1017/S0004972717000405 Published online by Cambridge University Press

Case 2. Assume that -1 is nonsquare and that ν is even. Then:

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

(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

$$\begin{aligned} I_{2\nu-1} \oplus (z) &\approx I_{\nu-2} \oplus I_{\nu-2} \oplus I_3 \oplus (z) \approx I_{\nu-2} \oplus zI_{\nu-2} \oplus I_3 \oplus (z) \\ &\approx I_{\nu-1} \oplus zI_{\nu-1} \oplus I_2 \approx H_{2(\nu-1)} \oplus \begin{pmatrix} 1 & 0 \\ 0 & -z \end{pmatrix}. \end{aligned}$$

Case 3. Assume that -1 is nonsquare and that ν is odd. Then:

(a) $I_{2\nu} \approx I_{\nu-1} \oplus I_{\nu-1} \oplus I_2 \approx I_{\nu-1} \oplus zI_{\nu-1} \oplus I_2 \approx H_{2(\nu-1)} \oplus \left(\begin{smallmatrix} 1 & 0 \\ 0 & -z \end{smallmatrix}\right)$ and

$$\begin{aligned} I_{2\nu+1} &\approx I_{\nu-1} \oplus I_{\nu-1} \oplus I_2 \oplus (1) \approx I_{\nu-1} \oplus zI_{\nu-1} \oplus zI_2 \oplus (1) \\ &\approx I_\nu \oplus zI_\nu \oplus (z) \approx H_{2\nu} \oplus (z); \end{aligned}$$

(b) $I_{2\nu} \oplus (z) \approx I_{\nu-1} \oplus I_{\nu-1} \oplus I_2 \oplus (z) \approx I_{\nu-1} \oplus zI_{\nu-1} \oplus I_2 \oplus (z) \approx I_\nu \oplus zI_\nu \oplus (1) \approx H_{2\nu} \oplus (1)$ and $I_{2\nu-1} \oplus (z) \approx I_{\nu-1} \oplus I_{\nu-1} \oplus (1) \oplus (z) \approx I_\nu \oplus zI_\nu \approx H_{2\nu}$.

These calculations classify the symmetric inner products defined on a free R-module, where R is a finite local ring of odd characteristic, and they establish the following theorem.

Theorem 3.6. *Let R be a finite local ring of odd characteristic with a fixed nonsquare unit z and let V be a free R-module of rank $n \geq 2$ with a basis C equipped with a symmetric inner product β.*

(1) *If $n = 2\nu$ and $\det[\beta]_C \in (R^\times)^2$, then*

$$[\beta]_C \approx \begin{cases} H_{2\nu} & \text{if } -1 \in (R^\times)^2 \text{ or } \nu \text{ is even}, \\ H_{2(\nu-1)} \oplus \operatorname{diag}(1, -z) & \text{otherwise}. \end{cases}$$

(2) *If $n = 2\nu$ and $\det[\beta]_C \in z(R^\times)^2$, then*

$$[\beta]_C \approx \begin{cases} H_{2(\nu-1)} \oplus \operatorname{diag}(1, -z) & \text{if } -1 \in (R^\times)^2 \text{ or } \nu \text{ is even}, \\ H_{2\nu} & \text{otherwise}. \end{cases}$$

(3) *If $n = 2\nu + 1$ and $\det[\beta]_C \in (R^\times)^2$, then*

$$[\beta]_C \approx \begin{cases} H_{2\nu} \oplus (1) & \text{if } -1 \in (R^\times)^2 \text{ or } \nu \text{ is even}, \\ H_{2\nu} \oplus (z) & \text{otherwise}. \end{cases}$$

(4) *If $n = 2\nu + 1$ and $\det[\beta]_C \in z(R^\times)^2$, then*

$$[\beta]_C \approx \begin{cases} H_{2\nu} \oplus (z) & \text{if } -1 \in (R^\times)^2 \text{ or } \nu \text{ is even}, \\ H_{2\nu} \oplus (1) & \text{otherwise}. \end{cases}$$

https://doi.org/10.1017/S0004972717000405 Published online by Cambridge University Press

For convenience in the next observation, we conclude here that $[\beta]_C$ in the above theorem is congruent to one and only one of

$$S_{2\nu+\delta,\Delta} = \begin{pmatrix} 0 & I_\nu & \\ I_\nu & 0 & \\ & & \Delta \end{pmatrix} \quad \text{where } \Delta = \begin{cases} \emptyset \text{ (empty)} & \text{if } \delta = 0, \\ (1) \text{ or } (z) & \text{if } \delta = 1, \\ \operatorname{diag}(1, -z) & \text{if } \delta = 2. \end{cases}$$

Now, let R be a finite commutative ring of odd characteristic. It is well known that R is a direct product of finite local rings of odd characteristic, say,

$$R = R_1 \times R_2 \times \cdots \times R_t.$$

Consider $V_\delta = R^{2\nu+\delta}$, a free R-module of rank $2\nu + \delta$, where $\nu \geq 1$ and $\delta \in \{0, 1, 2\}$. We have the canonical one-to-one correspondence

$$\vec{x} = (x_1, x_2, \ldots, x_{2\nu+\delta}) \overset{\varphi}{\mapsto} ((x_1^{(j)})_{j=1}^t, (x_2^{(j)})_{j=1}^t, \ldots, (x_{2\nu+\delta}^{(j)})_{j=1}^t).$$

Note that if $\vec{x}, \vec{y} \in V_\delta$, then this correspondence induces the orthogonal map β on V_δ by

$$\begin{aligned}\beta(\vec{x}, \vec{y}) &= \beta(((x_1^{(j)})_{j=1}^t, (x_2^{(j)})_{j=1}^t, \ldots, (x_{2\nu+\delta}^{(j)})_{j=1}^t), ((y_1^{(j)})_{j=1}^t, (y_2^{(j)})_{j=1}^t, \ldots, (y_{2\nu+\delta}^{(j)})_{j=1}^t)) \\ &= (\beta_1(\vec{x}^{(1)}, \vec{y}^{(1)}), \beta_2(\vec{x}^{(2)}, \vec{y}^{(2)}), \ldots, \beta_t(\vec{x}^{(t)}, \vec{y}^{(t)})),\end{aligned}$$

where $\vec{x}^{(j)} = (x_1^{(j)}, x_2^{(j)}, \ldots, x_{2\nu+\delta}^{(j)}) \in V_\delta^{(j)} := R_j^{(2\nu+\delta)}$ and $(V_\delta^{(j)}, \beta_j)$ is an orthogonal space over R_j of rank $2\nu + \delta$ associated with the matrix $S_{2\nu+\delta_j,\Delta_j}$ arising from Theorem 3.6, for all $j \in \{1, 2, \ldots, t\}$. This induces, in a natural way, a decomposition of $S_{2\nu+\delta,\Delta}$. That is, $S_{2\nu+\delta,\Delta} = S_{2\nu+\delta_1,\Delta_1} \oplus S_{2\nu+\delta_2,\Delta_2} \oplus \cdots \oplus S_{2\nu+\delta_t,\Delta_t}$. Therefore, we have the following result for finite commutative rings.

Theorem 3.7. *Let R be a finite commutative ring of odd characteristic and let V be a free R-module of rank $n \geq 2$ with a symmetric inner product β. Then the associated matrix of β is congruent to one and only one of*

$$S_{2\nu+\delta,\Delta} = S_{2\nu+\delta_1,\Delta_1} \oplus S_{2\nu+\delta_2,\Delta_2} \oplus \cdots \oplus S_{2\nu+\delta_t,\Delta_t},$$

where $S_{2\nu+\delta_j,\Delta_j}$ is as presented above, for $j \in \{1, 2, \ldots, t\}$.

4. Number of symmetric inner products

Let R be a finite local ring with unique maximal ideal M and residue field $k = R/M$ and let V be a free R-module of rank $n = 2\nu + \delta$, where $\nu \geq 1$ and $\delta \in \{0, 1, 2\}$. In this section, we use the result over a finite field in [3] to find the number of symmetric inner products β defined on V, which are congruent to each $S_{2\nu+\delta,\Delta}$. We denote this number by $|[S_{2\nu+\delta,\Delta}]|$. In any free R-module V of rank $n \geq 2$, we let $N(V)$ denote the number of all symmetric inner products defined on V and let $I(V)$ denote the number of all symmetric inner products defined on V which are congruent to I_n.

https://doi.org/10.1017/S0004972717000405 Published online by Cambridge University Press

First, we discuss the results over a finite field. From MacWilliams [3], if k is a finite field of odd characteristic and V' is a free k-module of rank $n \geq 2$, then

$$N(V') = \prod_{i=1}^{\lfloor n/2 \rfloor} \frac{|k|^{2i}}{|k|^{2i} - 1} \prod_{i=0}^{n-1} (|k|^{n-i} - 1)$$

and

$$I(V') = \begin{cases} \dfrac{1}{2} N(V') & \text{if } n \text{ is odd,} \\ \dfrac{1}{2} \dfrac{|k|^s + 1}{|k|^s} N(V') & \text{if } n = 2s \text{ is even and } -1 \text{ is a square in } k, \\ \dfrac{1}{2} \dfrac{|k|^s + (-1)^s}{|k|^s} N(V') & \text{if } n = 2s \text{ is even and } -1 \text{ is a nonsquare in } k. \end{cases}$$

Let R be a finite local ring of odd characteristic with unique maximal ideal M and residue field $k = R/M$. Let V be a free R-module of rank $n \geq 2$ equipped with a symmetric inner product β. This induces an inner product space V' over k equipped with β', in an obvious manner. The results over a finite local ring may be considered as lifts from the results over its residue field.

Theorem 4.1 (Lifting theorem). *Let R be a finite local ring with unique maximal ideal M and residue field $k = R/M$ and let V be a free R-module of rank $n = 2\nu + \delta$, where $\nu \geq 1$ and $\delta \in \{0, 1, 2\}$, equipped with a symmetric inner product β. Suppose (V', β') is the induced symmetric inner product space over k. Then the associated matrix for β is congruent to $S_{2\nu+\delta,\Delta}$ if and only if the associated matrix for β' is congruent to $S'_{2\nu+\delta,\Delta}$.*

Proof. We first note that, by Theorem 2.1(3), a lift of a nonsquare unit in k is a nonsquare unit in R. This implies that a lift of $S'_{2\nu+\delta,\Delta}$ in V' is congruent to $S_{2\nu+\delta,\Delta}$ in V. Then the theorem follows from Theorem 3.6. □

The above theorem suggests that each symmetric inner product in a congruence class over the residue field is liftable to symmetric inner products in a congruence class over a given finite local ring by adding all symmetric matrices whose entries are in the maximal ideal. This approach allows us to deduce the number of congruent symmetric inner products in each congruence class.

Theorem 4.2. *Let R be a finite local ring with maximal ideal M and residue field $k = R/M$ and let V be a free R-module of rank $n \geq 2$ with the induced free k-module V'. Then*

$$N(V) = |M|^{n(n+1)/2} \prod_{i=1}^{\lfloor n/2 \rfloor} \frac{|R|^{2i}}{|R|^{2i} - |M|^{2i}} \prod_{i=0}^{n-1} \Big(\frac{|R|^{n-i} - |M|^{n-i}}{|M|^{n-i}} \Big).$$

Moreover, for a fixed nonsquare unit z in R:

(1) *if $n = 2\nu + 1$ is odd, then $|[S_{2\nu+1,\Delta}]| = \frac{1}{2} N(V)$, where $\Delta = (1)$ or (z); and*

https://doi.org/10.1017/S0004972717000405 Published online by Cambridge University Press

(2) *if $n = 2\nu + \delta, \delta \in \{0, 2\}$ is even, then*

$$|[S_{2\nu,\emptyset}]| = \frac{|R|^{\nu} + |M|^{\nu}}{2|R|^{\nu}} N(V) \quad \textit{and} \quad |[S_{2\nu+2,\mathrm{diag}(1,-z)}]| = \frac{|R|^{\nu+1} - |M|^{\nu+1}}{2|R|^{\nu+1}} N(V).$$

Proof. Let β' be a symmetric inner product defined on V' with the associated matrix B'. It is clear that all lifting symmetric inner products of β' defined on V have associated matrices of the form $B + m_n$, where B modulo M is B' and $m_n \in M^{n\times n}$ is symmetric. Then

$$N(V) = |M|^{n(n+1)/2} N(V').$$

Since $|k| = |R|/|M|$, we obtain $N(V)$, as desired.

Next, assume that $n = 2\nu + 1$ is odd. Then, by Theorem 4.1,

$$|[S_{2\nu+1,\Delta}]| = |M|^{n(n+1)/2} |[S'_{2\nu+1,\Delta}]|.$$

It follows from Theorem 3.6 that $|[S'_{2\nu+1,\Delta}]| = I(V')$ or $N(V') - I(V')$. In both cases, $|[S'_{2\nu+1,\Delta}]| = \frac{1}{2}N(V')$, so $|[S_{2\nu+1,\Delta}]| = |M|^{n(n+1)/2}\frac{1}{2}N(V') = \frac{1}{2}N(V)$.

Now assume that $n = 2\nu + \delta, \delta \in \{0, 2\}$ is even. Then, by Theorem 4.1,

$$|[S_{2\nu,\Delta}]| = |M|^{n(n+1)/2} |[S'_{2\nu,\Delta}]| \quad \text{and} \quad |[S_{2\nu+2,\Delta}]| = |M|^{n(n+1)/2} |[S'_{2\nu+2,\Delta}]|.$$

If $-1 \in (R^{\times})^2$, then, by Theorem 3.6,

$$|[S'_{2\nu,\Delta}]| = I(V') = \frac{1}{2}\frac{|k|^{\nu} + 1}{|k|^{\nu}} N(V'), \quad |[S'_{2\nu+2,\Delta}]| = N(V') - I(V') = \frac{1}{2}\frac{|k|^{s} - 1}{|k|^{s}} N(V'),$$

so

$$|[S_{2\nu,\Delta}]| = \frac{|R|^{\nu} + |M|^{\nu}}{2|R|^{\nu}} N(V) \quad \text{and} \quad |[S_{2\nu+2,\Delta}]| = \frac{|R|^{\nu+1} - |M|^{\nu+1}}{2|R|^{\nu+1}} N(V).$$

For the case $-1 \in z(R^{\times})^2$, the results follow by using similar arguments. □

Finally, let R be a finite commutative ring of odd characteristic and write

$$R = R_1 \times R_2 \times \cdots \times R_t$$

as a direct product of finite local rings of odd characteristic R_j, $j \in \{1, 2, \ldots, t\}$. Let V be a free R-module of rank n. Then $V = V_1 \oplus V_2 \oplus \cdots \oplus V_t$, where each V_j is a free R_j-module. From Theorem 4.2, we have the following result.

Theorem 4.3. *Let R be a finite commutative ring of odd characteristic and write $R = R_1 \times R_2 \times \cdots \times R_t$ as a direct product of finite local rings of odd characteristic R_j for $j \in \{1, 2, \ldots, t\}$. Let V be a free R-module of rank n. Then the number of symmetric inner products defined on V is given by*

$$N(V) = \prod_{j=1}^{t} N(V_j) = \prod_{j=1}^{t} |M_j|^{n(n+1)/2} \prod_{i=1}^{\lfloor n/2 \rfloor} \frac{|R_j|^{2i}}{|R_j|^{2i} - |M_j|^{2i}} \prod_{i=0}^{n-1} \Big(\frac{|R_j|^{n-i} - |M_j|^{n-i}}{|M_j|^{n-i}} \Big).$$

https://doi.org/10.1017/S0004972717000405 Published online by Cambridge University Press

Acknowledgements

This work grew out of the author's independent project as a PhD student at University of Wisconsin-Milwaukee. The author would like to thank Professor Yotsanan Meemark from Chulalongkorn University and Professor Yi Ming Zou from University of Wisconsin-Milwaukee for suggestions that greatly improved the manuscript.

References

[1] G. Bini and F. Flamini, *Finite Commutative Rings and Their Applications* (Spinger, New York, 2002).
[2] W. Casselman, 'Quadratic forms over finite fields', 2011, http://www.math.ubc.ca/ cass/siegel/Minkowski.pdf.
[3] J. MacWilliams, 'Orthogonal matrices over finite fields', *Amer. Math. Monthly* **76**(2) (1969), 152–164.
[4] B. R. McDonald, *Finite Rings with Identity* (Marcel Dekker, New York, 1974).
[5] B. R. McDonald and B. Hershberger, 'The orthogonal group over a full ring', *J. Algebra.* **51** (1978), 536–549.

SONGPON SRIWONGSA,
Department of Mathematical Sciences,
University of Wisconsin-Milwaukee, WI, 53211, USA
e-mail: songpon@uwm.edu

https://doi.org/10.1017/S0004972717000405 Published online by Cambridge University Press