CARPATHIAN J. MATH.
Volume **43** (2027), No. 1,
Pages 109-117

Online version at https://www.carpathian.cunbm.utcluj.ro/
Print Edition: ISSN 1584 - 2851; Online Edition: ISSN 1843 - 4401
DOI: https://doi.org/10.37193/CJM.2027.01.07

The largest cardinality of sets of pairwise orthogonal unimodular vectors over finite commutative rings

SIRIPONG SIRISUK[1] AND SONGPON SRIWONGSA[2]

ABSTRACT. Let R be a finite commutative ring of odd characteristic with identity, and let β be a non-degenerate symmetric bilinear form on the free module R^n. In this article, we determine the largest cardinality of a subset $S \subseteq R^n$ consisting of pairwise orthogonal unimodular vectors with respect to β such that S contains a basis for the submodule generated by S, whose elements have norm either 0 or a unit in R.

1. INTRODUCTION

Two classical problems on distinct distances and unit distances in the plane $\mathbb{R}^2$ were posed by Erdős [3]. The first asks for the minimum number of distinct distances determined by n points in the plane, while the second asks for the maximum number of unit distances among n points. These problems were later generalized to n-dimensional Euclidean space [4].

Analogous questions have been studied for points in the n-dimensional vector space over a finite field $\mathbb{F}_q$; see [2, 5, 6], for example. In [5], a distance was defined on $\mathbb{F}_q^n$, where q is an odd prime power, and the distinct distances problem was investigated. More generally, one may consider these problems using arbitrary quadratic forms on $\mathbb{F}_q^n$ as follows. Let β be a non-degenerate symmetric bilinear form on $\mathbb{F}_q^n$. The largest cardinality of a subset $S \subseteq \mathbb{F}_q^n$ of nonzero vectors that are pairwise orthogonal, i.e., $\beta(\vec{x}, \vec{y}) = 0$ for all distinct $\vec{x}, \vec{y} \in S$ was determined in [13]. The case $\beta(\vec{x}, \vec{y}) = l$ for $l \in \mathbb{F}_q$ was later studied in [1]. Extending these questions to finite commutative rings is natural, and in this paper we investigate the problem for free modules of rank n over finite local rings and, more generally, finite commutative rings with identity.

Throughout the paper, all rings are assumed to have an identity. For a commutative ring R and a positive integer $n > 1$, a *bilinear form* β on a free module R^n is a map $\beta : R^n \times R^n \to R$ such that

$$\beta(\vec{x} + \vec{y}, \vec{z}) = \beta(\vec{x}, \vec{z}) + \beta(\vec{y}, \vec{z}) \text{ and } \beta(r\vec{x}, \vec{z}) = r\beta(\vec{x}, \vec{z}),$$

and

$$\beta(\vec{x}, \vec{z} + \vec{w}) = \beta(\vec{x}, \vec{z}) + \beta(\vec{x}, \vec{w}) \text{ and } \beta(\vec{x}, s\vec{z}) = s\beta(\vec{x}, \vec{z}),$$

for all $\vec{x}, \vec{y}, \vec{z}, \vec{w} \in R^n$ and $r, s \in R$. Suppose that $C = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n\}$ is a basis of R^n. For each bilinear form β on R^n, we have the associated $n \times n$ matrix $[\beta]_C = \big(\beta(\vec{u}_i, \vec{u}_j)\big)_{i,j=1}^n$. A bilinear form β is said to be *symmetric* if its associated matrix $[\beta]_C$ is symmetric, and *non-degenerate* if $[\beta]_C$ is invertible. The *determinant* of a bilinear form β, denoted by $\det \beta$, is defined to be $\det[\beta]_C$. Note that the determinant is invariant under a change of basis. For simplicity, we define the *norm* of $\vec{x}$ by $\|\vec{x}\| = \beta(\vec{x}, \vec{x})$ for any $\vec{x} \in R^n$.

Received: 09.10.2025. In revised form: 12.02.2025. Accepted: 15.04.2026
2020 *Mathematics Subject Classification.* 05D05, 15A63, 13H99.
Key words and phrases. *Finite local rings, Unimodular vectors, Orthogonal sets.*
Corresponding author: Songpon Sriwongsa; songpon.sri@kmutt.ac.th

Let R be a finite commutative ring of odd characteristic equipped with a non-degenerate symmetric bilinear form β on R^n. We consider a subset $S \subseteq R^n$ of pairwise orthogonal unimodular vectors with respect to β such that S contains a basis for the submodule $\langle S \rangle_R$ generated by S, and the elements of this basis have norm either 0 or a unit in R. We determine the largest possible cardinality of such a set S. The results for this problem when R is a finite field can be found in [1, 13]. Since every finite commutative ring decomposes as a finite direct sum of finite local rings [7], we first study the problem over finite local rings and then extend the results to general finite commutative rings using elementary tools from ring theory.

2. Bilinear forms and unimodular vectors

Recall that a local ring is a commutative ring with unique maximal ideal. If M is the unique maximal ideal of a local ring R, then the group of units of R is $R \setminus M$. Note that if u is a unit in R, then $u + m$ is a unit for all $m \in M$. We denote the unit group of R by $R^\times$ and the set of all square-units of R by $(R^\times)^2$.

Let R be a finite local ring of odd characteristic. The classification of non-degenerate symmetric bilinear forms for R^n can be obtained from [12] as follows.

Lemma 2.1. *Let R be a finite local ring of odd characteristic. Suppose that β is a non-degenerate symmetric form on R^n. Then there exists a basis C such that only one of the following holds:*

(1) if n is even and $\det \beta \in (R^\times)^2$, then

$$[\beta]_C = \begin{cases} \operatorname{diag}(1,-1,\cdots,1,-1,1,-1) \text{ if } -1 \in (R^\times)^2 \text{ or } \frac{n}{2} \text{ is even}; \\ \operatorname{diag}(1,-1,\cdots,1,-1,1,-z) \text{ if otherwise}, \end{cases}$$

(2) if n is even and $\det \beta \notin (R^\times)^2$, then

$$[\beta]_C = \begin{cases} \operatorname{diag}(1,-1,\cdots,1,-1,1,-z) \text{ if } -1 \in (R^\times)^2 \text{ or } \frac{n}{2} \text{ is even}; \\ \operatorname{diag}(1,-1,\cdots,1,-1,1,-1) \text{ if otherwise}, \end{cases}$$

(3) if n is odd and $\det \beta \in (R^\times)^2$, then

$$[\beta]_C = \begin{cases} \operatorname{diag}(1,-1,\cdots,1,-1,1) \text{ if } -1 \in (R^\times)^2 \text{ or } \frac{n-1}{2} \text{ is even}; \\ \operatorname{diag}(1,-1,\cdots,1,-1,z) \text{ if otherwise}, \end{cases}$$

(4) if n is odd and $\det \beta \notin (R^\times)^2$, then

$$[\beta]_C = \begin{cases} \operatorname{diag}(1,-1,\cdots,1,-1,z) \text{ if } -1 \in (R^\times)^2 \text{ or } \frac{n-1}{2} \text{ is even}; \\ \operatorname{diag}(1,-1,\cdots,1,-1,1) \text{ if otherwise}, \end{cases}$$

where z is a fixed non-square unit in R.

Proof. By [12, Theorem 3.6], there are only two non-congruent forms of β for each integer $n \geq 2$. Assume that n is even. Let

$$A = \operatorname{diag}(1,-1,\cdots,1,-1,1,-1)$$

and

$$B = \operatorname{diag}(1,-1,\cdots,1,-1,1,-z).$$

Then $\det A = (-1)^{\frac{n}{2}}$ and $\det B = (-1)^{\frac{n}{2}} z$. If $-1 \in (R^\times)^2$ or $\frac{n}{2}$ is even, then $\det A$ is a square unit and $\det B$ is a non-square unit. This implies that the forms A and B are non-congruent and the results follow for this case. The similar arguments can be applied when n is odd. $\square$

For convenience in the remainder of this paper, when n is even, we define

$$\mathrm{diag}(1, -1, \cdots, 1, -1, 1, -1)$$

to be the form $\Delta(\emptyset)$ and

$$\mathrm{diag}(1, -1, \cdots, 1, -1, 1, -z)$$

to be the form $\Delta(z)$.

For a commutative ring R, a vector $\vec{x} = (x_1, x_2, \ldots, x_n)$ in R^n is said to be *unimodular* if the ideal generated by $\{x_1, x_2, \ldots, x_n\}$ is equal to R. In particular, if R is a field, then every non-zero vector is unimodular. For the case of a finite local ring R, we have the following lemma on unimodular vectors.

Lemma 2.2. [9, Theorem 2.2] *Let R be a finite local ring. Then a vector $(x_1, x_2, \ldots, x_n) \in R^n$ is unimodular if and only if x_j is a unit for some $j \in \{1, 2, \ldots, n\}$.*

Again, due to the fact that a finite commutative ring $R = R_1 \oplus R_2 \oplus \cdots \oplus R_t$ is a finite direct sum of finite local rings. It can be easily seen that a unimodular vector in R^n can be viewed as a finite direct sum of a unimodular vector in each R_i^n. This fact is a crucial tool for the case of finite commutative rings.

Lemma 2.3. [10, Proposition 1.2] *Let R be a finite commutative ring. A vector*

$$(x_1, x_2, \ldots, x_n) = \bigoplus_{i=1}^{t} (x_1^{(i)}, x_2^{(i)}, \ldots, x_n^{(i)}) \in R^n$$

is unimodular if and only if $(x_1^{(i)}, x_2^{(i)}, \ldots, x_n^{(i)})$ is unimodular over R_i for all $i \in \{1, 2, \ldots, t\}$.

Let R be a finite commutative ring of odd characteristic. For a non-degenerate symmetric bilinear form β on R^n, a *free unimodular orthogonal set* is a subset $S \subseteq R^n$ satisfying

(A1) every element in S is unimodular,
(A2) $\beta(\vec{x}, \vec{y}) = 0$ for any two distinct vectors $\vec{x}, \vec{y} \in S$, and
(A3) S contains a basis for $\langle S \rangle_R$, whose elements have norm either 0 or a unit in R.

We denote by $\mathcal{S}(R^n)$ the largest possible cardinality of a free unimodular orthogonal set in R^n. Our main objective for this paper is to find $\mathcal{S}(R^n)$ explicitly.

3. Main results

In this section, we provide the main results for this work.

3.1. Direct calculation for $\mathcal{S}(R^2)$.

We begin with some observations on the smallest case $n = 2$. The results for this case can be obtained by a direct calculation using properties of a finite local ring R.

Theorem 3.1. *Let R be a finite local ring of odd characteristic with the maximal ideal M. Suppose that β is a non-degenerate symmetric form on R^2.*

(i) If $\det \beta$ is square, then

$$\mathcal{S}(R^2) = \begin{cases} |R| - |M|, & \text{if } -1 \text{ is a square;} \\ 2, & \text{if otherwise.} \end{cases}$$

(ii) If $\det \beta$ is non-square, then

$$\mathcal{S}(R^2) = \begin{cases} 2, & \text{if } -1 \text{ is a square;} \\ |R| - |M|, & \text{if otherwise.} \end{cases}$$

Proof. Fix a non-square unit z in R. By Lemma 2.1, we first assume that

$$\beta(\vec{x},\vec{y}) = x_1y_1 - zx_2y_2 \tag{3.1}$$

for all $\vec{x} = (x_1, x_2), \vec{y} = (y_1, y_2) \in R^2$. This is for the case either

(1) $\det\beta$ is square but -1 is non-square in R, or
(2) $\det\beta$ is non-square but -1 is square in R.

Let S be a free unimodular orthogonal set in R^2 and $(a, b) \in S$. Since (a, b) is unimodular, a or b is a unit (by Lemma 2.2). Suppose that a is a unit. Then other vectors in S are of the form $(a^{-1}zby, y)$ where y is a unit in R. If $\vec{y}_1 = (a^{-1}zby_1, y_1), \vec{y}_2 = (a^{-1}zby_2, y_2) \in S$, then $\beta(\vec{y}_1, \vec{y}_2) = 0$ implies $1 = z(a^{-1}b)^2$, so $1 \in M$ or z is a square unit which is a contradiction. We have a similar argument for the case b is a unit. Thus, $\mathcal{S}(R^2) \leq 2$. Clearly, $\{(1, 0), (0, 1)\}$ is a free unimodular orthogonal set. Therefore, $\mathcal{S}(R^2) = 2$.

Next, consider the other assumptions, and we have

$$\beta(\vec{x},\vec{y}) = x_1y_1 - x_2y_2 \tag{3.2}$$

for $\vec{x} = (x_1, x_2), \vec{y} = (y_1, y_2) \in R^2$. Clearly,

$$S = \{(x, x) \mid x \in R \setminus M\}$$

is a free unimodular orthogonal set because it contains $(1, 1)$. Then $\mathcal{S}(R^2) \geq |R| - |M|$. We show that the converse of the inequality holds. Since $\mathrm{char}(R)$ is odd, $|R| - |M| \geq 2$. If $|R| - |M| = 2$, then $|R| = 3$ and $|M| = 1$, i.e., $R = \mathbb{F}_3$. By [1, Theorem 4], $\mathcal{S}(R^2) = 2 = |R| - |M|$. Assume that $|R| - |M| \geq 3$. Let S be a free unimodular orthogonal set in R^2 and $(a, b) \in S$. Since (a, b) is unimodular, a or b is a unit (by Lemma 2.2). Suppose that a is a unit. Then other vectors in S are of the form $(a^{-1}by, y)$ where y is a unit in R, so $|S| \leq |R| - |M| + 1$. If $\vec{y}_1 = (a^{-1}by_1, y_1)$ and $\vec{y}_2 = (a^{-1}by_2, y_2)$ are two distinct vectors in S, then $\beta(\vec{y}_1, \vec{y}_2) = 0$ implies $1 = (a^{-1}b)^2$, and so $(a, b) = (a^{-1}b^2, b)$ is also in that form. It can be argued similarly for the case that b is a unit. Thus, we have $\mathcal{S}(R^2) \leq |R| - |M|$. Therefore, the equality holds, and we have (2). □

From the proof of Theorem 3.1, we observe the following statements.

(1) If β is of the form (3.1), then all free unimodular orthogonal sets of R^2 with the largest possible cardinality are of the forms
   - $\{(a, b), (a^{-1}bzy, y)\}$ where $a \in R^\times$, $b \in R$ and $y \in R^\times$, or
   - $\{(a, b), (x, (bz)^{-1}ax)\}$ where $a \in M$ and $b, x \in R^\times$.

(2) If β is of the form (3.2), then all free unimodular orthogonal sets of R^2 with the largest possible cardinality are of the forms

$$\{(ux, x) \mid x \in R^\times\} \text{ or } \{(x, ux) \mid x \in R^\times\}$$

where $u \in R$ with $u^2 = 1$. In particular, if $R = \mathbb{Z}_{p^s}$ where p is an odd prime, then all maximal unimodular orthogonal sets of R^2 are

$$\{(x, x) \mid x \in R^\times\}, \{(-x, x) \mid x \in R^\times\} \text{ and } \{(x, -x) \mid x \in R^\times\}.$$

With the approach outlined above, the results remain valid even without assuming the freeness of S when $n = 2$. However, extending this method to larger n seems to be infeasible due to the increasing complexity of the equations. To advance our work, we introduce an alternative approach in the following subsection to achieve the desired results. This method is inspired by Ahmadi and Mohammadian's work on finite fields [1], with certain arguments modified to apply to the case of a finite local ring.

3.2. **Result for a general $\mathcal{S}(R^n)$.** To initiate some ideas, we begin with the construction of a set that satisfies the desired conditions, and also obtain a lower bound for $\mathcal{S}(R^n)$. For $i = 1, 2, \ldots, n$, let $\vec{e}_i$ denote a standard unit vector whose ith position is 1 and 0 elsewhere.

Theorem 3.2. *Let R be a finite local ring of odd characteristic with the maximal ideal M. Suppose that β is a non-degenerate symmetric form of R^n. Then $\mathcal{S}(R^n)$ is at least*

$$\begin{cases} |R|^{\frac{n-1}{2}} - |M|^{\frac{n-1}{2}} + 1, & \text{if } n \text{ is odd;} \\ |R|^{\frac{n}{2}} - |M|^{\frac{n}{2}}, & \text{if } n \text{ is even and } \beta \text{ takes the form } \Delta(\emptyset); \\ |R|^{\frac{n}{2}-1} - |M|^{\frac{n}{2}-1} + 2, & \text{if } n \text{ is even and } \beta \text{ takes the form } \Delta(z). \end{cases}$$

Proof. Consider the following cases.
Case 1: $n = 2m + 1$. Then we let

$$S_1 = \{(x_1, x_1, \ldots, x_m, x_m, 0) \mid (x_1, \ldots, x_m) \in R^m \setminus M^m\} \cup \{\vec{e}_n\}.$$

Note that $\langle S_1 \rangle_R$ is a free submodule with a basis

$$\{\vec{e}_1 + \vec{e}_2, \vec{e}_3 + \vec{e}_4, \ldots, \vec{e}_{n-2} + \vec{e}_{n-1}, \vec{e}_n\}.$$

Case 2: $n = 2m$ and β takes the form $\Delta(\emptyset)$. Then we let

$$S_2 = \{(x_1, x_1, \ldots, x_m, x_m) \mid (x_1, \ldots, x_m) \in R^m \setminus M^m\}.$$

Note that $\langle S_2 \rangle_R$ is a free submodule with a basis

$$\{\vec{e}_1 + \vec{e}_2, \vec{e}_3 + \vec{e}_4, \ldots, \vec{e}_{n-1} + \vec{e}_n\}.$$

Case 3: $n = 2m$ and β takes the form $\Delta(z)$. Then we let

$$S_3 = \{(x_1, x_1, \ldots, x_{m-1}, x_{m-1}, 0, 0) \mid (x_1, x_2 \ldots, x_{m-1}) \in R^m \setminus M^m\} \cup \{\vec{e}_{n-1}, \vec{e}_n\}.$$

In particular, $S_3 = \{\vec{e}_1, \vec{e}_2\}$ if $n = 2$. Note that $\langle S_3 \rangle_R$ is a free submodule with a basis $\{\vec{e}_1 + \vec{e}_2, \vec{e}_3 + \vec{e}_4, \ldots, \vec{e}_{n-3} + \vec{e}_{n-2}, \vec{e}_{n-1}, \vec{e}_n\}$.

Therefore, S_1, S_2 and S_3 are free unimodular orthogonal sets. By a trivial calculation of the cardinality of each set, we obtain the result in the theorem. □

In what follows, we show that the converse of the inequality in Theorem 3.2 also holds. Therefore, the main results of this paper can be obtained.

We recall some important ingredients from the theory of modules over a finite local ring R of odd characteristic. Let X be a subset of R^n and let $X^\perp$ be the subspace of R^n orthogonal to S, that is,

$$X^\perp = \{\vec{x} \in R^n \mid \beta(\vec{x}, \vec{v}) = 0 \text{ for all } \vec{v} \in S\}.$$

It is called the *dual subspace* of X.

Proposition 3.3. *Let R be a finite local ring of odd characteristic and let β be a non-degenerate symmetric bilinear form over R^n. If X is a free submodule of rank m, then $X^\perp$ is a free submodule of rank $n - m$. Therefore,* $\operatorname{rank} X + \operatorname{rank} X^\perp = n$.

Proof. Assume that β takes the form either $S = I_n$ or $I_{n-1} \oplus (z)$ where z is a fixed non-square unit in R as shown in [12, Theorem 3.5]. Let X be a free submodule of R^n of rank m. It follows from [11, Proposition 3.5] that X has a matrix representation $X = (I_m, 0_{m,n-m})U$, for some invertible matrix $U \in \mathrm{GL}_n(R)$. Let $W = S(U^{-1})^T S^{-1}$. Then $W \in \mathrm{GL}_n(R)$ and it can be shown that $X^\perp$ has a matrix representation

$$X^\perp = (0_{n-m,m}, I_{n-m})W.$$

Indeed, the free submodule corresponding to the right hand side matrix is contained in $X^{\perp}$. Next, if we let $\vec{x} \in R^n$ such that $(I_m, 0_{m,n-m})US\vec{x}^T = \vec{0}$, then

$$\vec{x}SU^T \in \langle \vec{e}_{m+1}S, \ldots, \vec{e}_nS \rangle_R,$$

and so

$$\vec{x} \in \langle \vec{e}_{m+1}S(U^{-1})^TS^{-1}, \ldots, \vec{e}_nS(U^{-1})^TS^{-1} \rangle_R.$$

Hence, the equality holds. This implies that $X^{\perp}$ is a free submodule of rank $n-m$, and so

$$\operatorname{rank} X + \operatorname{rank} X^{\perp} = n,$$

as desired. □

Let $\mathcal{N}_0 = \{\vec{x} \in R^n \mid \|\vec{x}\| = 0\}$ and $\mathcal{NU} = \{\vec{x} \in R^n \mid \|\vec{x}\| \in R^{\times}\}$. An *orthogonal submodule* of R^n is a submodule of R^n in which $\beta(\vec{x}, \vec{y}) = 0$ for all $\vec{x}, \vec{y} \in R^n$ with $\vec{x} \neq \vec{y}$. Clearly, every vector in an orthogonal submodule has zero norm.

Lemma 3.4. *Let R be a finite local ring and let β be a non-degenerate symmetric bilinear form over R^n. If $S \subseteq R^n$ is a free unimodular orthogonal set, then there exist an orthogonal free submodule N of R^n and a subset $T \subseteq R^n \cap \mathcal{NU}$ such that $S \subseteq N \cup T$ and $|T| \leq n - 2\operatorname{rank} N$.*

Proof. Let $S \subseteq R^n$ be a free unimodular orthogonal set and suppose that $B \subseteq S$ is a basis of $\langle S \rangle_R$ whose elements have norm either 0 or a unit in R. Then we have $B = (B \cap \mathcal{N}_0) \cup (B \cap \mathcal{NU})$. Let $B' = B \cap \mathcal{N}_0$ and $B'' = B \cap \mathcal{NU}$. Now, let $N = \langle B' \rangle_R$ and $T = B''$. Since $B' \subseteq S$, we have $\beta(\vec{x}, \vec{y}) = 0$ for all $\vec{x}, \vec{y} \in B'$. Then N is an orthogonal free submodule of R^n. If $T = \emptyset$, then $B = B'$ and $S \subseteq N$. Moreover, $N \subseteq N^{\perp}$ and by Proposition 3.3, we have $\operatorname{rank} N + \operatorname{rank} N^{\perp} = n$ which implies $2\operatorname{rank} N \leq n$.

Now, assume that $T = B'' = \{\vec{w}_1, \vec{w}_2, \ldots, \vec{w}_k\}$ for some $k \geq 1$. We show that $S \subseteq N \cup T$. Let $\vec{u} \in S \setminus T$. Then $\vec{u}$ can be written as a linear combination of elements in B' and B''. This implies that there exist $\vec{v} \in N$ and $c_1, c_2, \ldots, c_k \in R$ such that

$$\vec{u} = \vec{v} + \sum_{i=1}^{k} c_i\vec{w}_i.$$

For each $r \in \{1, 2, \ldots, k\}$, we obtain

$$c_r\|\vec{w}_r\| = \beta(\vec{v}, \vec{w}_r) + \sum_{i=1}^{k} c_i\beta(\vec{w}_i, \vec{w}_r) = \beta(\vec{u}, \vec{w}_r) = 0.$$

Since $\|\vec{w}_r\| \in R^{\times}$, it follows that $c_r = 0$. As r is arbitrary, we have $\vec{u} \in N$. Hence, $S \subseteq N \cup T$. Additionally, we see that $N \subseteq (N \cup T)^{\perp} \subseteq S^{\perp}$, therefore, by Proposition 3.3,

$$\operatorname{rank} N \leq \operatorname{rank}\langle S \rangle_R^{\perp} = n - \operatorname{rank}\langle S \rangle_R = n - (k + \operatorname{rank} N).$$

This shows that $|T| = k \leq n - 2\operatorname{rank} N$ and the proof is complete. □

The following theorem is the main result of this paper.

Theorem 3.5. *Let R be a finite local ring of odd characteristic with the maximal ideal M. Suppose that β is a non-degenerate symmetric form of R^n. Then $\mathcal{S}(R^n)$ is equal to*

$$\begin{cases} |R|^{\frac{n-1}{2}} - |M|^{\frac{n-1}{2}} + 1, & \text{if } n \text{ is odd;} \\ |R|^{\frac{n}{2}} - |M|^{\frac{n}{2}}, & \text{if } n \text{ is even and } \beta \text{ takes the form } \Delta(\emptyset); \\ |R|^{\frac{n}{2}-1} - |M|^{\frac{n}{2}-1} + 2, & \text{if } n \text{ is even and } \beta \text{ takes the form } \Delta(z). \end{cases}$$

Proof. It remains only to show that $\mathcal{S}(R^n)$ is bounded above by the right-hand side of the equation. Let S be a free unimodular orthogonal set of R^n. By Lemma 3.4, $S \subseteq N \cup T$, where N is an orthogonal free submodule of R^n and T is a subset of R^n with

$$|T| \leq n - 2 \operatorname{rank} N.$$

Assume that $k = \operatorname{rank} N$. Then $k \leq \lfloor \frac{n}{2} \rfloor$ and

$$|S| \leq |R|^k - |M|^k + |T| \leq |R|^k - |M|^k + n - 2k$$

because every vector in S is unimodular. Note that the right-hand side of the above inequality is largest when k takes its maximum. Indeed, for $|R| = p^s, |M| = p^t$ with $s > t \geq 0$, if $f(x) = p^{sx} - p^{tx} + n - 2x$ for $x \in \mathbb{R}_{>1}$, then

$$\begin{aligned} f'(x) &= p^{sx} s \ln p - p^{tx} t \ln p - 2 \\ &= \ln p (p^{sx} s - p^{tx} t) - 2 \\ &> (p^{sx} s - p^{tx} t) - 2 && \text{because } p \geq 3 \\ &> s(p^{sx} - p^{tx}) - 2 && \text{because } s > t \\ &\geq 0, \end{aligned}$$

that is, f is increasing on the given domain. Thus,

$$|S| \leq |R|^{\lfloor \frac{n}{2} \rfloor} - |M|^{\lfloor \frac{n}{2} \rfloor} + n - 2 \left\lfloor \frac{n}{2} \right\rfloor,$$

and the first and second cases of the result hold. To complete the proof, we show that $k \leq \frac{n}{2} - 1$ for the last case. With this assumption, R^n possesses a basis such that the matrix of β is of the form

$$\begin{pmatrix} 0_\nu & I_\nu & & \\ I_\nu & 0_\nu & & \\ & & 1 & \\ & & & -z \end{pmatrix},$$

where I_ν and 0_ν denote the identity matrix and the zero matrix of size ν, respectively, the empty spaces represent zero entries. Here we write $n = 2\nu + 2$. From the notion in [10], the submodule N is a totally isotropic free submodule of $R^{2\nu+2}$. Thus, $\operatorname{rank} N \leq \nu = \frac{n}{2} - 1$, as desired. □

Example 3.6. Consider the orthogonal space $\mathbb{Z}_9^3$ with the form $\beta = \operatorname{diag}(1, -1, 1)$. According to Theorem 3.5, $\mathcal{S}(\mathbb{Z}_9^3) = 9^1 - 3^1 + 1 = 7$. The set of units of $\mathbb{Z}_9$ is $U = \{1, 2, 4, 5, 7, 8\}$. One example of a free unimodular orthogonal set with the cardinality 7 is given in the proof of Theorem 3.2, which is

$$S_1 = \{(u, u, 0) \mid u \in U\} \cup \{(0, 0, 1)\}.$$

We note that this is not the only such set. In fact, one can construct more families; for instance,

$$\begin{aligned} S_2 &= \{(u, -u, 0) \mid u \in U\} \cup \{(0, 0, 1)\} \text{ and} \\ S_3 &= \{(0, u, u) \mid u \in U\} \cup \{(1, 0, 0)\}. \end{aligned}$$

Now we discuss the result in the case of a finite commutative ring R of odd characteristic. As mentioned, $R = R_1 \oplus R_2 \oplus \cdots \oplus R_t$ is a finite direct sum of finite local rings of odd characteristic. Then a non-degenerate symmetric bilinear form β on R^n can be regarded as a finite direct sum of the forms on each R_i^n, as stated in Lemma 2.1. By Lemma 2.3, a unimodular vector in R^n is a finite sum of unimodular vectors from each R_i^n. Moreover,

if B is a basis of a submodule N of R^n with the property that each element of B has norm either 0 or a unit in R, then $N = \oplus_{i=1}^{t} N_i$ and $B = \oplus_{i=1}^{t} B_i$, where N_i is a submodule of R_i^n having a basis B_i with the same property as B. Thus, we have the following theorem.

Theorem 3.7. *Let $R = R_1 \oplus R_2 \oplus \cdots \oplus R_t$ be a finite direct sum of finite local rings of odd characteristic. Then*

$$\mathcal{S}(R^n) = \prod_{i=1}^{t} \mathcal{S}(R_i^n),$$

where each $\mathcal{S}(R_i^n)$ is obtained from Theorem 3.5.

4. Concluding remarks

The problem of determining the largest cardinality of a pairwise orthogonal subset in $\mathbb{F}_q^n$ was solved in [1, 13]. In Theorem 3.1, we address a similar problem for free unimodular orthogonal sets in R^2, where R is a finite local ring of odd characteristic, using an elementary counting approach based on properties of R. Extending this method to larger dimensions appears challenging, as the complexity of the equations increases substantially. However, by drawing on the approximation techniques of Ahmadi and Mohammadian [1] for the finite field case, we observe that a modified version of their approach can be adapted to our setting with adjustments to the definition of the sets under consideration. In future work, one might consider relaxing the definition of a free unimodular orthogonal set and investigating the largest possible size under this relaxed criterion.

Acknowledgements

This work was supported by Thammasat University Research Unit in Algebra and Its Applications.

References

[1] Ahmadi, O.; Mohammadian, A. Sets with many pairs of orthogonal vectors over finite fields. *Finite Fields Appl.* **37** (2016), 179–192.
[2] Bourgain, J.; Katz, N. H.; Tao, T. A sum-product estimate in finite fields, and applications. *Geom. Funct. Anal.* **14** (2004), no. 1, 27–57.
[3] Erdős, P. On sets of distances of n points. *Amer. Math. Monthly* **53** (1946), 248–250.
[4] Erdős, P. On some problems of elementary and combinatorial geometry. *Ann. Mat. Pura Appl.* **103** (1975), no. 4, 99–108.
[5] Iosevich, A. ; Rudnev, M. Erdős distance problem in vector spaces over finite fields. *Trans. Amer. Math. Soc.* **359** (2007), no. 12, 6127–6142.
[6] Iosevich, A.; Shparlinski, I. E.; Xiong, M. Sets with integral distances in finite fields. *Trans. Amer. Math. Soc.* **362** (2010), no. 4, 2189–2204.
[7] McDonald, B.R. *Finite Rings with Identity*. Marcel Dekker, New York, 1974.
[8] McDonald, B.R.; Hershberger, B. The orthogonal group over a full ring. *J. Algebra* **51** (1978), no. 2, 536–549.
[9] Meemark, Y.; Puirod, T. Symplectic graphs over finite local rings. *European J. Combin.* **34** (2013), no. 7, 1114–1124.
[10] Sirisuk, S.; Meemark, Y. Generalized symplectic graphs and generalized orthogonal graphs over finite commutative rings. *Linear Multilinear Algebra* **67** (2019), no. 12, 2427–2450.
[11] Sirisuk, S. Enumeration of some matrices and free linear codes over commutative finite local rings. *Spec. Matrices* **10** (2022), 109–116.
[12] Sriwongsa, S. Congruence of symmetric inner products over finite commutative rings of odd characteristic. *Bull. Aust. Math. Soc.* **96** (2017), no.3, 389–397.
[13] Vinh, L. A. Maximal sets of pairwise orthogonal vectors in finite fields. *Canad. Math. Bull.* **55** (2012), no. 2, 418–423.

[1] Department of Mathematics and Statistics, Faculty of Science and Technology, Thammasat University, and Thammasat University Research Unit in Algebra and Its Applications, Pathum Thani 12120, Thailand

Email address: siripong@mathstat.sci.tu.ac.th

[2] Department of Mathematics, Faculty of Science, King Mongkut's University of Technology Thonburi (KMUTT), 126 Pracha Uthit Rd., Bang Mod, Thung Khru, Bangkok 10140, Thailand

Email address: songpon.sri@kmutt.ac.th