AIMS Mathematics

https://www.aimspress.com/journal/Math

AIMS Mathematics, 9(10): 29333–29345.
DOI: 10.3934/math.20241421
Received: 09 August 2024
Revised: 16 September 2024
Accepted: 29 September 2024
Published: 16 October 2024

Research article

The binary codes generated from quadrics in projective spaces

Lijun Ma, Shuxia Liu and Zihong Tian*

School of Mathematical Sciences, Hebei Normal University, Shijiazhuang 050024, China

* **Correspondence:** Email: tianzh68@163.com.

Abstract: Quadrics are important in finite geometry and can be used to construct binary codes. In this paper, we first define an incidence matrix M based on points and non-degenerate quadrics in the classical projective space $\mathrm{PG}(n-1, q)$, where q is a prime power. As a consequence, we establish a binary code $C(M)$ with the generator matrix M and determine the dimension of $C(M)$ when q and n are both odd. In particular, we study the minimum distances of $C(M)$ and $C^{\perp}(M)$ in $\mathrm{PG}(2, q)$ and give their upper bounds.

Keywords: quadric; conic; binary code; generator matrix; dimension
Mathematics Subject Classification: 05B25, 15A03, 51E20, 94B05

1. Introduction

The linear codes arising from combinatorial structures of finite geometry have attracted much attention in recent years. Lavrauw, Storme, and Voorde [15, 16] studied the linear codes generated by the incidence matrices of points versus hyperplanes and points versus k-spaces. Leung and Xiang [18] discussed the dimensions of linear codes from unitals. Bonini and Borello [3], Bonini, Lia, and Timpanell [6], and Wu et al. [29] investigated minimal linear codes constructed from blocking sets, Hermitian varieties, and partial spreads, respectively. Some other combinatorial objects in finite geometry have also been used to construct linear codes; refer to [5, 8, 11, 21, 23, 24].

Quadrics are important in finite geometry and can be used to construct binary linear codes. Abdukhalikov and Ho [1] discussed the linear codes from quadrics. They constructed some families of linear complementary dual cyclic codes by using characterizations of elliptic quadrics described in polar coordinates. Several classes of p-ary linear codes with two or three weights were constructed from quadratic Bent functions over the finite field $\mathbb{F}_p$ by Zhou et al. [31], where p is an odd prime. Xie, Ouyang, and Mao [30] constructed two classes of linear codes with few weights from the quadratic forms and completely determined the weight distributions of these codes.

In $\mathrm{PG}(2, q)$, a non-degenerate quadric is also called a conic. Droms and Mellinger [9] studied some low-density parity-check binary codes arising from the incidence matrices based on the various classes of points and lines created by a given conic, calculated the dimensions and the minimum distances of the codes, and gave four conjectures of the dimensions with the help of computer software MAGMA. Then the aforementioned dimension conjectures were confirmed in [19], [25], and [28]. More binary codes related to conics refer to [2, 14, 20, 27].

In this paper, we will continue to study the binary linear codes arising from quadrics in projective spaces. Throughout this paper, we always assume that q is an odd prime power and n is odd. In Section 2, we introduce the basic theory of quadrics, linear codes, and projective spaces over finite fields, which will be needed in subsequent sections. In Section 3, we first define an incidence matrix M of all points and all non-degenerate quadrics in PG$(n-1, q)$ and establish a binary linear code $C(M)$ with the generator matrix M and its dual code $C^{\perp}(M)$. We determine that the dimension of the code $C(M)$ is $\theta_n - 1$ with $\theta_n = \frac{q^n-1}{q-1}$. In Section 4, we particularly discuss the minimum distances $d(C(M))$ and $d(C^{\perp}(M))$ in PG$(2, q)$, and give their upper bounds, i.e., $d(C(M)) \leq q^2(q^2-1)$ and $d(C^{\perp}(M)) \leq 2(q-1)$.

2. Preliminaries

In this section, we recall some basic theory of quadrics, linear codes, and projective spaces over finite fields. For a set A, define $A^* = A\backslash\{0\}$.

2.1. Quadrics over finite fields

Let $\mathbb{F}_q$ be a finite field with q elements and $\mathbb{F}_q^n$ be an n-dimensional vector space over $\mathbb{F}_q$.

Definition 2.1. *A quadratic form on $\mathbb{F}_q^n$ is a map $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ satisfying:*
(1) *$\varphi(ax) = a^2\varphi(x)$ for all $x \in \mathbb{F}_q^n$ and $a \in \mathbb{F}_q$*; (2) *$B_\varphi : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ defined by*

$$B_\varphi(x, y) = \varphi(x + y) - \varphi(x) - \varphi(y)$$

is a bilinear form.

The bilinear form B_φ is called the *polar form* of φ. Notice that B_φ is symmetric. A quadratic form is called *degenerate* if there exists some $x \in \mathbb{F}_q^{n*}$ such that $\varphi(x) = 0$ and $B_\varphi(x, y) = 0$ for any $y \in \mathbb{F}_q^n$, where $\mathbb{F}_q^{n*}$ is the set of all non-zero vectors in $\mathbb{F}_q^n$. Otherwise, it is called *non-degenerate*. See Reference [10, 13] for a more detailed description of quadratic forms.

PG$(n-1, q)$ is an $(n-1)$-dimensional projective space, whose $(k-1)$-dimensional subspaces for $1 \leq k \leq n$ are the k-dimensional subspaces of the n-dimensional vector space $\mathbb{F}_q^n$.

Definition 2.2. *Suppose φ is a quadratic form on $\mathbb{F}_q^n$. A quadric is the set of points in PG$(n-1, q)$ satisfying $\varphi(x) = 0$, where x is a point in PG$(n-1, q)$.*

A quadric is called non-degenerate if the quadratic form is non-degenerate. There are some results of non-degenerate quadrics as follows:

Lemma 2.3. *[13] In PG$(n-1, q)$, when n is odd,*
(1) *There are θ_{n-1} points in a non-degenerate quadric*;
(2) *The number of non-degenerate quadrics is*

$$\rho_n = q^{(n^2-1)/4} \prod_{i=1}^{(n-1)/2} (q^{2i+1} - 1).$$

2.2. *Linear codes*

An $[n,k,d]_q$-code C is a q-ary linear code with code length n, dimension k, and minimum distance d. When $q = 2$, it is a binary linear code, and q can be omitted. For a linear code C, $w(\mathbf{c})$ represents the Hamming weight of a codeword $\mathbf{c} \in C$, and $d(C)$ represents the minimum distance of C. As we all know, the minimum distance $d(C)$ is the minimum weight of codewords in a q-ary linear code C, i.e., $d(C) = \min\{w(\mathbf{c}) : \mathbf{0} \neq \mathbf{c} \in C\}$, and it also equals to the minimum number of linearly dependent column vectors in its parity-check matrix.

The dual code of C is denoted by $C^\perp$. If $C^\perp \subseteq C$, C is *self-orthogonal*; if $C^\perp = C$, C is *self-dual*. C and $C^\perp$ have the following relationships.

Lemma 2.4. *[12] Suppose C is a q-ary linear code. Then*
(1) $(C^\perp)^\perp = C$;
(2) *If G is the generator matrix of C, then G is the parity-check matrix of $C^\perp$;*
If H is the parity-check matrix of C, then H is the generator matrix of $C^\perp$.

Lemma 2.5. *[12] (Singleton Bound) If there exists an $[n,k,d]_q$-code C, then*

$$d \leq n - k + 1.$$

For an $[n,k,d]_q$-code C, if $d = n - k + 1$, then C is called a *maximum distance separable code*, or an *MDS code* for short.

2.3. *Descriptions of points and hyperplanes in PG$(n-1,q)$*

For the need of Section 3, we give a description of PG$(n-1,q)$. It is well known that $\mathbb{F}_{q^n}$ is isomorphic to $\mathbb{F}_q^n$ and could be regarded as an n-dimensional vector space over $\mathbb{F}_q$. So the points and hyperplanes of PG$(n-1,q)$ could be represented by the elements of the field $\mathbb{F}_{q^n}$. Please refer to [17] for details.

For any point of PG$(n-1,q)$, it could be represented by $x\mathbb{F}_q$, $x \in \mathbb{F}_{q^n}^*$. Let α be a primitive element of $\mathbb{F}_{q^n}$. Then

$$\mathbb{F}_{q^n}^*/\mathbb{F}_q^* = \langle \alpha\mathbb{F}_q^* \rangle \cong \mathbb{Z}_{\theta_n},$$

where $\theta_n = \frac{q^n-1}{q-1}$. Each coset $\alpha^i\mathbb{F}_q^*$ with 0 is a point of PG$(n-1,q)$, $0 \leq i \leq \theta_n - 1$. For convenience, let $P_i = \alpha^i\mathbb{F}_q$ for $0 \leq i \leq \theta_n - 1$. Then $\mathcal{P} = \{P_i \ : \ 0 \leq i \leq \theta_n - 1\}$ is the set of points in PG$(n-1,q)$.

Define a inner product over $\mathbb{F}_{q^n}$ as

$$(x,y) = Tr_{n/1}(xy), \ \forall x,y \in \mathbb{F}_{q^n},$$

where $Tr_{n/1}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{n-1}}$ is the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. Obviously, this inner product is non-degenerate. Let

$$N = \{x \in \mathbb{F}_{q^n} \ : \ Tr_{n/1}(x) = 0\}.$$

Then $N = \{\, x^q - x : x \in \mathbb{F}_{q^n}\}$, $|N| = q^{n-1}$, and N is an $(n-1)$-dimensional subspace over $\mathbb{F}_q$ of $\mathbb{F}_{q^n}$. For an arbitrary $x \in \mathbb{F}_{q^n}^*$, xN is an $(n-1)$-dimensional subspace of $\mathbb{F}_{q^n}$ and has the orthogonal complement $(xN)^\perp = \langle x^{-1} \rangle$, where $\langle x^{-1} \rangle$ is the 1-dimensional subspace generated by x^{-1}. Therefore, $xN = yN$ if and only if $xy^{-1} \in \mathbb{F}_q^*$ for any $x, y \in \mathbb{F}_{q^n}^*$. Thus, the number of these $(n-1)$-dimensional subspaces of $\mathbb{F}_{q^n}$ with the form xN is θ_n.

Let

$$\widetilde{N} = \{P_i = \alpha^i\mathbb{F}_q : \alpha^i \in N, 0 \le i \le \theta_n - 1\},$$

then $\widetilde{N}$ is the point set of $(n-1)$-dimensional subspace N and

$$\alpha^j\widetilde{N} = \{P_{[i+j]_{\theta_n}} : P_i \in \widetilde{N}, 0 \le i \le \theta_n - 1\},\ 0 \le j \le \theta_n - 1,$$

are the all hyperplanes of $\mathrm{PG}(n-1, q)$, where $[i+j]_{\theta_n} \equiv i + j (\bmod\ \theta_n)$. We denote $\alpha^j\widetilde{N}$ by $\mathcal{H}_j$ for short with $0 \le j \le \theta_n - 1$.

3. Binary linear codes arising from non-degenerate quadrics

In this section, we introduce the incidence matrix M constructed by points and non-degenerate quadrics in $\mathrm{PG}(n-1, q)$ and construct a binary linear code with the generator matrix M. Furthermore, we determine the dimension of the binary linear code.

Let $\mathcal{Q}$ be the set of all non-degenerate quadrics in $\mathrm{PG}(n-1, q)$. Here, we define an incidence matrix $M = (m_{ij})$ of points and non-degenerate quadrics in $\mathrm{PG}(n-1, q)$, the rows are indexed by the points and the columns are indexed by the non-degenerate quadrics, and with entry

$$m_{ij} = \begin{cases} 1 & P_i \in \mathcal{O}_j; \\ 0 & P_i \notin \mathcal{O}_j, \end{cases}$$

where $P_i \in \mathcal{P}$, $\mathcal{O}_j \in \mathcal{Q}$, $0 \le i \le \theta_n - 1$, $0 \le j \le \rho_n - 1$. Then M is a $\theta_n \times \rho_n$ matrix, where ρ_n is given in Lemma 2.3.

Theorem 3.1. *For the incidence matrix M defined above, we have*

(1) *The number of* $1'$*s in each column is* $c = \frac{q^{n-1}-1}{q-1}$;

(2) *The number of* $1'$*s in each row is* $r = q^{(n^2-1)/4}(q^{n-1} - 1)\prod_{i=1}^{(n-3)/2}(q^{2i+1} - 1)$.

Proof. The number c of $1'$s in each column of M is the number of points in a non-degenerate quadric, that is θ_{n-1} from Lemma 2.3. Since points are transitive under the action of the projective linear group $\mathrm{PGL}(n, q)$, the number r of $1'$s in each row of M is the same. So $r\theta_n = c\rho_n$, we can obtain $r = q^{(n^2-1)/4}(q^{n-1} - 1)\prod_{i=1}^{(n-3)/2}(q^{2i+1} - 1)$. □

We construct a linear code $C(M)$ spanned from the rows of M over $\mathbb{F}_2$, which is a binary code with the generator matrix M. From Reference [12], the dual code $C^{\perp}(M)$ of $C(M)$ is also a binary linear code, and the sum of dimensions of $C(M)$ and $C^{\perp}(M)$ is the code length.

3.1. The dimension of $C(M)$

In this subsection, we determine the dimension of $C(M)$ and give a class of MDS codes. Our results are obtained by representing non-degenerate quadrics in terms of the trace functions from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$.

Define

$$Q = \{x : Tr_{n/1}(x^{q+1}) = 0\}$$

and

$$\widetilde{Q} = \{P_i = \alpha^i\mathbb{F}_q : \alpha^i \in Q, 0 \le i \le \theta_n - 1\}.$$

Then $\widetilde{Q}$ is a subset of points in PG$(n-1, q)$.

Further, let

$$I = \{i : P_i \in \widetilde{N}\} = \{i : Tr_{n/1}(\alpha^i) = 0, 0 \le i \le \theta_n - 1\}$$

and

$$J = \{j : P_j \in \widetilde{Q}\} = \{j : Tr_{n/1}(\alpha^{j(q+1)}) = 0, 0 \le j \le \theta_n - 1\}$$

be the index set of $\widetilde{N}$ and $\widetilde{Q}$, respectively. Then I is a $(\theta_n, \theta_{n-1}, \theta_{n-2})$-difference set (see [22] for details).

Lemma 3.2. $I = (q+1)J$.

Proof. If $i \in J$, then $i(q+1) \in I$, so $(q+1)J \subseteq I$. Because $\gcd(q+1, \theta_n) = 1$ when n is odd, $|(q+1)J| = |J| = |I|$. Thus, we have $(q+1)J = I$. □

Lemma 3.3. *Suppose τ is a map of $\mathbb{F}_{q^n}$ to itself such that $\tau(x) = x^q + x^{q^{n-1}}$ for any $x \in \mathbb{F}_{q^n}$, then τ is an isomorphic map of $\mathbb{F}_{q^n}$.*

Proof. For $x \in \mathbb{F}_{q^n}$, if $x \in ker(\tau)$, then $x^{q^{n-1}} = -x^q$. We have $x^{2q^{n-1}} = x^{2q}$, so there is $x^2 = (x^2)^{q^2}$ after both sides of this equation are raised to the q power. Thus $x^2 \in \mathbb{F}_{q^2}$. When n is odd, $\mathbb{F}_{q^2} \cap \mathbb{F}_{q^n} = \mathbb{F}_q$, then $x^2 \in \mathbb{F}_q$. As q is odd,

$$x^{q^2} = (x^{2q})^{\frac{q-1}{2}} \cdot x^q = ((x^2)^q)^{\frac{q-1}{2}} \cdot x^q = (x^2)^{\frac{q-1}{2}} \cdot x^q = x^{2q-1} = x,$$

i.e., $x \in \mathbb{F}_{q^2}$. Therefore, $x \in \mathbb{F}_q$. Further, for any $x \in \mathbb{F}_q$, $\tau(x) = x^q + x^{q^{n-1}} = 2x$, and $\tau(x) = 0$ if and only if $x = 0$ when q is odd. Therefore, τ is an isomorphic map of $\mathbb{F}_{q^n}$. □

Theorem 3.4. *The point set $\widetilde{Q}$ is a non-degenerate quadric in PG$(n-1, q)$.*

Proof. We only need to prove that the map φ such that $\varphi(x) = Tr_{n/1}(x^{q+1})$ for any $x \in \mathbb{F}_{q^n}$ is a non-degenerate quadratic form.

On the one hand, for any $a \in \mathbb{F}_q$ and $x \in \mathbb{F}_{q^n}$,

$$\varphi(ax) = Tr_{n/1}(a^{q+1}x^{q+1}) = a^2 Tr_{n/1}(x^{q+1}) = a^2\varphi(x).$$

For any $x, y \in \mathbb{F}_{q^n}$, suppose

$$B_\varphi(x, y) = \varphi(x+y) - \varphi(x) - \varphi(y).$$

Then $B_\varphi(x, y) = Tr_{n/1}((x^q + y^q)(x+y) - x^{q+1} - y^{q+1}) = Tr_{n/1}(x^q y + y^q x)$. It is easy to verify that $B_\varphi(x, y)$ is a bilinear form. So φ is a quadratic form.

On the other hand, suppose φ is degenerate, then there exists $x \in \mathbb{F}^*_{q^n}$ such that $\varphi(x) = 0$ and $B_\varphi(x, y) = 0$ for any $y \in \mathbb{F}_{q^n}$. Further,

$$B_\varphi(x, y) = Tr_{n/1}(x^q y + y^q x) = Tr_{n/1}(xy^{q^{n-1}} + y^q x) = Tr_{n/1}(x(y^q + y^{q^{n-1}})).$$

We know that $x(y^q + y^{q^{n-1}})$ runs through all the elements of $\mathbb{F}_{q^n}$ when y runs through all the elements of $\mathbb{F}_{q^n}$ from Lemma 3.3. So $B_\varphi(x, y)$ is not always 0, which contradicts the hypothesis.

Thus, φ is a non-degenerate quadratic form, and $\widetilde{Q}$ is a non-degenerate quadric. □

Let α be a primitive element of $\mathbb{F}_{q^n}$. α could define a linear transformation σ from $\mathbb{F}_{q^n}$ to itself by $\sigma(x) = \alpha x$ for any $x \in \mathbb{F}_{q^n}$. Define

$$\mathcal{O}_i = \alpha^i \widetilde{Q} = \{P_{[i+j]_{\theta_n}} : P_j \in \widetilde{Q}, 0 \leq j \leq \theta_n - 1\},\ 0 \leq i \leq \theta_n - 1.$$

Obviously, $\mathcal{O}_i$ is also a non-degenerate quadric in $\mathrm{PG}(n-1, q)$. For convenience, we call $\mathcal{O}_i$ a linear non-degenerate quadric in $\mathrm{PG}(n-1, q)$, or l-quadric for short, where $0 \leq i \leq \theta_n - 1$.

In particular, when $n = 2$, the set of l-quadrics (or l-conics) is a projective bundle introduced in [4]. Recently, Bariffi et al. [7] constructed new moderate-density parity-check codes from projective bundles and studied the relevant parameters.

In the following, we define an incidence matrix $M_1 = (m_{ij})$ of points and l-quadrics in $\mathrm{PG}(n-1, q)$, the ith row is indexed by P_i, the jth column is indexed by $\mathcal{O}_j$, and with entry

$$m_{ij} = \begin{cases} 1 & \text{if } P_i \in \mathcal{O}_j; \\ 0 & \text{if } P_i \notin \mathcal{O}_j, \end{cases}$$

where $0 \leq i, j \leq \theta_n - 1$. Then M_1 is a cyclic sub-matrix of M, and the numbers of $1'$s in each column and each row are both θ_{n-1}. Denote the binary code generated by the rows of M_1 by $C(M_1)$.

Lemma 3.5. $|\mathcal{O}_i \cap \mathcal{O}_j| = |\mathcal{H}_i \cap \mathcal{H}_j| = \theta_{n-2}$ *with* $0 \leq i, j \leq \theta_n - 1$*,* $i \neq j$*.*

Proof. Obviously, the index sets of $\mathcal{O}_i$ and $\mathcal{H}_i$ are $i + I$ and $i + J$, respectively, $0 \leq i \leq \theta_n - 1$. So

$$|\mathcal{O}_i \cap \mathcal{O}_j| = |(i + I) \cap (j + I)|,\ |\mathcal{H}_i \cap \mathcal{H}_j| = |(i + J) \cap (j + J)|,$$

where $i + I = \{i + t : t \in I\}$. From Lemma 3.2,

$$|\mathcal{O}_i \cap \mathcal{O}_j| = |(i + (q + 1)J) \cap (j + (q + 1)J)| = |(i + J) \cap (j + J)|.$$

That is $|\mathcal{O}_i \cap \mathcal{O}_j| = |\mathcal{H}_i \cap \mathcal{H}_j|$. Because $\mathcal{H}_i$ is a hyperplane of $\mathrm{PG}(n-1, q)$ for $0 \leq i \leq \theta_n - 1$, $\mathcal{H}_i \cap \mathcal{H}_j$ is an $(n-3)$-dimensional subspace of $\mathrm{PG}(n-1, q)$ for $i \neq j$. Then $|\mathcal{O}_i \cap \mathcal{O}_j| = |\mathcal{H}_i \cap \mathcal{H}_j| = \theta_{n-2}$. □

Theorem 3.6. *$C(M_1)$ is an MDS code with parameters* $[\theta_n, \theta_n - 1, 2]$*.*

Proof. Obviously, the length of $C(M_1)$ is θ_n, and the dimension of $C(M_1)$ is the 2-rank of M_1. From Theorem 3.1 and Lemma 3.5, due to $\theta_{n-1} \equiv 0 (\mathrm{mod}\ 2)$ and $\theta_{n-2} \equiv 1 (\mathrm{mod}\ 2)$ when n is odd, we have

$$M_1^T M_1 = \begin{pmatrix} 0 & 1 & \dots & 1 \\ 1 & 0 & \dots & 1 \\ \vdots & \vdots & & \vdots \\ 1 & 1 & \dots & 0 \end{pmatrix},$$

which is an alternating matrix and $rank_2(M_1^T M_1) = \theta_n - 1$. Then $rank_2(M_1) \geq \theta_n - 1$. On the other hand, the sum of all the row vectors of M_1 is the zero vector, then $rank_2(M_1) \leq \theta_n - 1$. Thus $rank_2(M_1) = \theta_n - 1$, that is the dimension of $C(M_1)$.

From the Singleton bound in Lemma 2.5, the minimum distance $d(C(M_1)) \leq 2$. Because the weight of the sum of any two codewords with even weights is also even, then the weights of codewords in $C(M_1)$ are always even. So $d(C(M_1)) = 2$. Thus $C(M_1)$ is a $[\theta_n, \theta_n - 1, 2]$-code, and it is an MDS code. □

Theorem 3.7. *The dimension of* $C(M)$ *is* $\theta_n - 1$.

Proof. The dimension of $C(M)$ is the 2-rank of M. M_1 is a sub-matrix of M, so $rank_2(M) \geq rank_2(M_1) \geq \theta_n - 1$. On the other hand, the sum of all the row vectors of M is also the zero vector, so $rank_2(M) \leq \theta_n - 1$. Thus $rank_2(M) = \theta_n - 1$. □

From the relationship between the dimension of C and the dimension of $C^{\perp}$, we have the following result.

Corollary 3.8. *The dimension of* $C^{\perp}(M)$ *is* $\rho_n - \theta_n + 1$.

3.2. The minimum distance of $C(M)$

In this subsection, we give a range of the minimum distance of $C(M)$ by analyzing the structure of M. Let group G be $\langle \alpha F_q^* \rangle$. For any non-degenerate quadric O, denote its orbit by $\overline{O}$ under the action of G.

Theorem 3.9. *For any non-degenerate quadric* O, $\left|\overline{O}\right| = \theta_n$.

Proof. Suppose G_0 is the stabilizer of O and $|G_0| = s$, then $\left|\overline{O}\right| = |G|/|G_0| = \theta_n/s$. Because the number of $1'$s in each column is θ_{n-1}, then $s|\theta_{n-1}$. Thus $s|\gcd(\theta_{n-1}, \theta_n)$. Due to

$$\gcd(\theta_{n-1}, \theta_n) = \gcd(\theta_{n-1}, \theta_n - \theta_{n-1}) = \gcd(\theta_{n-1}, q^{n-1}) = 1,$$

we have $s = 1$ and $\left|\overline{O}\right| = \theta_n$. □

From Theorem 3.9, we know that the matrix M can be divided into $\rho_n/\theta_n = q^{(n^2-1)/4}(q - 1)\prod_{i=1}^{(n-3)/2}(q^{2i+1} - 1)$ cyclic matrices, then $C(M)$ has a natural quasi-cyclic structure.

Theorem 3.10. $2\rho_n/\theta_n \leq d(C(M)) \leq \theta_{n-1}\rho_n/\theta_n$.

Proof. For any cyclic sub-matrix M' of M, it is not difficult to see that the minimum distance of the binary code generated by the rows of M' is at least 2, then $d(C(M)) \geq 2\rho_n/\theta_n$. Take a row of M; the weight of the corresponding codeword of $C(M)$ is $\theta_{n-1}\rho_n/\theta_n$ from Theorem 3.1, so $d(C(M)) \leq \theta_{n-1}\rho_n/\theta_n$. □

4. Binary linear codes arising from conics in PG$(2, q)$

A non-degenerate quadric is a conic in PG$(2, q)$. The matrix M defined in Section 3 is an incidence matrix of points and conics, and M is a $(q^2 + q + 1) \times q^2(q^3 - 1)$ matrix. In this section, we continue to study the binary codes from the matrix M and give smaller upper bounds of the minimum distances of $C(M)$ and $C^{\perp}(M)$ in PG$(2, q)$.

For convenience, we use vectors to represent points in PG$(2, q)$. When q is an odd prime power, the equation of a conic in PG$(2, q)$ can be represented by

$$XAX^T = 0,$$

where $X = (x, y, z)$ is a point, $A \in \mathbb{F}_q^{3\times3}$, $A = A^T$ and $|A| \neq 0$. So, we could represent a conic with the corresponding non-degenerate symmetric matrix. From Chapter 2 of [26], the equation of a conic can be carried by a projective transformation into the normal form $x^2 + yz = 0$ in PG$(2, q)$.

Theorem 4.1. *For the incidence matrix M defined above, we have*

(1) *The number of* $1'$*s in each column is* $c = q + 1$;

(2) *The number of* $1'$*s in each row is* $r = q^2(q^2 - 1)$;

(3) *The number of* $1'$*s in the same entries of any two rows is* $\lambda = q^2(q - 1)$.

Proof. From Theorem 3.1, we have (1) and (2). For (3), because any two different points could determine a unique line in $\mathrm{PG}(2, q)$ and $\mathrm{PGL}_3(\mathbb{F}_q)$ is transitive on the set of lines in $\mathrm{PG}(2, q)$, we can take two points $P_1 = (1, 0, 0)$ and $P_2 = (0, 1, 0)$. Let O_2 be a conic containing both points, and its corresponding symmetric matrix be

$$A = \begin{pmatrix} a & d & e \\ d & b & f \\ e & f & c \end{pmatrix}.$$

From $P_1, P_2 \in O_2$, we have $a = 0$ and $b = 0$, and the number of non-degenerate symmetric matrices satisfying these two conditions is $q^2(q-1)^2$. So, there are $q^2(q-1)$ conics containing any two different points, that is, the number of $1'$s in the same entries of any two rows. □

Theorem 4.2. *$C^{\perp}(M)$ is a self-orthogonal code.*

Proof. By Lemma 2.4 (1), $C^{\perp}(M)$ is a self-orthogonal code if and only if $C(M) \subseteq C^{\perp}(M)$. Take a codeword $\mathbf{v} \in C(M)$, for any codeword $\mathbf{c} \in C(M)$ ($\mathbf{v}$=$\mathbf{c}$ is possible), the number of $1'$s appearing in the same position of $\mathbf{v}$ and $\mathbf{c}$ is always even by Theorem 4.1. So $(\mathbf{v}, \mathbf{c}) = 0$, i.e., $\mathbf{v} \in C^{\perp}(M)$. Thus $C(M) \subseteq C^{\perp}(M)$, and $C^{\perp}(M)$ is a self-orthogonal code. □

From Theorem 3.7, we can obtain the dimension of $C(M)$ is $q^2 + q$. Hamming weights and parity-check matrices are usually applied to study the minimum distances of linear codes. Here, we use them to consider the minimum distances of $C(M)$ and $C^{\perp}(M)$.

For the rows of M corresponding to any m ($\leq q + 1$) collinear points, any two rows have $q^2(q - 1)$ $1'$s in the same entries, and any three rows have no 1 in the same entry by the properties of conics.

Lemma 4.3. *The weight of the sum of the codewords from row vectors of M corresponding to any m ($\leq q + 1$) collinear points is $mq^2(q - 1)(q - m + 2)$. Furthermore, there is*

$$q^2(q^2 - 1) \leq mq^2(q - 1)(q - m + 2) \leq \frac{1}{4}q^2(q^2 - 1)(q + 3).$$

Proof. Because there is no conic containing any three collinear points, the weight of the sum of the codewords corresponding to these m collinear points is $mr - m(m - 1)\lambda = mq^2(q - 1)(q - m + 2)$. This is a quadratic polynomial on the variate m; its lower bound is $q^2(q^2 - 1)$ and its upper bound is $\frac{1}{4}q^2(q^2 - 1)(q + 3)$ with $m = \frac{q+1}{2}$. □

Lemma 4.4. *There exist some codewords of $C(M)$ with weights*

$$(3q^2 + 4)(q - 1)^2, \;\; 4q^4 - 12q^3 + 24q^2 - 40q + 32, \;\; 4(q - 1)(q^3 - 2q^2 + 3q - 3).$$

Proof. The codewords of $C(M)$ are the linear combinations of the row vectors of M. We discuss the weights of the codewords in Theorem 4.1. Consider any m row vectors of M corresponding to m collinear points; the weights are given in Lemma 4.3.

Consider any three row vectors of M corresponding to non-collinear points; let C_1 be the set of conics containing these three points. By a calculation similar to Theorem 4.1, we have $|C_1| = (q-1)^2$, then there exists a codeword with weight $3(r-2\lambda)+4|C_1| = (3q^2+4)(q-1)^2$.

Consider any four row vectors of M corresponding to non-collinear points. If any three of them are non-collinear, the number of conics containing these four points is $q-2$. Applying the Exclusion Principle, there exists a codeword with weight $4r-12\lambda+16|C_1|-8(q-2) = 4q^4-12q^3+24q^2-40q+32$. If there are exactly three of them collinear, there is no conic containing these four points, and there exists a codeword with weight $4r-12\lambda+12|C_1| = 4(q-1)(q^3-2q^2+3q-3)$. □

Theorem 4.5. *$d(C(M)) \leq q^2(q^2-1)$.*

Proof. From Lemma 4.3, when $m=1$, there is $d(C(M)) \leq q^2(q^2-1)$. □

Using the software package MAGMA, we have known that the minimum distances of $C(M)$ are $72, 600$ for $q = 3, 5$, respectively. Therefore, we think that the bound of $d(C(M))$ is maybe tight.

To calculate the minimum distance of $C^{\perp}(M)$, let us first list all the points in PG$(2,q)$. Suppose that β is a primitive element of $\mathbb{F}_q$. Let

$$S_1 = \{(1,\beta^i,\beta^{i+j}) : 0 \leq i, j \leq q-2\};$$

$$S_2 = \{(1,\beta^j,0),(1,0,\beta^j),(0,1,\beta^j) : 0 \leq j \leq q-2\},$$

then the set of points in PG$(2,q)$ is $S_1 \cup S_2 \cup \{e_1,e_2,e_3\}$, where $e_1 = (1,0,0), e_2 = (0,1,0), e_3 = (0,0,1)$. For any point P in PG$(2,q)$, which is different from e_1,e_2,e_3, then any three distinct points in the set $\{P,e_1,e_2,e_3\}$ are not collinear if and only if $P \in S_1$.

Theorem 4.6. *$d(C^{\perp}(M)) \leq 2(q-1)$.*

Proof. We first separate the points of S_2 into three parts and choose the conics as follows:

$$R_{12} = \{(1,\beta^j,0) : 0 \leq j \leq q-2\};$$

$$R_{13} = \{(1,0,\beta^j) : 0 \leq j \leq q-2\};$$

$$R_{23} = \{(0,1,\beta^j) : 0 \leq j \leq q-2\},$$

and

$$Q_{12} = \{x^2-\beta z^2-\beta^{-u}xy = 0 : 0 \leq u \leq q-2\};$$

$$Q'_{12} = \{y^2-\beta z^2-\beta^{u}xy = 0 : 0 \leq u \leq q-2\}.$$

Then $R_{12} \cup R_{13} \cup R_{23} = S_2$. By calculation, we find that the points in the conic $x^2-\beta z^2-\beta^{-u}xy = 0$ ($\in Q_{12}$) are

$$e_2, (1,\beta^u,0), (1,\beta^u(1-\beta^{2j+1}),\beta^j),\ 0 \leq j \leq q-2.$$

Because q is odd, $(q-1) \nmid (2j+1)$. Then the points $(1,\beta^u(1-\beta^{2j+1}),\beta^j)$, $0 \leq j \leq q-2$, are in S_1. Similarly, the conic $y^2-\beta z^2-\beta^u xy = 0$ ($\in Q'_{12}$) consists of $e_1, (1,\beta^u,0)$ and $q-1$ points in S_1. For convenience, we denote the sub-matrices of M with rows indexed by the points of S_1 and columns indexed by the conics of Q_{12} and Q'_{12} by Q_1 and Q'_1, respectively. We take a sub-matrix M' of M, whose rows are indexed by $S_1, R_{12}, R_{13}, R_{23}, e_1, e_2, e_3$ and columns are indexed by Q_{12}, Q'_{12}. In particular, the points in R_{12} are arranged in the order:

$$(1,1,0),(1,\beta,0),\ldots,(1,\beta^{q-2},0),$$

and the conics are arranged in the order:

$$f_0, f_1, \ldots, f_{q-2};\ g_0, g_1, \ldots, g_{q-2},$$

where f_u is the conic $x^2-\beta z^2-\beta^{-u}xy=0$, g_u is $y^2-\beta z^2-\beta^{u}xy=0, 0\le u\le q-2$. Then

$$M' = \begin{array}{c} \\ S_1 \\ R_{12} \\ R_{13} \\ R_{23} \\ e_1 \\ e_2 \\ e_3 \end{array}\!\!\begin{array}{c} \begin{array}{cc} Q_{12} & Q'_{12} \end{array} \\ \begin{pmatrix} Q_1 & Q'_1 \\ E_{q-1} & E_{q-1} \\ 0 & 0 \\ 0 & 0 \\ 0 & J \\ J & 0 \\ 0 & 0 \end{pmatrix} \end{array},$$

where E_{q-1} is the identity matrix, and J is the matrix with every entry equal to 1.

For the minimum distance of $C^{\perp}(M)$, we consider the columns of M corresponding to the submatrices Q_1 and Q'_1. For Q_1, a point $(1,\beta^i,\beta^{i+j})$ is contained in a conic $x^2-\beta z^2-\beta^{-u}xy=0$ of Q_{12} if and only if $\beta^u(1-\beta^{2i+2j+1})-\beta^i=0$, where $0\le i,j,u\le q-2$. Notice that $q-1$ is even, then $(q-1)\nmid(2i+2j+1)$, and u is uniquely determined by the point $(1,\beta^i,\beta^{i+j})$. The number of $1'$s in each row of Q_1 is 1. Similar to Q_1, the number of $1'$s in each row of Q'_1 is also 1. Therefore, the columns of M corresponding to Q_1 and Q'_1 are linearly dependent. By Lemma 2.4 (2), $d(C^{\perp}(M))\le 2(q-1)$. □

5. Conclusions

In recent years, some combinatorial objects in finite geometry have been used to construct linear codes, such as hyperplanes, quadrics, conics, unitals, and so on. These linear codes have very good structure and properties. In particular, some parameters of these linear codes, including dimensions, minimum distances, weights, etc., are studied emphatically. In this paper, we first define an incidence matrix M arising from points and non-degenerate quadrics in PG$(n-1,q)$ when q is an odd prime power and n is odd. As a consequence, we establish a new binary linear code $C(M)$ with the generator matrix M, and completely determine the dimension of $C(M)$. Furthermore, we study the minimum distances of $C(M)$ and $C^{\perp}(M)$ in PG$(2,q)$, and give their upper bounds. Some linear codes arising from quadrics or conics in finite geometry are summarized in Table 1.

To conclude, we list here some of the possible developments of our results.

1) For the minimum distances of $C(M)$ and $C^{\perp}(M)$ in PG$(2,q)$, the exact values need further proofs.

2) It is an interesting problem to determine the parameters of $C(M)$ and $C^{\perp}(M)$ when q is an even prime power or n is even.

Table 1. Some linear codes arising from quadrics or conics in finite geometry.

Code length	Dimension	Minimum distance d	Reference	Geometric objects
q^2+1	4	q^2-q	[1]	Elliptic quadric
q^n	$n+2$	$2\|r$: $\min\{q^n-q^{n-1}-\varepsilon_Q q^{\frac{2n-r-2}{2}}(q-1),$ $q^n-q^{n-1}+\varepsilon_Q q^{\frac{2n-r-2}{2}}\},\varepsilon_Q=1$ or -1; $r\geq 3$ is odd: $q^n-q^{n-1}-q^{\frac{2n-r-1}{2}}$. $(*)$	[30]	Quadrics
q^n-1	$n+1$	The same as $(*)$		
$\frac{q^2+q}{2}$	$\frac{q^2-q}{2}$	3	[9]	Conics
q^2	$\frac{q^2+q}{2}$	$\frac{q+1}{2}\leq d\leq q-1$		
q^2+q+1	$\frac{q^2+q+2}{2}$	$\frac{q+1}{2}\leq d\leq q+1$		
q^2	$\frac{q^2-q}{2}$	$\frac{q+1}{2}\leq d\leq q+1,\ q\neq 3^t$		
$\frac{q^2-q}{2}$	$\frac{(q-1)^2}{4}$	$\frac{q+3}{2}\leq d\leq q-1$	[9,19]	
$\frac{q^2+q}{2}$	$q\equiv 1(\mathrm{mod}\ 4)$: $\frac{q^2-2q+5}{4}$ $q\equiv 3(\mathrm{mod}\ 4)$: $\frac{q^2-2q-3}{4}$	$\frac{q+1}{2}\leq d\leq q+1$, $q\neq 3^t$, 3 is non-square	[9,25]	
$\frac{q^2+q}{2}$	$q\equiv 1(\mathrm{mod}\ 4)$: $\frac{q^2-1}{4}$ $q\equiv 3(\mathrm{mod}\ 4)$: $\frac{q^2+3}{4}$	$\frac{q+1}{2}\leq d\leq q-1$	[9,28]	
$\frac{q^2-q}{2}$	$q\equiv 1(\mathrm{mod}\ 4)$: $\frac{q^2-4q-1}{4}$ $q\equiv 3(\mathrm{mod}\ 4)$: $\frac{q^2-4q+3}{4}$	$\frac{q+3}{2}\leq d\leq q+1$, $q\neq 3^t$, 3 is square		
$\frac{q^2-q}{2}$	$q\equiv 1(\mathrm{mod}\ 4)$: $\frac{q^2-1}{4}$ $q\equiv 3(\mathrm{mod}\ 4)$: $\frac{q^2+3}{4}$	\	[27]	
$\rho_n=$ $q^{\frac{n^2-1}{4}}\prod_{i=1}^{\frac{n-1}{2}}(q^{2i+1}-1)$	$\theta_n-1=$ $\frac{q^n-1}{q-1}-1$	$2\rho_n/\theta_n\leq d\leq\theta_{n-1}\rho_n/\theta_n$	Our paper	Quadrics

Author contributions

Lijun Ma, Shuxia Liu, Zihong Tian: Conceptualization, Methodology, Validation, Writing-original draft, Writing-review and editing. All authors have read and approved the final version of the manuscript for publication.

Acknowledgments

The authors wish to thank the referees for the hard work and the constructive comments. The work was supported by National Natural Science Foundation of China under Grant Numbers 12171139 and 11871019.

Conflict of interest

The authors state that there is no competing interest.

References

1. K. Abdukhalikov, D. Ho, Linear codes from arcs and quadrics, *Des. Codes Cryptogr.*, 2023. https://doi.org/10.1007/s10623-023-01255-z

2. M. Adams, J. H. Wu, 2-Ranks of incidence matrices associated with conics in finite projective planes, *Des. Codes Cryptogr.*, **72** (2014), 381–404. https://doi.org/10.1007/s10623-012-9772-5

3. M. Bonini, M. Borello, Minimal linear codes arising from blocking sets, *J. Algebr. Comb.*, **53** (2021), 327–341. https://doi.org/10.1007/s10801-019-00930-6

4. R. D. Baker, J. M. N. Brown, G. L. Ebert, J. C. Fisher, Projective bundles, *Bull. Belg. Math. Soc.*, **3** (1994), 329–336. https://doi.org/10.36045/bbms/1103408578

5. B. Bagchi, S. P. Inamdar, Projective geometric codes, *J. Combin. Theory Ser. A*, **99** (2002), 128–142. https://doi.org/10.1006/jcta.2002.3265

6. M. Bonini, S. Lia, M. Timpanella, Minimal linear codes from Hermitian varieties and quadrics, *Appl. Algebra Engrg. Comm. Comput.*, **34** (2023), 201–210. https://doi.org/10.1007/s00200-021-00500-z

7. J. Bariffi, S. Mattheus, A. Neri, J. Rosenthal, Moderate-density parity-check codes from projective bundles, *Des. Codes Cryptogr.*, **90** (2022), 2943–2966. https://doi.org/10.1007/s10623-022-01054-y

8. P. V. Ceccherini, J. W. P. Hirschfeld, The dimension of projective geometry codes, *Discrete Math.*, **106–107** (1992), 117–126. https://doi.org/10.1016/0012-365X(92)90538-Q

9. S. V. Droms, K. E. Mellinger, C. Meyer, LDPC codes generated by conics in the classical projective plane, *Des. Codes Cryptogr.*, **40** (2006), 343–356. https://doi.org/10.1007/s10623-006-0022-6

10. R. Elman, N. Karpenko, A. Merkurjev, *The algebraic and geometric theory of quadratic forms*, AMS Colloquium Publishing, 2008. https://doi.org/10.1090/coll2F056

11. V. Fack, S. L. Fancsali, L. Storme, G. Van de Voorde, J. Winne, Small weight codewords in the codes arising from Desarguesian projective planes, *Des. Codes Cryptogr.*, **46** (2008), 25–43. https://doi.org/10.1007/s10623-007-9126-x

12. K. Q. Feng, *Algebraic theory of error-correcting codes (Chinese)*, Beijing: Tsinghua University Press, 2005.

13. J. W. P. Hirschfeld, J. A. Thas, General Galois Geometries, London: Springer-Verlag, 2016. https://doi.org/10.1007/978-1-4471-6790-7

14. Z. L. Heng, C. S. Ding, The subfield codes of hyperoval and conic codes, *Finite Fields Appl.*, **56** (2019), 308–331. https://doi.org/10.1016/j.ffa.2018.12.006

15. M. Lavrauw, L. Storme, G. Van de Voorde, On the code generated by the incidence matrix of points and hyperplanes in $\mathrm{PG}(n,q)$ and its dual, *Des. Codes Cryptogr.*, **48** (2008), 231–245. https://doi.org/10.1007/s10623-008-9203-9

16. M. Lavrauw, L. Storme, G. Van de Voorde, On the code generated by the incidence matrix of points and k-spaces in $\mathrm{PG}(n,q)$ and its dual, *Finite Fields Appl.*, **14** (2008), 1020–1038. https://doi.org/10.1016/j.ffa.2008.06.002

17. S. Liu, C. Zhang, G. Meng, M. Wang, The subspace representations of finite field and its applications, *J. Math. Res. Expo.*, **28** (2008), 1021–1026.

18. K. H. Leung, Q. Xing, On the dimensions of the binary codes of a class of unitals, *Discrete Math.*, **309** (2009), 570–575. https://doi.org/10.1016/j.disc.2008.08.004

19. A. L. Madison, J. H. Wu, On binary codes from conics in PG$(2, q)$, *European J. Combin.*, **33** (2012), 33–48. https://doi.org/10.1016/j.ejc.2011.08.001

20. A. L. Madison, J. H. Wu, Conics arising from external points and their binary codes, *Des. Codes Cryptogr.*, **78** (2016), 473–491. https://doi.org/10.1007/s10623-014-0013-y

21. O. Polverino, F. Zullo, Codes arising from incidence matrices of points and hyperplanes in PG(n, q), *J. Combin. Theory Ser. A*, **158** (2018), 1–11. https://doi.org/10.1016/j.jcta.2018.03.013

22. H. Shen, *Theory of combinatorial design (Chinese)*, Shanghai: Shanghai Jiaotong University Press, 2008.

23. P. Sin, J. Sorci, Q. Xiang, Linear representations of finite geometries and associated LDPC codes, *J. Combin. Theory Ser. A*, **173** (2020), 105238. https://doi.org/10.1016/j.jcta.2020.105238

24. P. Sin, Q. Xiang, On the dimensions of certain LDPC codes based on q-regular bipartite graphs, *IEEE Trans. Inform. Theory*, **52** (2006), 3735–3737. https://ieeexplore.ieee.org/document/1661850

25. P. Sin, J. Wu, Q. Xiang, Dimensions of some binary codes aring from a conic in PG$(2, q)$, *J. Combin. Theory Ser. A*, **118** (2011), 853–878. https://doi.org/10.1016/j.jcta.2010.11.010

26. Z. X. Wan, *Geometry of classical groups over finite fields*, Beijing-New York: Science Press, 2002.

27. J. H. Wu, Conics arising from internal points and their binary codes, *Linear Algebra Appl.*, **439** (2013), 422–434. https://doi.org/10.1016/j.laa.2013.04.004

28. J. H. Wu, Proofs of two conjectures on the dimensions of binary codes, *Des. Codes Cryptogr.*, **70** (2014), 273–304. https://doi.org/10.1007/s10623-012-9682-6

29. X. Wu, W. Lu, X. W. Cao, G. J. Luo, Minimal linear codes constructed from partial spreads, *Cryptogr. Commun.*, **16** (2024), 601–611. https://doi.org/10.1007/s12095-023-00689-5

30. X. H. Xie, Y. Ouyang, M. Mao, Vectorial bent functions and linear codes from quadratic forms, *Cryptogr. Commun.*, **15** (2023), 1011–1029. https://doi.org/10.1007/s12095-023-00664-0

31. Z. C. Zhou, N. Li, C. L. Fan, T. Helleseth, Linear codes with two or three weights from quadratic bent functions, *Des. Codes Cryptogr.*, **81** (2016), 283–295. https://doi.org/10.1007/s10623-015-0144-9