Pairs of quadratic forms over finite fields

Alexander Pott
Faculty of Mathematics
Otto-von-Guericke University
Magdeburg, Germany
alexander.pott@ovgu.de

Kai-Uwe Schmidt
Department of Mathematics
Paderborn University
Paderborn, Germany
kus@math.upb.de

Yue Zhou[*]
Department of Mathematics and System Sciences
National University of Defense Technology
Changsha, China

Department of Mathematics
Augsburg University
Augsburg, Germany
yue.zhou.ovgu@gmail.com

Submitted: Jan 30, 2014; Accepted: Mar 29, 2016; Published: Apr 15, 2016
Mathematics Subject Classifications: 05E15, 05E30, 06E30

Abstract

Let $\mathbb{F}_q$ be a finite field with q elements and let X be a set of matrices over $\mathbb{F}_q$. The main results of this paper are explicit expressions for the number of pairs (A, B) of matrices in X such that A has rank r, B has rank s, and $A + B$ has rank k in the cases that (i) X is the set of alternating matrices over $\mathbb{F}_q$ and (ii) X is the set of symmetric matrices over $\mathbb{F}_q$ for odd q. Our motivation to study these sets comes from their relationships to quadratic forms. As one application, we obtain the number of quadratic Boolean functions that are simultaneously bent and negabent, which solves a problem due to Parker and Pott.

1 Introduction

Let $\mathbb{F}_q$ be a finite field with q elements. Let X be a set of matrices of the same size over $\mathbb{F}_q$ and let X_k contain all matrices in X of rank k. Define

$$N_X(r,s,k) = \left|\{(A,B) \in X_r \times X_s :\ A+B \in X_k\}\right|, \tag{1}$$

[*]Yue Zhou is partially supported by the National Natural Science Foundation of China (No. 11401579).

which is the number of pairs (A, B) of matrices in X such that A has rank r, B has rank s, and $A + B$ has rank k. We are interested in the numbers $N_X(r, s, k)$ when X is the set of $m \times m$ alternating matrices over $\mathbb{F}_q$ and when X is the set of $m \times m$ symmetric matrices over $\mathbb{F}_q$ (recall that a matrix is *alternating* if it is skew-symmetric and its diagonal contains only zeros). Our motivation to study these sets comes from their relationships to quadratic forms over finite fields. Some consequences of our results for quadratic forms are discussed later in this section.

Our main results are explicit expressions for the numbers $N_X(r, s, k)$, which involve the q^2*-binomial coefficient* given by

$$\begin{bmatrix} x \\ k \end{bmatrix} = \prod_{i=1}^{k} (q^{2x-2i+2} - 1)/(q^{2i} - 1)$$

for real x and nonnegative integral k (see [1] and [8], for example, for elementary properties of these numbers). For now we state our results for the most important case when $r = s = k = m$. The general results are postponed to later sections.

We begin with the case that X is the set of alternating matrices over $\mathbb{F}_q$. Recall that every alternating matrix has even rank (see [8, Lemma 10], for example). We have the following result, which holds for finite fields of arbitrary characteristic.

Theorem 1. *Let m be even and let X be the set of $m \times m$ alternating matrices over $\mathbb{F}_q$. Writing $n = m/2$, we have*

$$N_X(m, m, m) = \frac{v}{q^n} \sum_{i=0}^{n} (-1)^i \, q^{i(i-1)} \begin{bmatrix} n \\ i \end{bmatrix} \prod_{k=1}^{n-i} (q^{2k-1} - 1)^2,$$

where

$$v = q^{n(n-1)} \prod_{k=1}^{n} (q^{2k-1} - 1)$$

is the number of nonsingular matrices in X.

For the symmetric matrices we have the following result for finite fields of odd characteristic.

Theorem 2. *Let q be an odd prime power and let X be the set of $m \times m$ symmetric matrices over $\mathbb{F}_q$. Write $n = \lfloor (m + 1)/2 \rfloor$. Then, for odd m, we have*

$$N_X(m, m, m) = \frac{v}{q^n} \sum_{i=0}^{n} (-1)^i \, q^{i(i-1)} \begin{bmatrix} n \\ i \end{bmatrix} \prod_{k=1}^{n-i} (q^{2k-1} - 1)^2,$$

and for even m, we have

$$N_X(m, m, m) = \frac{v}{q^n} \sum_{i=0}^{n} (-1)^i \, q^{i(i-1)} \begin{bmatrix} n \\ i \end{bmatrix} \prod_{k=1}^{n-i} (q^{2k} - q)^2,$$

where

$$v = \begin{cases} q^{n(n-1)} \prod_{k=1}^{n} (q^{2k-1} - 1) & \text{for odd } m \\ q^{n(n+1)} \prod_{k=1}^{n} (q^{2k-1} - 1) & \text{for even } m \end{cases}$$

is the number of nonsingular matrices in X.

It can be shown that Theorem 2 also holds for even q and odd m. In particular, it can be shown that, if q is even and X is the set of $m \times m$ symmetric matrices over $\mathbb{F}_q$ and Y is the set of $m + 1 \times m + 1$ alternating matrices over $\mathbb{F}_q$, then

$$N_X(m, m, m) = N_Y(m + 1, m + 1, m + 1),$$

and so $N_X(m, m, m)$ can be obtained from Theorem 1. This follows from a relationship between two association schemes (see [16, Section 5], for example) and our discussion on association schemes in Section 2. We could not prove, but conjecture based on its verification for $m \in \{2, 4, 6\}$, that Theorem 2 also holds for even q and even m.

A quadratic form on $\mathbb{F}_q^m$ that is nonsingular is also called *bent* or a *quadratic bent function*. (There is a more general definition [2] of the bent property for arbitrary functions from $\mathbb{F}_q^m$ to $\mathbb{F}_q$, which however is not required here.) Recall that there is a one-to-one correspondence between quadratic forms on $\mathbb{F}_q^m$ and $m \times m$ alternating matrices over $\mathbb{F}_q$ if $q = 2$ and $m \times m$ symmetric matrices over $\mathbb{F}_q$ if q is odd. Thus, for $q = 2$ or odd q, a quadratic form on $\mathbb{F}_q^m$ is bent if the corresponding matrix is nonsingular.

Vector spaces of bent functions are important in cryptography and coding theory (see [2] and [3], for example) and m-dimensional spaces of bent functions on $\mathbb{F}_p^m$ for odd prime p (also called *planar* functions) are equivalent to commutative semifields of odd characteristic [5]. Our results give the number of 2-dimensional spaces of quadratic bent functions on $\mathbb{F}_2^m$. A related and more difficult problem is the determination of the number of inequivalent 2-dimensional spaces of quadratic bent functions on $\mathbb{F}_q^m$. This number is known for odd q and $m \in \{2, 3\}$ and equals 1 in these cases [13], [14].

A quadratic form on $\mathbb{F}_2^m$ is *negabent* if its associated alternating matrix M is such that $M + I$ is nonsingular, where I is the identity matrix [15] (again there is a more general definition of negabent functions from $\mathbb{F}_2^m$ to $\mathbb{F}_2$ [15], which we do not require here). A quadratic form on $\mathbb{F}_2^m$ is *bent-negabent* if it is simultaneously bent and negabent. Hence bent-negabent quadratic forms on $\mathbb{F}_2^m$ can only exist if m is even. It has been shown in [15, Theorem 8] that a quadratic form on $\mathbb{F}_2^m$ is bent-negabent if and only if its associated alternating matrix M is such that M and $M + I + J$ are both nonsingular, where I and J are the identity and the all-ones matrix, respectively.

Let X be the set of $m \times m$ alternating matrices over $\mathbb{F}_2$ and let X_k contain all matrices in X of rank k. Since $X_0, X_1, \dots, X_m$ are the fibres of an association scheme (see Sections 2 and 3), we find by a general property of association schemes that, for fixed $A \in X_r$, the number of $B \in X_s$ such that $A + B \in X_k$ is independent of the particular choice of A. Therefore, Theorem 1 gives the number of bent-negabent quadratic forms, solving a problem due to Parker and Pott [15, Problem 2].

Corollary 3. *The number of bent-negabent quadratic forms on $\mathbb{F}_2^{2n}$ is*

$$\frac{1}{2^n}\sum_{i=0}^{n}(-1)^i\,2^{i(i-1)}\begin{bmatrix}n\\i\end{bmatrix}\prod_{k=1}^{n-i}(2^{2k-1}-1)^2.$$

2 A general method

Suppose that $(X,+)$ is an abelian group of matrices over $\mathbb{F}_q$ (which is certainly true when X is the set of $m\times m$ alternating or symmetric matrices over $\mathbb{F}_q$). In this case the numbers $N_X(r,s,k)$ can be computed as follows. Recall that the *characters* of $(X,+)$ are the homomorphisms from $(X,+)$ to the multiplicative group of the complex numbers and form themselves a group, which is isomorphic to $(X,+)$.

Lemma 4. *Let $(X,+)$ be an abelian group of matrices over $\mathbb{F}_q$ and let X_k contain all matrices in X of rank k. Then the numbers defined in* (1) *satisfy*

$$N_X(r,s,k)=\frac{1}{|X|}\sum_{\phi}\sum_{A\in X_r}\phi(A)\sum_{B\in X_s}\phi(B)\sum_{C\in X_k}\phi(C),$$

where the first sum ranges over all characters ϕ of $(X,+)$.

Proof. Indeed, by an elementary property of characters, the sum

$$\frac{1}{|X|}\sum_{\phi}\phi(A+B-C)$$

equals 1 if $A+B=C$ and is zero otherwise. The lemma follows easily from this. □

The computation of the numbers $N_X(r,s,k)$ is particularly simple in the case that X has the structure of a (symmetric) translation scheme, which is an association scheme with additional properties. Let $X_0,X_1,\dots,X_m$ be a partition of X. Then X is a *translation scheme* with *fibres* $X_0,X_1,\dots,X_m$ if the following properties are satisfied:

(P1) X_0 contains only the identity of $(X,+)$.

(P2) For all $r\in\{1,\dots,m\}$, we have $x\in X_r$ if and only if $-x\in X_r$.

(P3) If $x-y\in X_r$, then the number of $z\in X$ such that $z-y\in X_s$ and $x-z\in X_k$ is a constant $p(r,s,k)$ (called the *intersection numbers*) depending only on r, s, and k, but not on the particular choice of x and y.

We refer to [6] and [9] for background on association schemes and in particular to [9, Section V] for background on translation schemes.

Let X_k contain all matrices in X of rank k and suppose that $X_0,X_1,\dots,X_m$ are the fibres of a translation scheme. Then by taking y equal to the zero matrix in (P3), it is readily verified that the numbers $N_X(r,s,k)$ can be computed from the intersection numbers $p(r,s,k)$ via

$$N_X(r,s,k) = |X_r| \cdot p(r,s,k). \tag{2}$$

Let $\widehat{X}$ be the group of characters of $(X,+)$. There is a unique partition $\widehat{X}_0, \widehat{X}_1, \dots, \widehat{X}_m$ of $\widehat{X}$ with the property that

$$\sum_{A \in X_k} \phi(A) \tag{3}$$

is constant for each $\phi \in \widehat{X}_i$. The numbers (3), denoted by $P_k(i)$, are the *eigenvalues* of the translation scheme. It then follows from Lemma 4 that

$$N_X(r,s,k) = \frac{1}{|X|} \sum_{i=0}^{m} |\widehat{X}_i| \; P_r(i) P_s(i) P_k(i),$$

which, via (2), gives a well known formula for the intersection numbers (see [10, p. 227], for example). Hence, to compute $N_X(r,s,k)$, it is sufficient to know the *multiplicities* $|\widehat{X}_i|$ and the eigenvalues $P_k(i)$ of the translation scheme.

This principle can be applied for example when X is the set of $m \times n$ matrices over $\mathbb{F}_q$. Without loss of generality, assume that $m \leqslant n$, in which case, $X_0, X_1, \dots, X_m$ are the fibres of an association scheme whose multiplicities and eigenvalues are given in [7]. The principle can also be applied in the case that X is the set of $m \times m$ alternating matrices over $\mathbb{F}_q$, which is discussed in Section 3. However, in general, the principle cannot be applied in the case that X is the set of $m \times m$ symmetric matrices over $\mathbb{F}_q$ since then (P3) in the definition of a translation scheme does not hold. We can however still apply Lemma 4 in this case, which we shall do in Section 4.

3 Alternating matrices

Throughout this section, let X be the set of $m \times m$ alternating matrices over $\mathbb{F}_q$ and write

$$n = \left\lfloor \frac{m}{2} \right\rfloor \quad \text{and} \quad c = q^{\frac{m(m-1)}{2n}},$$

so that $|X| = c^n$. Let X_k contain all matrices in X of rank k. It is well known that $X_0, X_1, \dots, X_m$ are the fibres of a translation scheme [8].

Let $v(k)$ be the cardinality of X_k. (It turns out that these numbers are the multiplicities of the translation scheme.) It is known (see [12, Theorem 3], for example) that $v(k) = 0$ for odd k and

$$v(2i) = \begin{bmatrix} n \\ i \end{bmatrix} \prod_{k=0}^{i-1} (c - q^{2k}) \tag{4}$$

for each $i \in \{0, \dots, n\}$. Let $A, S \in X$ and write a_{ij} and s_{ij} for their entries, respectively (indexed from 1 to m). Let χ be a nontrivial character of $(\mathbb{F}_q, +)$ and define $\phi_S : X \to \mathbb{C}$

by

$$\phi_S(A) = \chi\bigg(\sum_{1\leqslant i<j\leqslant m} s_{ij}a_{ij}\bigg).$$

Since X is an $\mathbb{F}_q$-vector space of dimension $m(m-1)/2$, the mapping ϕ_S ranges through all characters of $(X,+)$ as S ranges over X. For $S\in X_{2i}$, the numbers

$$P_k(i) = \sum_{A\in X_{2k}} \phi_S(A)$$

are well defined. They are the eigenvalues of the translation scheme and given by [8]

$$P_k(i) = \sum_{j=0}^{k}(-1)^{k-j}q^{(k-j)(k-j-1)}\begin{bmatrix}n-j\\n-k\end{bmatrix}\begin{bmatrix}n-i\\j\end{bmatrix}c^j. \tag{5}$$

The following result is now a straightforward consequence of Lemma 4.

Theorem 5. *Let X be the set of $m\times m$ alternating matrices over $\mathbb{F}_q$. Then the numbers defined in* (1) *satisfy*

$$N_X(r,s,k) = \frac{1}{|X|}\sum_{i=0}^{n} v(2i)\,P_r(i)P_s(i)P_k(i),$$

where $v(2i)$ and $P_k(i)$ are given in (4) *and* (5)*, respectively.*

To obtain Theorem 1 from Theorem 5, let m be even, so that $m=2n$, and observe that in this case

$$P_n(i) = (-1)^i q^{n(n-1)}\prod_{k=1}^{n-i}(q^{2k-1}-1). \tag{6}$$

This formula can be either obtained from (5) by a tedious calculation using the q-binomial theorem

$$\sum_{j=0}^{h} q^{j(j-1)}\begin{bmatrix}h\\j\end{bmatrix}x^{h-j}\,y^j = \prod_{k=0}^{h-1}(x+q^{2k}y)\quad\text{for real } x,y \tag{7}$$

or by observing that $P_n(0)=v(2n)$ and $P_n(i)$ satisfies the recurrence

$$P_n(i)(1-q^{2n-2i+1}) = P_n(i-1),$$

which can be obtained from [8, Lemma 12] and (5). From (4) we find that

$$v(2i) = q^{i(i-1)}\begin{bmatrix}n\\i\end{bmatrix}\prod_{k=n-i+1}^{n}(q^{2k-1}-1). \tag{8}$$

Theorem 1 is now easily obtained from Theorem 5 using (6) and (8).

4 Symmetric matrices

Throughout this section, let q be an odd prime power and let η be the quadratic character of $\mathbb{F}_q$. Let X be the set of $m \times m$ symmetric matrices over $\mathbb{F}_q$ and write

$$n = \left\lfloor \frac{m+1}{2} \right\rfloor \quad \text{and} \quad c = q^{\frac{m(m+1)}{2n}},$$

so that $|X| = c^n$. As usual, let X_k be the subset of X containing all matrices of rank k.

Let $A, S \in X$ and write a_{ij} and s_{ij} for their entries, respectively (indexed from 1 to m). Let χ be a nontrivial character of $(\mathbb{F}_q, +)$ and define $\phi_S : X \to \mathbb{C}$ by

$$\phi_S(A) = \chi\bigg(\sum_{i,j=1}^{m} s_{ij} a_{ij}\bigg).$$

Since X is an $\mathbb{F}_q$-vector space of dimension $m(m+1)/2$ and q is odd, the mapping $\phi_S(A)$ ranges through all characters of $(X, +)$ as S ranges over X.

Two matrices $A, B \in X$ are *equivalent* if there exists a nonsingular matrix L such that $LAL^T = B$. We recall some well known facts (see [11, Section 6.2], for example). Every matrix $A \in X$ of rank r is equivalent to a diagonal matrix with main diagonal $[d_1, \dots, d_r, 0, \dots, 0]$, where $d_1, \dots, d_r$ are nonzero. The value $\eta(d_1 \cdots d_r)$ is preserved under equivalence and is called the *type* of A (an empty product equals 1 by convention and so the all-zero matrix has type 1). Two matrices in X are equivalent if and only if they have the same rank and the same type.

Our further analysis crucially relies on the following lemma.

Lemma 6. *The number*

$$\sum_{A \in X_k} \phi_S(A)$$

depends only on the type and rank of S.

Proof. Let L be an arbitrary $m \times m$ matrix over $\mathbb{F}_q$. For $A \in X$, we readily verify the identity

$$\phi_{LSL^T}(A) = \phi_S(L^T AL).$$

If L is nonsingular, then the mapping $A \mapsto L^T AL$ induces a permutation on X_k and hence

$$\sum_{A \in X_k} \phi_{LSL^T}(A) = \sum_{A \in X_k} \phi_S(L^T AL) = \sum_{A \in X_k} \phi_S(A),$$

as required. □

In view of Lemma 6, we may write

$$P_k(i, \delta) = \sum_{A \in X_k} \phi_S(A),$$

where S is of rank i and of type δ.

The equivalence relation defined above partitions X into $2m+1$ equivalence classes. Let $v(i,\delta)$ be the cardinality of the equivalence class containing matrices of rank i and type δ. It will be convenient to write $v(0,-1)=0$ and $P_k(0,-1)=1$.

The following result is a consequence of Lemmas 4 and 6.

Theorem 7. *Let q be an odd prime power and let X be the set of $m\times m$ symmetric matrices over $\mathbb{F}_q$. Then the numbers defined in* (1) *satisfy*

$$N_X(r,s,k)=\frac{1}{|X|}\sum_{i=0}^{m}\sum_{\delta\in\{-1,1\}}v(i,\delta)\;P_r(i,\delta)P_s(i,\delta)P_k(i,\delta).$$

To apply Theorem 7 efficiently, we need to find explicit expressions for the numbers $v(i,\delta)$ and $P_k(i,\delta)$. The numbers $v(i,\delta)$ were computed by Carlitz [4] and will be given in Proposition 8. The numbers $P_k(i,\delta)$ will be given in Proposition 9. (These results depend on $\eta(-1)$, which equals 1 if $q\equiv 1 \pmod 4$ and equals -1 otherwise.)

Proposition 8 (Carlitz [4, Theorem 3]). *We have*

$$\begin{aligned}v(2s,\delta)&=\frac{(q^s+\eta(-1)^s\delta)}{2}\,\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{2s-1})}{(q^{2s}-1)(q^{2s}-q^2)\cdots(q^{2s}-q^{2s-2})},\\ v(2s+1,\delta)&=\frac{1}{2q^s}\,\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{2s})}{(q^{2s}-1)(q^{2s}-q^2)\cdots(q^{2s}-q^{2s-2})}.\end{aligned}$$

In what follows let $v(i)$ be the number of $m\times m$ symmetric matrices of rank i, so that $v(i)=v(i,1)+v(i,-1)$.

Proposition 9. *Write $\ell=\lfloor k/2\rfloor$. Let*

$$F(m,k,s)=(-1)^k\sum_{j=0}^{\ell}(-1)^{\ell-j}q^{(\ell-j)(\ell-j+1)}\begin{bmatrix}n-j-1\\ n-\ell-1\end{bmatrix}\begin{bmatrix}n-s-1\\ j\end{bmatrix}c^j$$

whenever this expression is defined and let $F(m,k,s)=0$ otherwise. Then $P_0(i,\delta)=1$ and $P_k(0,\delta)=v(k)$, and for $k,i\geqslant 1$, the numbers $P_k(i,\delta)$ are given by

$$P_k(2s+1,\delta)=F(m,k,s), \tag{9}$$

and

$$P_k(2s,\delta)=F(m,k,s-1)+\delta\,\eta(-1)^s\,q^{m-s}F(m-1,k-1,s-1). \tag{10}$$

To prove Proposition 9, we require the following recurrence relation for the numbers $P_k(i,\delta)$. Henceforth, we write $P_k^{(m)}(i,\delta)$ and $v^{(m)}(i)$ for $P_k(i,\delta)$ and $v(i)$, respectively, to indicate dependence on m.

Lemma 10. *For $1 \leqslant i, k \leqslant m$, we have*

$$P_k^{(m)}(i,\delta) = P_k^{(m)}(i-1,1) - (-\delta)^{i+1}\,\eta(-1)^s\,q^{m-s}\,P_{k-1}^{(m-1)}(i-1,1),$$

where $s = \lfloor i/2 \rfloor$.

We first deduce Proposition 9 from Lemma 10 and then prove Lemma 10.

Proof of Proposition 9. From the definition of $P_k(i)$ we see that $P_0(i,\delta)$ equals 1 and $P_k(0,\delta)$ is the number of symmetric $m \times m$ matrices of rank k, namely $v(k)$.

From this last identity and Lemma 10 we find that

$$P_k^{(m)}(1,\delta) = v^{(m)}(k) - q^m\,v^{(m-1)}(k-1).$$

With elementary manipulations we then deduce from Proposition 8 that

$$P_k^{(m)}(1,\delta) = \frac{(-1)^k}{q^\ell}\,\frac{(q^m-q)(q^m-q^2)\cdots(q^m-q^{2\ell})}{(q^{2\ell}-1)(q^{2\ell}-q^2)\cdots(q^{2\ell}-q^{2\ell-2})},$$

which we can write as

$$P_k^{(m)}(1,\delta) = (-1)^k \begin{bmatrix} n-1 \\ \ell \end{bmatrix} \prod_{j=1}^{\ell}(c-q^{2j}). \tag{11}$$

Using

$$\begin{bmatrix} n-j-1 \\ n-\ell-1 \end{bmatrix}\begin{bmatrix} n-1 \\ j \end{bmatrix} = \begin{bmatrix} \ell \\ j \end{bmatrix}\begin{bmatrix} n-1 \\ \ell \end{bmatrix},$$

we find that

$$F(m,k,0) = (-1)^k \begin{bmatrix} n-1 \\ \ell \end{bmatrix} \sum_{j=0}^{\ell} q^{j(j-1)} \begin{bmatrix} \ell \\ j \end{bmatrix} (-1)^j\,q^{2j}\,c^{\ell-j}.$$

Applying the q-binomial theorem (7), we then see from (11) that

$$P_k^{(m)}(1,\delta) = F(m,k,0), \tag{12}$$

as required. Now substitute the recurrence in Lemma 10 into itself to obtain

$$P_k^{(m)}(2s+1,\delta) = P_k^{(m)}(2s-1,1) - c\,q^{2(n-s-1)}\,P_{k-2}^{(m-2)}(2s-1,1). \tag{13}$$

Using

$$\begin{bmatrix} n-s \\ j \end{bmatrix} - q^{2(n-s-j)}\begin{bmatrix} n-s-1 \\ j-1 \end{bmatrix} = \begin{bmatrix} n-s-1 \\ j \end{bmatrix},$$

it is readily verified that

$$P_k^{(m)}(2s+1,\delta) = F(m,k,s)$$

satisfies the recurrence (13) for all $s \geqslant 1$. Combination with (12) proves (9). The identity (10) is a then straightforward consequence of Lemma 10 and (9). □

We now prove Lemma 10.

Proof of Lemma 10. Fix $i \in \{1, \dots, m\}$ and $\delta \in \{-1, 1\}$. Let S be an $m \times m$ diagonal matrix of rank i with diagonal $[z, 1, \dots, 1, 0, \dots, 0]$ such that $\eta(z) = \delta$, and let S' be an $(m-1) \times (m-1)$ diagonal matrix of rank $i-1$ with diagonal $[1, \dots, 1, 0, \dots, 0]$. We have

$$\begin{aligned} P_k^{(m)}(i-1, 1) - P_k^{(m)}(i, \delta) &= \sum_{A \in X_k^{(m)}} \big(\phi_{S'}(B) - \phi_S(A)\big) \qquad (14) \\ &= \sum_{A \in X_k^{(m)}} \phi_{S'}(B)\big(1 - \chi(za)\big), \qquad (15) \end{aligned}$$

where we write A as

$$A = \begin{bmatrix} a & v^T \\ v & B \end{bmatrix} \qquad (16)$$

for some $a \in \mathbb{F}_q$, some $v \in \mathbb{F}_q^{m-1}$, and some $(m-1) \times (m-1)$ symmetric matrix B over $\mathbb{F}_q$. The summand in (15) is zero for $a = 0$, so assume that a is nonzero. Writing

$$L = \begin{bmatrix} 1 & -a^{-1}v^T \\ 0 & I \end{bmatrix},$$

we have

$$L^T A L = \begin{bmatrix} a & 0 \\ 0 & C \end{bmatrix}, \quad \text{where} \quad C = B - a^{-1}vv^T.$$

Note that L is nonsingular. Therefore, as $a \in \mathbb{F}_q^*$, $C \in X_{k-1}^{(m-1)}$, and $v \in \mathbb{F}_q^{m-1}$ range over their possible values, the matrix A, given in (16), ranges over all elements of $X_k^{(m)}$, except for those matrices (16) satisfying $a = 0$. Hence, using the homomorphism property of $\phi_{S'}$, the sum (15) becomes

$$\sum_{a \in \mathbb{F}_q^*} \big(1 - \chi(za)\big) \sum_{C \in X_{k-1}^{(m-1)}} \phi_{S'}(C) \sum_{v \in \mathbb{F}_q^{m-1}} \phi_{S'}(a^{-1}vv^T). \qquad (17)$$

By definition we have

$$\sum_{C \in X_{k-1}^{(m-1)}} \phi_{S'}(C) = P_{k-1}^{(m-1)}(i-1, 1). \qquad (18)$$

Furthermore,

$$\begin{aligned} \sum_{v \in \mathbb{F}_q^{m-1}} \phi_{S'}(a^{-1}vv^T) &= q^{m-i} \sum_{v_1, \dots, v_{i-1} \in \mathbb{F}_q} \chi(a^{-1}(v_1^2 + \dots + v_{i-1}^2)) \\ &= q^{m-i} \left(\sum_{v \in \mathbb{F}_q} \chi(a^{-1}v^2) \right)^{i-1}. \qquad (19) \end{aligned}$$

Putting $\eta(0)=0$, the summation becomes

$$\begin{aligned}\sum_{v\in\mathbb{F}_q}\chi(a^{-1}v^2)&=\sum_{y\in\mathbb{F}_q}(1+\eta(y))\chi(a^{-1}y)\\&=\sum_{y\in\mathbb{F}_q}(1+\eta(ay))\chi(y)\\&=\eta(a)\,G(\eta,\chi),\end{aligned}\tag{20}$$

where

$$G(\eta,\chi)=\sum_{y\in\mathbb{F}_q}\eta(y)\chi(y)$$

is a Gauss sum. Substitute (20) into (19) and then (19) and (18) into (17), we find that (14) equals

$$P_{k-1}^{(m-1)}(i-1,1)\,q^{m-i}\,G(\eta,\chi)^{i-1}\sum_{a\in\mathbb{F}_q^*}\big(1-\chi(za)\big)\eta(a)^{i-1}.$$

The inner summation equals q for odd i and, by an argument similar to that leading to (20), equals $-\eta(z)G(\eta,\chi)$ for even i. Hence, since $\eta(z)=\delta$, we have

$$P_k^{(m)}(i-1,1)-P_k^{(m)}(i,\delta)=(-\delta)^{i+1}\,q^{m-2s}\,G(\eta,\chi)^{2s}\,P_{k-1}^{(m-1)}(i-1,1)$$

(where $s=\lfloor i/2\rfloor$). The proof is completed by recalling that

$$G(\eta,\chi)^2=\eta(-1)q$$

(see [11, Theorem 5.12 (iv)], for example). □

In the remainder of this section we sketch how Theorem 2 follows from Theorem 7 and Propositions 8 and 9.

We first consider the case that m is odd, thus $m=2n-1$. In this case, the expression $F(m-1,m-1,s)$ in Proposition 9 equals 0 for all s and we find that

$$P_m(2i,1)=P_m(2i,-1)=P_m(2i-1,1)=P_m(2i-1,-1).$$

Using the q-binomial theorem (7), we see that these numbers equal

$$(-1)^i q^{n(n-1)}\prod_{k=1}^{n-i}(q^{2k-1}-1).$$

Furthermore, from Proposition 8 we find that

$$v(2i,1)+v(2i,-1)+v(2i-1,1)+v(2i-1,-1)$$

equals

$$q^{i(i-1)}\begin{bmatrix}n\\i\end{bmatrix}\prod_{k=n-i+1}^{n}(q^{2k-1}-1).\tag{21}$$

It then follows from Theorem 7 that

$$N_X(m,m,m) = \frac{v(m)}{q^n} \sum_{i=0}^{n} (-1)^i q^{i(i-1)} \begin{bmatrix} n \\ i \end{bmatrix} \prod_{k=1}^{n-i} (q^{2k-1}-1)^2,$$

where $v(m)$, the number of nonsingular matrices in X, is given by

$$v(m) = q^{n(n-1)} \prod_{k=1}^{n} (q^{2k-1}-1)$$

(which can be obtained from (21) by putting $i = n$).

Next we consider the case that m is even, thus $m = 2n$. In this case, the expression $F(m, m, s)$ in Proposition 9 equals 0 for all s and therefore we have

$$P_m(2i+1, \delta) = 0$$

and

$$P_m(2i, \delta) = \delta\, \eta(-1)^i\, (-1)^i q^{n^2} \prod_{k=1}^{n-i} (q^{2k}-q).$$

Hence, by Theorem 7,

$$N_X(m,m,m) = \frac{1}{|X|} \sum_{i=0}^{n} (v(2i,1) - v(2i,-1)) P_m(2i,1)^3.$$

From Proposition 8 we find that

$$v(2i,1) - v(2i,-1) = \eta(-1)^i q^{i(i-1)} \begin{bmatrix} n \\ i \end{bmatrix} \prod_{k=n-i+1}^{n} (q^{2k}-q),$$

and therefore,

$$N_X(m,m,m) = \frac{v(m)}{q^n} \sum_{i=0}^{n} (-1)^i q^{i(i-1)} \begin{bmatrix} n \\ i \end{bmatrix} \prod_{k=1}^{n-i} (q^{2k}-q)^2,$$

where $v(m)$ is given by

$$v(m) = q^{n^2} \prod_{k=1}^{n} (q^{2k}-q).$$

References

[1] G. E. Andrews. *The Theory of Partitions*, volume 2 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 1976.

[2] C. Carlet. Boolean functions for cryptography and error-correcting codes. In Y. Crama and P. L. Hammer, editors, *Boolean models and methods in mathematics, computer science, and engineering*, pages 257–397. Cambridge University Press, 2010.

[3] C. Carlet. Vectorial boolean functions for cryptography. In Y. Crama and P. L. Hammer, editors, *Boolean models and methods in mathematics, computer science, and engineering*, pages 257–397. Cambridge University Press, 2010.

[4] L. Carlitz. Representations by quadratic forms in a finite field. *Duke Math. J.*, 21:123–137, 1954.

[5] R. S. Coulter and M. Henderson. Commutative presemifields and semifields. *Adv. Math.*, 217(1):282–304, 2008.

[6] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep. Suppl.*, 10, 1973.

[7] P. Delsarte. Bilinear forms over a finite field with applications to coding theory. *J. Combin. Theory Ser. A*, 25(3):226–241, 1978.

[8] P. Delsarte and J. M. Goethals. Alternating bilinear forms over GF(q). *J. Combin. Theory Ser. A*, 19(1):26–50, 1975.

[9] P. Delsarte and V. I. Levenshtein. Association schemes and coding theory. *IEEE Trans. Inf. Theory*, 44(6):2477–2504, 1998.

[10] C. D. Godsil. *Algebraic combinatorics*. Chapman and Hall Mathematics Series. Chapman & Hall, New York, 1993.

[11] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 2nd edition, 1997.

[12] J. MacWilliams. Orthogonal matrices over finite fields. *Amer. Math. Monthly*, 76:152–164, 1969.

[13] G. Menichetti. On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field. *J. Algebra*, 47(2):400–410, 1977.

[14] F. Özbudak and A. Pott. Uniqueness of $\mathbb{F}_q$-quadratic perfect nonlinear maps from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q^2$. *Finite Fields Appl.*, 29:49–88, 2014.

[15] M. G. Parker and A. Pott. On Boolean functions which are bent and negabent. In *Sequences, subsequences, and consequences*, volume 4893 of *Lecture Notes in Comput. Sci.*, pages 9–23. Springer, Berlin, 2007.

[16] K.-U. Schmidt. Symmetric bilinear forms over finite fields of even characteristic. *J. Combin. Theory Ser. A*, 117(8):1011–1026, 2010.