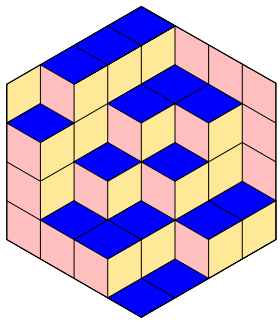


ALGEBRAIC COMBINATORICS

Kai-Uwe Schmidt

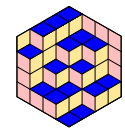
Quadratic and symmetric bilinear forms over finite fields and their association schemes

Volume 3, issue 1 (2020), p. 161-189.

<http://alco.centre-mersenne.org/item/ALCO_2020___3_1_161_0>

Algebraic Combinatorics is member of the
Centre Mersenne for Open Scientific Publishing
www.centre-mersenne.org

Algebraic Combinatorics
Volume 3, issue 1 (2020), p. 161–189
https://doi.org/10.5802/alco.88



Quadratic and symmetric bilinear forms over finite fields and their association schemes

Kai-Uwe Schmidt

Abstract Let $\mathscr{Q}(m,q)$ and $\mathscr{S}(m,q)$ be the sets of quadratic forms and symmetric bilinear forms on an m-dimensional vector space over $\mathbb{F}_q$, respectively. The orbits of $\mathscr{Q}(m,q)$ and $\mathscr{S}(m,q)$ under a natural group action induce two translation association schemes, which are known to be dual to each other. We give explicit expressions for the eigenvalues of these association schemes in terms of linear combinations of generalised Krawtchouk polynomials, generalising earlier results for odd q to the more difficult case when q is even. We then study d-codes in these schemes, namely subsets X of $\mathscr{Q}(m,q)$ or $\mathscr{S}(m,q)$ with the property that, for all distinct $A, B \in X$, the rank of $A-B$ is at least d. We prove tight bounds on the size of d-codes and show that, when these bounds hold with equality, the inner distributions of the subsets are often uniquely determined by their parameters. We also discuss connections to classical error-correcting codes and show how the Hamming distance distribution of large classes of codes over $\mathbb{F}_q$ can be determined from the results of this paper.

1. Introduction

Let q be a prime power and let $V = V(m,q)$ be an m-dimensional $\mathbb{F}_q$-vector space. Let $\mathscr{Q} = \mathscr{Q}(m,q)$ be the space of quadratic forms on V and let $\mathscr{S} = \mathscr{S}(m,q)$ be the space of symmetric bilinear forms on V. These spaces are naturally equipped with a metric induced by the rank function. The main motivation for this paper is to study d-codes in $\mathscr{Q}$ and $\mathscr{S}$, namely subsets X of $\mathscr{Q}$ or $\mathscr{S}$ such that, for all distinct $A, B \in X$, the rank of $A-B$ is at least d. We are in particular interested in the largest cardinality of d-codes in $\mathscr{Q}$ and $\mathscr{S}$ and in the structure of such sets when this maximum is attained. One of the applications is that d-codes in $\mathscr{Q}$ can be used to construct optimal subcodes of the second-order generalised Reed–Muller code and our theory can be used to determine the Hamming distance distributions of such codes.

For odd q, most of the results in this paper have been obtained by the author in [21]. The new results of this paper concern the more difficult case that q is even, although whenever possible we aim for a unified treatment of the two cases. For even q, some partial results were obtained previously by the author in [20].

The main tool for studying subsets of $\mathscr{Q}$ and $\mathscr{S}$ is the beautiful theory of association schemes. It is known that $\mathscr{Q}(m,q)$ and $\mathscr{S}(m,q)$ carry the structure of a translation association scheme with $\lfloor 3m/2 \rfloor$ classes. These have been studied by Wang, Wang, Ma, and Ma [25]. In particular the two schemes are dual to each other and, for odd q, they are isomorphic. Hence the association scheme on $\mathscr{Q}$ is self-dual

Manuscript received 1st June 2018, revised 14th June 2019, accepted 21st June 2019.

Keywords. Association scheme, symmetric bilinear form, quadratic form, code, distance distribution.

for odd q. These association schemes differ considerably from the classical association schemes typically studied by coding theorists, in the sense that the association schemes on $\mathscr{Q}$ and $\mathscr{S}$ are neither P-polynomial, nor Q-polynomial. This means that their most important parameters, namely the P- and Q-numbers (also known as the first and second eigenvalues), do not just arise from evaluations of sets of orthogonal polynomials (see [6, 23, 24] for the classical association schemes and their P- and Q-numbers).

For odd q, the Q-numbers (and the P-numbers by self-duality) of $\mathscr{S}$ have been determined by the author in [21]. For even q, the computation of these numbers appears to be more difficult and, so far, only very limited partial results are known. Recursive formulae were given by Feng, Wang, Ma, and Ma [11] and some special cases were computed by Bachoc, Serra, and Zémor [2]. The P-numbers of $\mathscr{Q}(m,2)$ have been determined by Hou [13] using an interesting coding-theoretic approach, which implicitly identifies $\mathscr{Q}(m,2)$ with $R(2,m)$ and $\mathscr{S}(m,2)$ with $R(m,m)/R(m-3,m)$, where $R(r,m)$ is the Reed–Muller code of order r and length 2^m. The main result of the present paper is the determination of the P- and Q-numbers of $\mathscr{Q}$ and, by duality, the Q- and P-numbers of $\mathscr{S}$. Although these numbers do not directly arise from evaluations of orthogonal polynomials, they can be expressed in terms of linear combinations of generalised Krawtchouk polynomials. This also simplifies the expressions given by Hou [13].

Using the Q-numbers of $\mathscr{Q}$ and $\mathscr{S}$, we then obtain tight bounds on the size of d-codes in $\mathscr{Q}$ and $\mathscr{S}$, except in $\mathscr{S}$ when d is even and (by self-duality) in $\mathscr{Q}$ when d is even and q is odd, and give explicit expressions for the inner distributions of d-codes when these bounds are attained. In the remaining cases, we obtain tight bounds for d-codes that are subgroups $(\mathscr{Q},+)$ or $(\mathscr{S},+)$.

In the final section of this paper we briefly discuss the connection between d-codes in $\mathscr{Q}$ and classical error-correcting codes, generalising results of [21] valid for odd q. It turns out that error-correcting codes obtained from maximal d-codes in $\mathscr{Q}$ often compare favourably to the best known codes. We show that the Hamming distance enumerators of these error-correcting codes are uniquely determined by their parameters. This at once gives the distance enumerators of large classes of error-correcting codes for which many special cases have been obtained previously using different methods, for example results for (extended) binary cyclic codes obtained by Berlekamp [4] and Kasami [14], recent results for q-ary cyclic codes obtained by Li [15], and many results for q-ary cyclic codes and odd q, as explained in [21]. In particular, Li [15] recently determined the true minimum distance of some narrow-sense primitive BCH codes and obtained their distance enumerators in the case that q is odd. These results are recovered in this paper and the distance enumerators are obtained for all q as corollaries of our results.

2. Quadratic forms and symmetric bilinear forms

In this section we recall the definitions and basic properties of the association schemes of symmetric bilinear forms and quadratic forms from [25]. We refer to [5], [8], and [3] for more background on association schemes and to [18, Chapter 21] and [16, Chapter 30] for gentle introductions.

A (symmetric) *association scheme* with n classes is a pair $(\mathscr{X},(R_i))$, where $\mathscr{X}$ is a finite set and $R_0,R_1,\dots,R_n$ are nonempty relations on $\mathscr{X}$ satisfying:

(A1) $\{R_0,R_1,\dots,R_n\}$ is a partition of $\mathscr{X}\times\mathscr{X}$ and $R_0=\{(x,x):x\in\mathscr{X}\}$;
(A2) Each of the relations R_i is symmetric;

(A3) If $(x,y) \in R_k$, then the number of $z \in \mathscr{X}$ such that $(x,z) \in R_i$ and $(z,y) \in R_j$ is a constant p_{ij}^k depending only on i, j, and k, but not on the particular choice of x and y.

Let $(\mathscr{X}, (R_i))$ be a symmetric association scheme with n classes and let D_i be the adjacency matrix of the graph $(\mathscr{X}, R_i)$. The vector space generated by $D_0, D_1, \ldots, D_n$ over the real numbers has dimension $n+1$ and is in fact an algebra, called the *Bose–Mesner algebra* of the association scheme. There exists another uniquely defined basis for this vector space, consisting of minimal idempotent matrices $E_0, E_1, \ldots, E_n$. We may write

$$D_i = \sum_{k=0}^{n} P_i(k) E_k \quad \text{and} \quad E_k = \frac{1}{|X|} \sum_{i=0}^{n} Q_k(i) D_i$$

for some uniquely determined numbers $P_i(k)$ and $Q_k(i)$, called the *P-numbers* and the *Q-numbers* of $(\mathscr{X}, (R_i))$, respectively.

Now let $V = V(m,q)$ be an m-dimensional $\mathbb{F}_q$-vector space. We denote by $\mathscr{Q} = \mathscr{Q}(m,q)$ the set of quadratic forms on V and by $\mathscr{S} = \mathscr{S}(m,q)$ the set of symmetric bilinear forms on V. Notice that $\mathscr{Q}$ and $\mathscr{S}$ are themselves $\mathbb{F}_q$-vectors spaces of dimension $m(m+1)/2$.

Let $G = G(m,q)$ be the direct product $\mathbb{F}_q^* \times \mathrm{GL}_m(\mathbb{F}_q)$. Then G acts on $\mathscr{Q}$ by $(g,Q) \mapsto Q^g$, where Q^g is given by $Q^g(x) = aQ(Lx)$ and $g = (a,L)$. The semidirect product $\mathscr{Q} \rtimes G$ acts transitively on $\mathscr{Q}$ by

$$((A,g),Q) \mapsto Q^g + A.$$

The action of $\mathscr{Q} \rtimes G$ extends to $\mathscr{Q} \times \mathscr{Q}$ componentwise and partitions $\mathscr{Q} \times \mathscr{Q}$ into orbits, which define the relations of a symmetric association scheme. Two pairs of quadratic forms (Q,Q') and (R,R') are in the same relation if and only if there is a $g \in G$ such that $(Q-Q')^g = R - R'$. This shows that the relation containing (Q,Q') depends only on $Q-Q'$, which is the defining property of a translation scheme [8, Chapter V].

The group G also acts on $\mathscr{S}$ by $(g,S) \mapsto S^g$, where S^g is given by $S^g(x,y) = aS(Lx,Ly)$ and $g = (a,L)$. The semidirect product $\mathscr{S} \rtimes G$ acts transitively on $\mathscr{S}$ by

$$((A,g),S) \mapsto S^g + A.$$

Again, the action of $\mathscr{S} \rtimes G$ extends to $\mathscr{S} \times \mathscr{S}$ componentwise and so partitions $\mathscr{S} \times \mathscr{S}$ into orbits, which define the relations of a symmetric association scheme. Two pairs of symmetric bilinear forms (S,S') and (T,T') are in the same relation if and only if there is a $g \in G$ such that $(S-S')^g = T - T'$, which again makes the association scheme a translation scheme.

When q is odd, every quadratic form $Q \in \mathscr{Q}$ gives rise to a symmetric bilinear form $S \in \mathscr{S}$ via

$$S(x,y) = Q(x+y) - Q(x) - Q(y), \tag{1}$$

from which we can recover Q by $Q(x) = \frac{1}{2}S(x,x)$. This shows that the association schemes on $\mathscr{Q}$ and $\mathscr{S}$ are isomorphic when q is odd. We shall see that this is not the case when q is even.

Now let $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ be a basis for $V(m,q)$. For every quadratic form $Q \in \mathscr{Q}$, there exist $A_{ij} \in \mathbb{F}_q$ such that

$$Q\Big(\sum_{i=1}^{m} x_i \alpha_i\Big) = \sum_{i,j=1}^{m} A_{ij} x_i x_j \tag{2}$$

for all $(x_1, x_2, \ldots, x_m) \in \mathbb{F}_q^m$. We say that the right hand side is the *coordinate representation* of Q (with respect to the basis chosen). The matrix $A = (A_{ij})$ is only

unique modulo the subgroup of $m \times m$ alternating matrices over $\mathbb{F}_q$. Accordingly we associate with Q the coset $[A]$ of alternating matrices containing A.

Let $\{\beta_1, \beta_2, \dots, \beta_m\}$ be another basis for $V(m,q)$. For every symmetric bilinear form $S \in \mathscr{S}$ we then have

$$S\Big(\sum_{i=1}^m x_i\beta_i, \sum_{j=1}^m y_j\beta_j\Big) = \sum_{i,j=1}^m B_{ij}x_iy_j,$$

for all $(x_1, x_2, \dots, x_m) \in \mathbb{F}_q^m$, where $B_{ij} = S(\beta_i, \beta_j)$. Again, we refer to the right hand side as the *coordinate representation* of S. We associate with every symmetric bilinear form the corresponding $m \times m$ symmetric matrix $B = (B_{ij})$.

Let $\chi : \mathbb{F}_q \to \mathbb{C}^*$ be a fixed nontrivial character of $(\mathbb{F}_q, +)$. Hence, if $q = p^k$ for a prime p and an integer k, then $\chi(y) = \omega^{\mathrm{Tr}(\theta y)}$ for some fixed $\theta \in \mathbb{F}_q^*$ and some fixed primitive complex p-th root of unity ω. Here, $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the *absolute trace function* on $\mathbb{F}_q$ defined by

$$\mathrm{Tr}(y) = \sum_{i=1}^k y^{p^i}.$$

For $Q \in \mathscr{Q}$ and $S \in \mathscr{S}$, write

$$\langle Q, S\rangle = \chi(\mathrm{tr}(AB)), \tag{3}$$

where $[A]$ is the coset of alternating matrices associated with Q and B is the symmetric matrix associated with S and tr is the matrix trace. Note that $\langle Q, S\rangle$ is well defined since $\mathrm{tr}(CD) = 0$ if C is alternating and D is symmetric. It is readily verified that $\langle \cdot\, , S\rangle$ ranges through all characters of $(\mathscr{Q}, +)$ when S ranges over $\mathscr{S}$ and that $\langle Q, \cdot\rangle$ ranges through all characters of $(\mathscr{S}, +)$ when Q ranges over $\mathscr{Q}$. Notice that this correspondence depends on the choice of the bases.

The following duality result was observed in [25].

Proposition 2.1 ([25, Proposition 3.2]). *For every $g \in G$ with $g = (a, L)$, we have*

$$\langle Q^g, S\rangle = \langle Q, S^h\rangle,$$

where $h = (a, L^T)$.

Proposition 2.1 shows that the association schemes on $\mathscr{Q}$ and $\mathscr{S}$ are dual to each other in the strong sense of [8, Definition 11].

In what follows, we shall describe the relations of $\mathscr{Q}$ and $\mathscr{S}$ explicitly. For a symmetric bilinear form $S \in \mathscr{S}$, the *radical* is defined to be

$$\mathrm{rad}(S) = \{x \in V : S(x, y) = 0 \text{ for every } y \in V\}.$$

The *rank* of S is the codimension of the radical and coincides with the rank of the symmetric matrix associated with S. For a quadratic form $Q \in \mathscr{Q}$, let $S_Q(x, y) = Q(x + y) - Q(x) - Q(y)$ be the associated symmetric bilinear form, and define the *radical* of Q to be

$$\mathrm{rad}(Q) = \{x \in \mathrm{rad}(S_Q) : Q(x) = 0\}.$$

The *rank* of Q is defined to be the codimension of its radical.

The following result describes the orbits of the action of G on $\mathscr{Q}$ and was essentially obtained by Dickson [9].

Proposition 2.2. *The action of G on $\mathscr{Q}(m,q)$ partitions $\mathscr{Q}(m,q)$ into $\lfloor 3m/2\rfloor + 1$ orbits, one of them contains just the zero form. There is one orbit for each odd rank r and one representative is, in coordinate representation,*

$$\sum_{i=1}^{(r-1)/2} x_{2i-1}x_{2i} + x_r^2.$$

There are two orbits for each nonzero even rank r and representatives from the two orbits are, in coordinate representation,

$$\sum_{i=1}^{r/2} x_{2i-1}x_{2i}, \tag{4}$$

$$\sum_{i=1}^{r/2-1} x_{2i-1}x_{2i} + Q_0, \tag{5}$$

where

$$Q_0 = \begin{cases} x_{r-1}^2 + x_{r-1}x_r + \alpha x_r^2 & \text{for } q \text{ even,} \\ x_{r-1}^2 - \beta x_r^2 & \text{for } q \text{ odd} \end{cases}$$

and $\alpha \in \mathbb{F}_q^*$ is a fixed element satisfying $\mathrm{Tr}(\alpha) = 1$ (for even q) and $\beta \in \mathbb{F}_q^*$ is a fixed nonsquare in $\mathbb{F}_q^*$ (for odd q).

If Q belongs to an orbit corresponding to (4), then Q is called *hyperbolic* or of *type* 1 and if Q belongs to an orbit corresponding to (5), then Q is called *elliptic* or of *type* -1. By convention, the zero form is a hyperbolic quadratic form of rank 0. Let $\mathscr{Q}_{2s+1}$ be the set of quadratic forms on V of rank $2s+1$ and let $\mathscr{Q}_{2s,1}$ and $\mathscr{Q}_{2s,-1}$ be the sets of hyperbolic and elliptic quadratic forms on V of rank $2s$, respectively. Write

$$I = \{2s+1 : s \in \mathbb{Z}\} \cup \{(2s, \tau) : s \in \mathbb{Z}, \tau = \pm 1\}$$

and, for every $i \in I$, define the relations

$$R_i = \{(Q, Q') \in \mathscr{Q} \times \mathscr{Q} : Q - Q' \in \mathscr{Q}_i\}. \tag{6}$$

The nonempty relations are then precisely the relations of the association scheme of quadratic forms.

It should be noted that, by joining the relations $R_{2s,1}$, $R_{2s,-1}$, and R_{2s-1} in $\mathscr{Q}(m,q)$, we obtain an association scheme studied by Egawa [10]. As shown in [10], this association scheme has the same parameters as the association scheme of alternating bilinear forms on an $(m+1)$-dimensional $\mathbb{F}_q$-vector space [7], which is reflected by (30) and (35) in the present paper. However, the determination of the P- and Q-numbers of our refined association scheme is considerably more difficult.

The following result describes the orbits of the action of G on $\mathscr{S}$ and was essentially obtained by Albert [1] (and, for odd q, also follows from Proposition 2.2 via (1)).

Proposition 2.3. *The action of G on $\mathscr{S}(m,q)$ partitions $\mathscr{S}(m,q)$ into $\lfloor 3m/2 \rfloor + 1$ orbits, one of them contains just the zero form. There is one orbit for each odd rank r and one representative is, in coordinate representation,*

$$\sum_{i=1}^{(r-1)/2} (x_{2i-1}y_{2i} + x_{2i}y_{2i-1}) + x_r y_r.$$

There are two orbits for each nonzero even rank r and representatives from the two orbits are, in coordinate representation,

$$\sum_{i=1}^{r/2} (x_{2i-1}y_{2i} + x_{2i}y_{2i-1}), \tag{7}$$

$$\sum_{i=1}^{r/2-1} (x_{2i-1}y_{2i} + x_{2i}y_{2i-1}) + S_0, \tag{8}$$

where

$$S_0 = \begin{cases} x_{r-1}y_r + x_r y_{r-1} + x_r y_r & \text{for even } q, \\ x_{r-1}y_{r-1} - \beta x_r y_r & \text{for odd } q, \end{cases}$$

and β is a fixed nonsquare of $\mathbb{F}_q^*$ (for odd q).

Let $\mathscr{S}_{2s+1}$ be the set of symmetric bilinear forms on V of rank $2s+1$ and let $\mathscr{S}_{2s,1}$ and $\mathscr{S}_{2s,-1}$ be the sets of symmetric bilinear forms on V of rank $2s$ corresponding to the orbits (7) and (8), respectively. Symmetric bilinear forms in $\mathscr{S}_{2s,\tau}$ are said to be of *type* τ. For even q, it can be shown [1] that $\mathscr{S}_{2s,1}$ contains precisely the alternating bilinear forms of rank $2s$. For every $i \in I$, define the relations

$$R_i' = \{(S, S') \in \mathscr{S} \times \mathscr{S} : S - S' \in \mathscr{S}_i\}. \tag{9}$$

The nonempty relations are then precisely the relations of the association scheme of symmetric bilinear forms.

Now write $v_i = |\mathscr{Q}_i|$ and $\mu_i = |\mathscr{S}_i|$, whose nonzero values are called the *valencies* of the association schemes on $\mathscr{Q}$ and $\mathscr{S}$, respectively. The numbers v_i have been determined by McEliece [19], following the work of Dickson [9]. Since the association schemes on $\mathscr{Q}$ and $\mathscr{S}$ are isomorphic for odd q, we have $\mu_i = v_i$ for odd q. For even q, the numbers μ_i were determined by MacWilliams [17]. We summarise the results in the following form.

Proposition 2.4. *We have*

$$v_{2s+1} = \mu_{2s+1} = \frac{1}{q^s} \frac{\prod_{i=0}^{2s} (q^m - q^i)}{\prod_{i=0}^{s-1} (q^{2s} - q^{2i})},$$

$$v_{2s,\tau} = \frac{q^s + \tau}{2} \frac{\prod_{i=0}^{2s-1} (q^m - q^i)}{\prod_{i=0}^{s-1} (q^{2s} - q^{2i})},$$

$$\mu_{2s,\tau} = \left(\alpha_\tau q^s + \tau \beta_s q^{-s}\right) \frac{\prod_{i=0}^{2s-1} (q^m - q^i)}{\prod_{i=0}^{s-1} (q^{2s} - q^{2i})},$$

where

$$\alpha_\tau = \begin{cases} \frac{1}{2}(1-\tau) & \text{for even } q, \\ \frac{1}{2} & \text{for odd } q \end{cases} \quad \text{and} \quad \beta_s = \begin{cases} 1 & \text{for even } q, \\ \frac{1}{2} q^s & \text{for odd } q. \end{cases}$$

We conclude this section by noting that our association scheme on $\mathscr{S}$ is slightly different from the association schemes on $\mathscr{S}$ in [25] and [21]. The difference is that in [25] and [21] the group G is just $\mathrm{GL}_m(\mathbb{F}_q)$, which increases the number of orbits from $\lfloor 3m/2 \rfloor + 1$ to $2m+1$ in the case that q is odd. Another difference to [21] is that the sets $\mathscr{S}_{2s,1}$ and $\mathscr{S}_{2s,-1}$, and so also the relations $R'_{2s,1}$ and $R'_{2s,-1}$ on $\mathscr{S}$, are interchanged when s is odd and $q \equiv 3 \pmod 4$.

3. Computation of the Q- and P-numbers

Throughout this section we identify quadratic forms with the corresponding cosets of alternating matrices and symmetric bilinear forms with the corresponding symmetric matrices. For $A, B \in \mathbb{F}_q^{m \times m}$, we write

$$\langle A, B \rangle = \chi(\mathrm{tr}(AB)),$$

where χ is the same nontrivial character as in (3). The Q-numbers and the P-numbers of the association scheme on $\mathscr{Q}$ are given by the character sums (see [8, Section V], for example)

$$Q_k(i) = \sum_{B \in \mathscr{S}_k} \langle A, B \rangle \quad \text{for } [A] \in \mathscr{Q}_i, \tag{10}$$

$$P_i(k) = \sum_{[A] \in \mathscr{Q}_i} \langle A, B \rangle \quad \text{for } B \in \mathscr{S}_k, \tag{11}$$

respectively, where $k, i \in I$. The Q-numbers $Q'_i(k)$ and the P-numbers $P'_k(i)$ of the association scheme on $\mathscr{S}$ satisfy

$$Q'_i(k) = P_i(k) \quad \text{and} \quad P'_k(i) = Q_k(i),$$

respectively. For convenience, we define $Q_k(i) = 0$ if $\mathscr{Q}_i = \varnothing$ and $P_i(k) = 0$ if $\mathscr{S}_k = \varnothing$.

In order to give explicit expressions for these numbers, it is convenient to use *q^2-analogs of binomial coefficients*, which are defined by

$$\begin{bmatrix} n \\ q \end{bmatrix} = \prod_{i=0}^{k-1} \frac{q^{2n} - q^{2i}}{q^{2k} - q^{2i}}$$

for integral n and k. These numbers satisfy the following identities

$$\begin{bmatrix} n \\ k \end{bmatrix} = q^{2k} \begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} = \begin{bmatrix} n-1 \\ k \end{bmatrix} + q^{2(n-k)} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}. \tag{12}$$

We also need the following numbers, which can be derived from generalised Krawtchouk polynomials [7, 6]. We define

$$F_r^{(m)}(s) = \sum_{j=0}^{r} (-1)^{r-j} q^{(r-j)(r-j-1)} \begin{bmatrix} n-j \\ n-r \end{bmatrix} \begin{bmatrix} n-s \\ j \end{bmatrix} c^j,$$

where

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

whenever this expression is defined and let $F_r^{(m)}(s) = 0$ otherwise. Equivalently, these numbers can be defined via the $n+1$ equations

$$\sum_{r=0}^{j} \begin{bmatrix} n-r \\ n-j \end{bmatrix} F_r^{(m)}(s) = \begin{bmatrix} n-s \\ j \end{bmatrix} c^j \quad \text{for } j \in \{0, 1, \ldots, n\} \tag{13}$$

(see [7, (29)]).

The following theorem contains explicit expressions for the Q-numbers of $\mathscr{Q}(m, q)$. For odd q, this is follows from [21, Theorem 2.2]. For even q, the result is new.

THEOREM 3.1. *The Q-numbers of the association scheme of quadratic forms $\mathscr{Q}(m, q)$ are as follows. We have $Q_{0,1}(i) = 1$ and $Q_k(0, 1) = \mu_k$ for all $i, k \in I$ and the other Q-numbers are given by*

$$\begin{aligned}
Q_{2r+1}(2s+1) &= -q^{2r} F_r^{(m-1)}(s), \\
Q_{2r+1}(2s, \tau) &= -q^{2r} F_r^{(m-1)}(s-1) + \tau\, q^{m-s+2r} F_r^{(m-2)}(s-1), \\
Q_{2r,\epsilon}(2s+1) &= \alpha_\epsilon\, q^{2r} F_r^{(m-1)}(s) + \epsilon\, \beta_r\, F_r^{(m)}(s), \\
Q_{2r,\epsilon}(2s, \tau) &= \alpha_\epsilon\, [q^{2r} F_r^{(m-1)}(s-1) - \tau\, q^{m-s+2r-2} F_{r-1}^{(m-2)}(s-1)] + \epsilon\, \beta_r\, F_r^{(m)}(s),
\end{aligned}$$

where α_ϵ and β_r are given in Proposition 2.4.

It is well known (and can be easily verified) that the P-numbers of $\mathscr{Q}$ can be computed from the Q-numbers of $\mathscr{Q}$ via

$$P_i(k) = \frac{v_i}{\mu_k} Q_k(i).$$

Proposition 2.4 then shows that $P_i(k) = Q_k(i)$ for odd q (as it should since the association scheme on $\mathscr{Q}$ is isomorphic to its dual in this case). For even q, the P-numbers of $\mathscr{Q}$ are given in the following theorem.

Theorem 3.2. *For even q, the P-numbers of the association scheme of quadratic forms $\mathscr{Q}(m,q)$ are as follows. We have $P_{0,1}(k) = 1$ and $P_i(0,1) = v_i$ for all $i, k \in I$ and the other P-numbers are given by*

$$\begin{aligned}
P_{2s+1}(2r+1) &= -q^{2s} F_s^{(m-1)}(r),\\
2P_{2s,\tau}(2r+1) &= q^{2s} F_s^{(m-1)}(r) + \tau\, q^s F_s^{(m)}(r),\\
2P_{2s,\tau}(2r,1) &= q^s(q^s+\tau) F_s^{(m)}(r),\\
2P_{2s,\tau}(2r,-1) &= q^{2s} F_s^{(m-1)}(r-1) + \tau\, q^s F_s^{(m)}(r),\\
P_{2s+1}(2r,1) &= (q^m - q^{2s}) F_s^{(m)}(r),\\
P_{2s+1}(2r,-1) &= -q^{2s} F_s^{(m-1)}(r-1).
\end{aligned}$$

In the remainder of this section, we shall prove Theorems 3.1 and 3.2. We begin with the following result, which is essentially known.

Proposition 3.3. *Let α_ϵ and β_r be as in Proposition 2.4. The Q-numbers of the association scheme $\mathscr{Q}(m,q)$ satisfy*

$$\begin{aligned}
\beta_r F_r^{(m)}(s) &= \alpha_{-1} Q_{2r,1}(2s,\tau) - \alpha_1 Q_{2r,-1}(2s,\tau)\\
&= \alpha_{-1} Q_{2r,1}(2s+1) - \alpha_1 Q_{2r,-1}(2s+1).
\end{aligned}$$

Proof. For odd q, the statement in the lemma can be deduced from [21, Lemma 6.3], so assume that q is even. Then $\mathscr{S}_{2r,1}$ is the set of alternating bilinear forms of rank $2r$ on V. By Proposition 2.2, every quadratic form in $\mathscr{Q}_{2s+1}$ can be represented by an $m \times m$ block diagonal matrix with the block (1) in the top left corner, followed by s copies of

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}. \tag{14}$$

It can be shown using Proposition 2.2 that the quadratic form $x^2+xy+\lambda y^2$ in $\mathscr{Q}(2,q)$ is of type $(-1)^{\mathrm{Tr}(\lambda)}$. Hence a quadratic form in $\mathscr{Q}_{2s,\tau}$ can be represented by the zero matrix or by an $m \times m$ block diagonal matrix with the block

$$\begin{bmatrix} \lambda & 1 \\ 0 & 1 \end{bmatrix} \tag{15}$$

in the top left corner, followed by $s-1$ copies of (14), where $(-1)^{\mathrm{Tr}(\lambda)} = \tau$. It follows from these observations that, for $k = (2r,1)$ the character sums (10) have been evaluated by Delsarte and Goethals [7, Appendix], which gives

$$Q_{2r,1}(2s,\tau) = Q_{2r,1}(2s+1) = F_r^{(m)}(s),$$

as required. □

In what follows we write, for every $i \in I$,

$$Q_{2r}(i) = Q_{2r,1}(i) + Q_{2r,-1}(i).$$

We shall also write $Q_k^{(m)}(i)$ for $Q_k(i)$ and $\mathscr{S}_k^{(m)}$ for $\mathscr{S}_k$ whenever we need to indicate dependence on m.

We have the following recurrences for the Q-numbers.

LEMMA 3.4. *For $k \geqslant 1$ and $s \geqslant 0$, we have*

$$Q_k^{(m)}(2s+1) = Q_k^{(m)}(2s,1) - q^{m-s}\, Q_{k-1}^{(m-1)}(2s,1) \tag{16}$$

and for $k \geqslant 1$ and $s \geqslant 1$, we have

$$Q_k^{(m)}(2s,\tau) = Q_k^{(m)}(2s-1) + \tau\, q^{m-s}\, Q_{k-1}^{(m-1)}(2s-1). \tag{17}$$

Proof. For odd q, the lemma can be deduced from [21, Lemma 6.1], so henceforth we assume that q is even.

To prove the identity (16), fix an integer s with $0 \leqslant s \leqslant (m-1)/2$ and let A be the $m \times m$ block diagonal matrix with the block (1) in the top left corner, followed by s copies of (14). Then A is a matrix of a quadratic form of rank $2s+1$. Let A' be the $(m-1) \times (m-1)$ matrix obtained from A by deleting the first row and the first column. Then we have

$$\begin{aligned} Q_k^{(m)}(2s,1) - Q_k^{(m)}(2s+1) &= \sum_{B \in \mathscr{S}_k^{(m)}} (\langle A', B' \rangle - \langle A, B \rangle) \\ &= \sum_{B \in \mathscr{S}_k^{(m)}} \langle A', B' \rangle (1 - \chi(a)), \end{aligned} \tag{18}$$

where χ is the nontrivial character of $(\mathbb{F}_q, +)$ used to define the pairing in (3) and we write B as

$$B = \begin{bmatrix} a & u^T \\ u & B' \end{bmatrix} \tag{19}$$

for some $a \in \mathbb{F}_q$, some $u \in \mathbb{F}_q^{m-1}$ and some $(m-1) \times (m-1)$ matrix B' over $\mathbb{F}_q$. The summand in (18) is zero for $a = 0$, so assume that $a \neq 0$. Writing

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

we have

$$L^T B L = \begin{bmatrix} a & 0 \\ 0 & C \end{bmatrix}, \quad \text{where} \quad C = B' - a^{-1} u u^T.$$

As a ranges over $\mathbb{F}_q^*$ and u ranges over $\mathbb{F}_q^{m-1}$ and C ranges over $\mathscr{S}_{k-1}^{(m-1)}$, the matrix B in (19) ranges over $\mathscr{S}_k^{(m)}$ with the constraint $a \neq 0$. Therefore the sum (18) is

$$\sum_{a \in \mathbb{F}_q^*} \sum_{u \in \mathbb{F}_q^{m-1}} \sum_{C \in \mathscr{S}_{k-1}^{(m-1)}} \langle A', C \rangle \langle A', a^{-1} u u^T \rangle (1 - \chi(a)).$$

We have

$$\sum_{C \in \mathscr{S}_{k-1}^{(m-1)}} \langle A', C \rangle = Q_{k-1}^{(m-1)}(2s),$$

and

$$\begin{aligned} \sum_{u \in \mathbb{F}_q^{m-1}} \langle A', a^{-1} u u^T \rangle &= q^{m-2s-1} \sum_{u_1, \ldots, u_{2s} \in \mathbb{F}_q} \chi\Big(a^{-1} \Big(\sum_{i=1}^{s} u_{2i-1} u_{2i} \Big) \Big) \\ &= q^{m-2s-1} \Big(\sum_{u, v \in \mathbb{F}_q} \chi(uv) \Big)^s \\ &= q^{m-s-1} \end{aligned}$$

for every $a \in \mathbb{F}_q^*$, and

$$\sum_{a\in\mathbb{F}_q^*}(1-\chi(a)) = q.$$

Substitute everything into (18) to obtain the first identity (16) in the lemma.

To prove the identity (17), fix an integer s with $1 \leqslant s \leqslant m/2$ and $\tau \in \{-1,1\}$. Let $\lambda \in \mathbb{F}_q$ be such that $(-1)^{\mathrm{Tr}(\lambda)} = \tau$ and let A be the $m \times m$ block diagonal matrix with the block (15) in the top left corner, followed by $s-1$ copies of (14). Then A is a matrix of a quadratic form of rank $2s$ and type τ. Let A' be the $(m-1)\times(m-1)$ matrix obtained from A by deleting the first row and the first column. Then we have

$$Q_k^{(m)}(2s-1) - Q_k^{(m)}(2s,\tau) = \sum_{B\in\mathscr{S}_k^{(m)}} \langle A', B'\rangle(1-\chi(a\lambda+u_1)), \tag{20}$$

where we write B as (19) and where $u = (u_1,\dots,u_{m-1})^T$. We split the summation in (20) into two parts: the sum S_1 is over all B with $a \neq 0$ and the sum S_2 is over all B with $a = 0$. Similarly as in the proof of the first identity (16), we have

$$\begin{aligned} S_1 &= \sum_{a\in\mathbb{F}_q^*}\sum_{u\in\mathbb{F}_q^{m-1}}\sum_{C\in\mathscr{S}_{k-1}^{(m-1)}} \langle A', C\rangle\langle A', a^{-1}uu^T\rangle(1-\chi(a\lambda+u_1)) \\ &= Q_{k-1}^{(m-1)}(2s-1)\sum_{a\in\mathbb{F}_q^*}\sum_{u\in\mathbb{F}_q^{m-1}} \langle A', a^{-1}uu^T\rangle(1-\chi(a\lambda)\chi(u_1)). \end{aligned} \tag{21}$$

For every $a \in \mathbb{F}_q^*$, we have

$$\begin{aligned} \sum_{u\in\mathbb{F}_q^{m-1}} \langle A', a^{-1}uu^T\rangle &= q^{m-2s}\sum_{u_1,\dots,u_{2s-1}\in\mathbb{F}_q} \chi\biggl(a^{-1}\biggl(u_1^2+\sum_{i=1}^{s-1}u_{2i}u_{2i+1}\biggr)\biggr) \\ &= q^{m-2s}\biggl(\sum_{u,v\in\mathbb{F}_q}\chi(uv)\biggr)^{s-1}\sum_{w\in\mathbb{F}_q}\chi(w) \\ &= 0 \end{aligned}$$

since the inner sum is zero, and similarly,

$$\begin{aligned} \sum_{u\in\mathbb{F}_q^{m-1}} \langle A', a^{-1}uu^T\rangle\chi(u_1) &= q^{m-2s}\biggl(\sum_{u,v\in\mathbb{F}_q}\chi(uv)\biggr)^{s-1}\sum_{w\in\mathbb{F}_q}\chi(a^{-1}w^2+w) \\ &= q^{m-s-1}\sum_{y\in\mathbb{F}_q}\chi(a(y^2+y)), \end{aligned}$$

by applying the substitution $w = ay$. The mapping is $y \mapsto y^2+y$ is 2-to-1 and its image is the set of elements in $\mathbb{F}_q$ whose absolute trace is zero. Since χ is nontrivial, there exists $\theta \in \mathbb{F}_q^*$ such that

$$\sum_{y\in\mathbb{F}_q}\chi(a(y^2+y)) = \sum_{y\in\mathbb{F}_q}(-1)^{\mathrm{Tr}(\theta a(y^2+y))},$$

which equals q if $a = 1/\theta$ and equals zero otherwise. Substitute everything into (21) to obtain

$$S_1 = -\tau\, q^{m-s}\, Q_{k-1}^{(m-1)}(2s-1),$$

since $\chi(\lambda/\theta) = (-1)^{\mathrm{Tr}(\lambda)} = \tau$.

We complete the proof by showing that the sum S_2, namely the summation in (20) over all B with $a = 0$, equals zero. Let A'' be the matrix obtained from A by deleting the first two rows and the first two columns. Then we have

$$S_2 = \sum_{\substack{B \in \mathscr{S}_k^{(m)} \\ a=0}} \langle A'', B'' \rangle \chi(c)(1 - \chi(b)), \tag{22}$$

where we now write

$$B = \begin{bmatrix} E & U^T \\ U & B'' \end{bmatrix} \quad \text{and} \quad E = \begin{bmatrix} a & b \\ b & c \end{bmatrix}$$

for some $b, c \in \mathbb{F}_q$, some $(m-2) \times 2$ matrix U and some $(m-2) \times (m-2)$ matrix B''. Henceforth we put $a = 0$. For $b = 0$, the summand in (22) equals zero, so we assume that b is nonzero and so E is invertible. Writing

$$M = \begin{bmatrix} I & -E^{-1}U^T \\ 0 & I \end{bmatrix},$$

we have

$$M^T B M = \begin{bmatrix} E & 0 \\ 0 & D \end{bmatrix}, \quad \text{where} \quad D = B'' - UE^{-1}U^T.$$

Then, arguing similarly as before, we obtain

$$\begin{aligned} S_2 &= \sum_{b \in \mathbb{F}_q^*} \sum_{c \in \mathbb{F}_q} \sum_{U \in \mathbb{F}_q^{(m-2)\times 2}} \sum_{D \in \mathscr{S}_{k-2}^{(m-2)}} \langle A'', D \rangle \langle A'', UE^{-1}U^T \rangle \chi(c)(1 - \chi(b)) \\ &= Q_{k-2}^{(m-2)}(2s-2, 1) \sum_{b \in \mathbb{F}_q^*} \sum_{c \in \mathbb{F}_q} \sum_{U \in \mathbb{F}_q^{(m-2)\times 2}} \langle A'', UE^{-1}U^T \rangle \chi(c)(1 - \chi(b)). \end{aligned}$$

There exists an invertible matrix 2×2 matrix N over $\mathbb{F}_q$ such that $NE^{-1}N^T$ is either the 2×2 identity matrix or

$$F = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

depending on whether $c \neq 0$ or $c = 0$, respectively. It is readily verified that

$$\begin{aligned} \sum_{U \in \mathbb{F}_q^{(m-2)\times 2}} \langle A'', UU^T \rangle &= \sum_{U \in \mathbb{F}_q^{(m-2)\times 2}} \langle A'', UFU^T \rangle \\ &= q^{2(m-2s)} \Bigg(\sum_{u,v \in \mathbb{F}_q} \chi(uv) \Bigg)^{2s-2} \\ &= q^{2(m-s-1)}. \end{aligned}$$

Therefore we have

$$S_2 = q^{2(m-s-1)}\, Q_{k-2}^{(m-2)}(2s-2, 1) \sum_{b \in \mathbb{F}_q^*} (1 - \chi(b)) \sum_{c \in \mathbb{F}_q} \chi(c) = 0,$$

since the inner sum is zero. This completes the proof of the identity (17). □

We shall now solve the recurrence relations in Lemma 3.4 using the initial values

$$Q_{0,1}^{(m)}(i) = 1 \tag{23}$$

for each $i \in I$ with $\mathscr{Q}_i \neq \varnothing$,

$$Q_{2r}^{(m)}(0, 1) = \mu_{2r,1}^{(m)} + \mu_{2r,-1}^{(m)}, \tag{24}$$

$$Q_{2r+1}^{(m)}(0, 1) = \mu_{2r+1}^{(m)} \tag{25}$$

for each $r \geqslant 0$, where we write $\mu_k^{(m)}$ for μ_k. These initial values follow immediately from (10).

Proposition 3.5. *For $k \geqslant 1$, the numbers $Q_k(2s+1)$ for $s \geqslant 0$ and the numbers $Q_k(2s,\tau)$ and $s \geqslant 1$ satisfy*

$$Q_{2r+1}(2s+1) = -q^{2r} F_r^{(m-1)}(s), \tag{26}$$

$$Q_{2r+1}(2s,\tau) = -q^{2r} F_r^{(m-1)}(s-1) + \tau\, q^{m-s+2r} F_r^{(m-2)}(s-1), \tag{27}$$

$$Q_{2r}(2s+1) = \quad q^{2r} F_r^{(m-1)}(s), \tag{28}$$

$$Q_{2r}(2s,\tau) = \quad q^{2r} F_r^{(m-1)}(s-1) - \tau\, q^{m-s+2r-2} F_{r-1}^{(m-2)}(s-1). \tag{29}$$

Proof. For odd q, the statements in the lemma are given by [21, Lemma 6.2]. However we prove the lemma for odd and even q simultaneously. Write

$$n = \lfloor (m-1)/2 \rfloor \quad \text{and} \quad c = q^{(m-1)(m-2)/(2n)}.$$

From (16) with $s = 0$ and the initial values (24) and (25) we have

$$Q_{2r}^{(m)}(1) = \mu_{2r,1}^{(m)} + \mu_{2r,-1}^{(m)} - q^m \mu_{2r-1}^{(m-1)},$$
$$Q_{2r+1}^{(m)}(1) = \mu_{2r+1}^{(m)} - q^m \big[\mu_{2r,1}^{(m-1)} + \mu_{2r,-1}^{(m-1)}\big].$$

From Proposition 2.4 we then find that

$$Q_{2r}^{(m)}(1) = -Q_{2r+1}^{(m)}(1) = \frac{1}{q^r} \frac{\prod_{i=1}^{2r}(q^m - q^i)}{\prod_{i=0}^{r-1}(q^{2r} - q^{2i})},$$

which we can write as

$$q^{2r} \begin{bmatrix} n \\ r \end{bmatrix} \prod_{j=0}^{r-1} (c - q^{2j}).$$

This latter expression equals $q^{2r} F_r^{(m-1)}(0)$ (see [7] or [21], for example) and therefore (26) and (28) hold for $s = 0$. Using the initial value (23), we see that (28) also holds for $r = 0$. Now substitute (17) into (16) to obtain

$$Q_k^{(m)}(2s+1) = Q_k^{(m)}(2s-1) - c q^{2(n-s+1)}\, Q_{k-2}^{(m-2)}(2s-1).$$

Using (12), we verify by induction that (26) and (28) hold for all $r, s \geqslant 0$. The identities (27) and (29) then follow (26) and (28) and the recurrence (17). □

Theorem 3.1 now follows directly from Propositions 3.5 and 3.3.

We shall now determine the P-numbers of $\mathscr{Q}(m,q)$ for even q from the Q-numbers and thereby prove Theorem 3.2. We begin with stating the Q-numbers of $\mathscr{Q}(m,q)$ in the following alternative form.

Proposition 3.6. *The Q-numbers $Q_k(i)$ of the association scheme of quadratic forms $\mathscr{Q}(m,q)$ satisfy*

$$\begin{aligned} F_r^{(m+1)}(s) &= Q_{2r,1}(2s-1) + Q_{2r,-1}(2s-1) + Q_{2r-1}(2s-1) \\ &= Q_{2r,1}(2s,\tau) + Q_{2r,-1}(2s,\tau) + Q_{2r-1}(2s,\tau), \end{aligned} \tag{30}$$

$$\tau\, q^{m-s} F_r^{(m)}(s) = Q_{2r,1}(2s,\tau) + Q_{2r,-1}(2s,\tau) + Q_{2r+1}(2s,\tau), \tag{31}$$

$$0 = Q_{2r,1}(2s+1) + Q_{2r,-1}(2s+1) + Q_{2r+1}(2s+1), \tag{32}$$

$$\begin{aligned} \beta_r F_r^{(m)}(s) &= \alpha_{-1} Q_{2r,1}(2s,\tau) - \alpha_1 Q_{2r,-1}(2s,\tau) \\ &= \alpha_{-1} Q_{2r,1}(2s+1) - \alpha_1 Q_{2r,-1}(2s+1) \end{aligned} \tag{33}$$

where α_ϵ and β_r are as in Proposition 2.4.

Proof. This follows from Propositions 3.3 and 3.5 using the identity

$$F_r^{(m+1)}(s) = q^{2r} F_r^{(m-1)}(s-1) - q^{2r-2} F_{r-1}^{(m-1)}(s-1), \tag{34}$$

which can be proved using (12). □

We now use Proposition 3.6 to prove the following counterpart of Proposition 3.6 for the P-numbers.

Proposition 3.7. *The P-numbers of the association scheme of quadratic forms $\mathscr{Q}(m,q)$ satisfy*

$$\begin{aligned} F_s^{(m+1)}(r) &= P_{2s,1}(2r-1) + P_{2s,-1}(2r-1) + P_{2s-1}(2r-1) \\ &= P_{2s,1}(2r,\epsilon) + P_{2s,-1}(2r,\epsilon) + P_{2s-1}(2r,\epsilon), \end{aligned} \tag{35}$$

$$\begin{aligned} q^s\, F_s^{(m)}(r) &= P_{2s,1}(2r,\epsilon) - P_{2s,-1}(2r,\epsilon) \\ &= P_{2s,1}(2r+1) - P_{2s,-1}(2r+1), \end{aligned} \tag{36}$$

$$\frac{\alpha_{-\epsilon}}{\beta_r}\,\epsilon\, q^m\, F_s^{(m)}(r) = P_{2s,1}(2r,\epsilon) + P_{2s,-1}(2r,\epsilon) + P_{2s+1}(2r,\epsilon), \tag{37}$$

$$0 = P_{2s,1}(2r+1) + P_{2s,-1}(2r+1) + P_{2s+1}(2r+1), \tag{38}$$

where α_ϵ and β_r are as in Proposition 2.4.

Proof. We use the orthogonality relation

$$\sum_{s=0}^{\lfloor m/2 \rfloor} F_p^{(m)}(s) F_s^{(m)}(r) = q^{m(m-1)/2} \delta_{r,p} \tag{39}$$

(see [7, (17)], for example). This shows that the matrix

$$F = \left(F_r^{(m)}(s) \right)_{0 \leqslant r,s \leqslant \lfloor m/2 \rfloor}$$

is invertible and its inverse is $q^{-m(m-1)/2} F$.

Let $\mathscr{Q}_s^-$ be the set of all quadratic forms in $\mathscr{Q}(m,q)$ of rank $2s$ or $2s-1$. Similarly, let $\mathscr{S}_r^-$ be the set of all symmetric matrices in $\mathscr{S}(m,q)$ of rank $2r$ or $2r-1$. From (30) and (10) we find that, for every $[A] \in \mathscr{Q}_s^-$, we have

$$F_p^{(m+1)}(s) = \sum_{B \in \mathscr{S}_p^-} \langle A, B \rangle.$$

Therefore, letting $B' \in \mathscr{S}_r^-$, we have

$$\begin{aligned} \sum_{s=0}^{\lfloor (m+1)/2 \rfloor} F_p^{(m+1)}(s) \sum_{[A] \in \mathscr{Q}_s^-} \langle A, B' \rangle &= \sum_{B \in \mathscr{S}_p^-} \sum_{[A] \in \mathscr{Q}} \langle A, B + B' \rangle \\ &= q^{m(m+1)/2}\, \delta_{r,p}, \end{aligned}$$

by the orthogonality of characters. From the orthogonality relation (39) we then conclude that

$$F_s^{(m+1)}(r) = \sum_{[A] \in \mathscr{Q}_s^-} \langle A, B' \rangle,$$

which, in view of the character sum representation (11) of the P-numbers, proves (35).

The other identities can be proved similarly. Let $\mathscr{Q}_s^+$ be the set of all quadratic forms in $\mathscr{Q}(m,q)$ of rank $2s$ or $2s+1$ and let $\mathscr{S}_r^+$ be the set of all symmetric matrices in $\mathscr{S}(m,q)$ of rank $2r$ or $2r+1$. From (31), (32), and (10) we see that

$$\sum_{B\in\mathscr{S}_p^+}\langle A,B\rangle=\begin{cases}\tau\,q^{m-s}F_p^{(m)}(s) & \text{for } [A]\in\mathscr{Q}_{2s,\tau},\\ 0 & \text{for } [A]\in\mathscr{Q}_{2s+1}.\end{cases}$$

Let $B'\in\mathscr{S}_r^+$. We then find that

$$\begin{aligned}\sum_{s=0}^{\lfloor m/2\rfloor}F_p^{(m)}(s)\sum_{\tau\in\{-1,1\}}\tau\,q^{m-s}\sum_{[A]\in\mathscr{Q}_{2s,\tau}}\langle A,B'\rangle&=\sum_{s=0}^{\lfloor m/2\rfloor}\sum_{[A]\in\mathscr{Q}_s^+}\langle A,B'\rangle\sum_{B\in\mathscr{S}_p^+}\langle A,B\rangle\\&=\sum_{B\in\mathscr{S}_p^+}\sum_{[A]\in\mathscr{Q}}\langle A,B+B'\rangle\\&=q^{m(m+1)/2}\,\delta_{r,p}.\end{aligned}$$

From (39) we conclude that

$$\sum_{[A]\in\mathscr{Q}_{2s,1}}\langle A,B'\rangle-\sum_{[A]\in\mathscr{Q}_{2s,-1}}\langle A,B'\rangle=q^s\,F_s^{(m)}(r),$$

which together with (11) proves (36).

To prove (37), we invoke (33) and (10) to obtain, for $B'\in\mathscr{S}_{2r,\epsilon}$,

$$\begin{aligned}\sum_{s=0}^{\lfloor m/2\rfloor}\beta_pF_p^{(m)}(s)\sum_{[A]\in\mathscr{Q}_s^+}\langle A,B'\rangle&=\sum_{s=0}^{\lfloor m/2\rfloor}\sum_{[A]\in\mathscr{Q}_s^+}\langle A,B'\rangle\sum_{\kappa\in\{-1,1\}}\kappa\,\alpha_{-\kappa}\sum_{B\in\mathscr{S}_{2p,\kappa}}\langle A,B\rangle\\&=\sum_{\kappa\in\{-1,1\}}\kappa\,\alpha_{-\kappa}\sum_{B\in\mathscr{S}_{2p,\kappa}}\sum_{[A]\in\mathscr{Q}}\langle A,B+B'\rangle\\&=\epsilon\,\alpha_{-\epsilon}\,q^{m(m+1)/2}\,\delta_{r,p},\end{aligned}$$

which, using (39), gives

$$\sum_{[A]\in\mathscr{Q}_s^+}\langle A,B'\rangle=\frac{\alpha_{-\epsilon}}{\beta_r}\,\epsilon\,q^m\,F_s^{(m)}(r).$$

Now (37) follows from (11). To prove (38), we take $B'\in\mathscr{S}_{2r+1}$ and obtain similarly as above,

$$\sum_{s=0}^{\lfloor m/2\rfloor}\beta_pF_p^{(m)}(s)\sum_{[A]\in\mathscr{Q}_s^+}\langle A,B'\rangle=0.$$

This implies that the inner sum is zero for every s and this gives (38). □

We now complete the proof of Theorem 3.2, which gives explicit expressions for the P-numbers.

Proof of Theorem 3.2. The P-numbers of $\mathscr{Q}(m,q)$ are uniquely determined by Proposition 3.7. We therefore just need to verify that the P-numbers claimed in the theorem satisfy the equations in Proposition 3.7. The identities (36), (37), and (38) are trivially satisfied. The identity (35) is verified using (34) and

$$F_s^{(m+1)}(r)=q^{2s}F_s^{(m)}(r)+(q^m-q^{2s-2})F_{s-1}^{(m)}(r).$$

For even m, this last identity can be proved directly using (12). For odd m, first apply (34) and then (12). □

4. Subsets of quadratic and symmetric bilinear forms

4.1. Inner distributions, codes, and designs. In what follows, let $\mathscr{X} = \mathscr{X}(m,q)$ be either $\mathscr{Q}(m,q)$ or $\mathscr{S}(m,q)$. Accordingly, for $i \in I$, let $\mathscr{X}_i$ be either $\mathscr{Q}_i$ or $\mathscr{S}_i$ and let (R_i) be the corresponding relations on $\mathscr{X}$ defined in (6) and (9). Let X be a subset of $\mathscr{X}$ and associate with X the rational numbers

$$a_i = \frac{|(X \times X) \cap R_i|}{|X|},$$

so that a_i is the average number of pairs in $X \times X$ whose difference is contained in $\mathscr{X}_i$. The sequence of numbers $(a_i)_{i\in I}$ is called the *inner distribution* of X. Let $Q_k(i)$ be the Q-numbers of $(\mathscr{X}, (R_i))$. The *dual inner distribution* of X is the sequence of numbers $(a'_k)_{k\in I}$, where

$$a'_k = \sum_{i\in I} Q_k(i)\, a_i. \tag{40}$$

It is a well known fact of the general theory of association schemes that the numbers a'_k are nonnegative (see [8, Theorem 3], for example).

It is readily verified that the mapping $\rho : X \times X \to \mathbb{Z}$, given by

$$\rho(A,B) = \operatorname{rank}(A - B),$$

is a distance function on $\mathscr{X}$. Accordingly, given an integer d satisfying $1 \leqslant d \leqslant m$, we say that X is a *d-code* in $\mathscr{X}$ if $\operatorname{rank}(A-B) \geqslant d$ for all distinct $A, B \in X$. Alternatively, writing

$$I_\ell = \{2s-1 : s \in \mathbb{Z},\, 1 \leqslant 2s-1 \leqslant \ell\} \cup \{(2s, \pm 1) : s \in \mathbb{Z},\, 2 \leqslant 2s \leqslant \ell\},$$

we can define X to be a d-code if

$$a_i = 0 \quad \text{for each } i \in I_{d-1}.$$

We say that X is a *t-design* if

$$a'_k = 0 \quad \text{for each } k \in I_t.$$

A subset X of $\mathscr{X}$ is *additive* if X is a subgroup of $(\mathscr{X}, +)$. Note that the inner distribution $(a_i)_{i\in I}$ of an additive subset X of $\mathscr{X}$ satisfies

$$a_i = |X \cap \mathscr{X}_i|,$$

for every $i \in I$. The *annihilator* of an additive subset Y of $\mathscr{Q}$ is defined to be

$$Y^\circ = \{S \in \mathscr{S} : \langle Q, S\rangle = 1 \text{ for each } Q \in Y\}$$

and the *annihilator* of an additive subset Z of $\mathscr{S}$ is defined to be

$$Z^\circ = \{Q \in \mathscr{Q} : \langle Q, S\rangle = 1 \text{ for each } S \in Z\}.$$

Note that $(Y^\circ)^\circ = Y$ and $(Z^\circ)^\circ = Z$ and

$$|\mathscr{Q}| = |Y|\,|Y^\circ| = |Z|\,|Z^\circ| = |\mathscr{S}|.$$

The following MacWilliams-type identity is a special case of a general property of association schemes (see [8, Theorem 27], for example).

Theorem 4.1. *Let X be an additive subset of $\mathscr{X}$ with inner distribution $(a_i)_{i\in I}$ and dual inner distribution $(a'_k)_{k\in I}$ and let X° be its annihilator with inner distribution $(a^\circ_k)_{k\in I}$. Then we have $|X|a^\circ_k = a'_k$.*

4.2. Subsets of symmetric bilinear forms. In this section, we prove bounds on the size of d-codes in $\mathscr{S}$. We begin with the following proposition.

Proposition 4.2. *Let Z be a subset of $\mathscr{S}(m,q)$ with inner distribution $(a_i)_{i\in I}$ and dual inner distribution $(a'_k)_{k\in I}$. Write*

$$\begin{aligned} A_r &= a_{2r,1} + a_{2r,-1} + a_{2r-1}, & A'_s &= a'_{2s,1} + a'_{2s,-1} + a'_{2s-1},\\ B_r &= a_{2r,1} + a_{2r,-1} + a_{2r+1}, & B'_s &= a'_{2s,1} + a'_{2s,-1} + a'_{2s+1},\\ C_r &= \frac{\alpha_{-1}}{\beta_r} a_{2r,1} - \frac{\alpha_1}{\beta_r} a_{2r,-1}, & C'_s &= q^{-s}(a'_{2s,1} - a'_{2s,-1}), \end{aligned}$$

where α_ϵ and β_r are given in Proposition 2.4. Then we have

$$\begin{aligned} A'_s &= \sum_r F_s^{(m+1)}(r) A_r,\\ C'_s &= \sum_r F_s^{(m)}(r) B_r,\\ B'_s &= q^m \sum_r F_s^{(m)}(r) C_r. \end{aligned}$$

Proof. Since the Q-numbers $Q_k(i)$ of $\mathscr{S}(m,q)$ are the P-numbers $P_i(k)$ of $\mathscr{Q}(m,q)$, the result follows directly from (40) and Proposition 3.7. □

The following theorem was obtained in [21] in the case that q is odd and in [20] in the case that q is even and d is odd. The case that q and d are even is new.

Theorem 4.3. *Let Z be a d-code in $\mathscr{S}(m,q)$, where Z is required to be additive if d is even. Then*

$$|Z| \leqslant \begin{cases} q^{m(m-d+2)/2} & \text{for } m-d \text{ even}\\ q^{(m+1)(m-d+1)/2} & \text{for } m-d \text{ odd.} \end{cases}$$

Moreover, in the case of odd d, equality occurs if and only if Z is a t-design for

$$t = 2\left(\left\lfloor \frac{m+1}{2} \right\rfloor - \frac{d-1}{2}\right).$$

Proof. As remarked above, the only new case arises when q is even. When q is odd, the theorem was proved in [21, Lemmas 3.5 and 3.6] using the identities for A'_s and C'_s in Proposition 4.2. Since these do not involve C_r (which is the only quantity in the conclusion of Proposition 4.2 that crucially depends on the parity of q), the proofs of [21, Lemmas 3.5 and 3.6] carry over verbatim to the case that q is even. □

We call a d-code Y in $\mathscr{S}(m,q)$ *maximal* if d is odd and equality holds in Theorem 4.3. We shall see in Section 5 that maximal d-codes in $\mathscr{S}$ exist for all possible parameters.

The situation for even d is somewhat mysterious. Theorem 4.3 gives bounds for the largest additive d-codes in $\mathscr{S}(m,q)$ in this case and there certainly exist d-codes that are larger than the largest possible additive d-code [22]. For example, the largest additive 2-code in $\mathscr{S}(3,2)$ has 16 elements by Theorem 4.3, whereas the largest 2-code in $\mathscr{S}(3,2)$ has 22 elements [22]. In fact, this 2-code is essentially unique and can be constructed by taking the zero matrix together with all 21 nonalternating 3×3 symmetric matrices of rank 2. Moreover, [22] contains (not necessarily optimal) d-codes in $\mathscr{S}(m,q)$ for many small values of q, m, and even d, which are larger than the largest additive d-codes in $\mathscr{S}(m,q)$.

4.3. Subsets of quadratic forms. In this section, we prove bounds on the size of d-codes in $\mathscr{Q}$. We begin with the following counterpart of Proposition 4.2.

Proposition 4.4. *Let Y be a subset of $\mathscr{Q}(m,q)$ with inner distribution $(a_i)_{i\in I}$ and dual inner distribution $(a'_i)_{i\in I}$. Write*

$$\begin{aligned} A_s &= a_{2s,1} + a_{2s,-1} + a_{2s-1}, & A'_r &= a'_{2r,1} + a'_{2r,-1} + a'_{2r-1},\\ B_s &= a_{2s,1} + a_{2s,-1} + a_{2s+1}, & B'_r &= a'_{2r,1} + a'_{2r,-1} + a'_{2r+1},\\ C_s &= q^{-s}(a_{2s,1} - a_{2s,-1}), & C'_r &= \frac{\alpha_{-1}}{\beta_r}a'_{2r,1} - \frac{\alpha_1}{\beta_r}a'_{2r,-1}, \end{aligned}$$

where α_ϵ and β_r are given in Proposition 2.4. *Then we have*

$$\begin{aligned} A'_r &= \sum_s F_r^{(m+1)}(s)A_s,\\ C'_r &= \sum_s F_r^{(m)}(s)B_s,\\ B'_r &= q^m \sum_s F_r^{(m)}(s)C_s. \end{aligned}$$

Proof. This follows directly from (40) and Proposition 3.6. □

In the next theorem, we give bounds for d-codes in $\mathscr{Q}$. Since the association schemes on $\mathscr{Q}(m,q)$ and $\mathscr{S}(m,q)$ are isomorphic for odd q, the statement of Theorem 4.3 still holds when Z is a d-code in $\mathscr{Q}(m,q)$ and q is odd. We therefore give bounds for d-codes in $\mathscr{Q}(m,q)$ only for even q.

Theorem 4.5. *Let q be even and let Y be a d-code in $\mathscr{Q}(m,q)$. Then*

$$|Y| \leqslant \begin{cases} q^{m(m-d+2)/2} & \text{for odd } m \text{ and odd } d,\\ q^{(m+1)(m-d+1)/2} & \text{for even } m \text{ and odd } d,\\ q^{(m-1)(m-d+2)/2} & \text{for even } m \text{ and even } d,\\ q^{m(m-d+1)/2} & \text{for odd } m \text{ and even } d. \end{cases}$$

Moreover, in the case of odd d, equality occurs if and only if Y is a t-design for

$$t = 2\left(\left\lfloor \frac{m+1}{2}\right\rfloor - \frac{d-1}{2}\right).$$

Proof. Let $(a_i)_{i\in I}$ be the inner distribution of Y. First assume that d is odd, say $d = 2\delta - 1$. Let A_s and A'_r be as defined in Proposition 4.4 and put

$$n = \lfloor (m+1)/2 \rfloor \quad \text{and} \quad c = q^{m(m+1)/(2n)}.$$

From Proposition 4.4 and (13) we obtain

$$\sum_{r=0}^{n-\delta+1} \begin{bmatrix} n-r \\ \delta-1 \end{bmatrix} A'_r = c^{n-\delta+1} \sum_{s=0}^{n} \begin{bmatrix} n-s \\ n-\delta+1 \end{bmatrix} A_s.$$

Since $A'_0 = |Y|$ and $A_0 = 1$ and $A_s = 0$ for $0 < s < \delta$, we obtain

$$\sum_{r=1}^{n-\delta+1} \begin{bmatrix} n-r \\ \delta-1 \end{bmatrix} A'_r = \begin{bmatrix} n \\ \delta-1 \end{bmatrix} (c^{n-\delta+1} - |Y|).$$

Since the numbers A'_r are nonnegative, the left-hand side is nonnegative, and therefore $|Y| \leqslant c^{n-\delta+1}$, as required. Moreover, this inequality is an equality if and only if $A'_1 = \cdots = A'_{n-\delta+1} = 0$, which is equivalent to Y being a t-design for $t = 2(n-\delta+1)$.

Now assume that d is even, say $d = 2\delta$. Let B_s and C'_r be as defined in Proposition 4.4 and put

$$n = \lfloor m/2 \rfloor \quad \text{and} \quad c = q^{m(m-1)/(2n)}.$$

From Proposition 4.4 and (13) we obtain

$$\sum_{r=0}^{n-\delta+1} \begin{bmatrix} n-r \\ \delta-1 \end{bmatrix} C'_r = c^{n-\delta+1} \sum_{s=0}^{n} \begin{bmatrix} n-s \\ n-\delta+1 \end{bmatrix} B_s$$

and find, similarly as above,

$$\sum_{r=1}^{n-\delta+1} \begin{bmatrix} n-r \\ \delta-1 \end{bmatrix} C'_r = \begin{bmatrix} n \\ \delta-1 \end{bmatrix} (c^{n-\delta+1} - |Y|).$$

Again, we have $|Y| \leqslant c^{n-\delta+1}$, which completes the proof. □

We call a d-code Y in $\mathscr{Q}(m,q)$ *maximal* if equality holds in Theorem 4.5 or in Theorem 4.3, unless q is odd and d is even. We shall see in Section 5 that maximal d-codes in $\mathscr{Q}$ exist for all possible parameters.

An interesting situation, in particular from the coding-theoretic viewpoint of Section 6, occurs for d-codes in $\mathscr{Q}$, when d and m are even and no difference between distinct elements is hyperbolic of rank d. We call such a set an *elliptic* d-code.

Theorem 4.6. *Let m and d be even and let Y be an elliptic d-code in $\mathscr{Q}(m,q)$. Then*

$$|Y| \leqslant q^{m(m-d+1)/2}.$$

Moreover, equality occurs if and only if Y is a t-design for $t = m - d + 1$.

Proof. Write $\delta = d/2$ and $n = m/2$. Let $(a_i)_{i\in I}$ be the inner distribution of Y and let A_s, A'_r, C_s, and B'_r be as defined in Proposition 4.4. From Proposition 4.4 and (13) we obtain

$$\sum_{r=0}^{n-\delta} \begin{bmatrix} n-r \\ \delta \end{bmatrix} (q^\delta A'_r + B'_r) = q^{(m+1)(n-\delta)} q^\delta \sum_{s=0}^{n} \begin{bmatrix} n-s \\ n-\delta \end{bmatrix} (A_s + q^\delta C_s)$$

and therefore, since $A_s = C_s = 0$ for $0 < s < \delta$,

$$\sum_{r=0}^{n-\delta} \begin{bmatrix} n-r \\ \delta \end{bmatrix} (q^\delta A'_r + B'_r) = q^{(m+1)(n-\delta)} q^\delta \left(\begin{bmatrix} n \\ \delta \end{bmatrix} (A_0 + q^\delta C_0) + A_\delta + q^\delta C_\delta \right).$$

We have

$$\begin{aligned} A_\delta + q^\delta C_\delta &= a_{2\delta,1} + a_{2\delta,-1} + a_{2\delta-1} + (a_{2\delta,1} - a_{2\delta,-1}) \\ &= 2a_{2\delta,1} + a_{2\delta-1} \\ &= 0 \end{aligned}$$

since Y is an elliptic (2δ)-code. Since $A_0 = C_0 = 1$ and $A'_0 = |Y|$ and $B'_0 = |Y| + a'_1$, we then obtain

$$\begin{bmatrix} n \\ \delta \end{bmatrix} a'_1 + \sum_{r=1}^{n-\delta} \begin{bmatrix} n-r \\ \delta \end{bmatrix} (q^\delta A'_r + B'_r) = \begin{bmatrix} n \\ \delta \end{bmatrix} (1+q^\delta)(q^{(m+1)(n-\delta)} q^\delta - |Y|).$$

Since the left-hand side is nonnegative, we find that

$$|Y| \leqslant q^{(m+1)(n-\delta)} q^\delta.$$

Moreover, equality occurs if and only if $q^\delta A'_r + B'_r = 0$ for all r satisfying $1 \leqslant r \leqslant n-\delta$, or equivalently if and only if Y is a t-design for $t = m - d + 1$. □

We call an elliptic (2δ)-code Y in $\mathscr{Q}(2n,q)$ *maximal* if equality holds in Theorem 4.6. We shall see in Section 5 that maximal elliptic d-codes in $\mathscr{Q}(m,q)$ exist for all possible parameters.

4.4. Inner distributions of maximal codes. If Z is a subset of $\mathscr{S}(m,q)$ such that the bound in Theorem 4.3 holds with equality, then in many cases [20] and [21] give explicit expressions for the inner distribution of Z. These results carry over to subsets of $\mathscr{Q}(m,q)$ in the case that q is odd.

In this section we provide explicit expressions for the inner distributions of maximal d-codes in $\mathscr{Q}(m,q)$. We note that, once we know Proposition 4.4 for even q, the results in this section can be proved with methods that are very similar to those of [21, Section 3.3]. Hence the proofs in this section are sketched only.

Our first result holds for d-codes in $\mathscr{Q}(m,q)$, where d is odd.

Theorem 4.7. *If Y is a maximal $(2\delta+1)$-code in $\mathscr{Q}(2n+1,q)$, then its inner distribution $(a_i)_{i\in I}$ satisfies*

$$a_{2s-1} = \begin{bmatrix} n \\ s-1 \end{bmatrix} \sum_{j=0}^{s-\delta-1} (-1)^j q^{j(j-1)} \begin{bmatrix} s \\ j \end{bmatrix} \left(q^{(2n+1)(s-\delta-j)} - 1\right),$$

$$a_{2s,\tau} = \frac{1}{2} q^s \left(q^s + \tau\right) \begin{bmatrix} n \\ s \end{bmatrix} \sum_{j=0}^{s-\delta-1} (-1)^j q^{j(j-1)} \begin{bmatrix} s \\ j \end{bmatrix} \left(q^{(2n+1)(s-\delta-j)} - 1\right)$$

for $s > 0$. If Y is a maximal $(2\delta+1)$-code in $\mathscr{Q}(2n,q)$, then its inner distribution $(a_i)_{i\in I}$ satisfies

$$a_{2s-1,\tau} = \frac{1}{2}(q^{2s}-1) \begin{bmatrix} n \\ s \end{bmatrix} \sum_{j=0}^{s-\delta-1} (-1)^j q^{j(j-1)} \begin{bmatrix} s-1 \\ j \end{bmatrix} q^{(2n+1)(s-\delta-j-1)+2j},$$

$$\begin{aligned} a_{2s,\tau} = {} & \frac{1}{2} \begin{bmatrix} n \\ s \end{bmatrix} \sum_{j=0}^{s-\delta} (-1)^j q^{j(j-1)} \begin{bmatrix} s \\ j \end{bmatrix} \left(q^{(2n+1)(s-\delta-j)+2j} - 1\right) \\ & + \frac{\tau}{2} q^s \begin{bmatrix} n \\ s \end{bmatrix} \sum_{j=0}^{s-\delta-1} (-1)^j q^{j(j-1)} \begin{bmatrix} s \\ j \end{bmatrix} \left(q^{(2n+1)(s-\delta-j)+2(j-s)} - 1\right) \end{aligned}$$

for $s > 0$.

Proof. If Y is a maximal d-code in $\mathscr{Q}(m,q)$, where d is odd, then Theorems 4.3 and 4.5 imply that Y is a t-design for

$$t = 2\left(\left\lfloor \frac{m+1}{2} \right\rfloor - \frac{d-1}{2}\right).$$

For odd q, the theorem is then [21, Theorem 3.9] and its proof relies just on Proposition 4.2. For even q, the proof is almost identical if we use Proposition 4.4 instead of Proposition 4.2. □

The next result holds for maximal d-codes in $\mathscr{Q}(m,q)$ when q is even and d is even. In this case, the inner distribution is only partially determined. It is not clear whether there exist such d-codes with different inner distributions.

Theorem 4.8. *If q is even and Y is a maximal (2δ)-code in $\mathscr{Q}(m,q)$, then its inner distribution $(a_i)_{i\in I}$ satisfies*

$$a_{2s,1}+a_{2s,-1}+a_{2s+1}=\begin{bmatrix}n\\ s\end{bmatrix}\sum_{j=0}^{s-\delta}(-1)^j q^{j(j-1)}\begin{bmatrix}s\\ j\end{bmatrix}\big(c^{s-\delta-j+1}-1\big)$$

for $s>0$, where $n=\lfloor m/2\rfloor$ and $c=q^{m(m-1)/(2n)}$.

Proof. Let B_s and C'_r be defined as in Proposition 4.4, so that

$$C'_r=\sum_s F_r^{(m)}(s)B_s.$$

In particular $B_s=a_{2s,1}+a_{2s,-1}+a_{2s+1}$. If Y is a maximal (2δ)-code in $\mathscr{Q}(m,q)$, then we conclude from the proof of Theorem 4.5 that $C'_r=0$ for all r satisfying $1\leqslant r\leqslant n-\delta+1$. This gives enough equations to solve for the numbers B_s. The solution is given by [21, Lemma 3.8]. □

The final result of this section concerns maximal elliptic (2δ)-codes in $\mathscr{Q}(2n,q)$.

Theorem 4.9. *If Y is a maximal elliptic (2δ)-code in $\mathscr{Q}(2n,q)$, then its inner distribution $(a_i)_{i\in I}$ satisfies*

$$a_{2s-1}=\frac{1}{2}(q^{2s}-1)\begin{bmatrix}n\\ s\end{bmatrix}\sum_{j=0}^{s-\delta-1}(-1)^j q^{j(j-1)}\begin{bmatrix}s-1\\ j\end{bmatrix}\big(q^{2n(s-\delta-j-1)}q^{s+j-1}-1\big),$$

$$a_{2s,\tau}=\frac{1}{2}(q^s+\tau)\begin{bmatrix}n\\ s\end{bmatrix}\sum_{j=0}^{s-\delta}(-1)^j q^{j(j-1)}\begin{bmatrix}s\\ j\end{bmatrix}\big(q^{2n(s-\delta-j)}q^j-\tau\big)$$

for $s>0$.

Proof. If Y is a maximal elliptic (2δ)-code in $\mathscr{Q}(2n,q)$, then by Theorem 4.6 we have $|Y|=q^{2n(n-\delta+1/2)}$ and Y is a $(2n-2\delta+1)$-design. The proof is then identical to that of the first part of [21, Proposition 3.10]. □

5. Constructions

In this section we provide constructions of maximal d-codes in $\mathscr{S}(m,q)$ and $\mathscr{Q}(m,q)$ using field extensions of $\mathbb{F}_q$. Throughout this section we take $V=\mathbb{F}_{q^m}$ and use the *relative trace function* $\mathrm{Tr}_m:\mathbb{F}_{q^m}\to\mathbb{F}_q$, which is given by

$$\mathrm{Tr}_m(y)=\sum_{i=1}^{m}y^{q^i}.$$

5.1. Canonical representations. In what follows we give canonical representations of quadratic forms Q and symmetric bilinear forms S on $\mathbb{F}_{q^m}$ and describe the pairing $\langle Q,S\rangle$ in terms of these representations.

Theorem 5.1. *Let $Q\in\mathscr{Q}(m,q)$ be a quadratic form and let $S\in\mathscr{S}(m,q)$ be a symmetric bilinear form.*

(1) *If m is odd, say $m=2n-1$, then there exist unique $f_0,\dots,f_{n-1}\in\mathbb{F}_{q^m}$ and $g_0,\dots,g_{n-1}\in\mathbb{F}_{q^m}$ such that Q is given by*

$$Q(x)=\sum_{i=0}^{n-1}\mathrm{Tr}_m(f_i x^{q^i+1})$$

and S is given by

$$S(x,y) = \mathrm{Tr}_m(g_0xy) + \sum_{i=1}^{n-1} \mathrm{Tr}_m(g_i(xy^{q^i} + x^{q^i}y)).$$

Moreover, there are $\mathbb{F}_q$-bases for $\mathbb{F}_{q^m}$ such that with respect to these bases we have

$$\langle Q, S\rangle = \chi\left(\sum_{i=0}^{n-1} \mathrm{Tr}_m(f_ig_i)\right).$$

(2) *If m is even, say $m = 2n$, then there exist unique $f_0, \ldots, f_{n-1} \in \mathbb{F}_{q^m}$ and $g_0, \ldots, g_{n-1} \in \mathbb{F}_{q^m}$ and $f_n, g_n \in \mathbb{F}_{q^n}$ such that Q is given by*

$$Q(x) = \sum_{i=0}^{n-1} \mathrm{Tr}_m(f_ix^{q^i+1}) + \mathrm{Tr}_n(f_nx^{q^n+1})$$

and S is given by

$$S(x,y) = \mathrm{Tr}_m(g_0xy) + \sum_{i=1}^{n-1} \mathrm{Tr}_m(g_i(xy^{q^i} + x^{q^i}y)) + \mathrm{Tr}_m(g_nxy^{q^n}).$$

Moreover, there are $\mathbb{F}_q$-bases for $\mathbb{F}_{q^m}$ such that with respect to these bases we have

$$\langle Q, S\rangle = \chi\left(\sum_{i=0}^{n-1} \mathrm{Tr}_m(f_ig_i) + \mathrm{Tr}_n(f_ng_n)\right).$$

To prove Theorem 5.1, we require some notation and a lemma. Given a linearised polynomial $L \in \mathbb{F}_{q^m}[X]$ of the form

$$L = \sum_{k=0}^{m-1} c_kX^{q^k}, \tag{41}$$

we associate with L its *Dickson matrix* D_L, given by $(D_L)_{1\leqslant i,j\leqslant m} = c_{j-i}^{q^i}$, where the index of c_k is taken modulo m. Henceforth the entries of an $m \times m$ matrix M are denoted by M_{ij}, where $1 \leqslant i, j \leqslant m$.

Lemma 5.2. *Let $L \in \mathbb{F}_{q^m}[X]$ be the linearised polynomial* (41)*. Let $\{\xi_1, \xi_2, \ldots, \xi_m\}$ be an $\mathbb{F}_q$-basis for $\mathbb{F}_{q^m}$ and let $M \in \mathbb{F}_q^{m\times m}$ be given by $M_{ij} = \mathrm{Tr}_m(\xi_iL(\xi_j))$. Then we have*

$$M = PD_LP^T,$$

where $P \in \mathbb{F}_q^{m\times m}$ is given by $P_{ij} = \xi_i^{q^j}$.

Proof. We can write $M = PR$, where $R_{ij} = L(\xi_j)^{q^i}$. For every $x \in \mathbb{F}_{q^m}$, we have

$$L(x)^{q^i} = \sum_{k=1}^{m} c_{k-i}^{q^i}\, x^{q^k},$$

where the index is taken modulo m. We conclude that $R = D_LP^T$, as required. □

We now prove Theorem 5.1.

Proof of Theorem 5.1. It is easy to see that the possible choices for the f_i's and the g_i's yield $q^{m(m+1)/2}$ quadratic forms and $q^{m(m+1)/2}$ symmetric bilinear forms. In order to prove that these are distinct, it is sufficient to show that Q or S is the zero form if and only if the f_i's are all zero or the g_i's are all zero, respectively. For $\mathscr{S}(m,q)$ and odd m, this is accomplished by the proof of Theorem 5.3. The other

cases can be proved similarly, which we leave to the reader. This proves the existence and uniqueness of the f_i's and the g_i's.

It remains to prove the expressions for the pairing $\langle Q, S\rangle$. We present the proof only in the case that m is odd. Slight modifications also give a proof for even m. Let $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ and $\{\beta_1, \beta_2, \dots, \beta_m\}$ be a pair of dual $\mathbb{F}_q$-bases for $\mathbb{F}_{q^m}$, that is

$$\mathrm{Tr}_m(\alpha_i\beta_j) = \delta_{ij} \quad \text{for all } i, j.$$

We use the former basis to associate cosets of alternating matrices with quadratic forms and the latter to associate symmetric matrices with symmetric bilinear forms. It will be convenient to define the $m\times m$ matrices U and V by $U_{ij} = \alpha_i^{q^j}$ and $V_{ij} = \beta_i^{q^j}$. Notice that the duality of the two involved bases implies $UV^T = I$, and so $U^TV = I$.

Define the linearised polynomials

$$F_0 = f_0X, \quad F_1 = \sum_{i=1}^{n-1}(f_iX^{q^i} + f_i^{q^{m-i}}X^{q^{m-i}}), \quad F_2 = \sum_{i=1}^{n-1} f_iX^{q^i},$$

$$G_0 = g_0X, \quad G_1 = \sum_{i=1}^{n-1}(g_iX^{q^i} + g_i^{q^{m-i}}X^{q^{m-i}}).$$

Then we have

$$S(x, y) = \mathrm{Tr}_m(x(G_0(y) + G_1(y)))$$

and so the matrix B of S is given by $B = B_0 + B_1$, where

$$(B_0)_{ij} = \mathrm{Tr}_m(\beta_iG_0(\beta_j)),$$
$$(B_1)_{ij} = \mathrm{Tr}_m(\beta_iG_1(\beta_j)).$$

To associate cosets of alternating matrices with quadratic forms, we distinguish the cases that q is odd or even.

For odd q, let A be the unique symmetric matrix associated with the quadratic form Q. From (2) we find that this matrix is given by

$$\begin{aligned} A_{ij} &= \tfrac{1}{2}(Q(\alpha_i + \alpha_j) - Q(\alpha_i) - Q(\alpha_j)) \\ &= \mathrm{Tr}_m(\alpha_i(F_0(\alpha_j) + \tfrac{1}{2}F_1(\alpha_j))). \end{aligned}$$

Write $F = F_0 + \frac{1}{2}F_1$ and $G = G_0 + G_1$ and use Lemma 5.2 to obtain

$$\mathrm{tr}(AB) = \mathrm{tr}(UD_FU^TVD_GV^T) = \mathrm{tr}(D_FD_G),$$

and therefore

$$\mathrm{tr}(AB) = \sum_{i=0}^{n-1} \mathrm{Tr}_m(f_ig_i),$$

as required.

For even q, let A' be the unique upper triangular matrix associated with Q. From (2) we find that this matrix is given by $A'_{ii} = Q(\alpha_i)$ and $A'_{ij} = Q(\alpha_i+\alpha_j)-Q(\alpha_i)-Q(\alpha_j)$ for $i < j$. In fact, it is more convenient to work with a slightly different matrix of Q, namely $A = A_0 + A_1$, where A_0 and A_1 are given by

$$(A_0)_{ij} = \mathrm{Tr}_m(\alpha_iF_0(\alpha_j))$$

$$(A_1)_{ij} = \begin{cases} \mathrm{Tr}_m(\alpha_iF_1(\alpha_j)) & \text{for } i < j \\ \mathrm{Tr}_m(\alpha_iF_2(\alpha_j)) & \text{for } i = j \\ 0 & \text{otherwise.} \end{cases} \tag{42}$$

Notice that $A - A'$ is alternating, which is in fact the off-diagonal part of A_0. Therefore A and A' represent the same quadratic form. We have

$$\operatorname{tr}(AB) = \operatorname{tr}(A_0B_0) + \operatorname{tr}(A_1B_1) + \operatorname{tr}(A_0B_1) + \operatorname{tr}(A_1B_0).$$

Using Lemma 5.2 we have

$$\operatorname{tr}(A_0B_0) = \operatorname{tr}(UD_{F_0}U^TVD_{G_0}V^T) = \operatorname{tr}(D_{F_0}D_{G_0}) = \operatorname{Tr}_m(f_0g_0).$$

Now define an inner product on alternating matrices in $\mathbb{F}_q^{m\times m}$ by

$$(X, Y) = \sum_{i<j} X_{ij}Y_{ij}.$$

This inner product satisfies

$$(WXW^T, Y) = (X, W^TYW)$$

for every $W \in \mathbb{F}_q^{m\times m}$. Using this property and Lemma 5.2, we obtain

$$\operatorname{tr}(A_1B_1) = (A_1 + A_1^T, B_1) = (UD_{F_1}U^T, VD_{G_1}V^T) = (D_{F_1}, D_{G_1}),$$

and therefore

$$\operatorname{tr}(A_1B_1) = \sum_{i=1}^{n-1} \operatorname{Tr}_m(f_ig_i).$$

Now, since A_0 is symmetric and B_1 is alternating, we have $\operatorname{tr}(A_0B_1) = 0$. From Lemma 5.2, we find that $B_0 = VD_{G_0}V^T$, where D_{G_0} is a diagonal matrix. We claim that $A_1 = UEU^T$, where E has only zeros on the main diagonal. This implies that

$$\operatorname{tr}(A_1B_0) = \operatorname{tr}(UEU^TVD_{G_0}V^T) = \operatorname{tr}(ED_{G_0}) = 0,$$

and so completes the proof.

It remains to prove the claim. The required matrix E is given by $E = V^TA_1V$, and so for every i, we have using (42)

$$\begin{aligned}
E_{ii} &= \sum_{k,\ell} \beta_k^{q^i} (A_1)_{k\ell}\, \beta_\ell^{q^i} \\
&= \sum_k \beta_k^{q^i} \operatorname{Tr}_m(\alpha_k F_2(\alpha_k))\beta_k^{q^i} + \sum_{k<\ell} \beta_k^{q^i} \operatorname{Tr}_m(\alpha_k F_1(\alpha_\ell))\beta_\ell^{q^i} \\
&= \sum_k \beta_k^{q^i} \operatorname{Tr}_m(\alpha_k F_2(\alpha_k))\beta_k^{q^i} + \sum_{k<\ell} \beta_k^{q^i} \operatorname{Tr}_m(\alpha_k F_2(\alpha_\ell) + \alpha_\ell F_2(\alpha_k))\beta_\ell^{q^i} \\
&= \sum_{k,\ell} \beta_k^{q^i} \operatorname{Tr}_m(\alpha_k F_2(\alpha_\ell))\beta_\ell^{q^i} \\
&= v_i^TUD_{F_2}U^Tv_i = (v_i^TU)D_{F_2}(v_i^TU)^T,
\end{aligned}$$

where v_i is the i-th column of V. Since $V^TU = I$, we find that the main diagonal of E equals the main diagonal of D_{F_2}, which is zero. This proves the claim. □

5.2. The constructions. We now give constructions of maximal d-codes in $\mathscr{S}(m, q)$ and $\mathscr{Q}(m, q)$. We begin with recalling constructions from [20] and [21] of additive d-codes in $\mathscr{S}(m, q)$.

Theorem 5.3 ([21, Theorem. 4.4]). *Let d be an integer with the same parity as m satisfying $1 \leqslant d \leqslant m$ and let Z be the subset of $\mathscr{S}(m, q)$ formed by the symmetric*

bilinear forms

$$S : \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} \to \mathbb{F}_q$$
$$S(x,y) = \mathrm{Tr}_m(g_0 xy) + \sum_{i=1}^{(m-d)/2} \mathrm{Tr}_m(g_i(xy^{q^i} + x^{q^i} y)), \quad g_i \in \mathbb{F}_{q^m}.$$

Then Z is an additive d-code in $\mathscr{S}(m,q)$ of size $q^{m(m-d+2)/2}$. In particular, Z is a maximal d-code in $\mathscr{S}(m,q)$ for odd m and is maximal among additive d-codes in $\mathscr{S}(m,q)$ for even m.

Whenever $m-d$ is odd, Theorem 5.3 gives $(d+2)$-codes Z in $\mathscr{S}(m+1,q)$ for which equality holds in Theorem 4.3. Let W be an m-dimensional subspace of $V(m+1,q)$ and define the *punctured* set (with respect to W) of Z to be

$$Z^* = \big\{S|_W : S \in Z\big\},$$

where $S|_W$ is the restriction of S onto W. Then Z^* is a d-code in $\mathscr{S}(m,q)$ for which again equality holds in Theorem 4.3. This shows that Z^* is a maximal d-code in $\mathscr{S}(m,q)$ for odd d and is maximal among additive d-codes in $\mathscr{S}(m,q)$ for even d.

For odd q, Theorem 5.1 of course also gives corresponding sets of quadratic forms by associating a quadratic form Q with S via $Q(x) = \frac{1}{2}S(x,x)$. It therefore remains to give constructions of maximal d-codes in $\mathscr{Q}(m,q)$ for even q. The following consequence of Theorems 5.1 and 5.3 gives a construction for d-codes in $\mathscr{Q}(m,q)$ when both m and d are odd (and where q can have either parity).

Theorem 5.4. *Let m and d be odd integers satisfying $1 \leqslant d \leqslant m$ and let Y be the subset of $\mathscr{Q}(m,q)$ formed by the quadratic forms*

$$Q : \mathbb{F}_{q^m} \to \mathbb{F}_q$$
$$Q(x) = \sum_{i=(d-1)/2}^{(m-1)/2} \mathrm{Tr}_m(f_i x^{q^i+1}), \quad f_i \in \mathbb{F}_{q^m}.$$

Then Y is additive and a maximal d-code in $\mathscr{Q}(m,q)$ of size $q^{m(m-d+2)/2}$.

Proof. It is plain that Y is additive and has size $q^{m(m-d+2)/2}$. From Theorems 5.1 and 5.3 we find that the annihilator of Y° of Y is a maximal $(m-d+3)$-code in $\mathscr{S}(m,q)$. Theorem 4.3 implies that Y° is a $(d-1)$-design and Theorem 4.1 then implies that Y is a d-code. From Theorem 4.5 we find hat Y is maximal. □

Whenever d is odd and m is even, Theorem 5.4 gives maximal $(d+2)$-codes Y in $\mathscr{Q}(m+1,q)$. In fact, Theorem 4.5 implies that Y is also a maximal $(d+1)$-code in $\mathscr{Q}(m+1,q)$. Let W be an m-dimensional subspace of $V(m+1,q)$ and define the *punctured* set (with respect to W) of Y to be

$$Y^* = \big\{Q|_W : Q \in Y\big\},$$

where $Q|_W$ is the restriction of Q onto W. Then Y^* is a maximal d-code in $\mathscr{Q}(m,q)$. This leaves the case that m and d are both even. In this case we have the following construction, which identifies V with $\mathbb{F}_{q^{m-1}} \times \mathbb{F}_q$ and is essentially contained in [7].

THEOREM 5.5. *Let q be even, let m and d be even integers satisfying $1 \leqslant d \leqslant m$, and let Y be the subset of $\mathscr{Q}(m,q)$ formed by the quadratic forms*

$$Q : \mathbb{F}_{q^{m-1}} \times \mathbb{F}_q \to \mathbb{F}_q$$

$$Q(x,u) = \sum_{i=1}^{m/2-1} \operatorname{Tr}_{m-1}\left((f_0 x)^{q^i+1}\right) + u \operatorname{Tr}_{m-1}(f_0 x) + \sum_{i=1}^{(m-d)/2} \operatorname{Tr}_{m-1}\left(f_i x^{q^i+1}\right),$$

where $f_i \in \mathbb{F}_{q^{m-1}}$. Then Y is a maximal d-code in $\mathscr{Q}(m,q)$ of size $q^{(m-1)(m-d+2)/2}$.

Proof. The quadratic form Q polarises to the bilinear form

$$\operatorname{Tr}_{m-1}(f_0^2 xy + f_0 y \operatorname{Tr}_{m-1}(f_0 x) + f_0(uy+vx)) + \sum_{i=1}^{(m-d)/2} \operatorname{Tr}_{m-1}(f_i(xy^{q^i} + x^{q^i} y)).$$

It is known [7, Theorem 9] that the difference between two such forms for distinct $(f_0, f_1, \ldots, f_{(m-d)/2})$ has rank at least d. Therefore Y is a d-code in $\mathscr{Q}(m,q)$ of size $q^{(m-1)(m-d+2)/2}$, hence a maximal d-code in $\mathscr{Q}(m,q)$ by Theorem 4.5. □

We close this section by giving a construction for maximal elliptic d-codes in $\mathscr{Q}(m,q)$.

THEOREM 5.6. *Let m be even and write $m = 2n$. Let δ be an integer satisfying $1 \leqslant \delta \leqslant n$ and let Y be the subset of $\mathscr{Q}(m,q)$ formed by the quadratic forms*

$$Q : \mathbb{F}_{q^m} \to \mathbb{F}_q$$

$$Q(x) = \sum_{i=\delta}^{n-1} \operatorname{Tr}_m(f_i x^{q^i+1}) + \operatorname{Tr}_n(f_n x y^{q^n}), \quad f_i \in \mathbb{F}_{q^m}, f_n \in \mathbb{F}_{q^n}.$$

Then Y is a maximal elliptic (2δ)-code in $\mathscr{Q}(m,q)$ of size $q^{m(n-\delta+1/2)}$.

Proof. It is plain that Y is additive. A straightforward computation gives

$$Q(x+y) - Q(x) - Q(y) = \operatorname{Tr}_m(yL(x)),$$

where

$$L(x) = f_n x^{q^n} + \sum_{i=\delta}^{n-1} \left(f_i x^{q^i} + f_i^{q^{2n-i}} x^{q^{2n-i}} \right).$$

Since $L(x^{q^{2n-\delta}})$ is induced by a polynomial of degree at most $2n - 2\delta$, we find that Q has rank at least 2δ, unless $f_\delta = \cdots = f_n = 0$. Hence Y is (2δ)-code of size $q^{m(n-\delta+1/2)}$.

Let $(a_i)_{i \in I}$ be the inner distribution of Y and let A_s, A'_r, C_s, and B'_r be as defined in Proposition 4.4. By Theorems 5.1 and 5.3, the annihilator Y° of Y is a $(2n-2\delta+2)$-code in $\mathscr{S}(m,q)$. Thus Theorem 4.1 implies that $A'_r = B'_r = 0$ for all r satisfying $1 \leqslant r \leqslant n - \delta$. As in the proof of Theorem 4.6, we find that

$$\begin{bmatrix} n \\ \delta \end{bmatrix} (q^\delta A'_0 + B'_0) = q^{(m+1)(n-\delta)} q^\delta \left(\begin{bmatrix} n \\ \delta \end{bmatrix} (A_0 + q^\delta C_0) + A_\delta + q^\delta C_\delta \right).$$

Since $A'_0 = B'_0 = |Y| = q^{m(n-\delta+1/2)}$ and $A_0 = C_0 = 1$, we conclude that

$$A_\delta + q^\delta C_\delta = 0.$$

We have $A_\delta + q^\delta C_\delta = 2a_{2\delta,1} + a_{2\delta-1}$ by definition and $a_{2\delta-1} = 0$ since Y is a (2δ)-code. Therefore $a_{2\delta,1} = 0$, and so Y is an elliptic (2δ)-code, hence a maximal elliptic (2δ)-code in $\mathscr{Q}(m,q)$ by Theorem 4.6. □

6. Applications to classical coding theory

In this section we construct classical error-correcting codes over finite fields from subsets of $\mathscr{Q}(m,q)$, extending results from [21] for odd q.

A *code* over $\mathbb{F}_q$ of *length* n is a subset of $\mathbb{F}_q^n$; such a code is *additive* if it is a subgroup of $(\mathbb{F}_q^n,+)$. The (Hamming) *weight* of $c\in\mathbb{F}_q^n$, denoted by $\mathrm{wt}(c)$, is the number of nonzero entries in c. This weight induces a distance on $\mathbb{F}_q^n$ and the smallest distance between two distinct elements of a code $\mathcal{C}$ is called the *minimum distance* of $\mathcal{C}$. We associate with a code $\mathcal{C}$ the polynomials

$$\alpha(z)=\sum_{c\in\mathcal{C}} z^{\mathrm{wt}(c)}$$

and

$$\beta(z)=\frac{1}{|\mathcal{C}|}\sum_{b,c\in\mathcal{C}} z^{\mathrm{wt}(c-b)},$$

which are called the *weight enumerator* and the *distance enumerator* of $\mathcal{C}$, respectively. Note that, if $\mathcal{C}$ is additive, then its weight enumerator coincides with its distance enumerator.

As usual, we let $V=V(m,q)$ be an m-dimensional $\mathbb{F}_q$-vector space and $\mathscr{Q}(m,q)$ the set of quadratic forms on V. Since for every quadratic form $Q:V\to\mathbb{F}_q$ we have $Q(0)=0$, we shall identify functions from V to $\mathbb{F}_q$ with vectors $\mathbb{F}_q^{V^*}$, where $V^*=V-\{0\}$.

Let $R_q(1,m)^*$ be the set of all q^{m+1} affine functions from V to $\mathbb{F}_q$. This code has length q^m-1 and is the punctured version of the generalised first-order Reed–Muller code $R_q(1,m)$ of length q^m. If we identify V with $\mathbb{F}_{q^m}$, then $R_q(1,m)^*$ consists of the functions

$$\begin{aligned}\mathbb{F}_{q^m}&\to\mathbb{F}_q\\ x&\mapsto \mathrm{Tr}_m(ax)+c,\quad a\in\mathbb{F}_{q^m},\ c\in\mathbb{F}_q.\end{aligned}$$

We shall associate codes with subsets Y of $\mathscr{Q}(m,q)$ by taking cosets of $R_q(1,m)^*$ with coset representatives from Y. Care must be taken in the case that $q=2$ since $x^2=x$ for all $x\in\mathbb{F}_2$, which implies that every quadratic form in $\mathscr{Q}(m,2)$ of rank 1 is in fact also a linear function. Accordingly, we define a subset Y of $\mathscr{Q}(m,q)$ to be *nondegenerate* if $q>2$ or if $q=2$ and Y contains no forms of rank 1. For every nondegenerate subset Y of $\mathscr{Q}(m,q)$, we define the code $\mathcal{C}(Y)$ of size $q^{m+1}\,|Y|$ by

$$\mathcal{C}(Y)=\bigcup_{Q\in Y} Q+R_q(1,m)^*.$$

If Y equals $\mathscr{Q}(m,q)$, then $\mathcal{C}(Y)$ is the punctured version $R_q(2,m)^*$ of the generalised second-order Reed–Muller code $R_q(2,m)$ of length q^m.

For $i\in I$, define the polynomial

$$\omega_i(z)=n_1z^{w_1}+n_2z^{w_2}+n_3z^{w_3}+n_4z^{w_4}+n_5z^{w_5}+n_6z^{w_6},$$

where

$$\begin{aligned}
w_1&=q^{m-1}(q-1)-q^{m-s-1}-1 & n_1&=\tfrac12(q^{2s}(q-1)-q^s)(q-1)\\
w_2&=q^{m-1}(q-1)-q^{m-s-1} & n_2&=\tfrac12(q^{2s}+q^s)(q-1)\\
w_3&=q^{m-1}(q-1)-1 & n_3&=(q^m-q^{2s}(q-1))(q-1)\\
w_4&=q^{m-1}(q-1) & n_4&=q^m-q^{2s}(q-1)\\
w_5&=q^{m-1}(q-1)+q^{m-s-1}-1 & n_5&=\tfrac12(q^{2s}(q-1)+q^s)(q-1)\\
w_6&=q^{m-1}(q-1)+q^{m-s-1} & n_6&=\tfrac12(q^{2s}-q^s)(q-1)
\end{aligned}$$

for $i = 2s+1$ and

$$\begin{aligned}
w_1 &= (q^{m-1} - \tau q^{m-s-1})(q-1) - 1 & n_1 &= (q^{2s-1} - \tau q^{s-1})(q-1)\\
w_2 &= (q^{m-1} - \tau q^{m-s-1})(q-1) & n_2 &= q^{2s-1} + \tau q^{s-1}(q-1)\\
w_3 &= q^{m-1}(q-1) - 1 & n_3 &= (q^m - q^{2s})(q-1)\\
w_4 &= q^{m-1}(q-1) & n_4 &= q^m - q^{2s}\\
w_5 &= q^{m-1}(q-1) + \tau q^{m-s-1} - 1 & n_5 &= (q^{2s-1}(q-1) + \tau q^{s-1})(q-1)\\
w_6 &= q^{m-1}(q-1) + \tau q^{m-s-1} & n_6 &= (q^{2s-1} - \tau q^{s-1})(q-1)
\end{aligned}$$

for $i = (2s, \tau)$. The following result relates the polynomial $\omega_i(z)$ with the weight enumerator of cosets of $R_q(1,m)^*$. This result can be proved using the standard theory of quadratic forms. (Recall that $\mathscr{Q}_{2s+1}$ contains all quadratic forms of rank $2s+1$ and $\mathscr{Q}_{2s,\tau}$ contains all quadratic forms of rank $2s$ and type τ.)

LEMMA 6.1 ([15, Propositions 4.1 and 5.1]). *Let $Q \in \mathscr{Q}(m,q)$ be a quadratic form with $Q \in \mathscr{Q}_i$. Then $\omega_i(z)$ is the weight enumerator of the coset $Q + R_q(1,m)^*$.*

Now, since $R_q(1,m)^*$ is additive, the distance enumerator of $\mathcal{C}(Y)$ equals

$$\frac{1}{|Y|} \sum_{b,c \in Y} \sum_{a \in R_q(1,m)^*} z^{\mathrm{wt}(a+c-b)}.$$

The inner sum is the weight enumerator of the coset $c-b+R_q(1,m)^*$ and so Lemma 6.1 gives the distance enumerator of $\mathcal{C}(Y)$ in terms of the inner distribution of Y.

THEOREM 6.2. *Let Y be a nondegenerate subset of $\mathscr{Q}(m,q)$ with inner distribution $(a_i)_{i \in I}$. Then the distance enumerator of $\mathcal{C}(Y)$ is $\sum_{i \in I} a_i \omega_i(z)$.*

If Y equals $\mathscr{Q}(m,q)$, then Theorem 4.7 with $\delta = 0$ and Theorem 6.2 give the distance enumerator of $R_q(2,m)^*$. This complements results of McEliece [19], who determined the distance enumerator of the second-order generalised Reed–Muller code $R_q(2,m)$ itself. This latter result can also be recovered from Theorem 4.7 and a slightly modified version of Theorem 6.2.

Now let m and d be two integers of equal parity satisfying $1 \leqslant d \leqslant m$. If d is odd, let Y be a nondegenerate maximal d-code in $\mathscr{Q}(m,q)$ and if d is even, let Y be a maximal elliptic d-code in $\mathscr{Q}(m,q)$. Writing $\delta = \lfloor d/2 \rfloor$, we have by Theorems 4.3, 4.5, and 4.6

$$|Y| = q^{m(m-2\delta+1)/2}.$$

The code $\mathcal{C}(Y)$ has length $q^m - 1$, cardinality $q^{m(m-2\delta+3)/2+1}$, and minimum distance

$$q^{m-1}(q-1) - q^{m-\delta-1} - 1. \tag{43}$$

The distance enumerator of $\mathcal{C}(Y)$ is determined by Theorems 6.2 and 4.7 for odd d and by Theorems 6.2 and 4.9 for even d.

Now assume that Y is obtained from the specific constructions in Theorems 5.4 and 5.6, according to whether d is odd or even, respectively. Then $\mathcal{C}(Y)$ is a linear code and, in many cases, $\mathcal{C}(Y)$ is an optimal linear code or has the same parameters as the best known linear code [12]. Generalising work of Berlekamp [4], it was shown by Li [15, Proposition 2.5] that if

$$\frac{m}{3} \leqslant \delta \leqslant \frac{m}{2},$$

then $\mathcal{C}(Y)$ is a narrow-sense primitive BCH code of designed minimum distance (43). Hence, in this case, the true minimum distance of $\mathcal{C}(Y)$ equals its designed minimum distance. This recovers principal results of [4] for $q = 2$ and of [15] for odd q. Using

the results of [21] and additional arguments, the distance enumerator of $\mathcal{C}(Y)$ was obtained in [15] for odd q. Using entirely different methods, the distance enumerator of the extended version of $\mathcal{C}(Y)$ was also obtained for $q = 2$ in [4]. Our results give, in a uniform way, the distance enumerator of $\mathcal{C}(Y)$ for every prime power q.

Berlekamp [4] and Kasami [14] studied cyclic codes of the form $\mathcal{C}(Y)$ and related codes for other specific subsets Y of $\mathscr{Q}(m, 2)$. They determined the distance enumerators of such codes using methods that are completely different from our methods. Many of these results can be recovered and generalised to $q > 2$ using Theorems 4.7 and 4.9 together with Theorem 6.2 or some suitable modification.

We close this section by noting that, if Y is a maximal (2δ)-code in $\mathscr{Q}(m, q)$ and m and q are even, then $\mathcal{C}(Y)$ has length $q^m - 1$, cardinality $q^{m(m-2\delta+4)/2-(m-2\delta)/2}$, and minimum distance

$$(q^{m-1} - q^{m-\delta-1})(q-1) - 1.$$

For $q = 2$, the extended version of $\mathcal{C}(Y)$ is known as the Delsarte–Goethals code and for $2\delta = m$ it is known as the Kerdock code [18, Ch. 15].

Acknowledgements. I would like to thank Shuxing Li for helpful discussions on applications to error-correcting codes.

References

[1] Adrian A. Albert, *Symmetric and alternate matrices in an arbitrary field. I*, Trans. Am. Math. Soc. **43** (1938), no. 3, 386–436.

[2] Christine Bachoc, Oriol Serra, and Gilles Zémor, *An analogue of Vosper's theorem for extension fields*, Math. Proc. Camb. Philos. Soc. **163** (2017), no. 3, 423–452.

[3] Eiichi Bannai and Tatsuro Ito, *Algebraic combinatorics I: Association schemes*, The Benjamin/Cummings Publishing Co., Inc., Menlo Park, CA, 1984.

[4] Elwyn R. Berlekamp, *The weight enumerators for certain subcodes of the second order binary Reed–Muller codes*, Inf. Control **17** (1970), 485–500.

[5] Philippe Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. (1973), no. 10, vi+97.

[6] ———, *Properties and applications of the recurrence* $F(i+1, k+1, n+1) = q^{k+1}F(i, k+1, n) - q^k F(i, k, n)$, SIAM J. Appl. Math. **31** (1976), no. 2, 262–270.

[7] Philippe Delsarte and Jean-Marie Goethals, *Alternating bilinear forms over GF(q)*, J. Comb. Theory, Ser. A **19** (1975), no. 1, 26–50.

[8] Philippe Delsarte and Vladimir I. Levenshtein, *Association schemes and coding theory*, IEEE Trans. Inf. Theory **44** (1998), no. 6, 2477–2504.

[9] Leonard Eugene Dickson, *Linear groups: With an exposition of the Galois field theory*, Dover Publications, Inc., New York, 1958.

[10] Yoshimi Egawa, *Association schemes of quadratic forms*, J. Comb. Theory, Ser. A **38** (1985), no. 1, 1–14.

[11] Rongquan Feng, Yangxian Wang, Changli Ma, and Jianmin Ma, *Eigenvalues of association schemes of quadratic forms*, Discrete Math. **308** (2008), no. 14, 3023–3047.

[12] Markus Grassl, *Bounds on the minimum distance of linear codes and quantum codes*, Online available at `http://www.codetables.de`, 2007.

[13] Xiang-dong Hou, *The eigenmatrix of the linear association scheme on* $R(2, m)$, Discrete Math. **237** (2001), no. 1-3, 163–184.

[14] Tadao Kasami, *The weight enumerators for several classes of subcodes of the* 2*nd order binary Reed-Muller codes*, Inf. Control **18** (1971), 369–394.

[15] Shuxing Li, *The minimum distance of some narrow-sense primitive BCH codes*, SIAM J. Discrete Math. **31** (2017), no. 4, 2530–2569.

[16] J. H. van Lint and R. M. Wilson, *A course in combinatorics*, second ed., Cambridge University Press, Cambridge, 2001.

[17] F. Jessie MacWilliams, *Orthogonal matrices over finite fields*, Am. Math. Mon. **76** (1969), 152–164.

[18] F. Jessie MacWilliams and Neil J. A. Sloane, *The theory of error-correcting codes*, Amsterdam, The Netherlands: North Holland, 1977.

[19] Robert McEliece, *Quadratic forms over finite fields and second-order Reed-Muller codes*, JPL Space Programs Summary 37-58 **III** (1969), 28–33.
[20] Kai-Uwe Schmidt, *Symmetric bilinear forms over finite fields of even characteristic*, J. Comb. Theory, Ser. A **117** (2010), no. 8, 1011–1026.
[21] ———, *Symmetric bilinear forms over finite fields with applications to coding theory*, J. Algebr. Comb. **42** (2015), no. 2, 635–670.
[22] Miriam Schmidt, *Rank metric codes*, Master's thesis, University of Bayreuth (Germany), 2016.
[23] Dennis Stanton, *Some q-Krawtchouk polynomials on Chevalley groups*, Am. J. Math. **102** (1980), no. 4, 625–662.
[24] ———, *A partially ordered set and q-Krawtchouk polynomials*, J. Comb. Theory, Ser. A **30** (1981), no. 3, 276–284.
[25] Yangxian Wang, Chunsen Wang, Changli Ma, and Jianmin Ma, *Association schemes of quadratic forms and symmetric bilinear forms*, J. Algebr. Comb. **17** (2003), no. 2, 149–161.

Kai-Uwe Schmidt, Paderborn University, Department of Mathematics, Warburger Str. 100, 33098 Paderborn, Germany
E-mail : kus@math.upb.de