HERMITIAN RANK DISTANCE CODES

KAI-UWE SCHMIDT

Abstract. Let $X = X(n, q)$ be the set of $n \times n$ Hermitian matrices over $\mathbb{F}_{q^2}$. It is well known that $X$ gives rise to a metric translation association scheme whose classes are induced by the rank metric. We study $d$-codes in this scheme, namely subsets $Y$ of $X$ with the property that, for all distinct $A, B \in Y$, the rank of $A - B$ is at least $d$. We prove bounds on the size of a $d$-code and show that, under certain conditions, the inner distribution of a $d$-code is determined by its parameters. Except if $n$ and $d$ are both even and $4 \leq d \leq n - 2$, constructions of $d$-codes are given, which are optimal among the $d$-codes that are subgroups of $(X, +)$. This work complements results previously obtained for several other types of matrices over finite fields.

1. Introduction

Let $X$ be a set of matrices over a finite field with the same number of rows and columns. Given an integer $d$, we consider subsets $Y$ of $X$ with the property that, for all distinct $A, B \in Y$, the rank of $A - B$ is at least $d$. We call such a set a $d$-code in $X$. For fixed $d$, one is usually interested in $d$-codes containing as many elements as possible. Instances of this problem have been considered when $X$ is the set of unrestricted matrices [6], alternating matrices [7], and symmetric matrices [18], [19]. In all these cases, association schemes have been used critically to establish combinatorial properties of $d$-codes. In particular, bounds on the size of $d$-codes were obtained, which are often attained by constructions. Such results have found several applications in other branches of coding theory.

In this paper, we consider the case that $X = X(n, q)$ is the set of $n \times n$ Hermitian matrices over the finite field $\mathbb{F}_{q^2}$ with $q^2$ elements. Here, $q$ is a prime power and $\mathbb{F}_{q^2}$ is equipped with the involution $x \mapsto x^q$. We use the association scheme of Hermitian matrices to prove that every $d$-code $Y$ that is an additive subgroup of $(X, +)$ satisfies

$$|Y| \leq q^{n(n-d+1)}.$$  

In the case that $d$ is odd, we prove that the bound (1) also holds for $d$-codes that are not necessarily subgroups of $(X, +)$ and that, in case of equality in (1), the inner distribution of $Y$ is uniquely determined. In the case that $d$
is even, we show by example that the bound \((1)\) can be surpassed by \(d\)-codes not having the subgroup property and prove a larger bound that also holds for \(d\)-codes that are not necessarily subgroups of \((X,+)\). We also provide constructions of \(d\)-codes that are subgroups of \((X,+)\) and satisfy the bound \((1)\) with equality for all possible \(n\) and \(d\), except if \(n\) and \(d\) are both even and \(3 < d < n\).

It should be noted that related, but different, rank properties of sets of Hermitian matrices have been studied in \([9]\) and \([11]\).

2. The association scheme of Hermitian matrices

A (symmetric) association scheme with \(n\) classes is a finite set \(X\) together with \(n + 1\) nonempty relations \(R_0, R_1, \ldots, R_n\) that partition \(X \times X\) and satisfy:

(A1) \(R_0\) is the identity relation;

(A2) each of the relations is symmetric;

(A3) if \((x, y) \in R_k\), then the number of \(z \in X\) 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 \(y\).

For background on association schemes and connections to coding theory we refer to \([5]\), \([8]\), and \([16]\) and to \([15\), Chapter 21] and \([14\, Chapter 30]\) for gentle introductions.

Let \(q\) be a prime power and let \(\bar{x} = x^q\) be the conjugate of \(x \in F_{q^2}\). For a matrix \(A\) over \(F_{q^2}\), write \(A^*\) for the matrix obtained from \(A\) by conjugation of each entry and transposition. An \(n \times n\) matrix \(A\) with entries in \(F_{q^2}\) is Hermitian if \(A^* = A\). Let \(X = X(n, q)\) denote the set of \(n \times n\) Hermitian matrices over \(F_{q^2}\). Then \(X\) is an \(n^2\)-dimensional vector space over \(F_q\).

It is well known \([2\, Section 9.5]\) that \(X\) gives rise to an association scheme with \(n\) classes whose relations are given by

\[(A, B) \in R_i \iff \text{rank}(A - B) = i.\]

Alternatively these relations arise as orbits of a group action. Let \(G = GL_n(F_{q^2}) \times X\) be the semidirect product of the general linear group \(GL_n(F_{q^2})\) and \(X\), so that \(G\) acts transitively on \(X\) as follows

\[G \times X \to X\]

\[((T, D), A) \mapsto TAT^* + D.\]

The action of \(G\) extends to \(X \times X\) componentwise and so partitions \(X \times X\) into orbits, which are the relations defined above (see \([24\, Chapter 6]\), for example).

The relations just defined are invariant under the translation \((A, B) \mapsto (A + C, B + C)\), which is the defining property of a translation scheme. We shall make heavy use of the eigenvalues of this translation scheme, which are determined by the characters of \((X,+)\) \([8\, Section V]\). Let \(\chi : F_q \to \mathbb{C}\)
be a nontrivial character of \((\mathbb{F}_q,+)\) and, for \(A, B \in X\), write
\[
\langle A, B \rangle = \chi(\text{tr}(A^* B)),
\]
where \(\text{tr}\) is the matrix trace. For all \(A, A', B \in X\), we have
\[
\langle A + A', B \rangle = \langle A, B \rangle \langle A', B \rangle.
\]
Indeed, it is readily verified that the mapping \(A \mapsto \langle A, B \rangle\) ranges through all characters of \((X,+)\) as \(B\) ranges over \(X\). Let \(X_i\) be the subset of \(X\) containing all matrices of rank \(i\). For \(i, k \in \{0, 1, \ldots, n\}\), the numbers
\[
Q_k(i) = \sum_{A \in X_k} \langle A, B \rangle \quad \text{for } B \in X_i
\]
are independent of the choice of \(B\) and are the eigenvalues of the association scheme defined above (see [8, Section V] for details). For odd \(q\), these numbers have been determined by Carlitz and Hodges [3] and also by Stanton [21]. We shall require the eigenvalues in the following form
\[
Q_k(i) = (-1)^k \sum_{j=0}^{n} \left[ \begin{array}{c} n-j \\ n-k \end{array} \right] (-q)^{(k-j)+nj}.
\]
where, for integral \(m\) and \(\ell\) with \(\ell \geq 0\),
\[
\left[ \begin{array}{c} m \\ \ell \end{array} \right] = \prod_{i=1}^{\ell} (-q)^{m-i+1} - 1 / ((-q)^i - 1).
\]
is the negative \(q\)-binomial coefficient. A simple proof of the formula (4) for odd and even \(q\) is given in the appendix.

Equivalently, the eigenvalues are given by the \(n+1\) equations
\[
\sum_{k=0}^{j} \left[ \begin{array}{c} n-k \\ n-j \end{array} \right] Q_k(i) = (-1)^{(n+1)j} q^{nj} \left[ \begin{array}{c} n-i \\ j \end{array} \right],
\]
for \(j \in \{0, 1, \ldots, n\}\), which can be proved using the inversion formula
\[
\sum_{j=i}^{k} (-1)^{j-i} (-q)^{(j-i) \left[ \begin{array}{c} j \\ i \end{array} \right] \left[ \begin{array}{c} k \\ j \end{array} \right]} = \delta_{k,i}
\]
(see [7, (10)], for example), where \(\delta_{k,i}\) is the Kronecker \(\delta\)-function.

3. Combinatorial properties of subsets of \(X(n, q)\)

Let \(Y\) be a nonempty subset of \(X = X(n, q)\). The inner distribution of \(Y\) is the tuple \((A_0, A_1, \ldots, A_n)\) of rational numbers, which are given by
\[
A_i = \frac{|(Y \times Y) \cap R_i|}{|Y|}.
\]
In other words, \( A_i \) is the average number of pairs in \( Y \times Y \) whose difference has rank \( i \). Note that we always have \( A_0 = 1 \). The dual inner distribution of \( Y \) is the tuple \((A'_0, A'_1, \ldots, A'_n)\), whose entries are given by

\[
A'_k = \sum_{i=0}^{n} Q_k(i) A_i.
\]

Then \( A'_0 = |Y| \) and, as a consequence of a general property of association schemes (see [8, Theorem 3], for example), we have

\[
A'_k \geq 0 \quad \text{for each} \quad k \in \{0, 1, \ldots, n\}.
\]

Given an integer \( d \) satisfying \( 1 \leq d \leq n \), we say that \( Y \) is a \( d \)-code if \( A_1 = \ldots = A_{d-1} = 0 \). Equivalently, \( Y \) is a \( d \)-code if \( \text{rank}(A - B) \geq d \) for all distinct \( A, B \in Y \). We say that \( Y \) is a \( t \)-design if \( A'_1 = \ldots = A'_t = 0 \).

Now suppose that \( Y \) is a subgroup of \((X, +)\). In this case, we say that \( Y \) is additive. It is readily verified that, if \( Y \) has inner distribution \((A_0, A_1, \ldots, A_n)\), then \( A_i \) counts the number of matrices in \( Y \) of rank \( i \). We can associate with \( Y \) its dual

\[
Y^\perp = \{ B \in X : \langle A, B \rangle = 1 \text{ for each } A \in Y \},
\]

which is also additive and satisfies

\[
|Y| |Y^\perp| = |X|.
\]

It follows from a well known property of association schemes (see [8, Theorem 27], for example) that, if \( Y \) has dual inner distribution \((A'_0, A'_1, \ldots, A'_n)\), then the tuple

\[
\frac{1}{|Y|} (A'_0, A'_1, \ldots, A'_n)
\]

is the inner distribution of \( Y^\perp \). This implies in particular that the entries in the dual inner distribution of an additive set \( Y \) are divisible by \( |Y| \).

We use this fact and the property (8) to prove bounds on the size of \( d \)-codes.

**Theorem 1.** Every additive \( d \)-code \( Y \) in \( X(n, q) \) satisfies

\[
|Y| \leq q^{n(n-d+1)}.
\]

Moreover, if \( d \) is odd, then this bound also holds for arbitrary \( d \)-codes \( Y \) in \( X(n, q) \) and equality holds if and only if \( Y \) is an \((n-d+1)\)-design.

**Proof.** Let \((A_0, \ldots, A_n)\) and \((A'_0, \ldots, A'_n)\) be the inner distribution and the dual inner distribution of \( Y \), respectively. Use (7) and (5) to obtain, for each \( j \in \{0, 1, \ldots, n\} \),

\[
\sum_{k=j}^{n-j} \left( \frac{n-k}{n-j} \right) A'_k = \sum_{i=0}^{n} A_i \sum_{k=0}^{j} \left( \frac{n-k}{n-j} \right) Q_k(i) = (-1)^{(n+1)j} q^{nj} \sum_{i=0}^{n} A_i \left( \frac{n-i}{j} \right).
\]
Set \( j = n - d + 1 \) and use \( A_0 = 1 \) and \( A_1 = \cdots = A_{d-1} = 0 \) and the fact that \( \binom{m}{\ell} = 0 \) for \( m < \ell \) to find that

\[
\sum_{k=0}^{n-d+1} \binom{n-k}{d-1} A'_k = (-1)^{(n+1)(n-d+1)} q^{n(n-d+1)} \binom{n}{d-1}.
\]

(9)

If \( Y \) is additive, then the left-hand side is divisible by \( |Y| \), hence the right-hand side is divisible by \( Y \). Let \( p \) be the prime dividing \( q \). If \( Y \) is additive, then \( |Y| \) is a power of \( p \). It is readily verified that \( \binom{n}{d-1} \) is not divisible by \( p \), which implies that \( |Y| \) divides \( q^{n(n-d+1)} \), proving the bound for additive codes.

Now let \( d \) be odd. Note that the sign of \( \binom{m}{\ell} \) equals \((-1)^{\ell(m-\ell)} \). Hence, since \( d \) is odd, the binomial coefficients in the sum on the left-hand side of (9) are nonnegative. Since the numbers \( A'_k \) are also nonnegative by (8) and \( A'_0 = |Y| \), we find from (9) that

\[
\left[ \frac{n}{d-1} \right] |Y| \leq (-1)^{(n+1)(n-d+1)} q^{n(n-d+1)} \binom{n}{d-1},
\]

which gives the bound for general \( d \)-codes in the case that \( d \) is odd. Finally, equality occurs if and only if \( A'_1 = \cdots = A'_{n-d+1} = 0 \) in (9), which is equivalent to \( Y \) being an \((n-d+1)\)-design.

For even \( d \), the bound given in Theorem 1 cannot hold in general for arbitrary \( d \)-codes in \( X(n,q) \). For example, Theorem 1 asserts that the largest additive \( n \)-code in \( X(n,q) \) has size \( q^n \), whereas there exist \( n \)-codes in \( X(n,q) \) of size \( q^n + 1 \). This will be shown in Theorem 6.

The best bound we could prove for \( d \)-codes when \( d \) is even is contained in the following theorem.

**Theorem 2.** For even \( d \), every \( d \)-code \( Y \) in \( X(n,q) \) satisfies

\[
|Y| \leq (-1)^{n+1} q^{n(n-d+1)} \frac{((-q)^{n-d+2} - 1) + (-q)^n((-q)^{n-d+1} - 1)}{(-q)^{n-d+2} - (-q)^{n-d+1}}.
\]

**Proof.** Let \((A_0, \ldots, A_n)\) and \((A'_0, \ldots, A'_n)\) be the inner distribution and the dual inner distribution of \( Y \), respectively. As in the proof of Theorem 1, we have for each \( j \in \{0, 1, \ldots, n\} \),

\[
\sum_{k=0}^{j} \binom{n-k}{n-j} A'_k = (-1)^{(n+1)n} q^n \sum_{i=0}^{n} A_i \binom{n-i}{j}.
\]

Apply this identity with \( j = n - d + 1 \) and \( j = n - d + 2 \) to obtain, as in the proof of Theorem 1,

\[
\sum_{k=0}^{n-d+1} \binom{n-k}{d-1} A'_k = (-1)^{(n+1)(n-d+1)} q^{n(n-d+1)} \binom{n}{d-1},
\]

as desired. \( \square \)
and
\[
\sum_{k=0}^{n-d+2} \binom{n-k}{d-2} A'_k = (-1)^{(n+1)(n-d+2)} q^{n(n-d+2)} \left[ \binom{n}{d-2} \right].
\]
Notice that we can extend the summation range in the first identity up to \(n - d + 2\) without changing the value of the sum. Therefore, writing
\[
u_k = \binom{n-k}{d-1} \binom{n-1}{d-2} \quad \text{and} \quad v_k = \binom{n-k}{d-2} \binom{n-1}{d-1}
\]
and using that \(d\) is even, we find that
\[
(10) \quad (-1)^{n+1} \sum_{k=0}^{n-d+2} (u_k - v_k) A'_k
\]
\[
= q^{n(n-d+1)} \left( \binom{n}{d-1} \binom{n-1}{d-2} + (-q)^n \binom{n}{d-2} \binom{n-1}{d-1} \right).
\]
Next we show that the summands on the left-hand side are nonnegative. Since the sign of \(\binom{n}{\ell}\) is \((-1)^{\ell(\ell-n)}\), we find that \(\text{sign}(u_k) = (-1)^{n-k+1}\) and \(\text{sign}(v_k) = (-1)^n\). Therefore the left-hand side of (10) equals
\[
\sum_{k=0}^{n-d+2} \left( (-1)^k |u_k| + |v_k| \right) A'_k.
\]
We have
\[
\frac{u_k}{v_k} = \frac{(-q)^{n-k-d+2} - 1}{(-q)^{n-d+1} - 1},
\]
from which we find that \(|u_k| \leq |v_k|\) for each \(k \geq 1\). Hence the left-hand side of (10) can be bounded from below by
\[
(-1)^{n+1} \left( \binom{n}{d-1} \binom{n-1}{d-2} - \binom{n}{d-2} \binom{n-1}{d-1} \right) A'_0.
\]
Since this expression is positive and \(A'_0 = |Y|\), we obtain
\[
|Y| \leq (-1)^{n+1} q^{n(n-d+1)} \left[ \binom{n}{d-1} \binom{n-1}{d-2} + (-q)^n \binom{n}{d-2} \binom{n-1}{d-1} \right]
\]
\[
- \binom{n}{d-1} \binom{n-1}{d-2} - \binom{n}{d-2} \binom{n-1}{d-1}
\]
from which the desired bound can be obtained after elementary manipulations. \(\Box\)

For example, for \(d = n = 2\), the bound of Theorem 2 is
\[
|Y| \leq q^3 - q^2 + q.
\]
It is known that this bound is not tight; the largest 2-code in \(X(2,q)\) has size 5, 16, 24, 47 for \(q\) equal to 2, 3, 4, 5, respectively \[20\]. In these cases,
the optimal codes have been classified in [20]. For $q = 2$, the unique optimal construction arises as a special case of Theorem 6.

However, it is conjectured that Theorem 2 gives the optimal solution to the linear program, whose objective is to maximise

$$|Y| = \sum_{i=0}^{n} A_i,$$

subject to the nonnegativity of the numbers $A_i$ and $A'_i$ attached to $Y$. This has been checked with a computer for many small values of $n$ and $q$.

It is well known [11, Lemma 1] that there exists an $n$-code in $X(n, q)$ of size $N$ if and only if there exists a partial spread in the Hermitian polar space $H(2n - 1, q^2)$ of size $N + 1$. We can therefore obtain bounds for $n$-codes in $X(n, q)$ from bounds for partial spreads in $H(2n - 1, q^2)$ and vice versa. For example, Theorem 1 implies that, for odd $n$, a partial spread in $H(2n - 1, q^2)$ contains at most $q^n + 1$ elements. This gives another proof of a theorem due to Vanhove [22], [23]. In the other direction, from a result due to De Beule, Klein, Metsch, and Storme [1] we obtain

$$|Y| \leq \frac{q(q^2 + 1)}{2}$$

for every 2-code $Y$ in $X(2, q)$. This bound is tight for $q \in \{2, 3\}$. From a result due to Ihringer [12] we have

$$|Y| \leq \frac{q^{2n} - 1}{q + 1}$$

for every $n$-code in $X(n, q)$, which can be proved more directly using [12, Corollary 3.2] together with the explicit knowledge of the eigenvalues (13), in particular (14) and (15) for $k = 1$. This bound is slightly better than the corresponding bound $|Y| \leq q^{2n-1} - q^n + q^{n-1}$ of Theorem 2. Some improved bounds for $n$-codes in $X(n, q)$ in the case that $q$ is not a prime can be obtained from [13].

Our final result of this section gives the inner distribution of a $d$-code, provided that it is also an $(n - d)$-design.

**Theorem 3.** If $Y$ is a $d$-code and an $(n - d)$-design in $X(n, q)$, then its inner distribution $(A_i)$ satisfies

$$A_{n-i} = \sum_{j=i}^{n-d} (-1)^{j-i}(-q)^{(j-i)} \binom{j}{i} \left[ \frac{|Y|}{q^{n-j}} (-1)^{(n+1)j - 1} \right]$$

for each $i \in \{0, 1, \ldots, n - 1\}$.

**Proof.** Let $(A_0, \ldots, A_n)$ and $(A'_0, \ldots, A'_n)$ be the inner distribution and the dual inner distribution of $Y$, respectively. As in the proof of Theorem 1 we
have for each \( j \in \{0, 1, \ldots, n\}\),
\[
\sum_{k=0}^{j} \binom{n-k}{n-j} A_k' = (-1)^{(n+1)j} q^{nj} \sum_{i=0}^{n} A_i \binom{n-i}{j}.
\]
Since \( Y \) is a \( d \)-code and an \((n - d)\)-design, we find that, for each \( j \in \{0, 1, \ldots, n - d\}\),
\[
\binom{n}{j} \left( \frac{|Y|}{q^{nj}} (-1)^{(n+1)j} - 1 \right) = \sum_{i=0}^{n-d} A_{n-i} \binom{i}{j}.
\]
The proof is completed by applying the inversion formula (6). \( \square \)

Call a \( d \)-code \( Y \) in \( X(n, q) \) maximal additive if \( Y \) is additive and
\[ |Y| = q^{n(d+1)}, \]
so that \( Y \) meets the bound of Theorem 1 with equality. If \( d \) is odd, then \( Y \) is an \((n - d + 1)\)-design by Theorem 1 and so Theorem 3 implies that the inner distribution of \( Y \) is uniquely determined by its parameters. The situation is different for even \( d \). It was checked with a computer that there are exactly four different inner distributions of maximal additive 2-codes in \( X(3, 2) \) and at least three different inner distributions of maximal additive 2-codes in \( X(4, 2) \). The four possibilities for the inner distribution \((A_0, A_1, A_2, A_3)\) of a maximal additive 2-code in \( X(3, 2) \) are
\[
(1, 0, 21, 42), \quad (1, 0, 29, 34), \quad (1, 0, 37, 26), \quad (1, 0, 45, 18).
\]

4. CONSTRUCTIONS

Recall from the previous section that a maximal additive \( d \)-code in \( X(n, q) \) is a \( d \)-code that meets the bound of Theorem 1 with equality. In this section, we provide constructions of maximal additive \( d \)-codes in \( X(n, q) \) for all possible values of \( d \), except when \( n \) and \( d \) are both even and \( 4 \leq d \leq n - 2 \).

We shall work with Hermitian forms rather than with matrices. Let \( V = V(n, q^2) \) be an \( n \)-dimensional vector space over \( \mathbb{F}_{q^2} \). Recall that a Hermitian form on \( V \) is a mapping
\[ H : V \times V \to \mathbb{F}_{q^2}, \]
that is \( \mathbb{F}_{q^2} \)-linear in the first coordinate and satisfies \( H(y, x) = \overline{H(x, y)} \) for all \( x, y \in V \). The (left) radical of a Hermitian form \( H \) on \( V \) is the \( \mathbb{F}_{q^2} \)-vector space
\[ \text{rad}(H) = \{ x \in V : H(x, y) = 0 \text{ for all } y \in V \} \]
and its rank is \( n - \dim \text{rad}(H) \). Fixing a basis \( \xi_1, \ldots, \xi_n \) for \( V \) over \( \mathbb{F}_{q^2} \), we can identify a Hermitian form \( H \) on \( V \) with the \( n \times n \) Hermitian matrix
\[
(H_{ij} = H(\xi_i, \xi_j))_{1 \leq i, j \leq n}.
\]
It is readily verified that the rank of this matrix equals the rank of the Hermitian form \( H \). In fact this gives a one-to-one correspondence between \( X(n, q) \) and Hermitian forms on \( V \).
We shall identify the vector space $V(n, q^2)$ with $\mathbb{F}_{q^2}$ and use the relative trace function $\text{Tr} : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$, given by

$$\text{Tr}(x) = \sum_{k=0}^{n-1} x^{q^{2k}}.$$ 

It is easy to check that this trace function is $\mathbb{F}_{q^2}$-linear and satisfies $\text{Tr}(x^n) = \text{Tr}(x^q)$ for all $x \in \mathbb{F}_{q^2}$.

The following theorem contains a construction for maximal additive $d$-codes in $X(n, q^2)$ when $n - d$ is odd.

**Theorem 4.** Let $n$ and $d$ be integers of opposite parity satisfying $1 \leq d \leq n - 1$. Then, as $a_1, \ldots, a_{(n-d+1)/2}$ range over $\mathbb{F}_{q^2}$, the mappings

$$H : \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$$

$$H(x, y) = \text{Tr} \left( \sum_{j=1}^{(n-d+1)/2} (a_j x y^{q^{2j} - 1} + (a_j)^q x^{q^{2j}} y^q) \right)$$

form an additive $d$-code in $X(n, q^2)$ of size $q^n(n-d+1)$.

**Proof.** It is readily verified that the mappings $H$ are Hermitian and that the linearity of the trace function implies that the set under consideration is additive. It is therefore enough to show that $H$ has rank at least $d$ unless $a_1 = \cdots = a_{(n-d+1)/2} = 0$.

We may write

$$H(x, y) = \text{Tr}(y^q L(x)),$$

where $L$ is an endomorphism of $\mathbb{F}_{q^2}$, given by

$$L(x) = \sum_{j=1}^{(n-d+1)/2} ((a_j x)^{q^{2n-2j+2}} + (a_j)^q x^{q^{2j}}).$$

We have

$$L(x^{q^{n-d-1}}) = \sum_{j=1}^{(n-d+1)/2} ((a_j)^{q^{2n-2j+2}} x^{q^{n-d-2j+1}} + (a_j)^q x^{q^{n-d+2j-1}}).$$

If not all of $a_j$'s are zero, then this is a polynomial of degree at most $q^{2(n-d)}$ and so has at most $q^{2(n-d)}$ zeros. Now notice that

$$\mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$$

$$(u, v) \mapsto \text{Tr}(uv)$$

is a nondegenerate bilinear form. Therefore, since the kernel of a nonzero $L$ on $\mathbb{F}_{q^2}$ has dimension at most $n - d$ over $\mathbb{F}_{q^2}$, the radical of the corresponding Hermitian form also has dimension at most $n - d$ over $\mathbb{F}_{q^2}$. Therefore, $H$ has rank at least $d$ unless $a_1 = \cdots = a_{(n-d+1)/2} = 0$, as required. \qed
The following theorem contains a construction for $d$-codes in $X(n, q)$ when $n$ and $d$ are both odd.

**Theorem 5.** Let $n$ and $d$ be odd integers satisfying $1 \leq d \leq n$. Then, as $a_0$ ranges over $\mathbb{F}_{q^n}$ and $a_1, \ldots, a_{(n-d)/2}$ range over $\mathbb{F}_{q^{2n}}$, the mappings

$$H : \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}} \to \mathbb{F}_{q^2}$$

$$H(x, y) = \text{Tr} \left( a_0 x y^{q^n} + \sum_{j=1}^{(n-d)/2} (a_j x y^{q^{n-2j+1}} + (a_j)^q x^{q^{n-2j+1}} y^q) \right)$$

form an additive $d$-code in $X(n, q)$ of size $q^{n(d+1)}$.

**Proof.** The proof is similar to that of Theorem 4 and so only a sketch is included. We may write

$$H(x, y) = \text{Tr} (y^q L(x)),$$

where $L$ is an endomorphism of $\mathbb{F}_{q^{2n}}$, given by

$$L(x) = (a_0 x)^{q^{n+1}} + \sum_{j=1}^{(n-d)/2} ((a_j x)^{q^{n+2j+1}} + (a_j)^q x^{q^{n-2j+1}}).$$

If not all of the $a_j$'s are zero, then $L(x^{q^{2n-d-1}})$ is induced by a polynomial of degree at most $q^{2(n-d)}$ and therefore, as in the proof of Theorem 4, we find that $H$ has rank at least $d$ unless $a_0 = \cdots = a_{(n-d)/2} = 0$. □

Theorems 4 and 5 give constructions of maximal additive $d$-codes in $X(n, q)$ for every possible $n$ and $d$ except when both $n$ and $d$ are even. Constructions of maximal additive $d$-codes in $X(n, q)$ are easy to obtain for $d = 2$ and for $d = n$, independently of whether $n$ is even or odd. For $d = n$, we can take an $\mathbb{F}_q$-vector space of $q^n$ symmetric matrices of size $n \times n$ over $\mathbb{F}_q$ with the property that every nonzero matrix in this space is nonsingular. Constructions of such sets are well known (see [10] or [19], for example). Another construction of maximal additive $n$-codes in $X(n, q)$ was given in [9]. For $d = 2$, we can take all matrices in $X(n, q)$ whose main diagonal contains only zeros [20, Theorem 6.1]. However, it is currently an open problem how to construct (if they exist) maximal additive $d$-codes in $X(n, q)$ when $n$ and $d$ are even integers satisfying $4 \leq d \leq n - 2$.

We close this section by showing that the bound for additive codes in Theorem 4 can be surpassed by non-additive codes whenever $n$ is even and $d = n$. This follows already from [11, Theorem 9]. Here we give a more direct construction. The main ingredient is a set $Z$ of $m \times m$ matrices over $\mathbb{F}_q$ with the property that $|Z| = q^m$ and $A - B$ is nonsingular for all distinct $A, B \in Z$. Such objects are equivalent to finite quasifields [4] and several constructions are known (see [6] for a canonical construction corresponding to finite fields).
**Theorem 6.** Let $n$ be an even positive integer and let $Z$ be a set of $q^n$ matrices over $\mathbb{F}_{q^2}$ of size $n/2 \times n/2$ with the property that $A - B$ is nonsingular for all distinct $A, B \in Z$. Let

$$Y = \left\{ \begin{pmatrix} I & A^* \\ A & AA^* \end{pmatrix} : A \in Z \right\} \cup \left\{ \begin{pmatrix} O & O \\ O & I \end{pmatrix} \right\},$$

where $O$ and $I$ are the zero and identity matrices of size $n/2 \times n/2$, respectively. Then $Y$ is an $n$-code in $X(n, q)$ of size $q^n + 1$.

**Proof.** By the assumed properties of $Z$, it is plain that

$$\begin{pmatrix} O & A^* - B^* \\ A - B & AA^* - BB^* \end{pmatrix}$$

is nonsingular for all distinct $A, B \in Z$. Moreover, for each $n/2 \times n/2$ matrix $A$ over $\mathbb{F}_{q^2}$, we have

$$\begin{pmatrix} I & O \\ -A & I \end{pmatrix} \begin{pmatrix} I & A^* \\ A & AA^* - I \end{pmatrix} = \begin{pmatrix} I & A^* \\ O & -I \end{pmatrix},$$

and the proof is completed. □

**Appendix A. Computation of the eigenvalues**

We now derive the explicit expressions for the numbers $Q_k(i)$. We begin with the following lemma, which gives a recurrence formula for the eigenvalues. Write $Q_k^{(n)}(i)$ for $Q_k(i)$ and $X_i(n)$ for $X_i$ to indicate dependence on $n$.

**Lemma 7.** For $1 \leq i, k \leq n$, we have

$$Q_k^{(n)}(i) = Q_k^{(n)}(i - 1) + (-q)^{2n-i} Q_{k-1}^{(n-1)}(i - 1).$$

**Proof.** We have

$$Q_k(i) = \sum_{A \in X_k(n)} \langle A, S \rangle,$$

where $S$ is an arbitrary element of $X_i(n)$. Take $S \in X_i(n)$ to be the diagonal matrix with diagonal $(1, \ldots, 1, 0, \ldots, 0)$ and let $S' \in X_{i-1}(n-1)$ be the diagonal matrix with diagonal $(1, \ldots, 1, 0, \ldots, 0)$. For an $n \times n$ Hermitian matrix $A$, we write

$$A = \begin{pmatrix} a & v^* \\ v & B \end{pmatrix},$$

so that $a \in \mathbb{F}_q$, $v \in (\mathbb{F}_{q^2})^{n-1}$, and $B$ is Hermitian of size $(n-1) \times (n-1)$. Then

$$Q_k^{(n)}(i - 1) - Q_k^{(n)}(i) = \sum_{A \in X_k(n)} (\langle B, S' \rangle - \langle A, S \rangle)$$

$$= \sum_{A \in X_k(n)} (\langle B, S' \rangle (1 - \chi(a))).$$

\[\tag{12}\]
If \( a = 0 \), then the summand is zero. Thus, to evaluate the sum, we may assume that \( A \) is such that \( a \in \mathbb{F}_q^* \). For \( A \) of the form (11), write

\[
L = \begin{pmatrix}
1 & 0 \\
-a^{-1}v & I
\end{pmatrix}
\]

(where \( I \) is the identity matrix of size \((n-1) \times (n-1)\)). Then \( L \) is nonsingular and

\[
LAL^* = \begin{pmatrix}
a & 0 \\
0 & C
\end{pmatrix}, \quad \text{where} \quad C = B - a^{-1}vv^*.
\]

If \( A \) has rank \( k \), then \( C \) has rank \( k - 1 \) since \( a \) is nonzero. Hence we find from (12) that

\[
Q_k(n)(i - 1) - Q_k(n)(i) = \sum_{C \in X_{k-1}(n-1)} \sum_{v \in (\mathbb{F}_q^2)^{n-1}} \sum_{a \in \mathbb{F}_q^*} \langle C + a^{-1}vv^*, S' \rangle (1 - \chi(a))
\]

using the homomorphism property (2). We have

\[
\sum_{C \in X_{k-1}(n-1)} \langle C, S' \rangle = Q_{k-1}^{(n-1)}(i - 1)
\]

and

\[
\sum_{v \in (\mathbb{F}_q^2)^{n-1}} \langle a^{-1}vv^*, S' \rangle = q^{2n-2i} \sum_{v_1, \ldots, v_{i-1} \in \mathbb{F}_q^2} \chi(a^{-1}(v_1v_1 + \cdots + v_{i-1}v_{i-1}))
\]

\[
= q^{2n-2i}(-q)^{i-1}
\]
since, for an arbitrary nontrivial character \( \psi \) of \((\mathbb{F}_q, +)\), we have

\[
\sum_{v \in \mathbb{F}_q^2} \psi(v\overline{v}) = 1 + (q + 1) \sum_{v \in \mathbb{F}_q^2} \psi(v) = -q.
\]

Moreover

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

Substitute everything into (13) to find that

\[
Q_k(n)(i - 1) - Q_k(n)(i) = q^{2n-2i+1}(-q)^{i-1}Q_{k-1}^{(n-1)}(i - 1),
\]

as required. \( \square \)

To obtain the explicit expression (4) for the eigenvalues, we use the recurrence of Lemma 7 together with the initial values

\[
Q_0(i) = 1,
\]

(14)

\[
Q_k(0) = |X_k|,
\]
which follow directly from (3). It is well known (see, for example, [3] or [21] for odd $q$ and [17] for the general case) that

$$|X_k| = (-1)^k \binom{n}{k} \prod_{j=0}^{k-1} ((-q)^n + (-q)^j).$$

We first verify that (4) gives the correct expressions for $Q_0(i)$ and $Q_k(0)$. The expression for $Q_0(i)$ holds trivially. Apply the following version of the $q$-binomial theorem

$$\sum_{j=0}^{h} (-q)^{\binom{h}{j}} \binom{h}{j} x^j y^{h-j} = \prod_{j=0}^{h-1} (x + (-q)^j y) \quad \text{for real } x, y,$$

to (15) to find that

$$|X_k| = (-1)^k \binom{n}{k} \sum_{j=0}^{k} (-q)^{\binom{k}{j}} \binom{k}{j} (-q)^{nj}.$$

Using the identity

$$\binom{n}{k} \binom{k}{j} = \binom{n-j}{n-k} \binom{n}{j},$$

we see that (4) gives the correct expression for $Q_k(0)$. Now invoke Lemma 7 and the following version of Pascal’s triangle identity

$$\binom{n - i + 1}{j} - (-q)^{n-i-j+1} \binom{n - i}{j-1} = \binom{n - i}{j}$$

to conclude that (4) gives the correct expression for $Q_k(i)$ for all $k, i \geq 0$.

References

[1] J. De Beule, A. Klein, K. Metsch, and L. Storme, Partial ovoids and partial spreads in Hermitian polar spaces, Des. Codes Cryptogr. 47 (2008), no. 1-3, 21–34.
[2] A. E. Brouwer, A. M. Cohen, and A. Neumaier, Distance-regular graphs, Springer-Verlag, Berlin, 1989.
[3] L. Carlitz and J. H. Hodges, Representations by Hermitian forms in a finite field, Duke Math. J. 22 (1955), 393–405.
[4] J. de la Cruz, M. Kiermaier, A. Wassermann, and W. Willems, Algebraic structures of MRD codes, Adv. Math. Commun. 10 (2016), no. 3, 499–510.
[5] Ph. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Rep. Suppl. 10 (1973).
[6] Ph. Delsarte, Bilinear forms over a finite field, with applications to coding theory, J. Combin. Theory Ser. A 25 (1978), no. 3, 226–241.
[7] Ph. Delsarte and J. M. Goethals, Alternating bilinear forms over GF(q), J. Combin. Theory Ser. A 19 (1975), no. 1, 26–50.
[8] Ph. Delsarte and V. I. Levenshtein, Association schemes and coding theory, IEEE Trans. Inform. Theory 44 (1998), no. 6, 2477–2504.
[9] J.-G. Dumas, R. Gow, and J. Sheekey, Rank properties of subspaces of symmetric and Hermitian matrices over finite fields, Finite Fields Appl. 17 (2011), no. 6, 504–520.
[10] E. M. Gabidulin and N. I. Pilipchuk, Symmetric matrices and codes correcting rank errors beyond the $\lfloor(d-1)/2\rfloor$ bound, Discrete Appl. Math. 154 (2006), no. 2, 305–312.
[11] R. Gow, M. Lavrauw, J. Sheekey, and F. Vanhove, Constant rank-distance sets of Hermitian matrices and partial spreads in Hermitian polar spaces, Electron. J. Combin. 21 (2014), no. 1, Paper 1.26.

[12] F. Ihringer, A new upper bound for constant distance codes of generators on Hermitian polar spaces of type $H(2d - 1, q^2)$, J. Geom. 105 (2014), no. 3, 457–464.

[13] F. Ihringer, P. Sin, and Q. Xiang, New bounds for partial spreads of $H(2d - 1, q^2)$ and partial ovoids of the Ree-Tits octagon, J. Combin. Theory Ser. A 153 (2018), 46–53.

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

[15] F. J. MacWilliams and N. J. A. Sloane, The theory of error-correcting codes, Amsterdam, The Netherlands: North Holland, 1977.

[16] W. J. Martin and H. Tanaka, Commutative association schemes, European J. Combin. 30 (2009), no. 6, 1497–1525.

[17] D.-J. Mercier, The number of solutions of the equation $Tr_{F_q / F_s} (f(x) + v \cdot x) = b$ and some applications, J. Pure Appl. Algebra 193 (2004), no. 1-3, 251–262.

[18] K.-U. Schmidt, Symmetric bilinear forms over finite fields of even characteristic, J. Combin. Theory Ser. A 117 (2010), no. 8, 1011–1026.

[19] , Symmetric bilinear forms over finite fields with applications to coding theory, J. Algebraic Combin. 42 (2015), no. 2, 635–670.

[20] M. Schmidt, Rank metric codes, Master’s thesis, University of Bayreuth, 2016.

[21] D. Stanton, A partially ordered set and $q$-Krawtchouk polynomials, J. Combin. Theory Ser. A 30 (1981), no. 3, 276–284.

[22] F. Vanhove, The maximum size of a partial spread in $H(4n + 1, q^2)$ is $q^{2n+1} + 1$, Electron. J. Combin. 16 (2009), no. 1, Note 13.

[23] , A geometric proof of the upper bound on the size of partial spreads in $H(4n + 1, q^2)$, Adv. Math. Commun. 5 (2011), no. 2, 157–160.

[24] Z.-X. Wan, Geometry of matrices, World Scientific Publishing Co., 1996.

Department of Mathematics, Paderborn University, Warburger Str. 100, 33098 Paderborn, Germany

E-mail address: kus@math.upb.de