The geometry of Hermitian self-orthogonal codes

Simeon Ball and Ricard Vilar

Abstract. We prove that if $n > k^2$ then a k -dimensional linear code of length n over $\mathbb{F}_{q^2}$ has a truncation which is linearly equivalent to a Hermitian self-orthogonal linear code. In the contrary case we prove that truncations of linear codes to codes equivalent to Hermitian self-orthogonal linear codes occur when the columns of a generator matrix of the code do not impose independent conditions on the space of Hermitian forms. In the case that there are more than n common zeros to the set of Hermitian forms which are zero on the columns of a generator matrix of the code, the additional zeros give the extension of the code to a code that has a truncation which is equivalent to a Hermitian self-orthogonal code.

1. Introduction

The main motivation to study Hermitian self-orthogonal codes is their application to quantum error-correcting codes. The most prevalent and applicative quantum codes are qubit codes, in which the quantum state is encoded on n quantum particles with two-states. In this case, the quantum code is a subspace of $(\mathbb{C}^2)^{\otimes n}$. More generally, a quantum code is a subspace of $(\mathbb{C}^q)^{\otimes n}$. The parameter q is called the *local dimension* and corresponds to the number of states each quantum particle of the system has. A qubit is then referred to as a quqit.

A quantum code with minimum distance d is able to detect errors, which act non-trivially on the code space, on up to $d - 1$ of the quqits and correct errors on up to $\frac{1}{2}(d - 1)$ of the quqits. If the code encodes k logical quqits onto n

Simeon Ball acknowledges the support of the Spanish Ministry of Science and Innovation Grant MTM2017-82166-P and PID2020-113082GB-I00 funded by MCIN/AEI/10.13039/501100011033.

quqits then we say the quantum code is an $[[n, k, d]]_q$ code. It has dimension q^k .

Suppose that $q = p^h$ is a prime power and let $\mathbb{F}_q$ denote the finite field with q elements. A linear code C of length n over $\mathbb{F}_q$ is a subspace of $\mathbb{F}_q^n$. If the minimum weight of a non-zero element of C is d then the minimum (Hamming) distance between any two elements of C is d and we say that C is a $[n, k, d]_q$ code, where k is the dimension of the subspace C . If we do not wish to specify the minimum distance then we say that C is a $[n, k]_q$ code.

A canonical Hermitian form on $\mathbb{F}_{q^2}^n$ is given by

$$(u, v)_h = \sum_{i=1}^n u_i v_i^q.$$

If C is a linear code over $\mathbb{F}_{q^2}$ then its *Hermitian dual* is defined as

$$C^{\perp_h} = \{v \in \mathbb{F}_{q^2}^n \mid (u, v)_h = 0, \text{ for all } u \in C\}.$$

The standard dual of C will be denoted by $C^\perp$. Observe that $v \in C^\perp$ if and only if $v^q \in C^{\perp_h}$, so both of the dual codes have the same weight distribution.

One very common construction of quantum stabiliser codes relies on the following theorem from Ketkar et al. [7, Corollary19]. It is a generalisation from the qubit case of a construction introduced by Calderbank et al. [2, Theorem2].

Theorem 1. *If there is a $[n, k]_{q^2}$ linear code C such that $C \leq C^{\perp_h}$ then there exists an $[[n, n - 2k, d]]_q$ quantum code, where d is the minimum weight of the elements of $C^{\perp_h} \setminus C$ if $k \neq \frac{1}{2}n$ and d is the minimum weight of the non-zero elements of $C^{\perp_h} = C$ if $k = \frac{1}{2}n$.*

If $C \leq C^{\perp_h}$ then we say the linear code C is *Hermitian self-orthogonal*. Theorem 1 is our motivation to study Hermitian self-orthogonal codes. We can scale the i -th coordinate of all the elements of C by a non-zero scalar v_i , without altering the parameters of the code. Such a scaling, together with a reordering of the coordinates, gives a code which is said to be *linearly equivalent* to C .

Thus, a linear code D is *linearly equivalent* to a linear code C over $\mathbb{F}_q$ if, after a suitable re-ordering of the coordinates, there exist non-zero $\theta_i \in \mathbb{F}_q$ such that

$$D = \{(\theta_1 u_1, \dots, \theta_n u_n) \mid (u_1, \dots, u_n) \in C\}.$$

A *truncation* of a code is a code obtained from C by deletion of coordinates. Observe that a truncation can reduce the dimension of the code but the dual minimum distance can only increase.

We will be interested in the following question: Given a linear $[n, k, d]_q$ code C , what truncations does C have which are linearly equivalent to Hermitian self-orthogonal codes?

In the special case that C is a k -dimensional Reed-Solomon code, the above question was answered by the authors in [1]. The code C has a truncation of

length $m \leq q^2$ which is linearly equivalent to a Hermitian self-orthogonal code if and only if there is a polynomial $g(X) \in \mathbb{F}_{q^2}[X]$ of degree at most $(q-k)q-1$ with the property that $g(x) + g(x)^q$, when evaluated at the elements $x \in \mathbb{F}_{q^2}$, has precisely $q^2 + 1 - m$ zeros.

2. Hermitian self-orthogonal codes

Let C be a linear code of length n over $\mathbb{F}_{q^2}$. We have that C is linearly equivalent to a Hermitian self-orthogonal code if and only if there are non-zero $\theta_i \in \mathbb{F}_{q^2}$ such that

$$\sum_{i=1}^n \theta_i^{q+1} u_i v_i^q = 0,$$

for all $u, v \in C$. Note that θ_i^{q+1} is a non-zero element of $\mathbb{F}_q$, so equivalently C is linearly equivalent to a Hermitian self-orthogonal code if and only if there are non-zero $\lambda_i \in \mathbb{F}_q$ such that

$$\sum_{i=1}^n \lambda_i u_i v_i^q = 0.$$

For any linear code C over $\mathbb{F}_{q^2}$ of length n , Rains [8] defined the *puncture code* $P(C)$ to be

$$P(C) = \{\lambda = (\lambda_1, \dots, \lambda_n) \in \mathbb{F}_q^n \mid \sum_{i=1}^n \lambda_i u_i v_i^q = 0, \text{ for all } u, v \in C\}.$$

Then, clearly we have the following theorem.

Theorem 2. *There is a truncation of a linear code C over $\mathbb{F}_{q^2}$ of length n to a linear over $\mathbb{F}_{q^2}$ of length $r \leq n$ which is linearly Hermitian self-orthogonal code if and only if there is an element of $P(C)$ of weight r .*

Thus, as emphasised in [6], the puncture code is an extremely useful tool in constructing Hermitian self-orthogonal codes. Observe that, the minimum distance of any quantum code, given by an element in the puncture code, will have minimum distance at least the minimum distance of $C^\perp$, since any element in the dual of the shortened code will be an element of $C^\perp$ if we replace the deleted coordinates with zeros.

Given a linear code C over $\mathbb{F}_{q^2}$ it is not obvious how one can efficiently compute the puncture code. Let $G = (g_{i\ell})$ be a generator matrix for C , i.e. a $k \times n$ matrix whose row-span is C . A straightforward approach would be to construct a $\binom{k+1}{2} \times n$ matrix $T(G) = (t_{ij,\ell})$ over $\mathbb{F}_{q^2}$, where for $\{i, j\} \subseteq \{1, \dots, k\}$ we define

$$t_{ij,\ell} = \begin{cases} g_{i\ell} g_{j\ell}^q & i < j, \\ g_{i\ell}^{q+1} & i = j. \end{cases} \quad (1)$$

Lemma 3. *The puncture code $P(C)$ is the intersection of the right-kernel of $T(G)$ with $\mathbb{F}_q^n$.*

Proof. For any $u, v \in C$,

$$u_\ell = \sum_{i=1}^k a_i g_{i\ell} \quad \text{and} \quad v_\ell = \sum_{j=1}^k b_j g_{j\ell}$$

for some $(a_1, \dots, a_k) \in \mathbb{F}_q^k$ and $(b_1, \dots, b_k) \in \mathbb{F}_q^k$.

Since

$$\sum_{\ell=1}^n \lambda_\ell u_\ell v_\ell^q = \sum_{i=1}^k \sum_{j=1}^k a_i b_j^q \sum_{\ell=1}^n \lambda_\ell g_{i\ell} g_{j\ell}^q,$$

we have that $\lambda = (\lambda_1, \dots, \lambda_n)$ is in the right-kernel of $T(G)$ if and only if

$$\sum_{\ell=1}^n \lambda_\ell u_\ell v_\ell^q = 0,$$

for all $u, v \in C$. □

Thus, the puncture code $P(C)$ can then be found by extracting the elements in the right-kernel of $T(G)$ all of whose coordinates are elements of $\mathbb{F}_q$. However, this quickly becomes unfeasible computationally for larger parameters.

Our first aim, which we will deal with now, is to construct a parity check matrix for $P(C)$, i.e. a matrix *over* $\mathbb{F}_q$ whose right-kernel is $P(C)$. This allows one to determine, given a linear code C over $\mathbb{F}_{q^2}$, all truncations of C which are linearly equivalent to a Hermitian self-orthogonal code, provided that the dimension of $P(C)$ is not too large.

Let $e \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

Let $M(G) = (m_{ij,\ell})$ be a $k^2 \times n$ matrix where, for $i, j \in \{1, \dots, k\}$, we define

$$m_{ij,\ell} = \begin{cases} eg_{i\ell}g_{j\ell}^q + e^q g_{i\ell}^q g_{j\ell} & i < j \\ g_{i\ell}g_{j\ell}^q + g_{i\ell}^q g_{j\ell} & i > j \\ g_{i\ell}^{q+1} & i = j \end{cases}.$$

Theorem 4. *The matrix $M(G)$ is a parity check matrix for $P(C)$. i.e. $M(G)$ is defined over $\mathbb{F}_q$ and its right-kernel is $P(C)$.*

Proof. Observe first that all the entries in the matrix $M(G)$ are in $\mathbb{F}_q$.

Suppose that $\lambda = (\lambda_1, \dots, \lambda_n)$ is in the right-kernel of $M(G)$. Hence, for all $i, j \in \{1, \dots, k\}$ with $i < j$,

$$\sum_{\ell=1}^n \lambda_\ell (eg_{i\ell}g_{j\ell}^q + e^q g_{i\ell}^q g_{j\ell}) = 0$$

and

$$\sum_{\ell=1}^n \lambda_{\ell} (g_{j\ell} g_{i\ell}^q + g_{j\ell}^q g_{i\ell}) = 0.$$

Multiplying the latter equation by e^q and subtracting the former implies

$$(e^q - e) \sum_{\ell=1}^n \lambda_{\ell} g_{i\ell} g_{j\ell}^q = 0.$$

Since $\lambda = (\lambda_1, \dots, \lambda_n)$ is in the right-kernel of $M(G)$ we also have that

$$\sum_{\ell=1}^n \lambda_{\ell} g_{i\ell}^{q+1} = 0.$$

Hence, λ is in the right-kernel of $T(G)$.

Since it is also in $\mathbb{F}_q^n$, by Lemma 3, $\lambda \in P(C)$.

Suppose that $\lambda = (\lambda_1, \dots, \lambda_n) \in P(C)$. Then, for all $i, j \in \{1, \dots, k\}$,

$$\sum_{\ell=1}^n \lambda_{\ell} g_{i\ell} g_{j\ell}^q = 0.$$

This implies that λ is in the right-kernel of $M(G)$. $\square$

Example 5. Theorem 4 can allow us to efficiently calculate the puncture code of a linear code. Then for each codeword of weight r in the puncture code, by Theorem 2, we can construct a quantum error correcting code of length r . For example, let C be the linear $[43, 7]_4$ code, which is dual to the cyclic linear $[43, 36, 5]_4$ code, constructed from the divisor of $x^{43} - 1$,

$$x^7 + ex^5 + x^4 + x^3 + e^2x^2 + 1,$$

where e is a primitive element of $\mathbb{F}_4$.

By Theorem 4, we can calculate the puncture code from the 49×43 matrix M over $\mathbb{F}_2$, which turns out to have rank 29. The puncture code $P(C)$ has weights $14 + 2j$ for all $j \in \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$.

The truncations to codes of length 14 give a $[14, 7, 6]_4$ code which is equal to its Hermitian dual. By Theorem 1, this implies the existence of a $[[14, 0, 6]]_2$ quantum code.

The truncations to codes of length $18 + 2j$ give a $[18 + 2j, 7]_4$ code with dual minimum distance 5, which by Theorem 1 implies the existence of a $[[18 + 2j, 4 + 2j, 5]]_2$ quantum code, for all $j \in \{0, 1, 2, 3, 4, 5, 6\}$.

These codes equal the best known qubit error-correcting codes, according to Grassl [5].

Example 6. Consider the dual C to the cyclic linear $[51, 42, 6]_4$ code, constructed from the divisor of $x^{51} - 1$,

$$x^9 + e^2x^8 + ex^6 + x^5 + e^2x^4 + e^2x^2 + e^2x + 1.$$

The dimension of the puncture code $P(C)$ is 10. The puncture code $P(C)$ has codewords of weight $18 + 2j$, for all $j \in \{0, 2, 3, 4, 6, 7, 8\}$, which implies that it truncates to codes equivalent to Hermitian self-orthogonal codes of length $18 + 2j$. One can check these are $[18 + 2j, 9]_4$ codes with dual minimum distance 6. By Theorem 1, this implies the existence of a $[[18 + 2j, 2j, 6]]_2$ quantum code, for all $j \in \{0, 2, 3, 4, 6, 7, 8\}$.

Example 7. Consider C the $[15, 5]_9$ code with generator matrix

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ e^7 & e^6 & e^5 & e^4 & 1 & e & e^3 & e^5 & e^4 & 1 & 0 & 0 & 1 & 0 & 0 \\ e^3 & e & e^4 & e^5 & 1 & e^6 & e^7 & e^4 & e^5 & 1 & 0 & 0 & 0 & 1 & 0 \\ e^6 & e^7 & e^5 & e^2 & e^4 & e^2 & e^6 & e^7 & e^3 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

The dual code $C^\perp$ is a linear $[15, 10, 5]_9$ code. The dimension of the puncture code $P(C)$ is 2 and has codewords of weight 9, 12 and 15. This implies that it truncates to codes equivalent to Hermitian self-orthogonal codes of length 9, 12 and 15 and one can check that these codes are a $[9, 4]_9$, a $[12, 5]_9$ and a $[15, 5]_9$ codes all with dual minimum distance 5. By Theorem 1, this implies the existence of a $[[9, 1, 5]]_3$, a $[[12, 2, 5]]_3$ and a $[[15, 5, 5]]_3$ code. The former of these attains the quantum Singleton bound, proved by Rains in [8], which states that

$$k \leq n - 2(d - 1).$$

It was proven in [1] that a $[9, 4, 6]_9$ MDS code does not come from a truncation of a generalised Reed-Solomon code. The only $[9, 4, 6]_9$ code which is not the truncation of a generalised Reed-Solomon code is the projection of Glynn's $[10, 5, 6]_9$ MDS code, see [4].

3. The geometry of Hermitian self-orthogonal codes

Let $\text{PG}(k - 1, q)$ denote the $(k - 1)$ -dimensional projective space over $\mathbb{F}_q$.

A Hermitian form is given by

$$H(X) = \sum_{1 \leq i < j \leq k} (h_{ij} X_i X_j^q + h_{ij}^q X_i^q X_j) + \sum_{i=1}^k h_{ii}^{q+1} X_i^{q+1}.$$

for some $h_{ij} \in \mathbb{F}_{q^2}$.

The set of Hermitian forms is a k^2 -dimensional vector space over $\mathbb{F}_q$.

Let $G = (g_{i\ell})$ be a $k \times n$ generator matrix for a linear code C whose dual minimum distance is at least three. Let $\mathcal{X}$ be the set of columns of G considered as points of $\text{PG}(k - 1, q)$. Observe that the condition that the dual code of C has minimum distance at least three ensures that $\mathcal{X}$ is a set (and not a multi-set). Such a code is often called a *projective code*. Observe that the set $\mathcal{X}$ is

the same for all codes linearly equivalent to C . Let $\text{HF}(\mathcal{X})$ be the subspace of Hermitian forms that are zero on $\mathcal{X}$.

Lemma 8. *The dimension of the left kernel of the matrix $M(G)$ is equal to $\dim \text{HF}(\mathcal{X})$.*

Proof. Let $x \in \mathcal{X}$ and consider a vector v in the left kernel of $M(G)$.

Observe that the coordinates of v are indexed by $i, j \in \{1, \dots, k\}$.

Since x is a column of G ,

$$\sum_{i,j=0}^k v_{ij}(ex_i x_j^q + e^q x_i^q x_j) + v_{ji}(x_i x_j^q + x_i^q x_j) + \sum_{i=1}^k v_{ii} x_i^{q+1} = 0.$$

Thus, defining

$$h_{ij} = ev_{ij} + v_{ji} \quad \text{and} \quad h_{ii}^{q+1} = v_{ii},$$

we have that

$$H(x) = 0.$$

Letting v run over a basis for the left kernel of $M(G)$, we obtain a set of linearly independent Hermitian forms. Indeed, let B be a basis for the left kernel of $M(G)$. Suppose there are $\lambda_v \in \mathbb{F}_q$, for $v \in B$, not all zero, such that, for all $i, j \in \{1, \dots, k\}$,

$$\sum_{v \in B} \lambda_v (ev_{ij} + v_{ji}) = 0, \quad \sum_{v \in B} \lambda_v v_{ii} = 0.$$

Since $e \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, this implies

$$\sum_{v \in B} \lambda_v v_{ij} = 0,$$

for all $i, j \in \{1, \dots, k\}$, contradicting the fact that B is a basis.

Vice-versa, if $H(x) = 0$ for some Hermitian form H , then we obtain v_{ij} by solving

$$h_{ij} = ev_{ij} + v_{ji} \quad \text{and} \quad h_{ii}^q = e^q v_{ij} + v_{ji},$$

where $v_{ij}, v_{ji} \in \mathbb{F}_q$, and $v_{ii} = h_{ii}^{q+1}$. Letting H run over a basis for $\text{HF}(\mathcal{X})$, we obtain a set of linearly independent vectors in the left kernel of the matrix $M(G)$. $\square$

The previous lemma allows us to calculate the dimension of the puncture code in terms of the dimension of the space of Hermitian forms which are zero on $\mathcal{X}$. In the following $\mathcal{X}$ is obtained, as before, as the set of columns of a generator matrix for C , viewed as points of $\text{PG}(k-1, q)$. Note, that the statement that $\mathcal{X}$ imposes r conditions on the space of Hermitian forms is to say that the co-dimension of $\text{HF}(\mathcal{X})$ is r .

Theorem 9. *The set $\mathcal{X}$ imposes $n - \dim P(C)$ conditions on the space of Hermitian forms and*

$$\dim P(C) = n - k^2 + \dim \text{HF}(\mathcal{X}).$$

Proof. By Lemma 8,

$$\dim \text{HF}(\mathcal{X}) = \dim \text{left kernel } M(G) = k^2 - \text{rank } M(G).$$

By Theorem 4,

$$n - \text{rank } M(G) = \dim P(C),$$

which proves the second statement. For the first statement, observe that $\dim \text{HF}(\mathcal{X}) = k^2 - r$, where r is the number of conditions imposed by $\mathcal{X}$ on the space of Hermitian forms. $\square$

Note that in the following statements the truncation may be the code itself.

Theorem 10. *The set of points $\mathcal{X}$ imposes $|\mathcal{X}|$ conditions on the space of Hermitian forms if and only if no truncation of C is equivalent to a Hermitian self-orthogonal code.*

Proof. Theorem 9 implies that the set of points $\mathcal{X}$ imposes n conditions on the space of Hermitian forms if and only if $\dim P(C) = 0$ which, by Theorem 2, is if and only if no truncation of C is equivalent to a Hermitian self-orthogonal code. $\square$

Thus, from Theorem 10, we deduce that to find codes contained in their Hermitian dual it is necessary and sufficient to find a set of points $\mathcal{X}$ which does not impose $|\mathcal{X}|$ conditions on the space of Hermitian forms.

Theorem 11. *The set of points $\mathcal{X}$ imposes less than $|\mathcal{X}|$ conditions on the space of Hermitian forms if and only if some truncation of C is linearly equivalent to a Hermitian self-orthogonal code.*

Theorem 11 has some immediate consequences.

Theorem 12. *A linear $[n, k]_{q^2}$ code for which $n > k^2$ has a truncation which is linearly equivalent to Hermitian self-orthogonal code.*

Proof. Since n is larger than the dimension of the space of Hermitian forms, $\mathcal{X}$ cannot impose n conditions on the space of Hermitian forms. Hence, Theorem 11 implies the statement.

Example 13. Let e be a primitive element of $\mathbb{F}_9$, where $e^2 = e + 1$. Let D be the cyclic linear $[73, 66, 6]_9$ code, constructed from the divisor of $x^{73} - 1$,

$$x^7 + ex^6 + e^6x^5 + e^3x^4 + e^7x^3 + e^2x^2 + e^5x + 2.$$

Let C be the $[60, 7]$ code obtained from $D^\perp$ by deleting coordinates 61–73. The dimension of the puncture code $P(C)$ is 11. The puncture code $P(C)$ has

codewords of weight $\{26, 27, \dots, 55\}$ which implies the existence of a $[[n, n - 14, 6]]_3$ quantum codes, for all $n \in \{26, 27, \dots, 55\}$.

The previous theorem and following theorem are the main results of this paper.

Theorem 14. *A linear $[n, k]_{q^2}$ code C of length n over $\mathbb{F}_{q^2}$ which has no truncations which are linearly equivalent to a Hermitian self-orthogonal code can be extended to C' , a $[n + 1, k]_{q^2}$ code which does have a truncation to a code which is linearly equivalent to a Hermitian self-orthogonal code, if and only if $\mathcal{X}$ imposes n conditions on the space of Hermitian forms and the set of common zeros of $\text{HF}(\mathcal{X})$ is larger than $|\mathcal{X}|$.*

Proof. ($\Rightarrow$) Let $\mathcal{X}'$ be the set of columns of a generator matrix for C' obtained by extending the matrix G . By Theorem 9, both $\mathcal{X}$ and $\mathcal{X}'$ impose n conditions on the space of Hermitian forms. Hence,

$$\text{HF}(\mathcal{X}) = \text{HF}(\mathcal{X}')$$

which implies that the set of common zeros of $\text{HF}(\mathcal{X})$ contains $\mathcal{X}'$.

($\Leftarrow$) Let $\mathcal{X}' = \mathcal{X} \cup \{x\}$ be a subset of the set of common zeros of $\text{HF}(\mathcal{X})$. Let C' be the code with generator matrix whose columns are the elements of $\mathcal{X}'$. Then $\mathcal{X}'$ imposes n conditions on the space of Hermitian forms, so Theorem 9 implies that $\dim P(C') = 1$. Thus, C' extends C to a $[n + 1, k]_{q^2}$ code which has a truncation to a code which is linearly equivalent to a Hermitian self-orthogonal code. $\square$

Theorem 14 indicates that to extend a linear code C to a Hermitian self-orthogonal code, we should calculate the set of common zeros of the Hermitian forms which are zero on the columns of a generator matrix for C .

Example 15. The $[13, 7]_4$ code generated by the matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & e & 0 & e^2 & e & e \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & e & e & e & 0 & e^2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & e & e^2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & e & 1 & 0 & e & 0 & e^2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & e^2 & e^2 & e & e & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & e^2 & e^2 & e & 1 & e^2 & e \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & e^2 & e & e^2 \end{pmatrix}$$

has dual minimum distance 6. As before, let $\mathcal{X}$ be the 13 points which are the columns of the matrix G . The dimension of $\text{HF}(\mathcal{X})$ is 36, so $\mathcal{X}$ imposes 13 conditions on the space of Hermitian forms. Theorem 9 implies that $\dim P(C) = 0$, so C has no truncations which are linearly equivalent to Hermitian self-orthogonal codes. However, there are 14 points which are common zeros of the zeros of $\text{HF}(\mathcal{X})$, the points of $\mathcal{X}$ and the point

$$(0, e, 0, 1, e, 1, 1).$$

Thus, Theorem 14 implies that the $[14, 7]_4$ code, with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & e & 0 & e^2 & e & e & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & e & e & e & 0 & e^2 & e \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & e & e^2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & e & 1 & 0 & e & 0 & e^2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & e^2 & e^2 & e & e & 0 & e \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & e^2 & e^2 & e & 1 & e^2 & e & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & e^2 & e & e^2 & 1 \end{pmatrix}$$

has a truncation which is Hermitian self-orthogonal. Indeed, one can check that the code itself is Hermitian self-orthogonal. Thus, from this code we can construct, by Theorem 1, a $\llbracket 14, 0, 6 \rrbracket_2$ code.

4. Conclusions and further work

In conclusion, we give a summary of the main results.

Suppose that $C^\perp$ is a $[n, n - k, d]_{q^2}$, where $d \geq 3$.

If $n > k^2$ then we have shown that there are truncations of C which are linearly equivalent to Hermitian self-orthogonal codes.

If $n \leq k^2$ and $\dim P(C) > 0$ then there are truncations of C which are linearly equivalent to Hermitian self-orthogonal codes.

If $n \leq k^2$ and $\dim P(C) = 0$ and there are points which are not in $\mathcal{X}$ but are zeros of the forms in $\text{HF}(\mathcal{X})$ then we can extend C to a $[n + 1, k]_{q^2}$ which does have truncations which are linearly equivalent to Hermitian self-orthogonal codes.

Finally, if $n \leq k^2$ and $\dim P(C) = 0$ and there are no points which are zeros of the forms in $\text{HF}(\mathcal{X})$ but which are not in $\mathcal{X}$ then C has no extension to a $[n + 1, k]_{q^2}$ which has truncations that are linearly equivalent to Hermitian self-orthogonal codes. In this case we can extend C trying to maintain the dual minimum distance. This will reduce the dimension of $\text{HF}(\mathcal{X})$ by one, which then creates the possibility that there are points which are not in $\mathcal{X}$ but are zeros of the forms in $\text{HF}(\mathcal{X})$. Indeed we can try and find extensions of C so that this is the case.

In all of the above we can construct a $\llbracket r, r - 2k', d \rrbracket_q$ code from a truncation of length r , for some $k' \leq k$.

It should be able to extend these methods to make use of the following recent result of Galindo and Hernando [3, Theorem 1.2], which is an extension of Theorem 1.

There is also the possibility to extend these methods to self-orthogonal codes, i.e. $C \leq C^\perp$. This will work well in the case that the characteristic is even, since λ^{q+1} is replaced by λ^2 and all elements in a field of even characteristic have

a square root. The role of the Hermitian form is then replaced by a quadratic form.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

Open Access. This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

- [1] Ball, S., Vilar, R.: Determining when a truncated generalised Reed-Solomon code is Hermitian self-orthogonal, [arXiv:2106.10180](https://arxiv.org/abs/2106.10180).
- [2] Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via codes over $GF(4)$. *IEEE Trans. Inform. Theory* **44**, 1369–1387 (1998)
- [3] Galindo, C., Hernando, F.: On the generalization of the construction of quantum codes from Hermitian self-orthogonal codes, [arxiv:2012.11998](https://arxiv.org/abs/2012.11998).
- [4] Glynn, D.G.: The non-classical 10-arc of $PG(4, 9)$. *Discrete Math.* **59**, 43–51 (1986)
- [5] Grassl, M.: Bounds on the minimum distance of linear codes and quantum codes, (available online at <http://www.codetables.de>).
- [6] Grassl, M., Rötteler, M.: Quantum MDS codes over small fields. In: *Proceedings of the International Symposium on Information Theory (ISIT)*, pp. 1104–1108 (2015).
- [7] Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P. K.: Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, **52** (2006) 4892–4914. (available online at <https://arxiv.org/abs/quant-ph/0508070>)
- [8] Rains, E.M.: *Nonbinary quantum codes*. *IEEE Trans. Inf. Theory* **45**, 1827–1832 (1999)

Simeon Ball and Ricard Vilar
Departament de Matemàtiques
Universitat Politècnica de Catalunya
Carrer Jordi Girona 1-3
08034 Barcelona
Spain
e-mail: simeon@ma4.upc.edu

Ricard Vilar
e-mail: ricard.vilar@upc.edu

Received: August 28, 2021.

Accepted: November 30, 2021.