# The Metric Structure of Linear Codes*

Diego Ruano†

**Abstract**

The bilinear form with associated identity matrix is used in coding theory to define the dual code of a linear code, also it endows linear codes with a metric space structure. This metric structure was studied for generalized toric codes and a characteristic decomposition was obtained, which led to several applications as the construction of stabilizer quantum codes and LCD codes. In this work, we use the study of bilinear forms over a finite field to give a decomposition of an arbitrary linear code similar to the one obtained for generalized toric codes. Such a decomposition, called the geometric decomposition of a linear code, can be obtained in a constructive way; it allows us to express easily the dual code of a linear code and provides a method to construct stabilizer quantum codes, LCD codes and in some cases, a method to estimate their minimum distance. The proofs for characteristic 2 are different, but they are developed in parallel.

## 1 Introduction

Error-correcting codes are used in digital communications in order to recover the information sent through a channel that may corrupt some of the information. The most studied, and in practice used, codes are linear codes [22]. A linear code is a vector subspace of $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is the finite field with $q$ elements. The dual code $\mathcal{C}^\perp \subset \mathbb{F}_q^n$, of a linear code $\mathcal{C} \subset \mathbb{F}_q^n$, is the orthogonal space to $\mathcal{C}$ with respect to the bilinear form $B : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$, $B(x, y) = \sum x_i y_i$. This bilinear form allows us to consider $\mathbb{F}_q^n$ as a metric space.

Generalized toric codes are an extension of toric codes [17], they are obtained by evaluating polynomials at the algebraic torus $(\mathbb{F}_q^*)^r$. Their metric structure was studied in [27], providing a direct method to compute the dual code of a generalized toric code and deduce that there exist no self-dual generalized toric codes. Moreover, $J$-affine variety codes [15], which include generalized toric codes as a particular case, have a similar metric structure. Stabilizer quantum codes with good parameters [12, 13,

*Published in Singularities, Algebraic Geometry, Commutative Algebra, and Related Topics, pages 537-561. Editors: G.-M. Greuel, L. Narváez Macarro, S. Xambó-Descamps. Springer Verlag. ISBN: 978-3-319-96826-1 (2018)

†IMUVA (Mathematics Research Institute), University of Valladolid, Spain, and Department of Mathematical Sciences, Aalborg University, Denmark, diego.ruano@uva.es

14, 15] and new binary and ternary LCD codes [16] were constructed using this characteristic metric structure of $J$-affine variety codes.

Quantum error-correcting codes are essential for quantum computing since they protect quantum information from decoherence and quantum noise [29]. Although quantum information cannot be cloned, one can construct stabilizer quantum codes from self-orthogonal classical codes [4, 5, 6, 20]. A linear code $\mathcal{C}$ is self-orthogonal if $\mathcal{C} \subset \mathcal{C}^{\perp}$.

A linear code $\mathcal{C}$ is called an LCD code (complementary dual code) if $\mathcal{C} \cap \mathcal{C}^{\perp} = \{0\}$ [23]. LCD codes are used in cryptography [7], they play an important role in counter-measures to passive and active side-channel analyses on embedded cryptosystems. LCD codes are also useful for obtaining lattices [19] and in network coding [3]. It has been proved in [8] that $q$-ary LCD codes are as good as linear codes for $q > 3$. Hence the study of LCD codes is mainly open for binary and ternary fields.

In this paper we give an affirmative answer to the natural question: *May the metric structure and its applications for generalized toric codes or $J$-affine variety codes be extended for an arbitrary linear code?* To answer this question the classification of bilinear forms on a vector space over a finite field is used [1, 9, 10, 11, 18]. We reproduce this classification in Section 3 providing constructive proofs. The classification of bilinear forms on vector spaces over finite fields has been already used in coding theory for self-dual and self-orthogonal codes, originally by V. Pless [24, 25, 26] and subsequent papers.

For an arbitrary linear code, in Section 4, we compute a structure similar to the one of generalized toric codes, called the geometric decomposition of a linear code. The results and their proofs are different for characteristic 2, but they are developed in parallel. The geometric decomposition of a linear code allows us to extend, in Section 5, the applications for generalized toric codes: it expresses the dual code of a linear code easily and gives a method to estimate their minimum distance (extending the method in [21]). Moreover, we provide a method for constructing stabilizer quantum codes and LCD codes.

# 2 Metric structure of generalized toric codes

Let us introduce generalized toric codes and their metric structure in this section (see [27]), this family of codes motivated this work, as we mentioned in the previous section. They are an extension of toric codes, which are algebraic geometric codes over toric varieties [17]. Let $U \subset H = (\{0, \ldots, q-2\})^r$, $T = (\mathbb{F}_q^*)^r$ and the vector space $\mathbb{F}_q[U] = \langle Y^u = Y_1^{u_1} \cdots Y_r^{u_r} \mid u = (u_1, \ldots, u_r) \in U \rangle \subset \mathbb{F}_q[Y_1, \ldots, Y_r]$. The **generalized toric code** $\mathcal{C}_U$ is the image of the $\mathbb{F}_q$-linear map

$$\begin{array}{rcl} \mathrm{ev} : \mathbb{F}_q[U] & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(t))_{t \in T} \end{array}$$

where $n = \#T = (q-1)^r$.

Let $B(x,y) = \sum x_i y_i$ with $x, y \in \mathbb{F}_q^n$. The following result considers the metric structure of a generalized toric code $\mathcal{C}_U \subset \mathbb{F}_q^n$ and computes its dual code.

**Theorem 1.** [2, 27] *With notations as above, if $u, v \in H$, then*

$$B(\mathrm{ev}(Y^u), \mathrm{ev}(Y^v)) = \begin{cases} 0 & \text{if } \overline{u+v} \neq 0, \\ (-1)^r & \text{if } \overline{u+v} = 0, \end{cases}$$

*where $u = \overline{u} + b_u$, with $\overline{u} \in H$ and $b_u \in ((q-1)\mathbb{Z})^r$. Let $U \subset H$, $u' = \overline{-u}$ and $U' = \{u' \mid u \in U\}$. Then, $\#U = \#U'$ and the dual code of $\mathcal{C}_U$ is $\mathcal{C}_{U^\perp}$, where $U^\perp = H \setminus U' = (H \setminus U)'$.*

Moreover we can order the elements of $H$ in such a way that the matrix of $B$ in the basis $\{\mathrm{ev}(Y^u) \mid u \in H\}$ of $\mathbb{F}_q^n$ has a characteristic form. We consider first in $H$ the pairs of elements $u$ and $u'$, with $u \neq u'$, such that $\overline{u+u'} = 0$ ($u \mapsto u'$ is an involution). Finally, we consider the elements $u \in H$ such that $u = u'$. The matrix $N$ of $B$ in such a basis verifies

$$(-1)^r N = \begin{pmatrix} 0 & 1 & & & & & & & \\ 1 & 0 & & & & & & & \\ & & \ddots & & & & & & \\ & & & 0 & 1 & & & & \\ & & & 1 & 0 & & & & \\ & & & & & 1 & & & \\ & & & & & & \ddots & & \\ & & & & & & & 1 & \end{pmatrix}.$$

The number of 1's in the main diagonal of the matrix is $2^r$ if $q$ is odd and 1 if $q$ is even. Therefore, there are no self-dual generalized toric codes. The previous basis and the characteristic matrix $N$ allowed us to obtain stabilizer quantum codes and LCD codes.

# 3 Bilinear forms on vector spaces over finite fields

In this section, we present an introduction to bilinear forms on vector spaces over finite fields. We refer the reader to [1, 9, 10, 11, 18] for a deeper discussion of the definitions and results in this section. All proofs provided are constructive.

A bilinear form over $\mathbb{F}_q^n$ is a bilinear map $B : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$. It is said to be symmetric if $B(x,y) = B(y,x)$ $\forall x, y \in \mathbb{F}_q^n$ and non-degenerate if

$$B(x,y) = 0 \ \forall y \in \mathbb{F}_q^n \Rightarrow x = 0,$$
$$B(x,y) = 0 \ \forall x \in \mathbb{F}_q^n \Rightarrow y = 0.$$

Let $\mathcal{B} = \{x_1, \ldots, x_n\}$ be a basis of $\mathbb{F}_q^n$; the associated matrix to $B$ in the basis $\mathcal{B}$ is

$$N = \begin{pmatrix} B(x_1,x_1) & \cdots & B(x_1,x_n) \\ \vdots & & \vdots \\ B(x_n,x_1) & \cdots & B(x_n,x_n) \end{pmatrix}.$$

Namely, if $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ in the basis $\mathcal{B}$, one has that $B(x, y) = xNy^t$, where $y^t$ is the transpose of $y$.

From now on, we will consider the metric structure given by the bilinear form $B(x, y) = \sum_{i=1}^{n} x_i y_i$, which is used to define the dual code of a linear code. Here and subsequently, $\mathbb{F}_q^n$ will be the vector space over $\mathbb{F}_q$ with the non-degenerate symmetric bilinear form $B$ whose associated matrix is the identity matrix. Therefore, $B$ is symmetric and non-degenerate.

Let $x, y \in \mathbb{F}_q^n$, $x$ and $y$ are said to be orthogonal if $B(x, y) = 0$ and we denote it $x \perp y$. Let $U$, $W$ be two vector subspaces of $\mathbb{F}_q^n$, $U$ and $W$ are said to be orthogonal if $x \perp y$ for all $x \in U$, $y \in W$. Let $U \subset \mathbb{F}_q^n$ be a vector subspace which is direct sum of pairwise orthogonal vector subspaces $U_1, \ldots, U_r$, then we say that $\mathbb{F}_q^n$ is the orthogonal sum of $U_1, \ldots, U_r$ and will denote it by $\mathbb{F}_q^n = U_1 \perp \cdots \perp U_r$. Let $U \subset \mathbb{F}_q^n$ be a vector subspace, the radical of $U$ consists in the vectors of $U$ that are orthogonal to $U$, that is $\mathrm{rad}(U) = U \cap U^{\perp}$. Let $x, y$ in $\mathbb{F}_q^n$, they are orthonormal if they are orthogonal and $B(x_1, x_1) = 1$, $B(x_2, x_2) = 1$. A vector $x \in \mathbb{F}_q^n$ is called isotropic if $B(x, x) = 0$, that is, if $\langle x \rangle \subset \mathrm{rad}(\langle x \rangle)$. A vector subspace $U \subset \mathbb{F}_q^n$ is called isotropic if $B(x, y) = 0$ for all $x, y \in U$, that is, if $U \subset \mathrm{rad}(U)$. Every isotropic space $U$ satisfies $\dim(U) \leq \left\lfloor \frac{n}{2} \right\rfloor$. An isotropic subspace $U \subset \mathbb{F}_q^n$ is called maximal when it is not strictly contained in any other isotropic subspace. The dimension of all of the maximal isotropic subspaces of a non-singular space $U$ is the same, it is called index of $U$.

A vector subspace $U \subset \mathbb{F}_q^n$ is said to be non-singular if $\mathrm{rad}(U) = (0)$, and singular otherwise. One has that $U$ is non-singular if and only if the bilinear form restricted to $U$ is non-degenerate. If $U \subset \mathbb{F}_q^n$ is non-singular, then $\mathbb{F}_q^n = U \perp U^{\perp}$ and $U^{\perp}$ is non-singular.

Let $H \subset \mathbb{F}_q^n$ be a two-dimensional vector subspace, $H$ is said to be a **hyperbolic plane** if there exist $x_1$, $x_2$ generating $H$ such that

$$\begin{aligned} B(x_1, x_1) &= 0, \\ B(x_2, x_2) &= 0, \\ B(x_1, x_2) &= 1. \end{aligned}$$

hence, $H$ is non-singular. Both ordered generators $x_1$, $x_2$ are called **geometric generators** or **geometric basis of** $H$.

**Lemma 2.** *Let $\mathbb{F}_q$ have odd characteristic. Then any two-dimensional non-singular subspace of $\mathbb{F}_q^n$ which contains an isotropic vector is a hyperbolic plane.*

*Proof.* Let $x_1$ be a non-zero isotropic vector. Let $y$ be a vector of the considered two-dimensional subspace linearly independent to $x_1$ and let $x_2 = \lambda_1 x_1 + \lambda_2 y$, for $\lambda_1$, $\lambda_2 \in \mathbb{F}_q$. One has that $B(x_1, x_2) = \lambda_2 B(x_1, y)$, moreover, $B(x_1, y) \neq 0$ since a plane is non-singular. Therefore, for $\lambda_2 = B(x_1, y)^{-1} \neq 0$, one has that $B(x_1, x_2) = 1$.

Moreover, $B(x_2, x_2) = 0$ if and only if $2\lambda_1 \lambda_2 B(x_1, y) + \lambda_2^2 B(y, y) = 0$. Since $\lambda_2 \neq 0$ and $B(x_1, y) \neq 0$ one has that if

$$\lambda_1 = \frac{-\lambda_2 B(y, y)}{2B(x_1, y)} = \frac{-B(y, y)}{2B(x_1, y)^2}$$

then $x_2$ is an isotropic vector. □ □

Note that the previous result does not hold in characteristic 2 as the next example shows.

**Example 1.** *Let $\mathbb{F}_q$ be a field of characteristic 2. Let $x = (x_1, x_2) \in \mathbb{F}_q^2$, $x$ is an isotropic vector if and only if $x_1^2 + x_2^2 = 0$, that is, if and only if $(x_2/x_1)^2 = 1$. Hence, $(1, 1)$ is an isotropic vector, moreover, only the vectors generated by $(1, 1)$ are isotropic, since we have the Frobenius isomorphism. Therefore, $\mathbb{F}_q^2$ contains an isotropic vector but it is not a hyperbolic plane.*

We say that a non-singular two-dimensional subvector space $E \subset \mathbb{F}_q^n$ is an **elliptic plane** if it is not a hyperbolic plane and there exist $x_1, x_2$ generating $E$ and such that

$$\begin{aligned} B(x_1, x_1) &= 0, \\ B(x_2, x_2) &= 1, \\ B(x_1, x_2) &= 1. \end{aligned}$$

We call $x_1$, $x_2$ the **geometric generators** or **geometric basis of** $E$. For instance $\{(1, 1), (0, 1)\}$ is a geometric basis of the elliptic plane $\mathbb{F}_q^2$, with $q$ even.

## 3.1 Characteristic different from 2

One has that $-1$ is a square element in the field $\mathbb{F}_q$ if and only if $q \equiv 1 \mod 4$. A non-zero vector $x = (x_1, x_2) \in \mathbb{F}_q^2$ is an isotropic vector if and only if $x_1^2 + x_2^2 = 0$, that is, if and only if $(x_2/x_1)^2 = -1$. If $-1$ is a square element in the field, the previous equation has at least one solution and therefore there exist isotropic vectors. If $-1$ is non-square element in $\mathbb{F}_q$ there is no isotropic vector and therefore $\mathbb{F}_q^2$ is not a hyperbolic plane (neither an elliptic).

In $\mathbb{F}_q^n$ there exist orthonormal bases for the bilinear form $B$, for instance the canonical basis. For $x \in \mathbb{F}_q^n$ one can only obtain a linearly dependent vector $y$ of $x$, with $B(y, y) = 1$, just by multiplying $x$ with the square root of $B(x, x)$, if $B(x, x)$ is a square element in $\mathbb{F}_q$. Therefore, for a linear variety $L = \langle x \rangle$ one has that $B(x, x)$ is equal to $a^2$ or $a^2 g$ where $g$ is a fixed non-square element in $\mathbb{F}_q$, moreover, multiplying $x$ by $a^{-1}$ we can assume that $B(x, x) = 1$ or $B(x, x) = g$ and then we say that $x$ is a geometric basis of $L$. From now on we regard $g$ as a fixed non-square element in $\mathbb{F}_q$.

The following result [28, Section 1.7] is used in Proposition 4 and in Lemma 5.

**Lemma 3.** *Let $a, b, c \in \mathbb{F}_q$ be different from zero. Then the following equation has at least one solution over $\mathbb{F}_q$*

$$aX^2 + bY^2 = c$$

The following result shows whether a non-singular plane is a hyperbolic plane, that is, whether it contains isotropic elements. And, moreover, whether it can be generated by two orthonormal elements, when it is not a hyperbolic plane.

**Proposition 4.** *Let $P = \langle x_1, x_2 \rangle \subset \mathbb{F}_q^n$ be a non-singular plane with $B(x_1, x_2) = 0$, $B(x_1, x_1) = a$ and $B(x_2, x_2) = b$. If $a = 0$ or $b = 0$ then $P$ is a hyperbolic plane. If $a \neq 0$ and $b \neq 0$, then*

- *For $q \equiv 1 \mod 4$, $P$ is a hyperbolic plane if and only if $b/a$ is a square element. When $P$ is not a hyperbolic plane it cannot be generated by two orthonormal vectors but can be generated by $y_1, y_2 \in \mathbb{F}_q^n$ such that $B(y_2, y_2) = 0$, $B(y_1, y_1) = 1$, $B(y_2, y_2) = g$, where $g$ is a non-square element in $\mathbb{F}_q$.*
- *For $q \equiv 3 \mod 4$, $P$ is a hyperbolic plane if and only if $b/a$ is a non-square element. When $P$ is not a hyperbolic plane it can be generated by two orthonormal vectors.*

*Proof.* If $a = 0$ or $b = 0$ then $P$ is a hyperbolic plane by Lemma 2.

Let $a \neq 0$ and $b \neq 0$. Let $\lambda_1, \lambda_2 \in \mathbb{F}_q$, $B(\lambda_1 x_1 + \lambda_2 x_2, \lambda_1 x_1 + \lambda_2 x_2) = \lambda_1^2 a + \lambda_2^2 b = 0$ if and only if $(\lambda_1/\lambda_2)^2 = -b/a$. Therefore, there are isotropic vector in $P$ (and hence $P$ is a hyperbolic plane by lemma 2) if and only if $-b/a$ is a square element.

For $q \equiv 1 \mod 4$, one has that $c \in \mathbb{F}_q^*$ is a square element in $\mathbb{F}_q$ if and only if $-c$ is a square element in $\mathbb{F}_q$, since $-1$ is a square element in $\mathbb{F}_q$. Let $y_1 = \lambda_1 x_1 + \lambda_2 x_2$, $B(y_1, y_1) = \lambda_1^2 a + \lambda_2^2 b$. By lemma 3 there exist $\lambda_1, \lambda_2 \in \mathbb{F}_q$ such that $B(y_1, y_1) = 1$, since $a \neq 0$, $b \neq 0$. Let $z \in P$ be non-zero and orthogonal to $y_1$. One has that $B(\lambda_1 y_1 + \lambda_2 z) = \lambda_1^2 + \lambda_2^2 B(z, z)$. Since there exist no isotropic vectors in $P$, $-B(z, z)$ is a non-square element in $\mathbb{F}_q$ or, equivalently, $B(z, z)$ is a non-square element in $\mathbb{F}_q$. Therefore, $B(\lambda_2 z, \lambda_2 z) \neq 1$, but for a fixed non-square element $g$ in $\mathbb{F}_q$, there exists $\lambda_2 \in \mathbb{F}_q$ such that for $y_2 = \lambda_2 z$, and one has that $B(y_2, y_2) = g$.

For $q \equiv 3 \mod 4$, one has that $c \in \mathbb{F}_q^*$ is a square element in $\mathbb{F}_q$ if and only if $-c$ is a non-square element in $\mathbb{F}_q$ since $-1$ is a non-square element in $\mathbb{F}_q$. Let $y_1 = \lambda_1 x_1 + \lambda_2 x_2$, $B(y_1, y_1) = \lambda_1^2 a + \lambda_2^2 b$. By Lemma 3, there exist $\lambda_1, \lambda_2 \in \mathbb{F}_q$ such that $B(y_1, y_1) = 1$, since $a \neq 0$, $b \neq 0$. Let $z \in P$ be non-zero and orthogonal to $y_1$. One has that $B(\lambda_1 y_1 + \lambda_2 z) = \lambda_1^2 + \lambda_2^2 B(z, z)$. Since there exist no isotropic vectors in $P$, $-B(z, z)$ is a non-square element in $\mathbb{F}_q$, or equivalently $B(z, z)$ is a square element in $\mathbb{F}_q$. Therefore, there exists $\lambda_2 \in \mathbb{F}_q$ such that for $y_2 = \lambda_2 z$, one has that $B(y_2, y_2) = 1$. □ □

The following result computes an isotropic vector in a non-singular space of dimension greater than or equal to 3.

**Lemma 5.** *Let $U \subset \mathbb{F}_q^n$ be non-singular with dimension greater than or equal to 3, then there exists at least one isotropic non-zero vector in $U$.*

*Proof.* Let $P$ be a non-singular plane of $U$ and $x_1 \in P^\perp$, assume that $B(x_1, x_1) \neq 0$ (in other case $x_1$ is isotropic). By lemma 3 one has that there exists $x_2 \in P$ such that $B(x_2, x_2) = -B(x_1, x_1)$. Therefore $x_1 + x_2 \neq 0$, $B(x_1 + x_2, x_1 + x_2) = 0$ and the result holds. □ □

Using the previous results one can prove the following proposition.

**Proposition 6.** *Let $U \subset \mathbb{F}_q^n$ be a non-singular $m$-dimensional vector space. If $q$ is odd, then one can decompose $U$ in the following way:*

*If $m$ is odd, then*

*(1)* $U = H_1 \perp \cdots \perp H_{(m-1)/2} \perp L$*, where each* $H_i$ *is a hyperbolic plane and* $L$ *is linear subspace of dimension 1.*

*If* $m$ *is even, then*

*(2) If the index of* $U$ *is* $m/2$*:* $U = H_1 \perp \cdots \perp H_{m/2}$*, where each* $H_i$ *is a hyperbolic plane.*

*(3) If the index of* $U$ *is* $m/2 - 1$*:* $U = H_1 \perp \cdots \perp H_{(m-2)/2} \perp L_1 \perp L_2$*, where each* $H_i$ *is a hyperbolic plane and* $L_1$ *and* $L_2$ *are two linear subspaces of dimension 1.*

*Proof.* Let $m$ be odd. Then one can apply Lemmas 2 and 5 to obtain a hyperbolic plane $H_1$ and therefore one has that $U = H_1 \perp (H_1^{\perp} \cap U)$. In the same way for $H_1^{\perp} \cap U$, one obtains another orthogonal hyperbolic planes. Iterating this process, one writes $U$ as the orthogonal sum of $(m-1)/2$ hyperbolic planes and a linear variety of dimension 1.

In the same way, when $m$ is even, we can apply Lemmas 2 and 5 successively until we compute $(m-2)/2$ pairwise orthogonal hyperbolic planes and a linear variety $W$ of dimension 2. By lemma 4, we may check whether $W$ contains isotropic vectors and therefore it is a hyperbolic plane and $U$ is decomposed as the orthogonal sum of $m/2$ hyperbolic planes, or on the contrary, it does not contain isotropic vectors and therefore it may be generated by two orthogonal elements and $U$ is decomposed as the orthogonal sum of $m/2 - 1$ hyperbolic planes and two linear varieties of dimension 1. □ □

Note that as a corollary of the previous result, one has that the index of an $m$-dimensional vector subspace is equal to $(m-1)/2$, if $m$ is odd, and $m/2$ or $m/2 - 1$, if $m$ is even.

## 3.2 Characteristic 2

In characteristic different from 2, whenever there exists an isotropic vector in a plane, one has a hyperbolic plane. However, as we have seen in Example 1, if $q$ is a power of 2, then $\mathbb{F}_q^2$ is a non-singular plane which contains an isotropic vector but it cannot be generated by two isotropic vectors.

Another important difference between even and odd characteristic is that every element of $\mathbb{F}_q$ is a square element in characteristic 2 (by the Frobenius isomorphism), while this is not the case in odd characteristic. Hence, if $x$ is a non-isotropic vector, then one can always find $y \in \langle x \rangle$ such that $B(y,y) = 1$ since every element in $\mathbb{F}_q^*$ is a square element. Thus, we may say that $y$ is a **geometric basis of** $L = \langle x \rangle$.

The following result allows us to compute a basis of the isotropic vectors in $\mathbb{F}_q^n$.

**Proposition 7.** *A vector* $x \in \mathbb{F}_q^n$*,* $x$ *is isotropic if and only if* $\sum_{i=1}^{n} x_i = 0$*. The* $n-1$ *vectors* $y_1 = (1,1,0,\ldots,0)$*,* $y_2 = (0,1,1,0,\ldots,0)$*,...,* $y_{n-1} = (0,\ldots,0,1,1)$ *form a basis of the vector space* $S$ *of isotropic vectors in* $\mathbb{F}_q^n$*. Furthermore,* $S$ *is non-singular if* $n$ *is odd and singular if* $n$ *is even.*

*Proof.* One has that $x$ is isotropic if and only if $B(x,x) = 0$. That is, $\sum_{i=1}^{n} x_i^2 = 0$ if and only if $(\sum_{i=1}^{n} x_i)^2 = 0$ or, equivalently, if $\sum_{i=1}^{n} x_i = 0$.

The isotropic vectors of $\mathbb{F}_q^n$ form a vector space. Trivially, one has that $y_i$ is isotropic $\forall i$ and that $y_1, \ldots, y_{n-1}$ are linearly independent. Let us check that $\{y_1, \ldots, y_{n-1}\}$ generates the vector space of isotropic vectors. Let $x = (x_1, \ldots, x_n)$ be isotropic, we define then the coefficients of the linear combination

$$\begin{cases} \lambda_1 = x_1, \\ \lambda_2 = x_1 + x_2, \\ \vdots \\ \lambda_{n-1} = x_1 + x_2 + \cdots + x_{n-1}. \end{cases}$$

One has that $\sum_{i=1}^{n-1} \lambda_i y_i = (x_1, \ldots, x_{n-1}, \sum_{i=1}^{n-1} x_i) = (x_1, \ldots, x_{n-1}, x_n)$. The last equality follows from $x_n = \sum_{i=1}^{n-1} x_i$, since $x$ is isotropic. One has that $S^{\perp} = \langle (1, \ldots, 1) \rangle$ and the result holds because $(1, \ldots, 1) \in S$ if and only if $n$ is even. □ □

As a corollary of this result, we have that $\mathbb{F}_q^n$ with $n$ even, cannot be decomposed as an orthogonal sum of $n/2$ hyperbolic planes. Note the difference between this case and the one when $\mathbb{F}_q$ is of characteristic different from 2.

Another consequence of the previous result is that, when $n$ is even, $z = (1, \ldots, 1) \in \mathbb{F}_q^n$ is orthogonal to every isotropic vector in $\mathbb{F}_q^n$. Therefore, no plane containing $z$ can be a hyperbolic plane and we will have to consider an elliptic plane for this element. This explains the phenomenum of Example 1.

Although the following result follows from the previous proposition, we present a constructive proof that will allow us to compute a geometric basis.

**Lemma 8.** *If $P \subset \mathbb{F}_q^n$ is a vector subspace of dimension greater than or equal to 2, then there exists at least one isotropic vector in $P$.*

*Proof.* Let $x_1$, $x_2$ be two linearly independent vectors of $P$ that are non-isotropic. Let $y = \lambda_1 x_1 + \lambda_2 x_2$, with $\lambda_1, \lambda_2 \in \mathbb{F}_q$. One has that $B(y,y) = \lambda_1^2 B(x_1,x_1) + \lambda_2^2 B(x_2,x_2) = 0$, if and only if $(\lambda_1/\lambda_2)^2 = B(x_2,x_2)/B(x_1,x_1)$. Since in a field of characteristic 2 every element is a square, one has that for $\lambda_1 = \sqrt{B(x_2,x_2)}$ and $\lambda_2 = \sqrt{B(x_1,x_1)}$, $y$ is isotropic. □ □

The following result shows that any non-singular vector space of dimension 2 is either a hyperbolic plane or an elliptic plane.

**Proposition 9.** *Let $P \subset \mathbb{F}_q^n$ be a two-dimensional non-singular vector subspace. Then $P$ is a hyperbolic plane if and only if $\sum x_i = 0$ for all $x \in P$. If $P$ is not a hyperbolic plane then it is an elliptic plane and it may be generated by two orthonormal elements.*

*Proof.* Let $S \subset \mathbb{F}_q^n$ be the vector space of isotropic vectors, there exist two independent isotropic vectors in $P$ if and only if $P \subset S$. One has that $P \subset S$ if and only if $\sum x_i = 0$, $\forall x \in P$ by Proposition 7.

Let $P \subset S$, then there exist $x_1,\ x_2 \in P$ isotropic and linearly independent, therefore $\lambda = B(x_1, x_2)$ is not equal to zero (because $B$ is non-degenerate). Let $y_1 = x_1$, $y_2 = \lambda^{-1}x_2$, one has that $y_1$, $y_2$ are the geometric generators of a hyperbolic plane, that is, $B(y_1, y_1) = B(y_2, y_2) = 0$ and $B(y_1, y_2) = 1$.

Let $P \not\subset S$, then there exist $x_1,\ x_2 \in P$ isotropic and linearly independent, with $x_1$ isotropic and $x_2$ non-isotropic. Let $\lambda = B(x_1, x_2)$ and $\mu = B(x_2, x_2) \neq 0$. One has that $y_1 = (\lambda^{-1}\sqrt{\mu})x_1$ and $y_2 = \sqrt{\mu^{-1}}x_2$ are the geometric generators of an elliptic plane, that is, $B(y_1, y_1) = 0$ and $B(y_1, y_2) = B(y_2, y_2) = 1$.

Let $y_1,\ y_2$ be the two generators of the elliptic plane $P$, then $y_1' = y_1 + y_2,\ y_2' = y_2$ . One has that $y_1', y_2'$ form a basis of $P$, since they are linearly independent. Moreover, $B(y_1', y_1') = 1$ and $B(y_1', y_2') = 0$, therefore $P$ can be generated by two orthonormal elements. □ □

The following lemma decomposes a non-singular vector space of dimension greater than or equal to 3 as the orthogonal sum of a hyperbolic plane and its orthogonal subspace.

**Lemma 10.** *Let $U \subset \mathbb{F}_q^n$ be a non-singular vector subspace of dimension greater than or equal to 3. Then there exists a hyperbolic plane $H$ such that $U = H \perp U'$ where $U'$ is a non-singular vector subspace.*

*Proof.* By Lemma 8, we can find an isotropic vector $x \in U$ and one has that $U = \langle x \rangle \perp U_1$, where $U_1 = \langle x \rangle^{\perp} \cap U$. Since $U_1$ is a non-singular vector subspace of dimension greater than or equal to 2, by Lemma 8, there exists an isotropic vector $y \in U$. Therefore, by Proposition 9, $\{x, y\}$ generates a hyperbolic plane $H$, and $U = H \perp U'$, where $U' = H^{\perp} \cap U$. □ □

The following result decomposes a non-singular subspace of dimension greater than or equal to 3 as an orthogonal sum of hyperbolic planes and a linear subspace of dimension lower than or equal to 2

**Proposition 11.** *Let $U \subset \mathbb{F}_q^n$ be an $m$-dimensional non-singular vector subspace with characteristic of $\mathbb{F}_q$ equal to 2. One can decompose $U$ in the following way:*

*If $m$ is odd*

*(1) $U = H_1 \perp \cdots \perp H_{(m-1)/2} \perp L$, where each $H_i$ is a hyperbolic plane and $L$ is a one-dimensional linear subspace.*

*If $m$ is even*

*(2) $U = H_1 \perp \cdots \perp H_{m/2}$, where each $H_i$ is a hyperbolic plane.*

*(3) $U = H_1 \perp \cdots \perp H_{m/2-1} \perp L_1 \perp L_2$, where each $H_i$ is a hyperbolic plane and $L_1,\ L_2$ are one-dimensional linear subspaces.*

*Proof.* Let $m$ be odd, we can apply lemma Lemma 10 to obtain a hyperbolic plane $H_1$ and therefore one has that $U = H_1 \perp (H_1^{\perp} \cap U)$. In the same way, we can make further computations in $H_1^{\perp} \cap U$ to obtain more hyperbolic planes pairwise orthogonal. Thus, repeating the process, we write $U$ as the orthogonal sum of $(m-1)/2$ hyperbolic planes and a one-dimensional linear variety.

In the same way, when $m$ is even, we can apply Lemma 10 successively in order to obtain $m/2-1$ pairwise orthogonal hyperbolic planes and a two-dimensional linear variety. By Proposition 9, this two-dimensional linear variety is a hyperbolic plane when every element $x$ in it verifies $\sum x_i = 0$. Otherwise it can be generated by two orthonormal vectors. □
□

Let $U = \mathbb{F}_q^n$ with $n$ even, then $U$ can only have a decomposition of type (3), because in $\mathbb{F}_q^n$ there are just $n-1$ linearly independent isotropic vectors (Proposition 7).

# 4 Geometric decompositions of linear codes

For an arbitrary linear code, in this section we compute a structure similar to the one of generalized toric codes, called the geometric decomposition of a linear code.

## 4.1 Characteristic different from 2

Let $\mathbb{F}_q$ be a finite field of characteristic different from 2. Using the previous results we can write $\mathbb{F}_q^n$ as the orthogonal sum of hyperbolic planes and linear varieties of dimension 1.

We say that $\mathbb{F}_q^n$ has a **geometric decomposition of type** $r, s, t$ if

$$\mathbb{F}_q^n = H_1 \perp \cdots \perp H_r \perp L_1 \perp \cdots \perp L_{s+t}$$

where $H_1, \ldots, H_r$ are hyperbolic planes and $L_1, \ldots, L_{s+t}$ are one-dimensional linear varieties, such that each hyperbolic plane is generated by two geometric generators $H_i = \langle x_{2i-1}, x_{2i} \rangle$, $i = 1, \ldots, r$, each linear variety of dimension 1 is generated by $L_i = \langle x_{2r+i} \rangle$, with $B(x_{2r+i}, x_{2r+i}) = 1$, $i = 1, \ldots, s$, and the other varieties of dimension 1 are generated by $L_i = \langle x_{2r+s+i} \rangle$, with $B(x_{2r+s+i}, x_{2r+s+i}) = g$, $i = 1, \ldots, t$, where $g$ is a fixed non-square element in $\mathbb{F}_q$. One has that $\{x_1, \ldots, x_n\}$ is a basis of $\mathbb{F}_q^n$ and we say that it is a **basis of the geometric decomposition**.

Let $M$ be the matrix whose rows are the elements of the basis of the geometric decomposition, then one has that $MM^t = J_{r,s,t}$. That is, $J_{r,s,t}$ is the matrix of $B$ in such a basis, then we have

$$J_{r,s,t} = \begin{pmatrix} 0 & 1 & & & & & & & & & \\ 1 & 0 & & & & & & & & & \\ & & \ddots & & & & & & & & \\ & & & 0 & 1 & & & & & & \\ & & & 1 & 0 & & & & & & \\ & & & & & 1 & & & & & \\ & & & & & & \ddots & & & & \\ & & & & & & & 1 & & & \\ & & & & & & & & g & & \\ & & & & & & & & & \ddots & \\ & & & & & & & & & & g \end{pmatrix}$$

where $g$ is a fixed non-square element in $\mathbb{F}_q^*$.

A basis $\{x_1, \ldots, x_n\}$ of $\mathbb{F}_q^n$ is said to be a **compatible basis with respect to a decomposition of type** $r, s, t$ if each $\{x_{2i-1}, x_{2i}\}$, with $i = 1, \ldots, r$, is a geometric basis of a hyperbolic plane, and each $x_{2r+i}$, with $i = 1, \ldots s+t$, generates a one-dimensional linear variety in such a way that all of these subspaces are pairwise orthogonal. Or equivalently, if the matrix of $B$ in such a basis is equal to $J_{r,s,t}$.

Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a linear code, we say that $\mathcal{C}$ is **compatible with a geometric decomposition of type** $r, s, t$ if there exists a basis $\{x_1, \ldots, x_n\}$ of $\mathbb{F}_q^n$ compatible with such a decomposition, in such a way that there exists $I \subset \{1, \ldots, n\}$ such that $\{x_i \mid i \in I\}$ is a basis of $\mathcal{C}$.

The following results allows us to compute a geometric decomposition compatible with a given code in characteristic different from 2.

**Theorem 12.** *Let the characteristic of $\mathbb{F}_q$ be different from 2. Any linear code $\mathcal{C} \subset \mathbb{F}_q^n$ is compatible with at least one geometric decomposition. Furthermore, there is a computable geometric basis, called standard, compatible with $\mathcal{C}$, of type $r, s, t$ with $s + t \leq 4$ and $t \leq 2$.*

*Proof.* Let $\mathcal{C} = \mathrm{rad}(\mathcal{C}) \perp \mathcal{C}_1$, where $\mathrm{rad}(\mathcal{C}) = \langle x_1, \ldots, x_l \rangle$.

We claim that we can compute $x_1', \ldots, x_l' \in \mathbb{F}_q^n$ such that $x_i, x_i'$ are the geometric generators of a hyperbolic plane and, moreover, the hyperbolic planes $H_i = \langle x_i, x_i' \rangle$ and $\mathcal{C}_1$ are pairwise orthogonal. That is, one has that

$$\mathcal{C}' = H_1 \perp \cdots \perp H_l \perp \mathcal{C}_1,$$

where $\mathcal{C}'$ contains $\mathcal{C}$ and is non-singular. We prove the construction of $\mathcal{C}'$ by induction on $l$ (this is Theorem 3.8 in [1]).

For $l = 0$ there is nothing to prove. The subspace $\mathcal{C}_0 = \langle x_1, \ldots, x_{l-1} \rangle \perp \mathcal{C}_1$ is orthogonal to $x_l$ but does not contain it. One has that $x_l \in \mathcal{C}_0^\perp$ but $x_l \notin \mathrm{rad}(\mathcal{C}_0^\perp) = \mathrm{rad}(\mathcal{C}_0)$, therefore there exists $y \in \mathcal{C}_0^\perp$ such that $B(x_l, y) \neq 0$. The plane generated by $\{x_l, y\}$ is non-singular, is contained in $\mathcal{C}_0^\perp$ and by lemma 2 is generated by a geometric basis $H_l = \langle x_l, x_l' \rangle$. Since $H_l \subset \mathcal{C}_0^\perp$, then $\mathcal{C}_0 \perp H_l$ and $\mathcal{C}_0 \subset H_l^\perp$. As the radical of $\mathcal{C}_0$ has dimension $l-1$, by inductive hypothesis we can find geometric bases $\{x_i, x_i'\}$ of $H_i$ in $H_l^\perp$, for $i = 1, \ldots, l-1$ such that they are pairwise orthogonal and also to $\mathcal{C}_1$, and since they are orthogonal to $H_l$ and $H_l$ is orthogonal to $\mathcal{C}_1$, the construction of $\mathcal{C}'$ holds.

Therefore, we have $\mathcal{C}' = H_1 \perp \cdots \perp H_l \perp \mathcal{C}_1$, where $H_i = \langle x_i, x_i' \rangle$, with $x_i' \notin \mathcal{C}$. Moreover, $\mathcal{C}'$ is non-singular and one has that $\mathbb{F}_q^n = H_1 \perp \cdots \perp H_l \perp \mathcal{C}_1 \perp \mathcal{C}'^\perp$.

Since $\mathcal{C}_1$ is non-singular, by Proposition 6, we can write $\mathcal{C}_1$ as a sum of hyperbolic planes and a one or two-dimensional linear space $W$ (if the dimension of $\mathcal{C}_1$ is lower than 3 we do not consider any hyperbolic plane and $\mathcal{C}_1 = W$). Hence, we have $\mathcal{C}_1 = H_{l+1} \perp \cdots \perp H_m \perp W$, where $H_{l+i} = \langle x_{l+i}, x_{l+i}' \rangle$.

By Proposition 6, we have 3 different geometries for $W$

(a) If $\dim(W) = 1$, we write $W = \langle x \rangle$. Moreover, $x$ is non-isotropic since $B$ is non-degenerate. We can consider $x_{m+1} \in W$ such that $B(x_{m+1}, x_{m+1})$ is equal to 1 (if $(B(x_{m+1}, x_{m+1})$ is a square element) or $g$, where $g$ is a fixed non-square element and $W = L_1 = \langle x_{m+1} \rangle$.

(b) If $\dim(W) = 2$ and $W$ contains some isotropic vector, then $W$ is a hyperbolic plane and $W = H_{m+1} = \langle x_{m+1}, x'_{m+1} \rangle$, by Lemma 2.

(c) If $\dim(W) = 2$ and $W$ does not contain any isotropic vector, then $W$ can be generated by two orthogonal vectors $L_1 = \langle x_{m+1} \rangle$, $L_2 = \langle x_{m+2} \rangle$, where $W = L_1 \perp L_2$, by Proposition 4.

We decompose $\mathcal{C}'^{\perp}$ in the same way as $\mathcal{C}_1$ (using Proposition 6) to obtain

$$\mathcal{C}'^{\perp} = H'_1 \perp \cdots \perp H'_{m'} \perp W'$$

Therefore, with notations as above, we have the geometric decomposition of $\mathbb{F}_q^n$

(a) $\mathbb{F}_q^n = H_1 \perp \cdots \perp H_m \perp L_1 \perp H'_1 \perp \cdots \perp H'_{m'} \perp W'$ and $\mathcal{C} = \langle x_1, \ldots, x_l, x_{l+1}, x'_{l+1}, \ldots, x_m, x'_m, x_{m+1} \rangle$

(b) $\mathbb{F}_q^n = H_1 \perp \cdots \perp H_m \perp H_{m+1} \perp H'_1 \perp \cdots \perp H'_{m'} \perp W'$ and $\mathcal{C} = \langle x_1, \ldots, x_l, x_{l+1}, x'_{l+1}, \ldots, x_{m+1}, x'_{m+1} \rangle$

(c) $\mathbb{F}_q^n = H_1 \perp \cdots \perp H_m \perp L_1 \perp L_2 \perp H'_1 \perp \cdots \perp H'_{m'} \perp W'$ and $\mathcal{C} = \langle x_1, \ldots, x_l, x_{l+1}, x'_{l+1}, \ldots, x_m, x'_m, x_{m+1}, x_{m+2} \rangle$

From the construction of the previous basis of $\mathbb{F}_q^n$ and Proposition 4, it follows that a linear code can be written as the linear subspace generated by a part of a geometric basis of type $r, s, t$ with $s + t \leq 4$, because we have generated hyperbolic planes until their complement ($W$ and $W'$) is a linear subspace of dimension lower than or equal to two. We also have that $t \leq 2$ because in the bases of $W$ and $W'$ there is at most one element $x$ such that $B(x, x) = g$. Note that for $q \equiv 3 \mod 4$ one has that $t = 0$. □ □

We say that a linear code $\mathcal{C}$ given by the generators $\mathcal{C} = \langle x_1, \ldots, x_k \rangle$ is given in the **standard geometric form** if the matrix of $B$ restricted to $x_1, \ldots, x_k$ is the same matrix as the one of $B$ restricted to the generators of $\mathcal{C}$ of the basis obtained in Theorem 12.

Next example shows a geometric decomposition of $\mathbb{F}_3^{12}$ compatible with the Golay code $\mathcal{G}_{12}$ [22], which is a self-dual code.

**Example 2.** *The Golay code $\mathcal{G}_{12}$ is a self-dual code over $\mathbb{F}_3$ with generator matrix [22]:*

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

*One has that for $\mathcal{G}_{12} \subset \mathbb{F}_3^{12}$, the standard decomposition of $\mathbb{F}_3^{12}$ compatible with $\mathcal{G}_{12}$ is the orthogonal sum of 6 hyperbolic planes, where the first geometric generator of each one belongs to the code and the second one does not. The matrix $M$ of a standard geometric decomposition is*

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 & 2 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 2 \\ 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 2 & 0 & 0 & 2 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 2 & 0 & 2 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 1 & 2 & 2 & 1 & 0 & 2 \end{pmatrix}$$

*A basis of the code are the rows 1,3,5,7,9,11. One has that*

$$J_{6,0,0} = MM^t = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

## 4.2 Characteristic 2

Now let $\mathbb{F}_q$ be a field of characteristic two. By the results in Section 3 we can write $\mathbb{F}_q^n$ as an orthogonal sum of hyperbolic planes, one-dimensional linear varieties and, at most, one elliptic plane.

We say that $\mathbb{F}_q^n$ has a **geometric decomposition of type** $r, s, t$ if

$$\mathbb{F}_q^n = H_1 \perp \cdots \perp H_r \perp L_1 \perp \cdots \perp L_s, \text{ with } t = 0, \text{ or}$$

$$\mathbb{F}_q^n = H_1 \perp \cdots \perp H_r \perp L_1 \perp \cdots \perp L_s \perp E, \text{ with } t = 1$$

where $H_1, \ldots, H_r$ are hyperbolic planes, $L_1, \ldots, L_s$ are non-isotropic one-dimensional linear varieties and $E$ is an elliptic plane. Each hyperbolic plane is generated by two geometric generators $H_i = \langle x_{2i-1}, x_{2i} \rangle$, $i = 1, \ldots, r$, each one-dimensional linear variety is generated by a geometric generator $L_i = \langle x_{2r+i} \rangle$, $i = 1, \ldots, s$ and the elliptic plane is generated by two geometric generators, $E = \langle x_{n-1}, x_n \rangle$ if $t = 1$. One has that $\{x_1, \ldots, x_n\}$ is a basis of $\mathbb{F}_q^n$, called **basis of the geometric decomposition**.

Let $M$ be the matrix whose rows are the elements of the the geometric decomposition, then one has that $MM^t = J_{r,s,t}$. That is, $J_{r,s,t}$ is the

matrix of $B$ in such a basis.

$$J_{r,s,0} = \begin{pmatrix} 0 & 1 & & & & & & & \\ 1 & 0 & & & & & & & \\ & & \ddots & & & & & & \\ & & & 0 & 1 & & & & \\ & & & 1 & 0 & & & & \\ & & & & & 1 & & & \\ & & & & & & \ddots & & \\ & & & & & & & 1 & \end{pmatrix}$$

$$J_{r,s,1} = \begin{pmatrix} 0 & 1 & & & & & & & & \\ 1 & 0 & & & & & & & & \\ & & \ddots & & & & & & & \\ & & & 0 & 1 & & & & & \\ & & & 1 & 0 & & & & & \\ & & & & & 1 & & & & \\ & & & & & & \ddots & & & \\ & & & & & & & 1 & & \\ & & & & & & & & 0 & 1 \\ & & & & & & & & 1 & 1 \end{pmatrix}$$

A basis $\{x_1, \ldots, x_n\}$ of $\mathbb{F}_q^n$ is said to be a **compatible basis with respect to a decomposition of type** $r, s, t$ if each $\{x_{2i-1}, x_{2i}\}$, with $i = 1, \ldots, r$, is a geometric basis of a hyperbolic plane; each $x_{2r+i}$, with $i = 1, \ldots s$, generates a one-dimensional linear variety; $\{x_{2r+s+1}, x_{2r+s+2}\}$ is a geometric basis of an elliptic plane (if $t = 1$) in such a way that all of these subspaces are pairwise orthogonal. Or equivalently, if the matrix of $B$ in such a basis is equal to $J_{r,s,t}$.

Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a linear code, we say that $\mathcal{C}$ is **compatible with a geometric decomposition of type** $r, s, t$ if there exists a basis $\{x_1, \ldots, x_n\}$ of $\mathbb{F}_q^n$ compatible with such a decomposition, in such a way that there exists $I \subset \{1, \ldots, n\}$ such that $\{x_i \mid i \in I\}$ is a basis of $\mathcal{C}$.

The next results allows us to compute a geometric decomposition compatible with a given code in characteristic 2.

**Theorem 13.** *Let $\mathbb{F}_q$ be of characteristic 2. Any linear code $\mathcal{C} \subset \mathbb{F}_q^n$ is compatible with at least one geometric decomposition. Furthermore, there is a computable geometric basis, called standard, compatible with $\mathcal{C}$, of type $r, s, t$ with $s \leq 4$ and $t = 0$, or, $s \leq 2$ and $t = 1$. A geometric decomposition with an elliptic plane ($s \leq 2$, $t = 1$) is only possible when $(1, \ldots, 1) \in \mathrm{rad}(\mathcal{C})$, that is, when $(1, \ldots, 1) \in \mathcal{C}$ and all the elements of $\mathcal{C}$ are isotropic.*

*Proof.* One has that $\mathcal{C} = \mathrm{rad}(\mathcal{C}) \perp \mathcal{C}_1$. We shall consider two cases, $z = (1, \ldots, 1) \in \mathrm{rad}(\mathcal{C})$ with $n$ even, and the general case. In this particular case ($z \in \mathrm{rad}(\mathcal{C})$ with $n$ even) we consider an elliptic plane because $z$ cannot belong to a hyperbolic plane, since, as we proved in proposition 7, there exists no isotropic vector in $\mathbb{F}_q^n$ orthogonal to $z$.

Let $z \in \mathcal{C}$, one has that $z \in \mathrm{rad}(\mathcal{C})$ if and only if all the elements of $\mathcal{C}$ are isotropic, that is, if $\mathcal{C} \subset S$. For instance, for a self-dual code we consider an elliptic plane: let $\mathcal{C}$ be a self-dual code, one has that $z \in \mathcal{C} = \mathrm{rad}(\mathcal{C})$ because otherwise the direct sum of $\mathcal{C}$ and $\langle z \rangle$ would be a vector subspace of index $n/2 + 1$.

First, we prove the general case and, then, the case $(1, \ldots, 1) \in \mathrm{rad}(\mathcal{C})$ with $n$ even. Let $\mathcal{C} = \mathrm{rad}(\mathcal{C}) \perp \mathcal{C}_1$, where $\mathrm{rad}(\mathcal{C}) = \langle x_1, \ldots, x_l \rangle$. Let $S'$ be equal to $S$ for $n$ odd and to $\langle y_1, \ldots y_{n-2} \rangle$ for $n$ even, where $\{y_1, \ldots, y_{n-2}, (1, \ldots, 1)\}$ is a basis of $S$. One has that $S'$ is non-singular, has dimension greater than or equal to $n-2$ and that $\mathrm{rad}(\mathcal{C}) \subset S'$ (by Proposition 7).

We claim that we can compute $x'_1, \ldots, x'_l \in \mathbb{F}_q^n$ such that $x_i, x'_i$ are the geometric generators of a hyperbolic plane and, moreover, the hyperbolic planes $H_i = \langle x_i, x'_i \rangle$ and $\mathcal{C}_1$ are pairwise orthogonal. That is, one has that

$$\mathcal{C}' = H_1 \perp \cdots \perp H_l \perp \mathcal{C}_1$$

where $\mathcal{C}'$ contains $\mathcal{C}$ and is non-singular. We prove the construction of $\mathcal{C}'$ by induction on $l$.

For $l = 0$ there is nothing to prove. The subspace $\mathcal{C}_0 = \langle x_1, \ldots, x_{l-1} \rangle \perp \mathcal{C}_1$ is orthogonal to $x_l$ but does not contain it. One has that $x_l \in \mathcal{C}_0^\perp$ but $x_l \notin \mathrm{rad}(\mathcal{C}_0^\perp) = \mathrm{rad}(\mathcal{C}_0)$. Let $\mathcal{C}_0^\perp = \langle x_1, \ldots, x_{l-1} \rangle \perp U$. One has that $U \cap S'$ is a non-singular vector space that contains $x_l$. Therefore there exists $y \in U \cap S'$ such that $B(x_l, y) \neq 0$, since $x_l$ is isotropic. The plane generated by $x_l, y$ is non-singular and is contained in $\mathcal{C}_0^\perp$, so by Proposition 9 it is generated by a geometric basis $H_l = \langle x_l, x'_l \rangle$. Since $H_l \subset \mathcal{C}_0^\perp$, then $\mathcal{C}_0 \perp H_l$ and $\mathcal{C}_0 \subset H_l^\perp$. As the radical of $\mathcal{C}_0$ has dimension $l-1$, by inductive hypothesis we can compute geometric bases $\{x_i, x'_i\}$ of $H_i$ in $H_l^\perp$, for $i = 1, \ldots, l-1$ such that they are pairwise orthogonal and also to $\mathcal{C}_1$, and since they are orthogonal to $H_l$ and $H_l$ is orthogonal to $\mathcal{C}_1$, the construction of $\mathcal{C}'$ holds.

Therefore, we have $\mathcal{C}' = H_1 \perp \cdots \perp H_l \perp \mathcal{C}_1$, where $H_i = \langle x_i, x'_i \rangle$, with $x'_i \notin \mathcal{C}$. Moreover, $\mathcal{C}'$ is non-singular and one has that $\mathbb{F}_q^n = H_1 \perp \cdots \perp H_l \perp \mathcal{C}_1 \perp \mathcal{C}'^\perp$.

Since $\mathcal{C}_1$ is non-singular, by Proposition 11 we can consider $\mathcal{C}_1$ as a sum of hyperbolic planes and a vector subspace $W$ of dimension 1 or 2 (if the dimension of $\mathcal{C}_1$ is lower than 3 we do not consider any hyperbolic plane and $\mathcal{C}_1 = W$). Hence, we have $\mathcal{C}_1 = H_{l+1} \perp \cdots \perp H_m \perp W$, where $H_{l+i} = \langle x_{l+i}, x'_{l+i} \rangle$.

By Proposition 11 we can have three different geometries for $W$:

(a) If $\dim(W) = 1$, we write $W = \langle x \rangle$. Moreover, $x$ is non-isotropic since $B$ is non-degenerate. We consider $x_{m+1} \in W$ such that $B(x_{m+1}, x_{m+1})$ is equal to 1 and $W = L_1 = \langle x_{m+1} \rangle$.

(b) If $\dim(W) = 2$ and $W$ contains two linearly independent isotropic vectors (or equivalently $\sum x_i = 0$, for all $x \in W$) then $W$ is a hyperbolic plane, $W = H_{m+1} = \langle x_{m+1}, x'_{m+1} \rangle$, by proposition 9.

(c) If $\dim(W) = 2$ and $W$ does not contain two lines of isotropic vectors (or equivalently, there exists $x \in W$ with $\sum x_i \neq 0$) then, by Proposition 9, $W$ is an elliptic plane and it can be generated by two orthonormal vectors $L_1 = \langle x_{m+1} \rangle$, $L_2 = \langle x_{m+2} \rangle$, where $W = L_1 \perp L_2$.

We decompose $\mathcal{C}'^{\perp}$ in an analogous way to $\mathcal{C}_1$ (using Proposition 11) and we obtain

$$\mathcal{C}'^{\perp} = H'_1 \perp \cdots \perp H'_{m'} \perp W'$$

With notations as above, we have the following geometric decomposition of $\mathbb{F}_q^n$

(a) $\mathbb{F}_q^n = H_1 \perp \cdots \perp H_m \perp L_1 \perp H'_1 \perp \cdots \perp H'_{m'} \perp W'$ and
$\mathcal{C} = \langle x_1, \ldots, x_l, x_{l+1}, x'_{l+1}, \ldots, x_m, x'_m, x_{m+1} \rangle$

(b) $\mathbb{F}_q^n = H_1 \perp \cdots \perp H_m \perp H_{m+1} \perp H'_1 \perp \cdots \perp H'_{m'} \perp W'$ and
$\mathcal{C} = \langle x_1, \ldots, x_l, x_{l+1}, x'_{l+1}, \ldots, x_{m+1}, x'_{m+1} \rangle$

(c) $\mathbb{F}_q^n = H_1 \perp \cdots \perp H_m \perp L_1 \perp L_2 \perp H'_1 \perp \cdots \perp H'_{m'} \perp W'$ and
$\mathcal{C} = \langle x_1, \ldots, x_l, x_{l+1}, x'_{l+1}, \ldots, x_m, x'_m, x_{m+1}, x_{m+2} \rangle$

From the construction of the previous basis of $\mathbb{F}_q^n$, it follows that a linear code $\mathcal{C}$, such that $(1, \ldots, 1) \notin \mathrm{rad}(\mathcal{C})$ with $n$ even, can be written as the linear subspace generated by a part of a geometric basis of type $r, s, t$ with $s \leq 4$ and $t = 0$, because we have generated hyperbolic planes until their complement ($W$ and $W'$) is a linear subspace of dimension lower than or equal to two which may be decomposed using Proposition 9.

Let us consider $z \in \mathrm{rad}(\mathcal{C})$, when $n$ is even. Let $\mathrm{rad}(\mathcal{C}) = \langle x_1, \ldots, x_l, z \rangle$ and $R = \langle x_1, \ldots, x_l \rangle$. Let $\mathcal{C}_R = R \perp \mathcal{C}_1$, since $z \notin \mathrm{rad}(\mathcal{C}_R) = R$, as in the general case, we can compute $x'_1, \ldots, x'_l \in \mathbb{F}_q^n$ such that $x_i, x'_i$ are the geometric generators of a hyperbolic plane and, moreover, the hyperbolic planes $H_i = \langle x_i, x'_i \rangle$, and $\mathcal{C}_1$ are pairwise orthogonal. That is, one has that

$$\mathcal{C}'_R = H_1 \perp \cdots \perp H_l \perp \mathcal{C}_1$$

where $\mathcal{C}'_R$ contains $\mathcal{C}_R$ and is non-singular.

Since $\mathcal{C}_1$ is non-singular, by Proposition 11 we can consider $\mathcal{C}_1$ as a sum of hyperbolic planes, that is, we have the geometry (b) of the general case since all the elements of $\mathcal{C}_1$ are isotropic. Therefore, we have $\mathcal{C}_1 = H_{l+1} \perp \cdots \perp H_m$, where $H_{l+i} = \langle x_{l+i}, x'_{l+i} \rangle$.

Hence, since all the elements of $\mathcal{C}_R$ are isotropic, one has that $U$, the direct sum of $\mathcal{C}'_r$ and $\langle z \rangle$ can be written in the following way $U = H_1 \perp \cdots \perp H_m \perp \langle z \rangle$. We claim that in $U^{\perp}$ there exists a non-isotropic vector $z'$ such that $z'$ is orthogonal to $\mathcal{C}'_R$ and $B(z, z') = 1$. Let $E = \langle z, z' \rangle$, we have that $E$ is an elliptic plane. Such vector $z'$ is one solution of the following linear system with at most $n$ equations and $n$ variables

$$\begin{cases} B(x_1, z') = 0, \\ B(x'_1, z') = 0, \\ \quad \vdots \\ B(x_m, z') = 0, \\ B(x'_m, z') = 0, \\ B(z, z') = 1, \\ B(z', z') = 1. \end{cases}$$

Therefore, one has that $U' = H_1 \perp \cdots \perp H_m \perp E$ is non-singular and contains $\mathcal{C}$. We decompose $U'^{\perp}$ using proposition 11 and obtain

$$U'^{\perp} = H'_1 \perp \cdots \perp H'_{m'} \perp W'$$

With notations as above, we have the following geometric decomposition of $\mathbb{F}_q^n$:

(d) $\mathbb{F}_q^n = H_1 \perp \cdots \perp H_m \perp E \perp H_1' \perp \cdots \perp H_{m'}' \perp W'$ and
$\mathcal{C} = \langle x_1, \ldots, x_l, x_{l+1}, x'_{l+1}, \ldots, x_{m+1}, x'_{m+1}, z \rangle$

From the construction of the previous basis of $\mathbb{F}_q^n$, it follows that a linear code $\mathcal{C}$, such that $(1, \ldots, 1) \in \mathrm{rad}(\mathcal{C})$ with $n$ even, can be written as the linear subspace generated by a part of a geometric basis of type $r, s, t$ with $s \leq 2$ and $t = 1$, because we have generated hyperbolic planes in $U'^{\perp}$ until $W'$ is a linear subspace of dimension lower than or equal to two that may be decomposed using Proposition 9. □ □

We say that a linear code $\mathcal{C}$ given by the generators $\mathcal{C} = \langle x_1, \ldots, x_k \rangle$ is given in the **standard geometric form** if the matrix of $B$ restricted to $x_1, \ldots, x_k$ is the same matrix as the one of $B$ restricted to the generators of $\mathcal{C}$ of the basis obtained in Theorem 13.

From Theorem 13 it follows that the standard geometric decomposition of $\mathcal{C} = \mathbb{F}_q^n$ is of type $n/2 - 1, 2, 0$ for $n$ even, and $(n-1)/2, 1, 0$ for $n$ odd. The following example shows the geometric decomposition of a self-dual code in characteristic 2.

**Example 3.** *Let $\mathcal{C} \subset \mathbb{F}_2^6$ be the code with generator matrix*

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

*One has that $\mathcal{C}$ is a self-dual code because it has dimension $n/2$ and the sum of the coordinates of the generators of the code, that is, the rows of the generator matrix, are 0 (Proposition 7).*

*Hence, the standard decomposition is given by 2 hyperbolic planes and an elliptic plane. In particular, one has that the matrix $M$ of a standard geometric decomposition is*

$$M = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

*A basis of the code are the rows 1, 3 and 5 of the matrix $M$, which in this case form the same basis as we have previously considered. The geometric decomposition obtained is $\mathbb{F}_2^6 = H_1 \perp H_2 \perp E$. That is, a geometric decomposition of type 2,0,1, hence*

$$J_{2,0,1} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

The following example illustrates how to deal with an elliptic plane when $(1,\dots,1) \notin \mathrm{rad}(\mathcal{C})$.

**Example 4.** *Let $\mathcal{C}$ be the linear code over $\mathbb{F}_2$ with generator matrix*

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

*Let $x_1 = (1,1,0,0)$ and $x_2 = (0,0,0,1)$. One has that $x_1$ is an isotropic vector and that $x_2$ is non-isotropic. Let $x_1' = (0,1,1,0)$, one has that $x_1, x_1'$ are a geometric basis of an hyperbolic plane $H_1 = \langle x_1, x_1' \rangle$ which is orthogonal to $x_2$. An orthogonal vector to $H_1$ and linearly independent to $x_2$ is $y = (1,1,1,1)$. One has that $y$ is isotropic and $y, x_2$ form a geometric basis of an elliptic plane. However, we can consider $x_3 = x_2 + y = (1,1,1,0)$ in such a way that $L_2 = \langle x_2 \rangle$ and $L_3 = \langle x_3 \rangle$ are two non-isotropic linear varieties. Therefore, one has a geometric decomposition of $\mathbb{F}_2^4$ compatible with $\mathcal{C}$ of type $1,2,0$, given by $\mathbb{F}_2^4 = H_1 \perp L_1 \perp L_2$.*

# 5 Linear codes and bilinear algebra

Since we have proved that a linear code is compatible with a geometric decomposition for arbitrary characteristic, from now on, we will work over an arbitrary positive characteristic.

Let $\{x_1,\dots,x_n\}$ be a geometric basis of a geometric decomposition of type $r,s,t$. Let $i \in \{1,\dots,n\}$. We define $i'$ as

- $i+1$ if $x_i$ is the first generator of a hyperbolic plane $H$,
- $i-1$ if $x_i$ is the second generator of a hyperbolic plane $H$,
- $i$ if $x_i$ generates a one-dimensional linear space $L$,
- $i+1$ if $x_i$ is the first generator of an elliptic plane $E$.

We do not define $i'$ when $x_i$ is the second geometric generator of an elliptic plane, because we only consider geometric decompositions with at most one elliptic plane $E$ and where only the first generator of $E$ belongs to the code. In the case where both geometric generators of the elliptic plane $E$ belong to the code, by Proposition 9, we consider two orthonormal generators of linear subspaces $L$ (as in Example 4).

For $I \subset \{1,\dots,n\}$ we define $I' = \{i' \mid i \in I\}$ and $I^\perp = \{1,\dots,n\} \setminus I'$. In this way we can compute the dual code of a linear code using the following result. Note that this result extends Theorem 1 for an arbitrary linear code.

**Theorem 14.** *Let $\mathcal{C}$ be a linear code with geometric decomposition of type $r,s,t$ given by the basis $\{x_1,\dots,x_n\}$ of $\mathbb{F}_q^n$. Let $I \subset \{1,\dots,n\}$ such that $\mathcal{C} = \langle x_i \mid i \in I \rangle$. Then the dual code of $\mathcal{C}$ is $\mathcal{C}^\perp = \langle x_i \mid i \in I^\perp \rangle$.*

*Proof.* From the matrix $J_{r,s,t}$ of the bilinear form $B$ in the geometric basis it follows that $\langle x_i \rangle^\perp = \langle x_j \mid j \neq i' \rangle$. Therefore, $\mathcal{C}^\perp = \langle x_j \mid j \notin I' \rangle = \langle x_i \mid i \in I^\perp \rangle$. □ □

Let $\mathcal{C}$ be a linear code of dimension $k$ with a geometric decomposition of type $r, s, t$ given by the basis $\{x_1, \ldots, x_n\}$ of $\mathbb{F}_q^n$ and $I \subset \{1, \ldots, n\}$ such that $\mathcal{C} = \langle x_i \mid i \in I \rangle$. Furthermore, let $M$ be the $n \times n$-matrix whose rows are the elements of the basis $\{x_1, \ldots, x_n\}$, then one has that $MM^t = J_{r,s,t}$. Let $M(I)$ be the $k \times n$-matrix consisting of the $k$ rows given by $I$, then $M(I)$ is a generator matrix of $\mathcal{C}$. In the same way, $M(I^\perp)$ is a control matrix of $\mathcal{C}$, that is, $M(I^\perp)$ is a generator matrix of the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$.

**Example 5.** *Consider the Matrix $M$ given in Example 3 and the geometric decomposition of type 2,0,1 given by the rows of the matrix $M$, $\{x_1, \ldots, x_6\}$. One has that $\mathbb{F}_2^6 = H_1 \perp H_2 \perp E$.*

*Let $I = \{1, 2, 3\}$ and $\mathcal{C} = \langle x_i \mid i \in I \rangle$. By Theorem 14, the dual code of $\mathcal{C}$ is $\langle x_i \mid i \in I^\perp \rangle$, where $I' = \{2, 1, 4\}$ and $I^\perp = \{1, \ldots, 6\} \setminus I' = \{3, 5, 6\}$.*

We have only considered an elliptic plane at the geometric decomposition when the first geometric generator of the elliptic plane belongs to the code and the second one does not. Its motivation rests on the following fact: if $x_i$ is the second generator of an elliptic plane, then $\langle x_i \rangle^\perp = \langle x_j \mid j \neq i, i-1 \rangle + \langle x_i + x_{i-1} \rangle$, but $x_i + x_{i-1}$ is not an element of the basis of $\mathbb{F}_q^n$ considered.

## 5.1 Stabilizer quantum codes

Stabilizer codes can be constructed from self-orthogonal classical linear codes using the CSS construction (due to Calderbank, Shor and Steane [6, 29]).

**Theorem 15.** [6, 20] *Let $\mathcal{C}$ be a linear $[n, k, d]_q$ error-correcting code such that $\mathcal{C} \subset \mathcal{C}^\perp$. Then, there exists an $[[n, n-2k, \geq d^\perp]]_q$ stabilizer quantum code, where $d^\perp$ denotes the minimum distance of $\mathcal{C}^\perp$.*

If we have a geometric decomposition, we can easily check whether a linear code is self-orthogonal and construct a quantum code using the CSS construction.

**Theorem 16.** *Let $\mathcal{C}$ be a linear $[n, k, d]$ code with geometric decomposition of type $r, s, t$ given by the basis $\{x_1, \ldots, x_n\}$ of $\mathbb{F}_q^n$. Consider $I \subset \{1, \ldots, n\}$ such that $\mathcal{C} = \langle x_i \mid i \in I \rangle$. Let $I \subset I^\perp$, then there exists an $[[n, n-2k, \geq d^\perp]]_q$ stabilizer quantum code.*

*Proof.* By Theorem 14, the dual code of $\mathcal{C}$ is $\mathcal{C}^\perp = \langle x_i \mid i \in I^\perp \rangle$. Thus if $I \subset I^\perp$, the code $\mathcal{C}$ is self-orthogonal and, by Theorem 15, the result holds. □ □

**Example 6.** *Consider the Matrix $M$ given in Example 3 and the geometric decomposition of type 2,0,1 given by the rows of the matrix $M$, $\{x_1, \ldots, x_6\}$. One has that $\mathbb{F}_2^6 = H_1 \perp H_2 \perp E$.*

*Let $I = \{1, 3\}$ and $\mathcal{C} = \langle x_i \mid i \in I \rangle$. Then $I' = \{2, 4\}$ and $I^\perp = \{1, \ldots, 6\} \setminus I' = \{1, 3, 5, 6\}$. By Theorem 16, we can construct a stabilizer quantum code from $\mathcal{C}$ since $I \subset I^\perp$.*

The technique given in the previous result was used in [12, 13, 14, 15] to compute stabilizer quantum codes of $J$-affine variety codes (and toric codes). Theorem 16 shows which codes, with a geometric decomposition as in section 4, can provide stabilizer quantum codes. That is, one can extend the method in [12, 13, 14, 15] for an arbitrary family of codes. Algebraic-geometric codes will be considered in future works. Moreover, an analogous CSS construction also holds for Hermitian duality when the classical code $\mathcal{C}$ is defined over $\mathbb{F}_{q^2}$. The Hermitian metric structure will be studied in future works as well.

## 5.2 LCD codes

LCD codes are linear codes whose radical is equal to zero [23], that is, $\mathcal{C}$ is LCD if $\mathcal{C} \cap \mathcal{C}^\perp = \{0\}$. If we have a geometric decomposition, we can easily check whether a linear code is LCD.

**Theorem 17.** *Let $\mathcal{C}$ be a linear code with geometric decomposition of type $r, s, t$ given by the basis $\{x_1, \ldots, x_n\}$ of $\mathbb{F}_q^n$. Let $I \subset \{1, \ldots, n\}$ such that $\mathcal{C} = \langle x_i \mid i \in I \rangle$. One has that $\mathcal{C}$ is LCD if and only if $I \cap I^\perp = \emptyset$.*

*Proof.* By Theorem 14, the dual code of $\mathcal{C}$ is $\mathcal{C}^\perp = \langle x_i \mid i \in I^\perp \rangle$. Thus, $I \cap I^\perp = \emptyset$ if and only if $\mathcal{C} \cap \mathcal{C}^\perp = \{0\}$. □ □

**Example 7.** *Consider the Matrix $M$ given in Example 3 and the geometric decomposition of type 2,0,1 given by the rows of the matrix $M$, $\{x_1, \ldots, x_6\}$. One has that $\mathbb{F}_2^6 = H_1 \perp H_2 \perp E$.*

*Let $I = \{1, 2, 3, 4\}$ and $\mathcal{C} = \langle x_i \mid i \in I \rangle$. We have that $I' = \{2, 1, 4, 3\}$ and $I^\perp = \{1, \ldots, 6\} \setminus I' = \{5, 6\}$. By Theorem 17, $\mathcal{C}$ is an LCD code since $I \cap I^\perp = \emptyset$.*

The tecnique given in the previous result was used in [16] to compute new LCD codes from $J$-affine variety codes (and toric codes). Theorem 17 shows which codes, with a geometric decomposition as in section 4, are LCD. In the same way as for quantum codes, one can extend the method in [16] for an arbitrary family of codes. LCD codes coming from affine variety codes will be considered in future works.

## 5.3 Minimum distance of a linear code

The following result extends [21, Proposition 1] and [27, Proposition 8] of generalized toric codes for arbitrary linear codes.

**Theorem 18.** *Let $\mathcal{C}$ be a linear code of dimension $k$ with geometric decomposition of type $r, s, t$ given by the basis $\{x_1, \ldots, x_n\}$ of $\mathbb{F}_q^n$ and $I \subset \{1, \ldots, n\}$ such that $\mathcal{C} = \langle x_i \mid i \in I \rangle$. Let $M$ be the $n \times n$-matrix such that $MM^t = J_{r,s,t}$, where a generator matrix of $\mathcal{C}$ is $M(I)$ and $M(I, J)$ is the submatrix of $M$ corresponding to the rows of $I$ and columns of $J$, i.e. $M(I, J) = (m_{i,j})_{i \in I, j \in J}$.*

*(a) Let $d$ be the lowest positive integer such that for every set $J \subset \{1, \ldots, n\}$ with $\#J = n - d + 1$ there exists some $K \subset J$ with $\#K = k$ such that $\det M(I, K) \neq 0$. Then the minimum distance of $\mathcal{C}$ is $d$.*

*(b) Let $d$ be the largest positive integer such that for all $J \subset \{1,\dots,n\}$ with $\#J = d-1$ there exists $D \subset I^\perp$ with $\#D = d-1$ such that $\det(D,J) \neq 0$. Then the minimum distance of $\mathcal{C}$ is $d$.*

*Besides, both previous ways of computing the minimum distance are equivalent.*

*Proof.* (a) One has that the minimum distance of a linear code is $d$ if for any $n-d+1$ columns of a generator matrix there exist $k$ linearly independent columns and there are $n-d$ columns that do not contain $k$ linearly independent columns. A generator matrix of $\mathcal{C}$ is $M(I)$, hence the minimum distance of $\mathcal{C}$ is the greatest positive integer $d$ such that any $n-d+1$ columns of $M(I)$ contain $k$ linearly independent columns, and the result holds.

(b) One has that the minimum distance of a linear code is $d$ if any $d-1$ columns of a control matrix are linearly independent and there exist $d$ linearly independent columns. A control matrix of $\mathcal{C}$ is $M(I^\perp)$, hence the minimum distance of $\mathcal{C}$ is the largest positive integer $d$ such that any $d-1$ columns of $M(I^\perp)$ are linearly independent, which is equivalent to the fact that for every $J \subset \{1,\dots,n\}$, $\#J = d-1$, there exists one minor $M(I^\perp, J)$ of size $d-1$ whose determinant is different from 0, and the result holds.

The equivalence between these two results is clear because both compute the minimum distance of a linear code $\mathcal{C}$ and, moreover, both ways of computing the minimum distance are dual. In order to prove it we use Plücker geometry.

Let $M$ be the matrix whose rows are the elements of the basis $\{x_1,\dots,x_n\}$ of $\mathbb{F}_q^n$, that is, the matrix of the linear transformation from the canonical basis $\{e_1,\dots,e_n\}$ into $\{x_1,\dots,x_n\}$, $N = \{1,\dots,n\}$ and $M^*$ the matrix of the linear transformation from the canonical basis $\{e_1^*,\dots,e_n^*\}$ into $\{x_1^*,\dots,x_n^*\}$. Therefore, $x_1 \wedge \cdots \wedge x_k = \sum_{j_i \in N} \det(M(I,K)) e_{j_1} \wedge \cdots \wedge e_{j_k}$, where $K = j_1,\dots,j_k$. Since $MM^t = J_{r,s,t}$, one has that $M^* = J_{r,s,t}M$.

Let $\zeta(x_1 \wedge \cdots \wedge x_k) = x_{k+1}^* \wedge \cdots \wedge x_n^*$. Then

$$\zeta(x_1 \wedge \cdots \wedge x_k) = \sum_{j_i \in N \setminus K} \det(M^*(N \setminus I, N \setminus K)) e_{j_1}^* \wedge \cdots \wedge e_{j_{n-k}}^*$$

but since $\zeta$ is linear, one has that $\zeta(x_1 \wedge \cdots \wedge x_k) =$

$$\sum_{j_i \in K} \det(M(I,K)) \zeta(e_{j_1} \wedge \cdots \wedge e_{j_k}) = \sum_{j_i \in K} \det(M(I,K)) e_{j_1}^* \wedge \cdots \wedge e_{j_k}^*$$

Hence one has that $\det(M(I,K)) = \det(M^*(N \setminus I, N \setminus K)) = \det(J_{r,s,t}M(N \setminus I, N \setminus K)) = \det(M(I \setminus I', N \setminus K)) = \det(M(I^\perp, N \setminus K))$. □ □

In [21, Proposition 1], which is extended by the previous result, the structure of Vandermonde matrix in several variables of the generator matrix of the generalized toric code is used to compute explicitly the minimum distance of two families of codes. For an arbitrary linear code we do not have such an structure and the previous result is not a priori useful. However, the geometric decomposition of a linear code may give rise to

the explicit computation of the minimum distance of certain families of linear codes. This will be studied in future works.

## acknowledgement

This problem was proposed by Antonio Campillo, I thank him for his many helpful comments. The author gratefully acknowledges the support from RYC-2016-20208 (AEI/FSE/UE), the support from The Danish Council for Independent Research (Grant No. DFF–4002-00367), and the support from the Spanish MINECO/FEDER (Grants No. MTM2015-65764-C3-2-P and MTM2015-69138-REDT).

## References

[1] E. Artin: *Algèbre géométrique*. Cahiers Scientifiques, Paris Gauthier-Villars, Editeur (1967).

[2] M. Bras-Amorós, M.E. O'Sullivan: Duality for some families of correction capability optimized evaluation codes. Adv. Math. Commun. **2**(1), 15–33 (2008).

[3] M. Braun, T. Etzion, A. Vardy: Linearity and complements in projective space. *Linear Algebra Appl.*, **430** 57–70 (2013).

[4] A.R. Calderbank, E.M. Rains, P.W. Shor, N.J.A. Sloane: Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.* **76** 405–409 (1997).

[5] A.R. Calderbank, E.M. Rains, P.W. Shor, N.J.A. Sloane: Quantum error correction via codes over GF(4). *IEEE Trans. Inf. Theory* **44** (1998) 1369–1387.

[6] A.R. Calderbank, P. Shor: Good quantum error-correcting codes exist. *Phys. Rev. A* **54** 1098-1105 (1996).

[7] C. Carlet and S. Guilley: Complementary dual codes for countermeasures to side-channel attacks. *Adv. Math. Commun.*, **10**(1) 131–150 (2016).

[8] C. Carlet, S. Mesnager, C. Tang, Y. Qi: Linear codes over $\mathbb{F}_q$ which are equivalent to LCD codes. *ArXiv:*1703.04346 (2017).

[9] L.E. Dickson: *Linear groups. with an exposition of the Galois field theory*. Dover Publications (1958).

[10] J. Dieudonné: *La géométrie des groupes classiques (troisième édition)*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 5, Springer-Verlag (1971).

[11] J. Dieudonné: *Sur les groupes classiques (troisième édition)*. Publications de L'Institut de Mathématique de L'Université de Strasbourg, Hermann Paris (1981).

[12] C. Galindo, O. Geil, F. Hernando, D. Ruano: On the distance of stabilizer quantum codes from $J$-affine variety codes. *Quantum Inf. Process.* **16**, 111 (2017).

[13] C. Galindo, F. Hernando: Quantum codes from affine variety codes and their subfield subcodes. *Des. Codes Crytogr.* **76**, 89–100 (2015).

[14] C. Galindo, F. Hernando, D. Ruano: New quantum codes from evaluation and matrix-product codes. *Finite Fields Appl.* **36**, 98–120 (2015).

[15] C. Galindo, F. Hernando, D. Ruano: Stabilizer quantum codes from $J$-affine variety codes and a new Steane-like enlargement. *Quantum Inf. Process.* **14**, 3211–3231 (2015).

[16] C. Galindo, F. Hernando, D. Ruano: New binary and ternary LCD codes. *ArXiv:*1710.00196 (2017).

[17] J.P. Hansen: *Toric varieties Hirzebruch surfaces and error-correcting codes*. Appl. Algebra Engrg. Comm. Comput. **13**(4) 289–300 (2002).

[18] J.W.P. Hirschfeld: *Projective geometries over finite fields, second edition*. Oxford Mathematical Monographs, Oxford University Press (1998).

[19] X. Hou, F. Oggier: On LCD codes and lattices. *Proc. IEEE Int. Symp. on Inform. Theory* 1501–1505 (2016).

[20] A. Ketkar, A. Klappenecker, S. Kumar, P.K. Sarvepalli: Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inf. Theory* **52** 4892–4914.

[21] J. Little, R. Schwarz: *On toric codes and multivariate Vandermonde matrices*. Appl. Algebra Engrg. Comm. Comput. **18**(4), 349–367 (2007).

[22] F.J. Macwilliams, N.J.A. Sloane: *The theory of error-correcting codes*. North-Holland mathematical library, vol. 16, North-Holland (1977).

[23] J.L. Massey: Linear codes with complementary duals. *Discrete Math.*, **106/107** 337–342 (1992).

[24] V. Pless: *On the uniqueness of the Golay codes*. J. Combin. Theory **5**, 215–228 (1968).

[25] V. Pless: *A classification of self-orthogonal codes over GF(2)*. Discrete Math. **3**, 209–246 (1972).

[26] V. Pless: N.J.A. Sloane: *On the classification and enumeration of self-dual codes*. J. Combin. Theory Ser. A **18**, 313–335 (1975).

[27] D. Ruano: *On the structure of generalized toric codes*. J. Symbolic Comput. **44**(5) 499–506 (2009).

[28] J.-P. Serre: *Cours d'arithmétique*. Le Mathématicien, Presses Universitaires de France (1970).

[29] A.M. Steane: Simple quantum error correcting codes. *Phys. Rev. Lett.* **77** 793–797 (1996).