

# Metric Structure of Linear Codes and Algebraic-Geometry Codes

José Ignacio Farrán\*, Diego Ruano†

January 24, 2007

## Abstract

We use the study of bilinear forms over a finite field to give a decomposition of the linear codes similar to the one in [10] for generalized toric codes. Such decomposition, called geometric decomposition of a linear code and which can be obtained in a constructive way, allows to express easily the dual of a linear code and gives a method to estimate the minimum distance. The proofs for characteristic 2 are different, but they will be developed parallel. This allows us to obtain a new paradigm to define the family of linear codes. We also study this decomposition for Algebraic Geometry Codes.

Generalized toric codes are an extension of Toric codes [2]. The metric structure of generalized toric codes [10] gave rise to this work, which obtains a similar structure for an arbitrary linear code. Moreover, we extend the main results in [10] to arbitrary linear codes.

One can find an introduction to geometry over finite fields, and in particular to bilinear forms, in [3]. We refer to [1] for the results over bilinear forms. Some applications to self-dual and self-orthogonal codes of the geometry over finite fields can be found in [7, 8, 9].

From now on, we will only 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 [6]. Here and subsequently,  $\mathbb{F}_q^n$  will be the vector space over  $\mathbb{F}_q$  with the non-degenerated symmetric bilinear form  $B$  whose associated matrix is the identity matrix, we consider linear codes  $C \subset \mathbb{F}_q^n$ .

Let  $H \subset \mathbb{F}_q^n$  be a two-dimensional subvector space, it is said that  $H$  is a **hyperbolic plane** if there exist  $x_1, x_2$  such that they generate  $H$  and

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

---

\*Partially supported by MEC MTM2004-00958 (Spain) Address: Department of Applied Mathematics, University of Valladolid, 40005-Sevogia, Spain. E-mail: ignfar@eis.uva.es

†Partially supported by DASM0D-Cluster of Excellence in Rhineland-Palatinate (Germany) and MEC MTM2004-00958 (Spain). Address: Department of Mathematics, University of Kaiserslautern, 67653-Kaiserslautern, Germany. E-mail: ruano@mathematik.uni-kl.de

hence,  $H$  is non-singular. Both ordered generators  $x_1, x_2$  are called **geometric generators or geometric basis of  $H$** , the matrix of  $B$  restricted to  $H$  in the geometric basis is

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

**Proposition 1.** *Let  $\mathbb{F}_q$  with characteristic different from 2. A two-dimensional non-singular subspace of  $\mathbb{F}_q^n$  which contains an isotropic vector is a hyperbolic plane.*

In this first result one can see that the study for characteristic 2 is different from the other case. In particular, this result is not valid for characteristic 2 as the next example shows.

**Example 2.** 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.

In the basis  $\{(1, 1), (0, 1)\}$  of  $\mathbb{F}_q^2$  the associated matrix of  $B$  is

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

and we therefore say that  $\mathbb{F}_q^2$  is an elliptic plane.

Namely, we say that a non-singular two-dimensional subvector space  $E \subset \mathbb{F}_q^n$  is an **elliptic plane** if there exist  $x_1, x_2$  which generate  $E$  and such that

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

Both ordered generators  $x_1, x_2$  are called **geometric generators or geometric basis of  $E$** , the matrix of  $B$  restricted to  $E$  in the geometric basis is

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

## 1 Geometric decompositions in characteristic different from 2

Firstly, we present  $B$  with characteristic different from 2 and then, in section 2, with characteristic 2 since, as we have already said, its study is different.

One has that  $-1$  is a square in the field  $\mathbb{F}_q$  if and only if  $q \equiv 1 \pmod{4}$ . 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 in the field, the previous equation has at least one solution and therefore there are isotropic vectors. If





basis of the code. We prove that every linear code over a field of characteristic 2 is compatible with a geometric decomposition with  $s \leq 4$  and  $t = 0$  or, if the code is self-dual,  $s = 0$  and  $t = 1$ .

**Theorem 4.** *Let  $\mathbb{F}_q$  have characteristic 2. Any linear code  $\mathcal{C} \subset \mathbb{F}_q^n$  is compatible with at least one geometric decomposition.*

*Proof (Sketch).*

Let  $\mathcal{C} = \text{rad}(\mathcal{C}) \perp \mathcal{C}_1$ , where  $\text{rad}(\mathcal{C}) = \langle x_1, \dots, x_l \rangle$ . We consider two cases,  $l = n/2$  with  $n$  even and the rest of the cases. First, we prove the general case ( $l \neq n/2$ ) and, then, the case  $l = n/2$  for  $n$  even.

One can compute  $x'_1, \dots, x'_l \in \mathcal{C}_1$  such that  $x_i, x'_i$  are the geometric generators of a hyperbolic plane and, moreover, the hyperbolic planes  $H_i = \langle x_i, x'_i \rangle$  are orthogonal to each other and to  $\mathcal{C}_1$ .

Since  $\mathcal{C}_1$  is non-singular we can consider  $\mathcal{C}'$  as a sum of hyperbolic planes and a one or two-dimensional linear space  $W$ , which gives us 3 different geometric decompositions (compatible with  $\mathcal{C}$ ) for  $\mathbb{F}_q^n$ .

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

Let  $l = n/2$  with  $n$  even, that is,  $\mathcal{C}$  is self-dual. We can compute  $x'_1, \dots, x'_{n/2}$  in  $\mathcal{C}_1$  such that  $x_i, x'_i$  are geometric generators of an hyperbolic plane for  $i = 1, \dots, n/2 - 1$  and  $x_{n/2}, x'_{n/2}$  are geometric generators of an elliptic plane. Furthermore, the hyperbolic planes  $H_i = \langle x_i, x'_i \rangle$  and the elliptic plane  $E = \langle x_{n/2}, x'_{n/2} \rangle$  are orthogonal to each other.

Hence, we have the following geometric decomposition of  $\mathbb{F}_q^n$

- (d)  $\mathbb{F}_q^n = H_1 \perp \dots \perp H_{n/2-1} \perp E$  and  
 $\mathcal{C} = \langle x_1, \dots, x_{n/2} \rangle$

□

### 3 Dual code and minimum distance of a linear code

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 characteristic. When the characteristic is different from 2, we set  $t = 0$  because we do not consider hyperbolic planes in the geometric decomposition.

In this section we extend the results in [10], the computation of the dual code and the minimum distance of generalized toric codes to linear codes.

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 linear space  $L$
- $i + 1$  if  $x_i$  is the first generator of an elliptic plane  $E$

We do not need to define  $i'$  when  $x_i$  is the second geometric generator of a hyperbolic plane because we will 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 hyperbolic plane  $E$  belong to the code we may consider two orthonormal generators of linear subspaces  $L$ .

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

**Proposition 5.** *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  $\mathcal{C}$  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,

$$\mathcal{C}^\perp = \langle x_j \mid j \notin I' \rangle = \langle x_i \mid i \in I^\perp \rangle$$

□

In this way, we have in one matrix both a linear code and its dual code. Let  $\mathcal{C}$  be a linear code with a geometric decomposition of type  $r, s, t$  given by the basis  $\{x_1, \dots, x_n\}$  of  $\mathbb{F}_q^n$  and  $I \subset \{1, \dots, n\}$  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  $\{x_1, \dots, x_n\}$ , therefore one has that  $MM^t = J_{r,s,t}$ . Let  $M(I)$  be the  $k \times n$ -matrix consisting of the  $k$  rows with  $i \in I$ , then  $M(I)$  is a generator matrix of  $\mathcal{C}$ . In the same way,  $M(I^\perp)$  is a control matrix of  $\mathcal{C}$ .

The following result extends for arbitrary linear codes [5, Proposition 2.1] and proposition [10, Proposition 8] of generalized toric codes. Furthermore, we prove that both ways of computing the minimum distance are equivalent.

**Theorem 6.** *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  $\mathbb{F}_q^n$  and  $I \subset \{1, \dots, n\}$  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 all set  $J \subset \{1, \dots, n\}$  with  $\#J = n - d + 1$  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  $\#J = d - 1$  exists  $D \subset I^\perp$  with  $\#D = d - 1$  such that  $\det(D, J) \neq 0$ . Then the minimum distance of  $\mathcal{C}$  is  $d$ .

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

## 4 Orthogonal Group and Linear Codes

In this section we develop another application of the geometric structure of linear codes, namely, its relation with the orthogonal group.

The geometric decomposition of a linear code given by theorems 3 and 4 allows us to compute a generator matrix and control matrix of a linear code using subsets of rows of a matrix whose product by its transpose matrix is equal to  $J_{r,s,t}$  with  $(s, t) \in \{0, 1, 2, 3, 4\} \times \{0\} \cup \{0\} \times \{1\}$  and  $2r = n - s - 2t$ , we only consider  $r, s, t$  in this subset. Reciprocally, any subset of rows of a matrix of this type can be considered as a generator matrix of a linear code. Therefore, we have a new description of the linear code and its dual in terms of a new family of matrices. We also show the relationship between this new form of defining the linear codes and the orthogonal group.

For a bilinear form  $B : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$  the **orthogonal group** is the group of linear transformations  $L : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ , which verify  $B(L(x), L(y)) = B(x, y)$  for all  $x, y \in \mathbb{F}_q^n$ , with operation composition of linear transformations. The identity element is the linear transformation  $L(x) = x$ , for all  $x \in \mathbb{F}_q^n$ .

The orthogonal group of the bilinear form  $B$  whose associated matrix is the identity matrix it is denoted by  $\mathcal{O}(n)$  and it is isomorphic to the  $n$ -sized square matrices,  $\mathcal{M}_{n \times n}$ , whose product by its transpose is equal to the identity matrix. That is,

$$\mathcal{O}(n) = \{A \in \mathcal{M}_{n \times n} \mid AA^t = Id\}$$

The group operation of  $\mathcal{O}(n)$  is the product of matrices and its identity element is the identity matrix  $Id$ .

There is a bijective correspondence between the matrices of the orthogonal group,  $\mathcal{O}(n)$ , and the matrices of  $\mathcal{M}_{r,s,t} = \{M \in \mathcal{M}_{n \times n} \mid MM^t = J_{r,s,t}\}$ . Such bijective correspondence is given by any matrix  $T \in \mathcal{M}_{r,s,t}$ : for every  $N \in \mathcal{O}(n)$  we consider  $\phi(N) = TN$ , hence for each  $M \in \mathcal{M}_{r,s,t}$ ,  $\phi^{-1}(M) = T^{-1}N$ . It is obvious that  $\phi$  gives a bijective correspondence of sets between  $\mathcal{O}(n)$  and  $\mathcal{M}_{r,s,t}$  but it is not an isomorphism of groups since the product of two matrices  $M_1, M_2 \in \mathcal{M}_{r,s,t}$  does not verify  $(M_1M_2)(M_1M_2)^t = J_{r,s,t}$ .

Although we do not have an isomorphism of groups between  $\mathcal{O}(n)$  and  $\mathcal{M}_{r,s,t}$ , we can represent the orthogonal group in a way that it acts over  $\mathcal{M}_{r,s,t}$ . For  $r, s, t$  fixed, we consider the group consisting of the set of matrices  $O \in \mathcal{M}_{n \times n}$  such that  $OJ_{r,s,t}O^t = J_{r,s,t}$ , with the multiplication of matrices, that is  $\mathcal{O}_{J_{r,s,t}} = \{O \in \mathcal{M}_{n \times n} \mid OJ_{r,s,t}O^t = J_{r,s,t}\}$ .

**Proposition 7.** Let  $J = J_{r,s,t}$  fixed, then  $\mathcal{O}_J$  is a group with the multiplication of matrices isomorphic to the orthogonal group  $\mathcal{O}(n)$ .

*Proof (Sketch).*

Let  $O_1, O_2 \in \mathcal{O}_J$ , then  $(O_1O_2)J(O_1O_2)^t = O_1O_2JO_2^tO_1^t = O_1JO_1^t = J$ , hence  $\mathcal{O}_J$  is a group whose identity element is the identity matrix.

Since  $J$  and the identity matrix  $Id$  are matrices of the bilinear form  $B$  on different bases, there exists an invertible matrix  $T$  such that  $TT^t = J$ .

For  $O \in \mathcal{O}_J$  let  $\phi(O) = T^{-1}OT$ , then  $\phi$  gives the isomorphism between both groups  $\square$

Therefore, one has that the orthogonal group has the same cardinality as  $\mathcal{M}_{r,s,t}$  and moreover  $\mathcal{O}(n)$  acts over it, because  $MN \in \mathcal{M}_{r,s,t}$  and  $OM \in \mathcal{M}_{r,s,t}$ , with  $N \in \mathcal{O}(n)$  and  $O \in \mathcal{O}_{J_{r,s,t}}$ . That is, the orthogonal group in its two isomorphic versions which we have presented acts over the set of matrices of  $M \in \mathcal{M}_{r,s,t}$ ,  $\mathcal{O}(n)$  on the right and  $\mathcal{O}_{J_{r,s,t}}$  on the left.

This new paradigm of the set of linear codes developed in this work, together with the action of the orthogonal group, opens a new way of study where one can use group theory to solve, or at least in principle reformulate, classic problems of group theory.

Finally we study the geometric decomposition of the algebraic geometry codes [4].

## References

- [1] E. Artin. *Algèbre Géométrique*. Cahiers Scientifiques. Paris Gauthier-Villars, Editeur, 1967.
- [2] J.P. Hansen. Toric varieties Hirzebruch surfaces and error-correcting codes. *Appl. Algebra Engrg. Comm. Comput.*, 13:289–300, 2002.
- [3] J.W.P. Hirschfeld. *Projective Geometry over Finite Fields, second edition*. Oxford Mathematical Monographs. Oxford University Press, 1998.
- [4] T. Høholdt, J.H. van Lint, and R. Pellikaan. Algebraic geometry codes. In V. Pless, W.C. Huffman, and R.A. Brualdi, editors, *Handbook of Coding Theory*, volume 1, chapter 10. Elsevier, 1998.
- [5] J. Little and R. Schwarz. On  $m$ -dimensional toric codes. *ArXiv:cs.IT/0506102*, 2005.
- [6] F.J. Macwilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*, volume 16 of *North-Holland mathematical library*. North-Holland, 1977.
- [7] V. Pless. On the uniqueness of the Golay codes. *J. Combin. Theory*, 5:215–228, 1968.
- [8] V. Pless. A classification of self-orthogonal codes over  $\text{GF}(2)$ . *Discrete Math.*, 3:209–246, 1972.

- [9] V. Pless and N.J.A. Sloane. On the classification and enumeration of self-dual codes. *J. Combin. Theory Ser. A*, 18:313–335, 1975.
- [10] D. Ruano. On the structure of generalized toric codes. *ArXiv:cs.IT/0611010*, 2006. Submitted for publication.