UDC: 514.144:514.742
Original scientific paper

THREE-DIMENSIONAL LINEAR CODES AND COORDINATED FINITE PROJECTIVE PLANE

Flamure SADIKI[1*], Alit IBRAIMI[1], Ylldrita SALIHI[1], Miranda XHAFERI[1]

[1]Department of Mathematics, Faculty of Natural Sciences and Mathematics
**Corresponding author e-mail: flamure.sadiki@unite.edu.mk*

Abstract

In this paper, we study the connections between linear codes and projective geometries over finite fields. Each of these two topics is interesting by itself and has been subject to substantial research. In the last decade, a lot of progress has been made in both areas. We introduce some of the basic ideas and connections between finite projective spaces and coding theory. We begin by studying projective geometries, from this, we introduce a very interesting action in projective planes which lead to many other interesting areas of finite geometry, coordination of the plane. We will coordinate the lines using point coordination.
Our focus then shifts to coding theory and in particular three-dimensional linear codes. The linear code $C_{s,t}\ n, q$ of s-spaces and t-spaces in a projective space $PG\ (n, q), q = p^d$, p prime, is defined as the vector space spanned over Fqby the rows of the incidence matrix of s-spaces and t-spaces. Three-dimensional code applied on the constructed projective model: Fano Plane, like a3-dimensional vector space over F_2. The Fano plane, like a model, occurs in algebraic geometry and geometric algebra in a number of cases, constructing a link between such important mathematical concepts. There are given different ways of constructing the model, taking in consider that it is impossible to label the Fano plane in such a way that all or just five of its lines would be ordinary.

Keywords: Finite Projective space, Fano plane, Coordination, Vector space, Generator matrix, Linear codes.

1. Introduction

Let consider only the finite fields F_q from where $q = p^d$, and p a prime number. We suppose that some of the basic knowledge for finite fields and vector spaces are known [5]. For F_q^x a set of elements from F_q not equal to zero, we define the followings:

Definition 1.1. The pair $G = (\Omega, I)$ is a finite geometry from where Ω is a finite set and $I$is a symmetric and reflexive relation in Ω. Where I is known as an incidence relation in Ω.

Definition 1.2. An n- dimensional projective space on F_q is the set of non- empty spaces of F_q^{n+1}. It is written as $PG_n(F_q)$ or as $PG_n(q)$.

Remark 1.1.$PG_n(q)$is a finite geometry, where Ω is the set of non- empty subspaces of F_q^{n+1}, and I is a symmetric inclusion. One- dimensional subspaces of F_q^{n+1} are known as points, two- dimensional subspaces of F_q^{n+1} are known as straight lines, and n- dimensional subspaces of F_q^{n+1} are known as hyperplanes of a geometry. There are always $1 + q + \cdots + q^n$ points and each straight line contains $q + 1$ points.

Definition 1.3. Let the $a_1, a_2, \dots, a_m$ be the points of $PG_n(q)$. They are collinear if there exists a straight line which contains each a_i point. We can say that the point $p = (x_0, \dots, x_n)$ lies on straight line $L = [y_0, \dots, y_n]$ if and only if $x_0y_0 + x_1y_1 + \cdots + x_ny_n = 0$.
There is a more general definition of projective geometry. Every projective space, for $n \geq 3$, is $PG_n(q)$, if q is a prime number power[4,7]. Anyways, for $n = 2$, there are so many examples of projective spaces that are not a part of F_q^{n+1} structure. In this case, we will describe the general definition of a projective plane:

Definition 1.4. An n- order projective plane is the set (P, B, I) from where P is the set of points, B is the set of straight lines and *I*is the incidence relation between them. The number of points is $n^2 + n + 1$ and the number of straight lines is also $n^2 + n + 1$. Each straight line contains $n + 1$ points and $n + 1$ straight lines intersect in each point. We require that each two points define a unique straight line and that each two straight lines intersect at a unique point[6].

Definition 1.4'. Projective planes. A projective plane is a set of points and lines satisfying the following three axioms.

(A_1) Through every two points, there is exactly one line.
(A_2) Every two lines meet in exactly one point.
(A_3) There exist four points, no three of which are collinear

Example 1.1. (The smallest projective plane model) $PG_2(2)$ is a non- empty subspace of F_2^3. This is a projective plane of order 2, the Fano plane, which is the smallest projective plane. It consists of seven lines and seven points, with three points on a line and, dually, three lines per point, where every pair of points is connected by a line, every line intersects every other line, and there are four points such that no line contains more than two of them. It means $1 + 2 + 2^2 = 7$points, each of them is a vector on a vectorial space.

Fig ure 1. $PG_2(2)$ Fano plane[4]. This is the three- dimensional vectorial space on F_2. We write the points with brackets, and straight lines with square brackets. It is worth to emphasize that although the straightlines seem to intersect, they do not unless the meet at any point.

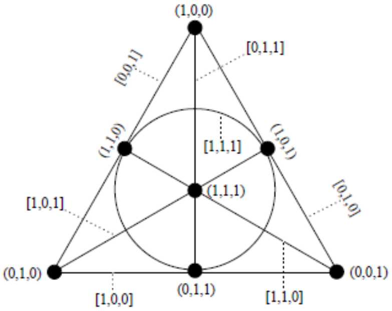

Fig 1.

There are thirty different ways to label the points of the Fano plane by integers from 1 to 7, two labeled Fano planes having zero, one or three lines in common, and each line occurring in six Fano planes. The set of thirty labeled Fano planes can be uniquely partitioned into two sets of fifteen elements each, such that any two labeled Fano's in the same set have just one line in common.

There are the constructed Fano planes, where for triples $\{x, y, z\}$ we add xyz. For a line xyz, we can take $1 \le x < y < z \le 7$ we shall distinguish between the cases when $x + y = c$ and $x + y \ne z$ and call the former/latter ordinary/defective.

A point of the labeled Fano plane is said to be of order s, $0 \le s \le 3$ if there are s defective lines passing through it; hence, in addition to two different kinds of lines, a labeled Fano plane can potentially feature up to four distinct types of points[5,6].

The first 15, added like *F* group of Fano planes are given:

$$F_1 = \{124, 136, 157, \overline{235}, 267, \overline{347}, 456\},\ F_2 = \{127, 136, \overline{145}, 234, 256, 357, 467\},\ F_3 = \{125, 136, 147, 237, \overline{246}, 345, 567\},$$

$$F_4 = \{125, \overline{134}, \overline{167}, 236, 247, 357, 456\},\ F_5 = \{127, 135, 146, 236, 245, \overline{347}, 567\},\ F_6 = \{124, 137, \overline{156}, 236, \overline{257}, 345, 467\},$$

$$F_7 = \{\overline{123}, 147, \overline{156}, 245, 267, 346, 357\},\ F_8 = \{124, 135, \overline{167}, 237, 256, 346, 457\},\ F_9 = \{126, 137, \overline{145}, \overline{235}, 247, 346, 567\},$$

$$F_{10} = \{\overline{123}, \overline{145}, \overline{167}, \overline{246}, \overline{257}, \overline{347}, 356\},\ F_{11} = \{126, \overline{134}, 157, 237, 245, 356, 467\},\ F_{12} = \{125, 137, 146, 234, 267, 356, 457\},$$

$$F_{13} = \{\overline{123}, 146, 157, 247, 256, 345, 367\},\ F_{14} = \{127, \overline{134}, \overline{156}, \overline{235}, \overline{246}, 367, 457\},\ F_{15} = \{126, 135, 147, 234, \overline{257}, 367, 456\}$$

The second 15, added like *F'* group of Fano planes are given:

$$F_1^{'} = \{127, 136, \overline{145}, \overline{235}, \overline{246}, \overline{347}, 567\},\ F_2^{'} = \{125, 136, 147, 234, 267, 357, 456\},\ F_3^{'} = \{124, 136, 157, 237, 256, 345, 467\},$$

$$F_4^{'} = \{127, \overline{134}, \overline{156}, 236, 245, 357, 467\},\ F_5^{'} = \{124, 135, \overline{167}, 236, \overline{257}, \overline{347}, 456\},\ F_6^{'} = \{125, 137, 146, 236, 247, 345, 567\},$$

$$F_7^{'} = \{\overline{123}, \overline{145}, \overline{167}, 247, 256, 346, 357\},\ F_8^{'} = \{126, 135, 147, 237, 245, 346, 567\},\ F_9^{'} = \{124, 137, \overline{156}, \overline{235}, 267, 346, 457\},$$

$$F_{10}^{'} = \{\overline{123}, 146, 157, 245, 267, \overline{347}, 356\},\ F_{11}^{'} = \{125, \overline{134}, \overline{167}, 237, \overline{246}, 356, 457\},\ F_{12}^{'} = \{126, 137, \overline{145}, 234, \overline{257}, 356, 467\},$$

$$F_{13}^{'} = \{\overline{123}, 147, \overline{156}, \overline{246}, \overline{257}, 345, 367\},\ F_{14}^{'} = \{126, \overline{134}, 157, \overline{235}, 247, 367, 456\},\ F_{15}^{'} = \{127, 135, 146, 234, 256, 367, 457\}$$

A detailed inspection of each of the 30 labeled Fano planes shows that they fall, into eight different types, summarized in Table 1. The types α and γ do not exist, because it is impossible to label the Fano plane in such a way that all or just five of its lines would be ordinary [6].

In the Table 1.each of eight types are being uniquely characterized by the number of points of every particular order.

Table 1. The eight distinct types of labeled Fano plane

Type	Points of order			
	0	1	2	3
(α)	(7)	(0)	(0)	(0)
α'	0	0	0	7
β	4	3	0	0
β'	0	0	3	4
(γ)	(2)	(3)	(1)	(0)
γ'	0	1	4	2
δ	1	3	3	0
δ'	0	3	3	1
σ	0	6	0	1
σ'	1	0	6	0

1.2. Coordinating the Projective plane: To show that $\Pi_2(K)$ planes are not the only examples of the projective planes, we need to find other methods to present projective planes and to show that when two given projective planes are isomorphic.

Let consider Π an *n*- order projective plane and let R be the set of symbols with the n- cardinal number so that $1,2 \in R$, $1 \neq 2$. We can spot the "∞" symbol which it does not belong to the *R*.

We choose a straight line from Π and we write it with the l_∞ symbol. Then we consider the two straight lines l_1, l_2 so that the l_1, l_2, l_∞ represent the sides of a triangle.

We consider $X = l_2 l_\infty$, $Y = l_\infty l_1$ and $O = l_1 l_2$. Let the *I* be a point non incident with the sides of the triangle. Now we will use the elements of the R set and the "∞" symbol to coordinate the Π plane according to the *O, X, Y, I* rectangle[5]. Firstly, we consider the three other points: $A = XI \cap l_1$, $B = YI \cap l_2$, $J = AB \cap l_\infty$.

To coordinate Π, we will associate the points from $l_1 \backslash Y$ to the elements of set R, from where 0 will associate with *O* and one will associate with A. If $c \in R$ corresponds to the point $C \in l_1$, then the coordinates of the point *C*are (0, *c*) which can be written as *C* (0, *c*).

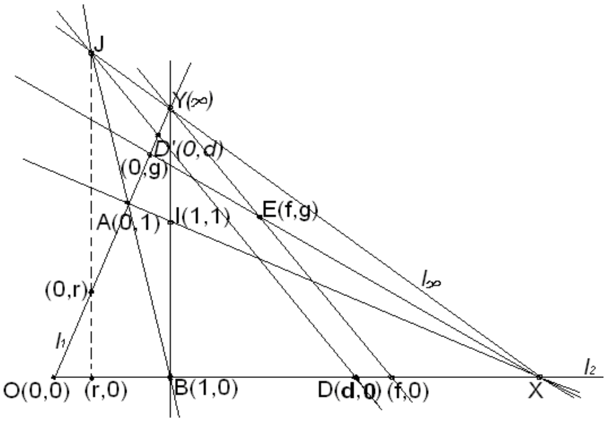

Fig 2.

For any point *D* incident with l_2, $D \neq X$, denote $D' = JD \cap l_1$ and if *D'*(0,*d*), then *D* (0,*d*). Since 0 is associated with the point *O*, then *O*(0,0).

Let *E* be any non-incident point with l_∞.

If $XE \cap l_1$ is the point (0, *g*) and $YE \cap l_2$ is the point (*f*, 0), then point *E*(*f*, *g*). Thus every point from Π^{l_∞} has single coordinates (x, y), where $x,y \in R$.

Let *M* be a point incident with the line l_∞,$M \neq Y$ and *l* the line. If $l \cap l_1 = (0,m)$, then the point M has the coordinate (*m*).

We coordinate the point *Y* with (∞) and in this way, we coordinate every point of Π.

Coordination mainly depends only on the choice of points O, X, Y, I, and the way in which we associate the elements from R with the points of $l_1 \backslash Y$.

(Fig ure 2 and Fig ure 3).

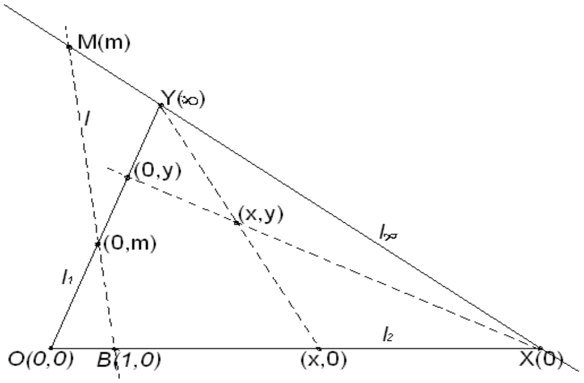

Fig 3.

We will now coordinate the lines using point coordination[4,5]. Let *l* be any straight line not containing the point *Y*.

$\cap\; l_\infty$ =*M(m)* and $l_1 \cap l$=(0,k)then we will denote the coordinates [*m*, *k*] on the line *l*.

Let *l* be the line that contains the point *Y* and $l \neq l_\infty$. If $l \cap l_2$ =(*k',0*) we will denote the line *l* with [k'].

At the end, we denote the line l_∞ with[∞]and in this way we have coordinated each line of Π (Fig ure 4).

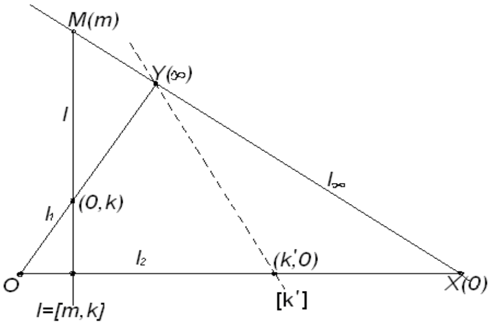

Fig 4.

The Fano plane, like a model, occurs in algebraic geometry and geometric algebra in a number of cases, constructing a link between such important mathematical concepts as design theory, error-correcting codes, Latin squares, skew-Hadamard matrices, Klein's quartic curve etc. [1].

Cardinalities of individual types, listed in Table 2. note a pronounced asymmetry between sets *F* and *F'* of Fano planes constructed in Example 1.1.

Table 2. Cardinalities of individual 8 types of Fano plane

Type	(α)	β	(γ)	δ_1	δ_2	α'	β'	γ'	δ_1'	δ_2'
Set *F*	-	1	-	0	1	1	7	5	0	0
Set *F'*	-	0	-	2	0	5	0	5	1	2
Total	-	1	-	2	1	6	7	10	1	2

2. Linear codes

Theorem 2.1. Let p be a prime number. Then $F_p = Z/pZ$ is a field.

Theorem 2.2. For every power of prime number p^r exists a field F_{p^r} of that order.

Definition 2.1. Let $F_q$be a field with q elements. One q-ary linear code of length *n* and dimension *k* is a linear subspace $C \subseteq F_q^n$of the vector space with dimension k. If its minimum distance is, then the parameters of $C[n, k, d]_q$.
For fixed q we want to construct the code$[n, k, d]_q$with big d, big k and small n. Recall that a code with a minimum distance d allows the correction of transmission errors e, when $2e < d$.
A linear code *C* of length n and dimension k over a finite field *F* is a *k*-dimensional subspace of F^n, and is often called a linear [*n*, *k*] code over *F*[2].
Linear codes are block codes and besides their easy to grasp description, the advantages of linear codes lie in the algebraic structure of the code. In particular, they allow more efficient encoding and decoding algorithms compared to most other codes.

Definition 2.1. A code of length n over an alphabet *A* of size *q*, $q \geq 2$, is a set of words constructed from *A*, i.e. n-tuples with entries in *A*.

Definition 2.2. A linear [*n*, *k*, *d*]-code *C* over F_q is a *k*-dimensional sub-space of the *n*-dimensional vector space $F^n{}_q$ with minimum distance d. From this we see that $|C| = q^k$.

Definition 2.3. The Hamming distance between to code words$x, y \in F_q^n$, denoted $d(x, y)$ is the number of positions in which$x_i \neq y_i$, for $x = (x_1, x_2, ..., x_n)$and$y = (y_1, y_2, ..., y_n)$.

Definition 2.4. The minimum distance *d* of a linear code *C* is the smallest number of positions in which two different elements of *C* differ, $d = \min\{d(x, y) | x, y \in C, x \neq y\}$.

Propositions 2.1. The minimum distance d of a linear code $[n, k, d]_q$ is equal to its minimum weight. Here the weight of a coded word is the number of coordinates with a nonzero entry and the minimum is taken over the nonzero words of the code[1,2].

Definition 2.5. Let *V* be a vector space defined over the field *K* and$v_1, v_2, \dots, v_m \in V$. A linear combination of $v_1, v_2, \dots, v_m$is a decomposition in the form

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m ,$$

where $\lambda_i \in K$. If there exists a linear combination such that $\sum_{i=1}^{m} \lambda_i v_i = 0$ and not all λ_i =0, then the set $\{v_1, \dots, v_m\}$ is called linearly dependent. It is called linearly independent if it is not linearly dependent.
Recall also that a base of a vector space is a maximum set of linearly independent vectors, and that the dimension of *V* is the number of elements in a base. Our linear codes are subspaces of F_q^n, the group of all *n*-bundles, *n*-bundles form a vector space of dimension *n*[3,8].

Definition 2.6. For a code, we have two matrices that determine the code:

1. A generator matrix G of a linear $[n, k, d]$-code C is a $k \times n$ matrix over F_q whose rows form a basis of C.
2. A parity check matrix H of a linear $[n, k, d]$-code C is a $(n - k) \times n$ matrix over F_q whose rows form a basis of $C^{\perp}$.

Propositions 2.2. Let C be a $[n, k]_q$-code and G be a matrix whose rows are words of C. The following properties are equivalent [8]:

1. G is a generating matrix.
2. G has range of k.
3. There exists (k, k) - submatrix with a determinant other than zero.
4. The lines of G are linearly independent

2.1. Three dimensional codes and projective planes: In this section we want to learn how to interpret linear codes geometrically[1,2]. The starting point is a code generating matrix. We are limited to the case of three-dimensional codes. The basic geometry is the design plane PG (2, q).

- Remember the basics:
  The points of PG (2, q) are called one-dimensional subspaces of F_q^3, two-dimensional subspaces are called lines. There are $q^2 + q + 1$points and as many as lines.
- Lines form the blocks of a model, a Steiner S system (2, q + 1, q2 + q + 1) (in particular each line has q + 1 point). The smallest projection plane is PG (2,2) (7 points, 7 lines, each line has 3 points, each point is on 3 lines, each pair of points is on exactly 1 line). This PG projection binary plane (2.2) is also known as the Fano plane.

Each nonzero vector (x, y, z) of PG (2, q) generates a one-dimensional subspace, i.e. a point. We can label the points with these triplets. The difference between triplets and points is that triplets, which are multiple scales of each other, define the same point.

The Fano Plane is described in Example1.1 [2]. As an example, consider the binary code with the generator matrix here is the relation to the geometry: we consider the G columns as points of S example, consider the binary code with the generating matrix, here is the relation to the geometry: we consider the G columns as points of PG(2,2).

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

In this case each point of the Fano plane occurs exactly once as a column. A geometer would identify this C code (or this generating matrix).

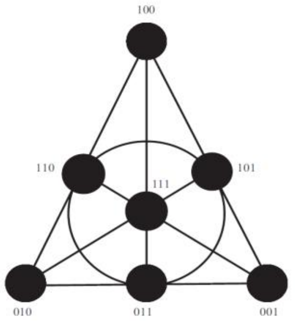

Fig 5. Fano plane

What is the minimum dimension d of this code [7,3, d]2 or more generally, what are the weights of the words [2,3,4]?

We denote the lines G by z_1, z_2, z_3 . Code words are linear combinations of $\lambda_1 z_1 + \lambda_2 z_2 + \lambda_3 z_3$. Fix a coordinate. The corresponding column of G is a point P of PG (2,2). The question arises when we will mark the code word with 0 in the column e G? Let P = (x, y, z). The notation 0 means $\lambda_1 x + \lambda_2 x + \lambda_3 x = 0or(\lambda_1, \lambda_2, \lambda_3) \cdot P = 0$.

Let us summarize: each coordinate is indexed by a point P of PG (2,2) (the corresponding column of the generating matrix) [2,3].

Each nonzero code word is given by a nonzero triple $(\lambda_1, \lambda_2, \lambda_3)$ (the coded word is $\lambda_1 z_1 + \lambda_2 z_2 + \lambda_3 z_3$). This code word is denoted by 0 in this coordinate if and only if the point product disappears:

$$(\lambda_1, \lambda_2, \lambda_3) \cdot P = 0.$$

The point product represents a non-trivial linear equation at P = (x, y, z). These points P are therefore exactly the points of a two-dimensional subspace, in other words, of a line. Add again: each nonzero code word defines a straight line l (scale multiples define the same line). Each coordinate is indexed by a point P. The corresponding notation of the code word disappears (= 0) if P ∈ l. The weight of the coded word is therefore the number of dots which are not in l. This description is true for any three-dimensional code. In our example, the 7 coordinates are described by the 7 points of the Fano plane. Since each line has 3 points, there are 4 points outside each line. We have seen that our code is a code [7,3,4]2, more precisely every nonzero word of our code has weight 4.

3. Conclusions

We have been able to introduce and discuss some of the many interesting structures in projective geometry. With this knowledge, we can continue to study in this area in the hope of finding new structures, larger k arches, or even more arches like the Glynn arc that is not a rational curve. The study of finite geometry is ever-changing, and with more advances, we see more connections with other areas of combinatorics. Whenever we learn more about geometry, we can learn more and advance further into the world of coding theory.

The above-described properties of labeled Fano planes as example of coordinated projective plane, clearly demonstrate that there is still much that this prominent object of discrete mathematics is likely to teach us.

References

[1]. Bierbrauer J. 2017. Introduction to coding theory second edition, Boca Raton: CRC Press / Taylor & Francis Group.

[2]. Lint J. V. 1998. Introduction to coding theory third edition. Eindhoven: *Springer*.

[3]. Ling S. and Xing C. 2004. Coding theory, A first course. New York: Cambridge University Press 2004.

[4]. Edgar T. and Betten A. 2004. Finite Projective Geometries and Linear Codes. *Fort Collins*, Colorado.

[5]. Mullen G.L., Stichtenoth H. and Recillas H.T. 2001. Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, *Oaxaca*, Mexico: *Springer*.

[6]. Klein A. and Storme L. 2011. Applications of finite geometry in coding. Ghent, Belgium.

[7]. Clark C. D. 2011. Applications of fifinite geometries to designs and codes. Michigan Technological University.

[8]. Longo G., Marchi M. and Sgarro A. 1990. Geometries, codes and cryptography. *Springer.*Wien-New York.

[9]. Garcia A. and Henning S. 2007. Topics in Geometry, Coding Theory and Cryptography. *Springer.* Dordolecht.