UDC: 514.16:519.854
Professional paper

SOME PROPERTIES OF PROJECTIVE GEOMETRY IN CODING THEORY

Flamure Sadiki[1], Alit Ibraimi[1], Agan Bislimi[2], Florinda Imeri[3]

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

Abstract

In this article we present the basic properties of projective geometry and coding theory and show how finite geometry can contribute to coding theory. Often good codes come from interesting structures in projective geometries. For example, MDS codes come from arcs (i.e. sets of points which are extremal in the sense that they admit no other than the obvious dependencies).We concentrate on introducing the basic concepts of these two research areas and give standard references for all these research areas. We also mention particular results involving ideas from finite geometry, and particular results in coding theory.

Keywords: Finite geometry, MDS codes, GDRS code, Hamming code, m arcs

Introduction

This dissertation will focus on the intersection of two areas of discrete mathematics: finite geometries, and coding theory. In each section, we will use finite geometry to construct and analyze new code objects, including new classes of designs and quantum codes. We will show how the structure of the finite geometries carries through to the new code objects and provides them with some of their best properties.
In this first section, we will give detailed definitions of the fundamental objects of our study, and examine the links between these objects.
A code is a mapping from a vector space of dimension m over a finite field K (denoted by $V,(K)$) into a vector space of higher dimension $n > m$ over the same field ($V(K)$).
A linear $[n,k]-$code of minimum distance d satisfies $d \leq n - k + 1-$the Singleton bound. A linear $[n,k]-$code meeting the Singleton bound is called a linear Maximum Distance Separable, or MDS code. Linear MDS codes are much studied in the mathematical and engineering sciences. In this short note we are concerned with the structure of an arbitrary MDS code
The study of $k-$arcs in $PG(n,q)$ is also interesting from a coding-theoretic point of view. The k-arcs of $PG(n,q)$ and the linear MDS codes (maximum distance separable codes) of dimension $H + 1$ and length k over $GF(q)$ are equivalent objects. Any result on k-arcs can be translated into an equivalent theorem on linear MDS codes. The k-arcs are subsets of a normal rational curve correspond to GRS (generalized Reed-Solomon) codes and GDRS (generalized doubly-extended Reed-Solomon) codes.

1. Introduction to projective geometry and coding theory

1.1. Introduction to projective geometry

The axioms of the projective plane are:

- (A1) Any two distinct points lie on a unique line.
- (A2) Any two distinct lines meet in a unique point.
- (A3) There exist at least four points of which no three are collinear.

In the following, all projective spaces will be of the form $PG(V)$ where V is a finite dimensional vector space over a finite field F_q of order q. Let $d + 1$ be the dimension of V, then we also write $PG(d, q)$ for $PG(V)$.

If V is a vector space over a finite field, then $PG(V)$ has a finite number of points and lines. *Theorem 1* counts them.

Theorem 1. ([10])
The projective space $PG(d, q)$ has

$$\frac{q^{d-1} - 1}{q - 1} = q^d + q^{d-1} + \cdots + q + 1 \text{ points}$$

$$\text{and } \frac{(q^d + q^{d-1} + \cdots + q + 1)(q^{d-1} + q^{d-1} + \cdots + q + 1)}{q + 1} \text{ lines.}$$

Each line of $PG(d, q)$ contains exactly $q + 1$ points.

1.2.Introduction to coding theory

Codes in general are often denoted by the letter C, and a code of length *n* and of rank *k* (i.e., having *k* code words in its basis and *k* rows in its generating matrix) is generally referred to as an (n, k) code.

A linear code of length *n* and rank *k* is a linear subspace C with dimension *k* of the vector space F_q^n where F_q is the finite field with q elements. Such a code is called a q −ary code.

The vectors in C are called codewords. The size of a code is the number of codewords and equals q^k. The weight of a codeword is the number of its elements that are nonzero and the distance between two codewords is the Hamming distance between them, that is, the number of elements in which they differ. The distance d of the linear code is the minimum weight of its nonzero codewords, or equivalently, the minimum distance between distinct codewords.

A linear code of length n, dimension k, and distance d is called an $[n, k, d]$ code. As a linear subspace of F_q^n the entire code C (which may be very large) may be represented as the span of a set of k codewords (known as a basis in linear algebra). These basis codewords are often collated in the rows of a matrix G known as a generating matrix for the code C. When G has the block

matrix form $G = [I_k \mid P]$, where I_k denotes the $k \times k$ identity matrix and P is some $k \times (n-k)$ matrix, then we say G is in standard form.

Definition 1.

The Hamming distance $d(x, y)$ of $x, y \in F_q^n$, with $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$, is

$$d(x, y) = |\{i \mid x_i \neq y_i\}|.$$

The Hamming distance of x to 0 is called the weight of x; $w(x) = d(x, 0)$.

A linear $[n, k]_q$ block code C is a k-dimensional subspace of F_q^n.

The minimum distance d of a linear $[n, k]_q$ block code C is defined as

$$d = \min_{x \neq y \in C} d(x, y) = \min_{0 \neq x \in C} w(x)$$

An $[n, k, d]_q$-code is an$[n, k]_q$-code with minimum distance d.

A main goal of coding theory is to determine for given n, k and q the largest d for which an $[n, k, d]_q$-code exists.

2. MDS and GDRS codes

We start with a very simple upper bound on the minimum distance of an $[n, k]_q$--code.

Consider the systematic generator matrix of an $[n, k]_q$-code:

$$G = \begin{pmatrix} 1 & & 0 & g_{1,k+1} & \cdots & g_{1,n} \\ & \ddots & & \vdots & & \vdots \\ 0 & & 1 & g_{k,k+1} & \cdots & g_{k,n} \end{pmatrix} = \left(I_k G_{k \times (n-k)}\right).$$

Each row of G has at most $n - k + 1$ nonzero entries and hence $n - k + 1 \geq d$.

Theorem 2. ([8])

An $[n, k, d]_q$ −code satisfies $n - k + 1 \geq d$.

A code C whose parameters satisfy $k + d = n + 1$ is called maximum distance separable or **MDS**. Such codes, when they exist, are in some sense best possible. Let C be an $[n, k, d]_q$ MDS code. Its parity check matrix H is an $(n-k) \times n$ matrix with the property that any $n - k$ columns of H are linearly independent.

Definition 2.

An r −arc of $PG(n, q)$ is a set of r points that span $PG(n, q)$ and such that any hyperplane contains at most n points of this r −arc.

The $(q + 1)$ −arc corresponding to a GDRS-code is called a *normal rational curve*.

Here, $\{(1, t, \dots, t^k - 1) \mid t \in F_q\} \cup \{(0, \dots, 0, 1)\}$ is the standard form for a normal rational curve in $PG(k-1, q)$.

Definition 3.

A linear $[n, k, n - k + 1]$ MDS code C over $GF(q)$ is called a GDRS (generalized doubly-extended Reed-Solomon) code if and only if C has a generator matrix, the columns of which constitute n points of the normal rational curve $\{(1, t, \dots, t^{k-1}) | \, t \in GF(q)^+\}$ in $PG(k - 1, q)$.

3. Some properties of projective geometry in codes

The study of linear MDS codes was performed mostly by geometrical methods. We mention a number of the most important results through lemmas, theorems and examples.

Definition 4.

Let C be a $(q + 2, 3)_q$-MDS code and define the incidence structure S by:

- Points of S: The words of C.
- Lines of S: All words in C with fixed entries in two fixed positions.
- Planes of S: All words in C with a fixed entry in a fixed position.

Lemma 1.

Given a point P and a line l in S, either P and l are coplanar (so P is joined to each point of l), or P is joined to exactly $\frac{q}{2}$ points of l.

Proof. Assume P and l are not coplanar. Let $P = (a_1, a_2, \dots, a_{q+2})$ and let l be the words in C of the form $(b_1, b_2, \dots)$ where $b_1 \neq a_1$ and $b_2 \neq a_2$ are fixed. For each i, $3 \leq i \leq q + 2$, there is a unique word of C with first entry b_1, second entry b_2 and $i'th$ entry a_i (Lemma 1.1). By Lemma 1.2 these words coincide in pairs, so exactly $\frac{q}{2}$ words of l are joined to P.[1]

Theorem 3. ([9])

For

- q an odd prime power,
- $2 \leq k < \sqrt{q}/4$,

every $[n = q + 1, k, d = q + 2 - k]$ −MDS code is a GDRS code.

This preceding result was obtained using methods from algebraic geometry and projection arguments.

The motivation for the next result is as follows.

The GDRS codes are MDS codes of length $q + 1$. Maybe they can be extended to MDS codes of length $q + 2$. The following result proves that this is practically never the case.

[1] For Lemma 1.1 and 1.2 see T.L. Alderson '' (6,3)-MDS codes over an alphabet of size 4'' page 2

Theorem 4. ([3])

Consider the $[q + 1, k, q - k + 2]_q$- GDRS code.

For q odd and $2 \leq k \leq q + 3 - 6\sqrt{q \cdot log\, q}$, and for q even and $4 \leq k \leq q + 3 - 6\sqrt{q \cdot log\, q}$, this $[q + 1, k, q + 2 - k]_q$ − GDRS code cannot be not extended to a $[q + 2, k, q + 3 - k]_q$ - MDS code.

Let K be a set of m points, $P_1, P_2, \ldots, P_m$ in $PG(n, q)$. Form the $(n + 1) \times m$ matrix G whose m columns are projective coordinates of each of the points. It then follows that:

Theorem 5.

K is an m −arc in $PG(n, q)$ if and only if G is the generator matrix of an $[m, n + 1]$ q −ary MDS code with minimum distance $m - n$.

We can use this theorem to provide examples of nontrivial MDS codes.

(Example) In $PG(2, q)$ the largest m-arcs have size $q + 1$ if q is odd and $q + 2$ if q is even. A $q + 1$ −arcin $PG(2, q)$ is called an *oval* and a $q + 2$ − arc is called a *hyperoval*. Hence, ovals give rise to $[q + 1,3]$ MDS codes and hyperovals give rise to $[q + 2, 3]$ MDS codes. For $q > 3$, these will be nontrivial MDS codes. For q odd, all ovals are of the same type, called a *conic*. For q even, there are several types of hyperovals, they have not yet been classified.

4. Conclusion

This article describing applications of finite geometry in coding theory, and also ideas from coding theory applied to projective geometry. For a collected work describing current research topics in finite geometry and their applications in coding theory, we refer to [1]. This paper collected work, can guide interested readers to research in finite geometry and its applications, enabling them to contribute to finite geometry and its applications. For all research areas, we have given standard references.

References

[1] L. Storme and J. De Baule, Current Research Topics in Galois Geometry, Ghent, Belgium: Nova Academic, 2011.

[2] J. Hirschfeld., Projective geometries over finite fields, Oxford Mathematical Monographs, 1998.

[3] L. Storme, "Completeness of normal rational curves," Boston, Kluwer Academic Publishers, 1992, p. 1:197–202.

[4] L. Storme and J. Thas, "Complete k-arcs in PG(n, q)," Gent, 1992, pp. 458-459.

[5] M. Blaum and R. Roth, "On Lowest Density MDS Code," IEEE, 1999.

[6] T. Alderson, "(6,3)-MDS codes over an alphabet of size 4.," 2006.

[7] V. Lint, Introduction to Coding Theory, Springer-Verlag, 1998.

[8] R. Singleton, "Maximum distance q-ary codes.," IEEE Transactions on Information Theory, 1964, p. 116–118.

[9] J. Thas, "Normal rational curves and k-arcs in Galois spaces," Gent, Rend. Mat, 1991, p. 331–334.

[10] L. Storme and A. Klein, "Applications of finite geometry in coding theory and cryptography," Ghent, 2011.