On Almost Maximum Distance Separable Codes

N.A.M. Al-seraji
Department of Mathematics, College of Science, Al-Mustansiriya University, Baghdad, Iraq

Abstract
The main goal of this paper is to make link between the subjects of projective geometry, vector space and linear codes. The properties of codes and some examples are shown. Furthermore, we will give some information about the geometrical structure of the arcs. All these arcs are give rise to an error-correcting code that corrects the maximum possible number of errors for its length.

Keywords: projective geometry, vector space, codes.

حول الشفرات المنفصلة ذات المسافات العظمى

نجم عبدالزهره مخرب السراجي
قسم الرياضيات، كلية العلوم، الجامعة المستنصرية، بغداد، العراق

الخلاصة
الهدف الرئيسي لهذا البحث هو عمل ربط بين مواضيع الهندسة الاسقاطية و فضاء المتجهات و الشفرة الخطية. خواص الشفرة مع بعض الأمثلة وضحت. كما إننا أعطينا بعض المعلومات حول التركيب الهندسي للأقواس. كل هذه الأقواس أعطت الارتفاع لتصحيح خطا الشفرة والقيام بتصحيح نهاية عظمى لعدد ممكن من ألأخطاء لأطوالها.

Introduction

The main goal of this work is to introduce theorems and some examples of Codes. The subject of the study depends on the subject of projective geometry over finite field, the vector space and linear codes see [1-5].

An $(n,M,d)_q$ code $\mathcal{C}$ is a set of M words, each with n symbols taken from an alphabet of size q, such that any two words differ in at least d places. A code $(n,M,d)_q$ has the following desirable properties:

- Small n: fast transmission;
- Large M: many messages;
- Large d: correct many errors.

If the code is linear, it can more easily be used for encoding and decoding; in this case, $M = q^k$ for some positive integer k, the dimension of the code is k, and $\mathcal{C}$ is called an $[n,k,d]_q$ code. The main Coding Theory problem is to find codes optimizing one parameter with the other two fixed. Mathematically, such a code can also be viewed as a set of n points in $PG(k-1,q)$ with at most $n-d$ points in a subspace of dimension $k-2$.

Previous Results

Definition (1)[5]: A $(k;3)$-arc in $PG(2,q)$ is a set of k points in which no four points but some three points are collinear.

Definition(2)[1]: An (n,M) code $\mathcal{C}$ over $\mathbb{F}_q$is a subset of $(\mathbb{F}_q)^n$ of size M. A linear $[n,k]_q$ code over Galois field $\mathbb{F}_q$ is a k-dimensional subspace

Email:najem_abdul@yahoo.com

of $(\mathbb{F}_q)^n$ and size $M = q^k$. The vectors in the linear code C are called codewords and we denote them by $x = x_1x_2 \dots x_n$, where $x_i \in \mathbb{F}_q$.

Definition (3)[1]: A generator matrix G for an $[n,k]_q$ code C is any $k \times n$ matrix G whose rows form a basis for C. For any set of k independent columns of a generator matrix G, the corresponding set of coordinates forms an information set for G. if the first k coordinates form an information set, the code has a unique generator matrix of the form $[I_k|A]$ where I_k is the $k \times k$ identity matrix; such a generator matrix is in standard form which means $[I_k|A]$.

Definition (4)[4]: The ordinary inner product of vectors $u = u_1u_2 \dots u_n, v = v_1v_2 \dots v_n$ in $(\mathbb{F}_q)^n$ is defined by

$$u.v = \sum_{i=1}^{n} u_i v_i.$$

Definition(5)[1]: The dual of the code C is the $[n, n-k]_q$ linear code $C^{\perp}$ defined as
$C^{\perp} = \{v \in (\mathbb{F}_q)^n | u.v = 0 \ \forall u \in C\}$.

Definition (6)[4]: A parity check matrix H of a linear $[n,k]_q$ code C is defined to be an $(n-k) \times n$ generator matrix of $C^{\perp}$.

Remark (7): From the previous definition, we deduce that
$C = \{x \in (\mathbb{F}_q)^n | Hx^T = 0\}$.

Theorem (8)[4]: If $G = [I_k|A]$ is a generator matrix for C in standard form, then $H = [-A^T|I_{n-k}]$ is a parity check matrix for $C^{\perp}$.

Definition (9)[1]: The (Hamming) distance $d(x,y)$ between two vectors x, y in $(\mathbb{F}_q)^n$ is defined to be the number of coordinate in which x and y differ. The distance d is a metric. The minimum distance d of a code C is the smallest distance between any pair of distinct codewords.

Definition (10)[1]: The (Hamming) weight $w(x)$ of a vector x in $(\mathbb{F}_q)^n$ is the number of its nonzero coordinates.

Definition (11)[1]: A code is almost maximum distance separable (AMDS) when
$d = n - k$.

Theorem (12)[4]: Let C be an $[n,k]$-code with parity-check matrix H. Then $d = \min d(x,y)$ if and only if some d columns of H are linearly dependent but every $d-1$ columns are linearly independent.

Example (13):
1. Ternary $[4,2]$-code with parity-check matrix
$H = \begin{bmatrix} 1 & 2 & 0 & 1 \\ 0 & 2 & 1 & 2 \end{bmatrix}$, $d = 3$.
2. Binary $[5,2]$-code with parity-check matrix
$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$, $d = 3$.
3. Binary $[8,4]$-code with parity-check matrix
$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$, $d = 4$.

Theorem (14)[4]:
Let $V(n,q)$ be an n-dimensional vector space over the field $\mathbb{F}_q$, a subset S of $V(n,q)$ is a subspace if

- $x + y \in S$ for all $x, y \in S$;
- $\lambda x \in S$ for all $x \in S, \lambda \in \mathbb{F}_q$.

Example (15): $\{(x_1,x_2,0) | x_i \in \mathbb{F}_q\}$ is a subspace of $V(3,q)$.

Example (16): The space $PG(r-1,q)$ contains $\frac{q^r-1}{q-1}$ points in projective space of order q.

$|V(2,5)| = 5^2$,
$|PV(2,5)| = \frac{5^2-1}{5-1} = 5 + 1 = 6$
$V(2,5) \setminus \{0\} =$
(1,0), (2,0), (3,0), (4,0)
(0,1), (0,2), (0,3), (0,4)
(1,1), (2,2), (3,3), (4,4)
(1,2), (2,4), (3,1), (4,3)
(1,3), (2,1), (3,4), (4,2)
(1,4), (2,3), (3,2), (4,1)
$PG(2,5)$ is the first column.

Definition(17)[3]: Given a homogenous polynomial F in three variables x_0, x_1, x_2 over $\mathbb{F}_q$, a curve $\mathcal{F}$ is the set
$\mathcal{F} = v(F) = \{P(X) : F(X) = 0\}$,
where $P(X)$ is the point of $PG(2,q)$ represented by $X = (x_0, x_1, x_2)$.
If F has degree three, that is,

$$F = \sum_{i,j,k=0,1,2} a_{ijk} x_i x_j x_k, i \le j \le k,$$

Then $\mathcal{F}$ is called a cubic. The multiplicity of P on $\mathcal{F}$, denoted $m_p(\mathcal{F})$, is the minimum of intersection multiplicities of the line ℓ and $\mathcal{F}$ at P, denoted $m_p(\ell,\mathcal{F})$, for all lines ℓ through P. Then P is a singular point of $\mathcal{F}$ if $m_p(\mathcal{F}) > 1$ and a non-singular point of $\mathcal{F}$ if $m_p(\mathcal{F}) = 1$. The cubic $\mathcal{F}$ is called singular or non-singular according to $\mathcal{F}$ does or does not have a singular point.

Results and Applications

Theorem (1): Let $r = n - k - 1$. An $(r+1) \times n$ matrix H is the parity-check matrix of a AMDS code if and only if, the n columns are vectors in $V(r,q)$ with every r linearly independent.

Proof: Theorem(12) says that an $[n,k]$ code is AMDS if an $(n-k) \times n$ parity-check matrix H has every $d-1 = n-k-1$ columns are linearly independent.

Put $[n,k,n-k] = [n,n-r-1,r+1]$. ■

Theorem (2): An $[n,k]$-code C has $d(C) = C$ if and only if, the n columns of a generator matrix G are vectors in $V(k,q)$ such that an prime, that is, a subspace of dimension $k-1$, contains at most $n-d$ of the n vectors.

Proof: Let

$$G = \begin{bmatrix} m_1 \\ \vdots \\ m_k \end{bmatrix};$$

So $x \in C$ if and only if, $x = \sum_1^k \lambda_i m_i$. Consider the j-th column:

$$\begin{bmatrix} y_1 \\ \vdots \\ y_k \end{bmatrix}$$

Then the j-th coordinate of x is zero when $\sum_1^k \lambda_i y_i = 0$. As x has at least d non-zero coordinates, it has at most $n-d$ zero coordinates; that is, of the n vectors in $V(k,q)$, an equation $\sum_1^k \lambda_i y_i = 0$ has at most $n-d$ solutions $(y_1, \dots, y_k)$. ■

Theorem (3): An $[n,k]$-code C is AMDS if the vectors in $V(k,q)$ given by the n columns of a generator matrix G have at most k in a prime; that is, every $k+1$ are linearly independent.

In theorem (2), put $d = n-k$; then $n-d = k$. ■

Remark: The dual code of an AMDS code need not to be AMDS as illustrated in the following example.

Example(4): Let C $[n,k,n-k+1]$-code be Maximum Distance Separable (MDS) code with parity check matrix

$$H = \begin{bmatrix} y_1 \\ \vdots \\ y_{n-k} \end{bmatrix}_{(n-k)\times n}$$

where y_i is the ith row of H. Choose $y \in V(n,q)$ which is not a linear combination of rows of H and which is of weight less than $k-1$. Consider

$$H_1 = \begin{bmatrix} y_1 \\ \vdots \\ y_{n-k} \\ y \end{bmatrix}_{(n-k+1)\times n}$$

As a parity check matrix of the $[n,k-1]$-code C_1. Then C_1 is an AMDS code but the dual is not.

Theorem (5): In an $[n,k]_q$ code C that is AMDS, the number of words of minimum weight $d = n-k$ is

$$(q-1)\binom{n}{n-k} = (q-1)\binom{n}{d}.$$

Proof: Let G be a generator matrix for the $[n,k]_q$ AMDS code C.

Since the first $k+1$ columns are linearly independent, row operations give the matrix G' in standard form

$G' = [I_k A]$,

Which is another generator matrix for C with $a_{i,j} \neq 0$ for all i, j.

Hence the number of words of C with 0 in the first k positions, and so weight $n-k$, is $q-1$; These words are just multiples of the last row of G'.

Hence the number of words of weight $n-k$ is

$$(q-1)\binom{n}{k} = (q-1)\frac{n!}{(n-k)!k!} =$$

$$(q-1)\binom{n}{n-k} = (q-1)\binom{n}{d}$$ ■

Example (6): Over Galois field of order four

$\mathbb{F}_4 = \{0,1,\omega,\omega^2 | 2 = \omega^2 + \omega + 1 = \omega^3 + 1 = 0\}$

The set of points in cubic curve

$F = X^3 + Y^3 + Z^3$

is given in the following table

$(0,1,1)$	$(1,0,1)$	$(1,1,0)$
$(0,1,\omega)$	$(1,0,\omega)$	$(1,\omega,0)$
$(0,1,\omega^2)$	$(1,0,\omega^2)$	$(1,\omega^2,0)$

To calculate the parameters of AMDS code $[n,k]_q$.

The generator matrix for the points in above table is,

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

As the last row of G reveals a word of weight 5, so $d = 5$.
Also $n = 8, \quad k = 3, \quad d = n - k = 8 - 3 = 5$.

Acknowledgment
I would like to thank my supervisor, Professor J.W.P. Hirschfeld for his suggestions which are helping me to complete this work.

References

1. Al-seraji N.A.M, **2010**, The Geometry of the Plane of Order Seventeen and Its Application to Error-Correcting Codes, Ph.D. Thesis, University of Sussex, UK.
2. Al-zangana E.B, **2011**, The Geometry Of The Plane Of Order Nineteen And Its Application to Error-Correcting Codes, Ph.D. Thesis, University of Sussex, UK.
3. Hirschfeld J.W.P, **1998**, Projective Geometries over Finite Fields, Second Edition, Oxford University Press, Oxford.
4. Hirschfeld J.W.P, **2008**, Lectures in Coding Theory, Sussex University, UK.
5. Hirschfeld J.W.P, Korchmáros G and Torres F, **2007**, Algebraic Curves over a Finite field, Oxford University Press, Oxford.