Linear Codes Arise From New Complete (n,r)-arcs in PG(2,29)

Shua'a M. Aziz
College of Computer Sciences and Mathematics
University of Mosul, Iraq

Received on: 16/07/2008 **Accepted on: 14/10/2008**

ABSTRACT

This paper presents the recently-discovered linear [n,3,d] codes over PG(2,29) that arises from a complete (n,r)-arcs which the paper[12] presented it for the first time. The aim of this paper is to formulate the recently discovered upper bounds and lower bound for (n,r)-arcs as bounds that will look familiar to coding theorists.New two lists in this paper appeared, the first list of 15 codes arranged from[164,3,156]-code up to [704,3,678]-code, the second list of 27 codes arranged from [28,3,25]-code up to [776,3,747]-code, they are appeared for the first time in this paper, all of these codes we can call them as complete codes as thier definition in this paper, they belong to the class of error-correcting codes (ECC). In this paper I made a computer programs to construct these new codes with Random Greedy Construction method (RGC) which is mentioned in [13].

Keywords: linear code, complete arc, finite field, Error-correcting codes,(n,r)-arcs .

الشفرات الخطية الناشئة من أقواس تامة جديدة من النمط-(n، r) في PG(2,29)

شعاع محمود عزيز
كلية علوم الحاسوب والرياضيات، جامعة الموصل

تاريخ الاستلام: 2008/07/16 **تاريخ القبول: 2008/10/14**

الملخص

يعرض هذا البحث أحدث الشفرات الخطية المكتشفة من النمط [n,3,d]-code المستنبطة من الاقواس التامة من النمط (n,r)-arcs والتي ذكرت في [12] لأول مرة. هدف هذا البحث هو صياغة القيود العليا والدنيا للاقواس التامة من النمط (n,r)-arcs لتكون قيوداً ملائمة للمتعاملين بالشفرات. تم في هذا البحث ذكر قائمتين من الشفرات الجديدة يتراوح مدى الاولى بين [164,3,156]-codeو[704,3,678]-code ، ويتراوح مدى القائمة الثانية بين [28,3,25]-code و[776,3,747]-code ،حيث تم ذكرها لأول مرة في هذا البحث، وأن كل هذه الشفرات تنتمي الى فئة شفرات تصحيح الاخطاء(ECC) وتم إعطاؤها تسمية الشفرات التامة حسب تعريفها في هذا البحث. كما تم استخدام برنامج حاسوبي لإيجاد هذه الشفرات مستخدماً الطريقة التوّاقة للبناء العشوائية(RGC) المذكورة في المصدر[13] .

الكلمات المفتاحية: شفرة خطية، قوس تام، حقل منتهي، شفرات تصحيح الأخطاء، اقواس-(n، r).

1. Introduction (Linear codes and Error-Correcting Codes)

Communicating information from one person to another is, of course, an activity that is as old as mankind. The (mathematical) theory of the underlying principles is not so old. It started in 1948, when C.E. Shannon gave a formal description of a communication system and, at the same time, also introduced a beautiful theory about the concept of information, including a good measure for the amount of information in a message.

The theory of error detecting and correcting codes (***ECC***) is that branch of engineering and mathematics which deals with the reliable transmission and storage of data. Information media are not 100% reliable in practice, in the sense that noise (any form of interference) frequently causes data to be distorted. To deal with this undesirable but inevitable situation, some form of redundancy is incorporated in the original data. With this redundancy, even if errors are introduced (up to some tolerance level), the original information can be recovered, or at least the presence of errors can be detected. We saw in class how adding to the original message the parity bit or the arithmetic sum allows the detection of a (certain type of) error. However, that kind of redundancy doesn't allow for the correction of the error. Error-correcting codes do exactly this: they add redundancy to the original message in such a way that it is possible for the receiver to detect the error and correct it, recovering the original message. This is crucial for certain applications where the re-sending of the message is not possible (for example, for interplanetary communications and storage of data). The crucial problem to be resolved then is how to add this redundancy in order to detect and correct as many errors as possible in the most efficient way. Error-correcting codes are particularly suited when the transmission channel is noisy. This is the case of wireless communication. Nowadays, all digital wireless communications use error-correcting codes.

This paper sets new codes that are not known until now, it's codes appeared from (n,r)-arcs in the finite projective plane PG(2,29), this information in this research finds new correcting codes that were not known before, so the benefit of this paper is to use it's codes in transmitting security information among large distance without using the normal used codes that may be exposed it's security .

2. Preliminary

At first I must give some definitions, a ***linear [n,k,d] code*** over finite field F_q is a k-dimensional subspace of the n-dimensional vector space V(n,q) over F_q such that d is the smallest number of positions in which two different elements of the code differ [6]. Let PG(2,q) be a ***finite projective***

plane Π of order q , where q= p^h , $h \geq 1$ this plane consists of q^2+q+1 lines and the same number of points , q+1 points on every line and q+1 lines passing through every point[8]. An ***(n,r)-arc*** is a set K of n points in PG(2,q) with at most r points on a line but there are no r+1 or more on any line[10], an (n,r)-arc is called ***complete***, if it is not contained in an (n+1,r)-arc [11]. A line L of the plane containing precisely i points of K, called an ***i-secant*** .Let T_i denote the total number of i-secants to K in PG(n,q). ***Hamming distance*** d on $F^n_q \times F^n_q$ is given by d(x;y) = #{i: $x_i \neq y_i$}, where x = $(x_1,\ldots, x_n)$ and y = $(y_1,\ldots y_n)$. The ***weight*** of x is defined by w(x) := d(x,o) ,where o := (0,…,0) [9]. The ***minimum distance*** of a code $C \subseteq F^n_q$ is given by d(C) := min{d(x,y) : x,y $\in$C, $x \neq y$}.For a linear code $C \subseteq F^n_q$ we have d(C) = min{w(x): $x \in C|\{0\}$}.Let $C \subseteq F^n_q$ be a linear code of dimension k,a ***generator matrix*** of C is a k × n matrix whose rows form an F_q-base of C. Let $C \subseteq F^n_q$ be a code, the ***dual code*** of C is the code $C^{\perp}$ defined by $C^{\perp}$:={$x \in F^n_q$: $\langle x, y\rangle$ =0, $\forall$ $y \in C$},where for

x = $(x_1,\ldots, x_n)$, y = $(y_1,\ldots,y_n)$, $\langle x, y\rangle := \sum_{i=1}^{n} x_i y_i$ is the usual bilinear form on $F^n_q \times F^n_q$.

Note that $C^{\perp}$ is indeed a linear code. For x $\in F^n_q$, let x^t denote its ***transpose***.

2.1 Lemma[3] Let $C \subseteq F^n_q$ a linear code of dimension k and M a generator matrix of C, Then

(1) $C^{\perp}$ = { x $\in F^n_q$: $Mx^t=0$};

(2) $C^{\perp}$ has dimension n-k.

2.2 Corollary[3]: Let C be a linear code and H a generator matrix of $C^{\perp}$. Then:

(1) C = $(C^{\perp})^{\perp}$;

(2) C={ x $\in F^n_q$:$Hx^t=0$}.

The ***redundancy*** of a k-dimensional linear code in F^n_q is n - k.

A ***parity check matrix*** of a linear code is any generator matrix of its dual.

2.3 Lemma[3]: Let C be a linear code and H a parity check matrix of C. Then:

(1) There exists x $\in$C of weight w if and only if there exist w columns of H which are F_q-linearly dependent.

(2) We have d(C) = min{$w \in Z^+$| $\exists$ w columns F_q-linearly dependent in H}.

2.4 Corollary[5] (***Singleton Bound***) For an F_q-linear code of length n, dimension k and minimum distance d, $d-1 \leq n-k$.

Definition[3] : An F_q-linear code of length n, dimension k and minimum distance d is called ***maximum distance separable (MDS)*** if d - 1 = n - k.
Definition[3] : The ***Singleton defect*** of an [n,k,d]-code C is $s(C)$ = n-k+1-d, So an MDS code is a code with Singleton defect equal to 0.

Definition[3] : Let C be an [n,k,d]-code, when the Singleton defect $s(C) = 1$, C is said to be an ***Almost MDS*** code (**AMDS** code for short).

2.5 Proposition[3]: The dual code of an MDS code is also MDS.

3. Points of Finite Projective Plane PG(2,29)

Let $f(x)=x^3-4x^2-x-1$ be an irreducible monic polynomial over GF(29) then companion matrix T of f(x)

$$T=\begin{bmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 1 & 4\end{bmatrix}$$

is cyclic projectivity on PG(2,29).
Let p_0 be the point $U_0=(1,0,0)$ then $p_i=p_0T^i$,i=0,…,870,are the 871 points of PG(2,29). (see Table(1.1))

Table(1.1) Points of PG(2,29)

i	P_i		
0	1	0	0
1	0	1	0
2	0	0	1
3	1	1	4
…		…	
869	1	8	10
870	1	4	28

4. Relation between linear codes and (n,r)-arcs

Write out the points of the (n,r)-arc K as columns of a matrix G, then form the code C as linear combinations of the rows of G. So, C is an [n,3,d]-code. What is d? Think of it in this way. The rows of G are as follows:

$r_1 = x_1\ \ x_2\ ...\ \ x_n$

$r_2 = y_1\ \ y_2\ ...\ \ y_n$

$r_3 = z_1\ \ z_2\ ...\ \ z_n$

If the line L with equation ax + by + cz =0 contains exactly s points of K, then the codeword

$ar_1 + br_2 + cr_3$ has weight n - s. This is because, if ax + by + cz is zero for the points $P_1,P_2,...,P_s$, it is not zero for the other n- s points of K.So, this

implies that, since any line contains at most r points, the weight of a codeword is at least n-r. Since some line contains exactly r points, so the minimum weight d = n-r.
Further, if you count the numbers T_i for K, where T_i is the number of lines meeting K in exactly i points, then the numbers $(q - 1)T_i$ give the ***weight distribution*** of the code.[4]

Definition: If the (n,r)-arc is complete then we call the corresponding code for it a ***complete code***.

Hence if one can get the matrix G so, he gets the code C (where G is it's generator matrix).For example if our arc contains from the following points {0,2,3,869,870} from the points of PG(2,29) so, the generator matrix G will be written as the coordinates of each point contains from the same arc {0 2 3 869 970} as written here

$$G=\begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 8 & 4 \\ 0 & 1 & 4 & 10 & 28 \end{bmatrix}$$ on the finite field F_{29} . For simplicity denote to the points by its order in the finite field without typing the coordinates for each one.

5. What is RGC-Method ?

When one wants to construct an object with certain structural constrains such as packings, covers, graphs without certain small subgraphs and arcs in a plane, random greedy construction is considered as a natural way to generate it : Randomly order all possible elements of the desired object and select each of them one by one in the order if and only if it together with already selected ones cause no conflict, i.e. no violation to the given constrains. Here we mean by "select" that we choose and permanently add it to the desired object being constructed. We may discard at each step all elements that cause any conflict with already selected ones and then randomly select a non-discarded one. This is an equivalent construction and will be called the Random Greedy Construction (RGC). For example, the RGC of a complete arc is the following. Initially, the arc being constructed is empty. At each step, discard all points contained in any secant of already selected points and select one non-discarded point uniformly at random. Then the set of all selected points is a complete arc. In many cases, it is believed that the RGC yields an almost optimal desired object.[13]

6.1 First List of ECC

It depends on the latest appeared maximum bounds for (n,r)-arcs which were not appeared even in [7] nor [2] but only (24,2)-arc appeared in [1]. So, I can set them as follows:
The following codes are now exist :

n	k	d	type
164	3	156	Complete code
191	3	182	Complete code
219	3	209	Complete code
247	3	236	Complete code
275	3	263	Complete code
303	3	290	Complete code
334	3	320	Complete code
421	3	404	Complete code
457	3	439	Complete code
489	3	470	Complete code
520	3	500	Complete code
570	3	548	Complete code
602	3	579	Complete code
631	3	607	Complete code
704	3	678	Complete code

6.2 Second List of ECC

It depends on the latest appeared minimum bounds for (n,r)-arcs which were not appeared even in [2].So, I can set them as follows:
The following codes are now exist :

n	k	d	type
28	3	25	Complete code
46	3	42	Complete code
62	3	57	Complete code
82	3	76	Complete code
100	3	93	Complete code
125	3	117	Complete code
152	3	143	Complete code
177	3	167	Complete code
203	3	192	Complete code
230	3	218	Complete code
254	3	241	Complete code

282	**3**	**268**	**Complete code**
310	**3**	**295**	**Complete code**
337	**3**	**321**	**Complete code**
363	**3**	**346**	**Complete code**
390	**3**	**372**	**Complete code**
422	**3**	**403**	**Complete code**
453	**3**	**433**	**Complete code**
484	**3**	**463**	**Complete code**
515	**3**	**493**	**Complete code**
548	**3**	**525**	**Complete code**
585	**3**	**561**	**Complete code**
616	**3**	**591**	**Complete code**
653	**3**	**627**	**Complete code**
691	**3**	**664**	**Complete code**
730	**3**	**702**	**Complete code**
776	**3**	**747**	**Complete code**

7. Two samples

For example the first two codes from the second list have the following generator matrices G_1 and G_2 respectively **:**

G_1 = [0 1 12 18 20 27 34 40 82 113 132 142 144 148 271 317 323 374 389 391 491 564 565 597 615 794 843 870].

G_2 = [0 1 4 5 37 47 67 86 93 116 129 161 165 196 212 218 226 233 249 258 264 278 299 341 374 384 386 391 394 400 439 443 459 529 587 588 602 611 654 669 699 705 745 786 807 829].

8. Conclusion :

This research finds new correcting codes that are not known before, so the benefit of this paper is to use it's codes in transmitting security informations among large distance without using the normal used codes that may be exposed it's security .

REFERENCES

[1] Chao,J. M. and Kaneta, H. (1996), *"A complete 24-arc in PG(2,29) with the automorphism group PSL(2,7)"*, Rendiconti di Matematica, Serie VII Volume 16 , Roma, 537-544

[2] Colbourn, Charles J. and Dinitz, Jeffrey H.(2007)"***The CRC Handbook of Combinatorial Designs***", Author Preparation Version 26 October 2007,a chapter done by Leo Storme (Active e-mail: ls@cage.ugent.be).

[3] Giulietti,M.(2004)," Notes on Algebraic-Geometric Codes",available at http://www.math.kth.se/math/forskningsrapporter/Giulietti.pdf

[4] Hirschfeld ,J.W.P(2001), *"Complete arcs"*, Discrete Math., North-Holland Mathematics Studies 123, North-Holland, Amsterdam, 243-250

[5] Hirschfeld, J.W.P, (1979),"***Projective Geometries over Finite Fields***", Oxford University Press, Oxford.

[6] Hirschfeld ,J.W.P. and Storme ,L. (2001), *" The packing problem in statistics, coding theory and finite projective spaces"*, update 2001, in: Finite Geometries, Developments in Mathematics 3, Kluwer , 201–246.

[7] Keri,G.,*"On the number of large complete arcs in PG(2,q), $23 \leq q \leq 32$"*, (Active e-mail: keri@sztaki.hu)

[8] Muhammad, H.H.(2006*),"The Maximum Size of (n,r)-arcs in the Projective Plane PG(2,q) "* M.Sc. Thesis, University of Mosul-Iraq.

[9] S.Ball and J.W.P.Hirschfeld (2005),*"Bounds on (n,r)-arcs and their application to linear codes"*, Finite Fields Appl. 11(2005), pp.326-336.

[10] Thas,J.A.(1987),"Complete arcs and algebraic curves in PG(2,q)", J.Algebra 106,451-464.

[11] Voloch,J.F.(1991)"Complete arcs in Galois planes of non-square order", Advances in Finite Geometries and Designs, Oxford University Press, Oxford, 401-406.

[12] Yahya, N.Y.K. and Aziz, S.M.(2008)" New values for $m_r(2,29)$ and $t_r(2,29)$ in PG(2,29)", to appear in Education and Science J, University of Mosul, Iraq .

[13] Vu,V.H and Kim J. H.(2003)"Small complete arcs in projective planes", Combinatorica archive Volume 23 , Issue 2, Pages:311-36**.**