Codes from cubic curves and their extensions

T. L. Alderson [*]
Mathematical Sciences
University of New Brunswick
Saint John, NB
E2L 4L5
Canada
tim@unbsj.ca

A. A. Bruen[†]
Electrical and Computer Engineering
University of Calgary
Calgary, AB
T2N 1N4
Canada
bruen@ucalgary.ca

Submitted: Aug 13, 2007; Accepted: Mar 4, 2008; Published: Mar 12, 2008
Mathematics Subject Classification: 94B27

Abstract

We study the linear codes and their extensions associated with sets of points in the plane corresponding to cubic curves. Instead of merely studying linear extensions, all possible extensions of the code are studied. In this way several new results are obtained and some existing results are strengthened. This type of analysis was carried out by Alderson, Bruen, and Silverman [*J. Combin. Theory Ser. A*, 114(6), 2007] for the case of MDS codes and by the present authors [*Des. Codes Cryptogr.*, 47(1-3), 2008] for a broader range of codes. The methods cast some light on the question as to when a linear code can be extended to a nonlinear code. For example, for p prime, it is shown that a linear $[n, 3, n-3]_p$ code corresponding to a non-singular cubic curve comprising $n > p + 4$ points admits only extensions that are equivalent to linear codes. The methods involve the theory of Rédei blocking sets and the use of the Bruen-Silverman model of linear codes.

1 Introduction

Much of the theory of linear codes is concerned with obtaining bounds on the length of such codes subject to certain constraints involving various parameters such as the minimum distance and with characterization of optimal cases. Similar remarks apply to finite geometries. There one wants to find bounds, for example, on the maximum or minimum number of points obeying certain combinatorial conditions and the structure in the optimal case. One thinks for example of the famous characterization of conics due

[*]The author acknowledges support from the N.S.E.R.C. of Canada
[†]The author acknowledges support from the N.S.E.R.C. of Canada

to B. Segre. Such problems have been well-studied and many interesting open problems remain open.

Here, a more general point of view is taken by studying the linear code associated with sets of points in the plane and their extensions. Our point of departure is that, instead of merely studying linear extensions, all possible extensions of the code are studied. In this way one can obtain several new results as well as a strengthening of existing results. This was carried out in [3] for the case of MDS codes. Moreover, the methods cast some light on the question as to when a linear code can be extended but not by a linear code. Here the focus is on the codes associated with cubic curves and results analogous to those in [3] are obtained. Our methods involve the theory of Rédei blocking sets and the use of the Bruen-Silverman model of linear codes.

Recall that a q-ary code of length n is a collection of n-tuples (codewords) over an alphabet $\mathcal{A}$ of size q. An $[n,k,d]_q$-code is a q-ary code consisting of q^k codewords of length n and minimum (hamming) distance d. In an $[n,k,d]_q$-code C there exist two codewords agreeing in $n-d$ coordinates and no two codewords agree in as many as $n-d+1$ (in particular, any $n-d+1$ coordinates form an information set). In the special case that $\mathcal{A} = GF(q)$ and C is a vector space of dimension k, C is a *linear* $[n,k,d]_q$-code.

Definition 1.1. The code C_1 of length $n_1 > n$ is said to be an *extension* of C if

1. the code C is obtained from C_1 upon deleting the entries in some fixed set of $n_1 - n$ positions of C_1 , and
2. the minimum distance of C_1 is $d + n_1 - n$,where d is the minimum distance of C.

The code C is said to be *maximal* if C admits no extensions.

Next, suppose that $n_1 = n+1$ where C is a linear $[n,k,d]$ code. Let X denote the set of all codewords in C_1 having a given symbol in a given position, say position j. Then, by deleting the jth coordinate position from X a code of length n os obtained, with minimum distance d and having q^{k-1} codewords.

This then gives rise to the following result.

Theorem 1.2. *An $[n,k,d]_q$ code C is extendable to a code C_1 of length $n+1$ if and only if there exists a partition $P = X_1, X_2, \ldots, X_q$ of C such that each X_i is a code of length n and minimum distance $d+1$.*

Consider a linear $[n,k,d]_q$-code C over $\mathcal{F} = GF(q)$ with generator matrix G. A linear extension of C arises by appending an appropriate column vector to G. There are in total q^k possible column vectors to check using an exhaustive search. Consider the $q^k \times n$ array M whose rows are the codewords of C. A general (*i.e.* not necessarily linear) extension arises by augmenting M with an appropriate column vector. Over $\mathcal{F}$ there are a total of q^{q^k} possible column vectors. The search for for an arbitrary extension of C therefore grows exponentially when one considers general, and not just linear, extensions. In investigating the maximality of a given linear code it may therefore be quite useful to know when nonlinear extensions can be ruled out.

2 A construction of codes from curves

Let Γ be a non-singular curve over a finite field $F = GF(q)$ of order q in the projective plane $\pi = PG(2, q)$. A well-known construction of codes using Γ is the family of so-called Goppa codes which generalize Reed-Solomon codes. Their construction uses linear systems of divisors on Γ and the machinery of algebraic geometry. These codes have been shown to be very useful in that, in certain cases, they improve on the Gilbert-Varshamov bound for the existence of linear codes: see [9] for further details.
Here a much more elementary construction for a code associated with Γ is used. This construction is described as follows. Suppose that Γ has degree t and that S is a subset of the points of Γ with $|S| = n$ say. Then S gives rise to a linear code C with generator matrix G of size $3 \times n$ where the columns of G correspond to the coordinates of the points in S. Assuming that the chosen points do not all lie on a line then G has rank 3.

Theorem 2.1. *If some line of π contains t points of S and not all points of S lie on a line then the code C is a linear $[n, 3, n-t]_q$-code.*

Proof. Suppose that some non-trivial linear combination of the rows of G has m zeros in it. Then the columns of G corresponding to these m column positions are linearly dependent. Thus, the columns correspond to a set of m points lying on a line. Since C is non-singular, and therefore irreducible, by the theorem of Bézout it follows that $m \le t$. Thus the minimum weight of the linear code C is at least $n - t$. Therefore the minimum distance of C is at least $n - t$. It follows that the code C is a linear $[n, 3, n-t]_q$-code. $\square$

3 Code extensions, the Bruen-Silverman model

One of our main new tools is the family of Bruen-Silverman codes [BRS codes] associated with a given linear code. Some pertinent details on this and related questions of code extensions are provided in what follows.
First we discuss equivalence of codes. Let C_1 and C_2 be codes of length n over an alphabet $\mathcal{A}$. Identify each code with a matrix, the rows of each matrix being the code words. The code C_2 is said to be *equivalent* to C_1 if C_2 can be obtained from C_1 by a sequence of operations of the following three types:

1. A permutation of the rows of C_1;
2. A permutation of the columns of C_1;
3. A permutation of the alphabet $\mathcal{A}$ is applied (entry-wise) to a column of C.

If two codes are equivalent then the codes are essentially identical. A code that is equivalent to a linear code is said to be *equivalent to linear*. Such a code need not be linear. For example, suitably permuting the symbols in a given column of a linear code removes the zero vector.

Let C be a linear $[n,3,d]_q$-code and take any $3\times n$ generator matrix G associated with C. Each codeword of C is a linear combination of the rows of G. Denote the entries of G as follows:

$$G=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ a_{31} & a_{32} & \cdots & a_{3n} \end{bmatrix}.$$

Then a code word w of C can be written as

$$w=\sum_{i=1}^{3}\alpha_i R_i \tag{3.1}$$

where R_i denotes the i^{th} row of G.
A better geometrical picture of C is desired. This may be obtained as follows.

Associate with C the projective space $\Sigma = PG(3,q)$ of dimension 3, having homogeneous coordinates (x_1,x_2,x_3,x_4). Assume the plane at infinity Π_∞ has equation $x_4=0$. Each column in G, say the i^{th} column, gives rise to a line ℓ_i in Π_∞ where ℓ_i is defined to be the solution set of the following system of equations:

$$\begin{cases} x_4=0, \\ a_{1i}x_1+a_{2i}x_2+a_{3i}x_3=0. \end{cases}$$

Let $E=\Sigma\setminus\Pi_\infty$ denote the associated 3-dimensional affine space. Thus E has q^3 points or vectors. Each point P in E has homogeneous coordinates $(\alpha_1,\alpha_2,\alpha_3,1)$. We wish to associate with P a code word $(\lambda_1,\lambda_2,\ldots,\lambda_n)$. The point P lies on a certain plane labeled $H_i(P)$ containing the line ℓ_i for each i, $1\le i\le n$. If the q planes of Σ other than Π_∞ containing ℓ_i are labeled, then P will lie on say the plane labeled $\lambda_i\in\mathcal{F}$. In this way the resulting code C_1 consists of q^3 code words $(\lambda_1,\lambda_2,\ldots,\lambda_n)$ of length n over $\mathcal{F}$.

The code C_1 will of course depend on the labeling of $H_i(P)$. Different labelings equate to symbol permutations of the code C_1. In [3] the following is shown.

Theorem 3.1. *The code C_1 is equivalent to the original code C. In particular C_1 is equivalent to linear.*

The code C_1 will be a *Bruen-Silverman (BRS) code* associated with C (or a *BRS model* of C). The BRS model was first introduced in [1].

To summarize, a code word w in C is identified with the set of coefficients $\alpha_1,\alpha_2,\alpha_3$ as in formula 3.1. Alternatively, the code word can be thought of as a point $P=(\alpha_1,\alpha_2,\alpha_3,1)$ in 3-dimensional affine space. To find the i^{th} coordinate of w, given P, the label of the unique plane containing ℓ_i and P is calculated. Here ℓ_i is a line of Π_∞ corresponding to the i^{th} column of G, the generator matrix of C.
From this picture it is clear that the set of code words with a given symbol in the i^{th} coordinate position corresponds to the points of $E=AG(3,q)$ contained in a certain

plane. The code words with given symbols in two fixed positions i and j correspond to the intersection of two planes, and so on. Hence, two code words w_1 and w_2 corresponding to the affine points P and Q will have t common entries if and only if the line PQ intersects Π_∞ in a point belonging to t of the ℓ_i's.
Next, let S be the set of n points in $\pi = PG(2,q)$ lying on a non-singular cubic curve Γ. As in Theorem 2.1, some line is incident with 3 points of S and no line is incident with as many as 4 points of S. Any such set in the plane is called a *cubic arc*. A cubic arc of size n is *complete* if it is not contained in a cubic arc of size $n+1$. A complete cubic arc in π therefore corresponds to a linear $[n,3,n-3]_q$ code admitting no linear extensions.
Dualizing, S may also be thought of as a *dual cubic arc (of lines)* T in π. Just as no four points of S lie on a line so also, no four lines of T pass through a point of π. A point of π lying on i lines of T is called an i-point of T for $i = 1,2,3$.

We will need the following definition.

Definition 3.2. Let T be a dual cubic arc in $\Pi = PG(2,q)$ and let $\Sigma = PG(3,q)$. Then, a point set W of size q^2 in $\Sigma \setminus \Pi$ is called a *transversal set* of T if no two points of W are collinear with a 3-point of T.

Considering Theorem 1.2 and the BRS model as above we have the following.

Theorem 3.3. *Let C be a linear $[n,3,n-3]_q$-code corresponding to the dual cubic arc T in $\Pi = PG(2,q)$. Consider Π as embedded in $\Sigma = PG(3,q)$ and let $E = \Sigma \setminus \Pi$. The code C can be extended if and only if there exists a partition $\{X_1, X_2, \ldots, X_q\}$ of E where each X_i is a transversal set of T.*

4 Geometry and Combinatorics of Cubic Curves

Part 1 of the following result uses an adaptation of a classical result (see *e.g.* [7]).

Theorem 4.1. *Let Γ be a non-singular cubic curve in $\pi = PG(2,q)$ with $|\Gamma| = n$. Let P be a point of Γ. Then*

1. *there are at most 4 lines on P that contain exactly 2 points of S;*
2. *there are at least $\frac{1}{2}(n-5)$ lines of π on P, each containing 3 points of Γ.*

Proof. A classical result implies that there are at most 4 points X unequal to P such that PX is a tangent to the curve Γ at X. Now if Z is any point on Γ such that the line PZ is a bi-secant to Γ it follows, since Γ is a cubic, that the line PZ is a tangent to Γ at Z. This proves part 1.
Let us denote by x, y and z the number of uni-secants, bi-secants and tri-secants of S on P. Counting the number of points of S yields $y + 2z = n - 1$. Since $y \leq 4$ it follows that $z \geq \frac{1}{2}(n-5)$. $\square$

Corollary 4.2. *Let Γ be a non-singular cubic curve in $\pi = PG(2,q)$ with $|\Gamma| = N$, and let S be any subset of the points of Γ with $|S| = n$. Let $\delta = N - n$ and let P be a point of S. Then there are at least $\frac{1}{2}(n-5-\delta)$ lines of π on P intersecting S in exactly 3 points.*

Proof. As in the previous theorem P is incident with at least $\frac{1}{2}(N-5)$ lines, each containing 3 points of Γ. It follows that P is incident with at least $\frac{1}{2}(N-5) - \delta = \frac{1}{2}(n-5-\delta)$ lines intersecting S in exactly 3 points. □

Theorem 4.3. *Let Γ be a non-singular cubic curve in $\pi = PG(2,q)$, $|\Gamma| = n$. Assume that $n > q+7$. Then each point P of π with P not on Γ lies on at least one tri-secant of Γ. In particular, Γ is a complete cubic arc.*

Proof. It is classical that P lies on at most 6 lines PX, $X \neq P$ such that PX is a tangent to Γ at X. Therefore, P lies on at most 6 bisecants to Γ since Γ is a cubic curve.
Let u, v, w denote the number of unisecants, bisecants and trisecants of Γ on P. Certainly $u + v + w \leq q + 1$. Counting the points of S gives

$$u + 2v + 3w = n.$$

This gives

$$n \leq q + 1 + v - 2w.$$

Since $v \leq 6$ the assumption $w = 0$ gives the result. □

Corollary 4.4. *Let C be a linear $[n,3,n-3]_q$-code corresponding to non-singular cubic curve. If $n > q+7$ then C admits no linear extensions.*

Let $\mathcal{N}_q(1)$ denote the maximum number of rational points on an elliptic curve over $GF(q)$. If $q = p^h$ then from the work of Waterhouse ([10]) it follows that

$$\mathcal{N}_q(1) = \begin{cases} q + \lfloor 2\sqrt{q} \rfloor & \text{if } p \mid \lfloor 2\sqrt{q} \rfloor \text{ and } h \geq 3 \text{ is odd,} \\ q + \lfloor 2\sqrt{q} \rfloor + 1 & \text{otherwise.} \end{cases} \tag{4.1}$$

Regarding the completeness of the cubic arcs arising from nonsingular cubic curves, Hirschfeld and Voloch [6] show the following.

Theorem 4.5. *If $q \geq 79$ is not a power of 2 or 3, then an elliptic curve Γ with n rational points is a complete cubic arc unless the j-invariant $j(\Gamma) = 0$, in which case the completion of Γ has at most $n+3$ points.*

Corollary 4.6. *Let Γ be an elliptic curve in $\pi = PG(2,q)$, $q \geq 79$ not a power of 2 or 3, having n rational points. If $j(\Gamma) \neq 0$ then the linear $[n,3,n-3]_q$-code corresponding to Γ admits no linear extensions.*

In the next section the maximality of codes corresponding to cubic curves is discussed.

5 The Main Results

The following theorem was shown in [2].

Theorem 5.1. *Let $\mathcal{K}$ be a cubic arc of size n in $PG(2,p)$, p a prime. Let C be the linear $[n,3,n-3]_p$-code corresponding to $\mathcal{K}$. If $n > \frac{3}{2}(p+5)$ then any extension of C is equivalent to a linear code.*

For codes corresponding to cubic curves a significant improvement to the bound in the previous theorem is obtained.

Theorem 5.2. *Let p be prime. Let C be a linear $[n,3,n-3]_p$ code corresponding to the non-singular cubic curve Γ in $\Pi = PG(2,p)$. If $n > p+4$ then every extension of C is equivalent to a linear code.*

Proof. It will be convenient to dualize Γ so that Γ may be thought of as a cubical set of n lines T in Π. The proof is more or less identical to that in [3]. However, let us give a sketch here. Let l be a line of T. Then, by 4.1 part 2 there are at least $\frac{1}{2}(n-5)$ 3-points of T on l. By our assumption on n this implies that the set Z of points on l which are not 3-points of T is less than $\frac{1}{2}(p+3)$. Let C_1 be an extension of C. As in 2.3 C_1 gives rise to a partition $\{X_1, X_2, \ldots, X_p\}$. Each X_i gives rise to a transversal set of T as in 3.2. Let X_1 correspond to the transversal set W in $\Sigma = PG(3,p)$. Each plane of $PG(3,p)$ on l intersects W in a set H of p points. Moreover, no two points of H are collinear with a 3-point of T. Thus, by a celebrated result on blocking sets due to Lovász and Schrijver [8] it follows that the set of points on H lie on a line in the plane.
This process may be repeated with another line l_1 of T. Then, exactly as in [3], it transpires that W is an affine plane. Consequently, the collection $X_1, X_2, \ldots X_p$ gives rise to a family of parallel planes. This family intersects the base plane Π in a line x which extends T (as a dual cubic arc). In other words, the set $Y = T \cup \{x\}$ gives a set of $n+1$ lines with no point of π lying on more than 3 points of Y. Moreover, the line x provides the linear extension of the code C. $\square$

Remark 5.3. Theorem 5.2 is notably restricted to the prime case. The reason for this is that in order to apply the result of Lovász and Schrijver (or related results such as those in [4, 5]) for q non-prime, Γ is required to hold a number of points exceeding the bounds (4.1).

Remark 5.4. In [2, 3] various classes of linear codes are shown to admit only linear extensions. It transpires that all codes for which these previous results apply necessarily meet the *Griesmer bound*:

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil .$$

Such codes are known as Griesmer codes. Theorem 5.2 offers an improvement on the previous bounds, however the codes meeting the conditions of Theorem 5.2 are also Griesmer codes. This gives rise to the following question:

Are there classes of linear codes that are not Griesmer codes yet admit only linear extensions?

More generally, given a set of n points S lying on a non-singular cubic curve Γ in $\Pi = PG(2,p)$ where p is a prime, consider the corresponding linear code C.

Theorem 5.5. *Let Γ be a nonsingular cubic arc in $\Pi = PG(2,p)$, p a prime, $|\Gamma| = N$. Let S be a subset of Γ with $|S| = n$ and let $\delta = N - n$. If $n - \delta > p + 4$ then the linear code C corresponding to S is a $[n,3,n-3]_p$-code and admits only linear extensions.*

Proof. Assume $n-\delta > p+4$. First note that as $|S| > p+4$, not all points of S are on a line and some line contains at least 3 points of S. So C is indeed a $[n,3,n-3]_p$ code. Next, observe that from the Corollary 4.2, each point of S is incident with at least $\frac{1}{2}(n-\delta-5)$ 3-lines of S. Dualizing as in Theorem 5.2 consider the dual cubic arc T corresponding to S. By assumption $n - \delta > p + 4$ whence each line of T is incident with at least $\frac{1}{2}(p-1)$ 3-points of T. The remainder of the proof follows as in the proof of Theorem 5.2. $\square$

From Theorem 5.2 and Corollary 4.4 the following is obtained.

Corollary 5.6. *Let C be a non-singular cubic in $\pi = PG(2,p)$ having at least $p+8$ points. Then the linear $[n,3,n-3]_p$-code corresponding to C is a maximal code.*

From Theorems 5.2 and 4.5 the following is obtained.

Corollary 5.7. *Let Γ be an elliptic curve in $\pi = PG(2,p)$, $p \geq 79$ a prime, having $n > p + 4$ points. Then the linear $[n,3,n-3]$-code C corresponding to Γ is a maximal code unless the j-invariant $j(\Gamma) = 0$, in which case C can be extended at most to a code of length $n + 3$ and any such extension is necessarily linear.*

References

[1] T. L. Alderson. On MDS codes and Bruen-Silverman codes. *PhD. Thesis, University of Western Ontario*, 2002.

[2] T. L. Alderson and A. A. Bruen. Coprimitive sets and inextendable codes. *Des. Codes Cryptogr.*, 47(1-3):113–124, 2008.

[3] T.L. Alderson, A. A. Bruen, and R. Silverman. Maximum distance separable codes and arcs in projective spaces. *J. Combin. Theory Ser. A*, 114(6):1101–1117, 2007.

[4] S. Ball. The number of directions determined by a function over a finite field. *J. Combin. Theory Ser. A*, 104(2):341–350, 2003.

[5] A. Blokhuis, S. Ball, A. E. Brouwer, L. Storme, and T. Szőnyi. On the number of slopes of the graph of a function defined on a finite field. *J. Combin. Theory Ser. A*, 86(1):187–196, 1999.

[6] J. W. P. Hirschfeld and J. F. Voloch. The characterization of elliptic curves over finite fields. *J. Austral. Math. Soc. Ser. A*, 45(2):275–286, 1988.

[7] Fred Lang. Geometry and group structures of some cubics. *Forum Geom.*, 2:135–146 (electronic), 2002.

[8] L. Lovász and A. Schrijver. Remarks on a theorem of Rédei. *Studia Sci. Math. Hungar.*, 16(3-4):449–454, 1983.

[9] Jacobus H. van Lint and Gerard van der Geer. *Introduction to coding theory and algebraic geometry*, volume 12 of *DMV Seminar*. Birkhäuser Verlag, Basel, 1988.

[10] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.