Skew Arcs and Wagner's $[23, 14, 5]$ code

Michelle Davidson
Department of Mathematics
University of Manitoba
Winnipeg, Manitoba
CANADA R3T 2N2

Lynn Batten
School of Information Technology
Deakin University
221 Burwood Highway
Burwood 3125
AUSTRALIA

Abstract

In 1966, Wagner used computational search methods to construct a [23,14,5] code. This code has been examined with much interest since that time, in hopes of finding a geometric construction and possible code extensions. In this article, we give a simple geometric construction for Wagner's code and consider extensions of this construction.

1 Introduction

In the early 1960's, T.J. Wagner [14] developed a search mechanism which produced several new, sporadic codes. One of these codes had parameters [23, 14, 5], and it is the subject of the current paper. Since Wagner's work appeared, a number of questions have been raised about this particular code: can a simple construction be given?; is it unique?; does it belong to a family of codes?

MacWilliams and Sloane first [12] formally studied the [23, 14, 5] code and in their Research Problem 18.3 asked for a simple construction. As far as we know, this problem has been open until the present article. In [3], Brouwer et al. give the weight distribution of certain cosets of the code. Simonis, in 2000 [13] proved that the code is unique as a consequence of his proof that the [24, 14, 6] code is unique.

In section 2 of this paper, we introduce the concept of a *skew arc* and give some examples. In section 3, we describe the relationships between skew arcs in $PG(m, 2)$ and binary linear codes. In section 4, we present several recursive constructions for skew arcs. Two of these constructions

JCMCC **56** (2006), pp. 191-201

(Theorem 3 and Corollary 4) are similar to those given by Chen in [8]; Chen's construction was analyzed in [1]. Finally, in section 5, we use the constructions from section 4 along with information concerning BCH codes [12] to construct Wagner's [23, 14, 5] code.

2 Skew arcs

Let $PG(m, 2)$ denote the projective geometry of dimension m over a finite field with 2 elements [11]. An *arc* in $PG(m, 2)$ is a set of points which contains no line. The connection between arcs and binary linear codes of minimum distance 4 has been studied by several authors [10] [4] etc. Our approach to the problem of codes with minimum distance 5 is similar.

Definition 1 We define a *skew arc* S to be a set of points in $PG(m, 2)$ such that:

1. S contains no lines.

2. Given any four distinct points of S, say s_1, s_2, s_3 and s_4, the third point on the line containing s_1 and s_2 is not on the line containing s_3 and s_4.

These two conditions also ensure that there are no more than 3 points of a skew arc on any plane. All lines in $PG(m, 2)$ have 3 points and all subspaces of dimension two are Fano planes. In the Fano plane, the maximum number of points that can satisfy the conditions of a skew arc is 3. We call 4 points that satisfy condition 1 but not condition 2 of the above definition a *planar quadrangle.*

Definition 2 Given a skew arc S, we define the set $\tilde{S} = \{s | \exists\, s_1,\, s_2 \in S,$ $\{s, s_1, s_2\}$ is a line $\}$.

We note that by the definition of a skew arc there must be a unique point in $\tilde{S}$ for each pair of distinct points in S. So if S is a skew arc with k points, then the size of $\tilde{S}$ will be $\frac{k(k-1)}{2}$ and $S \cup \tilde{S}$ will have $\frac{k(k+1)}{2}$ elements. This last is a necessary and sufficient condition for S to be a skew arc.

We can coordinatize the points of $PG(m, 2)$ with the nonzero $(m+1)$-*tuples* of zeros and ones using the induced vector space structure. Using these coordinates, the third point on a line containing points a_1 and a_2 is $a_1 + a_2$.

We can then rewrite the definition of $\tilde{S}$ as $\{s_1 + s_2 | s_1, s_2 \in S, s_1 \neq s_2\}$. We use this coordinatization to draw the correspondence between skew arcs and codes of minimum distance 5.

For an example, we can look at the following 8 points in $PG(5,2)$ which form a skew arc: $(1,0,0,0,0,0)$, $(0,1,0,0,0,0)$, $(0,0,1,0,0,0)$, $(0,0,0,1,0,0)$, $(0,0,0,0,1,0)$, $(0,0,0,0,0,1)$, $(1,1,1,1,0,0)$, $(0,0,1,1,1,1)$.

If S is the skew arc given above then $\tilde{S}$ will be: $(1,1,0,0,0,0)$, $(1,0,1,0,0,0)$, $(1,0,0,1,0,0)$, $(1,0,0,0,1,0)$, $(1,0,0,0,0,1)$, $(0,1,1,0,0,0)$, $(0,1,0,1,0,0)$, $(0,1,0,0,1,0)$, $(0,1,0,0,0,1)$, $(0,0,1,1,0,0)$, $(0,0,1,0,1,0)$, $(0,0,1,0,0,1)$, $(0,0,0,1,1,0)$, $(0,0,0,1,0,1)$, $(0,0,0,0,1,1)$, $(0,1,1,1,0,0)$, $(1,0,1,1,0,0)$, $(1,1,0,1,0,0)$, $(1,1,1,0,0,0)$, $(1,1,1,1,1,0)$, $(1,1,1,1,0,1)$, $(1,0,1,1,1,1)$, $(0,1,1,1,1,1)$, $(0,0,0,1,1,1)$, $(0,0,1,0,1,1)$, $(0,0,1,1,0,1)$, $(0,0,1,1,1,0)$, $(1,1,0,0,1,1)$.

We see that $\tilde{S}$ has 28 points, all of which are distinct from the 8 points of S. So $S \cup \tilde{S}$ has 36 points, as expected.

3 Codes

We now show the relation between skew arcs and binary linear codes.

Definition 3 A *codeword* is a tuple (in this case binary) of some fixed length, say n. We say the *distance* between two codewords (of the same length) is the number of positions in which the two words differ. A *code* is a collection of codewords and the *distance of a code* is the minimum of the distances taken over all pairs of codewords.

A $[n,k,d]$ *binary linear code* is a code having distance d with 2^k codewords, which are binary *n-tuples*, such that the sum of any two codewords is also a codeword. This means the code is a subspace of dimension k of the n dimensional vector space over $GF(2)$.

We can associate with a linear code a *parity check matrix* H of size $(n-k) \times n$. This matrix will have rows that are a basis of the dual space of the code. If H is the parity check matrix of the code C then $C = \{x | Hx^t = 0\}$.

Lemma 1 *If H is the parity check matrix of a code C then C is a code of distance at least d if any $d-1$ columns of H are linearly independent* [12].

Lemma 2 *Let S be a skew arc in $PG(m,2)$ with n_S points. Let H be the matrix whose columns are the elements of S (using their binary coordinates). Then H will be the parity check matrix of an $[n_S, n_S-(m+1), 5]$ code.*

Proof:

No three columns are dependant by part 1 of Definition 1. No four columns are dependant by part 2 of Definition 1.

This follows from Definition 1.

□

We note that the converse of Lemma 2 is also true. The columns of a parity check matrix of a code with distance at least 5 will form a skew arc.

For an example, we can look at the skew arc given in the previous section. So

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

is the parity check matrix of an $[8, 2, 5]$ code whose 4 codewords are $[0,0,0,0,0,0,0,0]$, $[1,1,1,1,0,0,1,0]$, $[0,0,1,1,1,1,0,1]$, $[1,1,0,0,1,1,1,1]$.

4 Some skew arc constructions

There are several known recursive constructions for arcs [4] [5] [6] [7] [9] [10]. For example, given an arc of size k in $PG(m, 2)$, an arc of size $2k$ can be constructed in $PG(m+1, 2)$. With this in mind, we attempted to find something similar for skew arcs, leading us to the following result which requires two separate skew arcs to start with.

Theorem 3 *If we have in $PG(m, 2)$ two skew arcs S_1 and S_2 of sizes k_1 and k_2 respectively such that $(S_1 \cup \tilde{S_1}) \cap (S_2 \cup \tilde{S_2}) = \emptyset$ then there exists in $PG(m+1, 2)$ a skew arc of size $k_1 + k_2 + 1$.*

Proof: We embed the copy of $PG(m, 2)$ into $\Pi = PG(m+1, 2)$ as follows via an isomorphism with a hyperplane of Π, which we will call H. Pick a point p in $\Pi \backslash H$.

Define $\vec{S_2^p}$ as $\{s_i + p | s_i \in S_2\}$. Now let $S = S_1 \cup \vec{S_2^p} \cup \{p\}$. We claim that S is the desired skew arc.

To see that it is a skew arc, we first show that S contains no lines. Since $S \cap H$ contains only elements of S_1, which is itself a skew arc, there are no lines of H in S. We consider lines that will have one point in H and two in $\Pi \backslash H$. The point p will not be on a line with a point of $\vec{S_2^p}$ and a point of S_1 since $S_1 \cap S_2 = \emptyset$. Two points of $\vec{S_2^p}$ will not be on a line with a point of S_1 since $S_1 \cap \tilde{S_2} = \emptyset$. Since all lines of Π meet H, we have shown S satisfies condition 1 of Definintion 1.

Now to see that there are no planar quadrangles we check that all sums of two elements of S are distinct. We note that the sum of any two elements in H will be in H, and also the sum of two elements in $\Pi \backslash H$ will be in H. Hence the only possibility for an element of $\tilde{S}$ to be in H is for it to be either the sum of two elements that are both from S_1 or the sum of two elements both from $\vec{S_2^p} \cup \{p\}$.

Two elements from S_1 have their sum in $\tilde{S_1}$ and two elements of $\vec{S_2^p}$ have their sum in $\tilde{S_2}$. Also, p and any element from $\vec{S_2^p}$ will have the sum in S_2. Hence all the elements of $\tilde{S} \cap H$ are distinct.

For sums in $\Pi \backslash H$, we look at the sum of two elements, one in H, the other in $\Pi \backslash H$. There are two types, $a + p$ and $a + b$ where $a \in S_1$ and $b \in \vec{S_2^p}$. A point of type $a + p$ and a point of type $a + b$ are distinct since $\tilde{S_1} \cap S_2 = \emptyset$. Two points of type $a + b$, where the a's and b's are distinct will be distinct since $\tilde{S_1} \cap \tilde{S_2} = \emptyset$ (If the a's are not distinct, then two sums of type $a + b$ will be distinct simply because the b's are distinct. The case where the b's are not distinct as well as the case of two points of type $a + p$ are similar). Hence S satisfies condition 2 of Definition 1.

□

Example 1 Let S_1 be $(1,0,0,0,0,0)$, $(0,1,0,0,0,0)$, $(0,0,1,0,0,0)$, $(0,0,0,1,0,0)$, $(0,0,0,0,1,0)$, $(0,0,0,0,0,1)$, $(1,1,1,1,0,0)$, $(0,0,1,1,1,1)$, and let $S_2 = \{(1,0,1,0,1,1),(0,1,1,1,0,1)\}$. Since $\tilde{S_2}$ is $(1,1,0,1,1,0)$, $(S_1 \cup \tilde{S_1}) \cap (S_2 \cup \tilde{S_2}) = \emptyset$. We embed $PG(5,2)$ into $PG(6,2)$ by identifying each element of $PG(5,2)$ with an element having its last coordinate zero. (i.e. $(1,0,0,0,0,0)$ in $PG(5,2)$ becomes identified with $(1,0,0,0,0,0,0)$ in $PG(6,2)$) Now using $(0,0,0,0,0,0,1)$ as p we get a skew arc with 11 points in $PG(6,2)$, namely $(1,0,0,0,0,0,0)$, $(0,1,0,0,0,0,0)$, $(0,0,1,0,0,0,0)$, $(0,0,0,1,0,0,0)$, $(0,0,0,0,1,0,0)$, $(0,0,0,0,0,1,0)$, $(1,1,1,1,0,0,0)$, $(0,0,1,1,1,1,0)$, $(0,0,0,0,0,0,1)$, $(1,0,1,0,1,1,1)$, $(0,1,1,1,0,1,1)$.

This result can easily be generalized to a case where we start with several skew arcs:

Corollary 4 *If we have in $PG(m,2)$ $n+1$ skew arcs $S_0, S_1, \cdots S_n$ of sizes $k_0, k_1, \cdots k_n$ respectively such that $(S_i \cup \tilde{S_i}) \cap (S_j \cup \tilde{S_j}) = \emptyset$ for $i \neq j$; $i,j = 0 \ldots n$ then we can find in $PG(m+n,2)$ a skew arc of size $k_0 + k_1 + \cdots + k_n + n$.*

Proof:

We can embed $PG(m,2)$ into a $PG(m+1,2)$ as above and use S_0 with S_1 to construct a new skew arc S using Theorem 3. From the proof, we can see that since all points of $\tilde{S}$ that intersect the original $PG(m,2)$ are either in $\tilde{S}_0$, S_1, or $\tilde{S}_1$, hence $(S \cup \tilde{S}) \cap (S_i \cup \tilde{S}_i) = \emptyset$ for $i = 2 \ldots n$. We continue in this manner n times. □

Example 2 Using S_1 and S_2 as in Example 1 and $S_3 = \{(1,1,0,1,1,1), (0,1,1,1,1,0)\}$, we get $(1,0,0,0,0,0,0,0)$, $(0,1,0,0,0,0,0,0)$, $(0,0,1,0,0,0,0,0)$, $(0,0,0,1,0,0,0,0)$, $(0,0,0,0,1,0,0,0)$, $(0,0,0,0,0,1,0,0)$, $(1,1,1,1,0,0,0,0)$, $(0,0,1,1,1,1,0,0)$, $(0,0,0,0,0,0,1,0)$, $(1,0,1,0,1,1,1,0)$, $(0,1,1,1,0,1,1,0)$, $(1,1,0,1,1,1,0,1)$, $(0,1,1,1,1,0,0,1)$, $(0,0,0,0,0,0,0,1)$ as a skew arc in $PG(7,2)$ with 14 points.

This generalization raises the question of how large the dimension needs to be in order to build the new skew arc. We show below that, with additional conditions, we can obtain a construction requiring fewer dimensions than used in Corollary 4.

For this, we introduce some new notation. If A and B are disjoint subsets of $PG(m,2)$ then $A+B = \{x | \exists a \in A, \exists b \in B \text{ such that} \{a,b,x\} \text{is a line}\}$. Alternately, if we are considering points according to their coordinitization, then this is simply $\{a+b | a \in A, b \in B\}$

Theorem 5 *If we have in $PG(m,2)$ four skew arcs S_0, S_1, S_2 and S_3 of sizes k_0, k_1, k_2 and k_3 respectively such that $(S_i \cup \tilde{S}_i) \cap (S_j \cup \tilde{S}_j) = \emptyset$ for $i \neq j$; $i,j = 0,1,2,3$ and if there is a point d in $PG(m,2)$ such that $d \notin S_i$, $d \notin S_i + S_j$, $i \neq j$, $d \notin S_i + S_j + S_k$ for distinct $i,j,k \in \{0,1,2,3\}$ and $d \notin S_0 + S_1 + S_2 + S_3$, then there exists in $PG(m+2,2)$ a skew arc of size $k_0 + k_1 + k_2 + k_3 + 3$.*

Proof:

We embed $PG(m,2)$ into $\Pi = PG(m+2,2)$ as follows via an isomorphism with a subspace H of Π. Let M_1, M_2, and M_3 be the hyperplanes of Π containing H. We pick $p_1 \in M_1 \backslash H$, $p_2 \in M_2 \backslash H$ and let p_3 be the point $p_1 + p_2 + d$. Note that $p_3 \in M_3 \backslash H$.

Now $S = S_0 \cup S_1^{\vec{p}_1} \cup \{p_1\} \cup S_2^{\vec{p}_2} \cup \{p_2\} \cup S_3^{\vec{p}_3} \cup \{p_3\}$ is the required skew arc, which we now show.

For $i = 1,2,3$, $S \cap M_i$ is constructed in exactly the same way as in Theorem 3. So when we check to ensure S has no lines, we already know that there are no lines in H, nor any in each M_i. All that is left to check is that there are no lines that have one point in each of the M_i's.

A line intersecting all of the M_i's would have one point in each $M_i \backslash H$. Without loss of generality, let these three points be denoted $a + p_1$, $b + p_2$, and $c + p_3$, where $a \in S_1 \cup \{0\}$, $b \in S_2 \cup \{0\}$, and $c \in S_3 \cup \{0\}$ (where $0 + p_i$ is simply the point p_i). We see that we would get $a + b + c + d = 0$, so $d = a + b + c$. If all three of a, b, and c were 0 then we would conclude that $d = 0$, which is a contradiction, since 0 does not represent any point in the geometry. All other cases would imply that $d \in S_1$, S_2, S_3, $S_1 + S_2$, $S_1 + S_3$, $S_2 + S_3$, or $S_1 + S_2 + S_3$.

When checking S for planar quadrangles, we again know that there are none that are contained in a single M_i from the proof of Theorem 3. All that is left to check is that the sum of two elements from $M_i \backslash H$ is disjoint from the sum of two elements of H or two elements of $M_j \backslash H$ (for $i \neq j$, $i, j \in \{1, 2, 3\}$) and that the sum of an element from $M_1 \backslash H$ with an element of $M_2 \backslash H$ is disjoint from the sum of an element in $M_3 \backslash H$ and an element of H.

As in the proof of Theorem 3, we notice that the sum of two elements of $S \cap H$ is in $S_0 \cup \tilde{S}_0$ and the sum of two elements of $S \cap M_i \backslash H$ for $i \in \{1, 2, 3\}$ is in $S_i \cup \tilde{S}_i$. These sums must be distinct.

For the last part, let us consider $a + p_1$ to be an element of $S \cap M_1 \backslash H$ where $a \in S_1 \cup \{0\}$, similarly with $b + p_2$ and $c + p_3$ as before, and let $z \in S \cap H$. If the sum of $a + p_1$ and $b + p_2$ were not distinct from the sum of $c + p_3$ and z, then we would have $a + b + c + d + z = 0$, hence $d = a + b + c + z$. This would imply that $d \in S_0$, $S_0 + S_1$, $S_0 + S_2$, $S_0 + S_3$, $S_0 + S_1 + S_2$, $S_0 + S_1 + S_3$, $S_0 + S_2 + S_3$, or $S_0 + S_1 + S_2 + S_3 + S_0$.

□

Example 3 This example is to show that it is possible to have 4 skew arcs that satisfy the conditions of Theorem 5, but exclude the possibility of a suitable d. Consider the following skew arcs. Let S_0 be $\{(1,0,0,0,0,0), (0,1,0,0,0,0), (0,0,1,0,0,0), (0,0,0,1,0,0), (0,0,0,0,1,0), (0,0,0,0,0,1), (1,1,1,1,0,0)\}$, let S_1 be $\{(1,0,1,0,1,0), (0,1,0,1,0,1), (1,1,0,0,1,1)\}$, let S_2 be $\{(1,0,0,0,1,1), (0,1,1,0,1,0), (1,1,0,1,0,1)\}$, and let S_3 be $\{(1,0,0,1,0,1), (0,1,0,0,1,1)$. Now we have four skew arcs such that $(S_i \cup \tilde{S}_i) \cap (S_j \cup \tilde{S}_j) = \emptyset$ for $i \neq j$ but we cannot build an 18 point skew arc in $PG(7,2)$ [3], and so no point d with the required properties can exist.

Example 4 We can start with the skew arc given in Section 2 (Also S_1 from Example 1), and let that be S_0. We let S_1 be $\{(1,0,1,0,1,1), (0,1,1,1,0,1)\}$, S_2 be $\{(1,1,0,1,1,1), (0,1,1,1,1,0)\}$ and let S_3 be $\{(0,1,0,1,0,1), (1,0,1,0,1,0)\}$. If $d = (1,0,1,1,0,0)$, we see it satisfies the conditions of Theorem 5. This gives us a skew arc with 17 points in $PG(7,2)$. The skew arc will have the following points if we choose p_1 to be $(0,0,0,0,0,0,1,0)$, and p_2 to be $(0,0,0,0,0,0,0,1)$: $(1,0,0,0,0,0,0,0)$, $(0,1,0,0,0,0,0,0)$, $(0,0,1,0,0,0,0,0)$, $(0,0,0,1,0,0,0,0)$, $(0,0,0,0,1,0,0,0)$, $(0,0,0,0,0,1,0,0)$, $(1,1,1,1,0,0,0,0)$, $(0,0,1,1,1,1,0,0)$, $(0,0,0,0,0,0,1,0)$, $(1,0,1,0,1,1,1,0)$, $(0,1,1,1,0,1,1,0)$, $(1,1,0,1,1,1,0,1)$, $(0,1,1,1,1,0,0,1)$, $(0,0,0,0,0,0,0,1)$, $(1,0,1,1,0,0,1,1)$, $(1,1,1,0,0,1,1,1)$, $(0,0,0,1,1,0,1,1)$.

5 A geometric construction of Wagner's [23, 14,5] code

We turn our attention now to a known class of codes, BCH codes. For this we view each element of $GF(2^n)$ as its length n binary expansion, represented as a column. If α is primitive in $GF(2^n)$, it is known that the parity check matrix of the BCH code with $d \geq 5$ is the following $2n \times (2^n - 1)$ matrix [12].

$$\begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^i & \cdots & \alpha^{(2^n-2)} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3i} & \cdots & \alpha^{3(2^n-2)} \end{bmatrix}$$

We can view these columns as points of $PG(2n-1,2)$ and we will refer to the set of these points (which is a skew arc - see comment following Lemma 2) as B_n. Also, we can view all points in $PG(2n-1,2)$ as 2-tuples over $GF(2^n)$ as well as $2n$-tuples over $GF(2)$.

Expecting to use skew arcs of type B_n in the construction, we discovered the following theorem which shows what $B_n \cup \tilde{B_n}$ looks like in $PG(2n-1,2)$.

Theorem 6

The set $M_x = \{x^3 + a^3 + b^3 | a + b = x\}$ for $x \neq 0$ is a (additive) subgroup of $GF(2^n)$ and $[GF(2^n) : M_x] = 2$.

<u>Proof:</u>

Suppose $a + b = x$ and $c + d = x$. Then $x^3 + a^3 + b^3 + x^3 + c^3 + d^3$

$$\begin{aligned} &= a^3 + b^3 + c^3 + d^3 \\ &= a^3 + b^3 + x^3 + c^2 d + cd^2 \\ &= x^3 + a^3 + b^3 + c^2(a + b + c) + c(a^2 + b^2 + c^2) \\ &= x^3 + (a^3 + ca^2 + c^2 a + c^3) + (b^3 + cb^2 + c^2 b + c^3) \\ &= x^3 + (a + c)^3 + (b + c)^3. \end{aligned}$$

Since $(a+c)+(b+c)=a+b=x$, we see that this is in M_x. Hence M_x is closed under addition. Since there are exactly 2^{n-1} pairs of elements that sum to x, we see that $[GF(2^n):M_x]=2$.

□

Let $M_x+x^3=N_x=\{a^3+b^3|a+b=x\}$. If n is even we let $t=(2^n-1)/3$. Recall that α is a primitive element in $GF(2^n)$. Since n is even, we know that $GF(2^n)$ contains a subfield of order 2 which will contain the elements $0, 1, \alpha^t, \alpha^{2t}$. Hence $1+\alpha^t+\alpha^{2t}=0$. So for $x \in GF(2^n)$ $x = x\alpha^t + x\alpha^{2t}$. Since $x^3=(x\alpha^t)^3=(x\alpha^{2t})^3$, we can see that $0 \in N_x$ and hence $N_x = M_x$. If n is odd, 3 and 2^n-1 are relatively prime, so $a^3 \neq b^3$ if $a \neq b$ for $a, b \in GF(2^n)$. So $0 \notin N_x$ hence N_x must be the other coset of M_x. So now we see that for any element y in $GF(2^n)$, all points in $B_n \cup \tilde{B_n}$ which have y in the first coordinate have either y^3 or a^3+b^3, where $a+b=y$, in the second. Hence $B_n \cup \tilde{B_n} = \{(y,z)|z \in N_y\}$.

We introduce now a small skew arc that we will use along with the BCH codes in constructions.

For x_i, y_i, $z_i \in GF(2^n)$, $i=1,2$, we have the following skew arc of seven points: $(0, x_2+y_2+z_2)$, (x_1, x_2), (x_1, x_2+z_2), (y_1, y_2), (y_1, y_2+x_2), (z_1, z_2), (z_1, z_2+y_2) where the triples $\{x_1, y_1, z_1\}$ and $\{x_2, y_2, z_2\}$ generate 8 element additive subgroups (not necessarily different) of $GF(2^n)$ for $n \geq 3$. We call this skew arc A_3, since the code it gives via Lemma 2 is isomorphic to that given by B_3 (i.e., the BCH code of length 7).

We see that $A_3 \cup \tilde{A_3}$ takes the following form, which is similar to the form of $B_n \cup \tilde{B_n}$. Elements that have a first element of 0 have as their second element one of $[x_2+y_2+z_2, x_2, y_2, z_2]$ (which is a coset of a 4 element subgroup of the group generated by x_2, y_2, z_2). Elements that have x_1 as their first element have as second element one of $[x_2, x_2+z_2, y_2+z_2, y_2]$ (again a coset), etc.

Let α be a primitive element in $GF(2^4)$, where $\alpha^4+\alpha+1$ is the generating polynomial. We let $\{x_1, y_1, z_1\}$ be $\{\alpha^{10}, \alpha^9, \alpha^6\}$ and $\{x_2, y_2, z_2\}$ be $\{\alpha^2, \alpha^8, \alpha^{10}\}$. We can see that this skew arc would intersect with B_4, so we change it by adding α^{13} to the second element of each column that has a first element α^{10} or α^6. We then get the following skew arc in $PG(7,2)$ with 7 points: $(0,\alpha^5)$, $(\alpha^{10},\alpha^{14})$, $(\alpha^{10},\alpha^{11})$, $(\alpha^9,1)$, (α^9,α^8), (α^6,α^9), (α^6,α^{12})

Now A_3 as given above along with B_4 fullfill the conditions of Theorem 3. Since A_3 has 7 points and B_4 has15 points,and are both in $PG(7,2)$, we can construct a skew arc of size 23 in $PG(8,2)$, giving rise to a $[23,14,5]$ code.

Research Problem 18.3 of [12] asks to find a simple construction of Wagner's $[23,14,5]$ code. This gives one, which unfortunately does not extend well. If we were to construct skew arcs with A_3 and B_n for $n \geq 5$, the associated codes would have parameters $[2^n+7, 2^n-2n+6, 5]$. If we compare these to shortened BCH codes with the same redundency we see that the shortened BCH is as good or better.

In this paper, we showed that A_3 is a skew arc with the same size as B_3 whose stucture is similar to that of B_3 in the sense that $A_3 \cup \tilde{A}_3$ in $PG(7,2)$ can be described in terms of cosets of additive subgroups of $GF(2^3)$. It may be possible to extend this idea by finding larger variations of A_3, eg. a skew arc A_n where $A_n \cup \tilde{A}_n$ has a similar description in $PG(2m+1,2)$ (for $m \geq n$).

References

[1] L. Batten, M. Davidson and L. Storme, An analysis of Chen's construction of minimum distance five codes, *IEEE Transactions on Information Theory* **46** (2000), 505–511.

[2] A.E. Brouwer, P. Delsarte and P. Piret, On the [23, 14, 5] Wagner code, *IEEE Transactions on Information Theory* **26** (1980), 742–743.

[3] A.E. Brouwer and T. Verhoeff, an upddated table of minimum-distance bounds for binary linear codes, *IEEE Transactions on Information Theory* **39** (1993), 662–677.

[4] A.A. Bruen, L. Haddad and D.L. Wehlau, Binary codes and caps, *J. Combin. Des.* **6** (1998), 275–284.

[5] A.A. Bruen and D.L. Wehlau, Codes, caps, graph coloring and line-free sets in projective space, talk given at 'combinatorics 96' in Assisi, Italy.

[6] A.A. Bruen and D.L. Wehlau, Long binary linear codes and large caps in projective space, *Des. Codes. Cryptogr.* **17** (1999), 37–60.

[7] P. Ceccherini and G. Tallini, Codes, caps and linear spaces, *London Math. Soc. Lecture Notes Ser.* **49** (1981), 72–80.

[8] C.L. Chen, Construction of some binary linear codes of minimum distance five, *IEEE Transactions on Information Theory* **37** (1991), 1429–1432.

[9] W.E. Clark, Blocking sets in finite projective spaces and uneven binary codes, *Discrete Math.* **94** (1991), 65–68.

[10] R. Hill, Caps and codes, *Discrete Math.* **22** (1978), 11–137.

[11] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, second ed., 1998.

[12] F. MacWilliams and N. Sloane, *The Theory of Error Correction codes*, North-Holland, Amsterdam, The Netherlands, 1977.

[13] J. Simonis, The [23, 14, 5] Wagner code is unique, *Discrete Math.* **213** (2000), 269–282.

[14] T.J. Wagner, A search technique for quasi-perfect codes, *Information and Control* **9** (1966), 94–99.