Partitions in finite geometry and related constant composition codes

Tim L. Alderson* Keith E. Mellinger†

Abstract

We look at the construction of constant composition codes (CCCs) from various types of partitions in finite projective spaces. In particular, we construct robust classes of codes using regular spreads of $\mathsf{PG}(2n-1,q)$ and Baer subgeometry partitions of $\mathsf{PG}(2n,q^2)$. For each class of codes, we bound the minimum distance by considering how such partitions can intersect. As such, we prove results about the intersection of regular spreads and Baer subgeometry partitions, two of the classical partitions generated by subgroups of a Singer group. In addition, we examine other partitions of objects embedded in finite projective spaces and their associated codes. In each case, we compare our codes to a code of comparable parameters that meets the Plotkin bound.

Keywords: spreads, Baer subgeometry partitions, constant composition codes

MSC 2000: 51E20,94B60

1. Introduction

Constant Composition Codes, or CCCs, have been recently examined as an effective form of error correcting coding over electric power lines [15]. They also arise in frequency hopping, when a schedule is needed to determine frequencies on which to transmit [9]. Two special cases of CCCs are constant weight binary codes and permutation codes, both of which have been studied in some depth.

*The first author acknowledges support from the N.S.E.R.C. of Canada.

†The second author acknowledges support by the National Security Agency under grant number H98230-06-1-0080.

Recently, many constructions of CCCs were presented in [4] using techniques in algebra and combinatorics.

In the present article, we look at the more general CCCs and construct examples using techniques from finite projective geometry. Our techniques involve the partitioning of projective spaces and objects embedded in projective spaces. Codewords correspond to partitions and determining bounds on the minimum distance requires an understanding of how distinct partitions intersect. As such, we study the intersection of spreads and Baer subgeometry partitions, as well as the intersection of partitions of quadratic cones, ovoids, hyperbolic quadrics, and unitals.

Let $\mathcal{C}$ be a k-ary code of length n and minimum distance d on the alphabet $\{1, 2, \ldots, k\}$. As usual, the elements of $\mathcal{C}$ are called codewords. The code $\mathcal{C}$ is said to have *constant weight composition* $[n_1, n_2, \ldots, n_k]$ if every codeword has n_i occurrences of symbol i for $i = 1, \ldots, k$. The code $\mathcal{C}$ is a *constant composition code*, or CCC$([n_1, n_2, \ldots, n_k], d)$. Let $A([n_1, n_2, \ldots, n_k], d)$ denote the maximum size of such a CCC. When writing compositions, the exponential notation $n_1^{t_1}, n_2^{t_2}, \ldots, n_h^{t_h}$ will be used to abbreviate

$$[\overbrace{n_1, \ldots, n_1}^{t_1}, \overbrace{n_2, \ldots, n_2}^{t_2}, \ldots, \overbrace{n_h, \ldots, n_h}^{t_h}] .$$

Codes with composition 1^n are also known as *permutation arrays* and are denoted by PA(n, d). They have been studied in depth in [3].

We recall Section 4 of [4] where CCCs are constructed from resolvable designs. Let X be a set of size n and $\mathcal{B}$ a collection of nonempty subsets of X (blocks) whose sizes belong to $\mathcal{K}$. If t and λ are positive integers, the pair $(X, \mathcal{B})$ is a *t-wise balanced design* with index λ if every subset of size t of X is contained in exactly λ blocks. We now restrict ourselves to the case when $\lambda = 1$.

A design $(X, \mathcal{B})$ is called *resolvable* if $\mathcal{B}$ can be partitioned into partitions, or *resolution classes*, of X. If in addition each resolution class contains the same number of blocks of each size, the design is called *class-uniformly resolvable*. When all blocks have the same size, say k, such designs are called *Steiner systems* and are denoted $S(t, k, n)$. For an $S(t, k, n)$ to be resolvable, we need $k \mid n$, and an easy count shows that there are $\binom{n}{t}/\binom{k}{t}$ blocks and $\binom{n-1}{t-1}/\binom{k-1}{t-1}$ resolution classes. Theorem 4.1 of [4] says that every such resolvable design D can be used to construct a CCC. We summarize this result for clarity.

Let D be the Steiner system $S(t, k, n)$ and define a code $\mathcal{C}_D$ of length n as follows. Label the coordinate positions of the codewords with the points of D. Every resolution class will correspond to a different codeword. For a resolution class R, arbitrarily assign to each block of the class a different element from the alphabet. Now create a codeword $\mathbf{c}_R$ in the natural way. If coordinate i

corresponds to point P lying in a block assigned with alphabet member j, then the i^{th} coordinate is given value j. In this fashion, we create a codeword with composition $[k^{n/k}]$. The minimum distance of $\mathcal{C}_D$ is determined by how two distinct resolutions can intersect. By the definition of $S(t,k,n)$, any two blocks meet in at most $t-1$ points. There are k points in each block and n/k blocks in a given resolution class. Given two resolution classes R_1 and R_2, the worst case scenario is that every pair of blocks $B_1 \in R_1$ and $B_2 \in R_2$ that have the same label actually meet in $t-1$ points. This implies that the two corresponding codewords have at most $\frac{n}{k}(t-1)$ coordinates in common. Hence, the two codewords differ in at least $d = n - \frac{n}{k}(t-1) = \frac{n}{k}(k-t+1)$ coordinates.

Note also that any particular resolution gives rise to multiple codewords by permuting the members of the alphabet using elements of a permutation array. Recall that a *permutation array*, $\mathsf{PA}(n,d)$, is simply a CCC with composition 1^n. Hence, a permutation array consists of a list of permutations of the integers $\{1,2,\ldots,n\}$ with the property that any two permutations agree in at most $n-d$ positions. It follows that permuting the members of our alphabet using a permutation array with parameters $\mathsf{PA}(n/k, \lceil d/k \rceil)$ will give us multiple codewords for every resolution class. In summary, the resolvable design gives rise to a $\mathsf{CCC}([k^{n/k}], \frac{n}{k}(k-t+1))$ having $r \cdot s$ codewords where $r = \binom{n-1}{t-1}/\binom{k-1}{t-1}$ is the number of resolution classes and s is the maximum size of a permutation array with parameters $\mathsf{PA}(n/k, \lceil d/k \rceil)$.

The permutation array plays an important role in establishing a lower bound on the size of our codes. In order for us to find the best possible lower bounds for our codes, we rely on some results about permutation arrays that can collectively be found in [5]. Let $M(n,d)$ be the maximum size of a permutation array of length n and minimum distance d. The following results will be useful in subsequent arguments.

Proposition 1.1. *For every n and $d \leq n$,*

$$M(n,d) \geq \max\{M(n-1,d), M(n,d+1)\}\,.$$

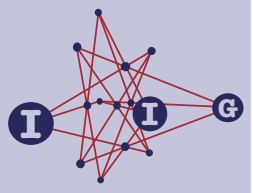
Proposition 1.2 ([3])**.** *If q is a prime power, then $M(q,q-1) = q(q-1)$.*

Proposition 1.3 ([6])**.** *If q is a prime power, then $M(q+1,q-1) = (q+1)q(q-1)$.*

Inductively applying Propositions 1.1 and 1.3 we get the following which shall prove useful in the sequel.

Corollary 1.4. *For fixed n and d let α be a prime power with $d < \alpha < n$. Then $M(n,d) \geq \alpha^3 - \alpha$.*

A natural construction of a CCC based on finite geometry appears in [4] and involves the *affine plane*. The classical affine plane of order q denoted



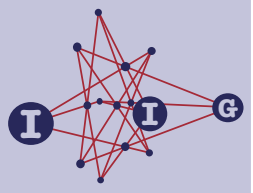
by AG$(2, q)$ is a resolvable design with parameters $S(2, q, q^2)$. Moreover, the maximum size of a permutation array PA$(q, q-1)$ is $q(q-1)$. Hence, we naturally construct a CCC$[q^q, q(q-1)]$ of size $(q+1)q(q-1)$ and distance $q(q-1)$ (note that $q+1$ is the number of parallel classes in an affine plane of order q). In this article we aim to generalize this type of construction using other partitioning ideas from finite geometry. In particular, we relax the condition that the resolution classes actually *partition* the blocks from the design. Rather, we allow for two distinct partitions to share a common block. With this relaxed condition, we are able to find many examples of CCCs that arise naturally from partitioning ideas in finite geometry. We describe each construction in detail and bound the minimum distance using geometric arguments.

By loosening the condition on how partitions can intersect, we lose the ability to apply the well-known *Plotkin bound* to our codes. The Plotkin bound states that a k-ary code of length n and minimum distance d has at most $\frac{d}{d-n+n/k}$ codewords, provided that the denominator is positive. Our partitions have the property that each of the subsets in the partition has the same size, say λ, implying that $n/k = \lambda$. Hence, the condition for the Plotkin bound is that $d > n-\lambda$. If we allow two partitions to have one subset in common, it follows that $d \leq n-\lambda$. So, one on hand, we lose the power of the Plotkin bound for determining the optimality of our codes. However, in every one of our constructions we are able to show that the minimum distance is not far from $n - \lambda$, and that our code contains many more codewords than would be obtained from a code with the same n and k, and with only slightly larger d (which is necessary to apply the Plotkin bound). We address this in more detail in Section 5 after discussing our constructions.

The article is structured as follows. Sections 2 and 3 give details about how regular spreads and Baer subgeometry partitions of finite projective spaces can intersect. We construct codes from these partitions and geometric arguments are then used to bound their minimum distances. Section 4 looks at other partitions, mostly of objects embedded in projective spaces, and we again bound minimum distances using the geometry. In each of these sections, bounds on the sizes of the relevant permutation arrays are given. The final section of the article summarizes our results and compares our codes to other codes that meet the Plotkin bound.

2. Regular spreads

Our first class of CCCs is developed using *spreads*. A spread of the projective space $\Sigma = \text{PG}(2n-1, q)$ is a partition of Σ into $(n-1)$-spaces. We start with an overview of spreads in PG$(3, q)$.



Definition 2.1. A *regulus* of $\Sigma = \mathsf{PG}(3, q)$ is a collection of $q + 1$ lines of Σ with the property that any other line meeting three of the regulus lines meets all of them.

A straight forward linear algebra argument shows the following.

Lemma 2.2. *Let l_1, l_2, and l_3 be three distinct, pairwise disjoint lines of Σ. Then there exists a unique regulus containing l_1, l_2, and l_3.*

For $q > 2$, we will say that a spread S of Σ is *regular* if for every three distinct elements of S, the unique regulus determined by them is a subset of S. There is a well-known connection between regular spreads of Σ and finite Desarguesian projective planes. More generally, every spread of Σ (regular or not) can be used to construct a finite projective plane of order q^2, not necessarily Desarguesian.

Simple counting can be used to show that Σ contains $(q^2 + 1)(q^2 + q + 1)$ lines. Moreover, basic linear algebra can be used to show the following.

Proposition 2.3. *Let $\mathcal{R}$ be a regulus of Σ and let l be a line of Σ that is skew to every line of $\mathcal{R}$. Then the exists a unique regular spread of Σ containing both $\mathcal{R}$ and l. Hence, two regular spreads of Σ intersect in at most $q + 1$ spread lines.*

Using some group theory, one can show that the number of regular spreads of Σ is $\frac{1}{2}q^4(q-1)(q^3-1)$ (see [11, Theorem 25.6.6]) and that every spread contains $q(q^2 + 1)$ reguli.

We now turn to the construction of a constant composition code from the lines of Σ. Let $\mathcal{C}_\mathcal{S}$ be the code of length q^3+q^2+q+1, each of whose coordinates is labeled with a point of Σ and let $\mathcal{S}$ be the set of all regular spreads of Σ. For each regular spread S of $\mathcal{S}$, we define a codeword $\mathbf{c}_S$ as follows. Every line of S is arbitrarily assigned a symbol in $\{1, 2, \ldots, q^2 + 1\}$, and coordinates corresponding to points lying on the same line of S are given that symbol in $\mathbf{c}_S$. Because two distinct regular spreads can only intersect in at most $q+1$ lines, we are able to bound the minimum distance. If two spreads met in $q + 1$ lines that were labeled identically, and the remaining identically labeled pairs of lines all met in a single point, the total number of common coordinates would be $(q + 1)(q + 1) + (q^2 - q) = 2q^2 + q + 1$.

Theorem 2.4. *The code $\mathcal{C}_\mathcal{S}$ described above is a $\mathsf{CCC}([(q + 1)^{q^2+1}], d)$ containing $\frac{1}{2}q^4(q-1)(q^3-1) \cdot s$ codewords, where $d \geq q^3 - q^2$ and s is the maximum size of a $\mathsf{PA}(q^2 + 1, q^2 - 2q + 2)$.*

Proof. The composition of the code $\mathcal{C}_\mathcal{S}$ follows from the construction. Since two codewords can have at most $2q^2 + q + 1$ coordinates in common, the minimum distance is at least $(q^3 + q^2 + q + 1) - (2q^2 + q + 1) = q^3 - q^2$.

Hence, the minimum distance for the associated permutation array is at least $\lceil \frac{d}{k} \rceil = \lceil (q^3 - q^2)/(q+1) \rceil = \left\lceil q^2 - 2q + 2 - \frac{2}{q+1} \right\rceil = q^2 - 2q + 2$. □

Proposition 1.1 implies that $M(q^2+1, q^2-2q+2) \geq M(q^2+1, q^2-1)$. Hence, from Proposition 1.3 it follows that $M(q^2+1, q^2-2q+2) \geq (q^2+1)q^2(q^2-1)$. This gives us the following.

Corollary 2.5. $A([(q+1)^{q^2+1}], q^3 - q^2) \geq \frac{1}{2}q^6(q^4-1)(q^3-1)(q-1) \approx \frac{1}{2}\,q^{14}$.

These codes can be generalized in a natural way using $(n-1)$-spreads of $\mathsf{PG}(2n-1, q)$. Lemma 2.2 still holds with the term "line" replaced with the more general "$(n-1)$-space". The size of the intersection of two spreads, as discussed in Proposition 2.3, however, is no longer bounded by $q+1$. In order to generalize our construction, one needs to determine the maximum possible intersection size for two regular spreads of $\mathsf{PG}(2n-1, q)$.

Theorem 2.6. *Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be regular spreads of $\mathsf{PG}(2n-1, q)$ with $n > 2$. Then, $\mathcal{S}_1$ and $\mathcal{S}_2$ intersect in at most $m+1$ spread elements where m is the size of the maximum proper subfield of $\mathsf{GF}(q^n)$.*

Proof. We consider the associated affine planes. Two distinct regular spreads, $\mathcal{S}_1$ and $\mathcal{S}_2$, of $\mathsf{PG}(2n-1, q)$ can be used to construct two Desarguesian affine planes coordinatized by the field $\mathsf{GF}(q^n)$. The spread, in this setting, corresponds to points on the line at infinity and can be viewed as the elements of the corresponding field, together with the new symbol ∞. These elements correspond to slopes in the Euclidean plane and more details about how one goes about coordinatizing a finite affine plane can be found in [12].

If two regular spreads have at least three $(n-1)$-spaces in common, then we can coordinatize the common spread elements vectorially with $x = 0$, $y = 0$, and $y = x$. Here, coordinates for affine points are represented with ordered pairs (x, y), and the spread elements correspond to our Euclidean notion of slope. Hence, we are choosing coordinates for our planes in such a way that the slopes corresponding to 0, 1, and ∞ are common to the two planes.

Let the first regular spread have coordinate field K and the second regular spread have coordinate field L. Then, the remaining spread elements (for either spread) can take the form $y = kx$ as k varies over the elements of K or L. So, the number of spread elements that $\mathcal{S}_1$ and $\mathcal{S}_2$ have in common is one more than the size of the intersection of K and L. The problem, therefore, boils down to determining the subfield structure of the finite field of order q^n. Letting m be the size of the maximum (proper) subfield of $\mathsf{GF}(q^n)$, we see that $|\mathcal{S}_1 \cap \mathcal{S}_2| \leq m+1$. □

Note that if n is prime, then the maximal possible subfield is $\mathsf{GF}(q)$ and the intersection of $\mathcal{S}_1$ and $\mathcal{S}_2$ is a regulus of size $q+1$ as discussed in Proposition 2.3. However, two spreads of $\mathsf{PG}(7,q)$, for instance, could intersect in as many as q^2+1 solids. The process of "lifting" and "retracting" equivalent spreads lying in projective spaces of different dimensions may shed some light on this (see [14] for an overview of this procedure). As an example, suppose $\mathcal{S}_1$ and $\mathcal{S}_2$ are two regular spreads of $\mathsf{PG}(3,q^2)$. Then, as discussed above, $\mathcal{S}_1$ and $\mathcal{S}_2$ could intersect in at most a regulus which, in this case, contains q^2+1 lines. Assume that this is the case. There is a lifting process that takes a line-spread of $\mathsf{PG}(3,q^2)$ to a solid-spread of $\mathsf{PG}(7,q)$ whereby each line in $\mathsf{PG}(3,q^2)$ lifts to a unique solid of $\mathsf{PG}(7,q)$. So, the q^2+1 lines forming a regulus (the intersection of $\mathcal{S}_1$ and $\mathcal{S}_2$) in $\mathsf{PG}(3,q^2)$ lift to q^2+1 solids of $\mathsf{PG}(7,q)$. Hence, the two corresponding spreads of $\mathsf{PG}(7,q)$ lifted from $\mathcal{S}_1$ and $\mathcal{S}_2$ each contain q^4+1 spread elements and meet in q^2+1 spread elements.

Now let $\mathcal{S}_n$ be the set of all regular spreads of $\mathsf{PG}(2n-1,q)$. It can be shown (again in [11]) that

$$|\mathcal{S}_n| = \frac{q^{2n(n-1)}}{n(q^n-1)} \prod_{i=1}^{2n-1} (q^i-1)\,.$$

As before, we construct a CCC $\mathcal{C}_{\mathcal{S}_n}$ by creating a codeword for each regular spread of $\mathsf{PG}(2n-1,q)$ in the same fashion as above.

Theorem 2.7. *Let k be the largest proper divisor of n and let s denote the maximum size of a* $\mathsf{PA}\left(q^n+1, \dfrac{(q^{2n-1}-q^{n+k-1})(q-1)}{q^n-1}\right)$. *The code $\mathcal{C}_{\mathcal{S}_n}$ is a*

$$\mathsf{CCC}\left(\left[\left(\frac{q^n-1}{q-1}\right)^{q^n+1}\right], d\right)$$

consisting of $\dfrac{q^{2n(n-1)}}{n(q^n-1)} \prod_{i=1}^{2n-1} (q^i-1) \cdot s$ *codewords, where* $d \geq q^{2n-1}-q^{n+k-1}$.

Proof. The composition of the code $\mathcal{C}_{\mathcal{S}}$ follows from the construction. Now suppose S_1 and S_2 are two regular spreads of $\mathsf{PG}(2n-1,q)$ corresponding to codewords $\mathbf{c}_1$ and $\mathbf{c}_2$. We wish to determine how many coordinates they could have in common. As before, the two spreads could share at most q^k+1 spread elements where $\mathsf{GF}(q^k)$ is the maximal subfield of $\mathsf{GF}(q^n)$. In addition, pairs of spread elements from the two spreads that are labeled the same could intersect in at most an $(n-2)$-space. Hence, the two codewords could share at most $(q^k+1)\frac{q^n-1}{q-1} + (q^n-q^k)\frac{q^{n-1}-1}{q-1} = \frac{1}{q-1}(q^{2n-1}+q^{n+k}-q^{n+k-1}-1)$ common coordinates. Subtracting this from the length of $\frac{q^{2n}-1}{q-1}$ gives us an upper bound

of $(q^{2n-1}-q^{n+k-1})$ for d. The parameters for the permutation array follow from the construction discussed in Section 1. □

The permutation array needed for the previous class of codes has minimum distance which is roughly q^n. Hence, we can use Propositions 1.1 and 1.3 to bound the minimum size of our desired permutation array and therefore give a lower bound on the size of these codes.

Corollary 2.8. *We have*

$$A\left(\left[\left(\frac{q^n-1}{q-1}\right)^{q^n+1}\right], q^{2n-1}-q^{n+k-1}\right) \geq \frac{q^{2n(n-1)}}{n(q^n-1)}\prod_{i=1}^{2n-1}(q^i-1)\cdot(q^n-1)q^n(q^n+1) \approx \frac{1}{n}q^{4n^2-n}.$$

3. Baer subgeometry partitions

We can construct similar codes using partitions of the finite projective plane $\mathsf{PG}(2,q^2)$. Recall that a Baer subplane of $\pi=\mathsf{PG}(2,q^2)$ is a subplane π_0 isomorphic to $\mathsf{PG}(2,q)$. It is well known how to construct a Baer subplane partition of π.

Let L be the finite field of order q^6 and let α be a primitive element of L. Then L can be viewed as a 3-dimensional vector space over the finite field $K=\mathsf{GF}(q^2)$, and therefore may be used as a model for $\mathsf{PG}(2,q^2)$. Powers of the primitive element represent projective points, and any two powers whose quotient is in K represent the same projective point. Therefore, the field elements

$$1,\alpha,\alpha^2,\alpha^3,\ldots,\alpha^{q^4+q^2}$$

represent the q^4+q^2+1 distinct projective points of $\mathsf{PG}(2,q^2)$. Note that the next field element, $\alpha^{q^4+q^2+1}$, when raised to the q^2-1 power gives $\alpha^{q^6-1}=1$. Therefore, $\alpha^{q^4+q^2+1}$ is an element of K and so represents the same projective point as the field element 1.

Now, let G be the group acting on π induced by multiplication by α. So, G is a cyclic group that acts regularly on the points of π, a Singer group. Let g be a generator of G and consider the subgroup $H<G$ generated by g^{q^2-q+1}. Clearly, H has order q^2+q+1 and it is well-known that the orbits of H in π form Baer subplanes. We say that the orbits of H form the *classical Baer subplane partition*.

It is also well-known [10] that there are many Singer groups that act regularly on the points (and lines) of π. As a result, many Baer subplane partitions can be constructed by simply using subgroups of different Singer groups. Using a group theoretic argument to count these groups [10, Theorem 4.35], it can be shown that the set of Baer subplane partitions $\mathcal{B}$ of π, satisfies

$$|\mathcal{B}| \geq \frac{1}{3}\, q^6(q^2-1)(q^4-1)$$

since each Singer subgroup gives rise to a classical Baer subplane partition. We note that there exist Baer subplane partitions that do not arise in this fashion. However, we will not make use of such non-classical partitions here. Let $\mathcal{B}$ be the set of all classical Baer subplane partitions. It follows that $|\mathcal{B}| = \frac{1}{3}\, q^6(q^2-1)(q^4-1)$. Moreover, it was shown in [16] that by counting the number of ordered triples (B_1, B_2, P) where B_1 and B_2 are Baer subplanes in the classical Baer subplane partition P, that there is a unique classical Baer subplane partition containing two fixed disjoint Baer subplanes.

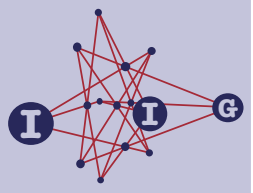
We now construct a constant composition code from the classical Baer subplane partitions of π in the same fashion that we constructed the codes from regular spreads. Let $\mathcal{C}_\mathcal{B}$ be the code of length q^4+q^2+1, each of whose coordinates is labeled with a point of π. For each Baer subplane partition B in $\mathcal{B}$, we define a codeword $\mathbf{c}_B$ as follows. Every Baer subplane of B is arbitrarily assigned a symbol in $\{1, 2, \ldots, q^2-q+1\}$, and coordinates corresponding to points lying on the same subplane of B are given that symbol in $\mathbf{c}_B$.

Theorem 3.1. *The code $\mathcal{C}_\mathcal{B}$ described above is a* $\mathsf{CCC}([(q^2+q+1)^{q^2-q+1}], d)$ *containing* $\frac{1}{3}\, q^6(q^2-1)(q^4-1)\cdot s$ *codewords where* $d \geq q(q-1)(q^2-1)$ *and* s *is the maximum size of a* $\mathsf{PA}(q^2-q+1, (q-1)^2)$.

Proof. The composition of the code $\mathcal{C}_\mathcal{B}$ follows from the construction. We bound d using the fact that two distinct Baer subplane partitions can only intersect in at most one Baer subplane. In [1] the different intersection patterns for two Baer subplanes of π were determined, and it was shown that the maximum number of points that two distinct Baer subplanes can have in common is $q+2$.

Now let $\mathbf{c}_1$ and $\mathbf{c}_2$ be two distinct codewords of $\mathcal{C}_\mathcal{B}$. We wish to determine the maximum number of coordinates these two codewords could have in common. To attain this maximum, we would have two corresponding partitions sharing a Baer subplane whose coordinates are labeled the same. In addition, all of the remaining pairs of commonly labeled Baer subplanes from the two partitions would meet in $q+2$ points each. Hence, the maximum number of coordinates that $\mathbf{c}_1$ and $\mathbf{c}_2$ could have in common is

$$(q^2+q+1) + (q^2-q)(q+2) = q^3+2q^2-q+1\,.$$



Hence, the minimum distance is at least

$$q^4+q^2+1-(q^3+2q^2-q+1)=q^4-q^3-q^2+q=q(q-1)(q^2-1)\,.$$

The minimum distance for the associated permutation array is then necessarily

$$\lceil q(q-1)(q^2-1)/(q^2+q+1)\rceil=\left\lceil q^2-2q+\frac{3q}{q^2+q+1}\right\rceil=(q-1)^2\,. \qquad \square$$

The known results on permutation arrays do not seem to provide much insight on a maximum size for a permutation array $\mathsf{PA}(q^2-q+1,(q-1)^2)$. We could certainly use cyclic shifts of the alphabet to obtain at least q^2-q+1 elements in our permutation array. These shifts give us at least a naive lower bound.

Corollary 3.2. *We have*

$$A\left(\left[(q^2+q+1)^{q^2-q+1}\right],q(q-1)(q^2-1)\right) \geq \frac{1}{3}q^6(q^2-1)(q^4-1)(q^2-q+1)\approx\frac{1}{3}q^{14}\,.$$

If the parameters of the code above satisfy the conditions of Corollary 1.4 then the bound attained is considerably improved.

Corollary 3.3. *Assume there exists a prime power α with $(q-1)^2<\alpha<q^2-q+1$. Then*

$$A\left(\left[(q^2+q+1)^{q^2-q+1}\right],q(q-1)(q^2-1)\right) \geq \frac{1}{3}q^6(q^2-1)(q^4-1)\cdot(\alpha^3-\alpha)\approx\frac{1}{3}q^{18}\,.$$

The above construction for CCCs from Baer subplanes can naturally be generalized to Baer subgeometries of $\mathsf{PG}(n,q^2)$ when n is even. A divisibility condition shows that n must be even in order for a Baer subgeometry partition to exist. We first look at the problem of determining the maximum number of points that two Baer subgeometries of $\mathsf{PG}(n,q^2)$ could have in common. We recall two theorems of [13].

Theorem 3.4 ([13, Theorem 1.3])**.** *Let $A_1,A_2,\ldots,A_k$ be subspaces of order q in $\mathsf{PG}(n,q^2)$. The following two statements are equivalent:*

1. *The subspaces $A_1,A_2,\ldots,A_k$ satisfy the following two conditions:*
   - $k\leq q+1$;

- $\langle A_1, A_2, \ldots, A_{i-1}, A_{i+1}, \ldots, A_k \rangle \cap A_i = \emptyset$ *for all* $i = 1, 2, \ldots, k$.

2. *There are Baer subgeometries* B *and* B' *in* $\mathsf{PG}(n, q^2)$ *such that* $A_1, A_2, \ldots, A_k$ *are the components of* $B \cap B'$.

Theorem 3.5 ([13, Theorem 1.4]). *There are at most* $q + 1$ *components in the intersection of two Baer subgeometries of* $\mathsf{PG}(n, q^2)$*, and they are independent.*

We claim that the above theorems imply a result on the maximum number of points that two Baer subgeometries could have in common.

Theorem 3.6. *Let* B *and* B' *be two Baer subgeometries of* $\mathsf{PG}(n, q^2)$*. Then the intersection* $B \cap B'$ *contains at most* $q^{n-1} + q^{n-2} + \cdots + q^2 + q + 2$ *points.*

Proof. We first claim that the only possible way for the intersection to contain at least q^{n-1} points is for the intersection to contain a Baer hyperplane (a copy of $\mathsf{PG}(n-1, q)$). Since Theorem 3.5 says that the intersection contains at most $q + 1$ components, the only way to accumulate q^{n-1} points is for at least one component to be a Baer hyperplane, or for roughly q components to be isomorphic copies of $\mathsf{PG}(n-2, q)$. But the latter case is impossible since the existence of two $\mathsf{PG}(n-2, q)$s in the intersection would contradict the second bullet in part 1 of Theorem 3.4. Hence, in order to have $|B \cap B'| \geq q^{n-1}$, the intersection of B and B' must contain exactly one hyperplane. This immediately implies that any additional components in the intersection would necessarily be points, and moreover, that there can only be one additional component. Hence, the maximum size of $B \cap B'$ is $q^{n-1} + q^{n-2} + \cdots + q^2 + q + 2$ and consists of a Baer hyperplane and one additional point. □

We now assume that n is even. In this case, the number of points of $\mathsf{PG}(n, q^2)$ factors as

$$\frac{q^{2n+2} - 1}{q^2 - 1} = \left(\frac{q^{n+1} - 1}{q - 1}\right)\left(\frac{q^{n+1} + 1}{q + 1}\right)$$

and one can show that the orbits of the Singer subgroup of order $\frac{q^{n+1}-1}{q-1}$ all form Baer subgeometries. Again using a group theoretic argument, one can show that the number of Singer groups acting on $\mathsf{PG}(n, q^2)$ is exactly equal to $\frac{1}{n} q^{n(n+1)} \Pi_{i=1}^{n} (q^{2i} - 1)$. For each Singer group, we can naturally take the Singer subgroup of order $\frac{q^{n+1}-1}{q-1}$ and use it to create a Baer subgeometry partition of $\mathsf{PG}(n, q^2)$. Hence, each Singer group gives rise to a classical Baer subgeometry partitions of $\mathsf{PG}(n, q^2)$. Let $\mathcal{B}_n$ be the set of all classical Baer subgeometry partitions. It follows that $|\mathcal{B}_n| = \frac{1}{n} q^{n(n+1)} \Pi_{i=1}^{n} (q^{2i} - 1)$.

The construction of a constant composition code from the set of Baer subgeometry partitions follows now just as in the case of spreads once we determine how two distinct Baer subgeometry partitions can intersect.

Theorem 3.7. *Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be two distinct Baer subgeometry partitions of $\mathsf{PG}(n, q^2)$, n even. Then, $\mathcal{P}_1$ and $\mathcal{P}_2$ have at most $\frac{m+1}{q+1}$ Baer subgeometries in common, where m is the size of the maximal subfield of $\mathsf{GF}(q^{n+1})$.*

Proof. We appeal to the well-known relationship between Baer subgeometry partitions of $\mathsf{PG}(n, q^2)$ and spreads of $\mathsf{PG}(2n+1, q)$ for n even. Suppose that $\mathcal{P}_1$ and $\mathcal{P}_2$ intersect in exactly i distinct Baer subgeometries. Furthermore, let $\mathcal{S}_1$ and $\mathcal{S}_2$ be the spreads of $\mathsf{PG}(2n+1, q)$ obtained from $\mathcal{P}_1$ and $\mathcal{P}_2$ via the lifting method described in [11]. It follows that each Baer subgeometry common to $\mathcal{P}_1$ and $\mathcal{P}_2$ will lift to a regulus of $\mathsf{PG}(2n+1, q)$. Hence, the corresponding spreads of $\mathsf{PG}(2n+1, q)$ intersect in $i(q+1)$ distinct n-spaces. But by Theorem 2.6, $\mathcal{S}_1$ and $\mathcal{S}_2$ meet in at most $m+1$ spread elements, where m is the maximum size of a subfield of $\mathsf{GF}(q^{n+1})$. Hence, $i \leq \frac{m+1}{q+1}$. □

We now construct a constant composition code from the classical Baer subgeometry partitions of $\mathsf{PG}(n, q^2)$ in the same fashion as before. Let $\mathcal{C}_{\mathcal{B}_n}$ be the code of length $q^{2n} + q^{2n-2} + \cdots + 1$, each of whose coordinates is labeled with a point of $\mathsf{PG}(n, q^2)$, n even. For each Baer subgeometry partition B in $\mathcal{B}_n$, we define a codeword $\mathbf{c}_B$ as follows. Every Baer subplane of B is arbitrarily assigned a symbol in $\{1, 2, \ldots, \frac{q^{n+1}+1}{q+1}\}$, and coordinates corresponding to points lying in the same subgeometry of B are given that symbol in $\mathbf{c}_B$.

Theorem 3.8. *Let k be the largest proper divisor of $n+1$ and let s denote the maximum size of a* $\mathsf{PA}\left(\frac{q^{n+1}+1}{q+1}, \left\lceil \frac{(q-1)(q^{n+1}-q^k)(q^n-1)}{(q+1)(q^{n+1}-1)} \right\rceil\right)$. *The code $\mathcal{C}_{\mathcal{B}_n}$ is a*

$$\mathsf{CCC}\left(\left[\left(\frac{q^{n+1}-1}{q-1}\right)^{\left(\frac{q^{n+1}+1}{q+1}\right)}\right], d\right)$$

consisting of $\frac{1}{n} q^{n(n+1)} \prod_{i=1}^{n} (q^{2i}-1) \cdot s$ codewords, where $d \geq \frac{(q^{n+1}-q^k)(q^n-1)}{q+1}$.

Proof. The composition of the code $\mathcal{C}_{\mathcal{B}_n}$ follows from the construction. We bound d using the fact that two distinct Baer subgeometry partitions can only intersect in at most one Baer subgeometry. By Theorem 3.6, two distinct Baer subgeometries can intersect in at most $q^{n-1} + q^{n-2} + \cdots + q^2 + q + 2 = \frac{q^n-1}{q-1} + 1$ points.

Now let $\mathbf{c}_1$ and $\mathbf{c}_2$ be two distinct codewords of $\mathcal{C}_{\mathcal{B}_n}$. We wish to bound the maximum number of coordinates these two codewords could have in common. The two corresponding partitions share at most $\frac{q^k+1}{q+1}$ Baer subgeometries (Theorem 3.7) whose coordinates may or may not be labeled the same; additionally,

each of the remaining pairs of commonly labeled Baer subgeometries from the two partitions meet in at most $\frac{q^n-1}{q-1}+1$ points each. Hence, the number of common coordinates between $\mathbf{c}_1$ and $\mathbf{c}_2$ is bounded above by

$$\left(\frac{q^k+1}{q+1}\right)\left(\frac{q^{n+1}-1}{q-1}\right)+\left(\frac{q^{n+1}+1}{q+1}-\frac{q^k+1}{q+1}\right)\left(\frac{q^n-1}{q-1}+1\right).$$

This gives

$$\begin{aligned} d &\leq \frac{q^{2n+2}-1}{q^2-1}-\frac{q^{2n+1}+q^{n+k+1}-q^{n+k}+q^{n+2}-q^{n+1}-q^{k+1}+q^k-1}{q^2-1} \\ &= \frac{(q^{n+1}-q^k)(q^n-1)}{q+1}. \end{aligned}$$

A similar calculation as before gives the parameters for the permutation array. □

Again, bounding the size of a permutation array with the parameters described above seems very difficult. If we again use a naive lower bound of the length $\frac{q^{n+1}+1}{q+1}$, we obtain the following.

Corollary 3.9. *We have*

$$\begin{aligned} A\left(\left[\left(\frac{q^{n+1}-1}{q-1}\right)^{\left(\frac{q^{n+1}+1}{q+1}\right)}\right], \frac{(q^{n+1}-q^k)(q^n-1)}{q+1}\right) \\ \geq \frac{1}{n}\,q^{n(n+1)}\prod_{i=1}^{n}(q^{2i}-1)\left(\frac{q^{n+1}+1}{q+1}\right) \\ \approx \frac{1}{n}\,q^{2n^2+3n}. \end{aligned}$$

If the parameters of the code above satisfy the conditions of Corollary 1.4 then we attain an improved bound.

Corollary 3.10. *Assume there exists a prime power α with*

$$\frac{q^{n+1}+1}{q+1} > \alpha > \left\lceil \frac{(q-1)(q^{n+1}-q^k)(q^n-1)}{(q+1)(q^{n+1}-1)} \right\rceil.$$

Then

$$A\left(\left[\left(\frac{q^{n+1}-1}{q-1}\right)^{\left(\frac{q^{n+1}+1}{q+1}\right)}\right], \frac{(q^{n+1}-q^k)(q^n-1)}{q+1}\right)$$
$$\geq \frac{1}{n}\, q^{n(n+1)} \prod_{i=1}^{n} (q^{2i}-1)\left(\alpha^3-\alpha\right)$$
$$\approx \frac{1}{n}\, q^{2n^2+5n}.$$

4. Codes from other partitions

We overview some other classes of partitions of finite projective spaces, and of objects embedded in finite projective spaces, that could be used in the construction of new classes of constant composition codes.

4.1. Ovoidal fibrations

As discussed above, one way to construct a regular spread uses a subgroup of a Singer group. Let L be the finite field of order q^4, viewed as a 4-dimensional vector space over the field $\mathsf{GF}(q)$. Let α be a primitive element for L. Then, the field elements

$$1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{q^3+q^2+q}$$

represent the distinct projective points in $\mathsf{PG}(3,q)$ and multiplication by α induces a collineation on $\mathsf{PG}(3,q)$. We denote this Singer group by G. So, G is a cyclic group of order q^3+q^2+q+1.

Now let H be the cyclic subgroup of G of order q^2+1. It was shown in [7] that the orbits of this subgroup form ovoids of $\mathsf{PG}(3,q)$ and the partition is known as an *ovoidal fibration*. Here we use the term *ovoid* to refer to a set of q^2+1 points of $\mathsf{PG}(3,q)$, no three collinear. Just as regular spreads could be used to generate CCCs, we can use ovoidal fibrations to generate new CCCs. As before, each partition of $\mathsf{PG}(3,q)$ will naturally give rise to a codeword. In order to bound the minimum distance of the code, we will again need to determine how two such partitions intersect.

Lemma 4.1. *If P_1 and P_2 be two partitions of $\mathsf{PG}(3,q)$ into ovoids as described above using two distinct Singer subgroups. Then, P_1 and P_2 intersect in at most one ovoid.*

Proof. It is known that the partition created by the group H is comprised of elliptic quadrics [7]. Moreover, it can be shown that this partition is in fact a pencil of quadrics as discussed in [2]. By the classification given in [2], there is a unique pencil of quadrics comprised entirely of elliptic quadrics forming a partition of $\mathsf{PG}(3,q)$. But two distinct quadrics uniquely determine a pencil. Hence, given two disjoint elliptic quadrics, there is a unique partition of our desired form through them. This immediately implies that P_1 and P_2 can meet in at most one ovoid. □

Proposition 4.2. *Two elliptic quadrics of* $\mathsf{PG}(3,q)$ *intersect in at most* $2(q+1)$ *points.*

The proof of Proposition 4.2 can be found in [8], but also follows from the classification of pencils of quadrics found in [2]. Since two elliptic quadrics can only intersect in this relatively small number of points, we can bound the minimum distance of the associated codes.

Theorem 4.3. *The code* $\mathcal{C}_{\mathcal{O}}$ *described above is a* $\mathsf{CCC}([(q^2+1)^{q+1}], d)$ *consisting of* $\frac{1}{2}q^4(q-1)(q^3-1)\cdot s$ *codewords, where* $d \geq q^3-2q^2-q$ *and* s *is the maximum size of a* $\mathsf{PA}(q+1,q-2)$.

Proof. By Lemma 4.1, any two ovoidal partitions meet in at most one ovoid. The remaining ovoids meet in at most $2(q+1)$ points each. So, the maximum number of coordinates in common between two corresponding codewords is $(q^2+1)+q[2(q+1)] = 3q^2+2q+1$. Therefore, the minimum number of coordinates where two codewords differ is $q^3+q^2+q+1-(3q^2+2q+1) = q^3-2q^2-q$. Since each partition arises from a subgroup of a Singer group, the number of such partitions is the same as the number of 1-spreads of $\mathsf{PG}(3,q)$. We obtain the parameters for the permutation array by noting that the alphabet has size $q+1$ and that $\left\lceil \frac{q^3-2q^2-q}{q^2+1} \right\rceil = q-2$. □

We can now use Propositions 1.1 and 1.3 to ensure that $M(q+1,q-2) \geq (q+1)q(q-1)$. This gives us a bound on the size of our codes.

Corollary 4.4. *We have*

$$A\big([(q^2+1)^{q+1}], q^3-2q^2-q\big) \geq \frac{1}{2}\,q^5(q-1)(q^2-1)(q^3-1) \approx \frac{1}{2}\,q^{11}\,.$$

4.2. Linear flocks of a quadratic cone

We repeat our construction with linear flocks of a quadratic cone. Let π be a plane sitting in $\Sigma = \mathsf{PG}(3,q)$ and let P be any point outside of π. Let O be an

oval in the plane π and consider the set of points $\mathcal{Q}$ lying on any of the $q+1$ lines joining P to a point of O, a so-called quadratic cone. Clearly $\mathcal{Q}$ contains q^2+q+1 points.

Now, let l be any line disjoint from $\mathcal{Q}$ and consider the set of planes through l. There are $q+1$ such planes and each plane meets the set $\mathcal{Q}$ in either a planar cross section forming another oval, or in the special point P. Hence, by deleting P, any line disjoint from $\mathcal{Q}$ corresponds to a partition of $\mathcal{Q} \setminus P$ into q planar sections, each of size $q+1$. These partitions are known as *linear flocks*.

Lemma 4.5. *Let l_1 and l_2 be two distinct lines disjoint from $\mathcal{Q}$. The flocks corresponding to l_1 and l_2 share at most one oval.*

Proof. Suppose that the flocks corresponding to l_1 and l_2 share two ovals. Let π_1 and π_2 be the two distinct corresponding planes of Σ containing these ovals. Then l_1 and l_2 lie in both π_1 and π_2. But two distinct planes meet in at most one line forcing $l_1 = l_2$, a contradiction. □

We now associate a CCC in the natural way. Define a code $\mathcal{C}_\mathcal{Q}$ of length q^2+q where each coordinate is labeled with a point of $\mathcal{Q} \setminus P$. Each flock of $\mathcal{Q}$ determines a codeword. For any particular codeword, if points lie in a common oval of the flock, they are given the same value in their corresponding coordinates. Our alphabet has size q and each letter of our alphabet will appear in each codeword exactly $q+1$ times.

Theorem 4.6. *For $q > 2$, the code $\mathcal{C}_\mathcal{Q}$ described above is a* CCC$([(q+1)^q], d)$ *consisting of $\left(\frac{q^4-q^3}{2}\right) \cdot s$ codewords, where $d \geq (q-1)^2$ and s is the maximum size of a* PA$(q, q-2)$.

Proof. Simple counting shows the number of lines exterior to the cone $\mathcal{Q}$ to be $\frac{q^4-q^3}{2}$. If two flocks share a common oval, then the corresponding codewords could agree in those corresponding $q+1$ coordinates. The remaining $q-1$ ovals in each flock could share at most two points. Hence, the maximum number of coordinates that two codewords could have in common is $(q+1)+2(q-1) = 3q-1$. Since the code has length q^2+q, the minimum distance is bounded below by $(q^2+q)-(3q-1) = q^2-2q+1 = (q-1)^2$. The distance for our permutation array is $\left\lceil \frac{(q-1)^2}{q+1} \right\rceil$. When $q > 2$, this expression simplifies to exactly $q-2$. □

Using Propositions 1.1 and 1.2, we know that a permutation array PA$(q, q-2)$ contains at least $q(q-1)$ elements. This bounds the size of our codes generated by linear flocks.

Corollary 4.7. $A([(q+1)^q],(q-1)^2) \geq q(q-1)\left(\frac{q^4-q^3}{2}\right) \approx \frac{1}{2}\,q^6$.

It should be noted that the parameters for our code obtained from linear flocks of a quadratic cone compare quite favorably to other known codes. For instance, in [4] a CCC$([q^q], q^2-q)$ is obtained using the structure of finite fields and it is shown that the code contains at least q^3-q codewords. Our code above has a very similar composition, but with many more codewords asymptotically.

Let $\mathcal{Q}$ be as above with vertex P. Consider a plane π meeting $\mathcal{Q}$ precisely in P and let ℓ_1 and ℓ_2 be lines of π not meeting P. If $\mathcal{F}_1$ and $\mathcal{F}_2$ are the linear flocks of $\mathcal{Q}$ associated with ℓ_1 and ℓ_2 respectively then $\mathcal{F}_1$ and $\mathcal{F}_2$ do not have a conic in common. Indeed, a conic shared by both $\mathcal{F}_1$ and $\mathcal{F}_2$ would necessarily be coplanar with ℓ_1 and with ℓ_2 contradicting the assumption that π meets $\mathcal{Q}$ precisely in P. Hence, using the construction above yields a code in which two codewords share at most $2q$ coordinates. As π contains precisely q^2 lines external to $\mathcal{Q}$, and $\left\lceil \frac{q(q-1)}{q+1} \right\rceil = q-1$, we obtain the following.

Theorem 4.8. *There exist a* CCC$([(q+1)^q], d)$ *consisting of* $q^2 \cdot s$ *codewords, where* $d \geq q(q-1)$ *and* s *is the maximum size of a* PA$(q, q-1)$.

Applying Proposition 1.2 directly gives us the following.

Corollary 4.9. $A([(q+1)^q], q(q-1)) \geq q^3(q-1) \approx q^4$.

4.3. Planar sections of a hyperbolic quadric

Let $\mathcal{H}$ be a hyperbolic quadric of $\Sigma = \mathrm{PG}(3,q)$. The classic example of a hyperbolic quadric is the set of points whose homogeneous coordinates satisfy the quadratic form $x_0x_1 + x_2x_3 = 0$. It is well known that $\mathcal{H}$ contains $(q+1)^2$ points that are ruled by two families of $q+1$ lines each.

Now let l be any line of Σ disjoint from the fixed hyperbolic quadric $\mathcal{H}$, and let π be any plane through l. Since l is disjoint from $\mathcal{H}$, it follows by dimensions that π must intersect every line that rules $\mathcal{H}$ in a point. In fact, the intersection of $\mathcal{H}$ and the plane π must be a set of $q+1$ points, no three collinear. Other planes of Σ meet $\mathcal{H}$ in ruling lines of $\mathcal{H}$. We will only be interested in the planes that intersect $\mathcal{H}$ in an oval as described above.

Now consider the set of all lines l disjoint from $\mathcal{H}$. We naturally associate with every such line l a partition of $\mathcal{H}$ into $q+1$ ovals. These partitions are known as *linear flocks*. Additionally, we consider the two natural partitions of $\mathcal{H}$ induced by families of ruling lines. We now mimic our construction from the previous section this time applied to the hyperbolic quadric rather than the quadratic cone. Again, the proof of this lemma is the same as that of Lemma 4.5.

Lemma 4.10. *Let l_1 and l_2 be two lines of Σ disjoint from $\mathcal{H}$. Then the partitions of $\mathcal{H}$ corresponding to these lines share at most one conic.*

Now define a CCC $\mathcal{C}_{\mathcal{H}}$ of length $(q+1)^2$ where each coordinate is labeled with a point of $\mathcal{H}$. Each partition of $\mathcal{H}$ determines a codeword. For any particular codeword, if points lie in a common oval of the partition, they are given the same value in their corresponding coordinates. In this setting, our alphabet has size $q+1$, each value appearing $q+1$ times.

Theorem 4.11. *The code $\mathcal{C}_{\mathcal{H}}$ defined above is a* $\mathsf{CCC}([(q+1)^{q+1}], d)$ *containing* $\left(\frac{1}{2}q^2(q-1)^2+2\right)\cdot(q+1)q(q-1)$ *codewords, where* $d \geq q^2-q$. *Hence,* $A\left([(q+1)^{q+1}], q^2-q\right)$ *is asymptotically greater than* $\frac{1}{2}q^7$.

Proof. The size of the code is determined by the number of partitions, or equivalently, the number of lines skew to a hyperbolic quadric. This number can be determined by elementary counting using properties of the hyperbolic quadric and is $\frac{1}{2}q^2(q-1)^2$.

We now determine the bound on d. Two partitions can intersect in at most one conic. This could lead to $q+1$ common coordinates. The remaining conics can pairwise intersect in at most two points. This could determine at most $2q$ additional common values. Since the length of the code is $(q+1)^2$, the minimum distance is at most $(q^2+2q+1)-(3q+1)=q^2-q$. The minimum distance for our permutation array is $\left\lceil \frac{q(q-1)}{q+1} \right\rceil = q-1$. By Proposition 1.3, it follows that the size of our required permutation array $\mathsf{PA}(q+1, q-1)$ is $(q+1)q(q-1)$. This gives us our desired result. □

Again we note that our codes obtained here seem to have quite good parameters. Again comparing to the $\mathsf{CCC}(q^q, q^2-q)$ constructed in [4], our code has a similar composition, but with many more codewords asymptotically.

4.4. Partitions of unitals

Our last construction deals with the classical Hermitian curve in $\mathsf{PG}(2, q^2)$. Any Hermitian curve is equivalent to the set of points (x, y, z) whose homogeneous coordinates satisfy the quadratic form $x^{q+1}+y^{q+1}+z^{q+1}=0$. Let $\mathcal{U}$ be the set of points satisfying this form.

It can be shown that $\mathcal{U}$ contains q^3+1 points and that every line of the plane meets $\mathcal{U}$ in either 1 or $q+1$ points forming an isomorphic copy of $\mathsf{PG}(1, q)$ (a so-called Baer subline). Now let P be any point of the plane outside of $\mathcal{U}$. It can be shown that q^2-q of the lines passing through P meet $\mathcal{U}$ in $q+1$ points each. Interestingly, the remaining $q+1$ lines passing through P meet $\mathcal{U}$ in a

single point each, and these $q+1$ points of $\mathcal{U}$, called the *feet* of P, are collinear. In fact, they form a Baer subline. Moreover (see [10, Chapter 12]), it can be easily shown that two points outside $\mathcal{U}$ can share at most one foot. Therefore, every point P determines a partition of $\mathcal{U}$ into q^2-q+1 disjoint Baer sublines. We can use these partitions to again create a CCC.

Lemma 4.12. *Any two partitions of $\mathcal{U}$ share at most one common Baer subline.*

Proof. The technique here mirrors that of Lemma 4.5. Two disjoint lines of $\mathcal{U}$ intersect in a unique point outside of $\mathcal{U}$. Hence, two distinct points outside of $\mathcal{U}$ cannot generate partitions sharing two distinct sublines. □

Now define a CCC $\mathcal{C}_{\mathcal{U}}$ of length q^3+1 where each coordinate is labeled with a point of $\mathcal{U}$. As before, each partition of $\mathcal{U}$ determines a codeword in the natural way. Our alphabet here has size q^2-q+1 and each value appears $q+1$ times.

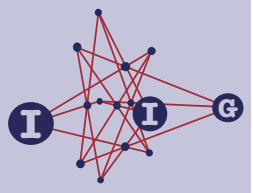
Theorem 4.13. *The code $\mathcal{C}_{\mathcal{U}}$ described above is a* $\mathsf{CCC}([(q+1)^{(q^2-q+1)}], d)$ *with $q^2(q^2-q+1)\cdot s$ codewords, where $d \geq q^3-q^2$ and s is the maximum size of a* $\mathsf{PA}(q^2-q+1, q^2-2q+2)$.

Proof. The length is determined by the number of points outside of $\mathcal{U}$. To bound the minimum distance, we again need to determine how many coordinates could be labeled the same in two distinct codewords. It is straight-forward to show that two distinct partitions share at most one Baer subline, and at most one foot. Therefore, the worst case scenario has two partitions sharing a Baer subline labeled the same, and every other element of the partition sharing one commonly labeled point with an element of the other partition. This gives us a maximum of $(q+1)+(q^2-q) = q^2+1$ commonly labeled coordinates. Hence, the minimum distance is bounded below by q^3-q^2. The parameters of the permutation array follow in the same way as before noting that $\left\lceil \frac{q^2(q-1)}{q+1} \right\rceil = q^2-2q+2$. □

As was the case with the Baer subgeometry partitions, the known results on permutation arrays do not seem to provide much insight on a maximum size for a permutation array $\mathsf{PA}(q^2-q+1, q^2-2q+2)$. Cyclic shifts of the alphabet give us at least a naive lower bound of q^2-q+1.

Corollary 4.14. $A([(q+1)^{(q^2-q+1)}], q^3-q^2) \geq q^2(q^2-q+1)^2 \approx q^6$.

If the parameters of the code above satisfy the conditions of Corollary 1.4 then we attain an improved bound.



Corollary 4.15. *Assume there exists a prime power α with*

$$q^2 - 2q + 2 < \alpha < q^2 - q + 1\,.$$

Then $A([(q+1)^{(q^2-q+1)}], q^3 - q^2) \geq q^2(q^2 - q + 1)\left(\alpha^3 - \alpha\right) \approx q^{10}$.

5. Summary and concluding remarks

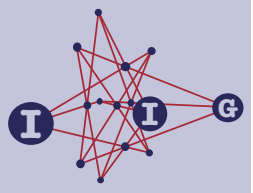
We exhibited many infinite classes of constant composition codes using various partitioning ideas in finite projective spaces. By carefully analyzing the manner in which two such partitions could intersect, we were able to bound the minimum distances of our codes. In some cases, our codes compare favorably to a class of codes constructed using the structure of finite fields.

Naturally, it would be nice to be able to apply the well-known Plotkin bound to our codes. Recall that the Plotkin bound states that a k-ary code of length n and minimum distance d has at most $\frac{d}{d-n+n/k}$ codewords, provided that the denominator is positive. As mentioned in the introduction, our codes yield compositions where each component has a common size. Hence, n/k is an integer and the denominator in the Plotkin bound is integral. Therefore, the Plotkin bound says that, for fixed n and k, the size of the code is bounded by a number which is at most d. By relaxing the condition that $d - n + n/k$ is positive, we are able to find many more codewords. In all of our codes, the minimum distances are asymptotically the same (in q) as the minimum distance required to apply the Plotkin bound. Table 1 provides a summary of our codes. The last column gives the required value of d needed to apply the Plotkin bound to a code with the same n and k as our code. This provides an estimate on the maximum size of a code with the same n and k as our code, but with a minimum distance satisfying $d > n - \lambda$. It seems reasonable to give up the slightly larger minimum distance in order to generate such a large number of codewords.

Acknowledgment. The authors would like to thank Norm Johnson for his guidance regarding the proof of Theorem 2.6.

References

[1] **R. C. Bose**, **J. W. Freeman** and **D. G. Glynn**, On the intersection of two Baer subplanes in a finite projective plane, *Util. Math.* **17** (1980), 65–77.



[2] **A. A. Bruen** and **J. W. P. Hirschfeld**, Intersections in projective space. II. Pencils of quadrics, *European J. Combin.* **9** (1988), 255–270.

[3] **W. Chu**, **C. J. Colbourn** and **P. Dukes**, Constructions for permutation codes in powerline communications, *Des. Codes Cryptogr.* **32** (2004), 51–64.

[4] _____ On constant composition codes, *Discrete Appl. Math.* **154** (2006), 912–929.

[5] **C. J. Colbourn** and **J. H. Dinitz**, editors, *Handbook of combinatorial designs*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, second edition, 2007.

[6] **M. Deza** and **S. A. Vanstone**, Bounds for permutation arrays, *J. Statist. Plann. Inference* **2** (1978), 197–209.

[7] **G. L. Ebert**, Partitioning projective geometries into caps, *Canad. J. Math.* **37** (1985), 1163–1175.

[8] **F .A. B. Edoukou**, Codes defined by forms of degree 2 on quadratic surfaces, preprint.

[9] **R. Fuji-Hara**, **Y. Miao** and **M. Mishima**, Optimal frequency hopping sequences: a combinatorial approach, *IEEE Trans. Inform. Theory* **50** (2004), 2408–2420.

[10] **J. W. P. Hirschfeld**, *Projective Geometries over Finite Fields*, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, second edition, 1998.

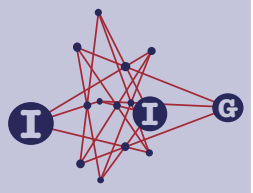
[11] **J. W. P. Hirschfeld** and **J. A. Thas**, *General Galois geometries*, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, Oxford Science Publications, 1991.

[12] **D. R. Hughes** and **F. C. Piper**, *Projective planes*, Graduate Texts in Mathematics **6**, Springer-Verlag, New York, 1973.

[13] **I. Jagos**, **G. Kiss** and **A. Pór**, On the intersection of Baer subgeometries of $\mathrm{PG}(n, q^2)$, *Acta Sci. Math. (Szeged)* **6** (2003), 419–429.

[14] **K. E. Mellinger**, A geometric relationship between equivalent spreads, *Des. Codes Cryptogr.* **30** (2003), 63–71.

[15] **N. Pavlidou**, **A. J. H. Vinck**, **J. Yazdani** and **B. Honary**, Power line communications: state of the art and future trends, *IEEE Comm. Magazine* (2003), 34–40.



[16] **J. Ueberberg**, Projective planes and dihedral groups, Combinatorics (Rome and Montesilvano, 1994), *Discrete Math.* **174** (1997), 337–345.

Tim L. Alderson

Department of Mathematical Sciences, University of New Brunswick Saint John, Saint John, NB, E2L 4L5, Canada

e-mail: tim@unbsj.ca

website: http://people.unb.ca/~tim

Keith E. Mellinger

Department of Mathematics, University of Mary Washington, 1301 College Avenue, Trinkle Hall, Fredericksburg, VA 22401, United States

e-mail: kmelling@umw.edu

website: http://people.umw.edu/~kmelling/

Table 1: Summary of CCCs

Description	Composition	Min. Dist.	Size	Plotkin
Spreads of $\mathsf{PG}(3,q)$	$(q+1)^{q^2+1}$	$\geq q^3-q^2$	$\approx \frac{1}{2}\,q^{14}$	q^3+q^2
Spreads of $\mathsf{PG}(2n-1,q)$	$\left(\frac{q^n-1}{q-1}\right)^{q^n+1}$	$\geq q^{2n-1}-q^{n+k-1}$	$\approx \frac{1}{n}\,q^{4n^2-n}$	$\approx q^{2n-1}$
Baer partitions of $\mathsf{PG}(2,q^2)$	$(q^2+q+1)^{q^2-q+1}$	$\geq q(q-1)(q^2-1)$	$\approx \frac{1}{3}\,q^{14}$	q^4-q
*Baer partitions of $\mathsf{PG}(2,q^2)$	$(q^2+q+1)^{q^2-q+1}$	$\geq q(q-1)(q^2-1)$	$\approx \frac{1}{3}\,q^{18}$	q^4-q
Baer partitions of $\mathsf{PG}(n,q^2)$	$\left(\frac{q^{n+1}-1}{q-1}\right)^{\left(\frac{q^{n+1}+1}{q+1}\right)}$	$\geq \frac{(q^{n+1}-q^k)(q^n-1)}{q+1}$	$\approx \frac{1}{n}\,q^{2n^2+3n}$	$\approx q^{2n+2}$
*Baer partitions of $\mathsf{PG}(n,q^2)$	$\left(\frac{q^{n+1}-1}{q-1}\right)^{\left(\frac{q^{n+1}+1}{q+1}\right)}$	$\geq \frac{(q^{n+1}-q^k)(q^n-1)}{q+1}$	$\approx \frac{1}{n}\,q^{2n^2+5n}$	$\approx q^{2n+2}$
Ovoidal fibration	$(q^2+1)^{q+1}$	$\geq q^3-2q^2-q$	$\approx \frac{1}{2}\,q^{11}$	q^3+q
Linear flocks (1)	$(q+1)^q$	$\geq (q-1)^2$	$\approx \frac{1}{2}\,q^6$	q^2-1
Linear flocks (2)	$(q+1)^q$	$\geq q(q-1)$	$\approx q^4$	q^2-1
Hyperbolic quadric	$(q+1)^{q+1}$	q^2-q	$\approx \frac{1}{2}\,q^7$	q^2+q
Unitals	$(q+1)^{(q^2-q+1)}$	q^3-q^2	$\approx q^6$	q^3-q
*Unitals	$(q+1)^{(q^2-q+1)}$	q^3-q^2	$\approx q^{10}$	q^3-q

* The conditions of Corollary 1.4 are assumed to be met.