q-Steiner Systems and their Automorphisms

by

Emily M. Dempsey

A dissertation submitted to the Graduate Faculty of
Auburn University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Auburn, Alabama
December 16, 2017

Keywords: subspace designs, network codes, 2-analog Steiner systems, finite geometry, hyperplanes, automorphisms

Copyright 2017 by Emily M. Dempsey

Approved by

Kevin Phelps, Chair, Professor of Mathematics
Pete Johnson, Professor of Mathematics
Curt Lindner Professor of Mathematics
Peter Nylen, Professor of Mathematics

Abstract

The q-analog of t-designs and Steiner systems arises canonically from replacing sets of conventional t-designs by vector spaces over $GF(q)$ and their orders with the dimensions. Thomas first introduced these generalizations in 1996 [21] and a few q-analogs of t-designs are known today. Minimal progress was made in constructing a q-Steiner system. In 2013, the first nontrivial q-Steiner system was constructed $S_2[2, 3, 13]$ by Etzion [4] using certain automorphisms groups. This paper focuses on properties of 2-Steiner systems, $S_2[2, 3, n]$, in a general sense. The notion of an embedded 'skew' $S(2, 4, 2^{n-1})$ is introduced and the consequences on existence are discussed. The smallest nontrivial $S_2[2, 3, n]$ that can exist is $n = 7$, and currently, its existence is unknown. Parameters from $S_2[2, 3, n]$ were applied to $S_2[2, 3, 7]$. Curious observations of the relationship between points in a hyperplane and 5-spaces were made leading to the notion of a 'special point'. Automorphisms of 2-Steiner systems, $S_2[2, 3, n]$ and $n = 7$, of odd order are investigated and theoretic proofs of nonexistence is given.

Acknowledgments

First, I would like to thank my adviser, Dr. Kevin T. Phelps, for his patience, direction and support. His office door was always open to me and he would allow me to talk about research as long as I want. I would also like to thank my advisory committee, Dr. Pete Johnson, Dr. Curt Lindner, Dr. Peter Nylen, as well as Dr. James Cross, for their support and contributions. I want to also thank all of my friends, colleagues and professors at Auburn University and in the Auburn University Mathematics Department.

Finally, I would like to thank my parents Mike and Jan for teaching me to love learning from birth. Their encouragement, unwavering love and late night phone calls kept me going. This extends to my grandparents, family and friends for understanding my love of math, passion for students and my desire to pass onto others an inquisitive desire to learn.

Table of Contents

Chapter 1

Introduction

1.1 Designs and Subspace Designs

A t-design with parameters $t-(v,k,\lambda)$ is a pair (V,B), where V is a set of v points and B is a collection of k-subsets of V (usually called blocks) such that every t-subset of V is contained in exactly λ blocks in B. A Steiner system $S(t,k,v)$ is a t-design with $\lambda=1$. A parallel class in a Steiner triple system (S,T) is a set of triples in T that partitions S. An STS (S,T) is resolvable if the triples in T can be partitioned into parallel classes. If STS(v) is one such system, it is also known as a Kirkman triple system of order v and denoted KTS(v). It is easy to see that in any KTS(v), the number of triples in each parallel class is $v/3$ and there are $\frac{v-1}{2}$ parallel classes.

A subspace design, denoted $t-(v,k,\lambda)_q$, is the vector space analog of a t-design with V, a vector space of dimension v over a finite field GF(q) and B a set of k-dimensional subspaces called blocks, such that each t-dimensional subspace of V is contained in exactly λ blocks. The q-analog of a Steiner system denoted by $S_q[t,k,v]$ is called a q-Steiner System.

Both designs and subspace designs can be approached using coding theory or from the perspective of finite projective geometry. The connections between these areas are well presented by Etzion and Storm[8].

1.2 Binary Linear Codes

A binary linear code, C, is just a linear subspace of a vector space $\mathbb{F}_2^n$. The dimension of any linear code is the cardinality of the basis. A basis for C has k words if and only if $|C|=2^k$. A codeword $x\in C$ has length n. The weight of x, denoted $wt(x)$, is number

of non-zero digits in x and the complement of x is defined to be $\bar{x} = x + \mathbf{1}$ where $\mathbf{1} \in \mathbb{F}_2^v$ is the all ones vector. The (Hamming) distance between any two codewords x, y denoted $d(x, y)$ and is the number of coordinate positions the codewords disagree. It is easy to see $d(x, y) = wt(x + y)$. The minimum (Hamming) distance of C, denoted by d, is the smallest distance between any pair of different codewords. The coset of a linear code C determined by u is $C + u = \{v + u | v \in C\}$ where u is any vector in $\mathbb{F}_2^v$. It should be noted that if C has dimension k then there are exactly 2^{v-k} different cosets of C, and each coset has exactly 2^k words.

If C is a linear code over $\mathbb{F}_2^v$ for any two $x, y \in \mathbb{F}_2^v$, the following conditions must be true:

(i) If x is in the coset $C + y$, then $C + x = C + y$,

(ii) If $x + y \in C$, then x and y are in the same coset,

(iii) Every element of $\mathbb{F}_2^v$ is contained in one and only one coset of C. So either $C+x = C+y$ or $\{C + x\} \cap \{C + y\} = \emptyset$.

An important family of perfect, error-correcting, binary linear codes is the Hamming code. Let $\mathcal{H}_n$ denote the Hamming code of length $2^n - 1$, dimension $2^n - n - 1$, and minimum distance 3. The parity check matrix for $\mathcal{H}_n$ can be formed by taking all $2^n - 1$ non-zero binary vectors of length n as columns in some order. If $\alpha \in \mathbb{F}_{2^n}$ is a primitive element, it is convenient to assign the i^{th} column of the parity check matrix to the binary n-vector of $\mathbb{F}_2^n$ corresponding to α^i. The support (or coordinates) of any codeword c is defined as $\text{supp}(c) = \{i | c_i \neq 0\}$. Note this means $c \in \mathcal{H}_n$ if an only if

$$\sum_{i \in \text{supp}(c)} \alpha^i = 0.$$

The support of a codeword in $\mathcal{H}_n$ corresponds to a subset of vectors in $\mathbb{F}_2^n$, and it will be convenient to consider words as subsets.

An example of the parity check matrix of $\mathcal{H}_3$ with the non-zero field elements of $\mathbb{F}_{2^3}$ as columns:

$$M = \begin{array}{c} \begin{matrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \end{array}.$$

The binary word $c = [1101000]$ is length 7 and is a codeword in $\mathcal{H}_3$ since $M \cdot c^T = \mathbf{0}$. The support of c, supp(c)=$\{0, 1, 3\}$, corresponds to the set of field elements $\{\alpha^0, \alpha, \alpha^3\}$ corresponding to the columns of M.

The extended Hamming code, denoted $\mathcal{H}_n^*$, has length 2^n, minimum distance 4. Adding a column of zeros and a row of all ones to the parity check matrix of $\mathcal{H}_n$ forms the parity check matrix for $\mathcal{H}_n^*$. The codewords of weight 3 in $\mathcal{H}_n$ correspond to 2-dimensional subspaces and form a Steiner triple system $S(2, 3, 2^n - 1)$. Similarly, the words of weight 4 in the extended code, $\mathcal{H}_n^*$, form a Steiner quadruple system $S(3, 4, 2^n)$.

A known approach to constructing combinatorial structures is to prescribe a certain group of automorphisms thereby reducing the search space. An introductory overview of this is presented below.

1.3 Automorphisms of t-designs and linear codes

An automorphism of a t-design, (V, B), is a permutation of the points, V, that maps blocks of B to themselves. A t-design, $t - (v, k, \lambda)$, is said to be cyclic if it has an automorphism consisting of a single v-cycle in which case the point set is usually chosen to be $\mathbb{Z}_v$, the integers $\pmod v$, and the automorphism is $\pi : i \to i + 1 \pmod v$. A multiplier automorphism of such a cyclic design is induced by multiplication, i.e. $\sigma : i \to mi \pmod v$ for $m \in \mathbb{Z}_v$, $\gcd(m, v) = 1$.

The automorphism group of a linear code consists of all permutations of the coordinates that map codewords to codewords. A cyclic shift maps a codeword $(c_0, c_1, \ldots, c_{v-1})$ to

$(c_{v-1}, c_0, c_1, \ldots, c_{v-2})$. A code is said to be cyclic if a cyclic shift is an automorphism of the code. The Hamming code, $\mathcal{H}_n$, as defined above is a cyclic code. Multiplication by α, that is $\pi : x \to \alpha x$, $x \in \mathbb{F}_2^n$, induces the cyclic automorphism.

If an element x is fixed by automorphism π then $\pi(x) = x$. The Frobenius automorphism of $\mathbb{F}_2^n$ is $\sigma : x \to x^2$, $x \in \mathbb{F}_2^n$. It too induces an automorphism of the Hamming code. The Galois group is the group of automorphism generated by σ. Define a translation permutation as addition in the field by an element, that is, for $\beta \in \mathbb{F}_2^n$, define $\tau : x \to x + \beta$, $x \in \mathbb{F}_2^n$. Translations induce automorphisms of the extended Hamming code in a similar manner (see [15]). Recall we are identifying codewords with subsets of $\mathbb{F}_2^n$ and thus τ acting on the subsets induces a mapping of the codewords.

1.4 Applications of Subspace Designs

The application of codes over vector spaces in network coding has motivated new research of q-analogs of t-designs. In 2014, the strongest result proving non-trivial $t-(n, k, \lambda)_q$ exist for all t and q provided that $k > 12(t + 1)$ and n is sufficiently large [26]. A q-Steiner system is also a constant dimension code. Constant dimension codes belong to the family of Grassmannian Codes and is considered the most important family of error-correction in random network coding.

A more recent application of constant dimensions codes is used in linear authentication codes introduced by Wang, Xing and Safavi-Naini [24]. In this sense, properties of the subspace code are used to detect tampering with authenticated methods. A new class of unconditionally secure authentication codes called linear authentication codes (or linear A-codes) have been characterized by subspace designs [24].

Chapter 2

Geometry of vector spaces and subspaces

In finite geometry, the projective space over $\mathcal{V}$ in general, denoted $PG(\mathcal{V})$, is defined as the set of all subspaces of $\mathcal{V}$. With that, the points of $PG(\mathcal{V})$ are the 1-dimensional subspaces of $\mathcal{V}$, lines the 2-dimensional subspaces, hyperplanes the $(n-1)$-dimensional subspaces, etc. The Gaussian coefficient, $\begin{bmatrix} n \\ k \end{bmatrix}_q$, known as the q-analog of the binomial coefficients, counts the number of subspaces of dimension k in a vector space of dimension n over $\mathbb{F}_q$ and is defined as follows

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{[n]_q!}{[k]_q![n-k]_q!}, \quad (k \leq n).$$

Let $\mathcal{W}$ be an arbitrary fixed vector space of dimension n over $\mathbb{F}_q$. The projective geometry of order n over $\mathbb{F}_q$, denoted by $\mathcal{P}_q(n)$, is the set of all subspaces of $\mathcal{W}$, including $\{\mathbf{0}\}$ and $\mathcal{W}$ itself. Given a non-negative integer $k \leq n$, the set of all subspaces $\mathcal{W}$ that have dimension k is also known as a Grassmannian, and is usually denoted by $\mathcal{G}_q(n,k)$. Therefore, an equivalent definition, $\mathcal{P}_q(n) = \cup_{0 \leq k \leq n} \mathcal{G}_q(n,k)$. It is known

$$|\mathcal{G}_q(n,k)| = \begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

The following are known but useful parameters involving subspaces.

Lemma 1. *Given X in $\mathcal{G}_q(n,k)$, there are $\begin{bmatrix} k \\ i \end{bmatrix}_q$ ways to choose an i-dimensional subspace Z of X. For a fixed Z, assuming $i \leq j$, the number of subspaces $Y \in \mathcal{G}_q(n,j)$ such that $X \cap Y = Z$ is*

$$\begin{bmatrix} n-k \\ j-i \end{bmatrix}_q q^{(j-i)(k-i)}.$$

Lemma 2. *Let $K(n, j, t, k)$ be the number of ways to choose a subspace of dimension j from a space of dimension n over GF(2) such that it intersects with a given subspace of dimension k at exactly 2^t points:*

$$K(n, j, t, k) = \begin{bmatrix} k \\ t \end{bmatrix} \cdot \frac{\Pi_{i=0}^{j-t-1}(2^n - 2^{k+i})}{\Pi_{i=0}^{j-t-1}(2^j - 2^{t+i})}.$$

Recall from basic geometry the following equation.

The Dimension Intersection Equation. *Given two subspaces U, V elements of $\mathcal{P}_q(n)$,*

$$dim(U + V) = dim(U) + dim(V) - dim(U \cap V).$$

In geometry, a *translate or translated subspace* in coding theory terms, is just a coset of code that corresponds to the same subspace.

Lemma 3. *For a fixed subspace $U \subseteq \mathbb{F}_q^n$ of dimension k there are $2^{n-k} - 1$ translates of U in its complement.*

Proof: Since U has $2^k - 1$ non zero points, there are $2^n - 2^k$ points in the complement of U. From properties of cosets given in Chapter 1, translates of a fixed subspace partition the remaining points and every translate contains 2^k points. Therefore, we must have

$$\frac{2^n - 2^k}{2^k} = 2^{n-k} - 1$$

translates of U in the complement. □

Translates $x + U$ and $y + V$ are parallel if

$$U \subset V \text{ or } V \subset U$$

given any two subspaces $U, V \in \mathcal{P}_q(n)$. In geometry, two lines are said to be skew if they are disjoint but not parallel; that is, one is not a translation of the other. By definition, skew lines cannot be coplanar.

The distance between any two subspaces can be defined as

$$d_S(U,V) = dim(U) + dim(V) - 2dim(U \cap V)$$

is considered as the q-analog of the Hamming metric for binary vectors. The equation defined above is known to be metric, hence both $\mathcal{P}_q(n)$ and $\mathcal{G}_q(n,k)$ can be regarded as metric spaces from which a code can be defined. It is worth noting, a q-Steiner System $S_q[t,k,n]$ is equivalent to a code in $\mathcal{G}_q(n,k)$ with $\begin{bmatrix} n \\ t \end{bmatrix}_q / \begin{bmatrix} k \\ t \end{bmatrix}_q$ codewords and minimum distance $d = 2(k-t+1)$. [9]

2.1 Subcodes, sub-designs and embedded codes

Given linear code C over $\mathbb{F}_q^n$, the set of words in C, all whose coordinates lie where $\mathbb{F}_q^k \subseteq \mathbb{F}_q^n$ is called a subfield subcode of C over $\mathbb{F}_q^k$ [cite book]. Here, we consider 2-Steiner systems $S_2[2,3,n]$ as subcodes of $\mathcal{H}_n$ for the following reasons. Every k-subspace, $b \subset \mathbb{F}_{2^n}$, corresponds to a $2^k - 1$ subset of non-zero elements. Every point in the subset has a binary n-tuple representation in $\mathbb{F}_2^n$. With the parity check matrix for $\mathcal{H}_n$ described as in Chapter 1, it is easy to see that there is a codeword, $c \in \mathcal{H}_n$ such that supp(c)=$\{i|\alpha^i \in b\}$. The converse is not true unless $k = 2$. Let c_b denote the codeword corresponding to the k-subspace b and let $C_b \subset \mathcal{H}_n$ denote the subcode of all codewords x such that supp(x)$\subseteq$ supp (c_b); then C_b is an embedded Hamming code in $\mathbb{F}_q^k$ with length $2^k - 1$.

2.2 Vector space dual and the dual of the Hamming code

Let $\mathcal{V} = \mathbb{F}_q^v$. Two vectors $x, y \in \mathcal{V}$ are said to be orthogonal if $x \cdot y = 0$. The dual of any subspace $K \subseteq \mathcal{V}$, denoted $K^\perp$, is also a subspace and is defined

$$K^\perp = \{u \in \mathcal{V} | a \cdot u = 0 \text{ for all } a \in K\}.$$

Note that the vectors in subspace $K^\perp$ have length v.

Associated with any linear code C is the dual code $C^\perp$. If G is a generator matrix for C, then $C^\perp$ is the solution space to

$$Gx^T = 0.$$

If C is linear, having length n and dimension k then its dual, is also a linear code $C^\perp \subseteq \mathcal{V}$ having dimension $n-k$. Applying this to Hamming codes, since $\mathcal{H}_n$ has length 2^n-1 and dimension 2^n-n-1, the dimension of $\mathcal{H}_n^\perp$ is n. If subspace K is fixed by an automorphism, its dual space $K^\perp$ is also fixed. A non-zero codeword y in $\mathcal{H}_n^\perp$ has weight 2^{n-1} therefore, the complement of y has weight $2^{n-1}-1$ and must also be a codeword. Hence, complements of words y in the dual correspond to hyperplanes in $\mathbb{F}_q^n$. The subcode consisting of all $c \in \mathcal{H}_n$ such that $\mathrm{supp}(c) \subseteq \mathrm{supp}(y)$ is an (embedded) extended Hamming code of length 2^{n-1}. We now have the following well-known fact concerning hyperplanes:

Lemma 4. *If $y+\mathbf{1} \in \mathcal{H}_n$ corresponds to hyperplane Y and $c_b \in \mathcal{H}_n$ corresponds to a k-subspace, then either $supp(c_b) \subseteq supp(y+\mathbf{1})$ or $|supp(c_b) \cap supp(y+\mathbf{1})| = 2^{k-1}-1$ (and $|supp(c_b) \cap supp(y)| = 2^{k-1}$).*

Proof: Let $x \in \mathrm{supp}(c_b) \cap \mathrm{supp}(y)$. For each $i \in \mathrm{supp}(c_b) \cap \mathrm{supp}(y+\mathbf{1})$ there is a codeword $c_{i,x}$ of weight 3 with $\mathrm{supp}(c_{i,x}) = \{i, x, i'\}$. Since $c_{i,x} \cdot y \equiv 0 \pmod 2$, then $i' \in \mathrm{supp}(y)$. Thus

$$|\mathrm{supp}(c_b) \cap \mathrm{supp}(y)| = |\mathrm{supp}(c_b) \cap \mathrm{supp}(y+\mathbf{1})| + 1,$$

and the result follows.

From Lemma 1, we know that any k-dimensional subspace b is contained in $2^{n-k}-1$ hyperplanes and thus there is a corresponding subspace of dimension $n-k$ in $\mathcal{H}_n^\perp$ containing non-zero codewords whose support is disjoint from that of c_b. Similarly, for any $(k-1)$-dimensional subspace, $b' \subset b$, there are 2^{n-k+1} non-zero words in the dual whose support is

disjoint from the support of $c_{b'}$. Hence, there are $2^{n-k+1} - 2^{n-k} = 2^{n-k}$ words in $\mathcal{H}_n^{\perp}$ whose support contains the support of $c_b + c_{b'}$ which has weight 2^{k-1}.

Chapter 3

2-analog $S_2[2,3,n]$

The notion of 2-analog is canonical since it arises by replacing sets of the traditional t-design by vector spaces over $GF(2)$ and their orders by dimensions of vector spaces. These generalizations were first introduced by Thomas [21] in 1996. There, he showed that certain kinds of $S_2[2,3,7]$ could not exist.

3.1 Combinatorial properties

A 2-analog Steiner system $S_2[2,3,n]$ is equivalent to a Steiner 2-design $S(2,7,2^n-1)$ since every pair of nonzero elements in $\mathbb{F}_2^n$ are independent and there are 2^3-1 nonzero elements in every subspace of dimension 3. Using traditional arguments from design theory we have the following condition on n:

Lemma 5. *A necessary condition for an $S_2[2,3,n]$ to exist is that $n \equiv 1$ or $3 \pmod 6$.*

Proof: The necessary conditions for a design $S(2,7,2^n-1)$ are

$$(2^n-1)(2^n-2) \equiv 0 \pmod{7 \cdot 6}$$

from which we conclude that $n \equiv 0,1 \pmod 3$ and

$$2^n - 2 \equiv 0 \pmod 6$$

which means $n-1$ is even. □

From now on we will assume that $n \equiv 1$ or $3 \pmod 6$. We will refer to 2-dimensional subspaces as triples and 3-dimensional subspaces in $S_2[2,3,n]$ as blocks. There are 2^2-1

points in a 2-dimensional subspace and 2^3-1 points in 3-dimensional subspace and therefore points in any block. A block is said to cover a triple if the elements in the triple are a subset of elements in the block. There are 2^3-1 points in blocks of $S_2[2,3,n]$ forming seven triples which is a triple system isomorphic STS(7).

An alternative definition of subspace designs given in [9] is as follows, a subspace design $S_2[t,k,n]$ is an (n,M,d,k) code in $\mathcal{G}_q(n,k)$ with $d=2(k-t+1)$.

3.2 $S_2[2,3,13]$ example

In 2013, Etzion et. al. produced the first example of a q-Steiner System. A $S_2[2,3,13]$ was found by prescribing the normalizer of a Singer subgroup of GL(13,2) as a group of automorphisms of the base blocks corresponding to columns of the 15 subspaces of $\mathbb{F}_2^{13}$. Equivalently, these are base blocks of a cyclic design mod $2^{13}-1$ having 2 as a multiplier automorphism.

$\{0,2181,2519,3696,6673,6965\}$, $\{0,13,4821,5178,7823,8052,8110\}$,
$\{0,21,2900,4226,4915,6087,8008\}$, $\{0,27,1190,3572,4989,5199,6710\}$,
$\{0,119,490,5941,6670,6812,7312\}$, $\{0,1,1249,5040,7258,7978,8105\}$,
$\{0,9,1144,1945,6771,7714,8102\}$, $\{0,17,291,1199,5132,6266,8057\}$,
$\{0,30,141,682,2024,6256,6406\}$, $\{0,37,258,2093,4703,5396,6469\}$,
$\{0,7,1857,6681,7259,7381,7908\}$, $\{0,11,209,1941,2926,3565,6579\}$,
$\{0,20,1075,3939,3996,4776,7313\}$, $\{0,31,814,1161,1243,4434,6254\}$,
$\{0,115,949,1272,1580,4539,4873\}$

3.3 Connections to Steiner Systems $S(2,4,2^{n-1})$

From Chapter 2, we know each hyperplane of $\mathbb{F}_2^n$ corresponds to an embedded Hamming subcode $\mathcal{H}_{n-1}\subset\mathcal{H}_n$ and the complement of a hyperplane (corresponding to a word in the dual) contains an embedded extended Hamming code as a subcode of length 2^{n-1}.

Let B be the collection of 3-subspaces or blocks of a $S_2[2,3,n]$ and let $\alpha \in \mathbb{F}_{2^n}$ be a primitive element. For each y in the dual of $\mathcal{H}_n$ define a pair (V_y, Q_y) where $V_y = \{\alpha^i | i \in \text{supp}(y)\}$ and $Q_y = \{V_y \cap b | b \in B\}$.

Lemma 6. *The design (V_y, Q_y) defined above is a $S(2,4,2^{n-1})$ and is a sub-design of the embedded $S(3,4,2^{n-1})$.*

Proof: For every pair $i,j \in \text{supp}(y)$ there is a unique block $b \in B$ with $\alpha^i, \alpha^j \in b$ thus (V_y, Q_y) is a 2-design. Since the intersection of subspaces is a subspace the blocks intersect the hyperplane in 3 or 7 points and thus intersects V_y in 0 or 4 points. The 4 points form a word in the code and thus a block of the $S(3,4,2^{n-1})$. □

Consider the design (V_y, Q_y) defined above. If $\{\alpha^i, \alpha^j, \alpha^k, \alpha^u\} \in Q_y$ then $\alpha^i + \alpha^j + \alpha^k + \alpha^u = 0$. The block $b \in B$ with $b \cap V_y = \{\alpha^i, \alpha^j, \alpha^k, \alpha^u\}$ is spanned by $\alpha^i, \alpha^j, \alpha^k$ and the subspace b' with $b' \cap V_y = \{\alpha^i + \beta, \alpha^j + \beta, \alpha^k + \beta, \alpha^u + \beta\}$ is spanned by $\alpha^i + \beta, \alpha^j + \beta, \alpha^k + \beta$. These subspaces have at least 2 elements in common: $\alpha^i + \alpha^j$ and $\alpha^i + \alpha^k$ and thus $b' \notin B$. In other words, the automorphism τ of the extended Hamming subcode on supp(y) corresponding to the translation of any β applied to the blocks of Q_y must give a disjoint set.

In geometry, two lines are said to be skew if they are disjoint but not parallel; that is, one is not a translation of the other. The words of weight 4 of the extended Hamming code of length 2^{n-1} can be thought of as planes in the affine geometry over $\mathbb{F}_2^{n-1}$. Define a skew $S(2,4,2^{n-1})$ then as a collection of "planes" in the extended Hamming code, no two of which are parallel (i.e. translates of one another). Therefore, the $S(2,4,2^{n-1})$, (V_y, Q_y) must be "anti-translation" or "skew".

3.4 Implications of 'Skewness'

The existence of $S_2[2,3,13]$ means that there exist skew $S(2,4,2^{12})$ in the $S(3,4,2^{12})$ contained in the extended Hamming code. It is open whether the converse is true in general;

Does the existence of an skew $S(2,4,2^{n-1})$ in the extended Hamming code of length 2^{n-1} imply the existence of an $S_2[2,3,n]$?

The words of weight 4 in the extended Hamming code of length 2^{n-1} will always contain a subset of codewords corresponding to a $S(2,4,2^{n-1})$ when $n-1$ is even; just pick an appropriate translate of an extended Preparata code (see [2],[12],[25],[15]). However, such $S(2,4,2^{n-1})$ are never "skew". In fact, they always contain translations as we show in Chapter 5. Using known Design Theory, arguments we have the following Lemmas.

3.5 Allocation of blocks in $S_2[2,3,n]$

Lemma 7. *A 4-dimensional subspace has at most one block of $S_2[2,3,n]$ contained in it.*

Proof: From the Grassmannian, we know there are seven 3-dimensional subspaces in any 4-subspace. By the dimension intersection equation, any two intersect in a triple since $3+3-4=2$. Therefore, at most one of the seven 3-spaces in a 4-space can be a block in the design. □

Consider the blocks of a skew $S(2,4,2^{n-1})$ over points in $\mathbb{F}_{2^{n-1}}$. For each $a \in \mathbb{F}_{2^{n-1}}$ the pairs $\{x, x+a\}$ must be covered by a block of the form $\{x, x+a, y, y+a\}$. There are 2^{n-2} of these pairs and thus the design must have 2^{n-3} such blocks. Moreover, the blocks must be disjoint and therefore must form a skew parallel class. The associated triples are of the form $\{a, x+y, x+y+a\}$ and there must be 2^{n-3} such triples for each nonzero $a \in F_{2^{n-1}}$.

Lemma 8. *Given an $S_2[2,3,n]$, every hyperplane must contain*

$$\frac{(2^{n-1}-1)(2^{n-3}-1)}{3(2^3-1)}$$

blocks and each point of the hyperplane is in exactly $\frac{2^{n-3}-1}{3}$ of those blocks.

Proof: Given y in the dual code and the complementary hyperplane on $y+\mathbf{1}$, the blocks in B corresponding to the skew $S(2,4,2^{n-1})$ design, (V_y, Q_y), cover $2^{n-3}(2^{n-1}-1)/3$ triples

in the complementary hyperplane on $y + \mathbf{1}$. The remaining $(2^{n-1} - 1)(2^{n-3} - 1)/3$ triples must be covered by blocks in the hyperplane giving

$$\frac{(2^{n-1} - 1)(2^{n-3} - 1)}{3(2^3 - 1)}$$

subsystems. There are at most 2^{n-3} blocks through a point which intersect the hyperplane in a triple since there are at most that many disjoint 4-tuples in the skew $S(2, 4, 2^{n-1})$. Thus each point is in at least $\frac{2^{n-3}-1}{3}$ blocks but each block is counted seven times and therefore at least

$$\frac{(2^{n-1} - 1) \cdot (2^{n-3} - 1)}{3 \cdot 7}$$

blocks. □

Lemma 9. *Let (V, Q) denote the points and blocks of an $S(3, 4, 2^m)$ and let $(V_0, Q_0), (V_1, Q_1)$ with $V = V_0 \cup V_1$ be two disjoint sub $S(3, 4, 2^{m-1})$ systems. Let (V, D) , $D \subset Q$ be a sub $S(2, 4, 2^m)$ then $|D \cap Q_0| = 2^{m-2}(2^{m-2} - 1)/6 = |D \cap Q_1|$.*

Proof: Since (V_0, Q_0) is a $S(3, 4, 2^{m-1})$ for any block $b \in D$ either $|b \cap V_0| = 4$ or $|b \cap V_0| = 2$. Let $y = |D \cap Q_0|$ and z denote the number of blocks in D intersecting V_0 in 2 points then $4z = 2^{m-1} \cdot 2^{m-1}$ and $6y + z = 2^{m-1}(2^{m-1} - 1)/2$ the result follows. □

Corollary 1. *For any two words x, y in the dual of the Hamming code, given $S(2, 4, 2^{n-1})$ subdesigns (V_x, Q_x), (V_y, Q_y), then if $V' = V_x \cap V_y$ and $Q' = Q_x \cap Q_y$,*

$$|Q'| = \frac{2^{n-3}(2^{n-3} - 1)}{6}$$

Note that if $x, y \in \mathcal{H}_n^\perp$ then $x + y \in \mathcal{H}_n^\perp$ and the corresponding hyperplanes intersect in an $n - 2$ dimensional subspace. Blocks of an $S_2[2, 3, n]$ that intersect $V' = V_x \cap V_y$ in 2 points must have one point in the subspace and 2 points in $V_x \cap V_{x+y}$ and $V_{x+y} \cap V_y$ as well.

Corollary 2. *Given an $S_2[2,3,n]$ then every n-2 dimensional subspace must contain*

$$\frac{(2^{n-3}-1)(2^{n-3}-2)}{7\cdot 6}$$

blocks.

Proof: Blocks of an $S_2[2,3,n]$ that intersect $V' = V_x \cap V_y$, $V_x \cap V_{x+y}$ or $V_{x+y} \cap V_y$ in four points cover a total of $3(2^{n-3}(2^{n-3}-1)/6)$ triples of the subspace corresponding to the intersection of the complementary 3 hyperplanes. The remaining triples must be covered by blocks. □

3.6 $S_2[2,3,7]$

From Corollary 2, we have that in a $S_2[2,3,7]$, every 5-dimensional subspace must contain 5 blocks. We also have from Lemma 8 any point in a 6-dimensional subspace is in exactly 5 blocks contained in that subspace; we believe this is no coincidence. These constraints combined with known subspace properties, 5-dimensional subspaces have become especially significant to study as well as the arrangement of the blocks contained in these subspaces.

Let $p \in \mathbb{F}_{2^7}$ be a non-zero point, define p to be a *special*-point in $S_2[2,3,7]$ if for any hyperplane containing p, the 5 blocks incident with it that are contained in the hyperplane span a 5-dimensional subspace.

3.6.1 5-dimensional subspaces in $\mathbb{F}_2^7$

Let $S \subset \mathbb{F}_2^7$ is a 5-dimensional subspace, by Corollary 2 there must be 5 blocks contained on the 31 non-zero points of S. With d_i the degree of the point $i \in S$, we have the equation

$$\sum_{i \in S} d_i = 35.$$

Any two blocks in S must intersect in a point since the dimension of the intersection is $3 + 3 - 5 = 1$ giving

$$\sum_{i \in S} \binom{d_i}{2} = 10.$$

If $d_i \geq 1$ for all i in S then the solution is unique and the 5 blocks in S must intersect in a point. Hence, if no 5-space exists containing a point of degree 0, every point must be a *special*-point. Since there are 63 5-subspaces in any hyperplane, it is feasible for every point in a given hyperplane to be special.

3.6.2 Derived geometric spreads

Lemma 10. *Triples from the intersection of the blocks in $S_2[2, 3, 7]$ through point a and hyperplane V where $a \notin V$ induce a spread in V.*

Proof: Given hyperplane V, any block not contained must intersect V it in a triple since $3 + 6 - 7 = 2$. By properties of the design, triples are disjoint and therefore must partition the points in V creating a parallel class or spread in V. □

In geometry, a spread is said to be regular (or geometric) if for any three triples A, B, C in the spread the 4-subspace generated by A, B either contains C or C is disjoint from that subspace. Any two blocks intersecting in a generate a 5-subspace which then must intersect hyperplane V disjoint with a in a 4-subspace. If point a is special, then the induced spread is regular. Conversely, if the spread in V induced by a is regular, it follows that the 5 blocks contained in the 5-space generated must all be incident to a.

Chapter 4

Automorphisms of $S_2[2, 3, n]$

Recently a large number of cyclic $S_2[2, 3, 13]$ were constructed [4] which in addition had the Frobenius automorphism. Prior to this, the problem had been studied by a number of authors without much success (e.g.[20],[21],[14],[10]). In 2008, Kohneri and Kurtz established the non-existence of $S_2[2, 3, 7]$ with a cyclic automorphism In addition, [4] established non-existence of $S_2[2, 3, 7]$ having the Galois group of order 7 as automorphisms. Similarly, the non-existence of $S_2[2, 3, 9]$ with a cyclic automorphism was established by Etzion[11] and independently by the authors. It was conjectured [4] that (cyclic) $S_2[2, 3, p]$, exist, for p a prime, $p > 7$, $p \equiv 1 \pmod 6$. It is well known, an automorphism of the Hamming code (or equivalently projective space) has $2^k - 1$ fixed points ($k \geq 0$) and has an embedded Hamming subcode on the set of fixed points[19],[7]. Similarly, an automorphism of an $S_2[2, 3, n]$ of odd order has an $S_2[2, 3, k]$ sub-design on the set of fixed points. A proof of this and other automorphisms properties is presented below.

4.1 Automorphisms of odd order

Theorem 1. *An automorphism of odd order of an $S_2[2, 3, n]$ has $2^k - 1$ fixed points, $k \geq 0$, and has a $S_2[2, 3, k]$ embedded sub-design on the set of fixed points.*

Proof: The triples on the set of fixed points are fixed pointwise therefore any block containing such triple must be fixed set-wise. In a block covering a triple of fixed points, the four remaining points must be mapped to themselves. This can only happen under an even order automorphism or the identity. Thus the block is contained in the set of fixed points. □

Corollary 3. *A block in $S_2[2,3,7]$ with an automorphism of odd order has $0, 1$ or 7 fixed points.*

Specifically, lets consider automorphisms of order 3.

Lemma 11. *Any automorphism of order 3 of an $S_2[2,3,n]$ with 2^s-1 fixed points must have $2^s - 1 \leq (2^{n-s}-1)/3$ if $(2^{n-s}-1)/3$ is not divisible by 3.*

Proof: As noted earlier, an automorphism of odd order of an $S_2[2,3,n]$ must have 2^s-1 fixed points and have an $S_2[2,3,s]$ on the set of fixed points. The remaining 2^n-2^s points fall into orbits. The orbits $\{x,y,z\}$ of an automorphism of order 3 are either triples or generate a 3-subspace. In either case $\gamma = x+y+z$ must be fixed. Any block fixed set-wise by the automorphism but not in $S_2[2,3,s]$ must contain a triple which is an orbit. Conversely, if the orbit $\{x,y,z\}$ is a triple and $f \neq 0$ is a fixed point then $\{x+f, y+f, z+f\}$ is also an orbit which generates a fixed 3-subspace. If there are 2^s-1 fixed points there would be $2^s(2^{n-s}-1)/3$ orbits. If x of these are triples then there must be $(2^s-1)x$ orbits which are not; thus

$$(2^s-1)x = 2^s(2^{n-s}-1)/3 - x$$

or $x = (2^{n-s}-1)/3$ orbits that generate a 3-space (and thus exactly that many set-wise fixed blocks). Each fixed point is in $(2^{s-1}-1)/3$ fixed blocks of the sub $S_2[2,3,s]$. The remaining $2^{s-1}(2^{n-s}-1)/3$ blocks through that point have orbits of size 1 or 3. If $(2^{n-s}-1)/3$ is not divisible by 3 there must be orbits of size 1 and thus $2^s - 1 \leq (2^{n-s}-1)/3$. □

Corollary 4. *Any automorphism of order 3 of an $S_2[2,3,7]$ must have one fixed point.*

Proof: From Corollary 3, the number of fixed points of an automorphism of an $S_2[2,3,7]$ must be 0, 1 or 7. The orbits $\{x,y,z\}$ of an automorphism of order 3 are either triples or generate a 3-subspace. In either case $f = x+y+z$ must be fixed. Any block fixed set-wise by the automorphism must contain a triple which is an orbit. Conversely if the orbit $\{x,y,z\}$ is a triple and $f \neq 0$ is a fixed point then $\{x+f, y+f, z+f\}$ is also an orbit which generates a

fixed 3-subspace. If there are 7 fixed points it must be a block. In this case there would be 40 orbits. If x of these are triples then there must be $7x$ orbits which are not; thus $7x = 40 - x$ or $x = 5$.

Each fixed point would be in 21 blocks which have to fall into orbits of length 1 or 3. Thus each fixed point would have to be in at least 3 fixed blocks which is impossible with only 5 fixed triples. □

It is known, a 3-dimensional subspace in $\mathbb{F}_2^7$ has 2^4 cosets which are isomorphic to $\mathbb{F}_2^4$. The triples through any non-zero point of the corresponding block must have two points in a coset and thus blocks through this point must intersect in a triple of cosets in two points each. For this reason, we consider $\mathbb{F}_2^7$ as $\mathbb{F}_2^3 \times \mathbb{F}_2^4$.

Let α denote the primitive element in $\mathbb{F}_{2^3}$ and β be the primitive element in $\mathbb{F}_{2^4}$. We can assume that $\mathbf{b_0} = \{(\alpha^i, 0) : i = 0, \ldots 6\}$ is a block of the $S_2[2, 3, 7]$. Note the dual of $\mathbf{b_0}$ is $\{0\} \times \mathbb{F}_2^4$.

Each triple T of $\mathbb{F}_{2^3}$ corresponds to a hyperplane $T \times \mathbb{F}_{2^4}$. The three triples in $\mathbb{F}_{2^3}$ intersecting any non-zero point α^i correspond to three hyperplanes in $\mathbb{F}_{2^7}$ intersecting in a 5-dimensional subspace $\{0, \alpha^i\} \times \mathbb{F}_{2^4}$.

Lemma 12. *Any automorphism of odd order mapping* $\mathbf{b_0}$ *to itself induces an automorphism of a Kirkman triple system on* $\{0\} \times \mathbb{F}_{16}$ *assuming the points of* $\mathbf{b_0}$ *are special.*

Proof: Any automorphism fixing $\mathbf{b_0}$ must also fix $\mathbf{b_0^\perp}$ set-wise. The 4-dimensional subspace $\mathbf{b_0^\perp}$ cannot contain a block since any two 3-dimensional subspaces contained in a 4-dimensional subspace must intersect in a triple and there are no fixed points in $\mathbf{b_0^\perp}$. Therefore the triples of $\mathbf{b_0^\perp}$ must be covered by blocks of $\{0, \alpha^i\} \times \mathbb{F}_2^4$. For any $i \in \{0, 1, \ldots 6\}$, the $\{0, \alpha^i\} \times \mathbb{F}_2^4$ is a 5-dimensional subspace containing 5 blocks. If these blocks intersect $\mathbf{b_0}$ in a point, then the intersection with $\mathbf{b_0^\perp}$ must be a Kirkman Triple System of order 15. □

There are two non-isomorphic Kirkman triple systems on the triples of $\mathbb{F}_2^4$ (see [16]) each having an automorphism group of order 168. In both cases, the automorphisms of order

three have 3 fixed points implying the automorphism of the $S_2[2,3,7]$ would have to have 7 fixed points which, as we shall see, cannot happen.

Thus, an automorphism of order 3 must have the 21 blocks fixed set-wise, each containing a fixed triple.

The following theorem was recently established computationally using computer search. Using the job scheduling system *Torque* of the Linux cluster of the University of Bayreuth the estimated run time was 27 600 000 CPU-days. This result however, is a simple conclusion from the theoretical approach discussed here.

Theorem 2. [13] *An $S_2[2,3,7]$, if it exists, cannot have an automorphism of order 3.*

Clearly, from the above arguments if an automorphism of the $S_2[2,3,7]$ fixes a block it induces an automorphism of a Kirkman triple system and thus the order must divide 168. With automorphisms of order 7 and 3 ruled out, this means only involutions (i.e. of order 2) could be an automorphism. The Hamming code has involutions (see [7]) so that would be a suitable direction for further research.

Chapter 5

Preparata codes

For background on extended General Preparata codes and their translates see [2],[12],or [15]. To make the paper self-contained we present a version of the construction of these codes and review some of the pertinent established properties.

Let $\sigma = 2^k$ and assume $\gcd(2^{2k} - 1, 2^r - 1) = 1$. Let α be a primitive element in $\mathbb{F}_2^r$. Define

$$H = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha & \dots & \alpha^{2^r-2} & 0 \\ 1 & \alpha^{\sigma+1} & \dots & (\alpha^{\sigma+1})^{2^r-2} & 0 \end{pmatrix}$$

Let the syndromes for $u, v \in \mathbb{F}_2^{2^r}$ be

$$uH^T = (s_0, s_1, s_{\sigma+1}),\ vH^T = (s_0^*, s_1^*, s_{\sigma+1}^*).$$

Then define $P(r, \sigma)$ as follows:

Definition 1 (General (extended) Preparata Code)**.** *For $r \geq 3$, r odd, then for $u, v \in \mathbb{F}_2^{2^r}$, $(u, v) \in P(r, \sigma)$ if and only if*

- $s_0 = s_0^* = 0$
- $s_1 = s_1^*$
- $s_{\sigma+1} + s_1^{\sigma+1} = s_{\sigma+1}^*$

The kernel of a (non-linear) code C is the subspace of all x such that $C = C + x$. The code C is the union of cosets of the kernel as is any translate of the code. We have then,

Lemma 13. *The kernel K of $P(r,\sigma)$ consists of all words (u,v) such that $s_1 = s_1^* = 0$.*

The kernel of the extended General Preparata code is invariant under translation. Moreover the extended General Preparata codes are subcodes of the extended Hamming code. The words of weight 4 in certain translates of the extended General Preparata are known to be $S(2,4,2^{r+1})$ designs. To prove these designs are not skew we just need to show that the coset of the kernel contains translates.

If we identify words in the extended Hamming code with subsets of $\mathbb{F}_2^r \times \{0,1\}$ then we can also identify words with pairs of subsets of $\mathbb{F}_2^r$.If we identify $u, v \in F_2^{2^r}$ with subsets $U, V \subseteq \mathbb{F}_2^r$ then a translate maps (U,V) to $(U+\alpha^i, V+\alpha^i)$, for $\alpha^i \in \mathbb{F}_2^r$ and induces a corresponding permutation on the words u, v.

Theorem 3. *A coset of the kernel of a extended general Preparata code contains translates.*

Proof: Let $K + x$ be a coset of the kernel, K, where x has weight 4 and x is in the extended Hamming code. Then x corresponds to either $(\{\alpha^i, \alpha^j, \alpha^i+\beta, \alpha^j+\beta\}, 0)$ or $(\{\alpha^i, \alpha^j\}, \{\alpha^i+\beta, \alpha^j+\beta\})$ for some $\beta \in \mathbb{F}_2^{2^r}$. But there is a codeword (u,u) in the kernel with corresponding subset (U,U) with $U = \{\alpha^i, \alpha^j, \alpha^i+\beta, \alpha^j+\beta\}$. In either case $x + (u,u)$ is a translate of x. □

Until [4] the only known examples of embedded $S(2,4,2^{r+1})$ in the extended Hamming code came from extended Preparata codes.

5.1 Normal Bases and Galois groups

We believe the conjecture that $S_2[2,3,p]$ exist when $p > 7$ is a prime [4] and presumably being cyclic and having Galois group as well as automorphisms, should be modified. To explain, we need to introduce normal bases.

A normal basis N of the field $\mathbb{F}_2^n$ over $\mathbb{F}_2$ is a basis of the form $N = \{\alpha, \alpha^2, \alpha^{2^2}, \ldots, \alpha^{2^{n-1}}\}$ for some $\alpha \in \mathbb{F}_2^n$. Let $\sigma(x) = x^2$ be the Frobenius automorphism then a normal basis is an orbit under σ. Of course, not every orbit of σ is a basis. An element $\alpha \in \mathbb{F}_2^n$ is said to

be a normal element or is said to generate a normal basis if its orbit under σ is a basis. Normal bases are of interest in cryptography and coding theory especially with respect to implementation of finite field arithmetic[3].

Define the trace of $\alpha \in \mathbb{F}_2^n$ as

$$Tr(\alpha) = \sum_{i=0}^{n-1} \sigma^i(\alpha) = \sum_{i=0}^{n-1} \alpha^{2^i}$$

Theorem 4. [1], [22] *The number of normal elements in $\mathbb{F}_2^n$ for n odd is*

$$v(n,2) = \prod_{d|n} (2^{\tau(d)} - 1)^{\phi(d)/\tau(d)}$$

where $\tau(d)$ is the order of 2 $\pmod d$ and $\phi(d)$ is Euler's totient function.

Obviously, we have the following.

Corollary 5. *For an odd prime p having 2 as a primitive element $\pmod p$, $\beta \in \mathbb{F}_{2^p}$, $\beta \neq 1$, β is normal if and only if $Tr(\beta) = 1$.*

Consider a (cyclic) $S_2[2,3,p]$, p a prime, having the Galois group of $\mathbb{F}_{2^p}$ as automorphisms. The Frobenius automorphism fixes a point and a hyperplane corresponding to elements β having $Tr(\beta) = 0$. The complement is a word y in the dual of the Hamming code, with $\text{supp}(y) = \{i | Tr(\alpha^i) = 1\}$. When 2 is a primitive element $\pmod p$, Then the orbits of length p in y are all normal basises and thus uniform.

Example Consider the field $\mathbb{F}_8$ and $y \in H_7$, $\text{supp}(y) = \{i | Tr(\alpha^i) = 1\}$. In this case the order of 2 is $\tau(7) = 3$ and $\phi(7) = 6$ thus there are 7^2 normal elements or 7 normal basis. Then $\text{supp}(y)$ consists of 9 orbits of length 7 under σ^* 7 of which correspond to normal basis.

∎

Example Consider the field $\mathbb{F}_2^{13}$ and $y \in H_{13}$, $\text{supp}(y) = \{i | Tr(\alpha^i) = 1\}$. In this case the order of 2 is $\tau(13) = 12$ and $\phi(13) = 12$ thus there are $2^{12} - 1$ normal elements or 315 normal

basis. Then supp(y) consists of 315 orbits of length 13 under σ^* all of which correspond to normal basis. ∎

If Artin's Conjecture on primitive elements is true, then there will be infinitely many primes which satisfy the conditions of the above corollary. For this reason, we believe the conjecture should have as an added condition that 2 is a primitive element $\pmod{p}$. Thus $S_2[2, 3, p]$ should exist for $p = 19$ but not for $p = 31$.

Chapter 6

Conjectures, Conclusions and Future Research

Regarding the existence of a $S_2[2,3,7]$, in 2016, Heden et. all proved a strengthened version of a classical result from Thomas [21] established 20 years earlier. Using the term α-point in place of *special*-point defined here in Chapter 3, they showed that every 6-dimensional subspace of $\mathcal{V} = \mathbb{F}_2^7$ must contain at least one point that is not an α-point [18] This would imply there exist 5-space S containing a point i such that $d_i = 0$. based on our analysis, we claim the following:

Conjecture. *If there are points in $\mathbb{F}_2^7$ that are not special-points, a $S_2[2,3,7]$ does not exist.*

Establishing this would involve proofs of further results and computational studies. Many of the theoretical techniques and ideas presented here will possibly be effective in establishing existence of larger $S_2[2,3,n]$ as well as automorphism orders.

References

[1] S. Akbik, Normal generators of Finite Fields, J. Number Theory 41(1992) 146-149.

[2] R.D. Baker, J.H. Van Lint, R. M. Wilson, On the Preparata and Goethals Codes, IEEE Trans. on Information Theory, 29,n. 3, pp342-345, 1983

[3] A. Menezes (ed.), Applications of Finite Fields, Kluwer Academic Publishers, 1993.

[4] M.Braun, T. Etzion, P. R. J. Östergård, A. Vardy and A. Wasserman, Existence of q-Analogs of Steiner systems, Forum Math Pi, 4(2016),e7.

[5] M. Braun, A. Kerber, R. Laue, Systematic construction of q-analogs of designs, Des. Codes. Cryptogr. 34(2005), 55-70.

[6] C.J Colbourn, J.H. Dinitz, (eds) Handbook of combinatorial designs, 2nd ed., Chapman and & Hall/CRC (2007)

[7] C. Fernández-Cordoba, K.T. Phelps, M. Villanueva, Involutions in Perfect Codes,IEEE Trans. Information Theory,56(2010), no. 6 ,pp. 2571-2582.

[8] T. Etzion, L.Storme, Galois Geometries and Coding Theory, Des. Codes, Crypto.78(2016),pp.311-350.

[9] T. Etzion and A. Vardy, "Error- Correcting Codes in Projective Space *IEEE Trans. Inform. Theory*, vol. 57(2), pp. 1165-1173, 2011

[10] T. Etzion and A. Vardy, On q-analogs of Steiner systems and covering designs, Adv. Math. Commun. 5(2011) 161-176.

[11] T. Etzion- Private Communication

[12] W. M. Kantor, On the inequivalence of generalized Preparata codes, IEEE Trans. on Information Theory, 29,n. 3, pp345-348, 1983.

[13] Kiermaier, M., Kurz, S., Wassermann, A., The order of the automorphism group of a binary q-analog of the Fano plane is at most two, Des. Codes Cryptogr. pp. 1-12, (2017).

[14] A Kohneri, S. Kurtz, Construction of large constant constant dimension codes with prescribed minimum distance, in Mathematical Methods in Computer Science, Lecture notes in Computer Sci. 5393 (2008)31-42. (Eds. J. Calmet, W. Geiselmann, J. Muller-Quade)

[15] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 1977.

[16] R. Mathon, K.T. Phelps, A. Rosa, Small Steiner triple systems and their properties, Ars Combin. 15(1983), pp3-110.

[17] V. S. Pless, W. C. Huffman, and R. A. Brualdi, *Handbook of Coding Theory : Volume I*, North-Holland, 1998.

[18] O. Heden and P. A. Sissokho. On the Existence of a (2, 3)-Spread in V (7, 2). preprint, 2011.

[19] P. R. J. Östergård, O. Pottonen, K. T. Phelps, The perfect binary one-error correcting codes of length 15: part II properties,IEEE Trans. Inform. Theory 56(2010) no. 6,2571-2582.

[20] D. K. Ray-Chaudhuri, N.M. Singhi, q-Analogs of t-designs and their existence, Linear Algebra Appl.114/115(1989) 57-68.

[21] S. Thomas, Designs and partial geometries over finite fields, Geom. Dedicata 63(1996) 247-253.

[22] J. von Xu Gathen, M. Giesbrecht, Constructing normal basis in finite fields, J. Symbol. Computation,10(1990)547-570.

[23] Z. T. Mateva, S. T. Topalova, Line Spreads of $PG(5, 2)$, J. Combin. Des., 17(2009), no.1,90-102

[24] H. Wang, C. Xing, R. Safavi-Naini, Linear Authentication Codes: Bounds and Constructions, IEEE Transactions on Information Theory, VOL. 49, NO. 4, APRIL 2003

[25] D. V. Zinoviev, V. A. Zinoviev, On the Preparata-like codes, Fourteenth International Workshop on Algebraic and

[26] Combinatorial Coding Theory,(2014) Svetlogorsk, Russia, pp342-347. Fazeli A., Lovett S., Vardy A.: Nontrivial t-designs over finite fields exist for all t. J. Comb. Theory Ser. A 127, 149160 (2014).