SOME ALGEBRAIC PROBLEMS FROM CODING THEORY

By

OGUL ARSLAN

A DISSERTATION PRESENTED TO THE GRADUATE SCHOOL
OF THE UNIVERSITY OF FLORIDA IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

UNIVERSITY OF FLORIDA

2009

To my family, who gave me unconditional love and support throughout my life

ACKNOWLEDGMENTS

Foremost, I would like to express my gratitude to my advisor Professor Peter Sin, for his guidance and inspiration. He was always there, with his immense knowledge and enthusiasm, whenever I needed help. This research would not be possible without his continuous support, patience, motivation and encouragement.

I am grateful to the rest of my supervisory committee: Dr. David Drake, Dr. Kevin Keating, Dr. Meera Sitharam, Dr. Pham Hu Tiep and Dr. Alexandre Turull, for their mentoring and encouragement. I give my sincere thanks to all my professors in both Wayne State University and the University of Florida, for inspiring me. I also give my thanks to creators of SAGE (Mathematical Software Version 3.4.1, http://www.sagemath.org), for making such a useful open-source software. I am grateful to the Department of Mathematics, for providing me support to carry out my graduate studies. I thank the staff of Department of Mathematics, for helping the department run smoothly and for assisting me. Very special thanks go out to my friends. Without their support in both mathematical and social ways, it would have been very hard to go through the graduate school. Last but not the least; I thank my parents, my brother, and my sister-in-law. It would have been impossible for me to come up to this level, without such a great family.

TABLE OF CONTENTS

LIST OF FIGURES

Abstract of Dissertation Presented to the Graduate School
of the University of Florida in Partial Fulfillment of the
Requirements for the Degree of Doctor of Philosophy

SOME ALGEBRAIC PROBLEMS FROM CODING THEORY

By

Ogul Arslan

August 2009

Chair: Peter Sin
Major: Mathematics

Let F be a finite field of size q and characteristic p. A low density parity check (LDPC) code is a finite dimensional subspace of a vector space over F. A parity check matrix of an LDPC code is a binary sparse matrix which is orthogonal to the code. In this work, we describe a family of LDPC codes called the LU(3,q) codes over F . Let M (P,L) be the point-line incidence matrix of the symplectic generalized quadrangle. We give a description of a submatrix H of M(P,L) such that, any LU(3,q) code has either H or the transpose of H as its parity check matrix.

Previously, Peter Sin and Qing Xiang derived a formula for the dimension of the LU(3,q) codes for the case where F has an odd characteristic. If F has an even characteristic , the field of the geometry and the parity check matrix have the same characteristic, hence the solution requires different techniques. In this research, we give a descriptions of the points and lines of the symplectic generalized quadrangle using characteristic functions and polynomials. Using representation theory of the symplectic group SP(4,q), we find a basis for the column space of M(P,L). We use this result to show that the 2-rank of H is $rank_2(M(P,L)) - 2q$. Hence, the dimension of an LU(3,2^t) code is $q^3 + 2q - rank_2(M(P,L))$. This completes the dimension problem for the LU(3,q) codes.

CHAPTER 1
FINITE GEOMETRIES

1.1 Incidence Structures

An *incidence structure (or incidence system)* is a triple $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ such that $\mathcal{P}$ and $\mathcal{B}$ are two disjoint finite sets and $\mathcal{I}$ is a subset of $\mathcal{P} \times \mathcal{B}$. The members of $\mathcal{P}$ are called the *points*, and the members of $\mathcal{B}$ are called the *blocks* or *lines*. If an ordered pair (p, B) is in $\mathcal{I}$ we say that p is *incident* with B, or that p is *in* B, or that b *contains* B. We denote incidence by $(p, B) \in \mathcal{I}$, or p I B. If the incidence structure is clear from the context, we may also denote the incidence structure with $\mathcal{S} = (\mathcal{P}, \mathcal{L})$.

Definition 1. *An incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{B}, I)$ with v points is called a $t-(v, k, \lambda)$ design (or just a t-design) if every line $\ell \in \mathcal{B}$ is incident with exactly k points and every t distinct points are incident with exactly λ lines.*

Definition 2. *Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ and $\mathcal{T} = (\mathcal{Q}, \mathcal{C}, \mathcal{J})$ be incidence structures, and let ϕ be a bijection from $\mathcal{P} \cup \mathcal{B}$ to $\mathcal{Q} \cup \mathcal{C}$. Then,*

- *if $\phi(\mathcal{P}) = \mathcal{Q}$ and $\phi(\mathcal{B}) = \mathcal{C}$ with $(p, B) \in \mathcal{I}$ if and only if $(\phi(p), \phi(B)) \in \mathcal{J}$, then ϕ is an isomorphism from $\mathcal{S}$ to $\mathcal{T}$ and we write $\mathcal{S} \approx \mathcal{T}$. If $\mathcal{S} = \mathcal{T}$, then ϕ is an automorphism or a collineation.*
- *if $\phi(\mathcal{P}) = \mathcal{C}$ and $\phi(\mathcal{B}) = \mathcal{Q}$ with $(p, B) \in \mathcal{I}$ if and only if $(\phi(B), \phi(p)) \in \mathcal{J}$ then ϕ is and anti-isomorphism from $\mathcal{S}$ to $\mathcal{T}$. If $\mathcal{S} = \mathcal{T}$ then ϕ is an anti-automorphism or correlation. If $\phi \circ \phi$ is the identity map then ϕ is called a polarity.*

Given an incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ with $|\mathcal{P}| = v$ and $|\mathcal{B}| = b$, we can index the elements of $\mathcal{P}$ by p_i where $1 \leq i \leq v$, and the elements of $\mathcal{B}$ by b_j where $1 \leq j \leq b$. An incidence matrix for $\mathcal{S}$ is a $v \times b$ matrix $A = (a_{ij})$ such that,

$$a_{ij} = \begin{cases} 1, & \text{if } (p_i, b_j) \in \mathcal{I}, \\ 0, & \text{if } (p_i, b_j) \notin \mathcal{I}. \end{cases}$$

An incidence matrix of $\mathcal{S}$ gives a complete description of the structure. For this reason it is natural to study the incidence matrices in order to understand the incidence structures.

Definition 3. *Given an incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, then the incidence structure $\mathcal{S}^* = (\mathcal{B}, \mathcal{P}, \mathcal{I}^*)$ where $(B, p) \in \mathcal{I}^*$ if and only if $(p, B) \in \mathcal{I}$ is called the dual of $\mathcal{S}$.*

Note that the dual of the dual of an incidence structure is itself. That is, $(\mathcal{S}^*)^* = \mathcal{S}$.

Definition 4. *An incidence structure is self-dual, if it is isomorphic to its dual.*

Note that if A is an incidence matrix of $\mathcal{S}$ then the transpose of A is an incidence matrix of $\mathcal{S}^*$. Hence we can get the complete information about $\mathcal{S}$ from its dual. Sometimes one of $\mathcal{S}$ or $\mathcal{S}^*$ is easier to work with than the other. So we are free to choose the easier one for our study.

1.2 Projective Spaces

Let V be a vector space of dimension $n + 1$ over a finite field K with origin 0. Consider the equivalence relation of scalar multiples over the nonzero vectors. That is, two nonzero vectors v_1 and v_2 are equivalent if and only if there exists a $c \in K$ such that $v_1 = cv_2$. The set of equivalence classes is called the *projective space* of dimension n over the field K. It is denoted by $PG(n, K)$.If the finite field K is a Galois field of order q we can also denote this projective space by $PG(n, q)$. One can refer to [12] for more detailed information about projective spaces.

Note that the elements of $PG(n, K)$ are the one-dimensional subspaces of V with the origin deleted. These are called the points of $PG(n, K)$.

For convenience, if we view a one-dimensional subspace of V as a point in $PG(n, K)$ we automatically assume that the origin is omitted. Conversely, if we view a point of $PG(n, K)$ as a one-dimensional subspace of V, then we automatically assume that the origin is added to the elements of the point.

A *representative* of a point $p \in PG(n, K)$ is a nonzero vector v in p such that $p = \langle v \rangle$. Another notation is the homogeneous coordinates. If $v = (v_0, v_1, \ldots, v_n)$ is a representative of a point p, we write $p = [v_0 : v_1 : \ldots : v_n]$. Two points are called *linearly independent* if their representative vectors are linearly independent.

An $(m+1)$-dimensional subspace of V is called an *m-space of $PG(n,K)$*, or just a *subspace of dimension m in $PG(n,K)$*. Then it will be natural to call the subspaces of dimensions one, two, and three in V as the *points, lines* and *planes* in $PG(n,K)$. The $n-1$ dimensional subspaces of $PG(n,K)$ are called the *hyperplanes*. These are the n-dimensional subspaces of V.

It is not hard to see that, if $K=\mathbb{F}_q$ for some prime power q and $0\leq r\leq n$, then the number of subspaces of V of dimension r is

$$\frac{(q^{n+1}-1)(q^n-1)\dots(q^{n-r+2}-1)}{(q^r-1)(q^{r-1}-1)\dots(q-1)}. \tag{1–1}$$

In particular, the number of one dimensional subspaces of V is

$$\frac{q^{n+1}-1}{q-1}=q^n+q^{n-1}+\ldots+q^0. \tag{1–2}$$

Let P and L denote the sets of points and lines of $PG(n,K)$. We say that a point $p\in P$ is incident with a line $\ell\in L$, if the subspace of p is contained in the subspace of ℓ. In this case, we write $p\in\ell$. Thus, the pair (P,L) with the relation of inclusion is an incidence system. Furthermore, if $0\leq r\leq n$ we can talk about the incidence systems (P,L_r), where L_r is the set of r-spaces of $PG(n,q)$.

One of the natural questions to ask is the p-rank of the incidence matrices of these systems. The following theorem can be found in [6]. It was deduced from Hamada's articles in [10] and [11].

Theorem 1. ***(Hamada)*** *Let $q=p^t$ for some prime p and a positive integer t, and let (P,L_r), where $0\leq r\leq n$, be the incidence system of points and r-spaces of $PG(n,q)$. Then the p-rank of the incidence matrix is*

$$1+\sum_{s_0}\dots\sum_{s_{t-1}}\prod_{j=0}^{t-1}\sum_{i=0}^{\lfloor\frac{ps_{j+1}-s_j}{p}\rfloor}(-1)^i\binom{n+1}{i}\binom{n+ps_{j+1}-s_j-ip}{n} \tag{1–3}$$

where $s_0 = s_t$ *and the summation is taken over the integers* s_j $(0 \le j \le t-1)$ *satisfying*

$$r+1 \le s_j \le n, \text{ and } 0 \le ps_{j+1} - s_j \le (n+1)(p-1), \tag{1–4}$$

and $\lfloor a \rfloor$ *denotes the greatest integer less than or equal to* a*.*

With the help of this theorem it is possible to find the point-line and point-hyperplane incidence matrices of $PG(n,q)$. The latter one turns out to be a simpler formula.

Corollary 2. *If* $q = p^t$*, the* p*-rank of the point-hyperplane incidence matrix of* $PG(n,q)$ *is*

$$\binom{n+p-1}{n}^t + 1 \tag{1–5}$$

This result was also proven by Graham and MacWilliams [9] for the plane, and by Goethals and Delsarte [8], MacWilliams and Mann [17], and by Smith [23] for general n. More general version of theorem 1 is obtained by P. Sin in [21]. The author proved a formula for the p-rank of the incidence matrix between the d-dimensional and e-dimensional subspaces of V such that the incidence relation is the non-trivial intersection.

1.3 Finite Generalized Quadrangles

Let G be a graph. The *distance* between the two vertices x and y of G is the length of the shortest path between x and y. The *diameter* of G is the largest distance in graph. The length of the shortest cycle of a graph is called the *girth* of the graph. A *bipartite graph* is a graph whose vertices can be divided into two disjoint sets A and B such that edges can occur between the elements of A and B only.

Given an incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{B}, I)$ the *incidence graph of* $\mathcal{S}$ is defined as follows. The vertex set of the incidence graph is $\mathcal{P} \cup \mathcal{B}$. The vertices in $\mathcal{P}$ are pairwise disconnected, similarly the vertices in $\mathcal{B}$ are pairwise disconnected. Two vertices $p \in \mathcal{P}$ and $\ell \in \mathcal{B}$ are connected by an edge if and only if $p\, I\, \ell$. It is easy to see that the incidence graph is a bipartite graph.

Definition 5. *An incidence structure $(\mathcal{P}, \mathcal{B}, I)$ which is a $1-(v, s+1, t+1)$ design with $s > 0$, $t > 0$ is called a generalized n-gon ($n \geq 2$) of order (s, t) if its incidence graph has girth $2n$ and diameter n.*

A *generalized polygon* is a generalized n-gon for some n. If the parameters s and t are equal we say that the polygon has order s. Generalized polygons were first introduced by J.Tits in [25], also see Dembowski [5].

Example 1. *Some examples of generalized polygons are as follows,*

- *If $n = 2$ we have a generalized $2-$gon in which every point is incident with every line.*
- *If $s = t = 1$ then the generalized polygon are the ordinary $n-$gons.*
- *If $n = 3$ the generalized polygon is a generalized triangle. In this case $s = t$ all the time. If the generalized polygon is not a triangle, then it is a projective plane of order s.*
- *A generalized 4-gon is called a generalized quadrangle.*

More information on generalized polygons can be found in [2]. The definition of a quadrangle can be rephrased as follows.

Definition 6. *A (finite) generalized quadrangle of order (s, t) is an incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{B}, I)$ in which I is a point-line incidence relation satisfying the following axioms:*

- *Each point is incident with $t + 1$ lines ($t \geq 1$) and two distinct points are incident with at most one line.*
- *Each line is incident with $s + 1$ points ($s \geq 1$) and two distinct lines incident with at most one point.*
- *If p is a point and L is a line not incident with p, then there is a unique pair $(q, M) \in \mathcal{P} \times \mathcal{B}$ for which $p\ I\ M$, $q\ I\ M$, and $q\ I\ L$.*

We will give only the necessary properties of the generalized quadrangles here. The more detailed information about them can be found in [19].

It is easy to see that if $\mathcal{S} = (\mathcal{P}, \mathcal{B})$ is a generalized quadrangle of order (s, t), then $\mathcal{S}^* = (\mathcal{B}, \mathcal{P})$, the dual of $\mathcal{S}$, is a generalized quadrangle of order (t, s).

Example 2. *Suppose that $\mathcal{S} = (\mathcal{P}, \mathcal{B}, I)$ is an incidence structure. And suppose also that we can write $\mathcal{B}$ as a union of two disjoint sets Δ and Λ such that any two lines from Δ (respectively from Λ) have no points in common, and a line from Δ and a line from Λ have one point in common precisely. Then $\mathcal{S}$ is called a grid. In the case that $|\Delta| = |\Lambda|$ this grid is a generalized quadrangle with $t = 1$. We can also talk about the dual grid by just switching the words point and line in the above description. In this case, the grid quadrangle would have $s = 1$.*

Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, I)$ be a generalized quadrangle. We say that two points $p_1, p_2 \in \mathcal{P}$ are *collinear* (or *orthogonal*, *perpendicular*) if there is a line $\ell \in \mathcal{B}$ such that $p_1 \, I \, \ell$ and $p_2 \, I \, \ell$. We write $p_1 \sim p_2$ in this case. Dually, we say that two lines $\ell_1, \ell_2 \in \mathcal{B}$ are *concurrent* (or *orthogonal*, *perpendicular*) if they have a point in common. We write $\ell_1 \sim \ell_2$ in this case.

Let $p^\perp$ be the set of points in all the lines through p including p itself. That is,

$$p^\perp = \{p' \in P |\, p' \sim p\} \tag{1–6}$$

Similarly, we define $\ell^\perp$ to be the set of all lines that are collinear to ℓ. That is,

$$\ell^\perp = \{\ell' \in \mathcal{B} |\, \ell' \sim \ell\} \tag{1–7}$$

The *trace* of a pair of points (or two lines) $\{p, p'\}$ is the intersection of $p^\perp$ and $p'^\perp$. We write this as

$$tr(p, p') = \{p,\, p'\}^\perp = p^\perp \cap p'^\perp \tag{1–8}$$

Note that if $p \sim p'$ and $p \neq p'$, then the only points in common between $p^\perp$ and $p'^\perp$ are the ones on the line through p and p'. Hence, $|\{p,\, p'\}^\perp| = s + 1$. On the other hand, if $p \not\sim p'$ then by quadrangle properties, for every line ℓ through p there is a unique line passing through p' and intersecting ℓ. Since there are $t + 1$ lines through p, we conclude that $|p^\perp \cap p'^\perp| = t+1$. Similarly, for $\ell,\, \ell' \in \mathcal{B}$, if $\ell \sim \ell'$, then $|\{\ell,\, \ell'\}^\perp| = t+1$ and otherwise $|\{\ell, \ell'\}^\perp| = s + 1$. In general, if $P \subset \mathcal{P}$ (respectively, if $L \subset \mathcal{B}$), then

$$P^{\perp} = \bigcap_{p \in P} p^{\perp}, \quad (\text{ respectively } L^{\perp} = \bigcap_{\ell \in L} \ell^{\perp}). \tag{1–9}$$

Let $p \neq p'$ be two points. Then, the *span* of these points is the set

$$\mathrm{Span}(p,\, p') = \{p,\, p'\}^{\perp\perp} = \{p \in \mathcal{P} |\, p \in r^{\perp},\, \forall r \in \{p,\, p'\}^{\perp}\} \tag{1–10}$$

We say that a pair of points $(p,\, p')$ is *regular* if either $p \sim p'$ and $p \neq p'$ or $p \not\sim p'$ and $|\,\mathrm{Span}(p,\, p')| = t = 1$. The point p is called regular if $(p,\, p')$ is regular for all $p' \in P$, $p \neq p'$.

Classical generalized quadrangles: Let V be an $n+1$ dimensional vector space over a field $\mathbb{F}$. Let $PG(n, \mathbb{F})$ be the projective space with set of points $\mathcal{P}$ and set of lines $\mathcal{L}$. Denote the set of points of the quadrangle by P, and the set of lines of the quadrangle by L.

All of the classical generalized quadrangles can be embedded in to $PG(n, \mathbb{F})$. Moreover their automorphism groups contain classical groups. There are three main classes depending on the group acting on them.

(1) Generalized quadrangles Q(n,q) for n=3,4,5: These generalized quadrangles are obtained from the quadric Q of projective index 1 in $PG(n, q)$ with $n = 3, 4, 5$. The automorphism group of these quadrangles contains the orthogonal groups,

$$\mathrm{O}(n+1, \mathbb{F}) = \{M \in \mathrm{GL}(n+1, q), \mathbb{F}) | M^T M = M M^T = I\} \tag{1–11}$$

We find the points and the lines of this quadrangle as follows. Donate V with the quadratic form $\mathrm{Q} : V \to \mathbb{F}$ such that,

$$\begin{aligned}
\mathrm{Q}(v) &= v_0 v_1 + v_2 v_3 \quad \text{for } v = (v_0, v_1, v_2, v_3) \in V, \text{ for } n = 3 \\
\mathrm{Q}(v) &= v_0^2 + v_1 v_2 + v_3 v_4 \quad \text{for } v = (v_0, v_1, v_2, v_3, v_4) \in V, \text{ for } n = 4 \\
\mathrm{Q}(v) &= f(v_0, v_1) + v_2 v_3 + v_4 v_5 \quad \text{for } v = (v_0, v_1, v_2, v_3, v_4, v_5) \in V, \text{ for } n = 5
\end{aligned}$$

where the function f is an irreducible binary quadratic form in the last case. The points of the generalized quadrangle $Q(n,q)$ are the points in $\mathcal{P}$ that are generated by the vectors $v \in V$ such that $\mathrm{Q}(v) = 0$. That is,

$$P = \{p \in \mathcal{P} |\ \mathrm{Q}(v) = 0 \,\forall\, v \in p\}.$$

Similarly, the lines of the quadrangle are the lines in $\mathcal{L}$ such that $\mathrm{Q}(v) = 0$ for each vector v in it. That is,

$$L = \{\ell \in \mathcal{L} |\ \mathrm{Q}(v) = 0 \,\forall\, v \in \ell\}.$$

These quadrangles have the following parameters. If $n = 3$, then $s = q,\ t = 1,\ |P| = (q+1)^2,\ |L| = 2(q+1)$. If $n = 4$, then $s = q,\ t = q,\ |P| = |L| = (q+1)(q^2+1)$. Finally, if $n = 5$, then $s = q,\ t = q^2,\ |P| = (q+1)(q^3+1), |L| = (q^2+1)(q^3+1)$.

Note that when $n = 3$, the quadrangle is trivial. It is a grid.

(2) Hermitian quadrangles H(n,q^2), for n=3,4: Suppose the field of the projective space $PG(n,\mathbb{F})$ has order q^2 where $n = 3, 4$ and attach a hermitian form $H : V \times V \to \mathbb{F}$ to V. Without loss of generality we can assume that the hermitian form is,

$$H(u,v) = \sum_{i=0}^{n} u_i v_i^{q+1},\ \text{for } u = (u_0, u_1, \ldots, u_n), v = (v_0, v_1, \ldots, v_n) \in V. \tag{1–12}$$

We describe the Hermitian quadrangles as follows. The set of points of the quadrangle is,

$$P = \{\langle v \rangle \in \mathcal{P} |\ H(v,v) = 0,\ \forall\, v \in V \setminus \{0\}\} \tag{1–13}$$

A subspace of V is said to be isotropic if $H(u,v) = 0$ whenever u and v are both in the subspace. The lines of the quadrangle are the totally isotropic 2-dimensional subspaces of V. That is,

$$L = \{\ell \in \mathcal{L} |\ H(u,v) = 0,\ \forall\, u, v \in \ell\} \tag{1–14}$$

The automorphism group of these quadrangles contains the unitary groups,

$$\mathrm{U}(n+1,q) = \{U \in \mathrm{GL}(n+1,q) |\ U^*U = UU^* = I\} \tag{1–15}$$

U^* here denotes the conjugate transpose (or hermitian conjugate) of U.

The Hermitian quadrangles have the following properties. If $n = 3$ then $s = q^2$, $t = q$, $|P| = (q^2+1)(q^3+1)$, $|L| = (q+1)(q^3+1)$. If $n = 4$ then $s = q^2$, $t = q^3$, $|P| = (q^2+1)(q^5+1)$, $|L| = (q^3+1)(q^5+1)$.

(3) Symplectic quadrangles W(3,q): These quadrangles are embedded in to $PG(3,q)$. We attach a non-singular alternating bilinear form $B : V \times V \to \mathbb{F}$ to V. Without loss of generality we can assume that

$$B(u,v) = u_0v_3 - u_3v_0 + u_1v_2 - u_2v_1, \text{ for } u = (u_0,u_1,u_2,u_3), v = (v_0,v_1,v_2,v_3) \in V. \quad (1\text{–}16)$$

The singular points and the totally isotropic lines of $PG(3,q)$ forms the Symplectic quadrangle $W(q)$. The automorphism group of this quadrangle contains the Symplectic group,

$$\mathrm{Sp}(4,q) = \{M \in GL(4,q) | M^T J M = J\} \quad (1\text{–}17)$$

where J is a non-singular, skew-symmetric matrix.

Some open p-rank problems: The following are list of some of the open problems in the area.

- Let V be a finite dimensional vector space over a field F of characteristic p. We assume that V has a Hermitian form (,). The p-rank of the singular point-totally isotropic line incidence matrix is still unknown. In particular when n=3 or 4, the p-rank problems of point-line incidence matrices of the generalized Hermitian quadrangles are still open.

- The orthogonal analog of the above problem is still open. But for the generalized quadrangle case, the p-rank of the point-line incidence matrix of Q(n,q) is trivial for n=2. The p-rank is known for n=4 since this is the dual of the symplectic quadrangle. The p-rank of Q(5,q) is the dual of the hermitian quadrangle H(3,q^2).

- In general, the Hermitian and orthogonal analogs of Hamada's formula are still unknown.

- More generally, the Hermitian and orthogonal analogs of P. Sin's formula for the p-rank of (d-1)-space, (e-1)-space incidence system in [21] is still unknown. By changing the incidence system from non zero intersection to something else one can find more open problems.

- The p-rank of the point-line and point-hyperplane incidence matrices of other generalized quadrangles are still unknown.

CHAPTER 2
LOW DENSITY PARITY CHECK (LDPC) CODES

2.1 Linear Codes

Definition 7. *An (n, k) linear code $\mathcal{C}$ is a k-dimensional subspace of an n-dimensional vector space over a finite field of $\mathbb{F}_q$. The parameter k is the dimension (or rank) of the code and the parameter n is the length of the code. The elements of $\mathcal{C}$ are called codewords.*

Hence, while working with the codes we often prefer to focus on a base of the subspace.

Definition 8. *The generator matrix of an (n, k) code $\mathcal{C}$ is a matrix G of row rank k whose rows are codewords from $\mathcal{C}$ spanning the whole code. Conversely, if G is a matrix of row rank k over $\mathbb{F}_q$ then the row space of G is called an (n, k) linear code generated by G.*

Given an (n, k) linear code $\mathcal{C}$ there is an associated code called the dual code. It is denoted by $\mathcal{C}^{\perp}$ and defined as

$$\mathcal{C}^{\perp} = \{a = (a_1, \ldots, a_n) |\ a_1x_1 + \ldots + a_nx_n = 0,\ \forall\, x = (x_1, \ldots, x_n) \in \mathcal{C}\}. \tag{2–1}$$

The rank of the dual code $\mathcal{C}^{\perp}$ is $n - \dim(\mathcal{C}) = n - k$. A generator matrix H of the dual code $\mathcal{C}^{\perp}$ is called a parity check matrix of the code $\mathcal{C}$. If $h : \mathbb{F}_q^n \to \mathbb{F}_q^{n-k}$ is the linear transformation of the parity check matrix H, the kernel of this transformation is the code $\mathcal{C}$. We can define the parity check matrix more formally as follows.

Definition 9. *Let $\mathcal{C}$ be an (n, k) linear code over $\mathbb{F}_q$. A parity-check matrix of $\mathcal{C}$ is a matrix H such that $Hx^T = 0$ if and only if $x \in \mathcal{C}$.*

Given a code $\mathcal{C}$ and $x = (x_1, x_2, \ldots), y = (y_1, y_2, \ldots) \in \mathcal{C}$, the *Hamming distance*, or just the distance, between x and y is

$$d(x, y) = |\{i :\ x_i \neq y_i\}|. \tag{2–2}$$

The *weight* of the codeword x is the number of non-zero components of x. It is denoted by $w(x)$. Hence it is easy to see that $d(x, y) = w(y - x)$.

The Hamming distance satisfies the axioms of a metric in the usual sense. The *minimum distance* of a code $\mathcal{C}$ is

$$d = d_{min}(C) = min\{d(x,y)|\, x,y \in \mathcal{C},\ x \neq y\}. \tag{2–3}$$

It is possible to prove that the minimum distance is the least number of columns of H, the parity check matrix of $\mathcal{C}$, that sums up to 0.

The minimum distance of a code gives us an information about how many errors can be corrected after transmitting the information. The relationship between the number of errors that can be corrected and the minimum distance is given in the following theorem.

Theorem 3. *A code $\mathcal{C}$ can detect up to $d-1$ errors and can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors.*

The proofs for this theorem can be found in various resources. Some of them are [6], [3] or [18].

The *rate* of an (n,k) code is the number of bits per channel use being transmitted. It is the ration k/n. In order to have a 'good' code we expect k/n and d to be large. So given a linear code, we would like to know is its dimension and minimum distance. If the code is obtained systematically then it is somewhat easier to find these. So, it is natural to look at the codes that arise from finite geometries.

2.2 Low-Density Parity Check Codes

Low-density parity check (LDPC) codes were invented by Gallager [7] in 1962. Their decoding performance is very good so they became popular recently.

Definition 10. *An LDPC code is a linear error correcting code whose parity check matrix H has two properties: there are few non-zero entries in each row and column, and the number of non-zero entries in common between any two columns is not greater than 1.*

These codes have a large minimum distance so they perform well in terms of error correcting. The LDPC codes are constructed in two ways, randomly and using finite geometries. While understanding the properties of the first one depends on the computers,

the codes obtained using finite geometries can be studied using the properties of geometry and by using other mathematical concepts.

The codes we will study in the next chapter are LDPC codes obtained from the symplectic generalized quadrangle $W(q)$.

CHAPTER 3
$LU(M, Q)$ CODES

In this chapter we describe the $LU(m, q)$ codes. Then, we talk about the properties of $LU(2, q)$ and $LU(3, q)$ codes and we give a short discussion about the properties of $LU(m, q)$ codes for $m > 3$.

3.1 Incidence Structure $\Gamma(q)$

Let $q = p^t$ where p is a prime. We construct the semiplane $\Gamma(q)$ as follows. Let $\mathcal{P}$ and $\mathcal{L}$ be two infinite dimensional vector spaces over $\mathbb{F}_q$. Thus, any element in these spaces is a vector with infinitely many components. The vector spaces $\mathcal{P}$ and $\mathcal{L}$ are called the points and lines of the semiplane $\Gamma(q)$. Any point $p \in \mathcal{P}$ will be denoted by (p), and any line $\ell \in \mathcal{L}$ will be denoted by $[\ell]$. That is, we will use parentheses and brackets in order to distinguish between the elements of $\mathcal{P}$ and $\mathcal{L}$. We can use the following indexing for the points and lines.

$$(p) = (p_1, p_{1.1}, p_{1.2}, p_{2.1}, p_{2.2}, p'_{2.2}, p_{2.3}, p_{3.2}, p_{3.3}, p'_{3.3}, \ldots, p'_{i.i}, p_{i.i+1}, p_{i+1.i}, p_{i+1.i+1}, \ldots)$$

$$[\ell] = [\ell_1, \ell_{1.1}, \ell_{1.2}, \ell_{2.1}, \ell_{2.2}, \ell'_{2.2}, \ell_{2.3}, \ell_{3.2}, \ell_{3.3}, \ell'_{3.3}, \ldots, \ell'_{i.i}, \ell_{i.i+1}, \ell_{i+1.i}, \ell_{i+1.i+1}, \ldots] \qquad (3\text{–}1)$$

such that

$$p_{-1.0} = \ell_{0.-1} = p_{1.0} = \ell_{0.1} = 0,\ p_{0.1} = p_1,\ \ell_{1.0} = \ell_1,\ p'_{1.1} = p_{1.1},\ \ell'_{1.1} = \ell_{1.1}. \qquad (3\text{–}2)$$

A point (p) is incident with a line $[\ell]$ if and only if the following conditions are satisfied for $i = 1, 2, 3, \ldots$

$$\begin{aligned} \ell_{i.i} - p_{i.i} &= \ell_1\, p_{i-1.i} \\ \ell'_{i.i} - p'_{i.i} &= p_1\, \ell_{i.i-1} \\ \ell_{i.i+1} - p_{i.i+1} &= p_1\, \ell_{i.i} \\ \ell_{i+1.i} - p_{i+1.i} &= \ell_1\, p'_{i.i} \end{aligned} \qquad (3\text{–}3)$$

The semiplane $\Gamma(q)$ with the above set of points and lines, and the incidence relation is an incidence structure. The incidence graph of this structure is $D(q)$.

Let $m \geq 2$ be an integer consider the incidence system $\Gamma(m,q) = (\mathcal{P}(m), \mathcal{L}(m), \ \mathrm{I}_{\ m})$ where $\mathcal{P}(m)$ and $\mathcal{L}(m)$ are set of vectors obtained from projecting the elements of $\mathcal{P}$ and $\mathcal{L}$ onto the first m components. For $(p) \in \mathcal{P}(m)$, and $[\ell] \in \mathcal{L}(m)$ we say (p) is incident with $[\ell]$ if and only if first m equations in condition (3–3) are satisfied. We let $D(m,q)$ denote the incidence graph of $\Gamma(m,q)$.

The following proposition can be found in [15].

Proposition 4. *Let $m \geq 2$. The incidence system $\Gamma(m,q)$ is a semiplane and $D(m,q)$ is a $q-$regular bipartite graph on $2q^m$ vertices containing no $4-$cycles.*

Theorem 5. *(i) If $m \geq 2$ is an odd integer then the girth of $D(m,q)$ is at least $m+5$ [15],*

(ii) If $m \geq 2$ is an even integer then the girth of $D(m,q)$ is at least $m+4$ [16].

3.2 LU(m,q) Codes

Let $H(m,q)$ be the incidence matrix of $\Gamma(m,q)$ where the rows are indexed by the lines $\mathcal{L}(m)$ and the columns are indexed by the points $\mathcal{P}(m)$. The binary linear codes obtained by the parity check matrices $H(m,q)$ and its transpose $H^T(m,q)$ are the $LU(m,q)$ codes. That is $LU(m,q)$ codes are the codes whose Tanner graph [24] are the $D(m,q)$. It is immediate that these codes have length q^m. The other properties like the minimum distance and dimension vary by the choice of m and q. These codes were first introduced in [13]. The authors also investigated the properties of $LU(2,q)$ and $LU(3,q)$ in [13]. While $LU(2,q)$ was completely described, the dimensions of $LU(3,q)$ were conjectured for the case where q is an odd prime power and the other case remained unknown for a while. In 2006, P. Sin and Q. Xiang proved the conjecture and gave a formula for the dimensions of $LU(3,q)$ codes for odd q in [22]. They also obtained a lower bound for the dimension when q is even. The given bound is the actual dimension by the computer calculations of J.-L. Kim up to $q = 16$. We prove the lower bound is the actual

dimension. Through out the process we used open source mathematics software SAGE for our calculations.

3.2.1 LU(2,q) Codes

We first examine the incidence structure $\Gamma(\mathcal{P}(2), \mathcal{L}(2), \ \mathrm{I}\ _2)$. By the description of points and lines in (3–1) we get

$$\mathcal{P}(2) = \{(p_1, p_{1.1}) : \ p_1, p_{1.1} \in \mathbb{F}_q\}, \tag{3–4}$$

and

$$\mathcal{L}(2) = \{[\ell_1, \ell_{1.1}] : \ \ell_1, \ell_{1.1} \in \mathbb{F}_q\}. \tag{3–5}$$

The incidence relation is the satisfaction of the first two conditions of (3–3). Hence a point $(p_1, p_{1.1})$ is incident with a line $[\ell_1, \ell_{1.1}]$ if and only if

$$\ell_{1.1} - p_{1.1} = \ell_1 \, p_{0.1} \tag{3–6}$$

and

$$\ell'_{1.1} - p'_{1.1} = p_1 \, \ell_{1.0} \tag{3–7}$$

are satisfied. Note that, with the equations in (3–2) these two conditions are the same. Hence, we can describe the $LU(2, q)$ codes as follows.

Suppose $(\mathcal{P}, \mathcal{L}, \ \mathrm{I}\ )$ is an incidence structure where

$$\mathcal{P} = \{(a, b) : \ a, b \in \mathbb{F}_q\}, \ \text{and} \ \mathcal{L} = \{[x, y] : \ x, y \in \mathbb{F}_q\} \tag{3–8}$$

. A point (a, b) is incident with a line $[x, y]$ if and only if $y = ax + b$. The incidence matrix of this structure is denoted by H. The binary $LU(2, q)$ codes are the codes obtained by the parity check matrices H and H^T.

Properties: The following properties are contained in [13].

- For $q \geq 2$, the Tanner graph $D(2, q)$ of $LU(2, q)$ has girth 6, and $D(2, q)$ has diameter 4.

- If q is odd, the two $LU(2,q)$ codes obtained from parity check matrices H and H^T are the same. These codes have length q^2, dimension $q-1$ and minimum distance $2q$.
- If $q = 2^t$ for some positive integer t, the $LU(2,q)$ codes have length q^2, dimension $q^2 - 3^t$ and minimum distance $q+2$.
- When $q = 2^t$, the $LU(2,q)$ codes are Euclidian Geometry Codes obtained from extensions of Type-I EG-LDPC codes from [14].

3.2.2 LU(3,q) Codes

We again start with the incidence structure $\Gamma(3) = (\mathcal{P}(3), \mathcal{L}(3), \mathrm{I}_3)$. By the descriptions of points and lines in (3–1) we get

$$\mathcal{P}(3) = \{(p_1, p_{1.1}, p_{1.2}) : p_1, p_{1.1}, p_{1.2} \in \mathbb{F}_q\} \tag{3–9}$$

and

$$\mathcal{L}(3) = \{[\ell_1, \ell_{1.1}, \ell_{1.2}] : \ell_1, \ell_{1.1}, \ell_{1.2} \in \mathbb{F}_q\}. \tag{3–10}$$

We say that a point $(p_1, p_{1.1}, p_{1.2})$ is incident with a line $[\ell_1, \ell_{1.1}, \ell_{1.2}]$ if and only if the first three of the conditions (3–3) are satisfied. That is,

$$\ell_{1.1} - p_{1.1} = \ell_1\, p_{0.1}, \tag{3–11}$$

$$\ell'_{1.1} - p'_{1.1} = p_1\, \ell_{1.0}, \tag{3–12}$$

$$\ell_{1.2} - p_{1.2} = p_1\, \ell_{1.1}. \tag{3–13}$$

Once again because of the equations in (3–2) the first two of these equations are equivalent. Hence we can describe the $LU(3,q)$ codes as follows.

Let $(\mathcal{P}, \mathcal{L}, \mathrm{I})$ be an incidence structure such that

$$\mathcal{P} = \{(a,b,c) : a,b,c \in \mathbb{F}_q\}, \text{ and } \mathcal{L} = \{[x,y,z] : x,y,z \in \mathbb{F}_q\} \tag{3–14}$$

.

From the conditions (3–11), (3–12), and (3–13) we obtain that a point $(a, b, c) \in \mathcal{P}$ is incident with a line $[x, y, z] \in \mathcal{L}$ if and only if

$$y = ax + b \text{ and } z = ay + c. \tag{3–15}$$

Let H be the incidence matrix of this structure. The binary $LU(3, q)$ codes are the linear codes obtained from the parity check matrices H and H^T.

The the more detailed explanations about the following properties can be found in [13].

- The Tanner graph $D(3, q)$ of $LU(3, q)$ codes has girth 8 and its diameter is 6 for $q > 2$.
- The minimum weight of an $LU(3, q)$ code obtained from H is $2q$.
- If an $LU(3, q)$ code is obtained from H^T the minimum weight is at least $2q$. By computations we observe that some of these codes have minimum weight bigger than $2q$.

3.2.3 LU(m,q) Codes for m>3

When $m > 3$ the conditions (3–3) gives a more complicated structure for the incidence relation. However, since these graphs have girths bigger than $2\lceil m/2 \rceil + 4$, we have the following theorem about the lower bound on the minimum distance.

Theorem 6. *The minimum distance d of $LU(m, q)$ satisfies*

$$d \geq \begin{cases} 2\,\frac{(q-1)^{\lfloor m/4 \rfloor + 1} - 1}{q-2} & \text{if } m \equiv 0 \bmod 4; \\ 2\,\frac{(q-1)^{\lfloor m/4 \rfloor + 2} - 1}{q-2} & \text{if } m \equiv 3 \bmod 4; \\ 2\,\frac{(q-1)^{\lfloor m/4 \rfloor + 1} - 1}{q-2} + \frac{2}{q}(q-1)^{\lfloor m/4 \rfloor + 1} & \text{if } m \equiv 1, 2 \bmod 4. \end{cases}$$

When $q = 2$ the fraction $\frac{(q-1)^{\lfloor m/4 \rfloor + 1} - 1}{q-2}$ is understood to be $\lfloor m/4 \rfloor + 1$, and $\frac{(q-1)^{\lfloor m/4 \rfloor + 2} - 1}{q-2}$ to be $\lfloor m/4 \rfloor + 2$.

CHAPTER 4
DIMENSIONS OF $LU(3,Q)$ CODES

In this chapter we give formulas for the dimensions of $LU(3,q)$ codes. This problem is solved in two cases, q odd and q even.

4.1 Another Description for LU(3,q) Codes

Let V be a $4-$dimensional vector space over the field $\mathbb{F}_q$ of q elements. We assume that V has a nonsingular alternating bilinear form (v,v'), that is, (v,v') is linear in both components and $(v,v) = 0$ for all v. Let $\mathrm{Sp}(4,q)$ be the symplectic group of linear automorphisms preserving this form. We pick a symplectic basis $\{e_0, e_1, e_2, e_3\}$ of V, with $(e_i, e_{3-i}) = 1$ for $i = 0, 1$. Thus, for $v = \sum_{i=0}^{3} x_i\, e_i,\ \ v' = \sum_{i=0}^{3} y_i\, e_i \in V$, the symplectic form is given by

$$(v,v') = x_0y_3 - x_3y_0 \ + \ x_1y_2 - x_2y_1. \tag{4–1}$$

Consider the projective space $P(V)$, the space of one dimensional subspaces of V. Let P be the set of points of $P(V)$, that is the set of one dimensional subspaces of V. We sometimes denote the elements of P using the homogeneous coordinates. So,

$$P = \{\langle v\rangle |\ v \in V, v \neq 0\} = \{(a:b:c:d)|\ a,b,c,d \in \mathbb{F}_q,\ \text{not all zero }\} \tag{4–2}$$

A subspace of V is called *totally isotropic*, if $(v,v') = 0$ whenever v and v' are both in the subspace. We let L be the set of totally isotropic 2-dimensional subspaces of V. Hence,

$$L = \{\langle v,v'\rangle |\ \langle v\rangle, \langle v'\rangle \in P, \langle v\rangle \neq \langle v'\rangle,\ \text{and } (v,v') = 0\} \tag{4–3}$$

The triple (P,L,I) with the natural relation of incidence between the points and lines is an incidence structure. From now on all the incidence systems have the relation of inclusion so we will drop the letter I from the notations.

Note that every line of (P,L) has $q+1$ points in it and every point is contained in $q+1$ lines from L. Moreover, one can see that given any line ℓ and a point p not on that line there is a unique line that passes through p and intersects ℓ. Hence this incidence

structure satisfies the generalized quadrangle axioms with $s = t = q + 1$. In fact, (P, L) is the symplectic generalized quadrangle $W(q)$ from [19].

Fix a point $p_0 = \langle e_0 \rangle \in P$ and a line $\ell_0 = \langle e_0, e_1 \rangle \in L$. For a point $p \in P$, we define $p^\perp$ to be the set of points on all the lines that pass through p. Thus,

$$p_0^\perp = \{(a : b : c : 0) | \, a, b, c \in F_q\}. \tag{4–4}$$

Let P_1 be the set of points not in $p_0^\perp$ and L_1 be the set of lines which do not intersect ℓ_0. Hence other incidence systems of interest are (P_1, L_1), (P, L_1) and (P_1, L). Let $M(P, L)$ be the incidence matrix whose rows are indexed by P, and the columns by L. Similarly, we get the incidence matrix $M(P_1, L_1)$, which can be thought as a submatrix of $M(P, L)$. We can reorder the rows and columns of $M(P, L)$ so that the points in $p_0^\perp$ come on top and the lines in $L \setminus L_1$ come first. So, we can visualize the two incidence matrices as follows

$$M(P, L) = \left[\begin{array}{c|c} & \\ \hline & \\ & M(P_1, L_1) \\ & \end{array}\right] \tag{4–5}$$

Proposition 7. *The incidence systems* $(\mathcal{P}, \mathcal{L}, I)$ *from (3–14) and* (P_1, L_1) *from above are isomorphic.*

Proof. This result is from the appendix of [22]. □

Hence, $M(P_1, L_1)$ and its transpose are parity check matrices for $LU(3, q)$ codes. Since the $LU(3, q)$ code is binary, we want to know the 2-rank of the matrix $M(P_1, L_1)$.

4.2 Dimensions for C(P,L) and a Lower Bound for the Dimension of LU(3,q)

The dimension formulas for $C(P, L)$ are different for fields of odd and even characteristic p. In [22], P.Sin and Q.Xiang obtained the formula for the case of odd q. We use different methods to obtain the formula for the case of even q. We give detailed proofs for the even case and state the corresponding results of the odd case whenever possible.

We reorder the points in P as follows,

$$P = \{p_0,\, p_1,\, \ldots, p_{q^3+q^2+q}\}.$$

In this ordering p_0 is as we defined before. Then the next q points in this list are the remaining points in ℓ_0, and the next q^2 points are the remaining points in $p_0^{\perp}$. The last q^3 points are the points in P_1.

We can talk about a similar ordering for the set of lines. So,

$$L = \{\ell_0,\, \ell_1,\, \ldots, \ell_{q^3+q^2+q}\}.$$

where ℓ_0 is as before. The next q lines are the remaining lines through p_0, and the next q^2 lines are the other lines intersecting ℓ_0, and finally the last q^3 lines are the lines from L_1.

We denote by $F_2[P]$ the space of F_2-valued functions on P. We can think of elements of $F_2[P]$ as $q^3 + q^2 + q + 1$ component vectors whose entries are indexed by the points of P so that for any function f, the value of each entry is the value of f at the corresponding point. That is

$$f = (f(p_0),\, f(p_1),\, f(p_2),\, \ldots)$$

The characteristic function χ_p for a point $p \in P$ is the function whose value is 1 at p, and zero at any other point. Thus, χ_p is the $q^3 + q^2 + q + 1$ component vector whose entry that corresponds to p is 1, and all the other entries are zero. Hence,

$$\begin{aligned}
\chi_0 &= (1,\, 0,\, 0,\, 0,\, \ldots) \\
\chi_1 &= (0,\, 1,\, 0,\, 0,\, \ldots) \\
\chi_2 &= (0,\, 0,\, 1,\, 0,\, \ldots) \ldots etc.
\end{aligned}$$

The characteristic functions for all the points in P form a basis for $F_2[P]$. For any line $\ell \in L$, the characteristic function χ_ℓ is the function given by the sum of the $q+1$ characteristic functions of the points of ℓ. The subspace of $F_2[P]$ spanned by all the χ_ℓ is the F_2 code of (P, L), denoted by $C(P, L)$. We can think of it as the column space of $M(P, L)$. Thus the $2-$ rank of $M(P, L)$ gives us the dimension of the code $C(P, L)$. The first statement of the following theorem was proven in [Theorem 9.4, [1]], and the second was proven in [Theorem 1, [20]].

Theorem 8. *If q is odd, the 2-rank of $M(P, L)$ is $\frac{q^3+2q^2+q+2}{2}$. If q is even, the 2-rank of $M(P, L)$ is $1+\left(\frac{1+\sqrt{17}}{2}\right)^{2t}+\left(\frac{1-\sqrt{17}}{2}\right)^{2t}$.*

The following theorem and its corollary were proven in [22].

Theorem 9. *Assume q is a power of an odd prime. The 2-rank of $M(P_1, L_1)$ equals*

$$\frac{q^3+2q^2-3q+2}{2} \tag{4–6}$$

Corollary 10. *If q is a power of an odd prime, the dimension of $LU(3, q)$ is*

$$\frac{q^3-2q^2+3q-2}{2} \tag{4–7}$$

Here we prove the corresponding theorem and corollary for the even case.

Theorem 11. *Assume $q = 2^t$ for some positive integer t. The 2-rank of $M(P_1, L_1)$ is*

$$1+\left(\frac{1+\sqrt{17}}{2}\right)^{2t}+\left(\frac{1-\sqrt{17}}{2}\right)^{2t}-2^{t+1} \tag{4–8}$$

Corollary 12. *Assume $q = 2^t$ for some positive integer t. The dimension of $LU(3, q)$ is*

$$2^{3t}+2^{t+1}-1-\left(\frac{1+\sqrt{17}}{2}\right)^{2t}-\left(\frac{1-\sqrt{17}}{2}\right)^{2t} \tag{4–9}$$

For simplicity, most of the time we will not make a distinction between the lines and the characteristic functions of the lines. For example, we say a subspace spanned by lines instead of characteristic functions of lines.

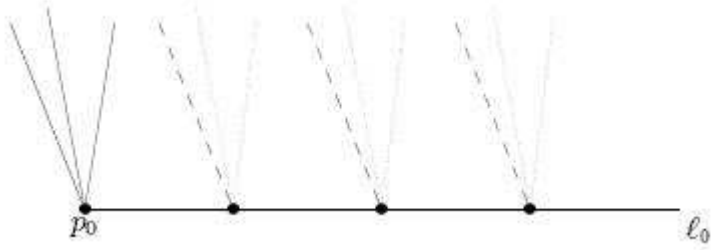

Figure 4-1. Lines that are incident with X and Y.

Let $C(P, L_1)$ be the subspace of $F_2[P]$ spanned by the lines of L_1, $C(P_1, L_1)$ denote the code of (P_1, L_1) viewed as a subspace of $F_2[P_1]$, and let $C(P_1, L)$ be the larger subspace of $F_2[P_1]$ spanned by the restrictions to P_1 of the characteristic functions of all lines of L. That is, if $M(P, L)$ is the matrix as in (4–5) where the blocks named as follows

$$M(P,L) = \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right] \tag{4–10}$$

Then $C(P, L_1)$ is the column space of $\left[\begin{smallmatrix} B \\ D \end{smallmatrix}\right]$, $C(P_1, L_1)$ is the column space of $[\,D\,]$, and $C(P_1, L)$ is the column space of $[\,C\ D\,]$.

We consider the natural projection map

$$\pi_{P_1} : F_2[P] \to F_2[P_1] \tag{4–11}$$

given by the restriction of functions to P_1. We denote its kernel by $ker\,\pi_{P_1}$.

Let X be the set of characteristic functions of the $q + 1$ lines passing through p_0, and let $X_0 = X \setminus \ell_0$. We also pick q lines that intersect ℓ_0 at q distinct points except p_0, and call the set of these lines as Y. In the figure 4-1 the solid lines represent the set X while the dashed lines represent a choice of Y.

Moreover, let $Z \subset C(P, L_1)$ be a set of characteristic functions of lines in L_1 which maps bijectively under π_{P_1} to a basis of $C(P_1, L_1)$. Remember that the lines in L_1 were the ones that does not intersect ℓ_0. So the lines in Z does not intersect ℓ_0 either.

It is immediate that the sets X, Y, and Z are disjoint. If a line ℓ is in X, all of its points are in $p_0^{\perp}$. Thus, its image under π_{P1} is all zero vector. So, $X \subset ker\, \pi_{P_1}$. Also we note that $|X_0 \cup Y| = 2q$, while $|Z| = dim_{F_2} C(P_1, L_1)$.

The following lemma and corollary were proven in [22].

Lemma 13. *$X_0 \cup Y \cup Z$ is linearly independent over F_2.*

Proof. Elements of Y contains a point of ℓ_0 in their support, and this point is not in the support of any other element of $X_0 \cup Y \cup L$. Moreover since X_0 is a linearly independent subset of $ker\, \pi_{P_1}$ and Z maps to a basis of L_1 under π_{P_1} it is clear that $X_0 \cup Z$ is linearly independent. Therefore the set $X_0 \cup Y \cup L$ is also linearly independent. □

Corollary 14. *Let q be an arbitrary prime power. Then*

$$\dim_{F_2} LU(3, q) \geq q^3 - \dim_{F_2} C(P, L) + 2q. \tag{4–12}$$

Proof. $M(P_1, L_1)$ is a parity-check matrix of $LU(3, q)$. So,

$$\dim_{\mathbb{F}_2} LU(3, q) = q^3 - \dim_{\mathbb{F}_2} C(P_1, L_1) \tag{4–13}$$

By the above lemma and the fact that $|X_0 \cup Y \cup Z| = 2q + \dim_{\mathbb{F}_2} C(P_1, L_1)$, we have

$$\dim_{\mathbb{F}_2} C(P, L) \geq 2q + \dim_{\mathbb{F}_2} C(P_1, L_1) \tag{4–14}$$

Combining the two inequalities we get the result. □

4.3 Grids of Lines

Unless otherwise stated, we assume that $q = 2^t$ for the rest of the chapter.

Lemma 15. *Let ℓ and ℓ' be two lines passing through $p \in \ell_0$. Then $\chi_\ell + \chi_{\ell'} \in C(P, L_1)$.*

Proof. We first show that there is a grid of lines between ℓ and ℓ'. This means there are two sets of lines Δ and Λ such that each set has q elements, each line in Δ intersects $\ell \setminus \{p\}$, and distinct lines of Δ intersect $\ell \setminus \{p\}$ in distinct points. Similarly, each line in Λ intersects $\ell' \setminus \{p\}$, and distinct lines of Λ intersect $\ell' \setminus \{p\}$ in distinct points. Moreover, every line of Δ intersects every line of Λ.

Pick a point $p^* \in P$ which is not in ℓ, ℓ', or ℓ_0. By quadrangle properties there is a unique line δ_0, through p^* that intersects ℓ. Similarly, there is a unique line λ_0, through p^* that intersects ℓ'. Let p_1 denote $\delta_0 \cap \ell$, and p_2 denote $\lambda_0 \cap \ell'$. We can see this in the figure 4-2.

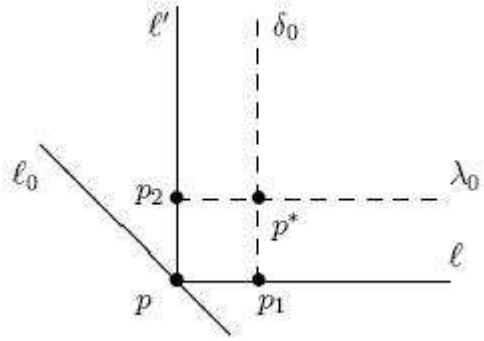

Figure 4-2. Lines λ_0 and δ_0.

Let $a, b, c, e \in V$ be the generators of the points p_1, p_2, p^*, and p respectively. That is, that $p_1 = \langle a \rangle$, $p_2 = \langle b \rangle$, $p^* = \langle c \rangle$ and $p = \langle e \rangle$. Without loss of generality we can assume that$(a, b) = (e, c) = 1$. We can write the lines δ_0 and λ_0 in terms of their generators as $\delta_0 = \langle a, c \rangle$ and $\delta_0 = \langle b, c \rangle$. Thus, the points of δ_0 other than p_1 are of the form $\langle c + \beta a \rangle$ where $\beta \in \mathbb{F}_q$. Similarly the points of λ_0 other than p_2 are of the form $\langle c + \gamma b \rangle$ for some $\gamma \in \mathbb{F}_q$.

Through every point of δ_0, there is a unique line intersecting ℓ'. Being in ℓ' these points are of the form $\langle b + \alpha e \rangle$ for some $\alpha \in \mathbb{F}_q$ as in figure 4-3.

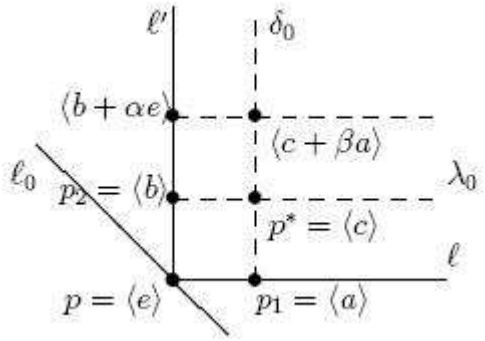

Figure 4-3. More lines in the grid.

Since the form (,) is an alternating bilinear form, and $\langle c+\beta a\rangle$, and $\langle b+\alpha 3\rangle$ are on the same line,

$$\begin{aligned} 0 &= (c+\beta a, b+\alpha e) && (4\text{–}15)\\ &= (c,b)+\alpha(c,e)+\beta(a,b)+\alpha\beta(a,e) && (4\text{–}16)\\ &= \alpha(c,e)+\beta(a,b) && (4\text{–}17)\\ &= \alpha+\beta && (4\text{–}18)\\ & && (4\text{–}19) \end{aligned}$$

Thus $\alpha = \beta$ in $\mathbb{F}_q$. Then for $\beta \in \mathbb{F}_q$, the line through $\langle c+\beta a\rangle$ that intersect ℓ' is $\lambda_\beta = \langle c+\beta a, b+\beta e\rangle$.(figure 4-4) Similarly, we can show that for $\gamma \in \mathbb{F}_q$, the line through

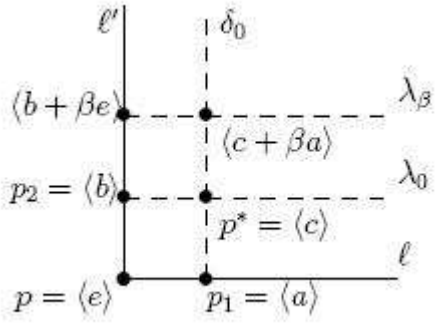

Figure 4-4. Lines of the grid

$\langle c + \gamma b \rangle$ that intersect ℓ is $\delta_\gamma = \langle c + \gamma b, a + \gamma e \rangle$.

Therefore,

$$\Delta = \{\delta_\gamma | \gamma \in \mathbb{F}_q, \ \ \delta_\gamma = \langle c + \gamma b, a + \gamma e \rangle\} \tag{4–20}$$

$$\Lambda = \{\lambda_\beta | \lambda \in \mathbb{F}_q, \ \ \lambda_\beta = \langle c + \beta a, b + \beta e \rangle\} \tag{4–21}$$

Note that the lines in Δ (respectively in Λ) do not intersect each other.

Now we pick two lines δ_γ and λ_β for some $\gamma, \beta \in \mathbb{F}_q^\times$. Then, $\delta_\gamma = \langle c + \gamma b, a + \gamma e \rangle$ and $\lambda_\beta = \langle c + \beta a, b + \beta e \rangle$. We want to show that these two lines have a non-zero intersection (figure 4-5).

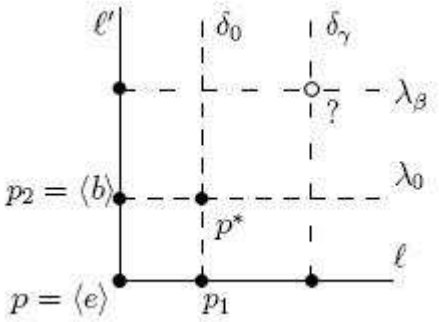

Figure 4-5. Intersection of λ_γ and δ_δ.

Hence, δ_γ and λ_β intersect at s, and by quadrangle properties this is the only point of intersection. Hence, every line in Δ intersects every line in Λ. Thus, there is a grid of lines between ℓ and ℓ'. Moreover, the lines in $\Delta \cup \Lambda$ are in L_1 (figure 4-6).

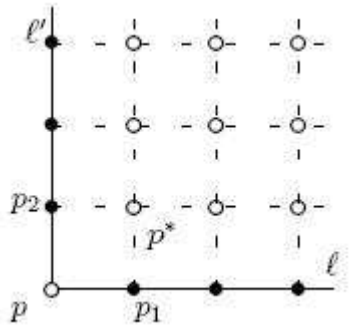

Figure 4-6. Summing lines in the grid.

□

An alternate proof to this result is using the regularity of the generalized quadrangle $W(q)$.

Proof. (Alternate) The points of the quadrangle $W(q)$ are regular as it is defined in [[19], section 1.3, p.4]. When q is even this quadrangle is known to be self-dual [[19], 3.2.1]. Hence, the lines of $W(q)$ are regular for the case of even q. Thus one can show that there is a grid of lines between ℓ and ℓ'. This means there are two sets of lines Δ and Λ such that each set has q elements, each line in Δ intersects $\ell \setminus \{p\}$ and distinct lines of Δ intersects $\ell \setminus \{p\}$ in distinct points. Similarly, each line in Λ intersects $\ell' \setminus \{p\}$ and distinct lines of Λ intersects $\ell' \setminus \{p\}$ in distinct points. Moreover, every line of Δ intersects every line of Λ.

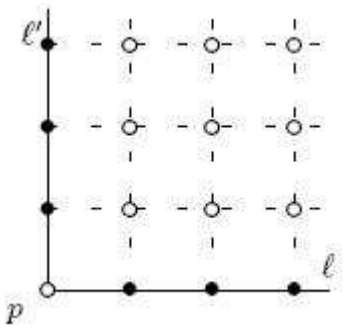

Figure 4-7. Grid lines between ℓ and ℓ'.

We add characteristic functions of these lines and get

$$\sum_{\gamma \in \Delta \cup \Lambda} \chi_\gamma = \chi_\ell + \chi_{\ell'} \in C(P, L_1). \tag{4–22}$$

□

Lemma 16. *For any choice of Y, $\ell \in L \setminus \{\ell_0\}$ and the all 1's vector $\mathbf{1}$ are in the span of $X_0 \cup Y \cup L_1$.*

Proof. It is enough to show that any line ℓ in $L \setminus (X \cup L_1)$ is in the span of $X_0 \cup Y \cup L_1$. It is immediate that ℓ intersects ℓ_0 at a point p other than p_0. Let ℓ' be the line in Y that intersect ℓ_0 at p. Then, by the previous result $\chi_\ell + \chi_{\ell'}$ is in the span of L_1. Thus $(\chi_\ell + \chi_{\ell'}) + \chi_{\ell'} = \chi_\ell$ is in the span of $Y \cup L_1$. Thus any line in $L \setminus \{\ell_0\}$ can be written as a linear combination of the lines in $X_0 \cup Y \cup L_1$.

In order to prove the second part of the lemma, we pick a line in L_1, say ℓ^*. Since ℓ^* does not intersect ℓ_0, all the lines that intersect ℓ^* are in $\langle X_0, Y, L_1 \rangle$. Hence we add all these lines, including ℓ^*, to get $\mathbf{1}$.

□

Lemma 17. *ℓ_0 is contained in the span of $X_0 \cup Y \cup L_1$.*

Proof.

$$\chi_{\ell_0} = \mathbf{1} + \sum_{\ell \cap \ell_0 \neq \emptyset,\ \ell \neq \ell_0} \chi_\ell \quad \in \quad \langle X_0, Y, L_1 \rangle. \tag{4–23}$$

□

Thus any line $\ell \in L$ is in the span of $X_0 \cup Y \cup L_1$. It remains to show the span of $X_0 \cup Y \cup L_1$ is the same as the span of $X_0 \cup Y \cup Z$.

In the next section we introduce a new way of representing the lines of P.

4.4 Approach by Using Polynomials

Let k denote the field $\mathbb{F}_q$ where $q = 2^t$ for some positive integer t, and let V be the 4-dimensional vector space over k as before. Consider the space, $k[V]$, of k-valued functions on V, where the elements of this space are vectors with q^4 components on k.

Let $R = k[x_0, x_1, x_2, x_3]$, be the ring of polynomials in four indeterminates over k. We can think of any polynomial in R as a function in $k[V]$. In order to find the value of $f(x_0, x_1, x_2, x_3) \in R$ at $v = (a_0, a_1, a_2, a_3) \in V$ we just substitute x_i with a_i for all i. Thus, there is an homomorphism from R to $k[V]$ that maps every polynomial to a function. One can prove that this homomorphism is in fact an isomorphism between R/I and $k[V]$, where I is the ideal generated by $\{(x_0^q - x_0), (x_1^q - x_1), (x_2^q - x_2), (x_3^q - x_3)\}$.

For each $f + I \in R/I$, there is a unique polynomial representative $f^* \in R$ such that each indeterminate in f^* is of degree less than or equal to $q-1$ and $f+I = f^*+I$. Let R^* be the set of all such representatives.

Definition 11. *A term of an element $f + I$ of R/I is a monomial of its representative f^* in R^*.*

Example 3. *Suppose $q = 2^t$ and $t > 2$. Let*

$$f + I = (x_0^{q+1}\, x_1\, x_2 + x_0^{q-1}\, x_1^{q+3}\, x_3^{q+2}) + I \ \in R/I$$

Then,

$$f^* = x_0\, x_1\, x_2 + x_0^{q-1}\, x_1^3\, x_3^2.$$

So, $x_0\, x_1\, x_2$ and $x_0^{q-1}\, x_1^3\, x_3^2$ are the terms of $f + I$.

Let $k[V \setminus \{0\}]$ be the space obtained by restricting functions of $k[V]$ to $V \setminus \{0\}$, and $k[V \setminus \{0\}]^{k^\times}$ be the subspace of $k[V \setminus \{0\}]$ fixed by $k^\times$. That is,

$$k[V \setminus \{0\}]^{k^\times} = \{f \in k[V \setminus \{0\}] |\ f(\lambda v) = f(v) \text{ for all } v \in V \setminus \{0\},\ \lambda \in k^\times\} \qquad (4\text{–}24)$$

Thus, for each $p = \langle v \rangle \in P$ the value of f on $p \setminus \{0\}$ will be constant. Hence f can be thought as a function on P. We can do this by projecting f on to the representatives of points in P. On the other hand, any function $f \in k[P]$ can be extended to a function $\bar{f} \in k[V \setminus \{0\}]^{k^\times}$ by defining the value of $\bar{f}(v)$ to be the same as $f(p)$, where p is the point so that $v \in p$. Thus, there is a one to one correspondence between $k[P]$ and $k[V \setminus \{0\}]^{k^\times}$, and $k[P]$ can be embedded into $k[V]^{k^\times}$.

Since $k[V] \simeq R/I$, there is a space R_P which is isomorphic to $k[P]$, and that can be embedded in to $(R/I)^{k^\times}$. Elements of R_P are classes of polynomials that map to $k[V]^{k^\times}$ under the isomorphism between R/I and $k[V]$. Let $R_P^* \subseteq R^*$ be the set of representatives of elements of R_P. It is not difficult to see that for any element $g + I$ of R_P the unique representative g^* in R_P^* will be a homogeneous polynomial whose terms have degrees which are multiples of $(q-1)$. In this case, the set of monomials of the form $x_0^{m_0} x_1^{m_1} x_2^{m_2} x_3^{m_3}$ in

R_P^* where $m_0+m_1+m_2+m_3$ is a multiple of $(q-1)$ will map to a basis of R_P. Since these monomials are in R_P^*, each $m_i \leq q-1$.

For a point $p \in P$, let δ_p^* be the polynomial in R_P^* that corresponds to the characteristic function χ_p of p in $k[P]$. So,

$$\delta_p^*(v) = \begin{cases} 1 & \text{if } \langle v \rangle = p, \\ 0 & \text{if } \langle v \rangle \neq p. \end{cases} \tag{4–25}$$

For a line $\ell \in L$, let δ_ℓ^* be the polynomial in R_P^* that corresponds to the characteristic function χ_ℓ of ℓ in $k[P]$. So,

$$\delta_\ell^*(v) = \begin{cases} 1 & \text{if } \langle v \rangle \in \ell, \\ 0 & \text{if } \langle v \rangle \notin \ell. \end{cases} \tag{4–26}$$

Example 4. *Let $p_0 = (1:0:0:0)$ then $\delta_{p_0}^* = (1+x_1^{q-1})(1+x_2^{q-1})(1+x_3^{q-1})$ would be the polynomial that corresponds to the characteristic function χ_{p_0}.*

Example 5. *Let $\ell_0 = \langle (1:0:0:0), (0:1:0:0) \rangle$, then $\delta_{\ell_0}^* = (1+x_2^{q-1})(1+x_3^{q-1})$ would be the polynomial that corresponds to the characteristic function χ_{ℓ_0}.*

The automorphism group of the generalized quadrangle $W(q)$ is isomorphic to $Sp(4,q)$. Moreover, $Sp(4,q)$ acts transitively on the characteristic functions of the lines of L. so it also acts transitively on the classes of characteristic functions of lines in R_P. Hence, by applying the elements of $Sp(4,q)$ to $\delta_{\ell_0}^*$, we can obtain all q^3+q^2+q+1 polynomials corresponding to the characteristic functions of lines of L. The code $C(P,L)$ is spanned by the classes of these polynomials. So $C(P,L)$ is spanned by the classes of polynomials of the form

$$(1+(\sum_{i=0}^{3} a_i x_i)^{q-1})(1+(\sum_{i=0}^{3} b_i x_i)^{q-1}) + I, \tag{4–27}$$

where $a_i, b_i \in k$ such that the 2-dimensional subspace of V given by

$$a_0x_0 + a_1x_1 + a_2x_2 + a_3x_3 = 0 \text{ and } b_0x_0 + b_1x_1 + b_2x_2 + b_3x_3 = 0 \tag{4–28}$$

is a line in L. Therefore for $c + I \in C$, the representative c^* is a homogeneous polynomial whose terms have degrees $0, q-1$ or $2(q-1)$. We also note that the degree of any variable in c^* must be less than or equal to $q-1$.

4.5 Digitizable Polynomials in R^*

The method of this section was first introduced in [4].

Definition 12. *We call a polynomial $f \in R^*$ digitizable if it is possible to find square free homogeneous polynomials, f_i, called digits of f, so that $f = f_0 f_1^2 f_2^{2^2} \dots f_{t-1}^{2^{t-1}}$. In this case, we denote f as $[f_0, f_1, \dots f_{t-1}]$, and call this notation the 2-adic t-tuple of f.*

Example 6. *Every monomial $m = x_0^{m_0} x_1^{m_1} x_2^{m_2} x_3^{m_3}$ in R^* is digitizable. Since each $m_i \leq q-1$, we can find $n_{i,j} \in \{0,1\}$ such that;*

$$m_i = n_{i,0} + 2n_{i,1} + 2^2 n_{i,2} + \dots + 2^{t-1} n_{i,t-1} \quad \text{for all } i.$$

The 2-adic t-tuple for m is $[f_0, f_1, \dots, f_{t-1}]$ where $f_i = x_0^{n_{0,i}} x_1^{n_{1,i}} x_2^{n_{2,i}} x_3^{n_{3,i}}$ for all i.

Example 7. *For $q = 8$, $f = x_0^3 x_1 x_3^6 + x_0 x_1^3 x_2^2 x_3^4$ is digitizable with digits $f_0 = x_0 x_1$, $f_1 = x_0 x_3 + x_1 x_2$, $f_2 = x_3$. Note that,*

$$f = [x_0 x_1, x_0 x_3 + x_1 x_2, x_3] = [x_0 x_1, x_0 x_3, x_3] + [x_0 x_1, x_1 x_2, x_3].$$

Let us consider the set of digits,

$$D = \{1, x_0, x_1, x_2, x_3, x_0 x_1, x_0 x_2, x_1 x_3, x_2 x_3, x_0 x_1 x_2, x_0 x_1 x_3, x_0 x_2 x_3, x_1 x_2 x_3, x_0 x_3 + x_1 x_2\}$$

We define,

$$\beta := \{[f_0, f_1, \dots, f_{t-1}] + I \mid f_i \in D \text{ for } 0 \leq i \leq t-1\} \tag{4–29}$$

Lemma 18. *The code $C(P, L)$ lies in the span of β.*

Proof. This just a special case of the theorem 5.2 in [4] with m=2 and r=2.

□

4.6 On the Kernel of the Projection Map

Let $k[P_1]$ denote the space of k-valued functions on P_1, and R_{P_1} be the space of classes of polynomials that corresponds to $k[P_1]$. As in the previous sections, we use $R^*_{P_1}$ to denote the set of unique representatives of the elements of R_{P_1}.

In this section we will find the dimension of $C(P,L) \cap ker\, \pi_{P_1}$, where $\pi_{P_1} : R_P \to R_{P_1}$ is the projection map. Elements of $ker\, \pi_{P_1}$ are the classes of polynomials whose values at the points of P_1 are zero. We know that

$$P_1 = \{(a : b : c : 1) | a, b, c \in \mathbb{F}_q\} \tag{4–30}$$

Thus, any element of the form $(1 + x_3^{q-1})f + I$ in R_P is in the kernel. On the other hand, $f + I = (x_3^{q-1} + 1)f + I$ for any class $f + I \in ker\, \pi_{P_1}$. This is because for any point $p \in P$, the value of $(x_3^{q-1} + 1)f$ is zero if $p \in P_1$, and $f(p)$ otherwise.

Lemma 19. *Any element of $ker\, \pi_{P_1}$ can be written in the form $(1 + x_3^{q-1})h + I$ where h is in R^*_P and h does not contain indeterminate x_3.*

Proof. Let $(x_3^{q-1} + 1)f + I$, $f \in R^*_p$, be an element of $ker \pi_{P_1}$. Since $x_3^q = x_3$,

$$x_3^{q-1}(x_0^i x_1^j x_2^k x_3^l) + I = x_0^i x_1^j x_2^k x_3^l + I, \text{ for } l \geq 1.$$

Thus, any term of $f + I$ that contains x_3 is invariant under multiplication by x_3^{q-1}. Hence, the terms with x_3 will disappear in the expansion $(x_3^{q-1} f + f) + I$. So, we can find a polynomial h without indeterminate x_3 and $(x_3^{q-1} + 1)f + I = (x_3^{q-1} + 1)h + I$.

□

For the rest of the section we fix an element $r + I$ of $ker \pi_{P_1} \cap C(P,L)$. Let r^* be its unique representative in R^*_P. Since $r^* + I$ is in the kernel, $r^* = (1 + x_3^{q-1})h(x_0, x_1, x_2)$ for some $h \in R^*_P$. Since $r^* + I$ is also in $C(P,L)$, and $C(P,L)$ is spanned by the characteristic functions of the lines, the terms of $r^* + I$ have degrees $0, q-1$ or $2(q-1)$. We also know by the lemma 18 that $r^* + I$ is in the span of β.

Lemma 20. *The degree of the digits of any non-constant monomial of h is 1.*

Proof. Let m be a non-constant monomial of h. Then $m = [g_0, g_1, \ldots, g_{t-1}]$ for some $g_i = x_0^{n_{0,i}} x_1^{n_{1,i}} x_2^{n_{2,i}}$, where $n_{j,i} \in \{0, 1\}$. Let $deg(g_i) = k_i$ for each i. Hence $x_3^{q-1} m = [x_3 g_0, x_3 g_1, \ldots, x_3 g_{t-1}]$ is a t-tuple of a monomial of r^*. Since $r^* + I$ is in the span of β, the digits of $x_3^{q-1} m$ cannot have degrees greater than 3. Thus, $k_i = 0, 1,$ or2 for each i.

Since $r^* + I$ is in $C(P, L)$, and $x_3^{q-1} m$ is a monomial of r^*, the degree of $x_3^{q-1} m$ is $q - 1$ or $2(q - 1)$. Since m is non-constant, $deg(m) = q - 1$. Hence,

$$k_0 + 2k_1 + \ldots 2^{t-1} k_{t-1} = 2^t - 1. \tag{4–31}$$

Since $2^t - 1$ is an odd number, $k_0 = 1$. Then we get

$$k_1 + 2k_2 + \ldots + 2^{t-2} k_{t-1} = 2^{t-1} - 1 \tag{4–32}$$

and so $k_1 = 1$. We repeat this process until we get $k_i = 1$ for all i.

□

Lemma 21. *h is in the span of the set*

$$\{[1, 1, \ldots, 1]\} \cup \{[g_0, \ldots, g_{t-1}] |\ g_i \in \{x_1, x_2\},\ \textit{for } 0 \leq i \leq t\}. \tag{4–33}$$

Proof. It is enough to show that h does not contain the variable x_0.

Suppose one of the monomials, say $[g_0, \ldots, g_{t-1}]$, of h has x_0 in it. So $g_i = x_0$ for some i. Then,

$$x_3^{q-1} [g_0, g_1, \ldots, g_{i-1}, x_0, \ldots, g_{t-1}] = [g_0 x_3, g_1 x_3, \ldots, g_{i-1} x_3, x_0 x_3, \ldots, g_{t-1} x_3] \tag{4–34}$$

is a monomial in r^*. We know that r^* is a linear combination of the elements of β, so, r^* should also contain the monomial

$$[g_0 x_3, g_1 x_3, \ldots, g_{i-1} x_3, x_1 x_2, \ldots, g_{t-1} x_3]. \tag{4–35}$$

Note that the degree of x_3 in this monomial is different from 0 or $q - 1$. However this is impossible since $r^* = x_3^{q-1} h + h$, the degree of x_3 in any monomial of r^* must be either 0

or $q-1$. Thus, r^* can not contain the monomial in (4–35). Hence, h does not contain the indeterminate x_0.

□

Corollary 22. $\dim(ker\pi_{P_1} \cap C(P,L)) = q+1$.

Proof. Since $X \subseteq ker\pi_{P_1} \cap C(P,L)$, and elements of X are linearly independent, $\dim(ker\pi_{R_{P_1}} \cap C) \geq q+1$.

Any element of $ker\pi_{R_{P_1}} \cap C(P,L)$ is of the form $(1+x_3^{q-1})h+I$, where, by the previous lemma, h lies in space of dimension at most $q+1$. Thus, $\dim(ker\pi_{P_1} \cap C(P,L)) = q+1$.

□

The following lemma was proven in [22], the proof works the same for the even case also.

Lemma 23. *$ker\pi_{P_1} \cap C(P,L_1)$ has dimension $q-1$; it has a basis consisting of the functions and having as basis the set of functions $\chi_\ell - \chi_{\ell'}$ where $\ell \neq \ell_0$ is an arbitrary but fixed line through p_0 and ℓ' varies over the $q-1$ lines through p_0 different from ℓ_0 and ℓ.*

Proof. By Lemma 15 applied to p_0, we see that if ℓ and ℓ' are any two lines through p_0 other than ℓ_0, the function $\chi_\ell - \chi_{\ell'}$ lies in $C(P,L_1)$. It is also in $ker\pi_{P_1}$. Thus, we can find $q-1$ linearly independent functions of this kind as described in the statement. Then the dimension of $ker\pi_{P_1} \cap C(P,L_1)$ is greater than or equal to $q-1$. On the other hand, since none of the lines in L_1 has a common point with ℓ_0, $C(P,L_1)$ is in the kernel of the restriction map to ℓ_0, while the image of the restriction of $ker\pi_{P_1} \cap C(P,L)$ to ℓ_0 has dimension 2, spanned by the images of χ_{ℓ_0} and χ_{p_0}. Thus, $ker\pi_{P_1} \cap C(P,L_1)$ has codimension at least 2 in $ker\pi_{P_1} \cap C(P,L)$, which has dimension $q+1$, by Corollary 12. Hence,

$$\dim\left(ker\pi_{P_1} \cap C(P,L_1)\right) \leq q-1. \tag{4–36}$$

□

Corollary 24. *The spans of $Z \cup X_0$ and $L_1 \cup X_0$ are the same.*

Proof. Let α be an element in the span of L_1. Since Z maps to a basis of $C(P_1, L_1)$, there is an element α' in the span of Z so that $\pi_{P_1}(\alpha) = \pi_{P_1}(\alpha')$. Hence, $\alpha - \alpha' \in ker\pi_{P_1} \cap C(P, L_1)$. By the previous lemma, $ker\pi_{P_1} \cap C(P, L_1)$ is contained in the span of X_0. Hence, we conclude that α is contained in the span of $X_0 \cup Z$.

□

Therefore, $Z \cup X_0 \cup Y$ spans $C(P, L)$ as a vector space. So,

$$\dim(C(P, L)) \leq \dim(C(P_1, L_1)) + 2q \tag{4–37}$$

and this implies

$$\dim LU(3, q) = q^3 - \dim(C(P, L)) + 2q. \tag{4–38}$$

REFERENCES

[1] B. Bagchi, A. Brouwer, H. Wilbrink, Notes on binary codes related to the o(5,q) generalized quadrangle for odd q, Gemonetriae Dedicata 39 (1991) 339–355.

[2] F. Buekenhout (ed.), Handbook of Incidence Geometry, Elsevier Science B.V., The Netherlands, 1995.

[3] P. Cameron, J. V. Lint, Graphs, Codes and Designs, Cambridge University Press, Cambridge, 1980.

[4] D. Chandler, P. Sin, Q. Xiang, Incidence modules for symplectic spaces in characteristic two, arXiv:math/0801.439201 (2008).

[5] P. Dembowski, Finite Geometries, Springer-Verlag, New York, 1968.

[6] J. E.F. Assmus, J. Key, Designs and Their Codes, Cambridge University Press, Cambridge, 1992.

[7] R. Gallager, Low-density parity-check codes, IRE Trans. Information Theory IT-8 (1962) 21–28.

[8] J. Goethals, P. Delsarte, On a class of majority-logic decodable cyclic codes, IEEE Trans. Information Theory 14 (1968) 182–188.

[9] R. Graham, F. MacWilliams, On the number of information symbols in difference-set cyclic codes, Bell System Tech. J. 45 (1966) 1057–1070.

[10] N. Hamada, The rank of the incidence matrix of points and d-flats in finite geometries, J. Sci. Hiroshima Univ. Ser. A-I 32 (1968) 381–396.

[11] N. Hamada, On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error correcting codes, Hiroshima Math. J. 3 (1973) 153–226.

[12] J. Hirschfeld, Projective Geometries Over Finite Fields, Oxford University Press, New York, 1979.

[13] J.-L. Kim, U. Peled, I. Pereplitsa, V. Pless, S. Friedland, Explicit construction of ldpc codes with no 4-cycles, IEEE Trans. Information Theory 50 (2004) 2378–2388.

[14] Y. Kuo, S. Lin, M. Fossorier, Low-density parity-check codes based on finite geometries: a rediscovery and new results, IEEE Trans. Information Theory 47 (2001) 2711–2736.

[15] F. Lazebnik, V. Ustimenko, Explicit construction of graphs with arbitrarily large girth and of size, Discrete Applied Math. 60 (1997) 275–284.

[16] F. Lazebnik, A. Woldar, General properties of some families of graphs defined by systems of equations, J. Graph Theory 38 (2001) 65–86.

[17] F. MacWilliams, H. Mann, On the p-rank of the design matrix of a difference set, Inform. and Control 12 (1968) 474–489.

[18] R. McEliece, The Theory of Information and Coding, Cambridge University Press, Cambridge, 2002.

[19] S. Payne, J. Thas, Finite Generalized Quadrangles, Pittman Advanced Publishing Program, Boston, 1984.

[20] N. Sastry, P. Sin, The code of a regular generalized quadrangle of even order, Proc. Symposia in Pure Mathematics 63 (1998) 485–496.

[21] P. Sin, The p-rank of the incidence matrix of intersecting linear subspaces, Designs Codes and Cryptography 31 (2004) 213–220.

[22] P. Sin, Q. Xiang, On the dimensions of certain ldpc codes based on q-regular bipartite graphs, IEEE Trans. Information Theory 52(8) (2006) 3735–3737.

[23] K. Smith, On the p-rank of the incidence matrix of points and hyperplanes in a finite projective geometry, Journal of Combinatorial Theory 7 (1969) 122–129.

[24] R. Tanner, A recursive approach to low complexity codes, IEEE Trans. Information Theory IT-27 (1981) 533–547.

[25] J. Tits, Sur la trialite et certains groupes qui s'en deduisent, Inst. Hautes Etudes Sci. Publ. Math. 2 (1959) 14–60.

BIOGRAPHICAL SKETCH

Ogul Arslan was born in 1975 in Turkey. She received a Bachelor of Science degree in mathematics education in 1997 from Middle East Technical University in Ankara. After graduation, Ogul worked as a high school mathematics teacher in Ankara for several years. She started graduate school at Wayne State University in 2002 and received a Master of Arts degree in mathematics in 2004. In the fall of 2004, Ogul started graduate school at University of Florida. She was awarded a Ph.D. degree in mathematics from University of Florida in August 2009.