THE DIMENSIONS OF LU(3,q) CODES
OGUL ARSLAN
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF FLORIDA

ABSTRACT: A family of LDPC codes, called LU(3,q) codes, has been constructed from q-
regular bipartite graphs. Recently, P. Sin and Q. Xiang determined the dimensions of these codes in the case that q is a power of an odd prime. They also obtained a lower bound for the dimension of an LU(3,q) code when q is a power of 2. In this paper we prove that this lower bound is the exact dimension of the LU(3,q) code. The proof involves the geometry of symplectic generalized quadrangles, the representation theory of Sp(4,q), and the ring of polynomials.

1. Introduction

Let $P^*$ and $L^*$ be two sets in bijection with $\mathbb{F}_q^3$, where $q$ is any prime power. In [4], an element $(a, b, c) \in P^*$ is defined to be incident with an element $[x, y, z] \in L^*$ if and only if $y = ax + b$ and $z = ay + c$. The binary incidence matrix with rows indexed by $P^*$ and columns indexed by $L^*$ is denoted by $H(3,q)$. The two binary codes having $H(3,q)$ and its transpose as parity check matrices are called $LU(3,q)$ codes in [4].

Let $V$ be a 4-dimensional vector space over the field $\mathbb{F}_q$ of $q$ elements. We assume that $V$ has an alternating bilinear form $(v, v')$, that is, $(v, v')$ is linear in both components and $(v, v) = 0$ for all $v$. Let $Sp(4,q)$ be the symplectic group of linear automorphisms preserving this form. We pick a symplectic basis $e_0, e_1, e_2, e_3$ of $V$.

We denote by $P$, the projective space $P(V)$, the space of one dimensional subspaces of $V$. These one-dimensional subspaces are called the points of $P$. 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 $V$, called the lines in $P$. The pair $(P, L)$, with the natural relation of incidence between the lines and points is called the symplectic generalized quadrangle. We can see that given any line $\ell$ and a point $p$ not on that line there is a unique line that passes through $p$ and intersects $\ell$.

We 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 $\overline{p}^\perp$ to be the set of points on all the lines that passes through $p$. Thus, $\overline{p_0}^\perp = \{(a : b : c : d) \mid (a, b, c, d) \in \mathbb{F}_q \}$, where $a : b : c : d$ is the homogeneous coordinates of a point. Let $P_1$ be the set of points not in $\overline{p_0}^\perp$ and $L_1$ be the set of lines which does not intersect $\ell_0$. We can also talk about the incidence systems $(P_1, L_1)$, $(P, L_1)$ and $(P_1, L)$. We denote by $M(P, L)$ the incidence matrix whose rows 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 $M(P, L)$. It was proven in [7, appendix] that the incidence systems $(P^*, L^*)$ and $(P_1, L_1)$ are equivalent. Hence, $M(P_1, L_1)$ and its transpose are parity check matrices for $LU(3,q)$ codes.

The 2-rank of $M(P, L)$ and $M(P_1, L_1)$ for $q$ a power of an odd prime, were proven to be $\frac{q^3 - 2q^2 + q + 2}{2}$ and $\frac{q^3 + q^2 - 3q + 2}{2}$ in [1, theorem 9.4] and [7, theorem1.1] respectively.

The formulas for the case where $q$ is a power of 2 is quite different. It was proven in [6, theorem 1] that the 2-rank of $M(P, L)$ is $1 + \left(\frac{1+\sqrt{17}}{2}\right)^{2t} + \left(\frac{1-\sqrt{17}}{2}\right)^{2t} - 2^{t+1}$.

In this paper we prove the following theorem.

**Theorem 1.** Assume $q = 2^t$ for some positive integer $t$. The 2-rank of $M(P_1, L_1)$ equals $1 + \left(\frac{1+\sqrt{17}}{2}\right)^{2t} + \left(\frac{1-\sqrt{17}}{2}\right)^{2t} - 2^{t+1}$.

The above formula was conjectured in [7] based on the computer calculations of J.-L. Kim.

P. Sin and Q. Xiang proved in [7, appendix] that $(P_1, L_1)$ and $(P^*, L^*)$ are equivalent incidence systems. Hence, $M(P_1, L_1)$ is a parity check matrix of the $LU(3,q)$ code given by the transpose of $H(3,q)$ and by theorem 1 above we get the following corollary.

**Corollary 2.** If $q = 2^t$, then the dimension of $LU(3,q)$ is $2^{3t} + 2^{t+1} - 1 - \left(\frac{1+\sqrt{17}}{2}\right)^{2t} - \left(\frac{1-\sqrt{17}}{2}\right)^{2t}$.
The dimension of \( LU(3, q) \) code for \( q \) a power of an odd prime was proven to be \( \frac{q^3 - 2q^2 + 3q - 2}{2} \) in [7].

For the rest of the section we can assume that \( q \) is an arbitrary prime power.

We denote by \( \mathbb{F}_q[P] \) the space of \( \mathbb{F}_q \) valued functions on \( P \). We can think of elements of \( \mathbb{F}_q[P] \) 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. The characteristic function \( \chi_p \) for a point \( p \in P \) is the function whose value is 1 at \( p \), and zero at any other point. Thus, \( \chi_p \) 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. The characteristic functions for all the points in \( P \) forms a basis for \( \mathbb{F}_q[P] \). For any line \( \ell \in L \), the characteristic function \( \chi_\ell \) is the function given by the sum of \( q + 1 \) characteristic functions of the points of \( \ell \). The subspace of \( \mathbb{F}_q[P] \) spanned by all the \( \chi_\ell \) is the \( \mathbb{F}_q \) code of \((P, L)\), denoted by \( C(P, L) \). We can think of it as the column space of \( M(P, L) \). Most of the time we will not make a distinction between the lines and the characteristic functions of the lines. For example, we will say, let \( C(P, L_1) \) be the subspace of \( \mathbb{F}_q[P] \) spanned by the lines of \( L_1 \). Let \( C(P_1, L_1) \) denote the code of \((P_1, L_1)\) viewed as a subspace of \( \mathbb{F}_q[P_1] \), and let \( C(P_1, L) \) be the larger subspace of \( \mathbb{F}_q[P_1] \) spanned by the restrictions to \( P_1 \) of the characteristic functions of all lines of \( L \).

We consider the natural projection map \( \pi_{P_1} : \mathbb{F}_q[P] \rightarrow \mathbb{F}_q[P_1] \) given by the restriction of functions to \( P_1 \). We denote its kernel by \( \ker \pi_{P_1} \).

Let \( Z \subseteq C(P, L_1) \) be a set of characteristic functions of lines in \( L_1 \) which maps bijectively under \( \pi_{P_1} \) to a basis of \( C(P_1, L_1) \). Let \( X \) be the set of characteristic functions of the \( q + 1 \) lines passing through \( p_0 \), and let \( X_0 = X \setminus \ell_0 \). Furthermore, we pick \( q \) lines that intersect \( \ell_0 \) at \( q \) distinct points except \( p_0 \), and call the set of these lines as \( Y \). These sets \( X, Y, \) and \( Z \) are disjoint, also note that \( X \subset \ker \pi_{P_1} \).

The following lemma and corollary were proven in [7].

**Lemma 3.** \( Z \cup X_0 \cup Y \) is linearly independent over \( \mathbb{F}_q \).

Hence, \( |X_0 \cup Y| = 2q \), while \( |Z| = \dim_{\mathbb{F}_q} C(P_1, L_1) \).

**Corollary 4.** Let \( q \) be an arbitrary prime power. Then \( \dim_{\mathbb{F}_q} LU(3, q) \geq \frac{q^3 - q^2 - q + 1}{2} \).

The proof of Theorem 1 will be completed if we can show that \( X_0 \cup Y \cup Z \) spans \( C(P, L) \) as a vector space over \( \mathbb{F}_q \). In section 2 we prove that \( X_0 \cup Y \cup L_1 \) spans \( C(P, L) \). Then we show in section 3 that the span of \( X_0 \cup Y \cup L_1 \) and \( X_0 \cup Y \cup Z \) are the same.

2. THE GRID OF LINES

**Lemma 5.** Let \( \ell \) and \( \ell' \) be two lines passing through \( p \in \ell_0 \). Then \( \chi_\ell - \chi_{\ell'} \in C(P, L_1) \).

**Proof.** We first prove that there exist lines \( h_\beta \) and \( v_\gamma \), for \( \beta, \gamma \in \mathbb{F}_q^\times \) so that each \( h_\beta \) is parallel to \( \ell \) and intersect \( \ell' \) at a distinct point and each \( v_\gamma \) is parallel to \( \ell' \) and intersect \( \ell \) at a different point. Moreover, for all \( \beta, \gamma \in \mathbb{F}_q^\times \), \( h_\beta \cap v_\gamma \neq \emptyset \) (i.e. there is a grid of lines).

Pick \( p^* \notin \ell \cup \ell' \cup \ell_0 \). By quadrangle properties there is a unique line, \( v_0 \), through \( p^* \) that intersect \( \ell \) at a point, \( p_1 \). Similarly, there is a unique line, \( h_0 \), through \( p^* \) that intersect \( \ell' \) at a point, \( p_2 \).
There are $a, b, c, d \in V$ so that $p_1 = \langle a \rangle$, $p_2 = \langle b \rangle$, $p^* = \langle c \rangle$ and $p = \langle e \rangle$, and $(a, b) = (e, c) = 1$.

Since $v_0 = \langle a, c \rangle$ and $h_0 = \langle b, c \rangle$, the points on $v_0 \setminus (\ell \cup p^*)$ and $h_0 \setminus (\ell^* \cup p^*)$ are of the form $\langle c + \alpha a \rangle$ and $\langle c + \gamma b \rangle$ for some $\beta, \gamma \in \mathbb{F}_q^*$, respectively.

For each point $\langle c + \alpha a \rangle \in v_0$ there is a unique line through it that intersect $\ell'$ at a point $\langle b + \alpha e \rangle$, for some $\alpha \in \mathbb{F}_q$. 

![Diagram](image_url)

Since $(\cdot, \cdot)$ was bilinear, and $\alpha, \beta \in \mathbb{F}_q^*$:

$0 = \langle c + \beta a, b + \alpha e \rangle = \langle c, b + \alpha e \rangle + \langle \beta a, b + \alpha e \rangle$

$0 = \langle c, b \rangle + \langle c, \alpha e \rangle + \langle \beta a, b \rangle + \langle \beta a, \alpha e \rangle$

$0 = \alpha \langle c, e \rangle + \beta \langle a, b \rangle$

Thus $\alpha = -\beta$ in $\mathbb{F}_q$. Then for $\beta \in \mathbb{F}_q^*$, the line through $\langle c + \alpha a \rangle$ that intersect $\ell'$ is $h_\beta = \langle c + \beta a, b - \beta e \rangle$.

Similarly, we can show that for $\gamma \in \mathbb{F}_q^*$, the line through $\langle c + \gamma b \rangle$ that intersect $\ell$ is $v_\gamma = \langle c + \gamma b, a - \gamma e \rangle$.

Note that, for all $\beta, \gamma \in \mathbb{F}_q^*$, $h_\beta$ and $v_\gamma$ are in $L_1$. Furthermore, for any $\beta_1, \beta_2, \gamma_1, \gamma_2 \in \mathbb{F}_q^*$ we have $h_{\beta_1} \cap h_{\beta_2} = \emptyset$ and $v_{\gamma_1} \cap v_{\gamma_2} = \emptyset$, these lines can be thought as horizontal and vertical lines.

Now we pick two lines $v_{\gamma'}$ and $h_{\beta'}$ for some $\gamma', \beta' \in \mathbb{F}_q^*$. We want to show that these two lines intersect. Note that, by the above calculations, $h_{\beta'} = \langle c + \beta' a, b - \beta' e \rangle$ and $v_{\gamma'} = \langle c + \gamma' b, a - \gamma' e \rangle$. 


Now, pick the point \( s = (c + \beta a + \gamma (b - \beta e)) \in h_{\beta'}. \) Let \( t = (c + \gamma b + \alpha (a - \gamma e)) \) be an arbitrary point on \( v_{\gamma'} \setminus \ell. \) Then, 
\[
(s, t) = ((c + \beta a + \gamma (b - \beta e), (c + \gamma b + \alpha (a - \gamma e))) \\
= (c + \beta a, c + \gamma b) + \alpha (c + \beta a, a - \gamma e) + \gamma (b - \beta e, c + \gamma b) + \gamma' (b - \beta e, a - \gamma e) \\
= \beta \gamma' (a, b) + \alpha \gamma (c, e) - \gamma' \beta' (e, c) + \gamma' \alpha (b, a) = 0
\]
Therefore, \( v_{\gamma} \) and \( h_{\beta'} \) intersect at \( s, \) and by quadrangle properties this is the only point of intersection. Hence, \( v_{\gamma} \) intersect \( h_{\beta} \) for each \( \gamma, \beta \in \mathbb{F}_q^*. \) So, we have a grid of lines, where each \( h_{\beta} \) and \( v_{\gamma} \) is in \( L_1 \) for each \( \beta, \gamma \in \mathbb{F}_q. \)

Finally we add characteristic functions of these lines and get:

\[
\sum_{\gamma \in \mathbb{F}_q} \chi_{v_{\gamma}} + \sum_{\beta \in \mathbb{F}_q} \chi_{h_{\beta}} = \chi_{\ell} - \chi_{\ell'} \in C(P, L_1).
\]

**Lemma 6.** For any choice of \( Y, \) \( \ell \in L \setminus \{\ell_0\} \) and \( 1 \) are in the span of \( X_0 \cup Y \cup L_1. \)

**Proof.** It is enough to show that any line, \( \ell, \) in \( L \setminus (X \cup L_1) \) is in the span of \( X_0 \cup Y \cup L_1. \) It is immediate that \( \ell \) intersects \( \ell_0 \) at a point \( p \) other than \( p_0. \) Let \( \ell' \) be the line in \( Y \) that intersect \( \ell_0 \) 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 \( \ell^*. \) Since \( \ell^* \) does not intersect \( \ell_0, \ell^* \) and all the lines that intersect \( \ell^* \) are in \( (X_0, Y, L_1). \) If \( q \) is even we add these lines, including \( \ell^* \), to get \( 1, \) otherwise, we add all these lines except \( \ell^* \) itself and get \( 1. \)

**Lemma 7.** For \( q = 2^k, \) \( \ell_0 \) is in the span of \( X_0 \cup Y \cup L_1. \)

**Proof.**

\[
\chi_{\ell_0} = 1 - \sum_{\ell \cap \ell_0 \neq \emptyset, \ell \neq \ell_0} \chi_{\ell} \in (X_0, Y, L_1).
\]
3. The Polynomial Approach

Unless otherwise stated, we assume \( q = 2^i \), \( k = \mathbb{F}_q \) in this section.

Consider the space, \( k[V] \), of \( k \)-valued functions on \( V \), where the elements of this space are vectors with \( q^i \) components on \( k \).

Let \( R = k[x_0, x_1, x_2, x_3] \), be the ring of polynomials in four indeterminates. 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. We 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 an 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. By a term of an element \( f + I \) of \( R/I \) we mean a monomial of its representative \( f^* \) in \( R^* \).

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 \( k^\times \). For any \( v \in V \setminus \{0\} \), \( f \in k[V \setminus \{0\}]^{k^\times} \) and \( \lambda \in k^\times \) we have \( f(\lambda v) = f(v) \). Thus, for each \( p = (v) \in P \) the value of \( f \) on \( p \setminus \{0\} \) will be constant. Hence \( f \) can be thought as a function on \( P \). On the other hand, any function \( f \in k[P] \) can be extended to a function \( f \in k[V \setminus \{0\}]^{k^\times} \) by defining the value of \( f(v) \) 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 in to \( k[V \setminus \{0\}]^{k^\times} \).

Since \( k[V] \cong R/I \), 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. Let \( R^*_P \subseteq R^* \) be the set of representatives of \( R_P \). For any element \( g + I \) of \( R_P \) the unique representative \( g^* \) in \( R^*_P \) will be a homogeneous polynomial whose terms have degrees multiples of \( (q - 1) \). In this case, the set of monomials of the form \( x_0^{m_0} x_1^{m_1} x_2^{m_2} x_3^{m_3} \) where \( m_0 + m_1 + m_2 + m_3 = n(q - 1) \) in \( R^*_P \) will map to a basis of \( R_P \). Being in \( R^*_P \), each \( m_i \leq q - 1 \).

For a point \( p \in P \), let \( \delta^*_p \) be the polynomial in \( R^*_P \) that corresponds to the characteristic function \( \chi_p \) of \( p \) in \( k[P] \). So;

\[
\delta^*_p(p_i) = \begin{cases} 1 & \text{if } p_i = p, \\ 0 & \text{if } p_i \neq p. \end{cases}
\]

For a line \( \ell \in L \), let \( \delta^*_\ell \) be the polynomial in \( R^*_P \) that corresponds to the characteristic function \( \chi_\ell \) of \( \ell \) in \( k[P] \). So;

\[
\delta^*_\ell(p) = \begin{cases} 1 & \text{if } p \in \ell, \\ 0 & \text{if } p \notin \ell. \end{cases}
\]

**Example:** Let \( \ell_0 = (1 : 0 : 0 : 0), (0 : 1 : 0 : 0) \), then \( \delta^*_\ell_0 = (1 + x_2^{q-1})(1 + x_3^{q-1}) \) would be the characteristic function for \( \ell_0 \).

The symplectic group \( Sp(4,q) \) 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 \((1 + \sum_{i=0}^{3} a_i x_i^{q-1})(1 + \sum_{i=0}^{3} b_i x_i^{q-1}) + I\), for some \( a_i, b_i \in k \) so that \((a_0 : a_1 : a_2 : a_3), (b_0 : \ldots \right)
3.1. Another way of representing the polynomials in $R^*$:

The method of this section was first introduced in [2].

**Definition:** 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 $f = f_0 f_1^2 f_2^3 \ldots f_{t-1}^i$. In this case, we denote $f$ as $[f_0, f_1, \ldots, f_{t-1}]$, and call this notation the $2$-adic t-tuple of $f$.

**Example:** Every monomial $m = x_0^{n_0} x_1^{n_1} x_2^{n_2} x_3^{n_3}$ in $R^*$ is digitizable. Since each $m_i \leq q - 1$, we can find $n_{i,j} \in \{0, 1\}$ such that:

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

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

**Example:** For $q = 8$, $f = x_0^3 x_1^2 + x_0 x_1^2 x_2^2 x_3^4$ 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 $\beta := \{[f_1, f_2, \ldots, f_t] + I | f_i \in \{1, x_0, x_1, x_2, x_3, x_0 x_1, x_0 x_2, x_1 x_3, x_2 x_3, x_0 x_3 + x_1 x_2 \}\}$

**Lemma 8.** The code $C(P, L)$ lies in the span of $\beta$.

**Proof.** $C(P, L)$ is spanned by the classes of polynomials of the form $(1 + a^{q-1})(1 + b^{q-1}) + I$ where $a = a_0 x_0 + a_1 x_1 + a_2 x_2 + a_3 x_3$ and $b = b_0 x_0 + b_1 x_1 + b_2 x_2 + b_3 x_3$ for some $a_i, b_i \in k$, and $t = \{(a_0 : a_1 : a_2 : a_3), (b_0 : b_1 : b_2 : b_3)\} \subset L$.

We will show every summand of the right hand side of the expansion $(1 + a^{q-1})(1 + b^{q-1}) = a^{q-1} + b^{q-1} + a^{q-1} b^{q-1} + 1$ is in the span of $\beta$. By the same argument $a^{q-1} b^{q-1}$ is in the span of $\beta$ also.

In order to show that $a^{q-1} b^{q-1} = (ab)(ab)^2(ab)^3 \ldots (ab)^{q-2}$ is in the span of $\beta$, it is enough to show that if $a b$ have terms $c_1 x_0 x_2$ and $c_2 x_1 x_2$ for some $c_1, c_2 \in k$ then $c_1 = c_2$. The summand that has this kind of terms in $ab$ is $(a_0 x_0 + a_1 x_1 + a_2 x_2 + a_3 x_3)(b_0 x_0 + b_1 x_1 + b_2 x_2 + b_3 x_3) = (a_0 b_3 + b_0 a_3) x_0 x_3 + (a_1 b_2 + a_2 b_1) x_1 x_2$. Since $t$ was isotropic, $(a_0 b_3 + b_0 a_3) + (a_1 b_2 + a_2 b_1) = 0$

Thus, $a_0 b_3 + b_0 a_3 = a_1 b_2 + a_2 b_1$. Therefore $a^{q-1} b^{q-1}$ is in the span of $\beta$.

Since constant term $1$ in the expansion is also in the span of $\beta$, we conclude that $(1 + a^{q-1})(1 + b^{q-1})$ is in the span of $\beta$. \hfill $\Box$

3.2. The kernel:

$k[P_1]$ is the space of $k$ valued functions on $P_1$. Let $R_{P_1}$ be the space of classes of polynomials that corresponds to $k[P_1]$. As before we use $R_{P_1}$ to denote the set of unique representatives of elements of $R_{P_1}$.

In this section we will find the dimension of $C(P, L) \cap \ker \pi_{P_1}$, where $\pi_{P_1} : R_{P} \rightarrow R_{P_1}$ 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. Any element of the form $(1 + a^{q-1})f + I$ 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 $p$, the value of $(x_3^{q-1} + 1)f$ is zero if $p \in P_1$, and $f(p)$ otherwise.
Lemma 9. Any element of \( \ker \pi_P \) 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 \( \ker \pi_P \). Since \(x_3^3 = x_3\), we get \(x_3^{q-1}(x_0^3 x_1^1 x_2^1 x_3^1) + I = x_0 x_1 x_2 x_3 + I\), for \(\ell \geq 1\). Thus, any term of \(f + I\) that contain \(x_3\) is invariant under multiplication by \(x_3^{q-1}\). Hence, the terms with \(x_3\) will disappear in the expansion \((x_3^{q-1} + 1)f + I\). So, we can find a polynomial \(h\) without indeterminate \(x_3\) and \((x_3^{q-1} + 1)f = \ker(1 + x_3^{q-1})h + I\).

3.3 The dimension of \(\ker \pi_P \cap C(P, L)\):

For the rest of the section we fix an element \(r + I\) of \( \ker \pi_P \cap C(P, L) \). 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 \(C(P, L)\), it is in the span of \(\beta\), and its terms have degrees \(0, q - 1\) or \(2(q - 1)\).

Lemma 10. The degree of the digits of any non-constant monomial, \(m\), of \(h\) is 1.

Proof. \(m = [g_0, g_1, \ldots, g_{t-1}]\) for some \(g_i = x_0^{n_i}, x_1^{n_i}, x_2^{n_i}, \ldots\), where \(n_{ij} \in \{0, 1\}\). 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 -tuple of monomials of \(r^*\). Since \(r^* + I\) is in the span of \(\beta\), these digits cannot have degrees greater than 2. Thus, \(k_i = 0\) or 1 for each \(i\).

Since \(x_3^{q-1} - m\) is in \(C(P, L)\), \(\deg(x_3^{q-1} - m) = 0, q - 1\) or \(2(q - 1)\). Since \(m\) is nonconstant, \(\deg(m) = k_0 + 2k_1 + 2^{t-1}k_{t-1} = 2^t - 1\). Since \(2^t - 1\) is an odd number, \(k_0 = 1\). Then we get \(k_1 + 2k_2 + \ldots + 2^{t-2}k_{t-1} = 2^{t-1} - 1\) and so \(k_1 = 1\). We repeat this process until we get \(k_i = 1\) for all \(i\).

Lemma 11. \(h\) is in the span of the set \([1, 1, \ldots, 1] \cup [g_i, \ldots, g_{t-1}]\), \(g_i \in \{x_1, x_2\}\), for \(0 \leq i \leq t\).

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

Suppose one of the monomials, say \([g_0, \ldots, g_{i-1}]\), of \(h\) has \(x_0\) in it. So \(g_i = x_0\) for some \(i\). Then, \(x_3^{q-1} [g_0, g_1, \ldots, x_0, \ldots, g_{t-1}] = [g_0 x_3, g_1 x_3, \ldots, x_0 x_3 + x_1 x_2, \ldots, g_{t-1} x_3]\) is in \(r^*\). We know that \(r^*\) is a linear combination of the elements of \(\beta\), so the coefficient of \([g_0 x_3, g_1 x_3, \ldots, x_0 x_3 + x_1 x_2, \ldots, g_{t-1} x_3]\) is non zero. Hence, \(r^*\) contains the monomial \([g_0 x_3, g_1 x_3, \ldots, x_1 x_2, \ldots, g_{t-1} x_3]\) also. Note that the degree of \(x_3\) in this monomial is different from \(0\) or \(q - 1\). However this is impossible since \(r^* = x_3^{q-1} - h\), the degree of \(x_3\) in any monomial of \(r^*\) is either \(0\) or \(q - 1\).

Corollary 12. \(\dim(\ker \pi_P \cap C(P, L)) = q + 1\).

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

Any element of \(\ker \pi_{R_P^*} \cap C(P, L)\) is of the form \((1 + x_3^{q-1})h + I\), where, by the previous lemma, \(h\) lies in space of dimension \(q + 1\). Thus, \(\dim(\ker \pi_P \cap C(P, L)) \leq q + 1\).

Following lemma was proven in [7], the proof works the same for even case also.

Lemma 13. \(\ker \pi_P \cap C(P_1, L_1)\) has dimension \(q - 1\) and basis the set of functions \(\chi_{\ell} - \chi_{\ell'}\) where \(\ell \neq \ell_0\) is an arbitrary but fixed line through \(p_0\) and \(\ell'\) varies over the \(q - 1\) lines through \(p_0\) different from \(\ell_0\) and \(\ell\).

Proof. By lemma 5 applied to \(p_0\), we see that if \(\ell\) and \(\ell'\) are any two lines through \(p_0\) other than \(\ell_0\), the function \(\chi_{\ell} - \chi_{\ell'}\) lies in \(C(P, L_1)\). It is also in \(\ker \pi_P\). Thus, we can find \(q - 1\) linearly independent functions of this kind as described in the statement. Then \(\ker \pi_{P_1} \cap C(P, L_1)\) has dimension \(\geq q - 1\). On the other hand, since none of the lines in \(L_1\) has a common point with \(\ell_0\), \(C(P, L_1)\) is in the kernel of the restriction map to \(\ell_0\), while the image of the restriction of \(\ker \pi_{P_1} \cap C(P, L_1)\) to \(\ell_0\) has dimension \(2\), spanned by the images of \(\chi_{\ell_0}\) and \(\chi_{p_0}\). 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 14. Hence, \(\dim(\ker \pi_P \cap C(P_1, L_1)) \leq q + 1 - 2 = q - 1\).
Corollary 14. The span of $Z \cup X_0$ and $L_1 \cup X_0$ are the same.

Proof. Let $\alpha$ 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 $\alpha'$ 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 $\ker \pi_{P_1} \cap C(P_1, L_1)$ is contained in the span of $X_0$. Hence, we conclude that $\alpha$ 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, $\dim(C(P, L)) \leq \dim(C(P_1, L_1)) + 2q$ and this implies $\dim LU(3, q) = q^3 - \dim(C(P, L)) + 2q$. 

\hfill \square
References:

[1] B. Bagchi, A.E. Brouwer, and H.A. Wilbrink, Notes on binary codes related to the O(5,q) generalized quadrangle for odd q, Geometriae Dedicata, vol. 39, 1991, pp. 339-355.

[2] D.B. Chandler, P. Sin, Q. Xiang, Incidence modules for symplectic spaces in characteristic two, preprint, arXiv:math/0801.4392v1.

[3] R. G. Gallager, Low-density parity-check codes, IRE Trans. Inform. Theory, vol. IT-8, Jan. 1962, pp. 21-28.

[4] J.-L. Kim, U. Peled, I. Pereplitsa, V. Pless, and S. Friedland, Explicit construction of LDPC codes with no 4-cycles, IEEE Trans. Inform. Theory, vol. 50, 2004, pp. 2378-2388.

[5] F. Lazebnik and V.A. Ustimenko, Explicit construction of graphs with arbitrarily large girth and of size, Discrete Applied Math., vol. 60, 1997, pp. 275-284.

[6] N.S.N. Sastry, P. Sin, The code of a regular generalized quadrangle of even order, Group Representations: Cohomology, Group Actions and Topology, ser. Proc. Symposia in Pure Mathematics, vol. 63, 1998, pp. 485-496.

[7] P. Sin, Q. Xiang, On the dimensions of certain LDPC codes based on q-regular bipartite graphs, IEEE Trans. Inform. Theory, vol. 52 (8), 2006, pp. 3735-3737.

Department of Mathematics, University of Florida, Gainesville, FL, 32611, USA
E-mail Address: ogul@math.ufl.edu