On the dimensions of certain LDPC codes based on 
q-regular bipartite graphs

Peter Sin and Qing Xiang

Abstract—An explicit construction of a family of binary LDPC codes 
called LU(3, q), where q is a power of a prime, was recently given. A 
conjecture was made for the dimensions of these codes when q is odd. The 
conjecture is proved in this note. The proof involves the geometry of 
a 1-dimensional symplectic vector space and the action of the symplectic group 
and its subgroups.

Index Terms—generalized quadrangle, incidence matrix, LDPC code, 
symplectic group.

I. INTRODUCTION

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 \( \langle v, v' \rangle \) and denote by \( \text{Sp}(V) \) the group of linear automorphisms of V which preserve this form. We choose a symplectic basis \( e_0, e_1, e_2, e_3 \) of V, with \( (e_i, e_{i+1}) = 1 \), for \( i = 0, 1 \).

Let \( P = V/(v) \) be the set of points of the projective space of V. A 
subspace of V is said to be totally isotropic if \( \langle v, v' \rangle = 0 \) whenever 
v and v’ are both in the subspace. Let L denote the set of totally 
isotropic 2-dimensional subspaces of V, considered as lines in P. The 
pair \((P, L)\), together with the natural relation of incidence between 
points and lines, is called the symplectic generalized quadrangle.

Except for in the appendix, the term “line” will always mean an 
element of L. It is easy to verify that \((P, L)\) satisfies the following 
quadrangle property: Given any line and any point not on the line, 
there is a unique line which passes through the given point and meets 
the given line.

Now fix a point \( p_0 \in P \) and a line \( \ell_0 \in L \) through \( p_0 \). We can 
assume that we chose our basis so that \( p_0 = (e_0) \) and \( \ell_0 = (e_0, e_1) \).

For \( p \in P \), denote by \( p^⊥ \) the set of points on lines through \( p \); 
\( p^* \in p^⊥ \) if and only if the subspace of V spanned by \( p \) and \( p^* \) 
is isotropic. Consider the set \( P_1 = P \setminus p^*_0 \) of points not collinear 
with \( p_0 \) and the set \( L_1 \) of lines which do not meet \( \ell_0 \). Then we 
can also consider the incidence systems \((P_1, L_1)\), \((P, L_1)\) and \((P_1, L)\).

Let \( M(P, L) \) and \( M(P_1, L_1) \) be the binary incidence matrices of 
the respective incidence systems, with rows indexed by points and 
columns by lines. The rows and columns of \( M(P, L) \) have weight 
q + 1 and, as a consequence of the quadrangle property, those of 
\( M(P_1, L_1) \) have weight q.

If q is odd we know by Theorem 9.4 of [1] that the 2-rank of 
\( M(P, L) \) is \( (q^3 + 2q^2 + q + 2)/2 \). Here we prove the following 
theorom.

Theorem 1.1: Assume q is a power of an odd prime. The 2-rank of 
\( M(P_1, L_1) \) equals \( (q^3 + 2q^2 - 3q + 2)/2 \).

In [2], a family of codes designated LU(3, q) was defined in the 
following way. Let \( P^* \) and \( L^* \) be sets in bijection with \( \mathbb{F}_q^3 \), 
where q is any prime power. An element \((a, b, c) \in P^* \) is incident 
with an element \([x, y, z] \in L^* \) if and only if
\[
y = ax + b \quad \text{and} \quad z = ay + c. \tag{1}
\]

The binary incidence matrix with rows indexed by \( L^* \) and columns 
indexed by \( P^* \) is denoted by \( H(3, q) \) and the two binary codes having 
\( H(3, q) \) and its transpose as parity check matrices are called LU(3, q) 
codes. The name comes from [3], where the bipartite graph with parts 
\( P^* \) and \( L^* \) and adjacency defined by the equations \ref{1} had been 
studied previously.

It is not difficult to show that the incidence systems \((P_1, L_1)\) and 
\((P^*, L^*)\) are equivalent. A detailed proof is given in the appendix. 
Thus, \( M(P_1, L_1) \) is a parity check matrix of the LU(3, q) code 
given by the transpose of \( H(3, q) \) and Theorem 1.1 has the following 
immediate corollary.

Corollary 1.2: If q is a power of an odd prime, the dimension of 
LU(3, q) is \( q^3 - 2q^2 + 3q - 2)/2 \).

The corollary was conjectured in [2]. There it was established that 
this number is a lower bound when q is an odd prime.

II. RELATIVE DIMENSIONS AND A LOWER BOUND FOR LU(3, q)

In this section q is an arbitrary prime power.

Let \( \mathbb{F}_2^q \) be the vector space of all \( \mathbb{F}_2 \)-valued functions on \( P \).

We can think of such a function as a vector in which the positions 
are indexed by the points of \( P \), and the entries are the values of 
the function at the points. For \( p \in P \), the characteristic function \( \chi_p \) 
is the vector with 1 in the position with index p and zero in the other 
positions. The set of all characteristic functions of points forms a 
basis of \( \mathbb{F}_2^q \). Let \( L \in L \). Its characteristic function \( \chi_L \in \mathbb{F}_2^q \) 
is the function which takes the value 1 at the q + 1 points of \( L \) and zero 
at all other points. The subspace of \( \mathbb{F}_2^q \) spanned by all the \( \chi_L \) is 
the \( \mathbb{F}_2 \)-code of \((P, L)\), denoted by \( C(P, L) \). One can think of \( C(P, L) \) 
as the column space of \( M(P, L) \). For brevity, we will sometimes 
blur the distinction between lines and their characteristic functions 
and speak, for instance, of the subspace of \( \mathbb{F}_2^q \) spanned by a set of 
lines. Let \( C(P_1, L_1) \) be the subspace of \( \mathbb{F}_2^q \) spanned by lines in \( L_1 \).

Let \( C(P_1, L_1) \) denote the code of \((P_1, L_1)\), viewed as a subspace of 
\( \mathbb{F}_2^q \), and let \( C(P_1, L) \) be the larger subspace of \( \mathbb{F}_2^q \) spanned 
by the restrictions to \( P_1 \) of the characteristic functions of all lines of 
\( L \).

Consider the natural projection map
\[
\pi_{P_1} : \mathbb{F}_2^q \rightarrow \mathbb{F}_2^q
\tag{2}
\]
given by restriction of functions. Its kernel will be denoted by 
\( \ker \pi_{P_1} \).

Let \( Z \subset C(P_1, L_1) \) 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 of \( L \) through 
\( p_0 \) and let \( X_0 = X \setminus \{\chi_{P_1}\} \). Finally, choose any q 
lines of \( L \) which meet \( \ell_0 \) in the q distinct points other than \( p_0 \) and let Y 
be the set of their characteristic functions. It is clear that the sets X, Y and 
\( Z \) are disjoint and that \( X \) is contained in \( \ker \pi_{P_1} \).

Lemma 2.1: \( Z \cup X_0 \cup Y \) is linearly independent over \( \mathbb{F}_2 \).

Proof: Each element of Y contains in its support a point of \( \ell_0 \) 
which is not in the support of any other element of \( Z \cup X_0 \cup Y \).
So it is enough to show that \( X_0 \cup Z \) is linearly independent. This is true 
because \( X_0 \) is a linearly independent subset of \( \ker \pi_{P_1} \) and \( Z \) maps 
bijectively under \( \pi_{P_1} \) to a linearly independent set.

We note that \( |Z| = \dim_{\mathbb{F}_2} C(P_1, L_1) \) and \( |X_0 \cup Y| = 2q \).

Corollary 2.2: Let q be an arbitrary prime power. Then
\[
\dim_{\mathbb{F}_2} LU(3, q) \geq q^3 - \dim_{\mathbb{F}_2} C(P, L) + 2q. \tag{3}
\]

Proof: From the definition of LU(3, q) and the equivalence of 
\((P^*, L^*) \) with \((P_1, L_1)\), we have
\[
\dim_{\mathbb{F}_2} LU(3, q) = q^3 - \dim_{\mathbb{F}_2} C(P_1, L_1). \tag{4}
\]

The corollary now follows from Lemma 2.1. 

P. Sin is with the Mathematics Department at the University of Florida. 
Q. Xiang is with the Mathematics Department at the University of 
Delaware. His work was supported by NSF grant DMS0400411.
III. Proof of Theorem 1.1

In this section we assume that $q$ is odd. In view of Corollary 2.2 and the known 2-rank of $M(P, L)$ the proof of Theorem 1.1 will be completed if we can show that $Z \cup X_0 \cup Y$ spans $C(P, L)$ as a vector space over $F_2$.

Lemma 3.1: Let $\ell \in L$. Then the sum of the characteristic functions of all lines which meet $\ell$ (excluding $\ell$ itself) is the constant function 1.

Proof: The function given by the sum takes the value $q \equiv 1$ (mod 2) at any point of $\ell$ and value 1 at any point off $\ell$, by the quadrangle property.

Lemma 3.2: Let $\ell \in L$ be a line, other than $\ell_0$, which meets $\ell_0$ at a point $p$. Let $\Phi_p$ be the sum of all the characteristic functions of lines in $L_1$ which meet $\ell$. Then

$$\Phi_p(p') = \begin{cases} 
0, & \text{if } p' = p; \\
q, & \text{if } p' \in \ell \setminus \{p\}; \\
0, & \text{if } p' \in P \setminus \ell; \\
1, & \text{if } p' \in P \setminus P^2.
\end{cases}$$

(5)

Proof: This is an immediate consequence of the quadrangle property.

Corollary 3.3: Let $p \in \ell_0$ and let $\ell, \ell'$ be two lines through $p$, neither equal to $\ell_0$. Then $\chi_\ell - \chi_{\ell'} \in C(P, L_1)$.

Proof: Since $q = 1$ in $F_2$, one easily check using Lemma 3.2 that

$$\chi_\ell - \chi_{\ell'} = \Phi_\ell - \Phi_{\ell'} \in C(P, L_1).$$

(6)

We now come to our main technical lemma.

Lemma 3.4: $\ker \pi_{P_1} \cap C(P, L)$ has dimension $q + 1$, with basis the set $X$ of characteristic functions of the $q + 1$ lines through $p_0$.

Proof: Let $G_{p_0}$ be the stabilizer in $Sp(V)$ of $p_0$.

From the definition,

$$\ker \pi_{P_1} = F_2[p_0^q] = F_2[\{p_0\}] \oplus F_2[p_0^{-1}] \setminus \{p_0\}$$

(7)

as an $F_2G_{p_0}$-module. Clearly $F_2[\{p_0\}]$ is a one-dimensional trivial $F_2G_{p_0}$-module. To find the structure of $F_2[p_0^{-1}] \setminus \{p_0\}$, we consider the following subgroups of $G_{p_0}$, which we will describe as matrix groups with respect to our chosen basis.

Let

$$Q = \left\{ \begin{pmatrix} a & b & c \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \mid a, b, c \in F_q \right\}$$

(8)

and

$$C = \left\{ \begin{pmatrix} 0 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid c \in F_q \right\}.$$  

(9)

The group $Q$ is a normal subgroup of $G_{p_0}$ and $C$ is the center of $Q$, with $Q/C$ elementary abelian of order $q^2$. It is easy to see by matrix computations that $C$ acts trivially on $p_0$ and that $Q$ stabilizes each line $\ell$ through $p_0$, acting transitively on the $q$ points of $\ell \setminus \{p_0\}$. These $q$ points have homogeneous coordinates of the form $[d : x : y : 0]$, where $[x : y]$ are homogeneous coordinates of a fixed point on a projective line, and $d$ varies over $F_q$. It is clear that the subgroup $Q[x : y]$ of index $q$ in $Q$ consisting of matrices $\Theta$ in which $ax + by = 0$ is the kernel of the action on $\ell \setminus \{p_0\}$ and so $F_2[\ell \setminus \{p_0\}]$ affords the regular representation of $Q/Q[x : y]$.

As $[x : y]$ varies over the projective line, we deduce that $F_2[p_0^q] \setminus \{p_0\}$ contains the trivial module of $Q/C$ with multiplicity $q + 1$. Thus since $Q$ has odd order, we have a $F_2G_{p_0}$-module decomposition

$$F_2[p_0^q] \setminus \{p_0\} = T \oplus W,$$

(10)

where $T$ is the $(q+1)$-dimensional space of $Q$-fixed points and $W$ has dimension $q^2 - 1$ and no $Q$-fixed points. Let $E$ be a splitting field for $Q$ over $F_2$, and consider the action of $G_{p_0}$ on the characters of $Q/C$ which occur in $E \otimes_{F_2} W$. Each of the $q^2 - 1$ nontrivial characters occurs once. The group of matrices of the form $\begin{pmatrix} \lambda & \mu & \mu^{-1} & \lambda^{-1} \end{pmatrix}$, with $\lambda, \mu \in F_q \setminus \{0\}$, lies in $G_{p_0}$ and acts transitively on the $q - 1$ nontrivial elements, hence also on the $q - 1$ nontrivial characters, of each $Q/Q[x : y]$. Then, since $G_{p_0}$ is transitive on the $q + 1$ lines through $p_0$, it follows that the $q^2 - 1$ nontrivial characters of $Q/C$ form a single $G_{p_0}$-orbit. By Clifford's Theorem (11.1) in [4] it follows that $E \otimes_{F_2} W$ is a simple $EG_{p_0}$-module. Hence $W$ is a simple $F_2G_{p_0}$-module.

We are now ready to consider the intersection

$$\ker \pi_{P_1} \cap C(P, L) = F_2[p_0^q] \setminus C(P, L),$$

(11)

which is an $F_2G_{p_0}$-submodule of $F_2[p_0^q]$. Clearly, $X$ is a linearly independent subset of this intersection. Moreover, each element of $X$ is a fixed point of $Q$. We must prove that the intersection is no bigger than the span of $X$. If it were, then by what we know of the $F_2G_{p_0}$-submodules of $F_2[p_0^q]$, we see that either $F_2[p_0^q] \cap C(P, L)$ must contain all the $Q$-fixed points of $F_2[p_0^q]$ or else it must contain $W$. The first possibility is ruled out because it implies that $C(P, L)$ contains the characteristic function of the point $p_0$, which is absurd since the number of points on a line is even. In the second case, we would have that $F_2[p_0^q] \cap C(P, L)$ is of codimension one in $F_2[p_0^q]$.

Then, for any point $p \in p_0$, since neither $\chi_p$ nor $\chi_{p_0}$ is in $C(P, L)$, we would have $\chi_p - \chi_{p_0} \in C(P, L)$. Then, by transitivity of $Sp(V)$ on $P$ and the connectedness of the adjacency graph of $P$, we would have that $\chi_p - \chi_{p_0} \in C(P, L)$ for all points $p \in P$, leading to the conclusion that $C(P, L)$ has codimension one in $F_2[P]$, contrary to known fact. Thus, the intersection is as claimed.

Lemma 3.5: $\ker \pi_{P_1} \cap C(P, L_1)$ has dimension $q - 1$, and basis the set of functions $\chi_\ell - \chi_{\ell'}$, where $\ell \neq \ell'$ 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 Corollary 3.3 applied to $p_0$, we see that if $\ell$ and $\ell'$ are any two of the $q$ lines through $p_0$ other than $\ell_0$, the function $\chi_\ell - \chi_{\ell'}$ lies in $C(P, L_1)$. It is obviously in $\ker \pi_{P_1}$. Clearly, we can find $q - 1$ linearly independent functions of this kind as described in the statement. Thus $\ker \pi_{P_1} \cap C(P, L_1)$ has dimension $q - 1$.

On the other hand $C(P, L_1)$ is in the kernel of the restriction map to $\ell_0$, while the image of the restriction of $\ker \pi_{P_1} \cap C(P, L)$ in $\ell_0$ has dimension 2, spanned by the images of $\chi_{\ell}$ and $\chi_{\ell'}$. 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 Lemma 3.4.

Our final lemma completes the proof of Theorem 1.1

Lemma 3.6: $Z \cup X_0 \cup Y$ spans $C(P, L)$ as a vector space over $F_2$.

Proof: By Lemma 3.5 the span of $X_0 \cup Z$ is equal to the subspace spanned by $X_0$ and $L_1$, since $\ker \pi_{P_1} \cap C(P, L_1)$ is contained in the span of $X_0$. We must show that the subspace spanned by $X_0 \cup Y$ and $L_1$ contains the characteristic functions of all lines intersecting $\ell_0$, including $\ell_0$. First, consider a line $\ell \neq \ell_0$ meeting $\ell_0$. We can assume that $\ell$ meets $\ell_0$ at a point other than $p_0$, since otherwise $\ell \in X_0$. Therefore $\ell$ meets $\ell_0$ in the same point $p$ as some element $\ell'$ of $Y$. Then Corollary 3.3 shows that $\chi_\ell$ lies in the subspace spanned by $Y$ and $L_1$. The only line still missing is $\ell_0$, so our last task is to show that $\chi_{\ell_0}$ lies in the span of the characteristic functions of all other lines. First, by Lemma 3.4 applied to $\ell_0$, we see that the constant function 1 is in the span. Finally, we see from Lemma 3.2 that

$$\sum_{\ell \in X_0} \Phi_\ell = 1 - \chi_{\ell_0}.$$  

(12)
so we are done. 

**Remark 3.7:** One can also consider the binary code $LU(3, q)$ when $q = 2^t$, $t \geq 1$. The exact dimension is not known yet, but Corollary 2.2 provides a lower bound, since by [5] we have

$$
\dim_{\mathbb{F}_2} C(P, L) = 1 + \left(1 + \sqrt{17}\right) 2^t + \left(1 - \sqrt{17}\right) 2^t.
$$

(13)

This formula is quite different from the one for odd $q$. Nevertheless, it may well be that the inequality (3) is an equality for even $q$, as it is for odd $q$, despite the difference in the $\dim_{\mathbb{F}_2} C(P, L)$ term. Computer calculations of J.-L. Kim verify this up to $q = 16$.

**APPENDIX**

In this appendix $q$ is an arbitrary prime power. Here we explain why our incidence system $(P_1, L_1)$ is equivalent to the incidence system $(P^*, L^*)$ defined by the equations (I). The explanation is given by the classical Klein correspondence.

We first look at $(P_1, L_1)$ in coordinates. Let $x_0, x_1, x_2, x_3$ be homogeneous coordinates of $P$ corresponding to our symplectic basis. Recalling that $p_0 = (e_0)$, we see that $P^*$ is the set of points such that $x_3 \neq 0$. If we represent such a point as $(a : b : c : 1)$ we have a bijection of $P^*_1$ with $\mathbb{F}_q^3$.

Our choice of basis of $V$ yields the basis $e_i \wedge e_j$, for $0 \leq i < j \leq 3$, of the exterior square $\wedge^2(V)$. Denote the corresponding homogeneous coordinates of the projective space $P(\wedge^2(V))$ by $p_{03}, p_{02}, p_{03}, p_{12}, p_{13}$ and $p_{23}$. A 2-dimensional subspace of $V$ spanned by vectors $\sum_{i=0}^3 a_i e_i$ and $\sum_{i=0}^3 b_i e_i$ defines, by taking its exterior square, a point of $P(\wedge^2(V))$ with coordinates $p_{ij} = a_i b_j - a_j b_i$, known as the Plücker or Grassmann coordinates of the subspace. The totality of points of $P(\wedge^2(V))$ obtained in this way from lines of $P(V)$ forms the set with equation $p_{03}p_{23} - p_{02}p_{13} + p_{03}p_{12} = 0$, called the Klein Quadric. The totally isotropic 2-dimensional subspaces of $V$, namely the lines of $L$, correspond to those points of the Klein quadric which satisfy the additional linear equation $p_{03} = -p_{12}$. Recalling that $e_0 = (e_0, e_1)$, the set $L_1$ is the subset of $L$ given by $p_{23} \neq 0$, so taking into consideration the quadratic relation, we see that $L_1$ consists of the points of $P(\wedge^2(V))$ which have Plücker coordinates $(z^2 + xy : x : z : -z : y : 1)$, hence is in bijection with $\mathbb{F}_q^3$. Next we consider when $(a : b : c : 1) \in P^*_1$ is contained in $(z^2 + xy : x : z : -z : y : 1) \in L_1$. Suppose the latter is spanned by points with homogeneous coordinates $(a_0 : a_1 : a_2 : a_3)$ and $(b_0 : b_1 : b_2 : b_3)$. The given point and line are incident if and only if all $3 \times 3$ minors of the matrix

$$
\begin{pmatrix}
 a & b & c \\
 a_0 & a_1 & a_2 & a_3 \\
 b_0 & b_1 & b_2 & b_3
\end{pmatrix}
$$

(14)

are zero. The four equations which result reduce to the two equations

$$
z = -cy + b, \quad x = cz - a.
$$

(15)

By a simple change of coordinates, these equations transform to (I). This shows that $(P_1, L_1)$ and $(P^*, L^*)$ are equivalent.

**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, pp. 339–355, 1991.

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

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

[4] C. W. Curtis and I. Reiner, Methods of Representation Theory, with Applications to Finite Groups and Orders. New York, NY: Wiley Interscience, 1981, vol. I.

[5] N. S. N. Sastry and F. Sin, “The code of a regular generalized quadrangle of even order,” in Group Representations: Cohomology, Group Actions and Topology, ser. Proc. Symposia in Pure Mathematics, vol. 63, 1998, pp. 445–496.

**Peter Sin** received the B.Sc. degree in mathematics from the University of Warwick in 1983 and the D.Phil. degree from the University of Oxford in 1986. He was an L. E. Dickson Instructor at the University of Chicago Department of Mathematics from 1986 to 1988. He joined the Mathematics Department of the University of Florida in 1989 and is now a Professor there. His research interests include the geometry and representation theory of finite and algebraic groups and their connections with combinatorics and algebraic coding theory.

**Qing Xiang** received the Ph.D. degree in mathematics from Ohio State University, Columbus, OH, in 1995. He was a Harry Bateman research instructor at Caltech, Pasadena, CA, from 1995 to 1997. Since 1997, he has been on the faculty of Department of Mathematical Sciences, University of Delaware, Newark, DE. His research interests include combinatorial design theory, algebraic coding theory and finite geometry.

Dr. Xiang was a recipient of the Kirkman Medal from the Institute of Combinatorics and its Applications in 1999.