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

Peter Sin,
University of Florida
Qing Xiang,
Univesity of Delaware

Presented at University of Delaware, 9th December, 2005

0. Overview

- A conjecture on some LDPC codes
- The symplectic generalized quadrangles
- An equivalence of incidence systems
- Proof of the conjecture
- Further research

1. A conjecture about LDPC codes

Recently, Kim et al. [2] studied some explicit LDPC (low density parity check) codes defined using the adjacency matrices of certain bipartite graphs from Lazebnik-Ustimenko [5] for parity check matrices.

- q, any prime power
- P^*, L^* be two sets in bijection with $\mathbf{F}_q{}^3$
- $(a, b, c) \in P^*$ is incident with $[x, y, z] \in L^*$ if and only if

$$y = ax + b \qquad \text{and} \qquad z = ay + c. \tag{1}$$

The binary incidence matrix of (P^*, L^*) and its transpose can be taken as parity check matrices of two codes. These codes are designated $\mathrm{LU}(3, q)$.

Conjecture. *[2] If q is odd, the dimension of* $\mathrm{LU}(3, q)$ *is* $(q^3 - 2q^2 + 3q - 2)/2$.

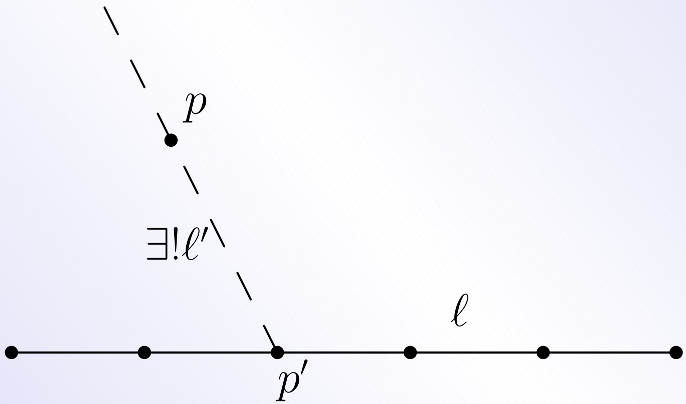
In [2] it was established that this number is a lower bound when q is an odd prime.
We will prove the conjecture in general, by relating it to the geometry of a 4-dimensional symplectic vector space and by applying the representation theory of the symplectic group and its subgroups.

2. The symplectic generalized quadrangle

- q, any prime power
- $(V, (.,.))$, a 4-dimensional $\mathbf{F}_q$-vector space with a non-singular alternating bilinear form
- e_0,e_1, e_2, e_3, a symplectic basis such that $(e_0, e_3) = (e_1, e_2) = 1$
- x_0, x_1, x_2, x_3, coordinates for basis
- $P = \mathbf{P}(V)$, the set of points of the projective space of V
- L, 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.*

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 though the given point and meets the given line.



Theorem 1. *(Bagchi-Brouwer-Wilbrink [1]) Assume q is a power of an odd prime. Then the 2-rank of $M(P,L)$ is $(q^3+2q^2+q+2)/2$.*

Theorem 2. *(Sastry-Sin [4]) Assume $q=2^t$. Then then the 2-rank of $M(P,L)$ is*

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

Now fix a point $p_0 \in P$ and a line $\ell_0 \in L$ through p_0. We can assume that $p_0 = \langle e_0 \rangle$ and $\ell_0 = \langle e_0, e_1 \rangle$.

- $p^\perp$, the set of points on lines through the point p
- $P_1 = P \setminus p_0^\perp$
- L_1, the set of lines in L which do not meet ℓ_0

We have new incidence systems (P_1, L_1), (P, L_1), (P_1, L).

Back
Full Screen
Close
Quit

In the next section we will prove that (P_1, L_1) is equivalent to the system (P^*, L^*).
The following theorem will then imply the conjecture.

Theorem 3. *Assume q is odd. The 2-rank of $M(P_1, L_1)$ equals $(q^3 + 2q^2 - 3q + 2)/2$.*

Note this number is $2q$ less than the 2-rank of $M(P, L)$.

3. Coordinates of points and lines

Let q be any prime power. Here we show, by introducing coordinates for (P_1, L_1), that it is equivalent to (P^*, L^*).

Coordinates of P_1

- x_0, x_1, x_2, x_3 be homogeneous coordinates of P
- $p_0 = \langle e_0 \rangle$

$$
\begin{aligned}
P_1 &= \{(x_0 : x_1 : x_2 : x_3) \mid x_3 \neq 0\} \\
&= \{(a : b : c : 1) \mid, a, b, c \in \mathbf{F}_q\} \cong \mathbf{F}_q{}^3.
\end{aligned} \tag{3}
$$

Coordinates of lines in $P(V)$

- $e_i \wedge e_j$, $0 \leq i < j \leq 3$, basis of the exterior square $\wedge^2(V)$
- $p_{01}, p_{02}, p_{03}, p_{12}, p_{13}, p_{23}$, homogeneous coordinates for $\mathbf{P}(\wedge^2(V))$
- If W is a 2-dimensional subspace of V then $\wedge^2(W) \in \mathbf{P}(\wedge^2(V))$.
- If $W = \langle (a_0 : a_1 : a_2 : a_3), (b_0 : b_1 : b_2 : b_3) \rangle$ then $\wedge^2(W)$ has coordinates $p_{ij} = a_i b_j - a_j b_i$, its *Grassmann-Plücker* coordinates.
- The totality of points of $\mathbf{P}(\wedge^2(V))$ obtained from all W forms the set with equation $p_{01}p_{23} - p_{02}p_{13} + p_{03}p_{12} = 0$, called the *Klein Quadric*.

Coordinates of L and L_1

- L corresponds to the subset of points of the Klein quadric which satisfy the additional linear equation $p_{03} = -p_{12}$.
- $\ell_0 = \langle (1:0:0:0), (0:1:0:0) \rangle$
- L_1 is the subset of L given by $p_{23} \neq 0$.

Taking into consideration the quadratic relation, we see that

$$\begin{aligned} L_1 &\cong \{(z^2 + xy : x : z : -z : y : 1) \mid x, y, z \in \mathbf{F}_q\} \\ &\cong {\mathbf{F}_q}^3. \end{aligned} \tag{4}$$

3.1. Incidence equations

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 3×3 minors of the matrix

$$\begin{pmatrix} a & b & c & 1 \\ a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & b_3 \end{pmatrix} \tag{5}$$

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

$$z = -cy + b, \qquad x = cz - a. \tag{6}$$

By a simple change of coordinates, these equations transform to (6). This shows that (P_1, L_1) and (P^*, L^*) are equivalent.

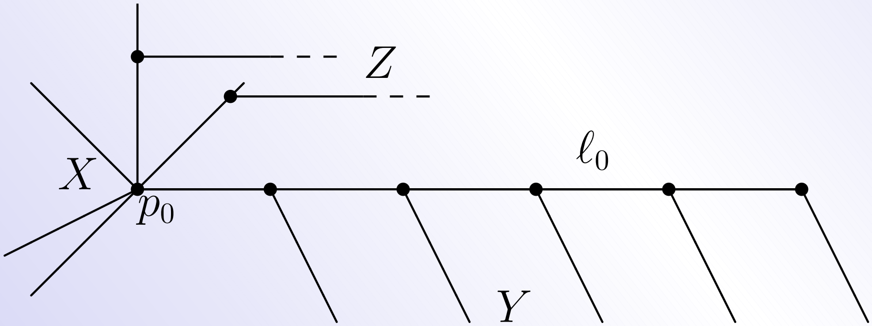
4. Relative dimensions and a bound

In this section q is an arbitrary prime power.

4.1. Notation

- $\mathbf{F}_2[P]$, the vector space of all $\mathbf{F}_2$-valued functions on P
- χ_p, the characteristic function of the point $p \in P$
- Let χ_ℓ, the characteristic function of the line $\ell \in L$
- $C(P, L)$, the subspace of $\mathbf{F}_2[P]$ spanned by the χ_ℓ, $\ell \in L$
- $C(P, L_1)$, the subspace generated by lines in L_1
- $\pi_{P_1} : \mathbf{F}_2[P] \to \mathbf{F}_2[P_1]$, natural projection map
- $C(P_1, L) = \pi_{P_1}(C(P, L))$, $C(P_1, L_1) = \pi_{P_1}(C(P, L_1))$

- $Z \subset C(P, L_1)$, a set of characteristic functions of lines in L_1 which maps bijectively under π_{P_1} to a basis of $C(P_1, L_1)$
- X, the set of characteristic functions of the lines through p_0 and let $X_0 = X \setminus \{\ell_0\}$
- Y be the set of characteristic functions of any q lines which meet ℓ_0 in the q distinct points other than p_0



Lemma 4. $Z \cup X_0 \cup Y$ *is linearly independent over* $\mathbf{F}_2$*.*

Proof. Each element of Y contains in its support a point of ℓ_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 π_{P_1} to a linearly independent set. $\square$

Corollary 5.

$$\dim_{\mathbf{F}_2} \mathrm{LU}(3, q) \geq q^3 - \dim_{\mathbf{F}_2} C(P, L) + 2q. \qquad (7)$$

5. Proof of Theorem 3

In this section we assume that q is odd. In view of Corollary 5 and the known 2-rank of $M(P, L)$ the proof of Theorem 3 will be completed if we can show that $Z \cup X_0 \cup Y$ spans $C(P, L)$ as a vector space over $\mathbf{F}_2$.

Lemma 6. *Let $\ell \in L$. Then the sum of the characteristic functions of all lines which meet ℓ (excluding ℓ itself) is the constant function 1.*

Proof. The function given by the sum takes the value $q \equiv 1$ at any point of ℓ and value 1 at any point off ℓ, by the quadrangle property. □

Lemma 7. *Let $\ell \neq \ell_0$ be a line which meets ℓ_0 at a point p. Let Φ_ℓ be the sum of all the characteristic functions of lines in L_1 which meet ℓ. Then*

$$\Phi_\ell(p') = \begin{cases} 0, & \text{if } p' = p; \\ q, & \text{if } p' \in \ell \setminus \{p\}; \\ 0, & \text{if } p' \in p^\perp \setminus \ell; \\ 1, & \text{if } p' \in P \setminus p^\perp. \end{cases} \tag{8}$$

□

Corollary 8. *Let $p \in \ell_0$ and let ℓ, ℓ' be two lines through p, neither equal to ℓ_0. Then $\chi_\ell - \chi_{\ell'} \in C(P, L_1)$.*

Proof. Since $q = 1$ in $\mathbf{F}_2$, one easily check using Lemma 7 that

$$\chi_\ell - \chi_{\ell'} = \Phi_\ell - \Phi_{\ell'} \in C(P, L_1). \tag{9}$$

□

Lemma 9. *$\ker \pi_{P_1} \cap C(P, L)$ has dimension $q+1$, with basis X.*

Proof. Omitted $\square$

The proof of this lemma is technical and of a different flavor, requiring some detailed calculations of the action of the subgroup of $\mathrm{Sp}(V)$ which stabilizes p_0 on the subspace $\mathbf{F}_2[p_0^\perp]$ and standard results from group representations, e.g. Clifford's Theorem.

Lemma 10. $\ker \pi_{P_1} \cap C(P, L_1)$ *has dimension* $q-1$, *and basis the set of functions* $\chi_\ell - \chi_{\ell'}$, *where* $\ell \neq \ell_0$ *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 Corollary 8 applied to p_0, we see that if ℓ and ℓ' are any two of the q lines through p_0 other than ℓ_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 $\geq q-1$. On the other hand $C(P, L_1)$ is in the kernel of the restriction map to ℓ_0, while the image of the restriction of $\ker \pi_{P_1}$ 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 $\ker \pi_{P_1}$, which has dimension $q+1$, by Lemma 9. $\square$

Lemma 11. *$Z \cup X_0 \cup Y$ spans $C(P, L)$ as a vector space over $\mathbf{F}_2$.*

Proof. By Lemma 10, the span of X_0 and Z is equal to the span of 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 span of $X_0 \cup L_1 \cup Y$ contains the characteristic functions of all lines through ℓ_0, including ℓ_0. First, consider a line $\ell \neq \ell_0$ through ℓ_0. We can assume that ℓ meets ℓ_0 at a point other than p_0, since otherwise $\ell \in X_0$. Therefore ℓ meets ℓ_0 in the same point p as some element $\ell' \in Y$. Then Corollary 8 shows that χ_ℓ lies in the span of Y and L_1. The only line still missing is ℓ_0, so our last task is to show that χ_{ℓ_0} lies in the span of the characteristic functions of all other lines. First, by Lemma 6 applied to ℓ_0, we see that the constant function 1 is in the span. Finally, we see from Lemma 7 that

$$\sum_{\ell \in X_0} \Phi_\ell = 1 - \chi_{\ell_0}, \tag{10}$$

so we are done. □

6. Further research

One can also consider the binary code $\mathrm{LU}(3, q)$ when $q = 2^t$, $t \geq 1$. The exact dimension is not known yet, but Corollary 5 provides a lower bound. The formulae for $\dim_{\mathbf{F}_2} C(P, L)$ are quite different for odd and even q. Nevertheless, it may well be that the inequality (7) is an equality for even q, just as it is for odd q. Computer calculations of J.-L. Kim verify this up to $q = 16$. We can get an idea of the difference between the odd and even cases by comparing the representation theory of $\mathrm{Sp}(V)$ in the two cases. In the odd case, the group and code are defined over fields of different characteristics, whereas in the even case, they are both in characteristic 2. The representation theory in the former case is closely related to the complex character theory, while in the latter case it more closely resembles the theory of rational representations of algebraic groups.

7. 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] 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.

[4] N. S. N. Sastry and P. 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. 485–496.

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