On the dimensions of LDPC codes defined by equations over finite fields

Peter Sin

USM, Penang, June 2009.

Overview

- LDPC (low density parity check) codes have attracted much attention recently, due to their good performance in theory and practice.
- A main division is into *random* and *structured* types.
- One structured family, constructed using certain bipartite graphs was studied by: J.-L. Kim, U. Peled, I. Perepelitsa, V. Pless, and S. Friedland (2004)
- They conjectured the dimensions of the codes.
- We'll describe the conjecture and its proof (with Q. Xiang).
- The proof involves the geometry of generalized quadrangles and the representation theory of $\mathrm{Sp}(4, q)$.

Overview

- LDPC (low density parity check) codes have attracted much attention recently, due to their good performance in theory and practice.
- A main division is into *random* and *structured* types.
- One structured family, constructed using certain bipartite graphs was studied by: J.-L. Kim, U. Peled, I. Perepelitsa, V. Pless, and S. Friedland (2004)
- They conjectured the dimensions of the codes.
- We'll describe the conjecture and its proof (with Q. Xiang).
- The proof involves the geometry of generalized quadrangles and the representation theory of $\mathrm{Sp}(4, q)$.

Overview

- LDPC (low density parity check) codes have attracted much attention recently, due to their good performance in theory and practice.
- A main division is into *random* and *structured* types.
- One structured family, constructed using certain bipartite graphs was studied by: J.-L. Kim, U. Peled, I. Perepelitsa, V. Pless, and S. Friedland (2004)
- They conjectured the dimensions of the codes.
- We'll describe the conjecture and its proof (with Q. Xiang).
- The proof involves the geometry of generalized quadrangles and the representation theory of $\mathrm{Sp}(4, q)$.

Overview

- LDPC (low density parity check) codes have attracted much attention recently, due to their good performance in theory and practice.
- A main division is into *random* and *structured* types.
- One structured family, constructed using certain bipartite graphs was studied by: J.-L. Kim, U. Peled, I. Perepelitsa, V. Pless, and S. Friedland (2004)
- They conjectured the dimensions of the codes.
- We'll describe the conjecture and its proof (with Q. Xiang).
- The proof involves the geometry of generalized quadrangles and the representation theory of $\mathrm{Sp}(4, q)$.

Overview

- LDPC (low density parity check) codes have attracted much attention recently, due to their good performance in theory and practice.
- A main division is into *random* and *structured* types.
- One structured family, constructed using certain bipartite graphs was studied by: J.-L. Kim, U. Peled, I. Perepelitsa, V. Pless, and S. Friedland (2004)
- They conjectured the dimensions of the codes.
- We'll describe the conjecture and its proof (with Q. Xiang).
- The proof involves the geometry of generalized quadrangles and the representation theory of $\mathrm{Sp}(4, q)$.

Overview

- LDPC (low density parity check) codes have attracted much attention recently, due to their good performance in theory and practice.
- A main division is into *random* and *structured* types.
- One structured family, constructed using certain bipartite graphs was studied by: J.-L. Kim, U. Peled, I. Perepelitsa, V. Pless, and S. Friedland (2004)
- They conjectured the dimensions of the codes.
- We'll describe the conjecture and its proof (with Q. Xiang).
- The proof involves the geometry of generalized quadrangles and the representation theory of $\mathrm{Sp}(4, q)$.

The codes $LU(3, q)$

- 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 $M_2(P^*, L^*)$ and its transpose can be taken as parity check matrices of two codes.
- These codes are designated $\mathrm{LU}(3, q)$. We have:

$$\dim \mathrm{LU}(3, q) = q^3 - \mathrm{rank} M_2(P^*, L^*).$$

The codes $LU(3, q)$

- 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 $M_2(P^*, L^*)$ and its transpose can be taken as parity check matrices of two codes.
- These codes are designated $\mathrm{LU}(3, q)$. We have:

$$\dim \mathrm{LU}(3, q) = q^3 - \mathrm{rank} M_2(P^*, L^*).$$

The codes $LU(3, q)$

- 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 $M_2(P^*, L^*)$ and its transpose can be taken as parity check matrices of two codes.
- These codes are designated $\mathrm{LU}(3, q)$. We have:

$$\dim \mathrm{LU}(3, q) = q^3 - \mathrm{rank} M_2(P^*, L^*).$$

The codes $LU(3, q)$

- 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 $M_2(P^*, L^*)$ and its transpose can be taken as parity check matrices of two codes.
- These codes are designated $\mathrm{LU}(3, q)$. We have:

$$\dim \mathrm{LU}(3, q) = q^3 - \mathrm{rank} M_2(P^*, L^*).$$

The codes $LU(3, q)$

- 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 $M_2(P^*, L^*)$ and its transpose can be taken as parity check matrices of two codes.
- These codes are designated $\mathrm{LU}(3, q)$. We have:

$$\dim \mathrm{LU}(3, q) = q^3 - \mathrm{rank} M_2(P^*, L^*).$$

- Conjecture: If q is odd, the dimension of $\mathrm{LU}(3, q)$ is $(q^3 - 2q^2 + 3q - 2)/2$.
- This number was known to be a lower bound when q is an odd prime.

- Conjecture: If q is odd, the dimension of $\mathrm{LU}(3, q)$ is $(q^3 - 2q^2 + 3q - 2)/2$.
- This number was known to be a lower bound when q is an odd prime.

The symplectic generalized quadrangle

- q, any prime power
- $(V, (.,.))$, a 4-dimensional $\mathbf{F}_q$-vector space with a nonsingular 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
- (P, L) is called the *symplectic generalized quadrangle*.

The symplectic generalized quadrangle

- q, any prime power
- $(V, (.,.))$, a 4-dimensional $\mathbf{F}_q$-vector space with a nonsingular 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
- (P, L) is called the *symplectic generalized quadrangle*.

The symplectic generalized quadrangle

- q, any prime power
- $(V, (.,.))$, a 4-dimensional $\mathbf{F}_q$-vector space with a nonsingular 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
- (P, L) is called the *symplectic generalized quadrangle*.

The symplectic generalized quadrangle

- q, any prime power
- $(V, (.,.))$, a 4-dimensional $\mathbf{F}_q$-vector space with a nonsingular 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
- (P, L) is called the *symplectic generalized quadrangle*.

The symplectic generalized quadrangle

- q, any prime power
- $(V, (.,.))$, a 4-dimensional $\mathbf{F}_q$-vector space with a nonsingular 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
- (P, L) is called the *symplectic generalized quadrangle*.

The symplectic generalized quadrangle

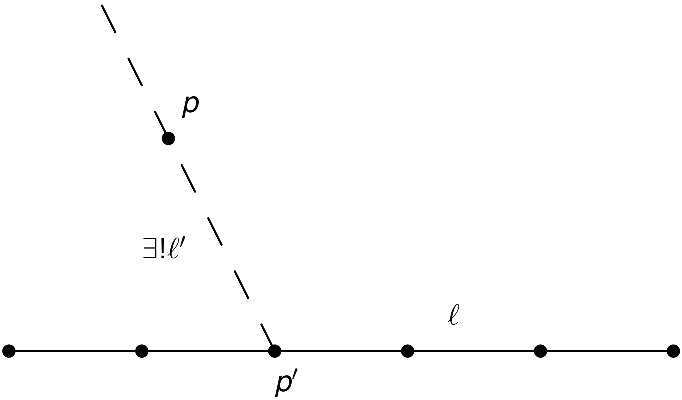
- q, any prime power
- $(V, (.,.))$, a 4-dimensional $\mathbf{F}_q$-vector space with a nonsingular alternating bilinear form
- e_0, e_1, e_2, e_3, a symplectic basis such that $(e_0, e_3) = (e_1, e_2) = 1$
- x_0, x_1, x_2, x_3, coordinates for basis
- $P = \mathbf{P}(V)$, the set of points of the projective space of V
- L, the set of totally isotropic 2-dimensional subspaces of V, considered as lines in P
- (P, L) is called the *symplectic generalized quadrangle*.

The symplectic generalized quadrangle

- q, any prime power
- $(V, (.,.))$, a 4-dimensional $\mathbf{F}_q$-vector space with a nonsingular 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
- (P, L) is called the *symplectic generalized quadrangle*.

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.



- $p_0 = \langle e_0 \rangle$ 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).

- $p_0 = \langle e_0 \rangle$ 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).

- $p_0 = \langle e_0 \rangle$ 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).

- $p_0 = \langle e_0 \rangle$ 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).

- $p_0 = \langle e_0 \rangle$ 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).

- We will see below that (P_1, L_1) is equivalent to the system (P^*, L^*).
- So we want to prove:

Theorem

Assume q is odd. The rank of $M_2(P_1, L_1)$ equals $(q^3 + 2q^2 - 3q + 2)/2$.

- A known result is:

Theorem

(Bagchi-Brouwer-Wilbrink) Assume q is a power of an odd prime. Then the rank of $M_2(P, L)$ is $(q^3 + 2q^2 + q + 2)/2$.

- Note that the difference in ranks is $2q$.

- We will see below that (P_1, L_1) is equivalent to the system (P^*, L^*).
- So we want to prove:

Theorem

Assume q is odd. The rank of $M_2(P_1, L_1)$ equals $(q^3 + 2q^2 - 3q + 2)/2$.

- A known result is:

Theorem

(Bagchi-Brouwer-Wilbrink) Assume q is a power of an odd prime. Then the rank of $M_2(P, L)$ is $(q^3 + 2q^2 + q + 2)/2$.

- Note that the difference in ranks is $2q$.

- We will see below that (P_1, L_1) is equivalent to the system (P^*, L^*).
- So we want to prove:

Theorem

Assume q is odd. The rank of $M_2(P_1, L_1)$ equals $(q^3 + 2q^2 - 3q + 2)/2$.

- A known result is:

Theorem

(Bagchi-Brouwer-Wilbrink) Assume q is a power of an odd prime. Then the rank of $M_2(P, L)$ is $(q^3 + 2q^2 + q + 2)/2$.

- Note that the difference in ranks is $2q$.

- We will see below that (P_1, L_1) is equivalent to the system (P^*, L^*).
- So we want to prove:

Theorem

Assume q is odd. The rank of $M_2(P_1, L_1)$ equals $(q^3 + 2q^2 - 3q + 2)/2$.

- A known result is:

Theorem

(Bagchi-Brouwer-Wilbrink) Assume q is a power of an odd prime. Then the rank of $M_2(P, L)$ is $(q^3 + 2q^2 + q + 2)/2$.

- Note that the difference in ranks is $2q$.

- We will see below that (P_1, L_1) is equivalent to the system (P^*, L^*).
- So we want to prove:

Theorem

Assume q is odd. The rank of $M_2(P_1, L_1)$ equals $(q^3 + 2q^2 - 3q + 2)/2$.

- A known result is:

Theorem

(Bagchi-Brouwer-Wilbrink) Assume q is a power of an odd prime. Then the rank of $M_2(P, L)$ is $(q^3 + 2q^2 + q + 2)/2$.

- Note that the difference in ranks is $2q$.

- We will see below that (P_1, L_1) is equivalent to the system (P^*, L^*).
- So we want to prove:

Theorem

Assume q is odd. The rank of $M_2(P_1, L_1)$ equals $(q^3 + 2q^2 - 3q + 2)/2$.

- A known result is:

Theorem

(Bagchi-Brouwer-Wilbrink) Assume q is a power of an odd prime. Then the rank of $M_2(P, L)$ is $(q^3 + 2q^2 + q + 2)/2$.

- Note that the difference in ranks is $2q$.

Next, see $(P_1, L_1) \cong (P^*, L^*)$, for q any prime power.

Coordinates of P_1

- x_0, x_1, x_2, x_3 be homogeneous coordinates of P
- $p_0 = \langle e_0 \rangle$
-
$$\begin{aligned} P_1 &= \{(x_0 : x_1 : x_2 : x_3) \mid x_3 \neq 0\} \\ &= \{(a : b : c : 1) \mid, a, b, c \in \mathbf{F}_q\} \cong \mathbf{F}_q{}^3. \end{aligned} \tag{2}$$

Coordinates of P_1

- x_0, x_1, x_2, x_3 be homogeneous coordinates of P
- $p_0 = \langle e_0 \rangle$
- $$\begin{aligned} P_1 &= \{(x_0 : x_1 : x_2 : x_3) \mid x_3 \neq 0\} \\ &= \{(a : b : c : 1) \mid, a, b, c \in \mathbf{F}_q\} \cong \mathbf{F}_q{}^3. \end{aligned} \tag{2}$$

Coordinates of P_1

- x_0, x_1, x_2, x_3 be homogeneous coordinates of P
- $p_0 = \langle e_0 \rangle$
- $$\begin{aligned} P_1 &= \{(x_0 : x_1 : x_2 : x_3) \mid x_3 \neq 0\} \\ &= \{(a : b : c : 1) \mid, a, b, c \in \mathbf{F}_q\} \cong \mathbf{F}_q{}^3. \end{aligned} \tag{2}$$

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 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 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 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 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 $p_{23} \neq 0$.
- The quadratic relation yields

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

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 $p_{23} \neq 0$.
- The quadratic relation yields

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

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 $p_{23} \neq 0$.
- The quadratic relation yields

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

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 $p_{23} \neq 0$.
- The quadratic relation yields

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

Incidence equations

- When is $(a : b : c : 1) \in P_1$ on $(z^2 + xy : x : z : -z : y : 1) \in L_1$?
- If the line 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

$$\begin{pmatrix} a & b & c & 1 \\ a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & b_3 \end{pmatrix} \tag{4}$$

are zero.

Incidence equations

- When is $(a : b : c : 1) \in P_1$ on $(z^2 + xy : x : z : -z : y : 1) \in L_1$?
- If the line 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

$$\begin{pmatrix} a & b & c & 1 \\ a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & b_3 \end{pmatrix} \tag{4}$$

are zero.

- The four equations which result reduce to the two equations

$$z = -cy + b, \qquad x = cz - a. \tag{5}$$

- Hence (P_1, L_1) and (P^*, L^*) are equivalent.

- The four equations which result reduce to the two equations
$$z = -cy + b, \qquad x = cz - a. \tag{5}$$
- Hence (P_1, L_1) and (P^*, L^*) are equivalent.

Relative dimensions and a bound

q is any prime power.

- $\mathbf{F}_2[P]$, the vector space of all $\mathbf{F}_2$-valued functions on P
- Abuse notation slightly, identify points and lines with their characteristic functions in $\mathbf{F}_2[P]$.
- $C(P, L)$, the subspace of $\mathbf{F}_2[P]$ spanned by the $\ell \in L$.
- $C(P, L_1)$, the subspace generated by lines in L_1
- $\pi_{P_1} : \mathbf{F}_2[P] \to \mathbf{F}_2[P_1]$, natural projection map
- $C(P_1, L) = \pi_{P_1}(C(P, L))$, $C(P_1, L_1) = \pi_{P_1}(C(P, L_1))$

Relative dimensions and a bound

q is any prime power.

- $\mathbf{F}_2[P]$, the vector space of all $\mathbf{F}_2$-valued functions on P
- Abuse notation slightly, identify points and lines with their characteristic functions in $\mathbf{F}_2[P]$.
- $C(P, L)$, the subspace of $\mathbf{F}_2[P]$ spanned by the $\ell \in L$.
- $C(P, L_1)$, the subspace generated by lines in L_1
- $\pi_{P_1} : \mathbf{F}_2[P] \to \mathbf{F}_2[P_1]$, natural projection map
- $C(P_1, L) = \pi_{P_1}(C(P, L))$, $C(P_1, L_1) = \pi_{P_1}(C(P, L_1))$

Relative dimensions and a bound

q is any prime power.

- $\mathbf{F}_2[P]$, the vector space of all $\mathbf{F}_2$-valued functions on P
- Abuse notation slightly, identify points and lines with their characteristic functions in $\mathbf{F}_2[P]$.
- $C(P, L)$, the subspace of $\mathbf{F}_2[P]$ spanned by the $\ell \in L$.
- $C(P, L_1)$, the subspace generated by lines in L_1
- $\pi_{P_1} : \mathbf{F}_2[P] \to \mathbf{F}_2[P_1]$, natural projection map
- $C(P_1, L) = \pi_{P_1}(C(P, L))$, $C(P_1, L_1) = \pi_{P_1}(C(P, L_1))$

Relative dimensions and a bound

q is any prime power.

- $\mathbf{F}_2[P]$, the vector space of all $\mathbf{F}_2$-valued functions on P
- Abuse notation slightly, identify points and lines with their characteristic functions in $\mathbf{F}_2[P]$.
- $C(P, L)$, the subspace of $\mathbf{F}_2[P]$ spanned by the $\ell \in L$.
- $C(P, L_1)$, the subspace generated by lines in L_1
- $\pi_{P_1} : \mathbf{F}_2[P] \to \mathbf{F}_2[P_1]$, natural projection map
- $C(P_1, L) = \pi_{P_1}(C(P, L))$, $C(P_1, L_1) = \pi_{P_1}(C(P, L_1))$

Relative dimensions and a bound

q is any prime power.

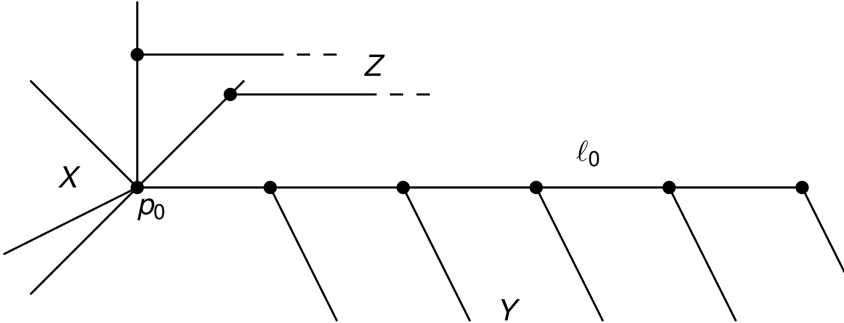
- $\mathbf{F}_2[P]$, the vector space of all $\mathbf{F}_2$-valued functions on P
- Abuse notation slightly, identify points and lines with their characteristic functions in $\mathbf{F}_2[P]$.
- $C(P, L)$, the subspace of $\mathbf{F}_2[P]$ spanned by the $\ell \in L$.
- $C(P, L_1)$, the subspace generated by lines in L_1
- $\pi_{P_1} : \mathbf{F}_2[P] \to \mathbf{F}_2[P_1]$, natural projection map
- $C(P_1, L) = \pi_{P_1}(C(P, L))$, $C(P_1, L_1) = \pi_{P_1}(C(P, L_1))$

Relative dimensions and a bound

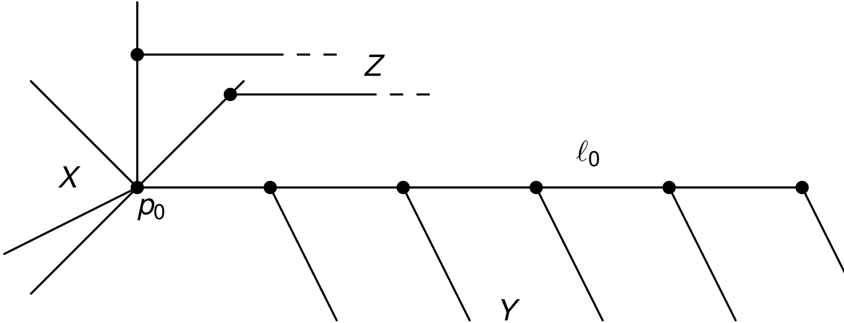
q is any prime power.

- $\mathbf{F}_2[P]$, the vector space of all $\mathbf{F}_2$-valued functions on P
- Abuse notation slightly, identify points and lines with their characteristic functions in $\mathbf{F}_2[P]$.
- $C(P, L)$, the subspace of $\mathbf{F}_2[P]$ spanned by the $\ell \in L$.
- $C(P, L_1)$, the subspace generated by lines in L_1
- $\pi_{P_1} : \mathbf{F}_2[P] \to \mathbf{F}_2[P_1]$, natural projection map
- $C(P_1, L) = \pi_{P_1}(C(P, L))$, $C(P_1, L_1) = \pi_{P_1}(C(P, L_1))$

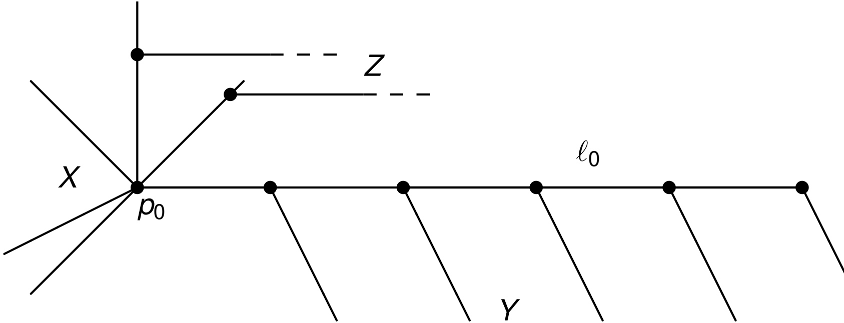
- $Z \subset C(P, L_1)$, a set of lines in L_1 which maps bijectively under π_{P_1} to a basis of $C(P_1, L_1)$
- X, the set of the lines through p_0 and let $X_0 = X \setminus \{\ell_0\}$
- Y be any q lines which meet ℓ_0 in the q distinct points other than p_0
- $|X_0 \cup Y| = 2q$ (cf. Theorem 1).



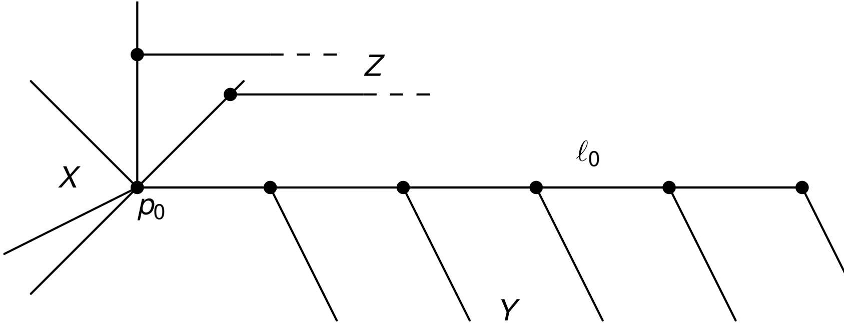
- $Z \subset C(P, L_1)$, a set of lines in L_1 which maps bijectively under π_{P_1} to a basis of $C(P_1, L_1)$
- X, the set of the lines through p_0 and let $X_0 = X \setminus \{\ell_0\}$
- Y be any q lines which meet ℓ_0 in the q distinct points other than p_0
- $|X_0 \cup Y| = 2q$ (cf. Theorem 1).



- $Z \subset C(P, L_1)$, a set 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 the lines through p_0 and let $X_0 = X \setminus \{\ell_0\}$
- Y be any q lines which meet ℓ_0 in the q distinct points other than p_0
- $|X_0 \cup Y| = 2q$ (cf. Theorem 1).



- $Z \subset C(P, L_1)$, a set 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 the lines through p_0 and let $X_0 = X \setminus \{\ell_0\}$
- Y be any q lines which meet ℓ_0 in the q distinct points other than p_0
- $|X_0 \cup Y| = 2q$ (cf. Theorem 1).



Lemma

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

Corollary

$$\dim_{\mathbf{F}_2} \mathrm{LU}(3, q) \geq q^3 - \dim_{\mathbf{F}_2} C(P, L) + 2q. \tag{6}$$

Lemma

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

Corollary

$$\dim_{\mathbf{F}_2} \mathrm{LU}(3, q) \geq q^3 - \dim_{\mathbf{F}_2} C(P, L) + 2q. \tag{6}$$

Proof of Theorem 1

Assume that q is odd. By Corollary 4 the proof of Theorem 1 will be completed if we can show that $Z \cup X_0 \cup Y$ spans $C(P, L)$ as a vector space over $\mathbf{F}_2$.

Geometric arguments

Lemma

Let $\ell \in L$. Then the sum 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. □

Geometric arguments

Lemma

Let $\ell \in L$. Then the sum 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. $\square$

Similarly:

Lemma

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

$$\Phi_\ell(p') = \begin{cases} 0, & \text{if } p' = p; \\ q, & \text{if } p' \in \ell \setminus \{p\}; \\ 0, & \text{if } p' \in p^\perp \setminus \ell; \\ 1, & \text{if } p' \in P \setminus p^\perp. \end{cases} \tag{7}$$

Corollary

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

Similarly:

Lemma

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

$$\Phi_\ell(p') = \begin{cases} 0, & \text{if } p' = p; \\ q, & \text{if } p' \in \ell \setminus \{p\}; \\ 0, & \text{if } p' \in p^\perp \setminus \ell; \\ 1, & \text{if } p' \in P \setminus p^\perp. \end{cases} \tag{7}$$

Corollary

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

Some representation theory

Lemma

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

Proof:

- Let G_{p_0} be the stabilizer in $\mathrm{Sp}(V)$ of p_0.
-
$$\ker \pi_{P_1} = \mathbf{F}_2[p_0^{\perp}] = \mathbf{F}_2[\{p_0\}] \oplus \mathbf{F}_2[{p_0}^{\perp} \setminus \{p_0\}] \qquad (8)$$

  as an $\mathbf{F}_2 G_{p_0}$-module. Clearly $\mathbf{F}_2[\{p_0\}]$ is a one-dimensional trivial $\mathbf{F}_2 G_{p_0}$-module.

Lemma

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

Proof:

- Let G_{p_0} be the stabilizer in $\mathrm{Sp}(V)$ of p_0.
- $$\ker \pi_{P_1} = \mathbf{F}_2[p_0^\perp] = \mathbf{F}_2[\{p_0\}] \oplus \mathbf{F}_2[{p_0}^\perp \setminus \{p_0\}] \qquad (8)$$

  as an $\mathbf{F}_2 G_{p_0}$-module. Clearly $\mathbf{F}_2[\{p_0\}]$ is a one-dimensional trivial $\mathbf{F}_2 G_{p_0}$-module.

Some representation theory

Lemma

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

Proof:

- Let G_{p_0} be the stabilizer in $\mathrm{Sp}(V)$ of p_0.
-
$$\ker \pi_{P_1} = \mathbf{F}_2[p_0^\perp] = \mathbf{F}_2[\{p_0\}] \oplus \mathbf{F}_2[{p_0}^\perp \setminus \{p_0\}] \qquad (8)$$

  as an $\mathbf{F}_2 G_{p_0}$-module. Clearly $\mathbf{F}_2[\{p_0\}]$ is a one-dimensional trivial $\mathbf{F}_2 G_{p_0}$-module.

- We consider the following subgroups of G_{p_0}.

$$Q = \left\{ \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & -a \\ 0 & 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbf{F}_q \right\}, \quad Z(Q) = \left\{ \begin{pmatrix} 1 & 0 & 0 & c \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \mid c \in \mathbf{F}_q \right\} \tag{9}$$

- $Q \lhd G_{p_0}$, $Q/Z(Q)$ is elementary abelian of order q^2 and $Z(Q)$ acts trivially on $p_0^{\perp}$.
- Since Q has odd order, it acts semisimply on $\mathbf{F}_2[p_0^{\perp}]$ and we can compute the decomposition.

- We consider the following subgroups of G_{p_0}.

$$Q = \left\{ \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & -a \\ 0 & 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbf{F}_q \right\}, \quad Z(Q) = \left\{ \begin{pmatrix} 1 & 0 & 0 & c \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \mid c \in \mathbf{F}_q \right\} \tag{9}$$

- $Q \lhd G_{p_0}$, $Q/Z(Q)$ is elementary abelian of order q^2 and $Z(Q)$ acts trivially on $p_0^\perp$.
- Since Q has odd order, it acts semisimply on $\mathbf{F}_2[p_0^\perp]$ and we can compute the decomposition.

- We consider the following subgroups of G_{p_0}.

$$Q = \left\{ \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & -a \\ 0 & 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbf{F}_q \right\}, \quad Z(Q) = \left\{ \begin{pmatrix} 1 & 0 & 0 & c \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \mid c \in \mathbf{F}_q \right\} \tag{9}$$

- $Q \lhd G_{p_0}$, $Q/Z(Q)$ is elementary abelian of order q^2 and $Z(Q)$ acts trivially on $p_0^{\perp}$.
- Since Q has odd order, it acts semisimply on $\mathbf{F}_2[p_0^{\perp}]$ and we can compute the decomposition.

- Applying Clifford's Theorem, we have a $\mathbf{F}_2 G_{p_0}$-module decomposition

$$\mathbf{F}_2[p_0^\perp] = T \oplus W, \tag{10}$$

where T is the $q+2$-dimensional space of Q-fixed points and W is simple of dimension $q^2 - 1$.
- The intersection

$$\ker \pi_{P_1} \cap C(P, L) = \mathbf{F}_2[p_0^\perp] \cap C(P, L), \tag{11}$$

is an $\mathbf{F}_2 G_{p_0}$-submodule of $\mathbf{F}_2[p_0^\perp]$.
- The $q+1$ lines through p_0 lie in the intersection, accounting for $q+1$ dimensions of T.
- We must argue that the intersection is no bigger than their span. If it were, then by (10), $\mathbf{F}_2[p_0^\perp] \cap C(P, L)$ must contain either W or all the Q-fixed points on $\mathbf{F}_2[p_0^\perp]$.
- Both possibilities lead immediately to contradictions.

- Applying Clifford's Theorem, we have a $\mathbf{F}_2 G_{p_0}$-module decomposition

$$\mathbf{F}_2[p_0^{\perp}] = T \oplus W, \tag{10}$$

where T is the $q+2$-dimensional space of Q-fixed points and W is simple of dimension q^2-1.
- The intersection

$$\ker \pi_{P_1} \cap C(P,L) = \mathbf{F}_2[p_0^{\perp}] \cap C(P,L), \tag{11}$$

is an $\mathbf{F}_2 G_{p_0}$-submodule of $\mathbf{F}_2[p_0^{\perp}]$.
- The $q+1$ lines through p_0 lie in the intersection, accounting for $q+1$ dimensions of T.
- We must argue that the intersection is no bigger than their span. If it were, then by (10), $\mathbf{F}_2[p_0^{\perp}] \cap C(P,L)$ must contain either W or all the Q-fixed points on $\mathbf{F}_2[p_0^{\perp}]$.
- Both possibilities lead immediately to contradictions.

- Applying Clifford's Theorem, we have a $\mathbf{F}_2 G_{p_0}$-module decomposition
$$\mathbf{F}_2[p_0^\perp] = T \oplus W, \tag{10}$$
where T is the $q+2$-dimensional space of Q-fixed points and W is simple of dimension q^2-1.
- The intersection
$$\ker \pi_{P_1} \cap C(P,L) = \mathbf{F}_2[p_0^\perp] \cap C(P,L), \tag{11}$$
is an $\mathbf{F}_2 G_{p_0}$-submodule of $\mathbf{F}_2[p_0^\perp]$.
- The $q+1$ lines through p_0 lie in the intersection, accounting for $q+1$ dimensions of T.
- We must argue that the intersection is no bigger than their span. If it were, then by (10), $\mathbf{F}_2[p_0^\perp] \cap C(P,L)$ must contain either W or all the Q-fixed points on $\mathbf{F}_2[p_0^\perp]$.
- Both possibilities lead immediately to contradictions.

- Applying Clifford's Theorem, we have a $\mathbf{F}_2 G_{p_0}$-module decomposition
$$\mathbf{F}_2[p_0^\perp] = T \oplus W, \qquad (10)$$
where T is the $q+2$-dimensional space of Q-fixed points and W is simple of dimension q^2-1.
- The intersection
$$\ker \pi_{P_1} \cap C(P, L) = \mathbf{F}_2[p_0^\perp] \cap C(P, L), \qquad (11)$$
is an $\mathbf{F}_2 G_{p_0}$-submodule of $\mathbf{F}_2[p_0^\perp]$.
- The $q+1$ lines through p_0 lie in the intersection, accounting for $q+1$ dimensions of T.
- We must argue that the intersection is no bigger than their span. If it were, then by (10), $\mathbf{F}_2[p_0^\perp] \cap C(P, L)$ must contain either W or all the Q-fixed points on $\mathbf{F}_2[p_0^\perp]$.
- Both possibilities lead immediately to contradictions.

- Applying Clifford's Theorem, we have a $\mathbf{F}_2 G_{p_0}$-module decomposition

$$\mathbf{F}_2[p_0^{\perp}] = T \oplus W, \tag{10}$$

  where T is the $q+2$-dimensional space of Q-fixed points and W is simple of dimension $q^2 - 1$.
- The intersection

$$\ker \pi_{P_1} \cap C(P, L) = \mathbf{F}_2[p_0^{\perp}] \cap C(P, L), \tag{11}$$

  is an $\mathbf{F}_2 G_{p_0}$-submodule of $\mathbf{F}_2[p_0^{\perp}]$.
- The $q+1$ lines through p_0 lie in the intersection, accounting for $q+1$ dimensions of T.
- We must argue that the intersection is no bigger than their span. If it were, then by (10), $\mathbf{F}_2[p_0^{\perp}] \cap C(P, L)$ must contain either W or all the Q-fixed points on $\mathbf{F}_2[p_0^{\perp}]$.
- Both possibilities lead immediately to contradictions.

Lemma

$\ker \pi_{P_1} \cap C(P, L_1)$ *has dimension* $q - 1$*, and basis the set of functions* $\ell - \ell'$*, 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*.*

Lemma

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

Proof:

- By Lemma 9, 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 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 7 shows that ℓ lies in the span of Y and L_1.

Lemma

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

Proof:

- By Lemma 9, 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 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 7 shows that ℓ lies in the span of Y and L_1.

Lemma

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

Proof:

- By Lemma 9, 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 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 7 shows that ℓ lies in the span of Y and L_1.

Lemma

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

Proof:

- By Lemma 9, 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 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 7 shows that ℓ lies in the span of Y and L_1.

- The only line still missing is ℓ_0.
- By Lemma 5 applied to ℓ_0, we see that the constant function 1 is in the span.
- Finally, we see from Lemma 6 that

$$\sum_{\ell \in X_0} \Phi_\ell = 1 - \ell_0, \tag{12}$$

so we are done.

- The only line still missing is ℓ_0.
- By Lemma 5 applied to ℓ_0, we see that the constant function 1 is in the span.
- Finally, we see from Lemma 6 that

$$\sum_{\ell \in X_0} \Phi_\ell = 1 - \ell_0, \tag{12}$$

so we are done.

- The only line still missing is ℓ_0.
- By Lemma 5 applied to ℓ_0, we see that the constant function 1 is in the span.
- Finally, we see from Lemma 6 that

$$\sum_{\ell \in X_0} \Phi_\ell = 1 - \ell_0, \tag{12}$$

so we are done.

Further research

- Consider the binary code $\mathrm{LU}(3, q)$ when $q = 2^t$, $t \geq 1$.
- Corollary 4 provides a lower bound for the dimension.
- Note, however, that $\dim_{\mathbf{F}_2} C(P, L)$ is quite different:

Theorem

(Sastry-Sin) Assume $q = 2^t$. Then then the rank of $M_2(P, L)$ is

$$1 + \left(\frac{1+\sqrt{17}}{2}\right)^{2t} + \left(\frac{1-\sqrt{17}}{2}\right)^{2t}. \qquad (13)$$

Nevertheless:

- Computer calculations of J.-L. Kim (up to $q = 16$) suggested that the inequality (6) is equality for even q as well.
- Ogul Arslan has found a proof (2007).

Further research

- Consider the binary code $\mathrm{LU}(3, q)$ when $q = 2^t$, $t \geq 1$.
- Corollary 4 provides a lower bound for the dimension.
- Note, however, that $\dim_{\mathbf{F}_2} C(P, L)$ is quite different:

Theorem

(Sastry-Sin) Assume $q = 2^t$. Then then the rank of $M_2(P, L)$ is

$$1 + \left(\frac{1+\sqrt{17}}{2}\right)^{2t} + \left(\frac{1-\sqrt{17}}{2}\right)^{2t}. \tag{13}$$

Nevertheless:

- Computer calculations of J.-L. Kim (up to $q = 16$) suggested that the inequality (6) is equality for even q as well.
- Ogul Arslan has found a proof (2007).

Further research

- Consider the binary code $\mathrm{LU}(3, q)$ when $q = 2^t$, $t \geq 1$.
- Corollary 4 provides a lower bound for the dimension.
- Note, however, that $\dim_{\mathbf{F}_2} C(P, L)$ is quite different:

Theorem

(Sastry-Sin) Assume $q = 2^t$. Then then the rank of $M_2(P, L)$ is

$$1 + \left(\frac{1+\sqrt{17}}{2}\right)^{2t} + \left(\frac{1-\sqrt{17}}{2}\right)^{2t}. \tag{13}$$

Nevertheless:

- Computer calculations of J.-L. Kim (up to $q = 16$) suggested that the inequality (6) is equality for even q as well.
- Ogul Arslan has found a proof (2007).

Further research

- Consider the binary code $\mathrm{LU}(3, q)$ when $q = 2^t$, $t \geq 1$.
- Corollary 4 provides a lower bound for the dimension.
- Note, however, that $\dim_{\mathbf{F}_2} C(P, L)$ is quite different:

Theorem

(Sastry-Sin) Assume $q = 2^t$. Then then the rank of $M_2(P, L)$ is

$$1 + \left(\frac{1+\sqrt{17}}{2}\right)^{2t} + \left(\frac{1-\sqrt{17}}{2}\right)^{2t}. \qquad (13)$$

Nevertheless:

- Computer calculations of J.-L. Kim (up to $q = 16$) suggested that the inequality (6) is equality for even q as well.
- Ogul Arslan has found a proof (2007).

Further research

- Consider the binary code $\mathrm{LU}(3, q)$ when $q = 2^t$, $t \geq 1$.
- Corollary 4 provides a lower bound for the dimension.
- Note, however, that $\dim_{\mathbf{F}_2} C(P, L)$ is quite different:

Theorem

(Sastry-Sin) Assume $q = 2^t$. Then then the rank of $M_2(P, L)$ is

$$1 + \left(\frac{1+\sqrt{17}}{2}\right)^{2t} + \left(\frac{1-\sqrt{17}}{2}\right)^{2t}. \tag{13}$$

Nevertheless:

- Computer calculations of J.-L. Kim (up to $q = 16$) suggested that the inequality (6) is equality for even q as well.
- Ogul Arslan has found a proof (2007).

Further research

- Consider the binary code $\mathrm{LU}(3, q)$ when $q = 2^t$, $t \geq 1$.
- Corollary 4 provides a lower bound for the dimension.
- Note, however, that $\dim_{\mathbf{F}_2} C(P, L)$ is quite different:

Theorem

(Sastry-Sin) Assume $q = 2^t$. Then then the rank of $M_2(P, L)$ is

$$1 + \left(\frac{1+\sqrt{17}}{2}\right)^{2t} + \left(\frac{1-\sqrt{17}}{2}\right)^{2t}. \tag{13}$$

Nevertheless:

- Computer calculations of J.-L. Kim (up to $q = 16$) suggested that the inequality (6) is equality for even q as well.
- Ogul Arslan has found a proof (2007).