Codes from incidence matrices and line graphs of Paley graphs

D. Ghinelli[*]
Dipartimento di Matematica
Università di Roma 'La Sapienza'
I-00185 Rome, Italy

J.D. Key[†]
School of Mathematical Sciences
University of KwaZulu-Natal
Pietermaritzburg 3209, South Africa

December 13, 2010

Abstract

We examine the p-ary codes from incidence matrices of Paley graphs $P(q)$ where $q \equiv 1 \pmod 4$ is a prime power, and show that the codes are $[\frac{q(q-1)}{4}, q-1, \frac{q-1}{2}]_2$ or $[\frac{q(q-1)}{4}, q, \frac{q-1}{2}]_p$ for p odd. By finding PD-sets we show that for $q > 9$ the p-ary codes, for any p, can be used for permutation decoding for full error-correction. The binary code from the line graph of $P(q)$ is shown to be the same as the binary code from an incidence matrix for $P(q)$.

Keywords: Paley graphs, codes, permutation decoding
Mathematics Subject Classifications: 05C45, 05B05, 94B05

1 Introduction

The codes from the row span of adjacency matrices of Paley graphs are the well-known quadratic residue codes and studied in many texts. We look here at the codes from the row span of incidence matrices of Paley graphs, following the ideas of some earlier papers that studied such codes for various classes of graphs and their line graphs, including Hamming graphs, complete graphs, and complete bipartite graphs: see [15, 16, 7, 8, 6].

An incidence matrix G for a graph $\Gamma = (V, E)$ is a $|V| \times |E|$ matrix with rows labelled by the vertices and columns by the edges and an entry 1 if a vertex is on edge, 0 otherwise. Thus every column has two non-zero entries 1 in it, and the row corresponding to a vertex has k non-zero entries 1, where k is the valency of the vertex. If Γ is regular, G can be regarded as an incidence matrix for a 1-design on $|E|$ vertices, called an incidence design for Γ. The p-ary codes, for any prime p, obtained from the row span of these incidence matrices for graphs from various infinite classes of regular connected graphs, have been shown to have certain common properties relating to dimension, minimum weight, minimum-weight vectors, and minimun weight of the dual code, *viz.*, the dimension is $|V|$ or $|V| - 1$, the minimum weight the valency k, the minimum words are the scalar multiples of the rows of G, and the minimum weight of the dual code is 4 when closed paths of length 4 are present, or 3 in the binary case: see [7, 8, 15, 16] for some classes of graphs. In addition, it has been observed that there is often a gap in the weight enumerator between k and $2(k-1)$, the latter arising

[*] dina@mat.uniroma1.it
[†] keyj@clemson.edu

from the difference of two rows. This recalls a similar gap in the codes from desarguesian projective planes: see [5] and [18, 23] for further results and a full bibliography of this property.

If $L(\Gamma)$ denotes the line graph of Γ, then the code $C_p(L(\Gamma))$ spanned by the rows of an adjacency matrix of $L(\Gamma)$ over $\mathbb{F}_p$ will be a subcode of $C_2(G)$ if $p = 2$, of minimum weight usually k or $2(k-1)$; if p is odd, the code is of little use, being of minimum weight at most 4 when Γ has closed paths of length 4.

We examine here these codes for the Paley graphs $P(q)$ which are defined to have vertices the set of elements of the finite field $\mathbb{F}_q$ where $q \equiv 1 \pmod 4$ and two vertices x, y are adjacent if $x - y$ is a non-zero square. Thus $P(q)$ is regular of valency $\frac{q-1}{2}$ and with $\frac{q(q-1)}{4}$ edges. Our main result is:

Theorem 1 *Let $P(q)$ denote the Paley graph on q vertices, where $q \geq 9$ is a prime power, and $q \equiv 1 \pmod 4$. Let $\mathcal{G}_q$ denote the 1-$(\frac{q(q-1)}{4}, \frac{q-1}{2}, 2)$ incidence design of $P(q)$. Then, for any prime p,*

1. *(a)*
$$C_2(\mathcal{G}_q) = [\frac{q(q-1)}{4}, q-1, \frac{q-1}{2}]_2, \; C_2(\mathcal{G}_q)^\perp = [\frac{q(q-1)}{4}, \frac{(q-1)(q-4)}{4}, 3]_2;$$
   (b)
$$C_p(\mathcal{G}_q) = [\frac{q(q-1)}{4}, q, \frac{q-1}{2}]_p, \; C_p(\mathcal{G}_q)^\perp = [\frac{q(q-1)}{4}, \frac{q(q-5)}{4}, 4]_p$$
   for p odd.

   The codes $C_p(\mathcal{G}_q)$ can correct $\frac{q-5}{4}$ errors.

2. *If $L(P(q))$ denotes the line graph of $P(q)$ and $C_p(L(P(q)))$ the code from the row span over F_p of an adjacency matrix for $L(P(q))$, then $C_2(L(P(q)) = C_2(\mathcal{G}_q))$, and for p odd, $C_p(L(P(q))$ has words of weight* 4.

3. *For q prime, let*
$$\mathcal{I} = \{[0,1], [1,2], \ldots, [q-1,0]\}, \; \mathcal{I}^* = \mathcal{I} \setminus \{[q-1,0]\},$$
   be sets of edges of $P(q)$. Then $\mathcal{I}$ is an information set for $C_p(\mathcal{G}_q)$ for p odd, and $\mathcal{I}^*$ is an information set for $C_2(\mathcal{G}_q)$. For $q \geq 13$ the set of automorphisms obtained from multiplication by the non-zero squares in $\mathbb{F}_q$ form a PD-set of size $\frac{q-1}{2}$ for $C_p(\mathcal{G}_q)$ for any prime p with information set $\mathcal{I}$ for p odd, or information set $\mathcal{I}^*$ for $p = 2$.

   For all $q > 9$, any subgroup of the automorphism group that is transitive on edges will form a PD-set for $C_p(\mathcal{G}_q)$ for all p.

The proof of the theorem follows from Propositions 3, 5, 6 and Corollary 4 in the sections to follow. Section 2 contains some background results and terminology, including a description of permutation decoding; Section 3 has a result that holds for any strongly regular graph. Our main results about the codes from the incidence matrices of Paley graphs are in Section 4. In Section 5 we obtain the PD-sets, in Section 6 we examine the codes from line graphs, and in Section 7 we obtain some computational results concerning the binary hulls of the codes. Computations were done with Magma [3, 4].

2 General observations and background

The notation for designs and codes is as in [1]. An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{J})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{J}$ is a t-(v, k, λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. The design is **symmetric** if it has the same number of points and blocks. The **code** $C_F(\mathcal{D})$ **of the design** $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F. If $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the **incidence vector** of $\mathcal{Q}$ by $v^{\mathcal{Q}}$, and if $\mathcal{Q} = \{P\}$ where $P \in \mathcal{P}$, then we will write v^P instead of $v^{\{P\}}$. Thus $C_F(\mathcal{D}) = \langle v^B \mid B \in \mathcal{B} \rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F. For any $w \in F^{\mathcal{P}}$ and $P \in \mathcal{P}$, $w(P)$ denotes the value of w at P. If $F = \mathbb{F}_p$ then the $\boldsymbol{p}$**-rank** of the design, written $\text{rank}_p(\mathcal{D})$, is the dimension of its code $C_F(\mathcal{D})$, which we usually write as $C_p(\mathcal{D})$.

All the codes here are **linear codes**, and the notation $[n, k, d]_q$ will be used for a q-ary code C of length n, dimension k, and minimum weight d, where the **weight** $\text{wt}(v)$ of a vector v is the number of non-zero coordinate entries. The **support**, $\text{Supp}(v)$, of a vector v is the set of coordinate positions where the entry in v is non-zero. So $|\text{Supp}(v)| = \text{wt}(v)$. The **distance** $d(u, v)$ between two vectors u, v is the number of coordinate positions in which they differ, i.e., $\text{wt}(u - v)$. A **generator matrix** for C is a $k \times n$ matrix made up of a basis for C, and the **dual** code $C^\perp$ is the orthogonal under the standard inner product $(,)$, i.e. $C^\perp = \{v \in F^n \mid (v, c) = 0 \text{ for all } c \in C\}$. If $C = C_p(\mathcal{D})$, where $\mathcal{D}$ is a design, then $C \cap C^\perp$ is the **hull** of $\mathcal{D}$ at p, or simply the **hull** of $\mathcal{D}$ or C if p and $\mathcal{D}$ are clear from the context. A **check matrix** for C is a generator matrix for $C^\perp$. The **all-one vector** will be denoted by $\boldsymbol{\jmath}$, and is the vector with all entries equal to 1. If we need to specify the length m of the all-one vector, we write $\boldsymbol{\jmath}_m$. A **constant** vector has all entries either 0 or some fixed non-zero $a \in F$, i.e. a scalar multiple of some incidence vector. We call two linear codes **isomorphic** if they can be obtained from one another by permuting the coordinate positions. An **automorphism** of a code C is an isomorphism from C to C. The automorphism group will be denoted by $\text{Aut}(C)$. Any code is isomorphic to a code with generator matrix in so-called **standard form**, i.e. the form $[I_k \mid A]$; a check matrix then is given by $[-A^T \mid I_{n-k}]$. The set of the first k coordinates in the standard form is called an **information set** for the code, and the set of the last $n-k$ coordinates is the corresponding **check set**.

The **graphs**, $\Gamma = (V, E)$ with vertex set V and edge set E, discussed here are undirected with no loops and no multiple edges. If $x, y \in V$ and x and y are adjacent, we write $x \sim y$, and $[\boldsymbol{x}, \boldsymbol{y}]$ for the edge in E that they define. The **valency** of a vertex is the number of vertices adjacent to it, and the graph is **regular** if all the vertices have the same valency.. If $[x_i, x_{i+1}]$ for $i = 1$ to $r - 1$, and $[x_r, x_1]$ are all edges of Γ, and the x_i are all distinct, then the sequence written $(x_1, \ldots, x_r)$ will be called a **closed path** or **circuit** of length r for Γ. A closed path that goes through every vertex of Γ exactly once is called a **Hamiltonian path** and if a graph has such a path, it is called **Hamiltonian**. If for every pair of vertices there is a path connecting them, the graph is **connected**.

An **adjacency matrix** A of a graph $\Gamma = (V, E)$ is a $|V| \times |V|$ matrix with entries a_{ij} such that $a_{ij} = 1$ if vertices v_i and v_j are adjacent, and $a_{ij} = 0$ otherwise. An **incidence matrix** of Γ is an $|V| \times |E|$ matrix B with $b_{i,j} = 1$ if the vertex labelled by i is on the edge labelled by j, and $b_{i,j} = 0$ otherwise. If Γ is regular with valency k, then the 1-$(|E|, k, 2)$ design with incidence matrix B is called the **incidence design** of Γ. The **neighbourhood design** of a regular graph is the 1-design formed by taking the points to be the vertices of the graph and the blocks to be the sets of neighbours of a vertex, for each vertex, i.e. regarding an adjacency matrix as an incidence matrix for the design.

The **line graph** of a graph $\Gamma = (V, E)$ is the graph $L(\Gamma)$ with E as vertex set and where adjacency is defined so that e and f in E, as vertices, are adjacent in $L(\Gamma)$ if e and f as edges of Γ share a vertex in Γ. A **strongly regular graph** Γ of type (n, k, λ, μ) is a regular graph on $n = |V|$ vertices, with valency k which is such that any two adjacent vertices are together adjacent to λ vertices and any two non-adjacent vertices are together adjacent to μ vertices. The complement of the graph Γ is also strongly regular of type $(n, n-k-1, n-2k+\mu-2, n-2k+\lambda)$. To avoid trivial cases, we require that a strongly regular graph and its complement are both connected, and so $0 < \mu < k < n-1$.

The **code** of a graph Γ over a finite field F is the row span of an adjacency matrix A over the field F, denoted by $C_F(\Gamma)$ or $C_F(A)$. The dimension of the code is the rank of the matrix over F, also written $\mathrm{rank}_p(A)$ if $F = \mathbb{F}_p$, in which case we will speak of the p**-rank** of A or Γ, and write $C_p(\Gamma)$ or $C_p(A)$ for the code. It is also the code over F_p of the neighbourhood design. Similarly, if B is an incidence matrix for Γ, $C_p(B)$ denotes the row span of B over F_p and is the code of the design with blocks the rows of B, in the case that Γ is regular. If M is an adjacency matrix for $L(\Gamma)$ where Γ is regular of valency k, $|V|$ vertices, $|E|$ edges, then

$$BB^T = A + kI_{|V|} \text{ and } B^TB = M + 2I_{|E|}, \tag{1}$$

where A is an adjacency matrix, and B an incidence matrix, for Γ.

Permutation decoding was first developed by MacWilliams [19] and involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and Sloane [20, Chapter 16, p. 513] and Huffman [10, Section 8]. In [12] and [17] the definition of PD-sets was extended to that of s-PD-sets for s-error-correction:

Definition 1 *If C is a t-error-correcting code with information set $\mathcal{I}$ and check set $\mathcal{C}$, then a* **PD-set** *for C is a set $\mathcal{S}$ of automorphisms of C which is such that every t-set of coordinate positions is moved by at least one member of $\mathcal{S}$ into the check positions $\mathcal{C}$.*

The algorithm for permutation decoding is given in [10] and requires that the generator matrix is in standard form.

Such sets might not exist at all, and the property of having a PD-set might not be invariant under isomorphism of codes, i.e. it depends on the choice of $\mathcal{I}$ and $\mathcal{C}$. Furthermore, there is a bound on the minimum size that the set $\mathcal{S}$ may have, due to Gordon [9], from a formula due to Schönheim [22], and quoted and proved in [10]:

Result 1 *If $\mathcal{S}$ is a PD-set for a t-error-correcting $[n, k, d]_q$ code C, and $r = n - k$, then*

$$|\mathcal{S}| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \dots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \dots \right\rceil \right\rceil \right\rceil .$$

This result can be adapted to s-PD-sets for $s \leq t$ by replacing t by s in the formula.

We will need the following results from [8]:

Result 2 *Let $\Gamma = (V, E)$ be a graph, $L(\Gamma)$ its line graph, G a $|V| \times |E|$ incidence matrix for Γ, and $\gamma = (P, Q, R, S)$ a closed path in Γ. Let*

$$u(\gamma) = v^{[P,Q]} + v^{[R,S]} - v^{[P,S]} - v^{[Q,R]}. \tag{2}$$

Then

1. *for any prime p, $u(\gamma) \in C_p(G)^\perp$; for p an odd prime, $u(\gamma) \in C_p(L(\Gamma))$;*
2. *if Γ is regular with valency k and $\mathcal{G}$ the 1-$(|E|, k, 2)$ incidence design for Γ, then $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\mathcal{G})$.*

For a regular graph $\Gamma = (V, E)$ of valency k, the incidence design $\mathcal{G}$ of Γ has a block of size k defined for each vertex P which we will denote by $\bar{P}$ where

$$\bar{P} = \{[P, Q] \mid Q \in V\}, \tag{3}$$

i.e. corresponding to the set of k edges through P.

The following is from [6, 14].

Result 3 *Let $\Gamma = (V, E)$ be a graph, G an incidence matrix for Γ, $C_p(G)$ the row-span of G over $\mathbb{F}_p$. If Γ is connected then $\dim(C_2(G)) = |V| - 1$, and if Γ is connected and has a closed path of odd length ≥ 3, then $\dim(C_p(G)) = |V|$ for odd p.*

Proof: Let $C = C_p(G)$. That $\dim(C) \geq |V| - 1$ for a connected graph, is well known, but can be proved by induction on $|V| = n$ by using a standard result concerning graphs, and proved in [2, Theorem 3.1.10], for example, that any connected graph with $|V| \geq 2$ has at least two non-cut vertices, where a cut vertex is one that when removed from a connected graph disconnects the graph. For then, since it is clearly true for $n = 2$, supposing the stated result is true for $n - 1$ vertices, and $|V| = n$, then by removing one of these non-cut vertices, say P, the remaining graph on $n - 1$ vertices will still give rank at least $n - 2$, and by adjoining P the rank becomes at least $n - 1$. Clearly there is equality for $p = 2$.

For p odd, let $w = \sum a_i r_i$ be a sum of multiples of the rows of G. We wish to show that if $w = 0$ then all the a_i are 0. So suppose $w = 0$. Denoting the vertices of the graph by the labels of the rows, if $[i, j]$ is an edge then $a_i = -a_j$. Taking a path of odd length $i_0, i_1, \ldots i_m$ we see that $a_{i_0} = -a_{i_1} = \ldots = a_{i_m} = -a_{i_0}$, so $a_{i_0} = 0$. Since the graph is connected, we thus get $a_i = 0$ for all i, as required. ■

Corollary 2 *If $\Gamma = (V, E)$ is a strongly regular graph with $\lambda \geq 1$, then the p-rank of an incidence matrix for Γ for p odd is $|V|$.*

Proof: If $\lambda \neq 0$ then clearly Γ has triangles, i.e. closed paths of length 3. ■

3 Incidence designs of strongly regular graphs

Now let Γ be a strongly regular graph with parameters (v, k, λ, μ). We assume that Γ is connected, that $0 < \mu < k < v - 1$ and that it has closed paths of length 4, so that from Result 2, for any prime p, the dual of the p-ary code from an incidence matrix has words of weight 4.

Proposition 1 *Let $\Gamma = (V, E)$ be a strongly regular graph with parameters (v, k, λ, μ). Let $\mathcal{G}$ be the 1-$(\frac{vk}{2}, k, 2)$ incidence design of Γ and let $C = C_p(\mathcal{G})$, where p is any prime.*

Let $\mathcal{B}$ denote the set of supports of the weight-4 vectors of $C^\perp$ as obtained in Result 2. Then $\mathcal{B}$ is the set of blocks of a 1-$(\frac{vk}{2}, 4, r)$ design $\mathcal{F}$ where

$$r = (k - \lambda - 1)(\mu - 1) + \lambda(\lambda - 1). \tag{4}$$

If $\mathcal{P}$ denotes the point set of $\mathcal{G}$, then for $X \in \mathcal{P}$ the number of blocks of $\mathcal{B}$ through X and another point $Y \in \mathcal{P}$ is in the set $\mathcal{N} = \{0, 1, 2, \mu - 1, \lambda - 1\}$.

Proof: We look at the closed paths (P, Q, R, S) of vertices of Γ and, taking a point $X = [P, Q] \in \mathcal{P}$, we count the number of paths that contain X.

Since $P \sim Q$ there are λ vertices in V adjacent to both P and Q, and $(k - \lambda - 1)$ vertices R adjacent to Q but not to P. The number of $S \in V$, excluding Q, that are adjacent to both P and R is $(\mu - 1)$, giving $(k - \lambda - 1)(\mu - 1)$ such paths. Now counting the paths where $R \sim P$ as well as $R \sim Q$, there are λ such R, and then $(\lambda - 1)$ such S, excluding Q, that are adjacent to R and P, giving another $\lambda(\lambda - 1)$ paths. This gives the asserted value for r.

Let $X = [P, Q]$ and count the number of blocks of $\mathcal{B}$ through X and Y for various types of $Y \in \mathcal{P}$:

1. if $Y = [Q, R]$ then we get either $\lambda - 1$ or $\mu - 1$ vertices S, depending on $P \sim R$ or not. The support of such a block would be $\{[P, Q], [P, S], [Q, R], [R, S]\}$. Similarly if $Y = [P, S]$.

2. if $Y = [R, S]$ where $R, S \neq P, Q$, then for X and Y to be on a block we need $[P, R]$ and $[Q, S]$, or $[P, S]$ and $[Q, R]$, or both, giving one, two or no blocks if none of these three options hold.

This completes the proof. ■

With the same notation as in Proposition 1:

Proposition 2 *Let Γ be a (v, k, λ, μ) strongly regular graph. Let $m = \max\{2, \lambda - 1, \mu - 1\}$. If s is the weight of a word in $C = C_p(\mathcal{G})$, then*

$$s \geq 1 + \frac{1}{m}\left((k - \lambda - 1)(\mu - 1) + \lambda(\lambda - 1)\right).$$

Proof: Let $w \in C$ and $\mathcal{S} = \text{Supp}(w)$, and $s = |\mathcal{S}|$. Let $X \in \mathcal{S}$. Using notation as in Proposition 1, we look at the blocks of $\mathcal{B}$ through X and note that they must meet $\mathcal{S}$ again, since the corresponding weight-4 vector is in $C^{\perp}$. Suppose there are z_i blocks in $\mathcal{B}$ through X that meet $\mathcal{S}$ in i points. So $z_0 = z_1 = z_i = 0$ for $i \geq 5$, and $r = z_2 + z_3 + z_4$. Suppose there are r_j points $Y \in \mathcal{S}$ such that X and Y are on j blocks of $\mathcal{B}$. So $j \in \mathcal{N} = \{0, 1, 2, \lambda - 1, \mu - 1\}$. Then $s = 1 + \sum_{j \in \mathcal{N}} r_j$ and counting incidences gives

$$r \leq z_2 + 2z_3 + 3z_4 = \sum_{j \in \mathcal{N}} j r_j = r_1 + 2r_2 + (\lambda - 1)r_{\lambda-1} + (\mu - 1)r_{\mu-1} \leq m(s - 1 - r_0). \qquad (5)$$

Since, from Equation (4), $r = (k - \lambda - 1)(\mu - 1) + \lambda(\lambda - 1)$, we get

$$s \geq 1 + r_0 + \frac{1}{m}\left((k - \lambda - 1)(\mu - 1) + \lambda(\lambda - 1)\right), \qquad (6)$$

giving a lower bound for the minimum weight of C. ■

Example 1 If $\lambda = \mu$ then the neighbourhood design is a 2-design, and from Equation (6) we obtain $s = k$, the valency, as the minimum weight of $C_p(\mathcal{G})$.

4 Paley graphs

Let q be a prime power with $q \equiv 1 \pmod 4$. The **Paley graph**, denoted by $P(q)$, has the finite field $\mathbb{F}_q$ of order q as vertex set and two vertices x and y are adjacent if and only if $x-y$ is a non-zero square in $\mathbb{F}_q$. Since $q \equiv 1 \pmod 4$, -1 is a square in $\mathbb{F}_q$. The condition that -1 is a square in $\mathbb{F}_q$ is required to ensure that $[x,y]$ is an edge if and only if $[y,x]$ is. Thus $P(q)$ is well-defined. The Paley graph is a strongly regular graph of type $(q, \frac{q-1}{2}, \frac{q-1}{4}-1, \frac{q-1}{4})$ and is isomorphic to its complement. We will also make use of the fact that $P(q)$ is Hamiltonian, as is well-known: see, for example, [21, 11].

Let $q = q_1^e$ where q_1 is a prime and $\mathbb{F}_q^* = \langle w \rangle$. For any $\sigma \in Aut(\mathbb{F}_q)$ and $a, b \in \mathbb{F}_q$ with $a \in \langle w^2 \rangle$, we define the map $\tau_{a,b,\sigma}$ on $\mathbb{F}_q$ by

$$\tau_{a,b,\sigma} : x \mapsto ax^\sigma + b, \tag{7}$$

for $x \in \mathbb{F}_q$. Then

$$A_q = \{\tau_{a,b,\sigma} \mid \sigma \in Aut(\mathbb{F}_q),\ a, b \in \mathbb{F}_q,\ a \text{ a non-zero square}\} \tag{8}$$

is well-known to be the automorphism group of $P(q)$, of order $\frac{1}{2}eq(q-1)$. It is transitive on vertices of $P(q)$ but not 2-transitive. Of course $A_q \subseteq A\Gamma L_1(\mathbb{F}_q)$.

We look here at the incidence design of $P(q)$ for $q \geq 9$, i.e. $\mathcal{G}_q$, a 1-$(\frac{q(q-1)}{4}, \frac{q-1}{2}, 2)$ design, from an incidence matrix $G(q)$ for $P(q)$, with point set

$$\mathcal{P} = \{[x, x+y] \mid x \in F_q, y \text{ a non-zero square of } \mathbb{F}_q\} \tag{9}$$

of size $\frac{q(q-1)}{4}$. There are q blocks, one defined for each $x \in F_q$, which we denote by $\bar{x}$, so that

$$\bar{x} = \{[x, x+y] \mid y \text{ a non-zero square of } \mathbb{F}_q\}. \tag{10}$$

The group A_q of Equation (8) acts on $\mathcal{G}_q$ and is transitive on $\mathcal{P}$, as can easily be verified. For notation we will use letters $x, y, z \in F_q$ etc. for the vertices of $P(q)$, i.e. elements of $\mathbb{F}_q$, and capital letters $P, Q, R \in \mathcal{P}$ etc. for the points of the incidence design $\mathcal{G}_q$.

Proposition 3 *Let $\Gamma = P(q)$ where $q \geq 9$, q a prime power, and $q \equiv 1 \pmod 4$. Let $\mathcal{G}_q$ be the 1-$(\frac{q(q-1)}{4}, \frac{q-1}{2}, 2)$ incidence design of $P(q)$. Then*

- $C_2(\mathcal{G}_q) = [\frac{q(q-1)}{4}, q-1, \frac{q-1}{2}]_2$, $\quad C_2(\mathcal{G}_q)^\perp = [\frac{q(q-1)}{4}, \frac{(q-1)(q-4)}{4}, 3]_2$;
- $C_p(\mathcal{G}_q) = [\frac{q(q-1)}{4}, q, \frac{q-1}{2}]_p$, $\quad C_p(\mathcal{G}_q)^\perp = [\frac{q(q-1)}{4}, \frac{q(q-5)}{4}, 4]_p$ *for p odd.*

For all p, $C_p(\mathcal{G}_q)$ can correct $\frac{q-5}{4}$ errors.

Proof: Let $C = C_p(\mathcal{G}_q)$. The dimension of the code in each case is as stated by Result 3 and Corollary 2. Let $w \in C$ and $\mathcal{S} = \mathrm{Supp}(w)$, and $s = |\mathcal{S}|$.

To get the minimum weight, we apply Propositions 1 and 2 since for $q \geq 9$, $P(q)$ has closed paths of length 4. The Paley graph $P(q)$ has $v = q \equiv 1 \pmod 4$ where q is a prime power, $k = \frac{q-1}{2}$, $\lambda = \frac{q-1}{4} - 1$, $\mu = \frac{q-1}{4} \geq 3$ for $q \geq 13$. So, in the notation of the propositions, $r = \frac{(q-5)^2}{8}$ and $m = \mu - 1 = \frac{q-5}{4}$ for $q \geq 13$. For $q = 9$, $\mu - 1 = 1$, but we still have $m = 1$ since the second type of point $[u,v]$ in the proof of Proposition 1 can only yield one 4-block through $[x,y]$ and $[u,v]$ for $q=9$, as can easily be verified directly. Thus $m=\mu-1$ in this case too.

The inequality from Equation (6) becomes, for $q \geq 9$:

$$s \geq r_0 + \frac{q-1}{2} - 1 \geq \frac{q-1}{2} - 1. \tag{11}$$

If $s = \frac{q-1}{2} - 1 = k-1$ then this implies that $r_0 = 0$ for all points of $\mathcal{S}$, i.e. every pair of points of $\mathcal{S}$ are together on a weight-4 block of $\mathcal{B}$. Furthermore, if $s = \frac{q-1}{2} - 1$, Equation (5) gives

$$r \leq z_2 + 2z_3 + 3z_4 \leq (\frac{q-5}{4})(\frac{q-1}{2} - 2) = r,$$

so $r = z_2 + z_3 + z_4 = z_2 + 2z_3 + 3z_4$ for all points of $\mathcal{S}$, and thus $z_3 = z_4 = 0$ for all points of $\mathcal{S}$.

For $p=2$, since the binary code is generated by vectors of even weight $k = \frac{q-1}{2}$, all the vectors of C must have even weight, so the minimum weight is $k = \frac{q-1}{2}$.

If $p \neq 2$, then for any point P of $\mathcal{S}$, every block of $\mathcal{B}$ that contains it must meet $\mathcal{S}$ just once again. The maximum number of blocks through P and another point Q is $\mu - 1$, and if $P = [x,y]$ then this occurs if $Q = [x,z]$ or $[y,w]$ if $\mu - 1 > 2$. Since there are $k-2$ points in $\mathcal{S}$ other than P, the number of blocks covered is at most $(k-2)(\mu-1) = (\frac{q-5}{2})(\frac{q-5}{2}) = r$, so that all the points must be of the form $Q = [x,z]$ or $[y,w]$, if $\mu - 1 > 2$. So for $q > 13$ this is the case and w is a constant word. If there are points of the form $[x,y_1]$ and $[y,x_1]$ then, since the deduction regarding the nature of the points in $\mathcal{S}$ is true for every point, we must have $x_1 = y_1$, and thus there is no other point $[x,y_2]$ nor $[y,x_2]$. So all the points of $\mathcal{S}$ have the form $[x,y_i]$ say, and hence $w - v^{\overline{x}}$ has weight 1, which is impossible. This proves the assertion for $q \geq 17$.

For $q = 13$, $k = 6$, $\mu - 1 = 2 = \lambda$, and the above argument will apply if all the points of $\mathcal{S}$ have the form $[x,z],[y,w]$. Otherwise there can be points of the form $[z,w]$ on two blocks with $[x,y]$, so that, from the proof of Proposition 1, $x \sim z, x \sim w, y \sim z, y \sim w$, and since $\lambda = 2$, there can be no other points of this type in $\mathcal{S}$. So there are at least three points other than $[x,y]$ of the type $[x,y_1]$ or $[y,x_1]$ and hence of the form $[x,x_i]$, by the above argument. Thus $w - v^{\overline{x}}$ has weight 3, a contradiction.

For $q = 9$, $k = 4$, $\mu - 1 = 1 = m = \lambda$, as pointed out before, and $r = 2$. If $P = [0,1] \in \mathcal{S}$ then the two blocks of $\mathcal{B}$ must meet $\mathcal{S}$ again, and this must be true for each of the three points in $\mathcal{S}$. Using the minimum polynomial $X^2 - X - 1$ to construct $\mathbb{F}_9$, and letting w be a primitive root of this, an examination of the blocks of $\mathcal{B}$ yields that the other two points of $\mathcal{S}$ must be $[w^2,w^7],[w^5,w^6]$. This has to have inner product 0 with every block in $\mathcal{B}$, which means the signs on any pair of these points must differ. This is impossible, which means the minimum weight is 4.

That C can correct $\frac{q-5}{4}$ errors follows from $\left\lfloor (\frac{q-1}{2} - 1)/2 \right\rfloor = \frac{q-5}{4}$, since $q \equiv 1 \pmod 4$.

For the statements about the dual codes, for $q \geq 9$ we have already used the fact that $C^{\perp}$ has words of weight 4 for all p. For $p = 2$, any triangle (x,y,z) of points in $P(q)$ will give a word

$$u = v^{[x,y]} + v^{[y,z]} + v^{[z,x]} \in C^{\perp}.$$

Clearly the minimum weight cannot be 2, so it is 3 for $p = 2$. For p odd, if there is a word w of weight 3 in the dual, the support will either be a triangle or part of a row corresponding to a vertex x, say. If a triangle with $\mathrm{Supp}(w) = \{[x,y],[y,z],[z,x]\}$, then $w([x,y]) = -w([y,z]) = w([z,x]) = -w([x,y])$

which is impossible for p odd. If $\mathrm{Supp}(w) = \{[x,y],[x,z],[x,u]\}$ where y,z,u are distinct, then $(w,\bar{y}) \neq 0$, a contradiction. ■

Note: (1). Computations using Magma [3, 4] show that the minimum words of the binary codes are the rows of the incidence matrix for $q = 9, 13, 17, 25$, and that it is also true (with scalar multiples) for the ternary codes for $q = 9, 13, 17$. We prove this below for all p for $q = 9$, and note that it has been shown in [14] to be true for $q > 17$. Also, for all computationally feasible values of q and p we found that the next weight after $\frac{q-1}{2}$ is that of the difference of two rows of the incidence matrix, i.e. $2(\frac{q-1}{2} - 1) = (q-3)$. There may be other vectors of this weight when $p \neq 2$.
(2). Computations also yielded that, for the binary case, for $q \geq 17$,

- every weight-4 vector in the dual code can be expressed as a sum of vectors of weight 3, i.e. from triangles of points in $P(q)$;
- the dual code is generated by the words of weight 3.

This does not hold for $q = 9, 13$ since there are insufficient triangles.

In the following we use the notation $u(\gamma)$, where γ is a closed path of length 4 in the graph, as given in Equation (2).

Proposition 4 *Let $\Gamma = P(9)$, $\mathcal{G}_9$ its 1-$(18,4,2)$ its incidence design. Then*

- $C_2(\mathcal{G}_9) = [18,8,4]_2$, $\quad C_2(\mathcal{G}_9)^\perp = [18,10,3]_2$, $\quad \mathrm{Hull}_2(\mathcal{G}_9) = [18,4,8]_2$ *;*
- $C_p(\mathcal{G}_9) = [18,9,4]_p$, $\quad C_p(\mathcal{G}_9)^\perp = [18,9,4]_p$ *for p odd.*

and the vectors of weight $\frac{q-1}{2} = 4$ of $C_p(\mathcal{G}_9)$, for all p, are the scalar multiples of the rows of an incidence matrix. Furthermore, there are no vectors in $C_p(\mathcal{G}_9)$ having weight m in the range $4 = \frac{q-1}{2} < m < 2(\frac{q-1}{2} - 1) = (q-3) = 6$ for $2 \leq p \leq 17$. If the minimum polynomial of $w \in \mathbb{F}_9$ is $X^2 - X - 1$ then

$$(0, 1, 2, w, w^3, w^6, w^5, w^7, w^2)$$

is a closed Hamiltonian path for $P(9)$.

If $\gamma = (x_0, x_1, x_2, x_3)$ is a closed path of length 4 in $P(9)$ with $x_0 \not\sim x_2$, $x_1 \not\sim x_3$, and if, for $0 \leq i \leq 3$, γ_i denotes the closed path of length 4 through x_i that meets γ only in x_i, then

$$\sum_{i=0}^{3} v^{\overline{x_i}} = \sum_{i=0}^{3} u(\gamma_i)$$

is a vector of weight 8 in $\mathrm{Hull}_2(\mathcal{G}_9)$.

Proof: For all p we know that the minumum weight of $C_p(\mathcal{G}_9)$ is 4 from Proposition 3. To show that the minimum words are as stated, for $p = 2$ we can simply use Magma.

Now take p odd, and suppose $P = [0,1] \in \mathcal{S}$. We need to show that words of this weight are the scalar multiples of the rows of an incidence matrix. For the design of supports of weight-4 vectors in the dual code, we have $r = \frac{(q-5)^2}{8} = 2$. Putting $s = 4$ in the Equation (11) gives $r_0 \leq 1$. If $r_0 = 0$ then one of the blocks of $\mathcal{B}$ through P must have three points in $\mathcal{S}$. But, by examining the nine blocks in $\mathcal{B}$, we see that the other block through one of these points cannot meet $\mathcal{S}$ again. Thus $r_0 = 1$ for every point on $\mathcal{S}$. This means that $\mathcal{S}$ consists of one point on each of the two blocks, b_1, b_2, of $\mathcal{B}$ through P, the point P, and one more point that is not on a block with P. If Q and R are the two points in $\mathcal{S}$ on b_1 and b_2 respectively, then the other blocks through these points must contain the last point, T, of the set $\mathcal{S}$. An analysis of the possibilities yields that the support is either the block $\bar{0}$ or $\bar{1}$ of $\mathcal{G}$. Thus the support is that of a block and since this is the minimum weight, it is clear that the word must be a scalar multiple of the row corresponding to that block.

For codewords of weight m in the range $\frac{q-1}{2} = 4 < m < 2(\frac{q-1}{2} - 1) = q - 3 = 6$, i.e. only $m = 5$ for $q = 9$, clearly it cannot happen for the even-weight code when $p = 2$, and the other primes up and including 17 were verified using Magma. Words of weight $2(\frac{q-1}{2} - 1)$ arise from the difference of two rows whose indexing vertices are adjacent.

The statement about the dual codes follows from Proposition 3 and that the path given is Hamiltonian is easily verified.

Finally, to prove the equality given for the word in the binary hull, the left-hand side is easily seen to have weight 8. For the right-hand side, first observe that each edge $[x_i, x_{i+1}]$ (suffixes modulo 4) determines a unique third point of a triangle $x_{i,i+1}$, since $\lambda = 1$, giving at most four more points. There is thus another point x that cannot be adjacent to any of the x_i, $0 \leq i \leq 3$ since all the adjacencies are used up, and thus must be adjacent to the $x_{i,i+1}$ (suffixes modulo 4) and these are thus all distinct. Thus $\gamma_i = (x_i, x_{i,i+1}, x, x_{i+3,i})$ (suffixes modulo 4) for $0 \leq i \leq 3$. The stated identity then follows. ■

5 Permutation decoding for $C_p(\mathcal{G}_q)$

We show that the codes from the incidence matrices for Paley graphs can be used for full error correction by permutation decoding. As before, $\mathcal{G}_q$ will denote the incidence 1-$(\frac{q(q-1)}{4}, \frac{q-1}{2}, 2)$ design for $P(q)$.

Lemma 1 *If $(x_1, \ldots, x_q)$ is a closed path of length q, $x_i \neq x_j$ for $i \neq j$, for the Paley graph $P(q)$ where $q \geq 9$, $q \equiv 1 \pmod 4$, then $\mathcal{I} = \{[x_1, x_2], [x_2, x_3], \ldots, [x_{n-1}, x_n], [x_n, x_1]\}$ is an information set for $C_p(\mathcal{G}_q)$ for p odd, and $\mathcal{I} \setminus \{[x_n, x_1]\}$ is an information set for $C_2(\mathcal{G}_q)$.*

In particular, if q is a prime, then $(0, 1, \ldots, q-1)$ is a closed Hamiltonian path.

Proof: The path exhibited in the statement clearly is a closed Hamiltonian path when q is a prime. That $\mathcal{I}$ (respectively $\mathcal{I} \setminus \{[x_n, x_1]\}$) is an information set for the p-ary (respectively binary) code follows by labelling the rows of the incidence matrix $G(q)$ by $x_1, \ldots, x_q$ and the columns by $[x_1, x_2], [x_2, x_3], \ldots, [x_n, x_1]$ (respectively $[x_1, x_2], [x_2, x_3], \ldots, [x_{n-1}, x_n]$) and noticing that a row-echelon-form can be obtained immediately. ■

We now establish PD-sets in the case where q is a prime. We take $q \geq 13$ since PD-sets are only needed for correcting at least two errors, so we only consider minimum weight at least 5. For q prime, we have $\sigma = 1$, the identity map, and we will write

$$\tau_{a,b} = \tau_{a,b,1}$$

in the notation of Equation (7). If $\mathbb{F}_q^* =< w >$ and $K_q =< w^2 >$, the subgroup of squares in the multiplicative group of the field, of order $\frac{q-1}{2}$, we write

$$T_q = \{\tau_{1,b} \mid b \in \mathbb{F}_q\}, \;\; Q_q = \{\tau_{a,0} \mid a \in K_q\} \;\text{ and }\; Q_q^* = \{\tau_{a^2,0} \mid a \in K_q\}. \qquad (12)$$

Then $A_q = T_q \rtimes Q_q$, T_q is the group of translations and $|Q_q^*| = \frac{q-1}{4}$.

Proposition 5 *Let $q \geq 13$ be a prime with $q \equiv 1 \pmod 4$, $P(q)$ the Paley graph on $\mathbb{F}_q$, $\mathcal{G}_q$ its incidence design. Let*

$$\mathcal{I} = \{[0,1],[1,2],\ldots,[q-1,0]\},\ \ \mathcal{I}^* = \mathcal{I} \setminus \{[q-1,0]\}.$$

Then Q_q of Equation (12) is a PD-set of size $\frac{q-1}{2}$ for $C_p(\mathcal{G}_q)$ for any prime p, with information set $\mathcal{I}$ for p odd, or information set $\mathcal{I}^*$ for $p = 2$.

Proof: For all p, $C = C_p(\mathcal{G}_q)$ corrects $t = \frac{q-5}{4}$ errors, by Proposition 3. Let $\mathcal{C}$ denote the check positions corresponding to $\mathcal{I}$. We wish to find an element of Q_q that will take a given t-set of points into $\mathcal{C}$.

Let $u = w^2$. The points of $\mathcal{G}_q$ are of the form $[x, x+u^k]$, for $x \in \mathbb{F}_q$, where $0 \leq k \leq \frac{q-1}{2} - 1$, and a point is in $\mathcal{I}$ if and only if $u^k = \pm 1$. Let

$$\mathcal{T} = \{[x_i, x_i + u^{k_i}] \mid 1 \leq i \leq t\}$$

be a set of t points. If $\mathcal{T} \subseteq \mathcal{C}$ then we can use the identity map $\tau_{1,0}$.

Otherwise, since

$$[x_i, x_i + u^{k_i}]\tau_{u^n,0} = [x_i u^n, x_i u^n + u^{k_i+n}],$$

where $0 \leq n \leq \frac{q-1}{2} - 1$, if we can choose n such that $u^{k_i+n} \neq \pm 1$ for all $1 \leq i \leq t$, then all the points will move into $\mathcal{C}$. Now $t = \frac{q-5}{4}$, so there are at most $2t = \frac{q-5}{2}$ values $\pm u^{-k_i}$ that u^n must not take, which leaves at least $\frac{q-1}{2} - \frac{q-5}{2} = 2$ values it can take. Thus we can find such an n for any t-set of points. This argument works for all primes p, taking $\mathcal{I}^*$ in the binary case. ■

Note: Result 1 gives $\frac{q-1}{4}$ for the lower bound on the size of a PD-set, and our result is double this size.

A closed Hamiltonian path for $P(q)$ when q is not a prime can also be constructed in such a manner that Q_q will be an s-PD-set, for partial permutation decoding. We first describe the construction of the closed Hamiltonian path, which is due to Aart Blokhuis [1]: let $q = r^h$ where r is prime, $q \equiv 1 \pmod 4$, and let $\{s_i \mid 1 \leq i \leq h\}$ be a set of non-zero squares of $\mathbb{F}_q$ that form a basis of $\mathbb{F}_q$ as a vector space over $\mathbb{F}_r$. Such a basis is possible, since the squares clearly generate $\mathbb{F}_q$ as a vector space over $\mathbb{F}_r$. Thus

$$\mathbb{F}_{r^h} = \{\sum_{i=1}^{h} a_i s_i \mid a_i \in \mathbb{F}_r, 1 \leq i \leq h\}.$$

Now choose a new basis $\{t_i \mid 1 \leq i \leq h\}$ for $\mathbb{F}_q$ over $\mathbb{F}_r$ as follows: for $1 \leq i \leq h$, let $t_i = s_i - \sum_{j=i+1}^{h} s_j$. Then $s_i = \sum_{j=i}^{h} t_j$. For $x \in \mathbb{F}_q$ in terms of the new basis, we write $x = \sum_{i=1}^{h} x_i t_i = (x_1, \ldots, x_h)$, where $x_i \in \mathbb{F}_r$, and order the elements of F_q lexicographically, starting with 0, then reading from the right, i.e. $(0,\ldots,1)$,$(0,\ldots,2)$,and so on until finally $(r-1,\ldots,r-1)$. We claim that these elements are adjacent in $P(q)$ and the difference between any two consecutive elements is some s_i for $1 \leq i \leq h$. Finally, $((r-1),\ldots(r-1))$ is joined to 0 because $t_1 + t_2 + \ldots t_h = s_1$ is a square. This then gives a Hamiltonian circuit for $P(q)$. It is clearly the same as the one given in Lemma 1 when $q = r$, i.e. $h = 1$, by taking $s_1 = 1$.

[1] The authors thank Aart Blokhuis for this construction

Corollary 3 *Let $q = r^h \geq 25$, where $q \equiv 1 \pmod 4$ and r is a prime and $h \geq 2$. Let $(z_1, \ldots, z_q)$ be the closed Hamiltonian path described in the paragraph above. Let*

$$\mathcal{I} = \{[z_1, z_2], [z_2, z_3], \ldots, [z_q, z_1]\}, \;\; \mathcal{I}^* = \mathcal{I} \setminus \{[z_q, z_1]\}.$$

Then Q_q of Equation (12) is an s-PD-set, where $s < \frac{q-1}{4h}$, of size $\frac{q-1}{2}$ for $C_p(\mathcal{G}_q)$ for any prime p, with information set $\mathcal{I}$ for p odd, or information set $\mathcal{I}^*$ for $p = 2$.

Proof: The proof follows that of Proposition 5 except that now we have to use the fact that all the points of our information set have differences in the set $\{\pm s_i \mid 1 \leq i \leq h\}$, and so we need to ensure that ℓ can be chosen so that $u^{k_i+\ell}$, for $1 \leq i \leq s$, avoids these elements. There are thus $\frac{q-1}{2} - 2hs$ available elements, and this is greater than 0 for $s < \frac{q-1}{4h}$. Thus we have the required s-PD-set. ■

Note: In case q is not a prime, we have not given an explicit information set, since it first needs to be constructed from a basis for $\mathbb{F}_q$ over $\mathbb{F}_r$ of squares in $\mathbb{F}_q$. For example, if $h = 2$ and w is a primitive element then $s_1 = 1, s_2 = w^2$ will clearly suffice, and hence $t_1 = 1 - w^2$, $t_2 = w^2$ would be the basis.

In case we do not wish to specify a particular information set, any transitive subgroup of A_q will suffice for full error-correction, by the following two results, the first from [13, Lemma 7]:

Result 4 *Let C be a code with minimum distance d, $\mathcal{I}$ an information set, $\mathcal{C}$ the corresponding check set and $\mathcal{P} = \mathcal{I} \cup \mathcal{C}$. Let A be an automorphism group of C, and n the maximum of $|\mathcal{O} \cap \mathcal{I}|/|\mathcal{O}|$, where $\mathcal{O}$ is an A-orbit. If $s = \min(\lceil \frac{1}{n} \rceil - 1, \lfloor \frac{d-1}{2} \rfloor)$, then A is an s-PD-set for C.*

This result is true for any information set. If the group A is transitive then $|\mathcal{O}|$ is the degree of the group and $|\mathcal{O} \cap \mathcal{I}|$ is the dimension of the code. This is applicable to codes from incidence matrices of connected regular graphs with automorphism groups transitive on edges, implying the following from [6]:

Result 5 *Let $\Gamma = (V, E)$ be a regular graph of valency v with automorphism group A transitive on edges. Let M be an incidence matrix for Γ. If, for p a prime, $C = C_p(M) = [|E|, |V| - \varepsilon, v]_p$, where $\varepsilon \in \{0, 1, \ldots, |V| - 1\}$, then any transitive subgroup K of A will serve as a PD-set for full error correction for C.*

Corollary 4 *Let q be a prime power with $q \equiv 1 \pmod 4$, $P(q)$ the Paley graph on $\mathbb{F}_q$, $\mathcal{G}_q$ its incidence design. For all primes p, the code $C_p(\mathcal{G}_q)$ can be used for full error correction for any information set by using the group $A_q \cap ASL_1(\mathbb{F}_q)$, or any subgroup of A_q that is transitive on edges.*

Proof: This follows from the previous two results. ■

6 Line graphs and binary hulls

If G is an incidence matrix for $\Gamma = (V, E)$, and M an adjacency matrix for $L(\Gamma)$ then, from Equation (1), $G^T G = M + 2I_{|E|}$. Thus for $p = 2$, we have $C_2(L(\Gamma)) \subseteq C_2(G)$. For p odd the codes $C_p(L(\Gamma))$ have minimum weight at most 4 as long as Γ has a closed path of length 4, by Result 2, so are of no interest for classification nor practical purposes.

Proposition 6 *For $q \geq 5$, $q \equiv 1 \pmod 4$, $C_2(L(P(q)) = C_2(\mathcal{G}_q)$.*

Proof: Let $G(q)$ denote an incidence matrix for $P(q)$, $M(q)$ an adjacency matrix for $L(P(q))$ and let $V(q)$ denote the row span of $G(q)^T$ over $\mathbb{F}_2$. Then $\dim(V(q)) = q-1$. The map $\tau : V(q) \rightarrow C_2(M(q))$ defined by $\tau : v = (v_1, \ldots, v_q) \mapsto (v_1, \ldots, v_q)G$, is such that $V(q)\tau = C_2(M(q))$ and $\dim(C_2(M(q))) + \dim\ \ker(\tau) = \dim(V(q)) = q-1$. A vector v is in the kernel if and only if $v \in V(q)$ and $vG(q) = \mathbf{0}$, and since $\jmath_q G(q) = \mathbf{0}$, we need determine when $\jmath_q \in V(q)$.

But $V(q)$ is spanned by vectors of weight 2, so it is an even-weight code. Since $q \equiv 1 \pmod 4$, it is odd, and so $\jmath_q \notin V(q)$. Thus $C_2(G(q)) = C_2(\mathcal{G}_q) = C_2(M(q)) = C_2(L(P(q))$. ■

Thus we have nothing new from the binary code from an adjacency matrix of $L(P(q))$, since everything is told from $C_2(G(q))$.

Now we consider an incidence matrix for $L(P(q))$. The incidence design is a 1-$(\frac{q(q-1)(q-3)}{8}, q-3, 2)$ design. The p-ary codes from these designs appear to share the properties mentioned in Section 1 that hold for the codes from incidence matrices of many classes of graphs as regards the minimum weight and minimum vectors, and also the gap in the weight enumerator. The graph $L(P(q))$ has closed paths of length 3 and 4, since $P(q)$ has such paths.

Lemma 2 *Let Γ be a regular graph of valency $k \geq 3$ with a closed path of length 3, G an incidence matrix for Γ, and L an incidence matrix for $L(\Gamma)$. Then $C_2(G)^\perp$ has minimum weight 3, and $\mathrm{Hull}(C_2(L))$ has words of weight $6(k-2)$.*

For $\Gamma = P(q)$, there are $\frac{q(q-1)(q-5)}{48}$ closed paths of length 3 (triangles), and thus at least this number of words of weight $3(q-5)$ in $\mathrm{Hull}(C_2(L))$.

Proof: Let (P, Q, R) be a close path in Γ. Then it is clear that

$$w = v^{[P,Q]} + v^{[Q,R]} + v^{[P,R]} \in C_2(G)^\perp.$$

For $L(\Gamma)$, recall that the blocks of the incidence design for $L(\Gamma)$ are of the form

$$\overline{[P,Q]} = \{[[P,Q],[P,R]] \mid R \neq Q\} \cup \{[[P,Q],[Q,R]] \mid R \neq P\},$$

and the valency is $2(k-1)$. If (P, Q, R) is a closed path in Γ, then let

$$w = v^{\overline{[P,Q]}} + v^{\overline{[Q,R]}} + v^{\overline{[P,R]}}.$$

Clearly $w \in C_2(L)$, and it can easily be verified that $(w, v^{\overline{[S,T]}}) = 0$ for every edge $[S,T]$ of Γ, so $w \in \mathrm{Hull}(C_2(L))$. Finally it is clear that $\mathrm{wt}(w) = 3(2(k-1)-2) = 6(k-2)$.

If $[x, y]$ is an edge in $P(q)$ then there are $\lambda = \frac{q-5}{4}$ points z that will give a triangle (x, y, z). The group A_q is transitive on edges, so the number of triangles is $\frac{1}{3}\frac{q(q-1)(q-5)}{16}$, as asserted. In this case $6(k-2) = 3(q-5)$. ■

Note: It frequently happens that $\mathrm{Hull}(C_2(G)) = \{0\}$ where G is the incidence matrix of a regular graph. In contrast, we see that the binary hull of an incidence matrix of a line graph cannot be $\{0\}$ under the given conditions.

For $\Gamma = P(q)$, $L(P(q))$ has $\frac{q(q-1)}{4}$ vertices and $\frac{q(q-1)(q-3)}{8}$ edges, and valency $q-3$. By Whitney [24], $L(P(q))$ has the same automorphism group A_q as $P(q)$. Furthermore, it is easy to see that $L(P(q))$ is Hamiltonian, since $P(q)$ is.

Example 2 For q a prime, we can use the Hamiltonian path $(0, 1, \ldots, q-1)$ for $P(q)$ to get a Hamiltonian path for $L(P(q))$ and hence an information set for the code from an incidence matrix for $L(P(q))$ as follows, using the notation of Equation (10): first let

$$S = \{[0,1], [1,2], \ldots, [q-2, q-1]\},$$

and recall that, for any $i \in \mathbb{F}_q$,

$$\bar{i} = \{[i, i+y] \mid y \text{ a non-zero square of } \mathbb{F}_q\}.$$

Let $S_i = \bar{i} \setminus S$ for $0 \le i \le q-1$. Then all the vertices in S_i are adjacent in $L(P(q))$, and

$$S_0, [0,1], S_1, [1,2], \ldots, [q-2, q-1], S_{q-1}$$

will form a path through all the vertices by taking care that repeats are not included.

For example, if $q = 13$ then the non-zero squares are $\{1, 3, 4, 9, 10, 12\}$, and $P(13)$ has 39 edges, the number of vertices of $L(P(13))$. A Hamiltonian path formed in this way for $L(P(13))$ is:
$[0,12], [0,3], [0,4], [0,9], [0,10], [0,1], [1,5], [1,4], [1,11], [1,10], [1,2], [2,12], [2,6], [2,11], [2,5], [2,3],$
$[3,7], [3,6], [3,12], [3,4], [4,7], [4,8], [4,5], [5,9], [5,8], [5,6], [6,10], [6,9], [6,7], [7,11], [7,10], [7,8],$
$[8,11], [8,12], [8,9], [9,12], [9,10], [10,11], [11,12].$

An information set for the p-ary code from an incidence matrix from this path will be

$$[[0,12],[0,3]], [[0,3],[0,4]], \ldots, [[10,11],[11,12]], [[11,12],[0,12]]$$

for p odd, and omitting the last element for $p = 2$.

Using this information set on the binary code C from an incidence matrix for $L(P(13))$, with Magma we verified that $C = [195, 38, 10]_2$ and that C has a PD-set (correcting four errors) of size 26 from the group $T_{13}Q_{13}^*$, of order 39, using the notation of Equation (12). The same PD-set worked for the ternary code, of dimension 39.

7 Computations on binary hulls

Using Magma [3, 4] we examined some binary hulls of the codes from the incidence matrices G of $P(q)$ and L of $L(P(q))$. The findings are given in Table 1, where in the table we write $CG = C_2(G)$, $CL = C_2(L)$, $H(CG) = \text{Hull}(CG)$, $H(CL) = \text{Hull}(CL)$, $d()$ for dimension, $w()$ for minimum weight, $\ell()$ for the length of the code. We have $\ell(CG) = \frac{q(q-1)}{4}$, $\ell(CL) = \frac{q(q-1)(q-8)}{8}$, $d(CG) = q-1$, $d(CL) = \frac{q(q-1)}{4} - 1$. Columns 2 to 5 relate to $P(q)$, and columns 6 to 9 to $L(P(q))$.

In addition, Magma showed that for $q = 9, 13$, $\text{Hull}(C_2(L))$ has $\frac{q(q-1)(q-5)}{48}$ (i.e. 6 and 26 respectively) words of minimum weight $3(q-5)$.

From these results we might make the following conjectures concerning the binary hulls:

- For $q \equiv 1 \pmod 8$, $\dim(\text{Hull}(C_2(G))) = \frac{q-1}{2}$; for $q \not\equiv 1 \pmod 8$, the length of the code is odd and $\text{Hull}(C_2(G)) = \{0\}$.

- If $q = 4t+1$, then $\dim(\text{Hull}(C_2(L)) = q(t-1) = \frac{q(q-5)}{4}$ and the minimum weight of $\text{Hull}(C_2(L))$ is $12(t-1) = 6(\frac{q-1}{2} - 2) = 3(q-5)$.

q	$\ell(CG)$	$d(CG)$	$d(H(CG))$	$w(H(CG))$	$\ell(CL)$	$d(CL)$	$d(H(CL))$	$w(H(CL))$
9	18	8	4	8	54	17	9	12
13	39	12	0	0	195	38	26	24
17	68	16	8	32	476	67	51	36
25	150	24	12	40	1650	149	125	≤ 60
29	203	28	0	0	2639	202	174	≤ 72
37	333	36	0	0	5661	332	296	≤ 96
41	410	40	20	140	7790	409	369	≤ 108

Table 1: Computations on binary hulls

Note that the minimum weight of $\text{Hull}(C_2(L))$ appears to be the weight found in Lemma 2 for words from triangles in $P(q)$, and that $\dim(\text{Hull}(C_2(L))) = \dim(C_2(G)^\perp) - 1$. This last observation appears to be related to the weight-3 words in $C_2(G)^\perp$ and the words of weight $3(q-5)$ in $\text{Hull}(C_2(L))$ constructed from the associated triangle.

Acknowledgement

This research was performed in the framework of PRIN 2008 (project: *Disegni, Grafi e i loro Codici e Gruppi*), GNSAGA of INDAM, and the Università di Roma “La Sapienza” (project: *Gruppi, Grafi e Geometrie*). The research started while Professor Key was Visiting Professor at the University of Rome “La Sapienza” in June 2010; she gratefully acknowledges the hospitality and financial support extended to her.

References

[1] E. F. Assmus, Jr and J. D. Key. *Designs and their Codes.* Cambridge: Cambridge University Press, 1992. Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[2] R. Balakrishnan and K. Ranganathan. *A Textbook of Graph Theory.* New York: Springer Verlag, 2000. Universitext.

[3] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comp.*, 24, 3/4:235–265, 1997.

[4] J. Cannon, A. Steel, and G. White. Linear codes over finite fields. In J. Cannon and W. Bosma, editors, *Handbook of Magma Functions*, pages 3951–4023. Computational Algebra Group, Department of Mathematics, University of Sydney, 2006. V2.13, http://magma.maths.usyd.edu.au/magma.

[5] K. Chouinard. *Weight distributions of codes from planes.* PhD thesis, University of Virginia, 2000.

[6] W. Fish, J. D. Key, and E. Mwambene. Codes from the incidence matrices and line graphs of Hamming graphs $H^k(n, 2)$ for $k \geq 2$. *Adv. Math. Commun.* (To appear).

[7] W. Fish, J. D. Key, and E. Mwambene. Binary codes of line graphs from the n-cube. *J. Symbolic Comput.*, 45:800–812, 2010.

[8] W. Fish, J. D. Key, and E. Mwambene. Codes from the incidence matrices and line graphs of Hamming graphs. *Discrete Math.*, 310:1884–1897, 2010.

[9] D. M. Gordon. Minimal permutation sets for decoding the binary Golay codes. *IEEE Trans. Inform. Theory*, 28:541–543, 1982.

[10] W. Cary Huffman. Codes and groups. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 1345–1440. Amsterdam: Elsevier, 1998. Volume 2, Part 2, Chapter 17.

[11] Bill Jackson. Hamilton cycles in regular 2-connected graphs. *J. Comb. Theory, Ser. B*, 29:27–46, 1980.

[12] J. D. Key, T. P. McDonough, and V. C. Mavron. Partial permutation decoding for codes from finite planes. *European J. Combin.*, 26:665–682, 2005.

[13] J. D. Key, T. P. McDonough, and V. C. Mavron. Information sets and partial permutation decoding for codes from finite geometries. *Finite Fields Appl.*, 12:232–247, 2006.

[14] J. D. Key, J. Moori, and B. G. Rodrigues. Codes from incidence matrices and line graphs of symplectic graphs. In preparation.

[15] J. D. Key, J. Moori, and B. G. Rodrigues. Codes associated with triangular graphs, and permutation decoding. *Int. J. Information and Coding Theory*, 1, No.3:334–349, 2010.

[16] J. D. Key and B. G. Rodrigues. Codes associated with lattice graphs, and permutation decoding. *Discrete Appl. Math.*, 158:1807–1815, 2010.

[17] Hans-Joachim Kroll and Rita Vincenti. PD-sets related to the codes of some classical varieties. *Discrete Math.*, 301:89–105, 2005.

[18] M. Lavrauw, L. Storme, P. Sziklai, and G. Van de Voorde. An empty interval in the spectrum of small weight codewords in the code from points and k-spaces of $PG(n, q)$. *J. Combin. Theory, Ser. A*, 116 (4):996–1001, 2009.

[19] F. J. MacWilliams. Permutation decoding of systematic codes. *Bell System Tech. J.*, 43:485–505, 1964.

[20] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* Amsterdam: North-Holland, 1983.

[21] C. St. J. A. Nash-Williams. Hamiltonian arcs and circuits. In *1971 Recent Trends in Graph Theory (Proc. Conf, New York, 1970)*, Lecture Notes in Mathematics, Vol. 186, pages 197–210. Springer, Berlin, 1970.

[22] J. Schönheim. On coverings. *Pacific J. Math.*, 14:1405–1411, 1964.

[23] Geertrui Van de Voorde. *Blocking sets in finite projective spaces and coding theory*. PhD thesis, University of Ghent, 2010.

[24] Hassler Whitney. Congruent graphs and the connectivity of graphs. *Amer. J. Math.*, 54:154–168, 1932.