Hulls of codes from incidence matrices of connected regular graphs

Ghinelli, D.; Key, J. D.; McDonough, Thomas

Published in:
Designs, Codes and Cryptography

DOI:
10.1007/s10623-012-9635-0

Publication date:
2014

Citation for published version (APA):
Ghinelli, D., Key, J. D., & McDonough, T. (2014). Hulls of codes from incidence matrices of connected regular graphs. *Designs, Codes and Cryptography*, *70*(1), 35-54. https://doi.org/10.1007/s10623-012-9635-0

Hulls of codes from incidence matrices of connected regular graphs

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

J.D. Key†
Department of Mathematics
and Applied Mathematics
University of the Western Cape
7535 Bellville, South Africa

T. P. McDonough‡
Institute of Mathematics and Physics
Aberystwyth University
Aberystwyth, Ceredigion SY23 3BZ, U.K.

January 26, 2012

Abstract

The hulls of codes from the row span over $\mathbb{F}_p$, for any prime p, of incidence matrices of connected k-regular graphs are examined, and the dimension of the hull is given in terms of the dimension of the row span of $A+kI$ over $\mathbb{F}_p$, where A is an adjacency matrix for the graph. If $p = 2$, for most classes of connected regular graphs with some further form of symmetry, it was shown in [8] that the hull is either $\{0\}$ or has minimum weight at least $2k - 2$. Here we show that if the graph is strongly regular with parameter set (n, k, λ, μ), then, unless k is even and μ is odd, the binary hull is non-trivial, of minimum weight generally greater than $2k - 2$, and we construct words of low weight in the hull; if k is even and μ is odd, we show that the binary hull is zero. Further, if a graph is the line graph of a k-regular graph, $k \geq 3$, that has an ℓ-cycle for some $\ell \geq 3$, the binary hull is shown to be non-trivial with minimum weight at most $2\ell(k - 2)$. Properties of the p-ary hulls are also established.

Keywords: Incidence matrix, graph, code, hull, permutation decoding
Mathematics Subject Classifications (2010): 05B05, 05C38, 94B05

1 Introduction

If C is a linear code and $C^\perp$ its dual, the hull of C is the code $C \cap C^\perp$, denoted by Hull(C), in the terminology that was introduced in [1]. This is a self-orthogonal code, and in the case where the code C is that from an incidence matrix of a finite plane, or some finite geometry, the hull has certain defining properties of the plane, or geometry, in question, as was discussed in [1]. In particular, the minimum weight and the nature of the minimum words led to a

*dina@mat.uniroma1.it
†keyj@clemson.edu
‡tpd@aber.ac.uk

possible characterisation of desarguesian projective planes of order q which is a power of the prime p as being, conjecturally, the only planes whose hull over $\mathbb{F}_p$ has minimum weight $2q$ and the vectors of this weight are the scalar multiples of the difference of the incidence vectors of two lines. Such a plane is called a "tame" plane in [1], and thus far no non-desarguesian tame plane is known, although many have been shown not to be tame.

In a similar way, the hulls of the p-ary codes from incidence matrices of regular graphs, i.e. the hulls of their incidence designs, can be examined. This study follows work on the codes over any field from incidence matrices of graphs: see [10, 32, 28, 29, 14] and most recently [8], where the findings of the previous papers are shown to be quite general. In particular, it is known that for many classes of connected regular graphs the code from the row span of an incidence matrix of $\Gamma = (V, E)$ over $\mathbb{F}_p$ has dimension $|V|$ for p odd and $|V| - 1$ for $p = 2$, and the words of minimum weight are the scalar multiples of the rows of the matrix, as in the case for codes from projective planes. Result 4 in Section 3 summarises some classes for which this is known to be true in the binary case. Results for the non-binary case are not fully established yet but the indications are that the results will be similar to the binary case. We mention here that earlier work on the binary codes from incidence matrices of graphs, the codes being called cut spaces, was done in [19, 18]. There the interest in the codes concerned their usefulness for majority logic decoding.

From these results we see that the codes from the incidence matrices of many classes of k-regular graphs have known minimum weight k, known dimension, and furthermore, at least in the binary case, the next weight is $2k-2$. Thus it makes sense to study the hull, in particular the binary hull, since it is a self-orthogonal code, and will have minimum weight at least $2k-2$ if it is non-zero. We show here that for some classes of graphs we can always say that the binary hull is non-zero and give some words in the hull.

Furthermore, for connected k-regular graphs the dimension of the p-ary hull can be given in terms of the dimension of the row span over $\mathbb{F}_p$ of the matrix $A + kI$, where A is an adjacency matrix of the graph: see Proposition 1. In Proposition 3, Section 4, we show that for a (n, k, λ, μ) strongly regular graph, the binary hull of the incidence design is non-trivial and construct at least n words in the hull, except in the case when k is even and μ is odd, where the hull is shown to be zero. Some similar conditions for the p-ary hull, where p is odd, are also established. We show in Proposition 5, Section 7, that for the line graph $L(\Gamma)$ of a k-regular graph Γ, $k \geq 3$, that has an ℓ-cycle for some $\ell \geq 3$, the binary hull of the incidence design of $L(\Gamma)$ is non-trivial. This leads immediately to a characterisation: see Corollary 3.

The paper is arranged as follows: in Section 2 we give definitions and background; Section 3 has a statement of the main result about codes from incidence matrices of graphs, and some related results, including Proposition 1, mentioned above; Section 4 has our main result, Proposition 3, on the hulls of incidence matrices of strongly regular graphs, and applications to some classes; in Section 5 we mention some known results about hulls from previous work for graphs that are not strongly regular; in Section 6 we show that if the prime p is sufficiently large, the p-ary hull of an incidence matrix of a regular graph is zero; Section 7 has our main result, Proposition 5, about line graphs, and Section 8 has an application to permutation decoding .

2 Background and terminology

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 $\boldsymbol{v^{\mathcal{Q}}}$, 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 $P \in \mathcal{P}$, $\boldsymbol{w(P)}$ denotes the value of w at P. If $F = \mathbb{F}_p$ then the **p-rank** of the design, written $\text{rank}_{\boldsymbol{p}}\boldsymbol{(\mathcal{D})}$, is the dimension of its code $C_F(\mathcal{D})$; for $F = \mathbb{F}_p$ we usually write $C_p(\mathcal{D})$ for $C_F(\mathcal{D})$.

All the codes here are **linear codes**, and the notation $[n, k, d]_q$ will be used to denote 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 $\mathbf{m}$ of the all-one vector, we write $\boldsymbol{\jmath}_{\mathbf{m}}$. 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, are simple. If $x, y \in V$ and x and y are adjacent, we write $x \sim y$, and $[x, y]$ or xy for the **edge** in E that they define. We write $x \not\sim y$ if $x \neq y$ and x is not adjacent to y. The **set of neighbours** of $x \in V$ is denoted by $N(x)$, and the **valency** or **degree**, $\deg(x)$, of x is $|N(x)|$. Γ is **regular** if all the vertices have the same valency. The **order** of Γ is $|V|$. A **path** of length r from vertex x to vertex y is a sequence x_i, for $0 \leq i \leq r - 1$, of distinct vertices with $x = x_0$, $y = x_{r-1}$, and $x_{i-1} \sim x_i$ for $1 \leq i \leq r - 1$. It is **closed** of length r if $x \sim y$, in which case we write it $(x_0, \ldots, x_{r-1})$ and call it a **cycle** or **r-cycle**. The graph is **connected** if there is a path between any two vertices, and $d(x, y)$ denotes the length of the shortest path from x to y. An **adjacency matrix** A is a $|V| \times |V|$ matrix with entries a_{ij} such that $a_{ij} = 1$ if vertices x_i and x_j are adjacent, and $a_{ij} = 0$ otherwise. An **incidence matrix** is a $|V| \times |E|$ matrix $G = [g_{i,j}]$ with $g_{i,j} = 1$ if the vertex labelled by i is on the edge labelled by j, and $g_{i,j} = 0$ 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 Γ is the symmetric 1-$(|V|, k, k)$ 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. an adjacency matrix for the graph as an incidence matrix for the design. The **line graph** of Γ 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 graph Γ, not complete or null, is **strongly regular graph** of type (n, k, λ, μ) if it is regular on $n = |V|$ vertices, has valency k, and 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 $(n, n - k - 1, n - 2k + \mu - 2, n - 2k + \lambda)$. The **code** of 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 $\text{rank}_p(A)$ 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 $\mathbb{F}_p$ of the neighbourhood design. Similarly, if G is an incidence matrix for Γ, $C_p(G)$ denotes the row span of G over $\mathbb{F}_p$ and is the code of the design with blocks the rows of G, in

the case that Γ is regular. If L is an adjacency matrix for $L(\Gamma)$ where Γ is regular of valency k, then

$$G^TG = L + 2I_{|E|} \text{ and } GG^T = A + kI_{|V|}, \tag{1}$$

where A is an adjacency matrix for Γ, and G an incidence matrix, with G^T its transpose.

Permutation decoding was first developed by MacWilliams [34] and involves finding a set of automorphisms of a code called a PD-set. The method is described in MacWilliams and Sloane [35, Chapter 16, p. 513] and Huffman [20, Section 8]. In [21] and [33] 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 $\mathcal{C}$.*

*For $s \leq t$ an s-***PD-set** *is a set $\mathcal{S}$ of automorphisms of C which is such that every s-set of coordinate positions is moved by at least one member of $\mathcal{S}$ into $\mathcal{C}$.*

The algorithm for permutation decoding is given in [20] 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 $\mathcal{I}$. Furthermore, there is a bound on the minimum size that the set S may have, due to Gordon [16], from a formula due to Schönheim [37], and quoted and proved in [20]:

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*

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

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

3 Codes from incidence matrices of graphs

If $\Gamma = (V, E)$ is a graph, x a vertex, $N(x)$ its neighbours, then we write

$$\overline{x} = \{[x,y] \mid y \in V,\, y \sim x\} = \{[x,y] \mid y \in N(x)\}, \tag{2}$$

i.e. the **edges** that correspond to non-zero entries in the row labelled by x of an incidence matrix for Γ. When Γ is k-regular, the $\overline{x}$ form the blocks of the incidence design $\mathcal{G}$, a 1-$(|E|, k, 2)$ design.

We also write

$$\overline{\overline{[x,y]}} = \{[x,z] \mid z \neq y\} \cup \{[y,z] \mid z \neq x\} = (\overline{x} \cup \overline{y}) \setminus \{[x,y]\} = N([x,y]), \tag{3}$$

for the **neighbours** $N([x,y])$ of $[x,y]$ in the line graph $L(\Gamma)$. Thus

$$v^{\overline{\overline{[x,y]}}} = \sum_{x \sim z \neq y} v^{[x,z]} + \sum_{y \sim z \neq x} v^{[y,z]} = v^{\overline{x}} + v^{\overline{y}} - 2v^{[x,y]}.$$

Lemma 1 *Let Γ be a graph, G an incidence matrix for Γ, $L(\Gamma)$ the line graph of Γ, and L an adjacency matrix of $L(\Gamma)$. Let $\pi = (x_0, ..., x_{l-1})$ be a cycle in Γ, and let*

$$w(\pi) = \sum_{i=0}^{l-1} (-1)^i v^{[x_i, x_{i+1}]}, \tag{4}$$

where subscripts are taken $(\mathrm{mod}\ l)$. *Then* $\mathrm{wt}(w(\pi)) = l$ *and*

A1. $w(\pi) \in C_p(G)^\perp$ *if $p = 2$ or l is even;*

A2. $w(\pi) \in C_p(L)$ *if p is odd and l is even.*

Proof: Let $x \in V(\Gamma)$. If $x \notin \{x_0, \ldots, x_{l-1}\}$, then $\overline{x}$ contains none of the edges $[x_i, x_{i+1}]$, $i = 0, \ldots, l-1$. Hence $(w(\pi), v^{\overline{x}}) = 0$. If $x = x_i$, then $\overline{x}$ contains two edges of the cycle, namely $[x_{i-1}, x_i]$ and $[x_i, x_{i+1}]$. If $1 \leq i \leq l-1$, then $(w(\pi), v^{\overline{x}}) = (-1)^{i-1} + (-1)^i = 0$. If $i = 0$, then $(w(\pi), v^{\overline{x}}) = (-1)^{l-1} + 1$ which is 0 if, and only if, l is even. This establishes A1.

If l is even then $2w(\pi) = \sum_{i=0}^{l-1}(-1)^i \left(2v^{[x_i,x_{i+1}]}\right) = \sum_{i=0}^{l-1}(-1)^i \left(v^{\overline{x_i}} + v^{\overline{x_{i+1}}} - v^{\overline{\overline{[x_i,x_{i+1}]}}}\right)$

$= -\sum_{i=0}^{l-1}(-1)^i v^{\overline{\overline{[x_i,x_{i+1}]}}} \in C_p(L)$. If p is odd also then $w(\pi) \in C_p(L)$. ■

We will need the following two results, the first from [10]:

Result 2 *Let $\Gamma = (V, E)$ be a regular graph with valency k and $\mathcal{G}$ the 1-$(|E|, k, 2)$ incidence design for Γ. Then* $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\mathcal{G})$.

The following is from [32, Result 2] and [23]:

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 cycle of odd length ≥ 3, then* $\dim(C_p(G)) = |V|$ *for odd p.*

The following proposition gives the dimension of the p-ary hull of an incidence matrix of a connected k-regular graph $\Gamma = (V, E)$ in terms of that of the row span over $\mathbb{F}_p$ of the matrices $A + kI$, where A is an adjacency matrix for the graph, and $I = I_{|V|}$.

Proposition 1 *Let $\Gamma = (V, E)$ be a connected k-regular graph, A a $|V| \times |V|$ adjacency matrix and G a $|V| \times |E|$ incidence matrix for Γ. For p any prime let $H_p = \mathrm{Hull}(C_p(G))$. Then if $I = I_{|V|}$,*

1. *for $p = 2$,* $\dim(H_2) = \dim(C_2(A + kI)^\perp) - 1$;
2. *for p odd, Γ not bipartite,* $\dim(H_p) = \dim(C_p(A + kI)^\perp)$;
3. *for p odd, Γ bipartite,* $\dim(H_p) = \dim(C_p(A + kI)^\perp) - 1$;
4. *for p odd and $p \mid k$, $\mathbf{j}_{|E|} \in H_p$.*

Proof: We work over $\mathbb{F}_p$ where p is a fixed prime. Notice first that for $m \in \mathbb{Z}$, $\mathbf{j}_{|V|} \in C_p(A + mI)^\perp$ if and only if $m \equiv -k \pmod{p}$. Suppose $H_p \neq \{0\}$ and that $w = \sum_{z \in V} \alpha_z v^{\overline{z}} \in H$, and $w \neq 0$. Then $(w, v^{\overline{x}}) = (\sum_{z \in V} \alpha_z v^{\overline{z}}, v^{\overline{x}}) = 0$ for all $x \in V$. We have $(v^{\overline{x}}, v^{\overline{x}}) = k$ for all $x \in V$, $(v^{\overline{x}}, v^{\overline{y}}) = 1$ if $x \sim y$, and $(v^{\overline{x}}, v^{\overline{y}}) = 0$ if $x \not\sim y$. Thus we have that $k\alpha_x + \sum_{z \sim x} \alpha_z = 0$ for all $x \in V$. This implies that if $t = (\alpha_x)'$ is the column vector with elements α_x in the same ordering as the adjacency matrix A, then $(A + kI)t = 0$. Thus $t \in C_p(A + kI)^\perp$.

Conversely, if $t = (\alpha_x)' \in C_p(A + kI)^\perp$ then $w = \sum_{z \in V} \alpha_z v^{\overline{z}} \in H_p$. The map $\phi : C_p(A + kI)^\perp \mapsto H_p$ by $\phi : t \mapsto w$ is linear and onto. Using Result 3, the kernel of ϕ is $\langle \mathbf{j}_{|V|} \rangle$ if $p = 2$, and $\{0\}$ if p is odd, unless Γ is bipartite on $V_1 \cup V_2$, in which case it is $\langle \mathbf{j}_{|V_1|} - \mathbf{j}_{|V_2|} \rangle$.

Finally, if p is odd then $\sum_{x \in V} v^{\overline{x}} = 2\mathbf{j}_{|E|} \neq 0$, so $\mathbf{j}_{|E|} \in C_p(G)$. If $p \mid k$ then also $\mathbf{j}_{|E|} \in H_p$. ■

In [8, Section 6] the following was proved for binary codes:

Result 4 *Let Γ be a connected k-regular graph on $|V| = n$ vertices, and G an incidence matrix for Γ. If Γ satisfies one of the conditions given below, then $C_2(G)$ has minimum weight k, the words of weight k are precisely the rows of the incidence matrix, and there are no words of weight l such that $k < l < 2k - 2$:*

1. *Γ is vertex-transitive, and has odd order or does not contain triangles;*
2. *Γ is edge-transitive and has $|V| \geq 4$;*

3. *each pair u, v of nonadjacent vertices of Γ satisfies*

$$|N(u) \cap N(v)| \geq \begin{cases} 2 & \text{if neither } u \text{ nor } v \text{ are on a triangle,} \\ 3 & \text{if at least one of } u, v \text{ is on a triangle.} \end{cases}$$

4. *any two non-adjacent vertices of Γ have at least three neighbours in common (from 3. above);*
5. *Γ is bipartite and any two vertices in the same partite set have at least two neighbours in common;*
6. *Γ is strongly regular graph with parameters (n, k, λ, μ) with either $\lambda = 0$ and $\mu \geq 2$, or with $\lambda \geq 1$ and $\mu \geq 3$ (from 3. above);*
7. *$k \geq (n+1)/2$ and if Γ is bipartite then $k > \lceil \frac{n+2}{4} \rceil$ is sufficient;*
8. *Γ has girth g, and* $\mathrm{diam}(\Gamma) \leq g - 2$.

Note: 1. There are other classes of graphs that share this property, some of which are mentioned in [8].
2. A similar result for p-ary codes for p odd has not yet been proved, although it is believed to hold. For this reason we will apply Proposition 1 mostly to binary hulls in this paper.

However, there is a similar result in [8] for p odd and Γ connected k-regular bipartite:

Result 5 *Let $\Gamma = (V, E)$ be a connected bipartite k-regular graph on $|V| = n$ vertices, and G an incidence matrix for Γ. Then for any prime p, $C_p(G)$ has minimum weight k, the words of weight k are precisely the non-zero scalar multiples of the rows of the incidence matrix, and there are no words of weight l such that $k < l < 2k - 2$, if at least one of the following conditions holds:*

1. *Γ is vertex-transitive;*
2. *Γ is edge-transitive and has $|V| \geq 4$;*
3. *each pair u, v of nonadjacent vertices satisfies $|N(u) \cap N(v)| \geq 2$;*
4. *Any two non-adjacent vertices have at least two neighbours in common;*
5. *Γ is strongly regular graph with parameters (n, k, λ, μ) with $\lambda = 0$ and $\mu \geq 2$.*

Example 1 Let $\Gamma = K_{n,n}$ be the complete bipartite graph of degree n, $n \geq 2$. Then from Result 5 and Proposition 1, the minimum weight of the non-zero hull of an incidence matrix G will be at least $2n - 2$, and it is easy to see that $\dim(\mathrm{Hull}(C_p(G))) = 2n - 3$ if $p \mid n$ and $\mathrm{Hull}(C_p(G)) = \{0\}$ otherwise. ■

If G is an incidence matrix for a graph Γ, the subcode of $C_p(G)$ that is spanned by the differences of all the pairs of rows is denoted by $E_p(G)$. These differences give words of weight $2k - 2$ for rows corresponding to adjacent vertices (where Γ is k-regular), and are referred to in Result 4. Previous studies of some classes of graphs have shown that the scalar multiples of these differences are precisely the words of this weight. Thus the question of when such words are in $\mathrm{Hull}(C_2(G))$ is of importance since the answer can improve the lower bound on the minimum weight of $\mathrm{Hull}(C_2(G))$.

Lemma 2 *Let $\Gamma = (V, E)$ be a k-regular graph where $k \geq 2$. Let G be an incidence matrix for Γ and $C = C_p(G)$, where p is any prime. Then for $x, y \in V$, $x \neq y$, if $w = v^{\overline{x}} - v^{\overline{y}} \in \mathrm{Hull}(C)$,*

- *if $x \sim y$, then $k \equiv 1 \pmod{p}$, $N(x) - \{y\} = N(y) - \{x\}$, and $\mathrm{wt}(w) = 2k - 2$;*
- *if $x \not\sim y$, then $k \equiv 0 \pmod{p}$, $N(x) = N(y)$, and $\mathrm{wt}(w) = 2k$.*

Proof: The proof is quite direct, examining the fact that $(v^{\overline{z}}, w) = 0$ modulo p for all $z \in V$. ■

For the complete graph K_n we get an immediate answer, since $E_p(G)$ was studied in [28] where it was shown that the words of weight $2k-2$ are precisely the scalar multiples of the differences of two rows corresponding to adjacent vertices.

Proposition 2 *Let $\Gamma = (V, E) = K_n$, the complete graph on n vertices, where $n \geq 3$. If G_n denotes an incidence matrix for K_n, $E_p(G_n)$ the subcode of $C_p(G_n)$ that is spanned over $\mathbb{F}_p$, for any prime p, by the differences of all the pairs of rows of G_n, then*

- *for $p = 2$, if n is odd,* $\mathrm{Hull}(C_2(G_n)) = \{0\}$*; if n is even,* $\mathrm{Hull}(C_2(G_n)) = E_2(G_n)$*, is a $[\binom{n}{2}, n-2, 2(n-2)]_2$ code;*
- *for p odd, if $n \equiv 2 \pmod p$,* $\mathrm{Hull}(C_p(G_n)) = E_p(G_n)$ *is a $[\binom{n}{2}, n-2, 2(n-2)]_p$ code; if $n \equiv 1 \pmod p$ then* $\mathrm{Hull}(C_p(G_n)) = \langle \boldsymbol{\jmath}_{|E|} \rangle$*; for all other n,* $\mathrm{Hull}(C_p(G_n)) = \{0\}$*.*

Proof: For $p = 2$, let $w = \sum_{i=1}^{r} v^{\overline{x_i}} \neq 0$, where $\{x_i \mid 1 \leq i \leq r < n\} \subset V$, and suppose $w \in H = \mathrm{Hull}(C_2(G_n))$. Since we have the complete graph, $(v^{\overline{x}}, w) = r$ if $x \neq x_i$ for any i, and if $x = x_i$ for some i, then $(v^{\overline{x}}, w) = r - 1 + n - 1 = r + n - 2$. If n is odd then $n + r - 2 \not\equiv r \pmod 2$, so $H = \{0\}$.

For n even, $n + r - 2 \equiv r \pmod 2$, and so for any even r, $w \in H$, and $E_2(G_n) \subseteq H$. Since $H \neq C_2(G_n)$, it follows that $H = E_2(G_n)$.

For p odd, Proposition 1 and [28, Proposition 5] give the result stated. ■

Corollary 1 *Let $\Gamma = (V, E)$ be a connected k-regular graph and G an incidence matrix. If for all pairs of distinct vertices x, y, $|N(x) \cap N(y)| \equiv 1 \pmod 2$ then* $\mathrm{Hull}(C_2(G)) = \{0\}$*.*

Proof: Let $w = \sum_{z \in V} \alpha_z v^{\overline{z}} \in H = \mathrm{Hull}(C_2(G))$, and $w \neq 0$. Then, as in the proof of Proposition 1, we have $\sum_{z \sim x} \alpha_z = 0$ for all $x \in V$ if k is even, and $\sum_{z \sim x} \alpha_z = \alpha_x$ for all $x \in V$ if k is odd. Thus if $t = (\alpha_x)'$, $At = 0$ for k even, and $At = t$ for k odd.

Now using $|N(x) \cap N(y)| \equiv 1 \pmod 2$ gives $A^2 = J + I$ for k even, and $A^2 = J$ for k odd, so $Jt = t$ in both cases and hence t is constant, and $w = 0$, contradicting our assumption. ■

4 Strongly regular graphs

Recall that if Γ is strongly regular of type (n, k, λ, μ) then the complement Γ^c is strongly regular of type $(n, n-k-1, n-2k+\mu-2, n-2k+\lambda)$. The parameters for Γ are linked by the equation

$$(n-k-1)\mu = k(k-\lambda-1). \tag{5}$$

See [6, Chapter 2], for example, for proof of these properties. Furthermore, we exclude the complete and the null graphs. Note that this equation shows that not both k and λ can be odd, since if k is odd then n must be even (since $|E| = \frac{1}{2}kn$), so the left-hand side of Equation (5) is even, while the right-hand side is odd if λ is odd.

We will need some further standard results about adjacency matrices of strongly regular graphs; these can be found in [6, Chapter 2]. Thus for A an adjacency matrix for $\Gamma = (V, E)$, strongly regular of type (n, k, λ, μ),

$$A^2 = kI + \mu(J - I) + (\lambda - \mu)A, \tag{6}$$

where J is the $n \times n$ matrix with all entries 1, and $I = I_n$ is the identity $n \times n$ matrix.

Our main result for the hull of an incidence matrix of a strongly regular graph, in particular for the binary hull, is given in the following proposition. Note that the dimension of the p-ary hull is given in terms of the p-rank of the matrices $A + kI$, where A is an adjacency matrix, in Proposition 1.

Proposition 3 *Let $\Gamma = (V, E)$ be a strongly regular graph with parameters (n, k, λ, μ) with $k \geq 2$, and let G be an $n \times \frac{1}{2}kn$ incidence matrix and A an adjacency matrix for Γ. Let p be a prime and let $C = C_p(G)$ and $H_p = Hull(C)$. For each $x, y \in V$ with $x \neq y$ define*

$$u(x) = \sum_{z \sim x} v^{\overline{z}};\ v_\xi(x) = u(x) + \xi v^{\overline{x}} \text{ (where } \xi \in \mathbb{F}_p);\ w(x, y) = u(x) - u(y). \tag{7}$$

Then

(i) *if $p \mid k$ and $p \nmid \mu$ then $H_p = \begin{cases} \{0\} & \text{if } p = 2, \\ \langle \boldsymbol{j}_{|E|} \rangle & \text{for } p \text{ odd.} \end{cases}$*
If $p \mid \mu$, $p \nmid k$, and $p \nmid \lambda$ then p is odd and $H_p = \{0\}$.

(ii) *$u(x) \in H_p$ if $p \mid k$, $p \mid \lambda$ and $p \mid \mu$.*

(iii) *$v_{-1}(x) \in H_p$ if $p \mid \mu$ and $p \mid k + \lambda - 1$; $v_{-\lambda}(x) \in H_p$ if $p \mid \mu$ and $p \mid k$.*

(iv) *$w(x, y) \in H_p$ if $p \mid k - \mu$ and $p \mid \lambda$.*

(v) *$\mathrm{wt}(u(x)) = k(k - \lambda)$ for $p = 2$; $\mathrm{wt}(u(x)) = k(k - \frac{1}{2}\lambda)$ for p odd.*

(vi) *$\mathrm{wt}(v_1(x)) = k(k - 1 - \lambda)$ for $p = 2$; $\mathrm{wt}(v_{-1}(x)) = k(k - 1 - \frac{1}{2}\lambda)$ for p odd; $\mathrm{wt}(v_\xi(x)) = k(k - \frac{1}{2}\lambda)$ for p odd and $\xi \neq -1$.*

(vii) *$\mathrm{wt}(w(x, y)) \geq 2\lambda$ if $x \sim y$; $\mathrm{wt}(w(x, y)) \geq 2(k - \mu)$ if $x \not\sim y$. In particular, $w(x, y)) \neq 0$ if $x \neq y$.*

(viii) *$H_2 \neq \{0\}$ if $2 \nmid k$ or $2 \mid \mu$; in these cases, H_2 has minimum weight at least $2k - 2$ if $\lambda = 0$ and $\mu \geq 2$ or $\lambda \geq 1$ and $\mu \geq 3$.*

(ix) *For p odd, $H_p \neq \{0\}$ and $H_p \neq \langle \boldsymbol{j}_{|E|} \rangle$ if $p \mid k$ and $p \mid \mu$ or $p \mid k + \lambda - 1$ and $p \mid \mu$ or $p \mid k - \mu$ and $p \mid \lambda$.*

Proof: (i): Suppose $w \in H_p$ and $w \neq 0$. Then $w = \sum_{z \in V} \alpha_z v^{\overline{z}}$ where $\alpha_z \in \mathbb{F}_p$ for all $z \in V$. Let $t = (\alpha_x)'$. From the proof of Proposition 1, $(A + kI)t = 0$. So, $At = -kt$. From Equation (6) we get $k^2 t = A^2 t = kt + \mu(Jt - t) - (\lambda - \mu)kt$, that is, $(k^2 - k + (\lambda - \mu)k + \mu)t = \mu Jt$.

If $p \mid k$ and $p \nmid \mu$, the coefficient of t on the lefthand side is non-zero and the righthand side is a constant vector. Hence, t is a multiple of $\boldsymbol{j}$. But this is impossible if $p = 2$ since $w \neq 0$ and $\sum_{z \in V} v^{\overline{z}} = 0$. So, $H_2 = 0$ in this case. If p is odd then $H_p = \langle \boldsymbol{j}_{|E|} \rangle$ since $\boldsymbol{j}_{|E|} \in H_p$ from Proposition 1.

If $p \mid \mu$, $p \nmid k$, and $p \nmid \lambda$, then from Equation (5), $p \mid (k - \lambda - 1)$, so $p \neq 2$. Then $k + \lambda - 1 = k - \lambda - 1 + 2\lambda$, so $p \nmid k + \lambda - 1$. Thus $(k^2 - k + (\lambda - \mu)k + \mu)t = \mu Jt$ becomes $(k^2 - k + \lambda k)t = 0 = k(k + \lambda - 1)t$, and thus $t = 0$ and $H_p = \{0\}$.

(ii) and (iii): By definition, $u(x), v_\xi(x), w(x, y) \in C$. We now establish that, under certain conditions, they are in $C^\perp$ also. Statements A1-A3 result from easy calculations:

A1. $(u(x), v^{\overline{x}}) = k$ and $(v_\xi(x), v^{\overline{x}}) = k(\xi + 1)$,
A2. $(u(x), v^{\overline{z}}) = k + \lambda$ and $(v_\xi(x), v^{\overline{z}}) = k + \lambda + \xi$ if $z \sim x$,
A3. $(u(x), v^{\overline{z}}) = \mu$ and $(v_\xi(x), v^{\overline{z}}) = \mu$ if $z \not\sim x$.

These statements establish (ii) immediately. $v_\xi(x) \in C^\perp$ if and only if $p \mid \mu$ and either $p \mid k$ and $p \mid (\lambda + \xi)$, or $p \mid (\xi + 1)$ and $p \mid (k + \lambda + \xi)$. Since $\xi \in \mathbb{F}_p$, this establishes (iii).

(iv): Statements B1-B6 result from easy calculations:

B1. $(w(x, y), v^{\overline{z}}) = 0$ if $z \sim x$ and $z \sim y$,
B2. $(w(x, y), v^{\overline{z}}) = k + \lambda - \mu$ if $z \sim x$ and $z \not\sim y$,
B3. $(w(x, y), v^{\overline{z}}) = -(k + \lambda - \mu)$ if $z \not\sim x$ and $z \sim y$,
B4. $(w(x, y), v^{\overline{z}}) = 0$ if $z \not\sim x$ and $z \not\sim y$,
B5. $(w(x, y), v^{\overline{x}}) = -\lambda$ and $(w(x, y), v^{\overline{y}}) = \lambda$ if $y \sim x$,
B6. $(w(x, y), v^{\overline{x}}) = k - \mu$ and $(w(x, y), v^{\overline{y}}) = \mu - k$ if $y \not\sim x$.

Hence, $w(x, y) \in C^\perp$ if, and only if, $p \mid \lambda$ and $p \mid (k - \mu)$.

(v): In the sum $u(x) = \sum_{z \sim x} v^{\overline{z}}$, the base vector $v^{[a,b]}$ will occur once if exactly one of a and b is adjacent to x and will occur twice if both are adjacent to x. For every $a \sim x$ there are exactly λ choices for b with $b \sim x$. Hence there are $\frac{1}{2}k\lambda$ base vectors occurring twice and $k(k-\lambda)$ base vectors occurring once. If $p = 2$ then the base vectors occurring twice cancel, leaving a total weight of $k(k-\lambda)$. If p is odd then the total base vectors occurring is $\frac{1}{2}k\lambda + k(k-\lambda) = k(k-\frac{1}{2}\lambda)$. Note that the base vectors of the form $v^{[a,x]}$ occur in $u(x)$ with coefficient 1.

(vi): From the last sentence of (v), we see that the contribution of $\xi v^{\overline{x}}$ to $v_\xi(x)$ will cancel completely with the corresponding terms in $u(x)$ or no cancellation will take place. The former happens if, and only if, $\xi = -1$. This establishes (vi).

(vii): Suppose first that $x \sim y$. If $a \sim x$ and $a \sim y$, the base vector $v^{[a,x]}$ occurs in $u(x)$ with coefficient 1 and occurs in $u(y)$ with coefficient 0 or 2 according as $p = 2$ or p is odd. Since there are λ values of a and we can apply a similar argument to $v^{[a,y]}$, $w(x,y)$ has weight at least 2λ in this case. Suppose now that $x \not\sim y$. If $a \sim x$ and $a \not\sim y$, the base vector $v^{[a,x]}$ occurs in $u(x)$ with coefficient 1 and does not occur in $u(y)$. Since there are $k-\mu$ values of a and we can apply a similar argument to $v^{[a,y]}$, $w(x,y)$ has weight at least $2(k-\mu)$ in this case.

(viii): If $2 \nmid k$ then $2 \mid n$ since $\frac{1}{2}kn$ is an integer. From Equation (5), $2 \mid \lambda$. If $2 \mid \mu$ then $2 \mid k+\lambda-1$ and hence $v_1(x) \in H_2$ for any $x \in V$ by (iii). If $2 \nmid \mu$ then $2 \mid k-\mu$ and hence $w(x,y) \in H_2$ for any $x, y \in V$ by (iv).

Now suppose that $2 \mid k$ and $2 \mid \mu$. If $2 \mid \lambda$, then $u(x) \in H_2$ for any $x \in V$ by (ii). If $2 \nmid \lambda$ then $2 \mid k+\lambda-1$ and hence $v_1(x) \in H_2$ for any $x \in V$ by (iii).

The statement involving the bound on the minimum weight follows from Result 4 (6) since $(v^{\overline{x}}, v^{\overline{y}}) = 1$ if $x \sim y$.

(ix) If $p \mid k$ and $p \mid \mu$ then $v_{-\lambda}(x) \in H_p$ from (iii). If $p \mid k+\lambda-1$ and $p \mid \mu$ then $v_{-1}(x) \in H_p$ from (iii). If $p \mid \lambda$ and $p \mid k-\mu$ then $w(x,y) \in H_p$ from (iv). Since none of the elements $v_{-\lambda}(x)$, $v_{-1}(x)$ and $w(x,y)$ are multiples of $\boldsymbol{j}_{|E|}$, this completes (xi). ■

Note: The statement *(viii)* in the proposition that bounds the minimum weight of H_2 by $2k-2$ excludes parameter sets that are not included in Result 4. Thus for $\lambda = 0$ and $\mu = 1$, or for $\lambda \geq 1$ and $\mu = 1$ or 2 ($\mu = 0$ gives $\lambda = k-1$, and so is the complete graph which is covered by Proposition 2) the minimum weight of the non-zero hull would still need to be checked. Some cases are listed below in the applications. In fact the gap in the weight enumerator of the code from the incidence matrix does appear in all cases tested, and also for the p odd case.

k	0	0	1	1	0	0	1	1
λ	0	1	0	0	0	1	1	1
μ	0	0	0	1	1	1	1	0
H	$\neq \{0\}$	$\neq \{0\}$	$\neq \{0\}$	$\neq \{0\}$	$\{0\}$	$\{0\}$	-	-

Table 1: Parity of the parameters k, λ, μ

Table 1 shows the parity sets of the parameters k, λ, μ for which we can say that the binary hull of the incidence matrix of a strongly regular graph is non-trivial, by the proposition. In the table the numbers denote the mod 2 values of the parameters, and $H = H_2$ denotes the binary hull. The first six columns are covered by the proposition; the parameters of the last two columns are not possible: see our comment at the beginning of this section.

We can use results from [4, 17] concerning the dimension of the codes from adjacency matrices of strongly regular graphs.

Applications

In each of the examples given below, $H = H_2$ denotes the binary hull of an incidence design

of the relevant strongly regular graph Γ of type (n, k, λ, μ). We consider also H_p, for p odd, in some cases. When $p = 2$, we write $v_1(x) = v(x)$, since $v_0(x) = u(x)$. The length of the code is $\frac{1}{2}nk$ is each case.

1. The Paley graphs $P(q)$ are self-complementary of type $(q, \frac{q-1}{2}, \frac{q-1}{4} - 1, \frac{q-1}{4})$, where $q \equiv 1 \pmod 4$. Thus k is always even, but $\lambda \equiv 1 \pmod 2$ only if $q \equiv 1 \pmod 8$. In this case $k + \lambda$ is odd, and then that μ is even follows immediately since $\mu = \lambda + 1$. So $v(x) \in H$ and $u(x) \notin H$ for $q \equiv 1 \pmod 8$. Here $\mathrm{wt}(v(x)) = \frac{(q-1)^2}{8}$, and there are q such words. For $q \not\equiv 1 \pmod 8$, k is even and μ is odd, so $H = \{0\}$. Further, by Proposition 1, $\dim(H) = \frac{q-1}{2}$ when $q \equiv 1 \pmod 8$, since the codes $C_2(A)$, for A an adjacency matrix, are quadratic residue and have even dimension $\frac{q-1}{2}$, so that $\dim(C_2(A)^\perp) - 1 = \dim(H) = \frac{q-1}{2}$.
   - $q = 9$: here $P(9)$ is of type $(9, 4, 1, 2)$, and $\mathrm{wt}(v(x)) = 8$, the minimum weight as found by Magma [3, 7]: see also [14]. So H is a $[18, 4, 8]_2$ code.
   - $q = 17$: here $P(17)$ is of type $(17, 8, 3, 4)$, and $\mathrm{wt}(v(x)) = 32$, and the minimum weight as found by Magma [3, 7]: see also [14]. So H is a $[68, 8, 32]_2$ code. We constructed another $68 + 34 + 68$ words of weight 32 and, according to Magma, there are exactly 187 words of weight 32 in the hull.
     There are 68 words of weight 32 from the orbit of $w([0, 1]) = \sum_{x \in \{0,1,2,5,13,16\}} v^{\overline{x}}$, one for each of the 68 edges, where the subgraph on the set of six vertices $\{0, 1, 2, 5, 13, 16\}$ has two triangles $(0, 1, 2)$, $(0, 1, 16)$ and one 4-cycle $(0, 1, 5, 13)$, thus distinguishing the edge $[0, 1]$.
     There are 34 words of weight 32 from the orbit of $w(6) = \sum_{x \in \{0,6,12,13,16\}} v^{\overline{x}}$, two for each of the 17 vertices, where the subgraph on the set of five vertices $\{6, 0, 16, 12, 13\}$ has one 4-cycle $(0, 16, 12, 13)$, and one isolated vertex 6, thus distinguishing the vertex 6. The other set of vertices giving such a word from the vertex 6 is $\{6, 1, 3, 9, 11\}$.
     There are 68 words of weight 32 from the orbit of $y = \sum_{x \in \{0,12,2,14,4,16,8\}} v^{\overline{x}}$.
   - $q = 25$: here $P(25)$ is of type $(25, 12, 5, 6)$, and $\mathrm{wt}(v(x)) = 72$, but the minimum weight is 40 according to [14], so H is a $[150, 12, 40]_2$ code. We have constructed the 15 words of weight 40. If ω is a primitive element for the field $\mathbb{F}_{25}$ with minimal polynomial $X^2 + 4X + 2$, then $\pi = (1, \omega^3, \omega^4, \omega^{17}, \omega^{19})$ is a 5-cycle and the subgraph of $P(25)$ induced on it is the complete graph K_5. There are 15 of these, according to Magma, and the word of weight 40 is given by $w = \sum_{x \in \pi} v^{\overline{x}}$.
   - $q = 41$: here $P(41)$ is of type $(41, 20, 9, 10)$, and $\mathrm{wt}(v(x)) = 200$. The minimum weight is 140 according to [14], so H is a $[410, 20, 140]_2$ code. If π denotes the 10-cycle $(2, 4, 6, 7, 15, 40, 38, 36, 35, 27)$, then $w = \sum_{x \in \pi} v^{\overline{x}}$ is in H and has weight 140.
   - $q = 49$: here $P(49)$ is of type $(49, 24, 11, 12)$, and $\mathrm{wt}(v(x)) = 288$ but the minimum weight is 160 according to Magma, so H is a $[588, 24, 160]_2$.
     If ω is a primitive element for the field $\mathbb{F}_{49}$ with minimal polynomial $X^2 + 6X + 3$, then if $s = \{\omega^i \mid i \in \{3, 15, 25, 26, 32, 34, 40, 41\}\}$, $w = \sum_{x \in s} v^{\overline{x}} \in H$, and has weight 160. Note that the subgraph of the eight vertices in s is a connected 4-regular graph with 16 edges.
2. The triangular graphs $T(n) = L(K_n)$, with $n \geq 5$, are strongly regular of type $(\binom{n}{2}, 2(n-2), n-2, 4)$. The complement $T(n)^c$ is of type $(\binom{n}{2}, \binom{n-2}{2}, \binom{n-4}{2}, \binom{n-3}{2})$. For $T(n)$ the proposition implies that $v(x) \in H$ for $n \equiv 1 \pmod 2$, and $u(x) \in H$ for $n \equiv 0 \pmod 2$. Here $\mathrm{wt}(v(x)) = 2(n-2)(n-3)$, and $\mathrm{wt}(u(x) = 2(n-2)^2$. Note however, since $T(n)$ is the line graph of K_n which satisfies the conditions of Lemma 2 of [14], the binary hull is non-trivial for all n, and has words of weight $6(n-3)$. In all cases examined, this does seem to be the minimum weight of the hull. The binary codes from the adjacency

matrix are studied in [17, 26] and show, using Proposition 1 that the dimension of the hull is $\frac{1}{2}n(n-3)$ for n odd and $\binom{n-1}{2}$ for n even.

For the complement $T(n)^c$, the parity of the parameters varies modulo 4; the proposition shows that the hull is non-zero except when $n \equiv 2 \pmod 4$, when we have parity set $(0,1,1)$ and so $H = \{0\}$. Note that this implies that these graphs are not line graphs since the hull is never zero for line graphs, by Corollary 3. The binary codes from the adjacency matrices were examined in [13], and this implies that for $n \equiv 1 \pmod 4$, $\dim(H) = n-2$.

3. The lattice graphs, $L_2(n) = L(K_{n,n})$, are strongly regular of type $(n^2, 2(n-1), n-2, 2)$. For n odd $v(x) \in H$, and for n even $u(x) \in H$. The binary codes from the adjacency matrices were studied in [17, 31]. Using this and Proposition 1 we find that $\dim(H) = (n-1)^2$ for all $n \geq 2$. The complement is of type $(n^2, (n-1)^2, (n-2)^2, (n-1)(n-2))$, so $v(x) \in H$ for all n.

   Notice that $L_2(n)$ is the line graph of $K_{n,n}$, which has cycles of length 4, so we can use Proposition 5 to show that the hull is not zero.

4. The Brouwer-Haemers graph, Γ, is of type $(81, 20, 1, 6)$ and can be constructed from the vertex set $\mathbb{F}_{81}$ with $u \sim v$ if $u - v$ is a 4^{th} power. Here $\dim(H) = 60$, by Magma, and $\mathrm{wt}(v(x)) = 360$. The estimated minimum weight is 108. A word of weight 108 is obtained as follows: if ω is a root of the primitive polynomial X^4+2X^3+2, then $\pi_1 = (\omega^8, \omega^{78}, \omega^{58})$ and $\pi_2 = (\omega^{19}, \omega^{31}, \omega^{32})$ are 3-cycles and $w = \sum_{u\in\pi_1} v^{\overline{u}} + \sum_{u\in\pi_2} v^{\overline{u}} \in H$, of weight 108. For p odd, from the proposition $H_5 = \langle \boldsymbol{\jmath}_{810} \rangle$, and $H_3 = \{0\}$. Not covered by the proposition, but using Magma, are $H_7 = \{0\}$, where $7 \mid (k-\mu)$ but $7 \nmid \lambda$, and H_{11}, where $11 \nmid k, \mu, \lambda$, of dimension 60.

5. The symplectic graph, $\Gamma_{2m}(q)$, for $m \geq 2$ and q any prime power, is of type

$$(\frac{q^{2m}-1}{q-1}, \frac{q^{2m-1}-1}{q-1} - 1, \frac{q^{2m-2}-1}{q-1} - 2, \frac{q^{2m-2}-1}{q-1}),$$

   and the complement $\Gamma^c_{2m}(q)$ has type

$$(\frac{q^{2m}-1}{q-1}, q^{2m-1}, q^{2m-2}(q-1), q^{2m-2}(q-1)),$$

   i.e. $\lambda = \mu$ so the neighbourhood design is a 2-design.

   For $\Gamma^c_{2m}(q)$, for q odd, $k + \lambda$ is odd and μ is even, so $v(x) \in H$; for q even, k, λ, μ are even, so $u(x) \in H$; here words in the hull were also constructed in [23]. If $q = p^e$ then $p \mid k, \lambda, \mu$, so the proposition also implies that $u(x) \in H_p$.

   For $\Gamma_{2m}(q)$, if q is odd, k, λ, μ are even, so $u(x) \in H$. The 2-rank of an adjacency matrix for $\Gamma_{2m}(q)$ is given in [24], and with Proposition 1 this gives for the dimension of H $\frac{1}{2}(\frac{q^{2m}-1}{q-1} + q^m - 3)$ for m even, and $\frac{1}{2}(\frac{q^{2m}-1}{q-1} + q^m - 1)$ for m odd. For q even, k is even, λ, μ are odd, so $H = \{0\}$ in this case.

6. For parameter sets not included in Result 4 for which the lower bound of $2k-2$ for the minimum weight of the hull cannot be assumed, we have the Petersen graph, strongly regular of type $(10, 3, 0, 1)$, for which $w(x, y) \in H$. In [9], it was shown that H is a $[15, 4, 8]_2$ code, with weight distribution $(< 0, 1 >, < 8, 15 >)$. By computation, the Hoffman-Singleton graph of type $(50, 7, 0, 1)$ has H a $[175, 8, 64]_2$ code. Some other graphs with parameters in the excluded set are listed in [5]. We have not tested all of these; $P(9)$ we discussed above. The Shrikhande graph has type $(16, 6, 2, 2)$ with H a $[48, 9, 16]_2$ code, and the code from the incidence matrix has the gap between 6 and 10, with the words of weight 10 the differences of the intersecting rows.

5 Binary hulls for some classes of graphs

There are some specific classes of graphs, other than the strongly regular graphs discussed in the previous section, for which the binary hull of the incidence design has already been examined. These classes are among those that had been proved to satisfy the findings of Result 4 for codes over all prime fields. We describe some of these here. We first state a general result on the relationship of the binary hull of the incidence design of a graph Γ with the binary hull of the adjacency matrix of the line graph $L(\Gamma)$, from [9]:

Result 6 *Let Γ be a graph, G an incidence matrix for Γ, $C = C_2(G)$, $H = \mathrm{Hull}(C)$, L an adjacency matrix for $L(\Gamma)$, $C_L = C_2(L)$, and $H_L = \mathrm{Hull}(C_L)$. Then either $H = H_L$, or $H_L < H$ of codimension 1, or $H < H_L$ of codimension 1.*

Note that since the graphs discussed below all satisfy one of the conditions of Result 4 (except possibly for very small parameters), the minimum weight of the binary hull in each case is at least $2k-2$ where k is the valency.

5.1 Odd graphs $\mathcal{O}_k$ and $K_m \times \mathcal{O}_k$

The odd graphs $\mathcal{O}_k$ for $k \geq 2$ are the uniform subset graphs $\Gamma(2k+1, k, 0)$ whose vertices are the subsets of size k of a set of size $2k+1$, with two vertices being adjacent if the two k-subsets intersect in the empty set. Then $\mathcal{O}_k$ has valency $k+1$, i.e. it is $(k+1)$-regular. The binary codes from adjacency matrices of $\mathcal{O}_k$ were examined in [13]; see also [36]. Further, let $K_m \times \mathcal{O}_k = \mathcal{O}_k^m$, for $m \geq 2$, $k \geq 2$, denote the categorical product of the complete graph K_m with $\mathcal{O}_k$. This is a $(m-1)(k+1)$-regular graph. Write $\mathcal{O}_k^1 = \mathcal{O}_k$. Clearly if the 2-rank of an adjacency matrix for $\mathcal{O}_k$ is ρ, then, for $m \geq 2$, the 2-rank of $\mathcal{O}_k^m$ is $m\rho$ for m even, and $(m-1)\rho$ for m odd. In fact $\mathrm{rank}_2(\mathcal{O}_k) = \binom{2k}{k}$: see [13]. Also, if A is an adjacency matrix for $\mathcal{O}_k$ then $\mathrm{rank}_2(A+I) = \binom{2k}{k-1} + \binom{2k-1}{k-1} - 2^{k-1}$: see comments in [9]. Let G_k^m denotes an incidence matrix for $\mathcal{O}_k^m$. Then from [9, 13], by finding words in the hull, or using Proposition 1 when the valency is even:

Result 7 *For $k \geq 2$, $m \geq 1$, let G_k^m be an incidence matrix for $\mathcal{O}_k^m$, $C = C_2(G_k^m)$, $H_k^m = \mathrm{Hull}(C_2(G_k^m))$. Then*

$$\dim(H_k^m) = \begin{cases} \binom{2k-1}{k} + 2^{k-1} - 1 & \text{for } k \text{ even and } m = 1 \\ m\binom{2k}{k-1} - 1 & \text{for } k \text{ odd and } m = 1 \text{ or } m \text{ even;} \\ m\binom{2k}{k-1} + \binom{2k}{k} - 1 & \text{for } m \geq 3 \text{ odd.} \end{cases}$$

For k, m both even, $\dim(H_k^m) > \log_2(\binom{m}{2}\prod_{i=1}^{k}\binom{2i+1}{2}/k!)$.

Since $\mathcal{O}_k^m$ has an automorphism group that is transitive on edges, Result 4 applies and thus the binary hull has minimum weight at least $2\nu - 2$, where ν is the valency, and $\nu = k+1$ for $m = 1$, and $\nu = (m-1)(k+1)$ for $m \geq 2$.

5.2 Hamming graph $H(n, 2)$

The Hamming graph $H^k(n, m)$, for n, m, k integers, $m \geq 2$, $k < n$, has for vertices the m^n n-tuples of R^n, where R is a set of size m, and adjacency is defined by two n-tuples being adjacent if they differ in k coordinate position. The valency is $(m-1)^k\binom{n}{k}$. Codes from incidence matrices of these graphs were examined in [32]. For $k = 1$, the n-cube, also denoted by Q_n, is $H(n, 2)$ with $R = \mathbb{F}_2$, with valency n. The binary code from an adjacency matrix A for Q_n was studied in [30], and from the reflexive n-cube (with incidence matrix $A+I$) in [11], with a view to permutation decoding. Let G_n denote an incidence matrix for $H(n, 2)$. Then, from Proposition 1 and [30, 11]:

Result 8 *For $n \geq 3$,* $\dim(\mathrm{Hull}(C_2(G_n))) = 2^{n-1} - 1$.

The minimum weight is at least $2n - 2$.

5.3 Graphs on 3-sets

Let Ω be a set of size n, where $n \geq 3$. The set $\Omega^{\{3\}}$ of subsets of Ω of size 3 is the vertex set of the three graphs $A_i(n)$, for $i = 0, 1, 2$, with adjacency defined by two vertices (as 3-sets) being adjacent if the 3-sets meet in i elements, for $i = 0, 1, 2$, respectively. Let v_i denote the valency of $A_i(n)$ for $i = 0, 1, 2$, respectively, so $v_0 = \binom{n-3}{3}$, $v_1 = 3\binom{n-3}{2}$, $v_2 = 3(n-3)$. If $G_i(n)$ denotes a $\binom{n}{3} \times \frac{1}{2}v_i\binom{n}{3}$ incidence matrix for $A_i(n)$ and $C_p(G_i(n))$ the linear code from the row span of $G_i(n)$ over the field $\mathbb{F}_p$, where p is a prime. These codes were studied in [12]. The codes $C_2(A_i(n))$ were studied in [25]. Thus when the valency of $A_i(n)$ is even, we can use Proposition 1 and the results in [25] to get, using the notation just described:

Result 9 *Let $H_i(n) = \mathrm{Hull}(C_2(G_i(n))$ for $i = 0, 1, 2$ and $n \geq 7$. Then*

1. *$n \equiv 0 \pmod 4$: $\dim(H_0(n)) = \dim(H_1(n)) = n - 1$;*
2. *$n \equiv 1 \pmod 4$: $\dim(H_0(n)) = \binom{n}{2} - 1$, $\dim(H_2(n)) = \binom{n-1}{2} - 1$;*
3. *$n \equiv 3 \pmod 4$: $H_1(n) = \{0\}$; $\dim(H_0(n)) = \dim(H_2(n)) = \binom{n-1}{2} - 1$.*

The minimum weight of the non-zero binary hull is at least $2v_i - 2$ in all cases. The remaining hulls are from codes with odd valency, and require examination of the row span of $A + I$, which was not done in [25]. Computations with Magma for $7 \leq n \leq 13$ gave the results shown in Table 2, where $C_i = C_2(G_i(n))$ and $H_i = \mathrm{Hull}(C_i)$.

n	$\dim(C_i)$	$\dim(H_0)$	$\dim(H_1)$	$\dim(H_2)$
7	34	14	0	14
8	55	7	7	40
9	83	35	74	27
10	119	83	109	91
11	164	44	0	44
12	219	11	11	174
13	285	77	272	65
14	363	285	349	297

Table 2: Binary hulls for $G_i(n)$

The ternary codes from the A_i were studied in [27]. Proposition 1 will give the dimension of the ternary hull of an incidence matrix for $A_i(n)$ when $3 \mid v_i$. Since $3 \mid v_1, v_2$ for all n, and $3 \mid v_0$ for $n \equiv i \pmod 9$ for $i = 3, 4, 5$, we can use these results to obtain the dimension of the ternary hull in these cases, since $A + kI = A$ for $3 \mid k$.

6 Hulls over $\mathbb{F}_p$ where p is large

We will show here that the p-ary hulls for the graphs studied here will be zero for sufficiently large p. We establish the following proposition:

Proposition 4 *Let Γ be a connected k-regular graph, and G an incidence matrix for Γ. For any prime p, let $C_p = C_p(G)$ and $H_p = \mathrm{Hull}_p(C_p)$. Then there is a positive integer N such that $H_p = \{0\}$ for $p > N$.*

We first recall a basic result on the eigenvalues of an adjacency matrix of a regular graph.

Result 10 ([2, Proposition 3.1]) *Let Γ be a k-regular graph and A be an adjacency matrix of Γ. Then*

(i) k is an eigenvalue of A.
(ii) If Γ is connected then k has multiplicity 1 as an eigenvalue of A.
(iii) If δ is any eigenvalue of A then $|\delta| \leq k$.

Using the technique of proof in part (ii), it is easy to establish the following result.

Result 11 *Let Γ be a connected k-regular graph, let A be an adjacency matrix of Γ. Then $-k$ is an eigenvalue of A if, and only if, Γ is bipartite. In this case, $-k$ has multiplicity 1 as an eigenvalue of A.*

Corollary 2 *Let Γ be a k-regular graph with n vertices and let A be an adjacency matrix of Γ. Then, over $\mathbb{Q}$, $A + kI$ is non-singular if Γ is not bipartite and has rank $n-1$ if Γ is bipartite.*

We can now prove the proposition.

Proof: Let A be an adjacency matrix for Γ and, for any prime p, let B_p be the code spanned over $\mathbb{F}_p$ by the rows of $A + kI$. Also, let $n = |V(\Gamma)|$. We consider non-bipartite graphs and bipartite graphs separately.

Suppose that Γ is not a bipartite graph. By Result 11, $A + kI$ is non-singular. Hence, $\det(A + kI) \neq 0$. As $\det(A + kI)$ is an integer, we may let N be its largest prime factor or 2 if it has no prime factor. Then $\det(A + kI) \not\equiv 0 \pmod{p}$ if $p > N$. Hence, $\dim(B_p) = n$ if $p > N$ and so $\dim(B_p^\perp) = 0$ if $p > N$. By Proposition 1 (2), $\dim(H_p) = 0$.

Now suppose that Γ is a bipartite graph. By Result 11, 0 is an eigenvalue of $A + kI$ with multiplicity 1. Since $A + kI$ is a real symmetric matrix, its rank is $n-1$. Hence, for any prime p, $\dim(B_p) \leq n - 1$. Also, $A + kI$ has a non-singular $(n-1) \times (n-1)$ submatrix D. Since $\det D$ is a non-zero integer, we may let N be its largest prime factor or 2 if it has no prime factor. If $p > N$, there is a set of $n-1$ rows of $A + kI$ which are independent over $\mathbb{F}_p$. Hence, $\dim(B_p) \geq n - 1$ if $p > N$, and so $\dim(B_p) = n - 1$ if $p > N$. Hence, $\dim(B_p^\perp) = 1$ if $p > N$. By Proposition 1 (3), $\dim(H_p) = 0$. ■

7 Line graphs

Recall that for a graph $\Gamma = (V, E)$, if $x \in V$, then the degree of x is the valency of x and denoted by $\deg(x)$. If Γ is k-regular, then its line graph $L(\Gamma)$ is $2(k-1)$-regular. If G is an incidence matrix for Γ, and L an adjacency matrix for the line graph $L(\Gamma)$ then $G^T G = L + 2I_{|E|} = L$ over $\mathbb{F}_2$. Thus $C_2(L) \subseteq C_2(G)$, and if Γ is connected, $C_2(L)$ is the code $E_2(G)$ spanned by differences of the rows of G, and hence is either $C_2(G)$ or of codimension 1 in it. Since $\dim(C_2(L))$ is even (see for example [15, Proposition 2.1]), it follows from Result 3 that $\dim(C_2(L)) = n - 1$ if n is odd, and $\dim(C_2(L)) = n - 2$ if n is even. See a more detailed statement of this in [8, Corollary 6]. Note that the codes $C_p(L)$ for p odd are not very interesting if Γ has a cycle of small even length l, since then the minimum weight of $C_p(L)$ is at most l, by Lemma 1.

Proposition 5 *Let $\Gamma = (V, E)$ be a graph, $\pi = (x_0, \ldots, x_{l-1})$ an l-cycle in Γ with $l \geq 3$ and write $\rho_i = \deg(x_i)$ for $i = 0, \ldots, l-1$. Let $L(\Gamma)$ be the line graph of Γ, M an incidence matrix of $L(\Gamma)$, p a prime and $H_p = Hull(C_p(M))$. Define*

$$w(\pi) = \sum_{i=0}^{l-1} (-1)^i v^{\overline{[x_i, x_{i+1}]}},$$

with subscripts taken modulo l. Then

(i) $\mathrm{wt}(w(\pi)) = 2\sum_{i=0}^{l}\rho_i - 4l$;

(ii) $w(\pi) \in H_p$ *if and only if* $\rho_i + \rho_{i+1} \equiv 4 \pmod p$ *for* $i = 0, \ldots, l-1$.

Suppose that $\rho_i \geq 3$ *for some* i *with* $0 \leq i < l$. *Then* $H_p \neq \{0\}$ *if*

- l *is odd and there is a positive integer* ρ *such that* $\rho \equiv 2 \pmod p$ *and* $\rho_i \equiv \rho \pmod p$ *for* $i \geq 0$, *or*
- l *is even and either* $p = 2$ *and all* ρ_i *have the same parity, or* p *is odd and there are two positive integers* ρ *and* ρ' *such that* $\rho + \rho' \equiv 4 \pmod p$, $\rho_{2i} \equiv \rho \pmod p$ *and* $\rho_{2i+1} \equiv \rho' \pmod p$ *for* $i \geq 0$.

Moreover, if Γ *is connected and* k*-regular, with* $k \geq 3$, *and* $n = |V|$ *then* $\dim(H_2) = \frac{1}{2}n(k-2)+\delta$ *where* $\delta = 0$ *if* n *is odd, or* 1 *if* n *is even.*

Proof: Every base vector appearing in $w(\pi)$ has the form $v^{[[a,b],[a,c]]}$ where $[a,b]$ is an edge of π. Base vectors in which both $[a,b]$ and $[a,c]$ are edges of π occur twice and occur with opposite signs. All base vectors in which $[a,c]$ is not an edge of π occur once. It follows that the weight of $w(\pi)$ is

$$\sum_{i=0}^{l-1} |\overline{[x_i, x_{i+1}]}| - 2l = \sum_{i=0}^{l-1}(\rho_i + \rho_{i+1} - 2) - 2l = 2\sum_{i=0}^{l-1}\rho_i - 4l.$$

It is straightforward to verify that $(w(\pi), v^{\overline{[a,b]}}) = \pm(\rho_i + \rho_{i+1} - 4)$ if $[a,b]$ is the edge $[x_i, x_{i+1}]$ of π and $(w(\pi), v^{\overline{[a,b]}}) = 0$ if $[a,b]$ is any edge of Γ which is not an edge of π. Hence, $w(\pi) \in H_p$ if, and only if, $\rho_i + \rho_{i+1} \equiv 4 \pmod p$ for $i = 0, \ldots, l-1$. This condition is equivalent to $\rho_0 + \rho_1 \equiv 4 \pmod p$, $\rho_{2i} \equiv \rho_0 \pmod p$ and $\rho_{2i+1} \equiv \rho_1 \pmod p$ for $i \geq 0$ when l is even and $2\rho_0 \equiv 4 \pmod p$ and $\rho_i \equiv \rho_0 \pmod p$ for $i \geq 0$ when l is odd.

Now suppose that $\rho_i \geq 3$ for some i with $0 \leq i < l$. Then $\mathrm{wt}(w(\pi)) > 0$, so $w(\pi) \neq 0$. Hence, from the last remarks of the preceding paragraph, $w(\pi) \in H_p$ if either l is odd, p is any prime, and there is a positive integer ρ such that $\rho \equiv 2 \pmod p$ and $\rho_i \equiv \rho \pmod p$ for $i \geq 0$, or l is even and $p = 2$ and all ρ_i have the same parity, or p is odd and there are two positive integers ρ and ρ' such that $\rho + \rho' \equiv 4 \pmod p$, $\rho_{2i} \equiv \rho \pmod p$ and $\rho_{2i+1} \equiv \rho' \pmod p$ for $i \geq 0$.

Let L be an adjacency matrix of $L(\Gamma)$. If Γ is also connected, then $\dim(C_2(L)) = n - \epsilon$ where $\epsilon = 1$ if n is odd, and $\epsilon = 2$ if n is even. Since $L(\Gamma)$ has even degree, we can use Proposition 1 to get $\dim(H) = \frac{1}{2}nk - \dim(C_2(L)) - 1 = \frac{1}{2}nk - (n - \epsilon) - 1 = \frac{1}{2}nk - n + \epsilon - 1$, giving the stated result. □

Corollary 3 *Let* p *be a prime and let* Γ *be a connected* k*-regular graph, where* $k \geq 3$. *Let* G *be an incidence matrix for* Γ *and let* $H_p = Hull(C_p(G))$. *If* $H_p = \{0\}$ *and* Γ *is the line graph of a graph* Γ^* *then one of the following holds:*

- Γ^* *is regular,* p *is odd and* $k \not\equiv 2 \pmod p$;
- $\Gamma^* = K_{1,k}$ *and* $\Gamma = K_{k+1}$ *with* k *even if* $p = 2$ *or* $k \not\equiv 0, 1 \pmod p$ *if* p *is odd;*
- $\Gamma^* = (V_1 \cup V_2, E)$ *is a bipartite graph with vertex parts* V_1 *and* V_2, $k_i = \deg(x)$ *for* $x \in V_i$ $(i = 1, 2)$, $2 \leq k_1 < k_2$, $k = k_1 + k_2 - 2$ *and* $k \not\equiv 2 \pmod p$.

In particular, Γ *is not the line graph of a regular graph if* $H_2 = \{0\}$.

Proof: Suppose that $\Gamma = L(\Gamma^*)$ for some graph Γ^* and that $H_p = \{0\}$. Since isolated vertices of Γ^* contribute nothing to $L(\Gamma^*)$, we may suppose that Γ^* has no isolated vertices. As non-trivial connected components of Γ^* correspond to non-trivial components of Γ, Γ^* is also connected.

If Γ^* is regular, let l be its valency. Then $k = 2(l-1)$ is even. Hence, $k \geq 4$ and $l \geq 3$. So, Γ^* has an l'-cycle for some $l' \geq 3$. From Proposition 5, $H_p \neq \{0\}$ if $p = 2$ or p is odd and $l \equiv 2 \pmod{p}$. Hence, in this case, p is odd and $k = 2(l-1) \not\equiv 2 \pmod{p}$.

Now suppose that Γ^* is not regular. Since it is connected and Γ is k-regular, Γ^* is bipartite with vertex parts V_1 and V_2 and there are positive integers k_1 and k_2, with $k_1 < k_2$ and $k + 2 = k_1 + k_2$, such that a vertex of Γ^* has valency k_1 or k_2 according as it is in V_1 or V_2.

If $k_1 = 1$ then $\Gamma^* = K_{1,k+1}$ and $\Gamma = K_{k+1}$. From Proposition 2, it follows that k is even if $p = 2$, and if p is odd, $k \not\equiv 0, 1 \pmod{p}$.

If $k_1 > 1$ then Γ^* has a cycle of even length $l' \geq 4$. Hence, either $p = 2$ and $k_1 \not\equiv k_2 \pmod{2}$ (so k is odd) or p is odd and $k_1 + k_2 \not\equiv 4 \pmod{p}$ (so $k \not\equiv 2 \pmod{p}$). ■

Note: In the notation of Corollary 3:
1. If $\Gamma = L(\Gamma^*)$ where Γ^* is regular, we can have $H_p = \{0\}$ if p is odd and $k \not\equiv 2 \pmod{p}$: for example, if $\Gamma = L_2(3) = L(K_{3,3})$, $k = 4$, then $H_3 = \{0\}$.
2. If $\Gamma = L(\Gamma^*)$ where Γ^* is not regular, and Γ is not the complete graph, we can have $H_2 = \{0\}$: for example, if $\Gamma = L(K_{2,3})$, $k = 3$, $k_1 = 2$, $k_2 = 3$, then $H_2 = \{0\}$.
3. If Γ is 2-regular, then $\Gamma = C_n$, the circuit graph of order n, in which case $C_n \cong L(C_n)$. In this case, for G_n an incidence matrix (also an adjacency matrix), for all p, $\mathrm{Hull}_p(G_n) = \{0\}$ for $n \geq 3$ odd, and $\mathrm{Hull}_p(G_n) = \langle \boldsymbol{\jmath}_n \rangle$ for $n \geq 4$ even.

8 Permutation decoding

In [22, Lemma 7] the following was proved:

Result 12 *Let C be a linear code with minimum weight 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 value of $|\mathcal{O} \cap \mathcal{I}|/|\mathcal{O}|$, over the A-orbits $\mathcal{O}$. 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 holds 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, leading to the following result from [12]:

Result 13 *Let $\Gamma = (V, E)$ be a regular graph of valency k with automorphism group A transitive on edges. Let G be an incidence matrix for Γ. If, for p a prime, $C = C_p(G)$ is a $[|E|, |V| - \varepsilon, k]_p$ code, where $\varepsilon \in \{0, 1, \ldots, |V| - 1\}$, then any subgroup of A that is transitive on edges will serve as a PD-set for full error correction for C. In particular, A itself will be a PD-set.*

The implication of this for non-zero binary hulls of incidence designs of k-regular graphs with automorphism group transitive on edges and which satisfy one of the conditions given in Result 4 gives the following corollary:

Corollary 4 *Let $\Gamma = (V, E)$ be a regular graph of valency $k \geq 3$ with automorphism group A transitive on edges such that Γ satisfies one of the conditions of Result 4, and let G be an incidence matrix for Γ. Let $H = \mathrm{Hull}_2(G)$ be a $[|E|, d_H, w_H]_2$ non-zero code, and $s = \min(\lceil \frac{|E|}{d_H} \rceil - 1, \lfloor \frac{w_H - 1}{2} \rfloor)$. Then $\lfloor \frac{w_H - 1}{2} \rfloor \geq k - 2$, any subgroup of A that is transitive on edges will serve as an s-PD-set for H, and $s \geq \lfloor \frac{k-1}{2} \rfloor$ with $s > \lfloor \frac{k-1}{2} \rfloor$ if $k \geq 4$.*

Proof: From Result 4 we know that $w_H \geq 2k - 2$ so H corrects at least $k - 2$ errors, i.e. $\lfloor \frac{w_H - 1}{2} \rfloor \geq k - 2 \geq \lfloor \frac{k-1}{2} \rfloor$ for $k \geq 3$, and $> \lfloor \frac{k-1}{2} \rfloor$ for $k \geq 4$. Since $d_G = |V| - 1 = \dim(C_2(G)) > \dim(H) = d_H$, and since $\lceil \frac{|E|}{d_G} \rceil - 1 \geq \lfloor \frac{k-1}{2} \rfloor$ from Result 13, we have

$$\left\lceil \frac{|E|}{d_H} \right\rceil - 1 > \left\lceil \frac{|E|}{d_G} \right\rceil - 1 \geq \left\lfloor \frac{k-1}{2} \right\rfloor,$$

so $s = \min(\lceil \frac{|E|}{d_H} \rceil - 1, \lfloor \frac{w_H - 1}{2} \rfloor) \geq \lfloor \frac{k-1}{2} \rfloor$ for $k \geq 3$ and $> \lfloor \frac{k-1}{2} \rfloor$ for $k \geq 4$. ■

What follows from this is that, given the above conditions on Γ, the non-zero binary hull will correct more errors than the code from the incidence matrix when using a group transitive on edges as an s-PD-set, and permutation decoding. In fact it is very likely true that the words of weight $2k-2$ are the differences of incidence vectors of the rows of the incidence matrix corresponding to adjacent vertices, and thus that the minimum weight is at least $2k$, and much more than this in cases that are known.

Table 3 gives the value of the s in the corollary for the first few Paley graphs $P(q)$ when the binary hull of an incidence matrix is not zero. In the table, $d_H = \frac{q-1}{2}$, w_H, $t_H = \lfloor \frac{w_H - 1}{2} \rfloor$, $s_H = \min(\lceil \frac{|E|}{d_H} \rceil - 1, \lfloor \frac{w_H - 1}{2} \rfloor)$ denote the dimension, minimum weight, the full error-correction capability of the code, and value of s for the hull, and $d_G = q-1$, $w_G = \frac{q-1}{2}$, $t_G = \lfloor \frac{q-3}{4} \rfloor$, and $s_G = \min(\lceil \frac{|E|}{d_G} \rceil - 1, \lfloor \frac{w_G - 1}{2} \rfloor) = \min(\lceil \frac{q}{4} \rceil - 1, \lfloor \frac{q-3}{4} \rfloor) = \frac{q-5}{4}$, similarly for G. In all cases the minimum weight of the binary hull, found using Magma, is bigger than $2k-2$, where k denotes the valency $\frac{q-1}{2}$. The last two columns show $2k - 2 = q - 3$ and the length $|E| = \frac{1}{4}q(q-1)$ of the code. Since $d_H = \frac{q-1}{2}$, $\lceil \frac{|E|}{d_H} \rceil - 1 = \frac{q-1}{2} = k$, which is the value for s_H for $q \geq 17$.

From this it can be seen that the same set of automorphisms will correct more errors when using the binary hull than when using the code from the incidence matrix, although less data can be transmitted due to the lower dimension of the hull.

q	d_H	w_H	t_H	s_H	d_G	w_G	t_G	s_G	$2k-2$	$\|E\|$
9	4	8	3	3	8	4	1	1	6	18
17	8	32	15	8	16	8	3	3	14	68
25	12	40	19	12	24	12	5	5	22	150
41	20	140	69	20	40	20	9	9	38	410
49	24	160	79	24	48	24	11	11	46	588

Table 3: s-PD sets for the binary hull of an incidence matrix for $P(q)$

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 2011; 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] Norman Biggs, *Algebraic graph theory*, Cambridge: Cambridge University Press, 1974, Cambridge Tracts in Mathematics, Vol. 67.

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

[4] A. E. Brouwer and C. J. van Eijl, *On the p-rank of the adjacency matrices of strongly regular graphs*, J. Algebraic Combin. **1** (1992), 329–346.

[5] Andries Brouwer, http://www.win.tue.nl/ aeb/graphs/srg/srgtab.html.

[6] P. J. Cameron and J. H. van Lint, *Designs, graphs, codes and their links*, Cambridge: Cambridge University Press, 1991, London Mathematical Society Student Texts 22.

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

[8] P. Dankelmann, J. D. Key, and B. G. Rodrigues, *Codes from incidence matrices of graphs*, *Des. Codes Cryptogr.* (To appear, 2012).

[9] W. Fish, J. D. Key, and E. Mwambene, *Codes from odd graphs*, (Submitted).

[10] _____, *Codes from the incidence matrices and line graphs of Hamming graphs*, Discrete Math. **310** (2010), 1884–1897.

[11] _____, *Binary codes from designs from the reflexive n-cube*, Util. Math. **85** (2011), 235–246.

[12] _____, *Codes from the incidence matrices of graphs on* 3*-sets*, Discrete Math. **311** (2011), 1823–1840.

[13] Washiela Fish, *Codes from uniform subset graphs and cyclic products*, Ph.D. thesis, University of the Western Cape, 2007.

[14] Dina Ghinelli and Jennifer D. Key, *Codes from incidence matrices and line graphs of Paley graphs*, Adv. Math. Commun. **5** (2011), 93–108.

[15] C. Godsil and G. Royle, *Chromatic number and the* 2*-rank of a graph*, J. Combin. Theory, Ser. B **81** (2001), 142–149.

[16] Daniel M. Gordon, *Minimal permutation sets for decoding the binary Golay codes*, IEEE Trans. Inform. Theory **28** (1982), 541–543.

[17] Willem H. Haemers, René Peeters, and Jeroen M. van Rijckevorsel, *Binary codes of strongly regular graphs*, Des. Codes Cryptogr. **17** (1999), 187–209.

[18] S. L. Hakimi and J. G. Bredeson, *Graph theoretic error-correcting codes*, IEEE Trans. Inform. Theory **14** (1968), 584–591.

[19] S. L. Hakimi and H. Frank, *Cut-set matrices and linear codes*, IEEE Trans. Inform. Theory **11** (1965), 457–458.

[20] W. Cary Huffman, *Codes and groups*, Handbook of Coding Theory (V. S. Pless and W. C. Huffman, eds.), Amsterdam: Elsevier, 1998, Volume 2, Part 2, Chapter 17, pp. 1345–1440.

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

[22] _____, *Information sets and partial permutation decoding for codes from finite geometries*, Finite Fields Appl. **12** (2006), 232–247.

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

[24] _____, *Some binary codes from symplectic geometry of odd characteristic*, Util. Math. **67** (121-128), 2005.

[25] _____, *Binary codes from graphs on triples*, Discrete Math. **282/1-3** (2004), 171–182.

[26] _____, *Permutation decoding for binary codes from triangular graphs*, European J. Combin. **25** (2004), 113–123.

[27] _____, *Ternary codes from graphs on triples*, Discrete Math. **309** (2009), 4663–4681.

[28] ———, *Codes associated with triangular graphs, and permutation decoding*, Int. J. Inform. and Coding Theory **1, No.3** (2010), 334–349.

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

[30] J. D. Key and P. Seneviratne, *Permutation decoding for binary self-dual codes from the graph Q_n where n is even*, Advances in Coding Theory and Cryptology (T. Shaska, W. C. Huffman, D. Joyner, and V. Ustimenko, eds.), World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2007, Series on Coding Theory and Cryptology, 2, pp. 152–159.

[31] ———, *Permutation decoding of binary codes from lattice graphs*, Discrete Math. **308** (2008), 2862–2867.

[32] Jennifer D. Key, Washiela Fish, and Eric Mwambene, *Codes from the incidence matrices and line graphs of Hamming graphs $H^k(n, 2)$ for $k \geq 2$*, Adv. Math. Commun. **5** (2011), 373–394.

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

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

[35] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, Amsterdam: North-Holland, 1983.

[36] René Peeters, *On the p-ranks of the adjacency matrices of distance-regular graphs*, J. Algebraic Combin. **15** (2002), 127–149.

[37] J. Schönheim, *On coverings*, Pacific J. Math. **14** (1964), 1405–1411.