# Codes from incidence matrices of graphs

P. Dankelmann<sup>\*</sup> Department of Mathematics University of Johannesburg P.O. Box 524 Auckland Park 2006, South Africa J.D. Key<sup>†</sup>and B. G. Rodrigues<sup>‡</sup> School of Mathematical Sciences University of KwaZulu-Natal Durban 4041, South Africa

January 6, 2012

## Abstract

We examine the *p*-ary codes, for any prime *p*, from the row span over  $\mathbb{F}_p$  of  $|V| \times |E|$  incidence matrices of connected graphs  $\Gamma = (V, E)$ , showing that certain properties of the codes can be directly derived from the parameters and properties of the graphs. Using the edge-connectivity of  $\Gamma$  (defined as the minimum number of edges whose removal renders  $\Gamma$  disconnected) we show that, subject to various conditions, the codes from such matrices for a wide range of classes of connected graphs have the property of having dimension |V| or |V| - 1, minimum weight the minimum degree  $\delta(\Gamma)$ , and the minimum words the scalar multiples of the rows of the incidence matrix of this weight. We also show that, in the *k*-regular case, there is a gap in the weight enumerator between *k* and 2k-2 of the binary code, and also for the *p*-ary code, for any prime *p*, if  $\Gamma$  is bipartite. We examine also the implications for the binary codes from adjacency matrices of line graphs. Finally we show that the codes of many of these classes of graphs can be used for permutation decoding for full error correction with any information set.

Keywords: Incidence matrices, graphs, codes, permutation decoding Mathematics Subject Classifications (2010): 05B05, 05C38, 94B05

# 1 Introduction

In a number of recent papers, for example [15, 35, 33, 34, 17], the linear codes generated over any prime field by incidence matrices of some classes of regular connected graphs were studied. It was observed in these papers that all the codes share the property of having minimum weight the valency of the graph and minimum words the scalar multiples of the rows of the incidence matrix. This implies that in these cases the graph can be retrieved from the code. Furthermore, in some of the classes, these properties led to similar facts for the binary codes of the adjacency matrices of the associated line graphs, these being subcodes of the binary codes from the incidence matrices of the original graphs. Indeed, it was a study of the codes from the adjacency matrices of triangular graphs in [32] that pointed to this focus on the incidence matrices. Furthermore, it was noticed that the weight enumerator of the code of the incidence matrix had, in all cases studied, a gap between the weight k for the valency, and 2k - 2 for the difference of two rows, i.e. the valency of the line graph. This then immediately shows that, in these cases, the binary code of an adjacency matrix of the line graph of a graph  $\Gamma$  has the property that the minimum weight is either the valency of  $\Gamma$  or the valency of the line graph; in the latter case, that the

<sup>\*</sup>dankelma@gmail.com

<sup>&</sup>lt;sup>†</sup>keyj@clemson.edu

 $<sup>^{\</sup>ddagger}$ rodrigues@ukzn.ac.za

## 2 BACKGROUND AND TERMINOLOGY

words of that weight are the rows of the adjacency matrix might not necessarily follow, but does in fact seem to be true in some classes studied.

The question was thus asked whether these properties are in fact general for graphs satisfying certain conditions. We make a start at answering this question here by using the concept of edge-connectivity to show that this is indeed the case for many classes of graphs. Our result is wider for binary codes where we have the result for a large class of graphs: see Theorem 1 and Corollary 1. The proof does not extend directly to the same classes of graphs over  $\mathbb{F}_p$  for p odd, but a similar result can still be obtained, covering a smaller class of graphs: see Theorem 3, and Corollary 3. For bipartite connected graphs a proof similar to that for binary codes applies for all primes p, to thus cover the wider class of bipartite graphs: see Theorem 2 and Corollary 2.

The paper is arranged as follows: after giving the necessary terminology and some background results in Section 2 we state and prove our main results, Theorem 1 and its Corollary 1, for the binary codes of incidence matrices of connected graphs in Section 3, followed by Theorem 2 and Corollary 2 for the *p*-ary codes for p odd of incidence matrices of bipartite connected graphs in Section 4. In Section 5 we prove Theorem 3 and Corollary 3, our results for the *p*-ary codes of the non-bipartite graphs when p is odd. Section 6 deals with the question of the gap in the weight enumerator of these codes for both binary connected (Theorem 4) and *p*-ary bipartite connected (Theorem 5), with Corollaries 4 and 5 covering some applications. Section 7 deals with binary codes of adjacency matrices of line graphs, Section 8 deals with the dual codes, and finally some applications to permutation decoding are established in Section 9.

# 2 Background and terminology

## 2.1 Codes from designs

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- $(v, k, \lambda)$  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  $\lambda$  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  $C_F(\mathcal{D}) = \langle v^B | B \in \mathcal{B} \rangle$ , 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  $P \in \mathcal{P}, w(P)$  or  $w_P$  will denote the value of w at P. If  $F = \mathbb{F}_p$  then we 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 for a q-ary code C of length n, dimension k, and minimum weight d, where the **weight**  $\operatorname{wt}(v)$  of a vector v is the number of non-zero coordinate entries. The **support**,  $\operatorname{Supp}(v)$ , of a vector v is the set of coordinate positions where the entry in v is non-zero. So  $|\operatorname{Supp}(v)| = \operatorname{wt}(v)$ . 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.  $C^{\perp} = \{v \in F^n \mid (v, c) = 0 \text{ for all } c \in C\}$ . A **check matrix** for C is a generator matrix for  $C^{\perp}$ . 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  $\operatorname{Aut}(C)$ . 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**.

## 2.2 Graphs

The **graphs**,  $\Gamma = (V, E)$  with vertex set V, or  $V(\Gamma)$ , and edge set E, or  $E(\Gamma)$ , discussed here are undirected with no loops and no multiple edges. The **order** of  $\Gamma$  is |V|. If  $x, y \in V$  and x and y are adjacent, we write  $x \sim y$ , and xy, or [x, y], for the edge in E that they define. The **set of neighbours** of  $u \in V$  is denoted by N(u), and the **valency** or **degree** of u is |N(u)|, which we denote by  $\deg_{\Gamma}(u)$ . The **minimum** and **maximum** degrees of the vertices of  $\Gamma$  are denoted by  $\delta(\Gamma)$  and  $\Delta(\Gamma)$ , respectively. The graph is *k*-regular, where  $k \in \mathbb{N}_0$ , if all its vertices have degree k, and  $\Gamma$  is said to be **regular** if it is *k*-regular for some k. If S is a set of edges of  $\Gamma$ , then the **subgraph induced by** S, denoted by  $\Gamma[S]$ , is the subgraph of  $\Gamma$  whose vertex set consists of the vertices of  $\Gamma$  that are incident with an edge in S, and whose edge set is S. A **strongly regular graph**  $\Gamma$  of type  $(n, k, \lambda, \mu)$  is a regular graph on n = |V| vertices, with valency k which is such that any two adjacent vertices are together adjacent to  $\lambda$  vertices and any two non-adjacent vertices are together adjacent to  $\mu$  vertices.

If  $x_i x_{i+1}$  for i = 1 to r - 1, and  $x_r x_1$  are all edges of  $\Gamma$ , and the  $x_i$  are all distinct, then the sequence written  $(x_1, \ldots, x_r)$  will be called a **closed path**, **circuit** or **cycle**, of length r, also written  $C_r$ . If for every pair of vertices there is a path connecting them, the graph is **connected**. A **perfect matching** is a set S of disjoint edges such that every vertex is on exactly one member of S. The **girth**  $g(\Gamma)$  of  $\Gamma$ is the length of a shortest cycle in  $\Gamma$ . If  $\Gamma$  has a cycle of even length, then the **even girth**  $g_e(\Gamma)$  is the length of a shortest even cycle. The **distance** d(u, v) between two vertices u and v of a graph  $\Gamma$  is the minimum length of a path from u to v. The **diameter** of  $\Gamma$ , denoted by diam $(\Gamma)$  is the largest of all distances between vertices of  $\Gamma$ , i.e., diam $(\Gamma) = \max_{u,v \in V(\Gamma)} d(u, v)$ .

An adjacency matrix  $A = [a_{u,v}]$  of a graph  $\Gamma = (V, E)$  is a  $|V| \times |V|$  matrix with entries  $a_{u,v}$ ,  $u, v \in V$ , such that  $a_{u,v} = 1$  if  $u \sim v$  and  $a_{u,v} = 0$  otherwise. An incidence matrix of  $\Gamma$  is an  $|V| \times |E|$ matrix  $G = [g_{u,e}]$  with  $g_{u,e} = 1$  if the vertex u is on the edge e and  $g_{u,e} = 0$  otherwise. We denote the row of G corresponding to vertex v by  $G_v$ , and the column corresponding to edge e by  $G^e$ .

If  $\Gamma$  is regular with valency k, then the 1-(|E|, k, 2) design with incidence matrix G is called the **incidence design** of  $\Gamma$ . It was proved in [15] that if  $\Gamma$  is regular with valency k and  $\mathcal{G}$  the 1-(|E|, k, 2) incidence design for  $\Gamma$ , then Aut( $\Gamma$ ) = Aut( $\mathcal{G}$ ). 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  $\Gamma$  share a vertex in  $\Gamma$ .

The **code** of a graph  $\Gamma$  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 rank<sub>p</sub>(A) if  $F = \mathbb{F}_p$ , in which case we will speak of the *p*-rank of A or  $\Gamma$ , 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  $\Gamma$ ,  $C_p(G)$  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  $\Gamma$  is regular. If M is an adjacency matrix for  $L(\Gamma)$  where  $\Gamma$  is regular of valency k, |V| vertices, |E| edges, then

$$G^T G = M + 2I_{|E|},\tag{1}$$

where G is an incidence matrix for  $\Gamma$ .

If W, X are non-empty disjoint sets of vertices of  $\Gamma$ , then E(W, X) denotes the set of edges that have one end in W and the other end in X, and we write |E(W, X)| = q(W, X). An **edge-cut** of a connected graph  $\Gamma$  is a set  $S \subseteq E$  such that  $\Gamma - S = (V, E - S)$  is disconnected. The **edge-connectivity**  $\lambda(\Gamma)$  is the minimum cardinality of an edge-cut. The following well-known fact will be of use

$$\lambda(\Gamma) = \min_{\emptyset \neq W \subset V} q(W, V - W).$$
<sup>(2)</sup>

A **bridge** of a connected graph is an edge whose removal disconnects the graph. So  $\Gamma$  has a bridge if and only if  $\lambda(\Gamma) = 1$ . Whitney [51] observed that  $\lambda(\Gamma) \leq \delta(\Gamma)$  for every graph  $\Gamma$ ; this follows directly from the fact that removing the edges incident with a vertex of degree  $\delta(\Gamma)$  disconnects the graph. If  $\lambda(\Gamma) = \delta(\Gamma)$  and, in addition, the only edge sets of cardinality  $\lambda(\Gamma)$  whose removal disconnects  $\Gamma$  are the sets of edges incident with a vertex of degree  $\delta(\Gamma)$ . The concept of super-

## 3 BINARY CODES

edge-connectivity was first introduced by Bauer, Suffel, Boesch, and Tindell [3] in 1981, and it has been studied extensively since.

The following result is due initially to Björner and Karlander [4], but it is stated, and a short proof given, in [35]:

**Result 1** Let  $\Gamma = (V, E)$  be a connected graph, G an incidence matrix for  $\Gamma$ , and  $C_p(G)$  the row-span of G over  $\mathbb{F}_p$ . Then dim $(C_2(G)) = |V| - 1$ . For odd p, dim $(C_p(G)) = |V|$  if  $\Gamma$  has a closed path of odd length (i.e., if  $\Gamma$  is not bipartite), and dim $(C_p(G)) = |V| - 1$  if  $\Gamma$  has no closed path of odd length (i.e., if  $\Gamma$  is bipartite).

Recall that a graph is bipartite if and only if it does not have an odd cycle.

## 2.3 Permutation decoding

**Permutation decoding** was first developed by MacWilliams [41] and involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and Sloane [42, Chapter 16, p. 513] and Huffman [25, Section 8]. In [30] and [36] 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 S of automorphisms of C which is such that every t-set of coordinate positions is moved by at least one member of S into the check set  $\mathcal{C}$ .

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

The algorithm for permutation decoding is given in [25] 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 [19], from a formula due to Schönheim [46], and quoted and proved in [25].

## **3** Binary codes

We consider now the binary code  $C_2(G)$ , where G is an incidence matrix of a connected graph  $\Gamma$ . Note that  $C_2(G)$  is also known as the **cut space** of  $\Gamma$ , and examined for majority-logic decoding in [20, 21]. Our main result is as follows, where we use the notation as defined in Section 2.

**Theorem 1** Let  $\Gamma = (V, E)$  be a connected graph,  $G \mid V \mid \times \mid E \mid$  incidence matrix for  $\Gamma$ . Then

- 1.  $C_2(G) = [|E|, |V| 1, \lambda(\Gamma)]_2;$
- 2. if  $\Gamma$  is super- $\lambda$ , then  $C_2(G) = [|E|, |V| 1, \delta(\Gamma)]_2$ , and the minimum words are the rows of G of weight  $\delta(\Gamma)$ .

**Proof:** It follows from Result 1 that  $C_2(G)$  has dimension |V| - 1, so we only have to prove that  $C_2(G)$  has minimum weight  $\lambda(\Gamma)$ .

(1). Let x be a nonzero word in  $C_2(G)$  of minimum weight d. Then  $x = \sum_{v \in V} \mu_v G_v$  for some  $\mu_v \in \mathbb{F}_2$ , not all zero. This yields a labelling of the vertices of  $\Gamma$  with elements of  $\mathbb{F}_2$ , where v is labeled with  $\mu_v$ . If e = uv is an edge of  $\Gamma$ , then the entries  $G_{u,e}$  and  $G_{v,e}$  are the only nonzero entries in column  $G^e$ . Hence

$$x_e = \mu_u + \mu_v,\tag{3}$$

i.e.,  $x_e$  is the sum of the labels of the two vertices incident with e. So  $x_e = 0$  if and only if  $\mu_u + \mu_v = 0$ , i.e.  $\mu_u = \mu_v$ . So, if Supp(x) is the support of x, then for every edge uv in  $\Gamma$  we have

$$uv \in \operatorname{Supp}(x) \iff \mu_u \neq \mu_v.$$

## 3 BINARY CODES

Now consider the graph  $\Gamma_x = (V, E - \operatorname{Supp}(x))$ . If two vertices u, v are adjacent in  $\Gamma_x$ , then  $\mu_u + \mu_v = 0$ , and so  $\mu_u = \mu_v$ . It follows that for any two vertices u and v in the same component of  $\Gamma_x$  we have  $\mu_u = \mu_v$ . Thus  $\Gamma_x$  is disconnected since otherwise, if  $\Gamma_x$  were connected, all  $\mu_v$  would have the same value,  $\mu$  say, and so  $x = \mu \sum_v G_v = \mu 0 = 0$ , a contradiction. Hence  $\operatorname{Supp}(x)$  is an edge-cut of  $\Gamma$ , and so  $|\operatorname{Supp}(x)| \ge \lambda(\Gamma)$  and  $d = \operatorname{wt}(x) \ge \lambda(\Gamma)$ .

Now we construct a word of weight  $\lambda(\Gamma)$ . Let  $S \subseteq E$  be a minimal edge-cut of  $\Gamma$ . Then, due to the minimality of S,  $\Gamma - S = (V, E - S)$  has V partitioned into two connected components, W and V - W which are such that if  $u, v \in W$  and  $u \sim v$ , then  $uv \notin S$ , and similarly for V - W. Thus the edges in S are precisely the edges between W and V - W, and not those within either of the components. Let  $x = \sum_{v \in W} G_v = \sum_{v \in V} \mu_v G_v$ , where  $\mu_v = 1$  if  $v \in W$ , and  $\mu_v = 0$  if  $v \in V - W$ . Clearly, for an edge  $uv \in E$  we have

$$uv \in \operatorname{Supp}(x) \iff \mu_u \neq \mu_v \iff uv \in S.$$

Hence wt(x) =  $|\text{Supp}(x)| = |S| = \lambda(\Gamma)$ . This proves that the minimum weight of  $C_2(G)$  is  $\lambda(\Gamma)$ .

(2). Now suppose  $\Gamma$  is super- $\lambda$ . It follows from (1) that the minimum weight of  $C_2(G)$  is  $\lambda(\Gamma) = \delta(\Gamma)$ . We show that a word of this weight must be a row of G of weight  $\delta(\Gamma)$ . Let  $x = \sum_{v \in V} \mu_v G_v$  be a word in  $C_2(G)$  of weight  $\delta(\Gamma)$ . As in the argument in (1), it follows that  $\Gamma_x = (V, E - \operatorname{Supp}(x))$  is disconnected, and that  $\operatorname{Supp}(x)$  is an edge-cut of cardinality  $\lambda(\Gamma)$ . Since  $\Gamma$  is super- $\lambda$ , it follows that  $\Gamma_x$  has exactly two components, one consisting of a single vertex, v say, of degree  $\delta(\Gamma)$ , and the other component containing the vertices in  $V - \{v\}$ . Thus  $\operatorname{Supp}(x) = \{uv \mid u \in N(v)\}$  so x is clearly the row  $G_v$ , which proves (2).

The usefulness of part (1) of the above theorem lies in the fact that it shows that the minimum weight of the binary code from the incidence matrix of a graph equals the degree of the vertices of the graph for several graph classes for which it is known that  $\lambda(\Gamma) = \delta(\Gamma)$ . Below we give some sufficient conditions from the literature. We state the conditions for regular graphs since we mainly consider the incidence matrices of regular graphs, but in most cases the conditions apply also to graphs that are not necessarily regular.

**Result 2** Let  $\Gamma = (V, E)$  be a connected k-regular graph. Then  $\lambda(\Gamma) = k$  if one of the following conditions holds:

- 1.  $\Gamma$  is vertex-transitive (Mader [43]);
- Γ has diameter at most 2, i.e. any two vertices of Γ are adjacent or have a neighbour in common (Plesník [44]);
- 3.  $\Gamma$  is strongly regular with parameters  $(n, k, \lambda, \mu)$  and  $\mu \geq 1$  (follows from 2. above);
- 4.  $\Gamma$  is distance-regular and k > 2 (Brouwer and Haemers [6]);
- 5.  $k \ge (|V(\Gamma)| 1)/2$  (Chartrand [8]);
- 6.  $\Gamma$  has girth g and diam $(\Gamma) \leq g-1$  if g is odd, or diam $(\Gamma) \leq g-2$  if g is even (Soneoka, Nakada, Imase, Peyrat [26]).

Further,  $\Gamma$  is super- $\lambda$  if one of the following conditions is satisfied:

- 1a  $\Gamma$  is vertex-transitive and has no complete subgraph of order k (Tindell [48]);
- 2a.  $\Gamma$  has diameter at most 2, and in addition  $\Gamma$  has no complete subgraph of order k (Fiol [13]);
- 3a.  $\Gamma$  is strongly regular with parameters  $(n, k, \lambda, \mu)$ , and  $\mu \ge 1$ ,  $\lambda \le k-3$  (follows from 2a. above);
- 4a.  $\Gamma$  is distance-regular and k > 2 (Brouwer and Haemers [6]);

5a.  $k \ge \frac{|V|+1}{2}$  (Kelmans [29]);

## 4 BIPARTITE GRAPHS

6a.  $\Gamma$  has girth g, and diam $(\Gamma) \leq g-1$  if g is odd, or diam $(\Gamma) \leq g-2$  if g is even. (Fabrega, Fiol [11]).

We note that more conditions for a graph to satisfy  $\lambda(\Gamma) = \delta(\Gamma)$  can be found, for example, in the survey paper [24] by Hellwig and Volkmann.

These results, in conjunction with Theorem 1, imply the following.

**Corollary 1** Let  $\Gamma = (V, E)$  be a connected k-regular graph on |V| = n vertices, G an  $n \times \frac{nk}{2}$  incidence matrix for  $\Gamma$ . If any one of the conditions 1 - 6 of Result 2 holds, then the binary code  $C_2(G)$  has minimum weight k. If any one of the conditions 1a - 6a holds, then the only words of weight k are the rows of the incidence matrix.

# 4 Bipartite graphs

In general the statement of Theorem 1 does not hold for *p*-ary codes of incidence matrices of graphs if p is odd. For example it is easy to verify that the code  $C_p(K_4)$  contains a word of weight 2, *viz.* the word  $w = G_u + G_v - G_x - G_y$ , where u, v, x, y are the vertices of  $K_4$ , has wt(w) = 2, but  $\lambda(K_4) = 3$ .

We show below that for odd p the conclusions of Theorem 1 still hold in the case when  $\Gamma$  is connected bipartite. Of course the theorem itself, for p = 2, will hold for  $\Gamma$  connected bipartite.

**Theorem 2** Let  $\Gamma = (V, E)$  be a connected bipartite graph,  $G \mid V \mid \times \mid E \mid$  incidence matrix for  $\Gamma$ , and p an odd prime. Then

- 1.  $C_p(G) = [|E|, |V| 1, \lambda(\Gamma)]_p;$
- 2. if  $\Gamma$  is super- $\lambda$ , then  $C_p(G) = [|E|, |V| 1, \delta(\Gamma)]_p$ , and the the minimum words are the non-zero scalar multiples of the rows of G of weight  $\delta(\Gamma)$ .

**Proof:** (1). Let  $V = U \cup W$  be the bipartition of  $V(\Gamma)$  and let  $x = \sum_{v \in V} \mu_v G_v$ , be a nonzero word in  $C_p(\Gamma)$ . As in the proof of Theorem 1 we have, for every edge uv of  $\Gamma$ ,  $x_{uv} = \mu_u + \mu_v$  and so

$$uv \in \operatorname{Supp}(x) \iff \mu_u \neq -\mu_v.$$

Let  $\Gamma_x = (V, E - \operatorname{Supp}(x))$  and consider a component  $\Gamma_1$  of  $\Gamma_x$ . Let  $U_1 = V(\Gamma_1) \cap U$  and  $W_1 = V(\Gamma_1) \cap W$ . Fix a vertex v in one of the two partite sets of  $\Gamma_1$ , say  $v \in U_1$ , and let  $a = \mu_v$ . Then  $\mu_w = -a$  for each neighbour w of v in  $\Gamma_1$ . Each neighbour w of a neighbour of v in  $\Gamma_1$  has  $\mu_w = a$  and so on. We conclude that  $\mu_w = a$  for all  $u \in U_1$ , and  $\mu_w = -a$  for  $u \in W_1$ .

It follows from the above that no edge in  $\operatorname{Supp}(x)$  joins two vertices in the same component of  $\Gamma_x$ . Hence  $\Gamma_x$  is disconnected,  $\operatorname{Supp}(x)$  is an edge-cut of  $\Gamma$ , and  $|\operatorname{Supp}(x)| \ge \lambda(\Gamma)$ . Thus  $\operatorname{wt}(x) = |\operatorname{Supp}(x)| \ge \lambda(\Gamma)$ , as required.

Now we construct a word of weight  $\lambda(\Gamma)$ . Let  $S \subseteq E$  be a minimum edge-cut of  $\Gamma$ , and let  $V_1$  and  $V_2$  be the vertex sets of the two components  $\Gamma_1$  and  $\Gamma_2$ , respectively, of  $\Gamma - S = (V, E - S)$ , and let  $U_i = U \cap V_i$  and  $W_i = W \cap V_i$  for i = 1, 2. Define

$$\mu_v = \begin{cases} 1 & \text{if } v \in U_1 \cup W_2, \\ -1 & \text{if } v \in U_2 \cup W_1, \end{cases}$$

and consider the word  $x = \sum_{v \in V_1} \mu_v G_v$ . Clearly, for an edge  $uv \in E(\Gamma_1) \cup E(\Gamma_2)$  we have  $x_{uv} = \mu_u + \mu_v = 0$ , while for each edge  $uw \in S$  with  $u \in U$  and  $w \in W$  we have

$$x_{uv} = \mu_u + \mu_v = \begin{cases} 2 & \text{if } u \in U_1 \text{ and } w \in W_2, \\ -2 & \text{if } u \in U_2 \text{ and } w \in W_1, \end{cases}$$

and so Supp(x) = S. Hence  $\text{wt}(x) = |S| = \lambda(\Gamma)$ , and (1) follows.

## 4 BIPARTITE GRAPHS

(2). Now suppose that  $\Gamma$  is super- $\lambda$ . It follows by part (1) that the minimum weight of  $C_p(G)$  is  $\delta(\Gamma)$ . Let x be a non-zero word in  $C_p(G)$  of this weight. As in the proof of Theorem 1,  $\Gamma_x$  has exactly two components, one consisting of a single vertex v of degree  $\delta(\Gamma)$ , and the other component containing the vertices in  $V - \{v\}$ . Thus  $\operatorname{Supp}(x) = \{uv \mid u \in N(v)\}$ , and  $x = \sum_{u \in N(v)} \alpha_u v^{uv}$  (in the notation of Section 2.1), for some non-zero  $\alpha_u \in \mathbb{F}_p$ . If  $x \neq \alpha G_v$  then the  $\alpha_u$  are not constant over N(v), so for some  $\alpha \neq 0$ ,  $\alpha G_v - x$  has weight less than  $\delta(\Gamma)$  which contradicts (1). Thus x is a scalar multiple of the row  $G_v$ , which proves (2).

The sufficient conditions for  $\lambda(\Gamma) = k$  or for  $\Gamma$  to be super- $\lambda$  in Result 2 of course also apply to connected bipartite graphs. However, some sufficient conditions for  $\lambda(\Gamma) = \delta(\Gamma)$  can be relaxed in that case. Again from the literature we have the following:

## **Result 3** Let $\Gamma = (V, E)$ be a connected bipartite graph.

Then  $\lambda(\Gamma) = \delta(\Gamma)$  if one of the following conditions holds:

- 1.  $\Gamma = (V, E)$  and V consists of at most two orbits under Aut( $\Gamma$ ) (Liang [40]), and in particular if  $\Gamma$  is vertex-transitive (Tindell [48]);
- 2. every two vertices in one of the two partite sets of  $\Gamma$  have a common neighbour (Dankelmann and Volkmann [9]);
- 3. Γ has diameter at most 3 (Plesník, Znám [45]);
- 4.  $\Gamma$  is k-regular and  $k \ge (n+1)/4$  (Volkmann [49]);
- 5. If  $\Gamma$  has girth g and diam $(\Gamma) \leq g 1$  (Fabrega, Fiol [12]).
- If  $\lambda(\Gamma) = \delta(\Gamma)$  and  $\Gamma$  satisfies one of the following conditions, then it is super- $\lambda$ :
- 1a.  $\Gamma$  is vertex-transitive (Tindell [48]);
- 2a.  $\Gamma$  is k-regular and  $k \ge (n+3)/4$  (Fiol [13]).

These results, in conjunction with Theorem 2, imply the following.

**Corollary 2** Let  $\Gamma = (V, E)$  be a connected bipartite graph,  $G \mid V \mid \times \mid E \mid$  incidence matrix for  $\Gamma$ . If at least one of the conditions 1 - 5 of Result 3 holds, then the code  $C_p(G)$  has minimum weight  $\delta(\Gamma)$ . If  $\Gamma$  satisfies one of the conditions 1a - 2a of Result 3, then the words of minumum weight  $\delta(\Gamma)$  are the scalar multiples of the rows of G of weight  $\delta(\Gamma)$ .

The following example concerns bipartite graphs whose incidence matrices were considered in [16].

**Example 1** For  $\Omega$  a set of size  $n, n \geq k, l$ , and  $k, l \geq i$ , let  $\Gamma(n, k, l, i)$  denote the bipartite graph on two disjoint sets  $A_n = \Omega^{\{k\}}$  and  $B_n = \Omega^{\{l\}}$ , i.e. of  $\binom{n}{k} + \binom{n}{l}$  vertices,  $A_n \cup B_n$ , where  $a \in A_n$  is on an edge with  $b \in B_n$  if  $|a \cap b| = i$ . For vertices  $A_n$  the valency is  $\binom{k}{i}\binom{n-k}{l-i}$ ; for vertices in  $B_n$  it is  $\binom{l}{i}\binom{n-l}{k-i}$ . The number of edges is  $\binom{n}{k}\binom{k}{i}\binom{n-k}{l-i} = \binom{n}{l}\binom{l}{i}\binom{n-l}{k-i}$ . Then for n > k,  $\Gamma(n, k, l, i) \cong \Gamma(n, n - k, l, l - i)$ and for all p, dim $(C_p(M(n, k, l, i)) \leq \binom{n}{k} + \binom{n}{l} - 1$ , with equality if  $\Gamma(n, k, l, i)$  is connected. Clearly condition 1 of Result 3 holds, so the minimum weight is the minimum degree for these codes, for all p. When k = l we can also state that the words of weight  $\binom{k}{i}\binom{n-k}{l-i}$  are the multiples of the rows of an incidence matrix for  $\Gamma(n, k, k, i)$ , by condition 1a of Result 3.

# 5 Codes over $\mathbb{F}_p$ , p odd

We have not been able to prove a general theorem similar to Theorem 1 for p odd, although it indeed seems to hold for all the classes studied earlier in [15, 35, 33, 34, 17], for example. However, we give a result, Theorem 3, which is somewhat analogous to Theorem 1. It links the minimum distance of  $C_p(\Gamma)$ to a graph parameter,  $\lambda_{bip}(\Gamma)$  which is defined below. The parameter  $\lambda_{bip}(\Gamma)$  is new and has not been studied before.

We define a **bipartition set** of  $\Gamma = (V, E)$  to be a set  $S \subseteq E$  such that  $\Gamma - S = (V, E - S)$ has a bipartite component. We denote the minimum cardinality of a bipartition set of  $\Gamma$  by  $\lambda_{bip}(\Gamma)$ . Clearly,  $\lambda_{bip}(\Gamma) \leq \delta(\Gamma)$  since removing the edges incident with a vertex of degree  $\delta(\Gamma)$  creates a bipartite component. It appears that for some of the sufficient conditions that imply  $\lambda(\Gamma) = \delta(\Gamma)$  there are similar conditions implying  $\lambda_{bip}(\Gamma) = \delta(\Gamma)$ . We give two such conditions below. Following the terminology for  $\lambda(\Gamma)$ , we call a non-bipartite graph  $\Gamma$  **super**- $\lambda_{bip}$  if  $\lambda_{bip}(\Gamma) = \delta(\Gamma)$  and the only sets  $S \subseteq E(\Gamma)$  of cardinality  $\lambda_{bip}(\Gamma)$  whose removal creates a bipartite component are the sets of edges incident with a vertex of degree  $\delta(\Gamma)$ .

**Theorem 3** Let  $\Gamma = (V, E)$  be a connected graph that is not bipartite, p be an odd prime, and G be an incidence matrix for  $\Gamma$ . Then

- 1.  $C_p(G) = [|E|, |V|, \lambda_{bip}(\Gamma)]_p;$
- 2. if  $\Gamma$  is super- $\lambda_{bip}$  then  $C_p(\Gamma) = [|E|, |V|, \delta(\Gamma)]_p$ , and the minimum words are the non-zero scalar multiples of the rows of G of weight  $\delta(\Gamma)$ .

**Proof:** It follows from Result 1 that  $C_p(G)$  has dimension |V|, so we only have to prove that  $C_p(G)$  has minimum weight  $\lambda_{bip}(\Gamma)$ .

(1). Let d be the minimum weight of  $C_p(G)$ . We first show that  $d \ge \lambda_{bip}(\Gamma)$ . Let  $x = \sum_{v \in V} \mu_v G_v \in C_p(G)$  have weight d. Since  $x \ne 0$ , there is a vertex v with  $\mu_v \ne 0$ . Let  $\Gamma_1$  be the component of  $\Gamma_x = (V, E - \operatorname{Supp}(x))$  containing v, and let  $a = \mu_v$ . As in the proof of Theorem 2 the component  $\Gamma_1$  is bipartite with the values  $\mu_w = a$  if w is in the same partite set as v, and  $\mu_w = -a$  if w is in the other partite set. Hence  $\Gamma_x$  contains a bipartite component, and so  $\operatorname{Supp}(x)$  is a bipartition set. Therefore,

$$d = |\operatorname{Supp}(x)| \ge \lambda_{bip}(\Gamma)$$

as required.

To show that  $d \leq \lambda_{bip}(\Gamma)$  we construct a word of weight  $\lambda_{bip}(\Gamma)$ . Let S be a bipartition set of cardinality  $\lambda_{bip}(\Gamma)$  and let  $\Gamma_1$  be a bipartite component of  $\Gamma - S$ , with bipartite sets  $U_1$  and  $W_1$ . Define

$$\mu_{v} = \begin{cases} 1 & \text{if } v \in U_{1}, \\ -1 & \text{if } v \in W_{1}, \\ 0 & \text{if } v \in V - V(\Gamma_{1}), \end{cases}$$

and consider the word  $x = \sum_{v \in V_1} \mu_v G_v$ . Clearly, for an edge  $uv \in E(\Gamma_1)$  we have  $x_{uv} = \mu_u + \mu_v = 1 + (-1) = 0$ , and for the edges of  $\Gamma_x = (V, E - \operatorname{Supp}(x))$  joining two vertices in a component of  $\Gamma - S$  other than  $\Gamma_1$  we have  $x_{uv} = \mu_u + \mu_v = 0 + 0 = 0$ .

So Supp $(x) \subseteq S$ , and thus wt $(x) \leq \lambda_{bip}(\Gamma)$ . Since  $\Gamma$  is not bipartite, we have  $\Gamma_1 \neq \Gamma$ , and so there exist edges joining two vertices in the same partite set of  $\Gamma_1$ , or edges joining a vertex in  $\Gamma_1$  to a vertex not in  $\Gamma_1$ . For these edges we have  $x_e \neq 0$ , so x is not the zero-word. Hence wt $(x) \geq \lambda_{bip}(\Gamma)$ , as desired.

(2). Now suppose  $\Gamma$  is super- $\lambda_{bip}$ . It follows from (1) that the minimum weight of  $C_p(G)$  is  $\lambda_{bip}(\Gamma) = \delta(\Gamma)$ . We show that a word of this weight must be a scalar multiple of a row of G of weight  $\delta(\Gamma)$ . Let  $x = \sum_{v \in V} \mu_v G_v$  be a word in  $C_p(G)$  of weight  $\delta(\Gamma)$ . As in the proof of Theorem 2, it follows that

## 5 CODES OVER $\mathbb{F}_P$ , P ODD

 $\Gamma_x = \Gamma - \text{Supp}(x)$  contains a bipartite component and that Supp(x) is a bipartition set of  $\Gamma$ . Since  $\Gamma$  is super- $\lambda_{bip}$ , it follows that Supp(x) is the set of edges incident with some vertex v of degree  $\delta(\Gamma)$ .

Thus  $x = \sum_{u \in N(v)} \alpha_u v^{uv}$  (in the notation of Section 2.1), for some non-zero  $\alpha_u \in \mathbb{F}_p$ . If  $x \neq \alpha G_v$ then the  $\alpha_u$  are not constant over N(v), so for some  $\alpha \neq 0$ ,  $\alpha G_v - x$  has weight less than  $\delta(\Gamma)$  which contradicts (1). Thus x is a scalar multiple of the row  $G_v$ .

In Result 2 we gave sufficient conditions for a k-regular graph to satisfy  $\lambda(\Gamma) = k$ , and which then imply that  $C_2(G)$  has minimum weight k. Below we show that, in general, these conditions do not imply  $\lambda_{bip}(\Gamma) = k$ , hence they do not imply that  $C_p(G)$  has minimum weight k. However, we show that some of these conditions can be strengthened to imply  $\lambda_{bip}(\Gamma) = k$ .

Define  $b(\Gamma)$  to be the minimum cardinality of a set  $S \subseteq E$  such that  $\Gamma - S$  is bipartite. We note that  $|E| - b(\Gamma)$  is the maximum number of edges of a bipartite subgraph of  $\Gamma$ , a parameter for which several lower bounds are known. Unfortunately no lower bounds on  $b(\Gamma)$  seem to be known.

**Proposition 1** Let  $\Gamma = (V, E)$  be a connected graph that is not bipartite. Then

 $\lambda_{bip}(\Gamma) \ge \min\{\lambda(\Gamma), b(\Gamma)\}.$ 

- 1. If  $\Gamma$  is k-regular,  $b(\Gamma) \ge k$  and  $\lambda(\Gamma) = k$ , then  $\lambda_{bip}(\Gamma) = k$ .
- 2. If  $\Gamma$  is k-regular and super- $\lambda$ , and if  $b(\Gamma) > k$  then  $\Gamma$  is super- $\lambda_{bip}$ .

**Proof:** (1). Let  $S \subseteq E$  be a set of edges of cardinality  $\lambda_{bip}(\Gamma)$  such that  $\Gamma - S$  has a bipartite component. Then either  $\Gamma - S$  is connected, in which case  $\Gamma - S$  is bipartite and so  $|S| \ge b(\Gamma)$ , or  $\Gamma - S$  is disconnected, in which case  $|S| \ge \lambda(\Gamma)$ .

If  $\Gamma$  is k-regular and  $b(\Gamma) \geq k = \lambda(\Gamma)$ , then it follows from the above that  $\lambda_{bip}(\Gamma) \geq k$ . On the other hand we have  $\lambda_{bip}(\Gamma) \leq k$  since if S is the set of edges incident with a vertex v, then  $\Gamma - S$  has a component that is (trivially) bipartite, viz. the component consisting of vertex v.

(2) Now let  $\Gamma$  be super- $\lambda$  and  $b(\Gamma) > k$ . Let S be a bipartition set of cardinality k. Since  $\Gamma - S$  is not bipartite, it is disconnected. Hence S is an edge-cut of cardinality k, and thus, since  $\Gamma$  is super- $\lambda$ , S is the set of edges incident with some vertex. Hence  $\Gamma$  is super- $\lambda_{bip}$ .

**Proposition 2** Let  $\Gamma = (V, E)$  be a k-regular graph that is not bipartite with |V| = n and  $k \ge \frac{n+3}{2}$ . If  $n \ge 6$  then  $\Gamma$  is super- $\lambda_{bip}$ .

**Proof:** Since  $k \ge \frac{n+3}{2}$ , every two vertices have at least four common neighbours, so  $\Gamma$  is connected and furthermore contains 3-cycles, implying that  $\Gamma$  cannot be bipartite. By Result 2 (5),  $k \ge \frac{n+3}{2}$  implies that  $\Gamma$  is super- $\lambda$ . Since a bipartite graph of order n has at most  $\frac{n^2}{4}$  edges, we have

$$b(\Gamma) \ge |E| - \frac{n^2}{4} = \frac{k}{2}n - \frac{n^2}{4} = \frac{n}{2}(k - \frac{n}{2}).$$

If now  $k = \frac{n+3}{2}$ , then we get  $b(\Gamma) \ge \frac{3}{4}n \ge \frac{n+3}{2}$  where the first inequality is strict because n must be odd since k is an integer. If  $k \ge \frac{n+4}{2}$ , then we get  $b(\Gamma) \ge n > k$ . In all cases we get  $b(\Gamma) > k$ , and so Proposition 1(2) yields that  $\Gamma$  is super- $\lambda_{bip}$ .

**Proposition 3** Let  $\Gamma = (V, E)$ , where |V| = n, be a strongly regular graph that is not bipartite with parameters  $(n, k, \lambda, \mu)$ .

- 1. If  $\mu \geq 1$ ,  $\lambda \geq 1$ , and  $n \geq 6$  then  $\lambda_{bip}(\Gamma) = k$ . If  $n \geq 7$ ,  $\mu \geq 1$  and  $1 \leq \lambda \leq k-3$  then  $\Gamma$  is super- $\lambda_{bip}$ .
- 2. If  $\lambda = 0$ ,  $\mu \ge 1$  and  $n \ge 10$ , then  $\lambda_{bip}(\Gamma) = k$ . If n > 10 then  $\Gamma$  is super- $\lambda_{bip}$ .

## 5 CODES OVER $\mathbb{F}_P$ , P ODD

**Proof:** (1) We show that  $b(\Gamma) \ge k$ . Let  $S \subseteq E$  be a set of size  $b(\Gamma)$  such that  $\Gamma - S$  is bipartite.

Let t be the number of distinct triangles in  $\Gamma$ . Since each edge of  $\Gamma$  is on exactly  $\lambda$  triangles, and since  $\Gamma$  has  $\frac{1}{2}nk$  edges, we have

$$t = \frac{1}{3}|E|\lambda = \frac{1}{6}kn\lambda.$$

On the other hand, removing  $b(\Gamma)$  edges destroys at most  $\lambda b(\Gamma)$  triangles. Since  $\Gamma - S$  contains no triangles, we have

 $\lambda b(\Gamma) \ge t.$ 

From these two inequalities we get

$$\lambda b(\Gamma) \ge \frac{kn\lambda}{6} \ge k\lambda,$$

and so  $b(\Gamma) \geq k$ . Now  $\lambda(\Gamma) = k$  by Result 2 (3), hence  $\lambda_{bip}(\Gamma) = k$  by Proposition 1

The second statement of (1) follows from Proposition 1, since if  $|V| \ge 7$  the above inequalities yield  $b(\Gamma) > k$ , and by Result 2 (3a), since  $\lambda \le k - 3$  and  $\mu \ge 1$ ,  $\Gamma$  is super- $\lambda$ .

(2) Note first that  $k > \mu$  since otherwise  $\Gamma$  would be the complete bipartite graph on 2k vertices. Since  $n \ge 10$ , it follows that  $k \ge 3$  and thus  $\Gamma$  is super- $\lambda$  by Result 2 (3a). So, using Proposition 1, it suffices to show that

$$b(\Gamma) \ge \frac{n\kappa}{10}.$$

Fix a vertex v and let  $V_1 = N(v)$  and  $V_2 = V - (N(v) \cup \{v\})$ . Then  $|V_2| = n - k - 1 = \frac{k(k-1)}{\mu}$ , since it is well known that for strongly regular graphs  $(n - k - 1)\mu = k(k - \lambda - 1) = k(k - 1)$  (see [7, Proposition 2.6]).

Let  $q(V_2)$  be the number of edges of  $\Gamma$  on vertices in  $V_2$ . Since each vertex in  $V_2$  has  $\mu$  neighbours in  $V_1$ , it has  $k - \mu > 0$  neighbours in  $V_2$ . Hence

$$q(V_2) = \frac{1}{2}|V_2|(k-\mu) = \frac{k(k-1)(k-\mu)}{2\mu}$$

We now determine  $c_5(v)$ , the number of cycles of length 5 through v. Since  $\Gamma$  does not contain triangles, each 5-cycle through v contains exactly one edge that joins two vertices, u and w say, in  $V_2$ . Since uand v (and similarly w and v) share exactly  $\mu$  neighbours, there are  $\mu^2$  cycles  $C_5$  containing v and the edge uw. Hence

$$c_5(v) = \mu^2 q(V_2) = \frac{1}{2}\mu k(k-1)(k-\mu).$$

The total number of 5-cycles of the graph is therefore

$$c_5(\Gamma) = \frac{1}{5} \sum_{v \in V} c_5(v) = \frac{1}{10} (n\mu k(k-1)(k-\mu)).$$

We now determine  $c_5(uv)$ , the number of 5-cycles through a given edge vu of  $\Gamma$ . Each 5-cycle through uv contains a neighbour w of u in  $V_2$ , an edge ww' joining two vertices in  $V_2$ , and a path of length 2 joining w' and v. As above, u has k-1 neighbours  $w \in V_2$ . Each such w is adjacent to  $k - \mu$  other vertices in  $w' \in V_2$ , none of which is adjacent to u since  $\lambda = 0$ , and w' and v are joined by  $\mu$  paths of length 2. Hence we have

$$c_5(uv) = (k-1)(k-\mu)\mu.$$

Let S be a minimum set of edges such that  $\Gamma - S$  is bipartite. Then  $\Gamma - S$  does not contain a  $C_5$ . Since removing |S| vertices destroys at most  $|S|(k-1)(k-\mu)\mu$  cycles  $C_5$ , we have

$$|S|(k-1)(k-\mu)\mu \ge c_5(\Gamma) = \frac{1}{10}(n\mu k(k-1)(k-\mu)),$$

implying  $b(\Gamma) = |S| \ge \frac{1}{10}nk$ , as desired.

#### 5 CODES OVER $\mathbb{F}_P$ , P ODD

11

**Corollary 3** Let  $\Gamma = (V, E)$  be a connected k-regular graph that is not bipartite on |V| = n vertices, G an  $n \times \frac{nk}{2}$  incidence matrix for  $\Gamma$ , and p an odd prime. If

- 1.  $k \ge (n+3)/2$  and  $n \ge 6$ , or
- 2.  $\Gamma$  is strongly regular with parameters  $(n, k, \mu, \lambda)$ , where
  - (a)  $n \ge 7, \ \mu \ge 1, \ and \ 1 \le \lambda \le k-3, \ or$
  - (b)  $n \ge 11$ ,  $\mu \ge 1$ , and  $\lambda = 0$ ,

then the code  $C_p(G)$  has minimum weight k, and the minimum words are the non-zero scalar multiples of the rows of G.

**Example 2** The Hamming graph H(d,q), where  $d,q \ge 2$ , is the graph whose vertex set is the set of all words of length d over an alphabet with q elements. Two vertices are adjacent if their words differ in exactly one position. Clearly H(d,q) is k-regular, where k = d(q-1). Since Hamming graphs are known to be distance regular, it follows from Corollary 1 that their binary codes have minimum weight equal to k, and the only words of weight k are the rows of the incidence matrix. For p odd, the codes  $C_p(G)$  have the same property: for q = 2, H(d, 2) is bipartite, so Theorem 2 and Corollary 2 can be used. For  $q \ge 3$ , H(d,q) is the edge-disjoint union of  $dq^{d-1}$  complete graphs of order q (each of these complete graphs is obtained by fixing d-1 components of the words in H(d,q) and letting the remaining component vary over all elements in  $\{1, 2, \ldots, q\}$ ). This implies  $b(H(d,q)) \ge dq^{d-1} > k$  since any set of edges whose removal renders H(d,q) bipartite must contain at least one edge from each of the complete graphs. It follows by Proposition 1 that H(d,q) is super- $\lambda_{bip}$  for  $q \ge 3$ . By Theorem 3 the code  $C_p(G)$  has minimum weight k and the words of weight k are precisely the non-zero scalar multiples of the rows of G.

**Example 3** Some classes of strongly regular graphs that satisfy the hypothesis of Corollary 3 or Corollary 1 are lattice graphs  $L_2(m)$  for  $m \ge 3$ , triangular graphs T(m) for  $m \ge 5$ , Paley graphs P(q) for  $q \equiv 1 \pmod{4}$  and  $q \ge 5$  (see [17]), and symplectic graphs, along with their complements.

To see that the condition n > 10 in Proposition 3 and Corollary 3 is necessary, consider the Petersen graph  $\Gamma = (V, E)$  where  $V = \Omega^{\{2\}}$ ,  $\Omega = \{1, \ldots, 5\}$ , and  $a \sim b$  if  $a \cap b = \emptyset$ . It is a (10, 3, 0, 1) strongly regular graph and the *p*-ary codes for *p* odd have words of weight 3 (see [14]) other than the scalar multiples of the rows of an incidence matrix *G*. An example of such a word is constructed as follows: for  $\omega = \{1, 2, 3, 4\}$ , and  $r \in \omega^{\{2\}}$ , let  $\bar{r} = \omega - r$ , i.e. its complement. If  $r_i, \bar{r_i}$  for i = 1, 2, 3 denote the members of  $\omega^{\{2\}}$ , then it can be verified that,

$$w = v^{\{1,2\}\{3,4\}} + v^{\{1,3\}\{2,4\}} + v^{\{1,4\}\{2,3\}} = \sum_{i=1}^{3} (G_{r_i} + G_{\bar{r}_i}) - \frac{1}{2} \sum_{u \in \Omega^{\{2\}}} G_u \in C_p(G)$$

for  $p \neq 2$ , and is clearly not a row of G. If S = Supp(w), then  $\Gamma - S$  is bipartite, so  $\Gamma$  is not super- $\lambda_{bip}$ . The binary code has the required property, from Corollary 1.

In this section we showed that conditions 3a and 5a of Result 2 can be strengthened to guarantee that a graph is super- $\lambda_{bip}$ . We now briefly discuss conditions 1 and 2 in Corollary 1. While every connected k-regular vertex-transitive graph  $\Gamma$  satisfies  $\lambda(\Gamma) = k$ , it is not true that  $\lambda_{bip}(\Gamma) = k$  for every such graph. For example an odd cycle is 2-regular, but has  $\lambda_{bip}(\Gamma) = 1$ . Let  $\Gamma$  be the graph on 2n vertices  $u_0, u_1, \ldots, u_{n-1}, v_0, v_1, \ldots, v_{n-1}$ , with edges  $u_i u_{i+1}, v_i v_{i+1}, u_i v_i$  for  $i = 0, 1, \ldots, n-1$ , where n is odd and all indices are modulo n (so  $\Gamma$  is the cartesian product of an odd cycle and  $K_2$ ). It is easy to see that  $\Gamma$  is 3-regular, but  $\lambda_{bip}(\Gamma) = 2$  since  $\{u_0 u_1, v_0 v_1\}$  is a bipartition set of cardinality 2. It was conjectured by Erwin [private communication] that  $\lambda_{bip}(\Gamma) \geq k - 1$  for every k-regular non-bipartite vertex transitive graph. If true, this would imply that for each such graph the p-ary code of an incidence matrix has minimum distance k - 1 or k.

## 6 A GAP IN THE WEIGHT-ENUMERATOR

For a k-regular graph diam( $\Gamma$ )  $\leq 2$  implies  $\lambda(\Gamma) = k$ , but it is not true that it also implies  $\lambda_{bip}(\Gamma) = k$ . For example, if  $\Gamma$  is the graph obtained from the complete bipartite graph with partite sets  $\{u_1, u_2, \ldots, u_k\}$  and  $\{v_1, v_2, \ldots, v_k\}$  by deleting the edges  $u_1v_1, u_2v_2$  and adding  $u_1u_2, v_1v_2$ , then it is easy to see that for  $k \geq 3$   $\Gamma$  is k-regular, but since  $\{u_1u_2, v_1v_2\}$  is a bipartition set of cardinality 2, we have  $\lambda_{bip}(\Gamma) = 2 < k$ .

We do not know if conditions 4 and 6 of Result 2 imply that  $\lambda_{bip}(\Gamma) = k$ .

A consequence of the above theorems is that the minimum weight of the *p*-ary code generated by the incidence matrix of a connected graph  $\Gamma$  depends on  $\Gamma$  and on the parity of *p*, but not on the actual value of *p*. In fact from the previous work quoted concerning the codes from *G* for some classes of connected *k*-regular graphs, we have that  $\lambda_{bip}(\Gamma) = k$  for these classes.

# 6 A gap in the weight-enumerator

We now look for words of the next smallest weight in  $C_p(G)$ . For  $\Gamma = (V, E)$  a connected graph, a **restricted edge-cut** is a set  $S \subseteq E$  such that  $\Gamma - S$  is disconnected, and no component of  $\Gamma - S$  is an isolated vertex. It was shown in [10] that every graph  $\Gamma = (V, E)$  with  $|V| \ge 4$  which is not a star has a restricted edge-cut. The **restricted edge-connectivity**  $\lambda'(\Gamma)$  is the minimum number of edges in a restricted edge-cut, if such an edge-cut exists. Notice that if  $\Gamma = (V, E)$  is connected k-regular with  $k \ge 2$  and  $|V| \ge 4$ , then  $\lambda'(\Gamma) \le 2k - 2$ , since removing all the edges other than uv through adjacent vertices u and v will produce a restricted edge-cut of size 2(k - 1).

**Theorem 4** Let  $\Gamma = (V, E)$  be a connected k-regular graph with  $|V| \ge 4$ , G an incidence matrix for  $\Gamma$ ,  $\lambda(\Gamma) = k$  and  $\lambda'(\Gamma) > k$ . Let  $W_i$  be the number of codewords of weight i in  $C_2(G)$ . Then  $W_i = 0$  for  $k+1 \le i \le \lambda'(\Gamma) - 1$ , and  $W_{\lambda'(\Gamma)} \ne 0$  if  $\lambda'(\Gamma) > k + 1$ .

**Proof:** Let d be the minimum weight of  $C_2(G)$ . By Theorem 1 we have  $d = \lambda(\Gamma) = k$ . Let  $x \in C_2(G)$  be a word with wt(x) > d, and let  $\Gamma_x = (V, E - \operatorname{Supp}(x))$ . We show that  $wt(x) \ge \lambda'(\Gamma)$ .

As in the proof of Theorem 1 it follows that  $\Gamma_x$  is disconnected. Let  $\Gamma_i$  i = 1, 2, ..., t be the components of  $\Gamma_x$  and let  $V_i$  be their respective vertex sets. Now

$$\sum_{i=1}^{t} q(V_i, V - V_i) \le 2|\operatorname{Supp}(x)|,$$

since the sum on the left hand side counts each edge of  $\operatorname{Supp}(x)$  that joins vertices in distinct components of  $\Gamma_x$  exactly twice, while edges of  $\operatorname{Supp}(x)$  joining two vertices in the same component of  $\Gamma_x$  are not counted at all. On the other hand it follows from Equation (2) that  $q(V_i, V - V_i) \geq \lambda(\Gamma)$ . Hence

$$\sum_{i=1}^{t} q(V_i, V - V_i) \ge t\lambda(\Gamma).$$

The two inequalities yield that  $2|\operatorname{Supp}(x)| \ge t\lambda(\Gamma) = tk$ , and so  $|\operatorname{Supp}(x)| \ge \frac{1}{2}tk$ . If  $t \ge 4$  then we have  $|\operatorname{Supp}(x)| \ge 2k$ . Since  $\lambda'(\Gamma) \le 2k - 2$ , we have  $\operatorname{wt}(x) \ge \lambda'(\Gamma)$  in this case. Hence we can assume that  $2 \le t \le 3$ .

CASE 1: t = 2.

If one of the components of  $\Gamma_x$ , say  $\Gamma_1$ , consists of a single vertex v, then  $\operatorname{Supp}(x)$  contains all edges incident with v. Since all vertices u of  $\Gamma_2$  have the same value  $\mu_u$ , no edge of  $\operatorname{Supp}(x)$  joins two vertices of  $\Gamma_2$ . Hence  $\operatorname{Supp}(x)$  contains only the k edges of  $\Gamma$  incident with v, and so wt(x) = k, contradicting our assumption wt(x) > k. Hence we can assume that both components  $\Gamma_1$  and  $\Gamma_2$  of  $\Gamma_x = \Gamma - \operatorname{Supp}(x)$ contain at least two vertices. But then we have  $|\operatorname{Supp}(x)| \ge \lambda'(\Gamma)$ , by the definition of  $\lambda'(\Gamma)$ . CASE 2: t = 3.

## 6 A GAP IN THE WEIGHT-ENUMERATOR

If we have two components, say  $\Gamma_1$  and  $\Gamma_2$  of  $\Gamma_x$ , that are not joined by an edge in Supp(x), then  $E(V_1, V - V_1)$  and  $E(V_2, V - V_2)$  are disjoint, and each of the two sets has at least  $\lambda(\Gamma) = k$  edges by Equation (2). Hence

$$|\text{Supp}(x)| \ge q(V_1, V - V_1) + q(V_2, V - V_2) \ge 2k > \lambda'(\Gamma)$$

as desired. So we can assume that any two components of  $\Gamma_x$  are joined by an edge in  $\operatorname{Supp}(x)$ . Since  $|V| \ge 4$ , one of the components,  $\Gamma_1$  say, has at least two vertices. Consider the set  $\operatorname{Supp}(x)' = \operatorname{Supp}(x) \cap E(V_1, V_2 \cup V_3)$ . Clearly,  $\Gamma - \operatorname{Supp}(x)'$  has exactly two components, one containing the vertices in  $V_1$  and the other containing the vertices in  $V_2 \cup V_3$ . Since both components have at least two vertices, we have  $|\operatorname{Supp}(x)'| \ge \lambda'(\Gamma)$ , and so  $\operatorname{wt}(x) = |\operatorname{Supp}(x)| > |\operatorname{Supp}(x)'| \ge \lambda'(\Gamma)$ , as asserted.

Finally we need to construct a word of weight  $\lambda'(\Gamma)$  to show that  $W_{\lambda'(\Gamma)} \neq 0$ . Clearly if  $\lambda'(\Gamma) = 2k-2$ then we have a word of weight 2k - 2 from  $G_u - G_v$  where  $uv \in E$ . Suppose then that  $\lambda'(\Gamma) < 2k - 2$ and let S be a restricted edge-cut of minimum size  $\lambda'(\Gamma)$ . So  $\Gamma - S$  is disconnected and each component has at least three vertices, since otherwise |S| = 2k - 2. It follows that  $\Gamma - S$  has just two connected components, W and V - W, and all the edges in S are between W and V - W, and not within just one of the components. Define  $x = \sum_{u \in V} \mu_v G_v$ , where  $\mu_v = 1$  for  $v \in W$ , and  $\mu_v = 0$  for  $v \notin W$ . Thus as before we have  $\operatorname{Supp}(x) = S$ , of size  $\lambda'(\Gamma)$ . So  $W_{\lambda'(\Gamma)} \neq 0$ .

There is a similar argument for the bipartite case for p odd.

**Theorem 5** Let  $\Gamma = (V, E)$  be a connected bipartite k-regular graph with  $|V| \ge 4$ , G an incidence matrix for  $\Gamma$ ,  $\lambda(\Gamma) = k$  and  $\lambda'(\Gamma) > k$ . Let  $W_i$  be the number of codewords of weight i in  $C_p(G)$  where p is odd. Then  $W_i = 0$  for  $k + 1 \le i \le \lambda'(\Gamma) - 1$ , and  $W_{\lambda'(\Gamma)} \ne 0$  if  $\lambda'(\Gamma) > k + 1$ .

**Proof:** The proof is almost identical to the proof of Theorem 4, we therefore omit it.

For most of the sufficient conditions for  $\lambda(\Gamma) = k$  there are related conditions for  $\lambda'(\Gamma)$  to be equal to the minimum edge degree (which, for a k-regular graph, is always 2k - 2). Thus, from the literature, we have:

**Result 4** Let  $\Gamma = (V, E)$  be a connected graph.

Then  $\lambda'(\Gamma)$  is equal to the minimum edge degree if one of the following conditions hold:

- 1.  $\Gamma$  is vertex-transitive, and has odd order or does not contain triangles (Xu [52]);
- 2.  $\Gamma$  is edge-transitive and has  $|V| \ge 4$  (Li and Li [39]);
- 3. each pair u, v of nonadjacent vertices of  $\Gamma$  satisfies

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

(Hellwig and Volkmann [22]);

- 4. any two non-adjacent vertices of  $\Gamma$  have at least three neighbours in common (from 3. above);
- 5.  $\Gamma$  is bipartite and any two vertices in the same partite set have at least two neighbours in common (Yuan, Liu and Wang [53]);
- 6.  $\Gamma$  is strongly regular graph with parameters  $(n, k, \lambda, \mu)$  with either  $\lambda = 0$  and  $\mu \ge 2$ , or with  $\lambda \ge 1$ and  $\mu \ge 3$  (from 3. above);
- 7.  $k \geq \frac{1}{2}(n+1)$  (Wang and Li [50]), if  $\Gamma$  is bipartite then  $k > \lceil \frac{n+2}{4} \rceil$  is sufficient (Shang and Zhang [47]);
- 8.  $\Gamma$  has girth g, and diam $(\Gamma) \leq g 2$  (Balbuena, Garcia-Vázquez, Marcote, [2]).

We note that by a result of Hellwig and Volkmann [23] every graph for which  $\lambda'(\Gamma)$  equals the minimum edge-degree (which is 2k - 2 for k-regular graphs) is super- $\lambda$ . This, and Theorem 4, give the following:

**Corollary 4** Let  $\Gamma = (V, E)$  be a connected k-regular graph on |V| = n vertices, and G an incidence matrix for  $\Gamma$ . If  $\Gamma$  satisfies one of the conditions of Result 4, 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.

For the case of p odd and  $\Gamma$  connected k-regular bipartite, a similar set of results give the following applications:

**Corollary 5** Let  $\Gamma = (V, E)$  be a connected bipartite k-regular graph on |V| = n vertices, and G an incidence matrix for  $\Gamma$ . Then  $C_p(G)$  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.  $\Gamma$  is vertex-transitive;
- 2.  $\Gamma$  is edge-transitive and has  $|V| \ge 4$ ;
- 3. each pair u, v of nonadjacent vertices satisfies  $|N(u) \cap N(v)| \ge 2$ ;
- 4. any two non-adjacent vertices have at least two neighbours in common;
- 5.  $\Gamma$  is strongly regular graph with parameters  $(n, k, \lambda, \mu)$  with  $\lambda = 0$  and  $\mu \geq 2$ .

**Example 4** If  $\Gamma = K_{n,n}$ , the complete bipartite graph of degree  $n \geq 3$ , the codes from an incidence matrix G for this over any field  $\mathbb{F}_p$  were examined in [34]. These graphs satisfy the conditions of Theorems 1, 2, 4, 5, as was shown independently in [34].

# 7 Adjacency matrices of line graphs

Recall that if G is an incidence matrix for  $\Gamma$ , and M an adjacency matrix for the line graph  $L(\Gamma)$  then from Equation (1),  $G^T G = M + 2I_{|E|} = M$  over  $\mathbb{F}_2$ . Thus  $C_2(M) \subseteq C_2(G)$ , and if  $\Gamma$  is connected,  $C_2(M)$  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.

Thus information about  $C_2(G)$  leads to information about  $C_2(M)$ , and we can deduce a corollary to the previous theorems that will apply to some classes of line graphs.

**Corollary 6** Let  $\Gamma = (V, E)$  be a connected k-regular graph with  $|V| \ge 4$ , G an incidence matrix for  $\Gamma$ , and  $\lambda'(\Gamma) = 2k - 2$ . Let M be an adjacency matrix for the line graph  $L(\Gamma)$ , and  $E_2(G)$  the code spanned by differences of the rows of G over  $\mathbb{F}_2$ . Then  $C_2(M) = E_2(G)$  and

- 1.  $C_2(M) = [\frac{1}{2}|V|k, |V| 1, k]_2 = C_2(G)$  if |V| is odd;
- 2.  $C_2(M) = [\frac{1}{2}|V|k, |V| 2, 2k 2]_2 \subset C_2(G)$ , if |V| is even.

**Proof:** By the result from [23], quoted before Corollary 4, our assumption that  $\lambda'(\Gamma) = 2k - 2$  implies that  $\Gamma$  is super- $\lambda$  and thus  $\lambda(\Gamma) = k$ .

We make use of the well-known fact that the 2-rank of a symmetric matrix with 0-main-diagonal is always even (see for example [18, Proposition 2.1]), and of the fact that  $C_2(M)$  is either  $C_2(G)$  or of co-dimension 1 in it.

If |V| is odd, then  $C_2(M)$  has rank |V| - 1 and so  $C_2(M) = C_2(G)$ . If |V| is even, then  $C_2(M)$  has rank |V| - 2 and so is of co-dimension 1 in  $C_2(G)$ . Clearly  $C_2(M)$  does not contain any row of  $C_2(G)$ ,

#### 8 DUAL CODES

hence it does not contain any word of  $C_2(G)$  of weight k (by Theorem 1), and so, by Theorem 4, it contains only words of weight at least  $\lambda'(\Gamma) = 2k - 2$ , and thus this is the minimum weight.

For many classes of graphs that have been examined individually, it was found that not only are the words of minimum weight k in  $C_p(G)$  the scalar multiples of the rows of G for any p, but also the words of minimum weight 2k - 2 in the code  $E_p(G)$  are the scalar multiples of the differences of the rows of G from pairs of adjacent vertices. The complete graph  $K_n$  and the complete bipartite graph  $K_{n,n}$  are examples of this: see [33, 34].

For p odd,  $C_p(M)$  is not related in the same way to  $C_p(G)$ , and the code might not be particularly interesting or useful as regards classification, as the minimum weight might be small. We show below in Result 5 that an even cycle of length l in  $\Gamma$  gives rise to a word of weight l in  $C_p(M)$ , so the minimum weight of the code is at most the even girth: see [15, 35, 33, 34, 17] for some examples of this. In looking for words in  $C_p(G)^{\perp}$ , for all p, words in  $C_p(L(\Gamma))$  for p odd were found, as is described in Result 5 below. For xy an edge of  $\Gamma$ , write

$$\overline{xy} = \{xz \mid z \neq y\} \cup \{yz \mid z \neq x\} = N(xy),$$

for the neighbours N(xy) of xy in the line graph  $L(\Gamma)$ . Then, using notation as described in Section 2.1, [14, Lemma 1] is as follows:

**Result 5** ([14]) Let  $\Gamma$  be a graph,  $L(\Gamma)$  its line graph, and G an incidence matrix for  $\Gamma$ . If  $\pi = (x_1, \ldots, x_l)$  is a closed path in  $\Gamma$ , then

w(π) = Σ<sup>l-1</sup><sub>i=1</sub> v<sup>x<sub>i</sub>x<sub>i+1</sub></sup> + v<sup>x<sub>l</sub>x<sub>1</sub></sub> ∈ C<sub>2</sub>(G)<sup>⊥</sup>, and wt(w(π)) = l;
 if l = 2m and w(π) = Σ<sup>m</sup><sub>i=1</sub> v<sup>x<sub>2i-1</sub>x<sub>2i</sub> - Σ<sup>m-1</sup><sub>i=1</sub> v<sup>x<sub>2i</sub>x<sub>2i+1</sub> - v<sup>x<sub>2m</sub>x<sub>1</sub></sup>, then wt(w(π)) = l and w(π) ∈ C<sub>p</sub>(G)<sup>⊥</sup> for all primes p, and if p is odd,
</sup></sup></sup>

$$w(\pi) = -\frac{1}{2} \left[ \sum_{i=1}^{m} v^{\overline{x_{2i-1}x_{2i}}} - \sum_{i=1}^{m-1} v^{\overline{x_{2i}x_{2i+1}}} - v^{\overline{x_{2m}x_1}} \right] \in C_p(L(\Gamma)).$$

# 8 Dual codes

As noted in Result 5, words in the dual code  $C_p(G)^{\perp}$ , where G is an incidence matrix for a graph, can be constructed from cycles in the graph, so that the dual code usually has small minimum weight. We now make some general deductions using the graph properties about the existence of paths and words in  $C_p(G)^{\perp}$ . We note that when p = 2,  $C_2(G)^{\perp}$  is also known as the cycle space of  $\Gamma$ . Properties of this code were studied in [27, 28].

For an integer  $g \geq 3$  define  $\Gamma_q$  to be the graph obtained from two vertex-disjoint cycles

$$C = (u_0, u_1, \dots, u_{g-1})$$
 and  $C' = (v_0, v_1, \dots, v_{g-1})$ 

of length g, by identifying  $u_0$  and  $v_0$ . Thus  $\Gamma_g$  has 2g-1 vertices and 2g edges.

**Lemma 1** Let  $\Gamma = (V, E)$  be a connected graph of minimum degree at least 2 and of girth  $g \ge 3$ . Then at least one of the following is true:

- 1.  $\Gamma$  is a cycle of odd length;
- 2.  $\Gamma$  contains a cycle of even length;
- 3. |E| = 2g and  $\Gamma = \Gamma_g$ ;
- 4.  $|E| \ge 2g + 1$ .

## 8 DUAL CODES

**Proof:** The proof makes use of two well-known facts: in a graph in which every vertex has degree at least 2, no component is a tree (see for example [5, Theorem 3.3]) and so every component has a cycle; and an edge that is not a bridge is contained in a cycle (see for example [5, Theorem 2.14]), so in a graph with  $\lambda(\Gamma) \geq 2$ , every edge is contained in a cycle.

We may assume that  $\Gamma$  is not a cycle, and that it does not contain a cycle of even length.

CASE 1:  $\lambda(\Gamma) = 1$ , i.e.  $\Gamma$  has a bridge.

Let uv be a bridge of  $\Gamma$ . Let P be a longest path in  $\Gamma$  containing u and v such that all internal vertices of P have degree 2 in  $\Gamma$ . It is clear that u, v is such a path if  $\deg_{\Gamma}(u) \geq 3$  and  $\deg_{\Gamma}(v) \geq 3$ . If  $\deg_{\Gamma}(u) \geq 3$  and  $\deg_{\Gamma}(v) = 2$  then let  $v_1 \neq u$  be the other neighbour of v and consider the path  $(u, v, v_1)$ . If  $\deg_{\Gamma}(v_1) \geq 3$ , then  $(u, v, v_1)$  has the desired property. If  $\deg_{\Gamma} = 2$ , then consider the path  $(u, v, v_1, v_2)$ , and so on. Note that in the process of extending the path no vertex  $v_i$  can be repeated, so eventually we reach a vertex  $v_i$  of degree at least 3, for which the path  $(u, v, v_1, v_2, \ldots, v_i)$  has the desired property. If  $\deg_{\Gamma}(v) \geq 3$  and  $\deg_{\Gamma}(u) = 2$ , or if  $\deg_{\Gamma}(v) = \deg_{\Gamma}(u) = 2$ , then the same argument yields the desired path. Let  $u_1$  and  $v_1$  be the end vertices of P closest to u and v, respectively. Removing all internal vertices of P from  $\Gamma$  yields a graph  $\Gamma'$  with exactly two components which contain  $u_1$  and  $v_1$ , respectively. Since  $u_1$  and  $v_1$  have degree at least 3 in  $\Gamma$ , they have degree at least 2 in  $\Gamma'$ . The other vertices of  $\Gamma'$  have not lost a neighbour, so they still have degree at least 2. Hence each component of  $\Gamma'$  has a cycle, and thus contains at least g edges. In addition the graph  $\Gamma$  has  $|E(P)| \geq 1$  edges that are not in  $\Gamma'$  and so  $|E| \geq 2g + |E(P)| \geq 2g + 1$ , as desired.

#### CASE 2: $\lambda(\Gamma) \geq 2$ .

It follows from the remark at the beginning of the proof that  $\Gamma$  has a cycle C. Since  $\Gamma$  is not a cycle, there exists a vertex u of C which has a neighbour v not on C. Since  $\lambda(\Gamma) \geq 2$ , there is a cycle C' through uv.

We show that C and C' share no vertex other than u. Suppose not. Then C' contains a vertex  $w \neq u$  which is also on C. We can choose w such that C' contains a u - w path P' which does not contain any internal vertex that is in C. The path P and the two u - w paths in C form a set of vertex disjoint paths, such that the lengths of at least two of these paths have the same parity. These two paths together form a cycle of even length, contradicting the fact that  $\Gamma$  has no cycle of even length.

Since C and C' share only one vertex, viz. u, the two cycles are edge-disjoint, hence  $|E| \ge 2g$ . If |E| = 2g, then  $\Gamma$  does not contain any edge besides the edges on C and C', so  $\Gamma$  is isomorphic to  $\Gamma_g$ , which is only possible if  $\Delta(\Gamma) \ge 4$ . Hence, if  $\Delta(\Gamma) = 3$ , we have  $|E| \ge 2g + 1$ , as desired.

**Theorem 6** Let  $\Gamma$  be a connected graph of girth g and even girth  $g_e$ . Let G be an incidence matrix for  $\Gamma$ ,  $C = C_p(G)$  where p is any prime, and d the minimum weight of  $C^{\perp}$ .

- 1. If p = 2 or g is even then d = g.
- 2. If p is odd and g is odd then

$$d \ge \begin{cases} \min\{g_e, 2g\} & \text{if } \Delta(\Gamma) \ge 4, \\ \min\{g_e, 2g+1\} & \text{if } \Delta(\Gamma) \le 3, \end{cases}$$

**Proof:** We first show that  $d \ge g$  for all p. Let x be a word of weight d in  $C^{\perp}$ . Since  $Gx^t = 0$ , we have  $0 = G_v x^t = \sum_{e \in \operatorname{Supp}(x): v \in e} x_e$  for each vertex v of  $\Gamma$ . Hence each vertex v that is incident with an edge in  $\operatorname{Supp}(x)$  is incident with at least two edges in  $\operatorname{Supp}(x)$ . In other words, the subgraph  $\Gamma[\operatorname{Supp}(x)]$  of  $\Gamma$  induced by  $\operatorname{Supp}(x)$  has minimum degree at least 2. Hence  $\Gamma[\operatorname{Supp}(x)]$  contains a cycle, which implies that  $\Gamma[\operatorname{Supp}(x)]$  has at least g edges. Therefore,  $|\operatorname{Supp}(x)| \ge g$ , and so  $d \ge g$ .

Now let p and g be odd. As above, the graph  $\Gamma[\operatorname{Supp}(x)]$  has minimum degree at least 2. If  $\Gamma[\operatorname{Supp}(x)]$  contains an even cycle then we have  $\operatorname{wt}(x) = |\operatorname{Supp}(x)| \ge g_e(G)$  and we are done, so we may assume that  $\Gamma[\operatorname{Supp}(x)]$  does not contain an even cycle. Furthermore,  $\Gamma[\operatorname{Supp}(x)]$  is not an odd cycle. To see this suppose to the contrary that  $\Gamma[\operatorname{Supp}(x)]$  is an odd cycle, say,  $(v_1, v_2, \ldots, v_k)$ . Let

#### 9 PERMUTATION DECODING

 $a = x_{v_1v_2}$ , Then, since  $G_{v_2}x^t = 0$ , we have  $x_{v_2v_3} = -a$ . Since  $G_{v_3}x^t = 0$ , we get that  $x_{v_3v_4} = a$ and so on. Continuing in this fashion we conclude that  $x_{v_{k-1}v_k} = a$ . Hence  $G_{v_1}x^t = 2a$ . Since p is odd, this implies  $x_{v_1v_2} = a = 0$ , contradicting the fact that  $v_1v_2$  is in the support of x. Therefore,  $\Gamma[\operatorname{Supp}(x)]$  is not an odd cycle. By Lemma 1 the graph  $\Gamma[\operatorname{Supp}(x)]$  has at least 2g edges. Hence  $\operatorname{wt}(x) = |\operatorname{Supp}(x)| \ge \min\{2g, g_e\}$ , as desired. If  $\Delta(G) = 3$ , then  $\Gamma[\operatorname{Supp}(x)]$  cannot have a vertex of degree 4, so  $\Gamma[\operatorname{Supp}(x)]$  is not isomorphic to  $\Gamma_g$ , and thus  $\Gamma[\operatorname{Supp}(x)]$  has at least 2g + 1 edges, i.e.,  $\operatorname{wt}(x) \ge 2g + 1$ .

It follows from Result 5 in Section 7 that  $d \leq g$  if p = 2 or g is even. For completeness we give a short graph-theoretic proof of these facts. Suppose p = 2. Let E' be the set of edges of a cycle of length g in  $\Gamma$ , and let x be the characteristic vector of E', i.e.,  $x_e = 1$  if  $e \in E'$  and 0 otherwise. Then wt(x) = g and it follows that  $G_v x^t = 0$  for every vertex on the cycle. Since also  $G_v x^t = 0$  for each vertex not on the cycle, we conclude that  $Gx^t = 0$ , and so  $x \in C^{\perp}$ . Hence  $d \leq \operatorname{wt}(x) = g$ , as required.

Now suppose g is even. Let  $C = v_0, v_1, \ldots, v_{g-1}, v_0$  be a shortest cycle of  $\Gamma$ . Let  $e_i$  be the edge  $v_i v_{i+1}$ , for  $i = 0, 1, \ldots, g-1$ , where the indices are taken modulo g. Define  $x_{e_i} = (-1)^i$  for the edges  $e_i \in C$ , and  $x_e = 0$  if  $e \in E$ ,  $e \notin C$ . It is easy to see that x has weight g, and that  $Gx^t = 0$ , so  $x \in C^{\perp}$ . Hence  $d \leq \operatorname{wt}(x) = g$ , as asserted.

**Corollary 7** Let  $\Gamma$  be a connected graph of girth g, where g is odd, and even girth  $g_e$ , and let every vertex of  $\Gamma$  be on a cycle of length g. Let G be an incidence matrix for  $\Gamma$ ,  $C = C_p(G)$  where p is odd, and d the minimum weight of  $C^{\perp}$ .

- 1. If  $\Gamma$  is 3-regular then  $d = \min\{g_e, 2g+1\}$ .
- 2. If  $\Gamma$  is k-regular for  $k \ge 4$ , then  $\min\{g_e, 2g\} \le d \le \min\{g_e, 2g+1\}$ .

**Proof:** From Result 5,  $C^{\perp}$  has words of weight  $g_e$ . So if  $g_e \leq 2g$ , using Theorem 6, we have  $d = g_e$  and a cycle of length  $g_e$  will provide a word of this weight, as in Result 5. Otherwise  $g_e > 2g$ , but since it is even we have  $g_e > 2g + 1$ . We construct a word of weight 2g + 1.

Since we take  $g_e > 2g + 1$ , it follows that  $\Gamma$  contains no even cycle of length  $\leq 2g$ . Choose a vertex v of  $\Gamma$ . Then v is on a cycle C of length g. Let u be a neighbour of v not on C. Then u is also on a cycle C' of length g. If C and C' share a vertex, then, arguing as in Case 2 of the proof of Lemma 1, it follows that  $\Gamma$  has an even cycle of length  $\leq 2g$ , contradicting our assumption. Hence we may assume that the cycles C and C' are vertex disjoint. Let  $C = v_0, v_1, \ldots, v_{g-1}, v_0$  and  $C' = u_0, u_1, \ldots, u_{g-1}, u_0$ , where  $u = u_0$  and  $v = v_0$ . Define the word x by

$$x_{e} = \begin{cases} (-1)^{i} & \text{if } e = u_{i}u_{i+1} \text{ or } e = v_{i}v_{i+1}, \\ -2 & \text{if } e = uv, \\ 0 & \text{otherwise.} \end{cases}$$

It is easy to verify that  $Gx^t = 0$ , so  $x \in C^{\perp}$ , and has weight 2g + 1, and the stated results follow.

We note that Corollary 7 applies, for example, to vertex-transitive graphs.

# 9 Permutation decoding

In [31, Lemma 7] the following was proved:

**Result 6** 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 G be an automorphism group of C, and n the maximum value of  $|\mathcal{O} \cap \mathcal{I}|/|\mathcal{O}|$ , over the G-orbits  $\mathcal{O}$ . If  $s = \min(\lceil \frac{1}{n} \rceil - 1, \lfloor \frac{d-1}{2} \rfloor)$ , then G is an s-PD-set for C.

This result holds for any information set. If the group G 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 [16]:

**Result 7** Let  $\Gamma = (V, E)$  be a regular graph of valency k with automorphism group A transitive on edges. Let M be an incidence matrix for  $\Gamma$ . If, for p a prime,  $C = C_p(M) = [|E|, |V| - \varepsilon, k]_p$ , where  $\varepsilon \in \{0, 1, \ldots, |V| - 1\}$ , then any transitive subgroup of A will serve as a PD-set for full error correction for C.

Thus Result 7 will hold for many of the classes covered by the theorems we have presented, since for many of these classes the automorphism group is transitive on edges. Smaller PD-sets, or *s*-PD sets can of course also be found, but in this case specific information sets need to be found, and this can be difficult. A method of decoding introduced by Kroll and Vincenti [37, 38] in which a number of information sets need to be found rather than a set of permutations, could be applicable.

# References

- 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] C. Balbuena, P. Garcia-Vázquez, and X. Marcote, Sufficient conditions for λ'-optimality in graphs with girth g, J. Graph Theory 52 (2006), 73–86.
- [3] D. Bauer, F. Boesch, C. Suffel, and R. Tindell, Connectivity extremal problems and the design of reliable probabilistic networks, The Theory and Applications of Graphs, Kalamazoo MI, Wiley, New York, 1981, pp. 45–54.
- [4] A. Björner and J. Karlander, The mod p rank of incidence matrices for connected uniform hypergraphs, European J. Combin. 14 (1993), 151–155.
- [5] J.A Bondy and U.S.R. Murty, *Graph theory with applications*, New York: American Elsevier Publishing Co., Inc., 1976.
- [6] A.E. Brouwer and W.H. Haemers, *Eigenvalues and perfect matchings*, Linear Algebra Appl. 395 (2005), 155–162.
- [7] 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.
- [8] G. Chartrand, A graph theoretic approach to a communications problem., SIAM J. Appl. Math. 14 (1966), 778–781.
- P. Dankelmann and L. Volkmann, New sufficient conditions for equality of minimum degree and edge-connectivity, Ars Combin. 40 (1995), 270–278.
- [10] A.H. Esfahanian and S.L. Hakimi, On computing a conditional edge-connectivity of a graph, Inform. Process. Lett. 27 (1988), 195–199.
- [11] J. Fabrega and M.A. Fiol, Maximally connected digraphs., J. Graph Theory 13 (1989), 657–668.
- [12] \_\_\_\_\_, Bipartite graphs and digraphs with maximum connectivity, Discrete Appl. Math. 69 (1996), 271–279.
- [13] M.A. Fiol, On super-edge-connected digraphs and bipartite digraphs, J. Graph Theory 16 (1992), 545–555.
- [14] W. Fish, J. D. Key, and E. Mwambene, *Codes from odd graphs*, (Submitted).
- [15] \_\_\_\_\_, Codes from the incidence matrices and line graphs of Hamming graphs, Discrete Math. **310** (2010), 1884–1897.

- [16] \_\_\_\_\_, Codes from the incidence matrices of graphs on 3-sets, Discrete Math. **311** (2011), 1823–1840.
- [17] Dina Ghinelli and Jennifer D. Key, Codes from incidence matrices and line graphs of Paley graphs, Adv. Math. Commun. 5 (2011), 93–108.
- [18] C. Godsil and G. Royle, Chromatic number and the 2-rank of a graph, J. Combin. Theory, Ser. B 81 (2001), 142–149.
- [19] Daniel M. Gordon, Minimal permutation sets for decoding the binary Golay codes, IEEE Trans. Inform. Theory 28 (1982), 541–543.
- [20] S. L. Hakimi and J. G. Bredeson, Graph theoretic error-correcting codes, IEEE Trans. Inform. Th. 14 (1968), 584–591.
- [21] S. L. Hakimi and H. Frank, Cut-set matrices and linear codes, IEEE Trans. Inform. Th. 11 (1965), 457–458.
- [22] A. Hellwig and L. Volkmann, Sufficient conditions for λ'-optimality in graphs of diameter 2, Discrete Math. 283 (2004), 113–120.
- [23] A. Hellwig and L. Volkmann, Sufficient conditions for graphs to be λ'-optimal, super-edge-connected and maximally edge-connected, J. Graph Theory 48 (2005), 228–246.
- [24] A. Hellwig and L. Volkmann, Maximally edge-connected and vertex-connected graphs and digraphs - a survey, Discrete Math. 308 (2008), no. 15, 3265–3296.
- [25] 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.
- [26] M. Imase, H. Nakada, C. Peyrat, and T. Soneoka, Sufficient conditions for maximally connected dense graphs, Discrete Math. 63 (1987), 53 – 66.
- [27] Dieter Jungnickel and Scott A. Vanstone, Graphical codes A tutorial, Bull. Inst. Combin. Appl. 18 (1996), 45–64.
- [28] \_\_\_\_\_, Graphical codes revisited, IEEE Trans. Inform. Theory 43 (1997), 136–146.
- [29] A.K. Kelmans, Asymptotic formulas for the probability of k-connectedness of random graphs, Theory Probab. Appl. 17 (1972), 243–254.
- [30] 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.
- [31] \_\_\_\_\_, Information sets and partial permutation decoding for codes from finite geometries, Finite Fields Appl. **12** (2006), 232–247.
- [32] J. D. Key, J. Moori, and B. G. Rodrigues, Permutation decoding for binary codes from triangular graphs, European J. Combin. 25 (2004), 113–123.
- [33] \_\_\_\_\_, Codes associated with triangular graphs, and permutation decoding, Int. J. Inform. and Coding Theory 1, No.3 (2010), 334–349.
- [34] J. D. Key and B. G. Rodrigues, Codes associated with lattice graphs, and permutation decoding, Discrete Appl. Math. 158 (2010), 1807–1815.
- [35] Jennifer D. Key, Washiela Fish, and Eric Mwambene, Codes from the incidence matrices and line graphs of Hamming graphs  $H^k(n,2)$  for  $k \ge 2$ , Adv. Math. Commun. 5 (2011), 373–394.

- [36] Hans-Joachim Kroll and Rita Vincenti, PD-sets related to the codes of some classical varieties, Discrete Math. 301 (2005), 89–105.
- [37] \_\_\_\_\_, Antiblocking systems and PD-sets, Discrete Math. 308 (2008), 401–407.
- [38] \_\_\_\_\_, Antiblocking decoding, Discrete Appl. Math. **158** (2010), 1461–1464.
- [39] Q.L. Li and Q. Li, Super edge connectivity properties of connected edge symmetric graphs, Networks 33 (1999), 157–159.
- [40] Xiaodong Liang and Jixiang Meng, Connectivity of connected bipartite graphs with two orbits, Computational Science, ICCS 2007, vol. 4489, Springer, 2007, Lecture Notes in Computer Science, pp. 334–337.
- [41] F. J. MacWilliams, Permutation decoding of systematic codes, Bell System Tech. J. 43 (1964), 485–505.
- [42] F. J. MacWilliams and N. J. A. Sloane, The theory of error-correcting codes, Amsterdam: North-Holland, 1983.
- [43] W. Mader, Minimale n-fach kantenzusammenängende Graphen, Math. Ann. 191 (1971), 21–28.
- [44] J. Plesník, Critical graphs of given diameter, Acta Fac. Rerum Natur Univ. Comenian. Math 30 (1975), 79–93.
- [45] J. Plesník and S. Znám, On equality of edge-connectivity and minimum degree of a graph, Arch. Math. (Brno) 25 (1989), 19–25.
- [46] J. Schönheim, On coverings, Pacific J. Math. 14 (1964), 1405–1411.
- [47] L. Shang and H.P. Zhang, Sufficient conditions for a graph to be  $\lambda'$ -optimal and super- $\lambda'$ , Networks 49 (2007), no. 3, 234–242.
- [48] R. Tindell, Edge-connectivity properties of symmetric graphs, Preprint, Stevens Institute of Technology, Hoboken, NJ, 1982.
- [49] L. Volkmann, Bemerkungen zum p-fachen zusammenhang von Graphen, An. Univ. Bucuresti Mat. 37 (1988), 75–79.
- [50] Y.Q. Wang and Q. Li, Super edge-connected properties of graphs with diameter 2, J. Shanghai Jiaotong Univ. 33 (1999), no. 6, 646–649.
- [51] Hassler Whitney, Congruent graphs and the connectivity of graphs, Amer. J. Math. 54 (1932), 154–168.
- [52] J.M. Xu, Restricted edge-connectivity of vertex-transitive graphs, Chinese J. Contemp. Math. 21 (2000), no. 4, 369–374.
- [53] Jun Yuan, Aixia Liu, and Shiying Wang, Sufficient conditions for bipartite graphs to be super-krestricted edge connected, Discrete Math. 309 (2009), 2886–2896.