

Codes from incidence matrices of graphs

J. D. Key

Joint work with P. Dankelmann and B. Rodrigues

keyj@clemsn.edu
www.math.clemson.edu/~keyj

3ICMCTA

11-15 September 2011

Incidence matrix of a graph

An **incidence matrix** for an undirected graph $\Gamma = (V, E)$ is a $|V| \times |E|$ matrix $G = [g_{x,e}]$ with

- rows labelled by the vertices $x \in V$ and
- columns by the edges $e \in E$,

where $g_{x,e} = 1$ if $x \in e$, $g_{x,e} = 0$ if $x \notin e$.

Row span of incidence matrix of a graph

For any prime p let $C_p(G)$ be the row span of G over \mathbb{F}_p .

It has been found that for many classes of connected graphs that have some regularity and symmetry, these codes have parameters

$$[|E|, |V| - \varepsilon_p, \delta(\Gamma)]_p$$

where

- $\varepsilon_2 = 1$, $\varepsilon_p = 0, 1$ for p odd;
- $\delta(\Gamma)$ is the minimum degree of Γ ;
- the words of minimum weight are precisely the non-zero scalar multiples of the rows of G of weight $\delta(\Gamma)$.

Gap in the weight enumerator

Furthermore, it was found that there is often a **gap** in the weight enumerator between k and $2(k - 1)$, the latter weight arising from the difference of two rows, i.e. there are no words of weight m where

$$k < m < 2(k - 1).$$

Comment on the gap in the weight enumerator

This gap occurs for the p -ary code of the **desarguesian** projective plane $PG_2(\mathbb{F}_q)$, where $q = p^t$; also for other designs from desarguesian geometries $PG_{n,k}(\mathbb{F}_q)$: see [Cho00, LSdV08a, LSdV08b]

But, not always true for **non-desarguesian** planes: e.g. there are planes of order 16 that have words in this gap: see [GdRK08].

This has also shown that there are affine planes of order 16 whose binary code has words of weight 16 that are not incidence vectors of lines.

Note:

For $\Gamma = (V, E)$, the row span $C_p(\Gamma)$ of a $|V| \times |V|$ adjacency matrix for Γ over \mathbb{F}_p gives linear code of length $|V|$ that may have properties that are of use in classifications or in applications.

However no uniform properties of these codes, other than possibly their dimension over different p , seems to emerge, even for attractive infinite classes of graphs.

Exception: for the line graph $L(\Gamma)$,

$$C_2(L(\Gamma)) \subseteq C_2(G)$$

where G is an incidence matrix for Γ .

The code $C_2(G)$ has been referred to in the literature as the **bond space** or the **cut space**. See for example, Hakimi and Bredeson [HB68, BH67] for binary codes.

Their interest in the codes was for the application of majority logic decoding.

The codes $C_2(G)^\perp$ were termed **graphical codes** by Jungnickel and Vanstone and studied for a number of coding properties in [JV96, JV97b, JV99b, JV95, JV99a, JV97a].

Graphs terminology

The **graphs**, $\Gamma = (V, E)$ with vertex set V , $N = |V|$, and edge set E , are undirected with no loops.

- If $x, y \in V$ and x and y are adjacent, $x \sim y$, and $[x, y]$ or xy is the edge they define.
- A graph is **regular** if all the vertices have the same valency k .
- An **adjacency matrix** $A = [a_{i,j}]$ of Γ is an $N \times N$ matrix with $a_{ij} = 1$ if vertices $v_i \sim v_j$, and $a_{ij} = 0$ otherwise.
- 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.

Terminology and definitions continued

- The **neighbourhood design** $\mathcal{D}(\Gamma)$ of a regular graph Γ is the $1-(N, k, k)$ symmetric design with points the vertices of Γ and blocks the sets of neighbours of a vertex, for each vertex, i.e. an **adjacency matrix** of Γ is an **incidence matrix** for \mathcal{D} .
- An **incidence matrix** of Γ is an $N \times |E|$ matrix B with $b_{i,j} = 1$ if the vertex labelled by i is on the edge labelled by j , and $b_{i,j} = 0$ otherwise.
- If Γ is regular with valency k , then $|E| = \frac{Nk}{2}$ and the $1-(\frac{Nk}{2}, k, 2)$ design with incidence matrix B is called the **incidence design** $\mathcal{G}(\Gamma)$ of Γ .
- The **line graph** $L(\Gamma)$ of $\Gamma = (V, E)$ is the graph with vertex set E and e and f in E are adjacent in $L(\Gamma)$ if e and f as edges of Γ share a vertex in V .

Terminology and definitions continued

- The **code $C_F(\mathcal{D})$ of the design** \mathcal{D} over a field F is the space spanned by the incidence vectors of the blocks over F .
- For $X \subseteq \mathcal{P}$, the **incidence vector** in $F^{\mathcal{P}}$ of X is v^X .
- The **code $C_F(\Gamma)$ or $C_p(\mathbf{A})$ of graph Γ** over \mathbb{F}_p is the row span of an adjacency matrix A over \mathbb{F}_p . So $C_p(\Gamma) = C_p(\mathcal{D}(\Gamma))$ if Γ is regular.
- If G is an **incidence matrix** for Γ , $C_p(G)$ denotes the row span of G over F_p . So $C_p(G) = C_p(\mathcal{G}(\Gamma))$ if Γ is regular.
- If G is an **incidence matrix** for $\Gamma = (V, E)$, L is an **adjacency matrix** for $L(\Gamma)$, then

$$(G^T)G = L + 2I_{|E|}$$

Some classes of graphs studied

Infinite classes of graphs studied and found, by combinatorial and coding theoretic methods, along with induction, to have the properties described for $C_p(G)$, G an incidence matrix, include:

1. Hamming graphs $H^k(n, m)$ [FKM10, FKM11]

For n, k, m integers, $1 \leq k < n$, the Hamming graph $H^k(n, m) = (V, E)$ where

- V is the set of m^n n -tuples of R^n , where R is a set of size m ;
- two n -tuples are adjacent if they differ in k coordinate positions.

They are the graphs from the Hamming association scheme.

In particular, the n -cube: $Q_n = H(n, 2) = H^1(n, 2)$ ($R = \mathbb{F}_2$).

2. Uniform subset graphs $\Gamma(n, k, m)$

A uniform subset graph $\Gamma(n, k, m) = (V, E)$ where $V = \Omega^{\{k\}}$, where $|\Omega| = n$, and adjacency defined by $a \sim b$ if $|a \cap b| = m$.

The symmetric group $S_n \subseteq \text{Aut}(\Gamma(n, k, m))$.

All classes studied satisfy the properties described, and include:

- the odd graphs $\Gamma(2k + 1, k, 0)$ [FKMa]
- triangular graphs $\Gamma(n, 2, 1)$ (strongly regular) and $\Gamma(n, 2, 0)$ [FKMc]
- $\Gamma(n, 3, m)$ for $m = 0, 1, 2$. [FKMb]

3. Complete multipartite graphs K_{n_1, n_2, \dots, n_k}

- K_n the complete graph[KMR10]
- $K_{n,n}$ the complete bipartite graph[KR10]
- $K_{n,m}$ for $n \neq m$
- K_{n_1, n_2, \dots, n_k} where $n_i = n$ for $i = 1, \dots, k$

Some classes of graphs studied, continued

4. Strongly regular graphs (n, k, λ, μ)

A graph $\Gamma = (V, E)$ is strongly regular with parameters (n, k, λ, μ) if

- $|V| = n$;
- Γ is regular with valency (degree) k ;
- for any $P, Q \in V$ such that $P \sim Q$,

$$|\{R \in V \mid R \sim P \& R \sim Q\}| = \lambda;$$

- for any $P, Q \in V$ such that $P \not\sim Q$,

$$|\{R \in V \mid R \sim P \& R \sim Q\}| = \mu.$$

Some classes of graphs studied, continued

- **Triangular graphs** $T(n) = L(K_n)$, $n \geq 4$,
 $((\binom{n}{2}), 2(n-2), n-2, 4)$ [KMR10]
- **Paley graphs** $P(q)$, vertex set \mathbb{F}_q where $q \equiv 1 \pmod{4}$ and $x \sim y$ if $x - y$ is a non-zero square, $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$ [GK11]
- **Lattice graphs** $L_2(n) = L(K_{n,n})$, the line graph of the complete bipartite graph, $(n^2, 2(n-1), n-2, 2)$ [KS08]
- **Symplectic graphs** [KMR],
 $\Gamma_{2m}(q)$ with parameters $(\frac{q^{2m}-1}{q-1}, \frac{q^{2m-1}-1}{q-1} - 1, \frac{q^{2m-2}-1}{q-1} - 2, \frac{q^{2m-2}-1}{q-1})$
and complement
 $\Gamma_{2m}^c(q)$ with parameters $(\frac{q^{2m}-1}{q-1}, q^{2m-1}, q^{2m-2}(q-1), q^{2m-2}(q-1))$
where $m \geq 2$, q a prime power.

Result

$\Gamma = (V, E)$ is a connected graph, G an incidence matrix, then

- 1 $\dim(C_2(G)) = |V| - 1$.
- 2 If Γ has a closed path of **odd** length ≥ 3 , then $\dim(C_p(G)) = |V|$ for p odd.
- 3 If Γ is regular, and \mathcal{G} the incidence design, $\text{Aut}(\Gamma) = \text{Aut}(\mathcal{G})$.

Incidence vectors and notation

For $\Gamma = (V, E)$ a graph,

- for $X \subseteq E$, the **incidence vector** in F^E of X is v^X ;
- for $u \in V$, $N(u)$ the neighbours of u ,

$$\bar{u} = \{uv \mid v \in N(u)\}$$

where uv or $[u, v]$ denotes an edge;

- for $u \in V$,

$$v^{\bar{u}} = \sum_{e \in \bar{u}} v^e = \sum_{v \in N(u)} v^{uv},$$

i.e. the row G_u of the incidence matrix G corresponding to u .

Result

Let Γ be a graph, $L(\Gamma)$ its line graph, and G an incidence matrix for Γ .
If $\pi = (x_1, \dots, x_l)$ is a closed path in Γ , then

- 1 $w(\pi) = \sum_{i=1}^{l-1} v^{x_i x_{i+1}} + v^{x_l x_1} \in C_2(G)^\perp$;
- 2 if $l = 2m$ and

$$w(\pi) = \sum_{i=1}^m v^{x_{2i-1} x_{2i}} - \sum_{i=1}^{m-1} v^{x_{2i} x_{2i+1}} - v^{x_{2m} x_1},$$

then $w(\pi) \in C_p(G)^\perp$ for all primes p , and if p is odd,
 $w(\pi) \in C_p(L(\Gamma))$.

Methods of attack for specific classes

The graphs considered all had large automorphism groups, mostly transitive on vertices and on edges.

Method 1: Combinatorial

All the graphs has short paths of even length t , hence producing words of this weight in the dual code C^\perp .

Form a $1-(|E|, t, r)$ design of the supports of these words, compute r (the replication number) for this design, and then count incidence with the support of any word of C .

This frequently was good enough to get the minimum weight, and further the minimum words.

Method 2: Induction, linear algebra and coding theory

This works when taking a class for $n \in \mathbb{N}$, by embedding an incidence matrix for $n - 1$ in that for n , and using induction.

General method using edge-cuts in graphs

(Joint work with Peter Dankelmann and Bernardo Rodrigues of UKZN)

More general method showing that these properties hold for many classes of well-behaved connected graphs: see [DKR]

If $\Gamma = (V, E)$ is connected and $S \subset E$, let $\Gamma - S = (V, E - S)$.

If $\Gamma - S$ is disconnected then S is called an **edge-cut**.

The **edge-connectivity** $\lambda(\Gamma)$ of Γ is the minimum size of an edge-cut.

So $\lambda(\Gamma) \leq \delta(\Gamma)$ (the minimum degree of Γ) since removing all the edges containing a vertex disconnects the graph.

If $\lambda(\Gamma) = \delta(\Gamma)$ and the only edge sets of cardinality $\lambda(\Gamma)$ whose removal disconnects Γ are the sets of edges incident with a vertex of degree $\delta(\Gamma)$, then Γ is called **super- λ** .

Theorem for the binary case:

Theorem

Let $\Gamma = (V, E)$ be a connected graph, G a $|V| \times |E|$ incidence matrix for Γ . Then

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

Proof: $C = C_2(G)$ has dimension $|V| - 1$ by Result 1.

Let d be the minimum weight of C .

(1). Let

$$x = \sum_{u \in V} \mu_u v^{\bar{u}} \in C$$

where $\mu_v \in \mathbb{F}_2$, and $\text{wt}(x) = d$. Then

$$x(uv) = \mu_u + \mu_v.$$

So, for every edge $uv \in E$

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

Let $\Gamma_x = (V, E - \text{Supp}(x))$.

If $u \sim v$ in Γ_x , then $\mu_u + \mu_v = 0$, and so $\mu_u = \mu_v$.

So for any two vertices u and v in the same component of Γ_x we have $\mu_u = \mu_v$.

Thus Γ_x is disconnected since otherwise, if Γ_x were connected, all μ_v would have the same value, μ say, and so $x = \mu \sum_u v^{\bar{u}} = \mu 0$, a contradiction.

Hence $\text{Supp}(x)$ is an edge-cut of Γ , and so $|\text{Supp}(x)| \geq \lambda(\Gamma)$ and $d = \text{wt}(x) \geq \lambda(\Gamma)$.

Proof continued

Now construct a word of weight $\lambda(\Gamma)$.

Let $S \subseteq E$ be a minimal edge-cut of Γ .

Then $\Gamma - S = (V, E - S)$ 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 $x = \sum_{u \in V} \mu_u v^{\bar{u}}$, where $\mu_u = 1$ if $u \in W$, and $\mu_u = 0$ if $u \in V - W$. For an edge $uv \in E$ we have

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

Hence $\text{wt}(x) = |\text{Supp}(x)| = |S| = \lambda(\Gamma)$.

So the minimum weight of C is $\lambda(\Gamma)$.

(2). Now suppose Γ is super- λ .

The minimum weight of C is $\lambda(\Gamma) = \delta(\Gamma)$.

Let $x = \sum_{u \in V} \mu_u v^{\bar{u}}$ be a word in C of weight $\delta(\Gamma)$.

Then $\Gamma_x = (V, E - \text{Supp}(x))$ is disconnected, and $\text{Supp}(x)$ is an edge-cut of cardinality $\lambda(\Gamma)$.

Since Γ is super- λ , it follows that Γ_x has exactly two components, one consisting of a single vertex u of degree $\delta(\Gamma)$, and the other component containing the vertices in $V - \{u\}$.

Thus $\text{Supp}(x) = \{uv \mid v \in N(u)\}$ so $x = v^{\bar{u}}$, which proves (2). ■

Examples of super- λ

Let $\Gamma = (V, E)$ be a connected k -regular graph.

Then Γ is super- λ if one of the following conditions is satisfied, so $C_2(G)$ has minimum weight k and the words of weight k are the rows of G :

- 1a Γ is vertex-transitive and has no complete subgraph of order k (Tindell [Tin]);
- 2a. Γ has diameter at most 2, and in addition Γ has no complete subgraph of order k (Fiol [Fio92]);
- 3a. Γ is strongly regular with parameters (n, k, λ, μ) , and $\mu \geq 1$, $\lambda \leq k - 3$ (follows from 2. above);
- 4a. Γ is distance-regular and $k > 2$ (Brouwer and Haemers [BH05]);
- 5a. $k \geq \frac{|V|+1}{2}$ (Kelmans [Kel72]);
- 6a. Γ has girth g , and $\text{diam}(\Gamma) \leq g - 1$ if g is odd, or $\text{diam}(\Gamma) \leq g - 2$ if g is even. (Fabrega, Fiol [FF89]).

Argument for p odd

The same argument **does not** follow through for p odd (although the result is surely true for most nice classes of graphs).

If $w \in C_p(G)$, p odd, $w \neq 0$, and

$$w = \sum_{x \in V} \mu_x v^{\bar{x}},$$

then $\text{Supp}(w)$ is an edge-cut, but $\Gamma - \text{Supp}(w)$ might not be disconnected.

A modified argument yields a similar but somewhat more restrictive result.

Note: The same argument as in the binary case **does** follow for odd p for Γ connected and **bipartite**.

Counter example for p odd: Petersen graph \mathcal{O}_2

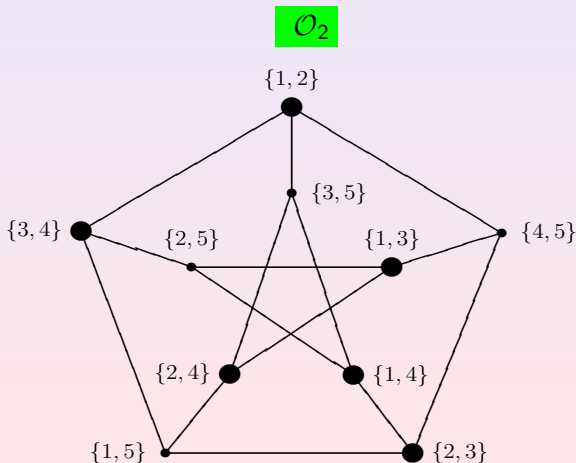
The **Petersen graph**, i.e. the smallest odd graph $\mathcal{O}_2 = (V, E)$, where $V = \Omega^{\{2\}}$, and $\Omega = \{1, 2, 3, 4, 5\}$ (strongly regular $(10, 3, 0, 1)$), yields a counterexample: (see [FKMa]).

Here \bar{x} denotes the support of the row of an incidence matrix indexed by $x \in V$. So, for example

$$\overline{\{1, 2\}} = \{\{1, 2\}\{3, 4\}, \{1, 2\}\{3, 5\}, \{1, 2\}\{4, 5\}\}.$$

Counter example: Petersen graph \mathcal{O}_2

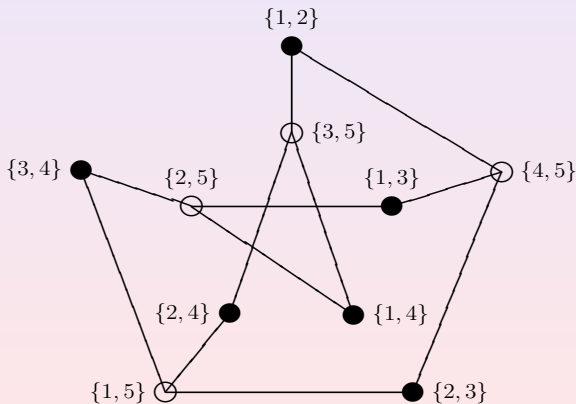
Let $w = v^{\overline{\{1,2\}}} + v^{\overline{\{3,4\}}} + v^{\overline{\{1,3\}}} + v^{\overline{\{2,4\}}} + v^{\overline{\{1,4\}}} + v^{\overline{\{2,3\}}} - \mathcal{J}_{15} = v^{\{1,2\}\{3,4\}} + v^{\{1,3\}\{2,4\}} + v^{\{1,4\}\{2,3\}} \in C_p(G)$ for p odd, since $\sum_{x \in V} v^{\bar{x}} = 2\mathcal{J}_{15} \in C_p(G)$ and is not 0 for p odd. w is not a row of G .



$\mathcal{O}_2 - \text{Supp}(w)$

So $\text{Supp}(w) = \{\{1, 2\}\{3, 4\}, \{1, 3\}\{2, 4\}, \{1, 4\}\{2, 3\}\}$, $\mathcal{O}_2 - \text{Supp}(w)$ is bipartite (connected) and $\text{Supp}(w)$ is not an edge-cut.

$\mathcal{O}_2 - \text{Supp}(w)$



For bipartite connected graphs the argument is similar for p odd to that for general connected graphs for $p = 2$:

Theorem

Let $\Gamma = (V, E)$ be a connected bipartite graph, G a $|V| \times |E|$ incidence matrix for Γ , and p any prime. Then

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

General theorem for p odd

For p odd we have:

Theorem

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 Γ , and p an odd prime. If

- ① $k \geq (n + 3)/2$ and $n \geq 6$, or
- ② Γ is strongly regular with parameters (n, k, μ, λ) , where
 - ① $n \geq 7$, $\mu \geq 1$, and $1 \leq \lambda \leq k - 3$, or
 - ② $n \geq 11$, $\mu \geq 1$, 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 .

Restricted edge-connectivity $\lambda'(\Gamma)$

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 [EH88] that every graph with $|V| \geq 4$ 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.

If Γ is k -regular with $k \geq 2$ and $|V| \geq 4$, then

$$\lambda'(\Gamma) \leq 2k - 2.$$

(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

Let $\Gamma = (V, E)$ be a connected k -regular graph with $|V| \geq 4$,
 G an incidence matrix for Γ ,
 $\lambda(\Gamma) = k$ and $\lambda'(\Gamma) > k$.

Let W_i be the number of codewords of weight i in $C_2(G)$. Then

- $W_i = 0$ for $k + 1 \leq i \leq \lambda'(\Gamma) - 1$,
- and $W_{\lambda'(\Gamma)} \neq 0$ if $\lambda'(\Gamma) > k + 1$.

Corollary

Let $\Gamma = (V, E)$ be a connected k -regular graph and G an incidence matrix for Γ . If Γ satisfies one of the conditions

- 1 Γ is vertex-transitive, and has odd order or does not contain triangles (Xu [Xu00]);
- 2 Γ is edge-transitive and has $|V| \geq 4$ (Li and Li [LL99]);
- 3 any two non-adjacent vertices of Γ have at least three neighbours in common;
- 4 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);

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 $k < \ell < 2k - 2$.

Codes from adjacency matrices of line graphs

$\Gamma = (V, E)$, M an $|E| \times |E|$ adjacency matrix for the line graph $L(\Gamma)$.
The rows of M are labelled by the edges $[P, Q] \in E$, which has neighbours:

$$N([P, Q]) = \overline{[P, Q]} = \{[P, R] \mid R \neq Q\} \cup \{[R, Q] \mid R \neq P\}.$$

Recall from Result 2:

If π is a closed path in Γ of even length t , p an **odd** prime, then $C_p(M)$ has words of weight t .

Binary codes of line graphs

So codes of adjacency matrices of line graphs (of graphs with closed paths of small even length t) over \mathbb{F}_p for p odd have minimum weight at most t , and are not of much interest if t is small, as it is for most interesting classes.

Recall:

if G is an incidence matrix for Γ , M an adjacency matrix for $L(\Gamma)$ then

$$G^T G = M + 2I_e.$$

So

$$C_2(M) \subseteq C_2(G),$$

spanned by the differences of pairs of rows of G .

Result

Let $\Gamma = (V, E)$ be a connected graph, G a $|V| \times |E|$ incidence matrix for Γ , and M an adjacency matrix for $L(\Gamma)$. Let $E(G)$ denote the binary code spanned by the differences of all pairs of rows of G . Then

- 1 $C_2(M) = E(G)$;
- 2 $C_2(M) = C_2(G)$ if and only if $|V|$ is odd; if V is even, $[C_2(G), C_2(M)] = 1$.

To prove this, 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 [GR01, Proposition 2.1]), and of the fact that $E(G)$ is either $C_2(G)$ or of co-dimension 1 in it.

Binary codes of line graphs

For classes of graphs examined here previously and from results using edge-cuts, it has now been found that the minimum weight of $C_2(M)$ is

- k if $C_2(M) = C_2(G)$;
- $2k - 2$ if not, i.e. $[C_2(G) : C_2(M)] = 1$.

There are no words of weight between k and $2k - 2$ in $C_2(G)$.

Permutation decoding

Permutation decoding, from MacWilliams [Mac64], involves finding a set of automorphisms of the code, called a PD-set.

See MacWilliams and Sloane [MS83, Chapter 16, p. 513] and Huffman [Huf98, Section 8].

Definition

Let C be a t -error-correcting code with information set \mathcal{I} and check set \mathcal{C} .

A **PD-set** for C is a set $S \subseteq \text{Aut}(C)$ such that:

every t -set of coordinate positions is moved by at least one member of S into the check positions \mathcal{C} .

For $s \leq t$ an **s -PD-set** is a set $S \subseteq \text{Aut}(C)$ such that:

every s -set of coordinate positions is moved by at least one member of S into \mathcal{C} .

In [KMM06, Lemma 7] the following was proved:

Result

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 .

Permutation decoding







This 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:








Result ([FKMb])








Let $\Gamma = (V, E)$ be a regular k -graph with $A = \text{Aut}(\Gamma)$ transitive on edges, and M be an incidence matrix for Γ .








If $C = C_p(M) = [|E|, |V| - \varepsilon, k]_p$, where $\varepsilon \in \{0, 1, \dots, |V| - 1\}$, then any transitive subgroup of A will serve as a PD-set for full error correction for C .







References

-  J. G. Bredeson and S. L. Hakimi, *Decoding of graph theoretic codes*, IEEE Trans. Inform. Th. **13** (1967), 348–3491.
-  A.E. Brouwer and W.H. Haemers, *Eigenvalues and perfect matchings*, Linear Algebra Appl. **395** (2005), 155–162.
-  K. Chouinard, *Weight distributions of codes from planes*, Ph.D. thesis, University of Virginia, 2000.
-  P. Dankelmann, J. D. Key, and B. Rodrigues, *Codes from incidence matrices of graphs*, (Submitted).
-  A.H. Esfahanian and S.L. Hakimi, *On computing a conditional edge-connectivity of a graph*, Inform. Process. Lett. **27** (1988), 195–199.
-  J. Fabrega and M.A. Fiol, *Maximally connected digraphs.*, J. Graph Theory **13** (1989), 657–668.

-  M.A. Fiol, *On super-edge-connected digraphs and bipartite digraphs*, J. Graph Theory **16** (1992), 545–555.
-  W. Fish, J. D. Key, and E. Mwambene, *Codes from odd graphs*, (Submitted).
-  _____, *Codes from the incidence matrices of graphs on 3-sets*, *Discrete Math.* (To appear).
-  W. Fish, K. Kumwenda, and E. Mwambene, *Codes and designs from triangular graphs and their line graphs*, (Submitted).
-  W. Fish, J. D. Key, and E. Mwambene, *Codes from the incidence matrices and line graphs of Hamming graphs*, *Discrete Math.* **310** (2010), 1884–1897.
-  _____, *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.
-  Dina Ghinelli, Marialuisa J. de Resmini, and Jennifer D. Key, *Minimum words of codes from affine planes*, *J. Geom.* **91** (2008), 43–51.

-  Dina Ghinelli and Jennifer D. Key, *Codes from incidence matrices and line graphs of Paley graphs*, Adv. Math. Commun. **5** (2011), 93–108.
-  C. Godsil and G. Royle, *Chromatic number and the 2-rank of a graph*, J. Combin. Theory, Ser. B **81** (2001), 142–149.
-  S. L. Hakimi and J. G. Bredeson, *Graph theoretic error-correcting codes*, IEEE Trans. Inform. Th. **14** (1968), 584–591.
-  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.
-  Dieter Jungnickel and Scott A. Vanstone, *An application of coding theory to a problem in graphical enumeration*, Arch. Math. **65** (1995), 461–464.
-  _____, *Graphical codes – A tutorial*, Bull. Inst. Combin. Appl. **18** (1996), 45–64.
-  _____, *An application of difference sets to a problem concerning graphical codes*, J. Statist. Plann. Inference **62** (1997), 43–64.

-  _____, *Graphical codes revisited*, IEEE Trans. Inform. Theory **43** (1997), 136–146.
-  _____, *q-ary graphical codes*, Discrete Math. **208/209** (1999), 375–386.
-  _____, *Ternary graphical codes*, J. Combin. Math and Combin. Comput. **29** (1999), 17–31.
-  A.K. Kelmans, *Asymptotic formulas for the probability of k-connectedness of random graphs*, Theory Probab. Appl. **17** (1972), 243–254.
-  J. D. Key, T. P. McDonough, and V. C. Mavron, *Information sets and partial permutation decoding for codes from finite geometries*, Finite Fields Appl. **12** (2006), 232–247.
-  J. D. Key, J. Moori, and B. G. Rodrigues, *Codes from incidence matrices and line graphs of symplectic graphs*, (In preparation).
-  _____, *Codes associated with triangular graphs, and permutation decoding*, Int. J. Inform. and Coding Theory **1, No.3** (2010), 334–349.

-  J. D. Key and B. G. Rodrigues, *Codes associated with lattice graphs, and permutation decoding*, Discrete Appl. Math. **158** (2010), 1807–1815.
-  J. D. Key and P. Seneviratne, *Permutation decoding of binary codes from lattice graphs*, Discrete Math. **308** (2008), 2862–2867.
-  Q.L. Li and Q. Li, *Super edge connectivity properties of connected edge symmetric graphs*, Networks **33** (1999), 157–159.
-  M. Lavrauw, L. Storme, and G. Van de Voorde, *On the code generated by the incidence matrix of points and hyperplanes in $PG(n, q)$ and its dual*, Des. Codes Cryptogr. **48** (2008), 231–245.
-  _____, *On the code generated by the incidence matrix of points and k -spaces in $PG(n, q)$ and its dual*, Finite Fields Appl. **14** (2008), 1020–1038.
-  F. J. MacWilliams, *Permutation decoding of systematic codes*, Bell System Tech. J. **43** (1964), 485–505.



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



R. Tindell, *Edge-connectivity properties of symmetric graphs*, Preprint, Stevens Institute of Technology, Hoboken, NJ, 1982.



J.M. Xu, *Restricted edge-connectivity of vertex-transitive graphs*, Chinese J. Contemp. Math. **21** (2000), no. 4, 369–374.