Codes from lattice and related graphs, and permutation decoding

Bernardo Rodrigues (rodrigues@ukzn.ac.za)[1]

[1]School of Mathematical Sciences
University of KwaZulu-Natal,
joint work with Jennifer Key, Clemson University

Symmetries of Discrete Objects
Queenstown, February 15, 2012

Motivation

Codes from the row span of incidence matrices of some classes of graphs share certain useful properties:

- $\Gamma = (V, E)$ regular connected graph of valency k, and $|V| = N$
- $\mathcal{G}$ an $N \times \frac{1}{2}Nk$ incidence matrix (vertices by edges) for Γ;
- $C_p(\mathcal{G})$ the code spanned by the rows of $\mathcal{G}$ over $\mathbb{F}_p$, for p prime, might be

$$[\frac{1}{2} \times Nk,\ N,\ k]_p \text{ or } [\frac{1}{2} \times Nk,\ N-1,\ k]_2;$$

with minimum vectors the scalar multiples of the rows of $\mathcal{G}$ of weight k.

Motivation

- There is often a gap in the weight enumerator between k and $2(k-1)$, the latter arising from the difference of two rows (when $p = 2$ the code of the adjacency matrix of the line graph).
- 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 $PG_{n,k}(Fq)$.
- But, not always true for non-desarguesian planes: e.g. there are planes of order 16 that have words in this gap. (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.)

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, $\mathbf{x} \sim \mathbf{y}$, then $[\mathbf{x}, \mathbf{y}]$ is the edge they define.
- A graph is regular if all the vertices have the same valency k.
- An a adjacency matrix $A = [a_{ij}]$ 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 $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ with **point set** $\mathcal{P}$ and **block set** $\mathcal{B}$ and incidence $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$ is a $t-(v, k, \lambda)$ design if $|\mathcal{P}| = v$; every block $B \in \mathcal{B}$ is incident with precisely $\mathbf{k}$ points; every $\mathbf{t}$ distinct points are together incident with precisely λ blocks.

- 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** for Γ is a $|V| \times |E|$ matrix $B = [b_{i,j}]$ 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.

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

$$BB^T = A + kI_N \text{ and } B^TB = M + 2I_e.$$

Coding theory terminology

- A linear code is a subspace of the n-dimensional vector space $\mathbb{F}_q^n$ over the finite field $\mathbb{F}_q$. (All codes are linear in this talk.)
- The (Hamming) distance between two vectors $u, v \in \mathbb{F}_q^n$ is the number of coordinate positions in which they differ.
- The weight of a vector v, written $\mathbf{wt(v)}$, is the number of non-zero coordinate entries. If a code has smallest non-zero weight d then the code can correct up to $\lfloor (d-1)/2 \rfloor$ errors by nearest-neighbour decoding. , i.e. if at most t errors occur in transmission then the nearest codeword to the received vector is the one that was sent.
- If a code C over a field of order q is of length n, dimension k, and minimum weight d, then we write $[n, k, d]_q$ to show this information.

UNIVERSITY OF KWAZULU-NATAL

Coding theory terminology - continued

- A generator matrix for the code is a $k \times n$ matrix made up of a basis for C.
- The dual code $C^{\perp}$ is the orthogonal under the standard inner product $(,)$, i. e.

$$C^{\perp} = \{v \in F^n | (v, c) = 0 \text{ for all } c \in C\}.$$

- A check matrix for C is a generator matrix H for $C^{\perp}$.
- Two linear codes of the same length and over the same field are isomorphic if they can be obtained from one another by permuting the coordinate positions.
- An automorphism of a code is any permutation of the coordinate positions that maps codewords to codewords.
- Any code is isomorphic to a code with generator matrix in standard form, i.e. the form $[I_k \,|\, A]$; a check matrix then is given by $[-A^T | I_{n-k}]$. The first k coordinates are the information symbols and the last $n-k$ coordinates are the check symbols.

Result

$\Gamma = (V, E)$ is a graph, G an incidence matrix, $\mathcal{G}$ the incidence design, $C_p(G)$ the row-span of G over F_p.

1. If Γ is connected then $\dim(C_2(G)) = |V| - 1$.
2. If Γ is connected and has a closed path of odd length ≥ 3, then $\dim(C_p(G)) = |V|$ for p odd.
3. If $[P, Q, R, S]$ is a closed path in Γ, then for any prime p,
$$u = v^{[P,Q]} + v^{[R,S]} - v^{[P,S]} - v^{[Q,R]} \in C_p(G)^{\perp}.$$
4. If Γ is regular, $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\Gamma)$.

Outline proof of 1 and 2

That $\dim(C_p(G)) = |V| - 1$ is folklore and easy to prove.
Clearly there is equality for $p = 2$.
For p odd, let $w = \sum a_i r_i = 0$ be a sum of multiples of the rows r_i of G, where r_i corresponds to the vertex i.
If $[\mathrm{i}, \mathrm{j}]$ is an edge then $a_i = -a_j$. Taking a closed path $(i_0, i_1, \ldots i_m)$ of odd length, so $a_{i_0} = -a_{i_1} = \ldots = a_{i_m} = -a_{i_0}$, and thus $a_{i_0} = 0$.
Since the graph is connected, we thus get $a_i = 0$ for all i.
Proof of (3) immediate, and of (4) quite direct.

The complete bipartite graph and its line graph the lattice graph L_n

- The **complete bipartite graph** $K_{n,n}$ on $2n$ vertices, $A \cup B$, where $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_n\}$, with n^2 edges.
- $K_{n,n}$ has for line graph, the **lattice graph** L_n, which has vertex set the set of ordered pairs $\{(a_i, b_j) \mid 1 \leq i, j \leq n\}$, where two pairs are adjacent if and only if they have a common coordinate.
- L_n is a strongly regular graph of type $(n^2, 2(n-1), n-2, 2)$.

Strongly regular (n, k, λ, μ) graph

A graph $\Gamma = (V, E)$ is strongly regular of type (n, k, λ, μ) if:

- $|V| = n$
- Γ is regular with degree (valency) 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 $P \nsim Q$,

$$|R \in V \mid R \sim P \& R \sim Q| = \mu;$$

Result

For $n \geq 5$, let C be the binary code from the row span of an adjacency matrix for the lattice graph of $K_{n,n}$ with vertices $A \times B$ where $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_n\}$. Then C is a $[n^2, 2(n-1), 2(n-1)]_2$ code and the set

$$\mathcal{I} = \{(a_i, b_n) \mid 2 \leq i \leq n-1\} \cup \{(a_n, b_i) \mid 1 \leq i \leq n\}$$

is an information set, and the set

$$\mathcal{S} = \{((i,n),(j,n)) \mid 1 \leq i \leq n,\ 1 \leq j \leq n\}$$

of permutations in $S_n \times S_n$ forms a PD-set of size n^2 for C for $\mathcal{I}$.

- For any $n \geq 2$, let $\mathcal{G}_n$ denote the incidence design of the complete bipartite graph $K_{n,n}$.
- $\mathcal{G}_n$ is a 1-$(n^2, n, 2)$ design.
- The point set of $\mathcal{G}_n$ will be denoted by $\mathcal{P}_n = A \times B$, where $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_n\}$.
- Writing $\Omega = \{1, \ldots, n\}$, we take for incidence matrix M_n
- The first n rows of M_n are labelled by the vertices of $K_{n,n}$ in A, and the next n rows by B.
- The columns are labelled

$$(a_1, b_1), \ldots, (a_1, b_n), (a_2, b_1) \ldots (a_2, b_n), \ldots, (a_n, b_1), \ldots, (a_n, b_n). \tag{1}$$

- For $a_i \in A$ the **block of $\mathcal{G}_n$** defined by the row a_i will be written as

$$\overline{a_i} = \{(a_i, b_j) \mid 1 \leq j \leq n\}, \tag{2}$$

and or $b_i \in B$ the **block of $\mathcal{G}_n$** defined by the row b_i will be written as

$$\overline{b_i} = \{(a_j, b_i) \mid 1 \leq j \leq n\}. \tag{3}$$

- The code of $\mathcal{G}_n$ over $\mathbb{F}_p$ will be denoted by C_n where

$$\mathbf{C_n} = \langle\, v^{\overline{x}} \mid \mathbf{x} \in \mathbf{A} \cup \mathbf{B} \rangle, \tag{4}$$

and the span is taken over $\mathbb{F}_p$.

-

$$\mathbf{E_n} = \langle\, v^{\overline{x}} - \; v^{\overline{y}} \mid \mathbf{x}, \mathbf{y} \in \mathbf{A} \cup \mathbf{B} \rangle. \tag{5}$$

- The rows of an adjacency matrix A_n for L_n give the blocks of the neighbourhood design $\overline{\mathcal{D}}_n$ of L_n.
- The matrix M_n of $\mathcal{G}_n$ satisfies

$$M_n^T M_n = A_n + 2I_{n^2}.$$

- The blocks of $\overline{\mathcal{D}_n}$ are

$$\overline{(a_i, b_j)} = \{(a_i, b_k) \mid k \neq j\} \cup \{(a_k, b_j) \mid k \neq i\} \tag{6}$$

  for each point $(a_i, b_j) \in \mathcal{P}_n$.
- $\overline{\mathcal{D}}_n$ is a symmetric 1-$(n^2, 2(n-1), 2(n-1))$ design for $n \geq 3$ and p-ary code

$$\overline{\mathbf{C}}_\mathbf{n} = \langle\ v^{\overline{(a_i, b_j)}} \mid (\mathbf{a_i}, \mathbf{b_j}) \in \mathcal{P}_\mathbf{n} \rangle. \tag{7}$$

- For the reflexive lattice graph L_n^R, we get the 1-$(n^2, 2n-1, 2n-1)$ design $\overline{\overline{\mathcal{D}}}_n$ with blocks

$$\overline{\overline{(a_i, b_j)}} = \overline{(a_i, b_j)} \cup \{(a_i, b_j)\} \tag{8}$$

for each point $(a_i, b_j) \in \mathcal{P}_n$, and p-ary code

$$\overline{\overline{\mathbf{C}}}_{\mathbf{n}} = \langle\, v^{\overline{\overline{(a_i, b_j)}}} \mid (\mathbf{a_i}, \mathbf{b_j}) \in \mathcal{P}_{\mathbf{n}} \rangle. \tag{9}$$

- The graph $\widetilde{L}_n$ is the complement of L_n and gives a symmetric 1-$(n^2, (n-1)^2, (n-1)^2)$ design $\widetilde{\mathcal{D}}_n$ with blocks

$$\widetilde{(a_i, b_j)} = \{(a_k, b_m) \mid k \neq i, m \neq j\} = \mathcal{P}_n \setminus \{\, \overline{\overline{(a_i, b_j)}}\} \tag{10}$$

for each point $(a_i, b_j) \in \mathcal{P}_n$, and p-ary code

$$\widetilde{\mathbf{C}}_{\mathbf{n}} = \langle\, v^{\widetilde{(a_i, b_j)}} \mid (\mathbf{a_i}, \mathbf{b_j}) \in \mathcal{P}_{\mathbf{n}} \rangle. \tag{11}$$

p-ary codes from L_n and related graphs

- From the reflexive graph $\widetilde{L}_n^R$ we get a 1-$(n^2, n^2-2n+2, n^2-2n+2)$ design $\widetilde{\widetilde{\mathcal{D}}}_n$ (for $n \geq 3$) with blocks

$$\widetilde{\widetilde{(a_i, b_j)}} = \widetilde{(a_i, b_j)} \cup \{(a_i, b_j)\} \tag{12}$$

for each point $(a_i, b_j) \in \mathcal{P}_n$, and p-ary code

$$\widetilde{\widetilde{\mathbf{C}_\mathbf{n}}} = \langle\, v^{\widetilde{\widetilde{(a_i,b_j)}}} \mid (\mathbf{a_i}, \mathbf{b_j}) \in \mathcal{P}_\mathbf{n} \rangle. \tag{13}$$

- If $\jmath$ denotes the all-one vector of length n^2, then, for all $(a,b) \in \mathcal{P}_n$, we have

$$v^{\overline{\overline{(a,b)}}} + v^{\widetilde{(a,b)}} = \jmath = v^{\overline{(a,b)}} + v^{\widetilde{\widetilde{(a,b)}}}. \tag{14}$$

- The group $G = S_n \wr S_2$ is the automorphism group of $K_{n,n}$.
- G acts on the edge set $\mathcal{P}_n = A \times B$ by its construction as an extension of the group $H = S_n \times S_n$ by $S_2 = \{1, \tau\}$, where $\tau = (1, 2)$.
- The element τ then acts on H via $(\alpha, \beta)^\tau = (\beta, \alpha)$, for $\alpha, \beta \in S_n$.
- G acts as a rank-3 group on $\mathcal{P}_n$ as follows:

$$(a_i, b_j)^{(\alpha,\beta)} = (a_{i^\alpha}, b_{j^\beta}), \ and \ (a_i, b_j)^\tau = (a_j, b_i). \qquad (15)$$

Lemma

For $n \geq 2$, if $\{i, j, k, m\} \subseteq \Omega$ where $i \neq k$, and $j \neq m$, then the vector

$$u = u((a_i, b_j), (a_k, b_m)) = v^{(a_i, b_j)} + v^{(a_k, b_m)} - v^{(a_i, b_m)} - v^{(a_k, b_j)} \quad (16)$$

is in $C_n^{\perp}$ for any prime p.

Proof: This is clear since $(\overline{x}, u) = 0$ for all choices of $x \in A \cup B$. ■

Theorem

1. For $n \geq 2$, any prime p, the code C_n of the incidence design $\mathcal{G}_n$ of the complete bipartite graph $K_{n,n}$ is a $[n^2, 2n-1, n]_p$ code.
2. For $n \geq 3$ the minimum-weight vectors are the scalar multiples of the incidence vectors of the blocks of $\mathcal{G}_n$.
3. For $n \geq 2$, $C_n = C_p(\mathcal{G}_n)$ where p is any prime, then
$$\mathcal{U} = \{u((a_i, b_j), (a_{i+1}, b_{j+1})) \mid 1 \leq i \leq n-1, 1 \leq j \leq n-1\}$$
is a basis for $C_n^{\perp}$.
4. For $n \geq 3$, $\mathrm{Aut}(\mathcal{G}_n) = \mathrm{Aut}(C_n) = S_n \wr S_2$ where $C_n = C_p(\mathcal{G}_n)$ and p is any prime.
5. For $n \geq 3$, let $E_n = \langle\ v^{\overline{x}} - \ v^{\overline{y}} \mid x, y \in A \cup B\rangle$ over $\mathbb{F}_p$ where p is any prime. Then E_n is a $[n^2, 2n-2, 2n-2]_p$ code and the words of weight $2n-2$ are the scalar multiples of $v^{\overline{a_i}} - \ v^{\overline{b_j}}$, for $1 \leq i, j \leq n$.

Outline of proof

Prof of (1) and (2):
Take a class for $n \in \mathbb{N}$, by embedding an incidence matrix for $n-1$ in that for n, and using induction.
Proof of (3):

- Consider $\mathcal{U}$ as a sequence ordered first through fixing i, and allowing j to take the values 1 to $n-1$ within each fixed i.
- Thus the sequence is

$$[u((a_1, b_1), (a_2, b_2)), u((a_1, b_2), (a_2, b_3)), \ldots, u((a_{n-1}, b_{n-1}), (a_n, b_n))]$$

- If the points of $\mathcal{P}_n$ are ordered as described for M_n in Equation (1), then the array of vectors from $\mathcal{U}$ is in echelon form.
- Since $|\mathcal{U}| = (n-1)^2 = n^2 - (2n-1) = \dim(C_n^{\perp})$, we have the result.

To prove (4) use Withney's Theorem and (1) and (2).

Permutation decoding

Definition

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

More specifically, if $\mathcal{I} = \{1, 2, \ldots, k\}$ are the information positions and $\mathcal{C} = \{k+1, k+2, \ldots, n\}$ the check positions, then every t-tuple from $\{1, 2, \ldots, n\}$ can be moved by some element of $\mathcal{S}$ into $\mathcal{C}$.

The Algorithm

C is a q-ary t-error-correcting $[n, k, d]_q$ code where $d = 2t + 1$ or $2t + 2$.
$G = [I_k \mid A]$ is a $k \times n$ generator matrix for C

- Any k-tuple v is encoded as vG. The first k columns are the information symbols, the last $n - k$ are the check symbols. $H = [-A^T \mid I_{n-k}]$ is an $(n - k) \times n$ check matrix for C. Suppose that x is sent and y is received and at most t errors occur. Let $\mathcal{S} = \{g_1, \ldots, g_m\}$ be the PD-set for C written in some chosen order.
- For $i = 1, \ldots, m$, compute yg_i and the syndromes $m_i = H(yg_i)^T$ until an i is found such that the weight of m_i is t or less;
- if $u = u_1\, u_2 \, \ldots u_k$ are the information symbols of yg_i, compute the codeword $c = uG$;
- decode y as cg_i^{-1}.

Why permutation decoding works?

Result

Let C be an $[n, k, d]_q$ t-error-correcting code. Suppose H is a check matrix for C in standard form, i.e. such that I_{n-k} is in the redundancy positions. Let $y = c + e$ be a vector, where $c \in C$ and e has weight less than or equal to t.
Then the information symbols in y are correct if and only if the weight of the syndrome Hy^T of y is less than or equal to t.

What is the minimum size of a PD-set ?

Counting shows that there is a bound on the minimum size that the set $\mathcal{S}$ may have. This result is due to Gordon, using a result of Schönheim

Result

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

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

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

Permutation decoding sets for the codes examined

Proposition

If $C_n = C_p(\mathcal{G}_n)$ where $n \geq 3$, and p is any prime, then

$$\mathcal{I}_n = \{(a_i, b_n) \mid 1 \leq i \leq n\} \cup \{(a_n, b_i) \mid 1 \leq i \leq n-1\}$$

is an information set for C_n and the set

$$S = \{((n,i),(n,i)) \mid 1 \leq i \leq n\},$$

of elements of $S_n \times S_n$, where $(i,j) \in S_n$ is a transposition and (k,k) is the identity of S_n, is a PD-set for C_n of size n for the information set $\mathcal{I}_n$.

Proposition

For $n \geq 3$, let $E_n = \langle\ v^{\overline{x}} -\ v^{\overline{y}} \mid x, y \in A \cup B \rangle$ over $\mathbb{F}_p$ where p is any prime. Then

$$\mathcal{I}_n^* = \{(a_i, b_n) \mid 1 \leq i \leq n\} \cup \{(a_n, b_i) \mid 1 \leq i \leq n-1\} \setminus \{(a_1, b_n)\}$$

is an information set for E_n and

$$S = \{((n,i),(n,j)) \mid 1 \leq i,j \leq n\}, \tag{17}$$

of elements of $S_n \times S_n$, where $(i,j) \in S_n$ is a transposition and (k,k) is the identity of S_n, is a PD-set of size n^2 for E_n using $\mathcal{I}_n^*$.