Binary codes from rectangular lattice graphs and permutation decoding

J. D. Key [a,*,1] P. Seneviratne [a]

[a] *Department of Mathematical Sciences, Clemson University, Clemson SC 29634, U.S.A.*

Abstract

We examine the binary codes obtained from the row span over the field $\mathbb{F}_2$ of an adjacency matrix of the rectangular lattice graphs $L_2(m, n)$ for $3 \leq m < n$ and show that permutation decoding can be used for full error-correction for these codes by finding explicit information sets and PD-sets for these information sets.

Key words: Codes, graphs, designs
PACS: 05, 51, 94

1 Introduction

For any integers m and n the rectangular graph $L_2(m, n)$ is defined to be the line graph of the complete bipartite graph $K_{m,n}$. It is a regular graph of valency $m + n - 2$ on $v = mn$ vertices, i.e. on the ordered pairs $\langle i, j \rangle$ where $1 \leq i \leq m$ and $1 \leq j \leq n$, with adjacency defined by $\langle i, j \rangle$ and $\langle k, l \rangle$ being adjacent if $i = k$ and $j \neq l$ or $j = l$ and $i \neq k$. If $m = n$ then this is the strongly regular square lattice graph, $L_2(n)$. In [KS] we applied permutation decoding to the square lattice graphs and obtained PD-sets of size n^2 for full error-correction, and so we exclude this case here, and thus assume that $m < n$. By similar reasoning to the square case we found that permutation decoding could be used for full error correction in the rectangular case as well, and we obtain the following theorem:

* Corresponding author.
[1] This work was supported by the DoD Multidisciplinary University Research Initiative (MURI) program administered by the Office of Naval Research under Grant N00014-00-1-0565.

Theorem 1 *If C is the binary code formed by the row space over $\mathbb{F}_2$ of an adjacency matrix for the rectangular lattice graph $L_2(m,n)$ for $2 \leq m < n$, then C is*

- $[mn, m+n-2, 2m]_2$ *for $m+n$ even*
- $[mn, m+n-1, m]_2$ *for $m+n$ odd*

with $S_m \times S_n$ as an automorphism group of C. The set

$$\mathcal{I} = \{\langle i, n\rangle \mid 1 \leq i \leq m\} \cup \{\langle m, i\rangle \mid 1 \leq i \leq n-1\}$$

is an information set for $m+n$ odd, and $\mathcal{I} \setminus \{\langle 1, n\rangle\}$ is an information set for $m+n$ even. Let

$$\mathcal{S}_e = \{((i,m),(j,n)) \mid 1 \leq i \leq m,\ 1 \leq j \leq m\} \cup \{id\},$$
$$\mathcal{S}_o = \{((i,m),(i,n)) \mid 1 \leq i \leq m\} \cup \{id\},$$

be sets of permutations in $S_m \times S_n$. Then for $3 \leq m < n$, $\mathcal{S}_e$ is a PD-set of m^2+1 elements for C for $m+n$ even, and $\mathcal{S}_o$ is a PD-set of $m+1$ elements for C for $m+n$ odd, using $\mathcal{I}$ as information symbols for $m+n$ odd, and $\mathcal{I} \setminus \{\langle 1, n\rangle\}$ for $m+n$ even, and where id denotes the identity map.

Note that we use (r, r) to denote the identity element of S_r. We also take $m \geq 3$ since we only need PD-sets for t-error-correction where $t \geq 2$. It follows from the theorem that the set of blocks

$$\mathcal{B}_I = \{\ \overline{\langle i, n\rangle} \mid 1 \leq i \leq m\} \cup \{\ \overline{\langle m, i\rangle} \mid 1 \leq i \leq n-1\}$$

forms a basis for C when $m+n$ is odd, and $\mathcal{B}_I \setminus \{\ \overline{\langle 1, n\rangle}\}$ for $m+n$ even. (Here we use the notation, explained in Section 3, for $1 \leq i \leq m$ and $1 \leq j \leq n$,

$$\overline{\langle i, j\rangle} = \{\langle i, k\rangle \mid k \neq j\} \cup \{\langle k, j\rangle \mid k \neq i\}$$

to denote the block defined by the point $\langle i, j\rangle$.)

The proof that the sets $\mathcal{S}_e$ and $\mathcal{S}_o$ are PD-sets for the given information sets is in Section 4. In Section 2 we give some background material and in Section 3 we obtain results about the codes and their duals, including finding the given information sets.

2 Background and terminology

Following generally the notation as in [AK92], an incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v, k, λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. The design is **symmetric** if it has the same number of points and blocks.

The **code C_F of the design** $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F. If the point set of $\mathcal{D}$ is denoted by $\mathcal{P}$ and the block set by $\mathcal{B}$, and if $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the incidence vector of $\mathcal{Q}$ by $v^{\mathcal{Q}}$. Thus $C_F = \left\langle v^B \mid B \in \mathcal{B} \right\rangle$.

The codes here are all **linear codes**, and we use the notation $[n, k, d]_q$ for a q-ary code of length n, dimension k, and minimum weight d. The **dual** of a code C will be denoted by $C^{\perp}$. A **check** matrix for C is a generator matrix H for $C^{\perp}$; the **syndrome** of a vector $y \in F^n$ is Hy^T. The **all-one vector** will be denoted by $\boldsymbol{\jmath}$, and is the vector with all its entries equal to 1. 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. Any code is isomorphic to a code with generator matrix in **standard form**, $[I_k \mid A]$. The first k coordinates are the **information symbols** and the last $n - k$ coordinates are the **check symbols**. An **automorphism** of a code C is an isomorphism from C to C and the automorphism group will be denoted by $\mathrm{Aut}(C)$.

Graphs will be undirected. $\Gamma = (V, E)$ denotes a graph with vertex set V and edge set E; the **valency** of a vertex is the number of edges containing the vertex, and Γ is **regular** if all the vertices have the same valency. The **line graph** of $\Gamma = (V, E)$ is the graph $\Gamma^t = (E, V)$ where e and f are adjacent in Γ^t if e and f share a vertex in Γ. The **complete bipartite graph** $K_{m,n}$ on $m + n$ vertices has for line graph the **rectangular lattice graph** $L_2(m, n)$, which has vertex set the set of ordered pairs $\{\langle i, j\rangle \mid 1 \le i \le m,\ 1 \le j \le n\}$, where two pairs are adjacent if and only if they have a common coordinate.

Permutation decoding was first developed by MacWilliams [Mac64] and involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and Sloane [MS83, Chapter 15] and Huffman [Huf98, Section 8]. A **PD-set** for a t-error-correcting code C is a set $\mathcal{S}$ of automorphisms of C which is such that every possible error vector of weight $s \le t$ can be moved by some member of $\mathcal{S}$ to another vector where the s non-zero entries have been moved out of the information positions. In other words, every t-set of coordinate positions is moved by at least one member of $\mathcal{S}$ to a t-set consisting only of check-position coordinates. That such a set will fully use the error-correction potential of the code follows easily and is proved in Huffman [Huf98, Theorem 8.1]. Such a set might not exist at all, and the property of having a PD-set might not be invariant under isomorphism of codes. Furthermore, there is a bound on the minimum size that the set $\mathcal{S}$ may have (see [Gor82],[Sch64], or [Huf98]):

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

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

The algorithm for permutation decoding is as follows: if C is an $[n,k,d]_q$ code that can correct t errors, with check matrix H in standard form, then the generator matrix $G = [I_k|A]$ and $H = [A^T|I_{n-k}]$, for some A, with the first k coordinate positions corresponding to the information symbols. Any vector v of length k is encoded as vG. Suppose x is sent and y is received and at most t errors occur. Let $\mathcal{S} = \{g_1, \dots, g_s\}$ be the PD-set. Compute the syndromes $H(yg_i)^T$ for $i = 1, \dots, s$ until an i is found such that the weight of this vector is t or less. Compute the codeword c that has the same information symbols as yg_i and decode y as cg_i^{-1}.

Note that PD-sets are only needed for $t > 1$ error-correction since correcting a single error can be done by using syndrome decoding.

3 The binary codes

Let $2 \leq m < n$ be integers and let $L_2(m,n)$ denote the rectangular lattice graph with vertex set $\mathcal{P}$ the mn ordered pairs $\langle i,j \rangle$, $1 \leq i \leq m$, $1 \leq j \leq n$. The 1-design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ will have point set $\mathcal{P}$ and for each point $\langle i,j \rangle \in \mathcal{P}, 1 \leq i \leq m, 1 \leq j \leq n$, a block, which we denote by $\overline{\langle i,j \rangle}$, is defined in the following way:

$$\overline{\langle i,j \rangle} = \{\langle i,k \rangle \mid k \neq j\} \cup \{\langle k,j \rangle \mid k \neq i\}.$$

Thus the block size is $m+n-2$ and $\mathcal{D}$ is a symmetric 1-design with block set

$$\mathcal{B} = \{ \ \overline{\langle i,j \rangle} \mid 1 \leq i \leq m, 1 \leq j \leq n\}.$$

The incidence vector of the block $\overline{\langle i,j \rangle}$ is

$$v^{\overline{\langle i,j \rangle}} = \sum_{k \neq j} v^{\langle i,k \rangle} + \sum_{k \neq i} v^{\langle k,j \rangle} = \sum_{k=1}^{n} v^{\langle i,k \rangle} + \sum_{k=1}^{m} v^{\langle k,j \rangle} \tag{1}$$

where, as usual with the notation from [AK92], the incidence vector of the subset $X \subseteq \mathcal{P}$ is denoted by v^X, but writing $v^{\langle i,j \rangle}$ instead of $v^{\{\langle i,j \rangle\}}$.

The group $S_m \times S_n$ acts naturally on $\mathcal{D}$ and thus on C in the following way: if $\sigma = (\sigma_1, \sigma_2)$ where $\sigma_1 \in S_m$ and $\sigma_2 \in S_n$, then for $\langle i,j \rangle \in \mathcal{P}$, $\langle i,j \rangle^\sigma = \langle i^{\sigma_1}, j^{\sigma_2} \rangle$.

Proposition 1 *Let C be the binary code of $L_2(m,n)$ where $1 \leq m < n$. Then*

$$\dim(C) = \begin{cases} m+n-1 & \textit{for } m+n \textit{ odd} \\ m+n-2 & \textit{for } m+n \textit{ even} \end{cases}$$

PROOF. Let M be a vertex–edge incidence matrix for $K_{m,n}$, where the two parts of the graph are $\Lambda_1 = \{1,\ldots,m\}$ and $\Lambda_2 = \{1,\ldots,n\}$, ordering the rows of M by taking the points of Λ_1 followed by the points of Λ_2, and ordering the edges by taking all the edges through the first point, followed by all the edges through the second point, and so on. Then $M^T M = A$ is an adjacency matrix for $L_2(m,n)$. If C_A denotes the row span of A over $\mathbb{F}_2$ and C_M that of M, then $C_A \subseteq C_M$. Clearly $\dim(C_M) = m+n-1$.

If V denotes the row span of M^T then $\tau : V \to C_A$ by $\tau : v \mapsto vM$ has $V\tau = C_A$, so $\dim(C_A) = m+n-1$ or $m+n-2$, the latter if and only if $\boldsymbol{\jmath} = (1,\ldots,1) \in \mathbb{F}_2^{m+n}$ is in V. Considering the form of M^T that we have chosen, it is easy to see that if both m and n are odd, then $\boldsymbol{\jmath} \in V$. Similarly if both are even, it follows that $\boldsymbol{\jmath} \in V$.

The only case that needs further consideration is when one is odd and other even, and in this case we show that $\boldsymbol{\jmath} \notin V$. The rows of M^T are arranged in m sections of n rows each; the columns are in two sections, the first of m columns, the second of n. If $\boldsymbol{\jmath} \in V$ then as a sum of the rows of M^T, $\boldsymbol{\jmath} = (x_1,\ldots,x_m,y_1,\ldots,y_n)$, where x_i is the number of rows in the sum from the i^{th} section of rows, for $i = 1,\ldots,m$. Thus x_i is odd for $i = 1,\ldots,m$. For the entries in the columns starting at the $(m+1)^{th}$ (i.e. the vertices through the Λ_2 points), suppose the i^{th} point, for $i = 1,\ldots,n$, in Λ_2 contributes $n_{i,j}$ to the vector from the j^{th} section of rows of M^T, for $j = 1,\ldots,m$, where $n_{i,j} = 0$ or 1, from the form of M^T. Thus $y_i = \sum_{j=1}^m n_{i,j}$ for $i = 1,\ldots,n$, and $x_i = \sum_{j=1}^n n_{j,i}$ for $i = 1,\ldots,m$. Summing by rows and by columns gives $s = \sum_{i,j} n_{i,j} = \sum_{i=1}^m x_i = \sum_{j=1}^n y_j$. If $m+n$ is odd, this contradicts all the x_i and y_j being odd, and thus $\boldsymbol{\jmath} \notin V$ in this case, which completes the proof. ■

Proposition 2 *Let C be the binary code of $L_2(m,n)$ where $1 \leq m < n$. Then C has minimum weight m if $m+n$ is odd, and $2m$ if $m+n$ is even.*

PROOF. If $m+n$ is odd then $C = C_M$ from the previous proposition, so clearly there are words of weight m. That there cannot be words of smaller weight in C_M is clear from the form of M.

In general we have from $\overline{v^{\langle i,j\rangle}} = \sum_{k=1}^{n} v^{\langle i,k\rangle} + \sum_{k=1}^{m} v^{\langle k,j\rangle}$ that

$$\sum_{j=1}^{n} \overline{v^{\langle i,j\rangle}} = n \sum_{k=1}^{n} v^{\langle i,k\rangle} + \boldsymbol{\jmath},$$

$$\sum_{i=1}^{m} \overline{v^{\langle i,j\rangle}} = m \sum_{k=1}^{m} v^{\langle k,j\rangle} + \boldsymbol{\jmath},$$

and

$$\overline{v^{\langle i,j\rangle}} + \overline{v^{\langle i,k\rangle}} = \sum_{l=1}^{m} v^{\langle l,j\rangle} + \sum_{l=1}^{m} v^{\langle l,k\rangle}.$$

If $m+n$ is even and $C \neq C_M$, then again the form of M shows that $2m$ is the next possible weight, and C does have such words, as is shown by the last equation above. ■

Proposition 3 *Let C be the binary code of $L_2(m,n)$ where $2 \leq m < n$. Then for i_1, i_2 distinct elements in $\{1,\ldots,m\}$ and j_1, j_2 distinct elements in $\{1,\ldots,n\}$, the vector*

$$u(i_1,i_2;j_1,j_2) = v^{\langle i_1,j_1\rangle} + v^{\langle i_1,j_2\rangle} + v^{\langle i_2,j_1\rangle} + v^{\langle i_2,j_2\rangle}$$

is a weight-4 vector in $C^{\perp}$.

If $s_i = \{i, i+1\}$ for $1 \leq i \leq m-1$ and $t_i = \{i, i+1\}$ for $1 \leq i \leq n-1$, the set of vectors $\{u(s_i;t_j) \mid 1 \leq i \leq m-1,\ 1 \leq j \leq n-1\}$ is a linearly independent set of $mn - m - n + 1$ vectors that forms a basis for $C^{\perp}$ for $m+n$ odd, and together with $\boldsymbol{\jmath}$ when $m+n$ is even. Furthermore, the set

$$\langle 1,1\rangle, \ldots, \langle 1,n-1\rangle, \langle 2,1\rangle, \ldots, \langle 2,n-1\rangle, \ldots, \langle m-1,1\rangle, \ldots, \langle m-1,n-1\rangle$$

of points is an information set for $C^{\perp}$ for $m+n$ odd, and together with $\langle 1,n\rangle$ for $m+n$ is even.

PROOF. It is easy to verify that the vectors $u(i_1,i_2;j_1,j_2)$ are in $C^{\perp}$. If the coordinate positions are then arranged as shown in the statement and the vectors $u(s_i;t_j)$ as rows in the order

$$(s_1;t_1), \ldots, (s_1;t_{n-1}), (s_2;t_1), \ldots, (s_{m-1};t_{n-1}),$$

then the resulting matrix is already in row echelon form. In the case of $m+n$ even, the vector $\boldsymbol{\jmath}$ can be added to obtain a further basis element. ■

Note that in fact it can easily be shown that the minimum weight of $C^{\perp}$ is precisely 4.

4 PD-sets

We now complete the proof of the theorem by showing that the set of permutations is a PD-set for the code. We take $m \geq 3$ since we only need PD-sets when at least two errors can be corrected.

Proof of Theorem 1: From Proposition 3, an information set for C is

$$\mathcal{I} = \{\langle i, n\rangle \mid 1 \leq i \leq m\} \cup \{\langle m, i\rangle \mid 1 \leq i \leq n-1\}$$

for $m+n$ odd and $\mathcal{I} \setminus \{\langle 1, n\rangle\}$ for $m+n$ even.

Suppose C can correct t errors and let

$$\mathcal{T} = \{(a_1, b_1), \ldots, (a_s, b_s)\}$$

be a set of $s \leq t$ points. We need an element from our set of involutions that maps $\mathcal{T}$ into the check positions $\mathcal{C}$. Let $\Omega_1 = \{a_i \mid 1 \leq i \leq s\}$ and $\Omega_2 = \{b_i \mid 1 \leq i \leq s\}$.

Take first $m+n$ even, so $t = m-1$. Then $|\Omega_i| \leq m-1 < n-1$. Thus we can find l such that $1 \leq l \leq m$ and $l \notin \Omega_2$. If there exists k such that $1 \leq k \leq m-1$ and $k \notin \Omega_1$, then the element $\sigma = ((k, m), (l, n)) \in \mathcal{S}_e$ will move all the elements of $\mathcal{T}$ into $\mathcal{C}$. If $\Omega_1 = \{1, \ldots, m-1\}$, then $\sigma = ((m, m), (l, n))$ will map $\mathcal{T}$ to $\mathcal{C}$, where (m, m) denotes the identity permutation. Including the identity automorphism covers the case where $\mathcal{T} \subset \mathcal{C}$.

If $m+n$ is odd, then the minimum weight is m so $t = \lfloor \frac{m-1}{2} \rfloor$. Thus $s \leq \frac{m-1}{2}$ and there exists k such that $1 \leq k \leq m$ and $k \notin \Omega_1$ and $k \notin \Omega_2$. The element $\sigma = ((k, m), (k, n)) \in \mathcal{S}_o$ will map $\mathcal{T}$ to $\mathcal{C}$. Again, including the identity automorphism covers the case where $\mathcal{T} \subset \mathcal{C}$. This completes the proof of the theorem ■

5 Concluding remarks

The bound from Result 1 in the case $m+n$ odd appears to be $\lceil \frac{m}{2} \rceil$; our PD-set has size $m+1$ and computations with Magma [BC94] using this set gave something close to $m+1$ in the cases we looked at. The bound for $m+n$ even is harder to establish, but appears to approach m as n increases, for fixed m. Clearly small PD-sets are desirable for applications. The codes are not in general spanned by their minimum-weight vectors, although $C^\perp$ is in the case of $m+n$ odd.

Codes from classes of graphs or structures that have automorphism groups that grow in similar order to the growth of the length of the code, as in this case, might have PD-sets for full error correction for all values of the parameters; we have further results for the line graphs of multipartite graphs, for example, and see also [KMR04,KMR]. However, codes from other graphs (e.g. Paley graphs, see [KL]) or from designs from finite geometries (see [KMMb] and [KMMa] where the notion of partial PD-sets is introduced) do not have PD-sets as the parameters grow beyond a certain number, since the bound of Result 1 is too large for the group order.

References

[AK92] 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).

[BC94] Wieb Bosma and John Cannon. *Handbook of Magma Functions*. Department of Mathematics, University of Sydney, November 1994. http://magma.maths.usyd.edu.au/magma/.

[Gor82] D. M. Gordon. Minimal permutation sets for decoding the binary Golay codes. *IEEE Trans. Inform. Theory*, 28:541–543, 1982.

[Huf98] W. Cary Huffman. Codes and groups. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 1345–1440. Amsterdam: Elsevier, 1998. Volume 2, Part 2, Chapter 17.

[KL] J. D. Key and J. Limbupasiriporn. Permutation decoding of codes from Paley graphs. *Congr. Numer.*, 170:143–155, 2004.

[KMMa] J. D. Key, T. P. McDonough, and V. C. Mavron. Information sets partial permutation decoding of codes from finite geometries. *Finite Fields Appl.*, To appear.

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

[KMR] J. D. Key, J. Moori, and B. G. Rodrigues. Permutation decoding of binary codes from graphs on triples. *Ars Combin.*, To appear.

[KMR04] J. D. Key, J. Moori, and B. G. Rodrigues. Permutation decoding for binary codes from triangular graphs. *European J. Combin.*, 25:113–123, 2004.

[KS] J. D. Key and P. Seneviratne. Permutation decoding of binary codes from lattice graphs. *Discrete Math.* (Special issue dedicated to J. Seberry), To appear.

[Mac64] F. J. MacWilliams. Permutation decoding of systematic codes. *Bell System Tech. J.*, 43:485–505, 1964.

[MS83] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1983.

[Sch64] J. Schönheim. On coverings. *Pacific J. Math.*, 14:1405–1411, 1964.