Discrete Applied Mathematics 158 (2010) 1807–1815

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Codes from lattice and related graphs, and permutation decoding

J.D. Key [a,*], B.G. Rodrigues [b]

[a] School of Mathematical Sciences, University of KwaZulu-Natal, Pietermaritzburg 3209, South Africa

[b] School of Mathematical Sciences, University of KwaZulu-Natal, Durban 4041, South Africa

ARTICLE INFO

Article history:
Received 17 March 2009
Received in revised form 30 June 2010
Accepted 5 July 2010
Available online 24 July 2010

Keywords:
Codes
Line graphs
Lattice graphs
Permutation decoding

ABSTRACT

Codes of length n^2 and dimension $2n-1$ or $2n-2$ over the field $\mathbb{F}_p$, for any prime p, that can be obtained from designs associated with the complete bipartite graph $K_{n,n}$ and its line graph, the lattice graph, are examined. The parameters of the codes for all primes are obtained and PD-sets are found for full permutation decoding for all integers $n \geq 3$.

1. Introduction

Codes obtained from an adjacency matrix of the line graph of a graph are closely related to codes from an incidence matrix of the original graph, and are, in fact, subcodes of this in the binary case. The codes from the incidence matrix of a graph, in case the graph has some regularity, have been found, in many cases, to have rank either the number v of vertices, or $v-1$, in particular the latter in the binary case: see [6,7,13]. Furthermore, their minimum weight is often the valency of the graph, and the minimum words simply the scalar multiples of the rows of the matrix. Thus it makes sense to look at these codes in conjunction with the codes from the adjacency matrix of the line graph, and codes associated with this adjacency matrix. In addition, binary codes from some line graphs have been found to be good candidates for permutation decoding: see [6,12,16,14,15,22].

In this paper we consider the lattice graph, where, for any n, the lattice graph is defined to be the line graph of the complete bipartite graph $K_{n,n}$. It is a strongly regular graph on $v = n^2$ vertices. The binary codes from the span of adjacency matrices of lattice graphs have been examined by various authors: see [3,4,9,23], and with a view to permutation decoding in [16,22]. We extend these results now to p-ary codes for all primes p; the p-rank of these and related graphs was examined in [20]. Taking the complete bipartite graph $K_{n,n}$ to have vertices from two disjoint sets $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_n\}$, the vertices of the lattice graph L_n are the n^2 pairs (a_i, b_j) with (a_i, b_j) and (a_k, b_m) adjacent if $i = k$ or $j = m$. If A_n denotes an adjacency matrix for L_n then $B_n = J - I - A_n$, where J is the all-one and I the identity $n^2 \times n^2$ matrix, will be an adjacency matrix for the graph $\widetilde{L}_n$ on the same vertices with adjacency defined by (a_i, b_j) adjacent to (a_k, b_m) if $i \neq k, j \neq m$. We examine the neighbourhood designs and p-ary codes, for any prime p, from A_n, $A_n + I$, B_n, $B_n + I$ and show that all the codes are inside the code or its dual obtained from an incidence matrix M_n for the graph $K_{n,n}$, noting that $M_n^T M_n = A_n + 2I$. Thus the codes from the row span of M_n, and some subcodes of codimension 1, are the ones that we examine for permutation decoding. Note that $A_n + I$ and $B_n + I$ are adjacency matrices for the graphs L_n^R and $\widetilde{L}_n^R$ obtained from L_n and $\widetilde{L}_n$, respectively, by including all loops, and thus referred to as reflexive graphs.

* Corresponding author.
E-mail address: keyj@ces.clemson.edu (J.D. Key).

0166-218X/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.dam.2010.07.003

We summarize our results below in a theorem; the specific results relating to the codes from $L_n, \tilde{L}_n, L_n^R, \tilde{L}_n^R$ are given as propositions and lemmas in the following sections. The notation is as explained in the paragraph above.

Theorem 1. *Let C_n be the p-ary code of an incidence matrix M_n for the complete bipartite graph $K_{n,n}$ where p is a prime and $n \geq 3$. The vertex set of $K_{n,n}$ is $A \cup B$, where $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_n\}$ and the edges are the pairs (a_i, b_j) where $a_i \in A$, $b_j \in B$. Then C_n is a $[n^2, 2n-1, n]_p$ code with information set*

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

For $n \geq 3$, the minimum words are the scalar multiples of the rows r_i of M_n, and $\mathrm{Aut}(C_n) = S_n \wr S_2$, where $\mathrm{Aut}(C_n)$ denotes the automorphism group of C_n. The set

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

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

Let $E_n = \langle r_i - r_j \mid r_i, r_j$ rows of $M_n\rangle$. Then for $n \geq 3$, E_n is an $[n^2, 2n-2, 2n-2]_p$ code and the minimum words are the scalar multiples of the $r_i - r_j$. Further, $\mathcal{I}_n^* = \mathcal{I}_n \setminus \{(a_1, b_n)\}$ is an information set, and

$$S^* = \{(t_{n,i}, t_{n,j}) \mid 1 \leq i, j \leq n\},$$

a PD-set of size n^2 for E_n using $\mathcal{I}_n^*$.

The p-ary codes from $L_n, \widetilde{L}_n, L_n^R, \widetilde{L}_n^R$ are either $\mathbb{F}_p^{n^2}$, $\langle \boldsymbol{\jmath} \rangle^\perp$, $C_n^\perp$, $E_n^\perp$, C_n or E_n.

We note that the binary code from the lattice graph is E_n: see Result 2 in Section 2.

The proof of the theorem follows from propositions and lemmas in the following sections. The full details about the codes from $L_n, \widetilde{L}_n, L_n^R, \widetilde{L}_n^R$ are in Proposition 8. Background definitions are given in Section 2, and notation for the graphs, designs and codes that we consider here is given in Section 3. Computations leading to these results were all done with Magma [5,2].

2. Background and terminology

Notation for designs and codes is as in [1, Chapters 1,2]. An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{J})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{J}$ is a t-(v, k, λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. The design is *symmetric* if it has the same number of points and blocks. The *code* $C_F(\mathcal{D})$ of *the design* $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F. If $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the *incidence vector* of $\mathcal{Q}$ by $v^{\mathcal{Q}}$, and if $\mathcal{Q} = \{P\}$ where $P \in \mathcal{P}$, then we will write v^P instead of $v^{\{P\}}$. Thus $C_F(\mathcal{D}) = \langle v^B \mid B \in \mathcal{B}\rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F. For any $w \in F^{\mathcal{P}}$ and $P \in \mathcal{P}$, $w(P)$ denotes the value of w at P. If $F = \mathbb{F}_p$ then the *p-rank* of the design, written $\mathrm{rank}_p(\mathcal{D})$, is the dimension of its code $C_F(\mathcal{D})$, which we usually write as $C_p(\mathcal{D})$.

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*, $\mathrm{wt}(v)$, of a vector v is the number of non-zero coordinate entries. 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. $C^\perp = \{v \in F^n | (v, c) = 0$ for all $c \in C\}$. A code is *self-orthogonal* if $C \subseteq C^\perp$. A self-orthogonal binary code is *doubly-even* if all the codewords have weight divisible by 4. If $C = C_p(\mathcal{D})$, where $\mathcal{D}$ is a design, then $C \cap C^\perp$ is the *hull* of $\mathcal{D}$ at p, or simply the *hull* of $\mathcal{D}$ or C if p and $\mathcal{D}$ are clear from the context. A *check matrix* for C is a generator matrix for $C^\perp$. The *all-one vector* will be denoted by $\boldsymbol{\jmath}$, and is the vector with all entries equal to 1. 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 $\mathrm{Aut}(C)$. 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 first k coordinates in the standard form are the *information symbols* and the last $n-k$ coordinates are the *check symbols*.

The *graphs*, $\Gamma = (V, E)$ with vertex set V and edge set E, discussed here are undirected with no loops, apart from the case where *all* loops are included, in which case the graph is called *reflexive*. The *order* of $\Gamma = (V, E)$ is $|V|$. A graph is *regular* if all the vertices have the same valency. An *adjacency matrix* A of a graph of order $|V| = n$ is an $n \times n$ matrix with entries a_{ij} such that $a_{ij} = 1$ if vertices v_i and v_j are adjacent, and $a_{ij} = 0$ otherwise. 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 the 1-$(|E|, k, 2)$ design with incidence matrix B is called the *incidence design* of Γ. 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. 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 Γ share a vertex in Γ. A *strongly regular graph* Γ of type (n, k, λ, μ) is a regular graph on $n = |V|$ vertices, with valency k which is such that any two adjacent vertices are together adjacent to λ vertices and any two non-adjacent vertices are together adjacent to μ vertices.

The *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, has for its 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 $(n^2, 2(n-1), n-2, 2)$.