Properties and Parameters of Codes from Line Graphs of Circulant Graphs

Pani Seneviratne
Department of Mathematics, Texas A&M University-Commerce,
P.O. Box 3011, Commerce, TX 75429-3011
padmapani.seneviratne@tamuc.edu

Jennifer D. Melendez
Department of Mathematics, Texas A&M University-Commerce,
P.O. Box 3011, Commerce, TX 75429-3011
jmelendez5@leomail.tamuc.edu

Alexander N. Westbrooks,
Department of Mathematics, Texas A&M University-Commerce,
P.O. Box 3011, Commerce, TX 75429-3011
awestbrooks@leomail.tamuc.edu

Abstract

Linear codes from neighborhood designs of strongly regular graphs such as triangular, lattice and Paley graphs have been extensively studied over the past decade. Most of these families of graphs are line graphs of a much larger class known as circulant graphs, $\Gamma_n(S)$. In this article we extend earlier results to obtain properties and parameters of binary codes $C_n(S)$ from neighborhood designs of line graphs of circulant graphs.

1 Introduction

Circulant graphs $\Gamma_n(S)$ are a well known family of graphs. They are examples of vertex transitive graphs and in fact automorphism groups of these graphs contain the cyclic group C_n as a subgroup acting sharply transitively on the vertices. Many important classes of graphs belongs to the family of circulant graphs.

Linear codes obtained from the row span of adjacency matrices of graphs were extensively studied over the last decade. These types of graph based codes were used as candidates for permutation decoding. In [9] and [10], linear codes obtained from triangular and square lattice graphs and further in [7], codes from line graphs of Paley graphs were studied. All of these families were examples

JCMCC 114 (2020), pp.353-360

of line graphs of circulant graphs. Properties of these classes of codes were independently studied of each other.

In this work we generalize the work done in [9, 10, 7] to obtain a unified formula for code parameters of line graphs of circulant graphs $L\Gamma_n(S)$. We show that parameters of these codes only depend on the number of vertices n of $\Gamma_n(S)$ and the defining set S.

The article is arranged as follows: In Section 2 we provide background material on codes, designs and graphs. We use Section 3 to define linear codes from line graphs of circulant codes and to derive their parameters and we discuss properties of these codes in Section 4.

2 Background

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, 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 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. Thus $C_F = \langle v^B \,|\, B \in \mathcal{B} \rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F.

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 of a vector 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 complement 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 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 C is an isomorphism from C to C. The automorphism group will be denoted by $aut(C)$. Any code is isomorphic to a code with generator matrix in so-called 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.

The graphs, $G = (V, E)$ with vertex set V and edge set E, discussed here are undirected with no loops. A graph is regular if all the vertices have the same valency. The line graph of a graph G is obtained by associating a vertex with each edge of the graph and connecting two vertices with an edge if and only if the corresponding edges of G have a vertex in common. The adjacency matrix A of a graph of order 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.

3 Codes from line graphs of circulant graphs

In this Section we define circulant graphs, $\Gamma_n(S)$ and list their properties. We define linear codes associated with line graphs $L\Gamma_n(S)$ of circulant graphs and give important examples from this class. Further, we derive code parameters for this particular class of codes. Definition, properties and examples of circulant graphs are found in [3].

Definition 1 *The circulant graph $\Gamma_n(S)$ is the graph with the vertex set $V = \{0, 1, 2, \ldots, n-1\} \subseteq \mathbb{Z}$ and any two vertices x and y are adjacent if and only if $|x-y|_n \in S$, where $S \subseteq V^* = \backslash\{0\}$ and*

$$|a|_n = \begin{cases} a & \text{if } 0 \leq a \leq n/2 \\ n-a & \text{if } n/2 < a < n \end{cases}$$

Suppose $S = \{a_1, a_2, \ldots, a_k\} \subseteq V^*$ then we define $gcd(n, S) = gcd(n, a_1, \ldots, a_k)$ for our convenience. The following properties of circulant graphs are well known.

Proposition 2 *Let $\Gamma_n(S)$ denote the circulant graph with the defining set $S = \{a_1, a_2, \ldots, a_k\}$. Then*

- *$\Gamma_n(S)$ is connected if and only if $gcd(n, S) = 1$.*
- *If $gcd(n, S) = d$ then $\Gamma_n(S)$ is the disjoint union of d copies of $\Gamma_{\frac{n}{d}}(\frac{a_1}{d}, \ldots, \frac{a_k}{d})$.*
- *Circulant graphs are examples of Cayley graphs.*
- *$\Gamma_n(S)$ is vertex transitive.*

The class of circulant graphs consists of many important families of graphs. We list three examples of strongly regular graphs [4] that have been studied in coding theory context.

Example 3 *Let $\Gamma_n(S)$ denote the circulant graph and $L\Gamma_n(S)$ denote the line graph of $\Gamma_n(S)$:*

1. *When $S = \{1, 2, \ldots, \lfloor n/2 \rfloor\}$, $\Gamma_n(S)$ is the complete graph and $L\Gamma_n(S)$ is the triangular graph.*
2. *When $S = \{1, 3, \ldots, 2\lfloor n/2 \rfloor + 1\}$, $\Gamma_n(S)$ is the complete bipartite graph and $L\Gamma_n(S)$ is the square lattice graph.*
3. *When $n \equiv 1(mod 4)$ and $S = \{x^2 : x \in \mathbb{Z}_n\}$ then $\Gamma_n(S)$ is the Paley graph.*

We define the set of vertices of $L\Gamma_n(S)$ to be

$$\mathcal{P} = \{\{x, y\} : |x-y|_n \in S, 1 \leq x, y \leq n\}.$$

The 1-design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ will have for point set $\mathcal{P}$ and for each point $\{x, y\} \in \mathcal{P}$, a block which we denote by $\overline{\{x, y\}}$ is defined in the following way:

$$\overline{\{x, y\}} = \{\{x, z\} :| x - z |\in S \text{ and } z \neq y\} \cup \{\{y, z\} :| y - z |\in S \text{ and } z \neq x\}.$$

The incidence vector of the block $\overline{\{x,y\}}$ is

$$v^{\overline{\{x,y\}}} = \sum_{|x-z|\in S} v^{\{x,z\}} + \sum_{|y-z|\in S} v^{\{y,z\}}.$$

where, as usual with the notation from [1], the incidence vector of the subset $X \subseteq \mathcal{P}$, is denoted by v^X. Further, if a, b, c are distinct integers in S so that $\{a,b\}$, $\{b,c\}$ and $\{a,c\} \in \mathcal{P}$, we write

$$v^{\overline{\{a,b,c\}}} = v^{\{a,b\}} + v^{\{b,c\}} + v^{\{a,c\}}$$

to denote this vector of weight 3 in the vector space spanned by the incident vectors. Also note that for distinct a, b and c,

$$v^{\overline{\{a,b\}}} + v^{\overline{\{b,c\}}} = v^{\overline{\{a,c\}}}$$

To avoid trivial cases we take $n \geq 4$. Then in all the following $C_n(S)$ will denote the binary code of $\mathcal{D}$ and of the span of the row space of an adjacency matrix of $L\Gamma_n(S)$.

The number of vertices of $L\Gamma_n(S)$ only depend on cardinality of the defining set S and whether the element $\frac{n}{2}$ belongs to S or not. If $\frac{n}{2} \notin S$ then the number of vertices of $L\Gamma_n(S)$ is $n|S|$ and if $\frac{n}{2} \in S$ then the number of vertices is $\frac{n}{2}(2|S|-1)$. Since the length of the code $C_n(S)$ is $|V(L\Gamma_n(S))|$ we have the following result.

Proposition 4 *$C_n(S)$ has length $n|S|$ if $\frac{n}{2} \notin S$ and length $\frac{n}{2}(2|S|-1)$ if $\frac{n}{2} \in S$.*

We will use following results in order to determine the dimension of $C_n(S)$ codes. The first result is due to Björner and Karlander [2] who determined dimensions of linear codes obtained from incidence designs of connected graphs.

Result 5 *Let $\Gamma = (V,E)$ be a connected graph, B an incidence matrix for Γ, and $C_2(B)$ the row-span of B over $\mathbb{F}_2$. Then $dim(C_2(B)) = |V| - 1$.*

Dankelmann, Key, and Rodrigues [5] used Result 5 to show that dimension of binary codes from a neighborhood design of a line graph of a connected graph only depends on the cardinality of the vertex set of the resulting graph. Further, they obtained minimum distances of such codes.

Result 6 *Let $\Gamma = (V,E)$ be a k-regular connected graph with $|V| \geq 4$. Let A be the adjacency matrix of the line graph $L\Gamma$. If V is odd then $C_2(A)$ has dimension $|V|-1$ and minimum distance k and if V is even then $C_2(A)$ has dimension $|V|-2$ and minimum distance $2k-2$.*

Notation

Let $n = 2^\alpha(1+2\beta) \geq 4$ and let $f(\alpha, S) = \left\lceil \frac{gcd(S) \bmod (2^\alpha)}{2^\alpha} \right\rceil$. Suppose $S = \{a_1, a_2, \ldots, a_l\}$ then define $gcd(n,S) = gcd(n, a_1, a_2, \ldots, a_l)$ and let $D = S \cup \{n\}$.

Next we give a unified formula for the dimension of $C_n(S)$ codes and the dimension does not depend on whether $n/2 \in S$ or not.

Proposition 7 *The dimension of the code $C_n(S)$ is $n-\frac{2\cdot gcd(n,S)}{(2-f(\alpha,D))}$ for all $n \geq 4$.*

Proof. When $n = 2^\alpha(1+2\beta)$ is odd, we have $\alpha = 0$ and hence $f(\alpha, S) = 0$. If $gcd(n, S) = 1$, graphs $\Gamma_n(S)$ are connected and we can apply Result 6 to get $dim(C_n(S)) = n-1$. Suppose $gcd(n, S) = d$ then $\Gamma_n(S)$ is a disjoint union of d circulant graphs $\Gamma_{\frac{n}{d}}(\frac{a_1}{d}, \frac{a_2}{d}, \dots, \frac{a_m}{d})$. Therefore the line graph $L\Gamma_n(S)$ is disjoint and the adjacency matrix A is a diagonal block matrix of the form.

$$A = \begin{bmatrix} A_1 & 0 & 0 & \dots & 0 \\ 0 & A_2 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & A_d \end{bmatrix} \tag{1}$$

Each component adjacency matrix A_i, $1 \leq i \leq d$ has rank $\frac{n}{d}-1$ and therefore A has rank $n-d = n - gcd(n, S)$.

When n is even we have $\alpha \neq 0$. If $gcd(n, S) = 1$ then $\Gamma_n(S)$ is connected and has even number of vertices and $f(\alpha, S) = 1$. By Result 6, $dim(C_n(S)) = n-2$. If $gcd(n, S) = 2^\alpha$ then we have $f(\alpha, S) = 0$ and $\Gamma_n(S)$ is isomorphic to 2^α copies of circulant graphs with $\frac{n}{2^\alpha}$ vertices. The adjacency matrix A has the same form as in Equation 1 with each component matrix having rank $\frac{n}{2^\alpha} - 1$. Therefore $dim(C_n(S)) = n - 2^\alpha$. If $gcd(n, S) = d \neq 2^\alpha$ we get $f(\alpha, S) = 1$ and $\Gamma_n(S)$ is isomorphic to d disjoint union of circulant graphs with an even number of vertices. By Result 6 and Equation 1 we get $dim(C_n(S)) = n - 2d$.

■

The minimum distance of these codes depend on whether $n/2 \in S$ or not, contrary to the dimension.

Proposition 8 *The minimum distance of $C_n(S)$ codes is $2+2(1+f(\alpha, S))(|S|-1)$ if $n/2 \notin S$ and $4(|S|-1)$ otherwise.*

Proof. When $n = 2^\alpha(1+2\beta)$ is odd, we have $\alpha = 0$ and $f(\alpha, S) = 0$. If $gcd(n, S) = 1$ then graphs $\Gamma_n(S)$ are connected with valency $2|S|$. By Result 6, minimum distance, $d(C_n(S))$, is equal to $2|S|$. If $gcd(n, S) = d$ then $\Gamma_n(S)$ is isomorphic to d disjoint union of circulant graphs Γ_i. But cardinality of the connection set in each of these graphs is equal to $|S|$. Therefore the vectors from row span of each component A_i in Equation 1 will have minimum weight $2|S|$.

When n is even and $\frac{n}{2} \in S$ then $\Gamma_n(S)$ is regular with valency $2|S|-1$, By Result 6, $d(C_n(S)) = 2(2|S|-1)-2 = 4(|S|-1)$. If $\frac{n}{2} \notin S$ then $f(\alpha, S) = 1$ and $\Gamma_n(S)$ is regular with valency $2|S|$. Therefore $d(C_n(S)) = 2(2|S|)-2 = 4|S|-2$.

■

Now, we list some important examples of codes for different values of n and S. All the listed codes are optimal when compared to parameters of codes in the code tables [8], that is, they have the maximum minimum distance for a given length n and dimension k.

n	S	$C_n(S)$	Type
6	$\{2,3\}$	$[9,4,4]$	two-weight
6	$\{1,2,3\}$	$[15,4,8]$	simplex code
8	$\{1,2,3,4\}$	$[28,6,12]$	two-weight
8	$\{2,3,4\}$	$[20,6,8]$	optimal
10	$\{1,2,3,4,5\}$	$[45,8,16]$	two-weight
12	$\{1,2,3,4,5,6\}$	$[66,10,20]$	three-weight

4 Properties of $C_n(S)$ codes

We will study properties of $C_n(S)$ codes in this Section. We find spanning sets for these codes for particular values of n and S, determine information sets and bases of minimum weight vectors. Moreover, we derive self-orthogonal codes from $L\Gamma_n(S)$ graphs by selecting appropriate defining sets.

Lemma 9 *Let A be the adjacency matrix of the circulant graph $\Gamma(n, S)$ and let $det(A)$ denote the determinant of A. Then $det(A) = 0(mod 2)$, when $\mid S \mid$ is even.*

Proof. The determinant of any $n \times n$ circulant matrix A with the first row $(a_0, a_1, a_2, \ldots, a_{n-1})$ is given by the formula [6]:

$$det(A) = \prod_{j=0}^{n-1} \left(a_0 + a_1\zeta^j + a_2\zeta^{2j} + \cdots + a_{n-1}\zeta^{h(n-1)}\right) \tag{2}$$

where $\zeta = e^{2\pi n/n}$ is a primitive n-th root of unity. We can separate the first term of the product in equation 2 in the following way.

$$det(A) = (a_0 + a_1 + a_2 + \cdots + a_{n-1}) \prod_{j=1}^{n-1} \left(a_0 + a_1\zeta^j + a_2\zeta^{2j} + \cdots + a_{n-1}\zeta^{h(n-1)}\right)$$

Since A is an adjacency matrix of a graph $a_0 = 0$ and $\sum_{i=0}^{n-1} a_i = 2 \mid S \mid$, we have $(a_0 + a_1 + a_2 + \cdots + a_{n-1}) = 0 \,(\mathrm{mod}\, 2)$ and hence $det(A) = 0$. ■

We know that from Section 3 that code parameters of $C_n(S)$ codes depend on the defining set S of $\Gamma_n(S)$. When S only contain the element $\frac{n}{2} \in \mathbb{Z}_n$ the resulting code is a trivial code.

Lemma 10 *Let $S = \{\frac{n}{2}\}$. Then $C(n, S)$ is the trivial $[\frac{n}{2}, 0, \frac{n}{2}]$ code for even values of n.*

Proof. When $S = \{\frac{n}{2}\}$, $\Gamma(n, S)$ is the disjoint union of $n/2$ path graphs, which are disconnected. Therefore the line graph $L(\Gamma(n, S))$ is an isolated graph consisting of $n/2$ vertices without any edges. Hence the adjacency matrix of this graph is the zero matrix and the result follows. ■

It is sometimes important to find a spanning set for a vector space that describes the whole space. Similarly, for codes if we know a spanning set, then we can use that set to generate all the code words. This helps to reduce the computational complexity of algorithms associated with encoding and decoding.

Proposition 11 *When $\alpha \in S$ and $gcd(n, S) = 1$, the set of $n-1$ vectors $\mathcal{B} = \left\{ v^{\overline{\{i,i+\alpha\}}} : 0 \leq i \leq n-2 \right\}$ is a spanning set for $C_n(S)$.*

Proof. It is easy to see that any vector in $C_n(S)$ of the form $v^{\overline{\{i,i+\alpha\}}}$ is in $\mathcal{B}$ for $0 \leq i \leq n-2$. Next, let $\{i, j\} \in \mathcal{P}$, where $|i-j|_n \neq \alpha$. Then

$$v^{\overline{\{i,j\}}} = v^{\overline{\{i,i+\alpha\}}} + v^{\overline{\{i+1,i+1+\alpha\}}} + \ldots + v^{\overline{\{j-2,j-1\}}} + v^{\overline{\{j-1,j\}}}.$$

Therefore, $v^{\overline{\{i,j\}}} \in span(\mathcal{B})$.

■

The following result follows from Propositions 7 and 11.

Corollary 12 *$C(n, S)$ has a basis of minimum vectors whenever $gcd(n, S) = 1$.*

Corollary 13 *The set of points $\mathcal{I} = \{\{i, i+\alpha\} : 0 \leq i \leq n-2\}$ is an information set for the code $C(n, S)$ whenever $\alpha \in S$ and $gcd(n, S) = 1$,*

Proof. Arrange the points $\mathcal{P}$ so that the first $n-1$ points are $\{\{i, i+\alpha\} : 0 \leq i \leq n-2\}$ followed by the remaining points. Similarly, arrange the incidence vectors that correspond with the rows of the generator matrix in the same order. Then by row reduction we get the generator matrix into standard form $[I|A]$. ■

Lemma 14 *When $n = 4l$ and $S = \{2k \mid 1 \leq k \leq n/4\}$ then $L(\Gamma(n, S))$ is a $\langle v = 2\binom{n/2}{2}, k = n-4, \lambda = \frac{n-4}{2}, \mu = \{0, 4\}\rangle$ graph.*

Proof. When $n = 4l$ and $S = \{2k \mid 1 \leq k \leq n/4\}$ then $gcd(n, S) = 2$ and by Proposition 2, $\Gamma_n(S)$ is the distinct union of 2 copies of $\Gamma_{2l}(\{1, 2, \ldots, l\})$. But $\Gamma_{2l}(\{1, 2, \ldots, l\})$ is a complete graph on $2l$ vertices. Therefore, $\Gamma_n(S)$ is the union of two copies of complete graphs of $2l$ vertices. The line graph of a complete graph on n vertices is a triangular graph with parameters $\langle v = \binom{n}{2}, k = 2(n-1), \lambda = n-1, \mu = 4\rangle$. Since, we have a disjoint union of graphs, the line graph is also disjoint. Hence, the resulting graph has parameters, $v = 2\binom{2l}{2}, k = 4l-4, \lambda = 2l-2, \mu = \{0, 4\}\rangle$. ■

A linear code C is called a self-orthogonal code, if the dual code $C^{\perp} \subseteq C$. We can use the above Lemma to generate self-orthogonal codes from $L\Gamma_n(S)$ graphs.

Theorem 15 *Let $S = \{2k \mid 1 \leq k \leq n/4\}$ and $C(n, S)$ be the binary code from $L(\Gamma(n, S))$. Then $C(n, S)$ is self-orthogonal when $n = 4l$.*

roof. When $n = 4l$ and $S = \{2k \mid 1 \leq k \leq n/4\}$, any two vertices will meet ther in $\lambda = \frac{n-4}{2}$ or $\mu = \{0, 4\}$ number of vertices. Hence, any two incidence ectors will intersect in $\frac{n-4}{2}$, 0 or 4 points. But, since $n = 4l$, we have this value qual to zero modulo 2. Therefore, the inner product of any incident vector ith another vector is zero and the result follows. ■

Acknowledgments

his material is based upon work supported by the National Research Experince for Undergraduate Program (NREUP) of the Mathematical Association of merica funded by the NSF Grant DMS-1652506. The authors would like to hank the anonymous referees for their careful review and valuable comments nd suggestions.

References

[1] E. F. Assmus, Jr and J. D. Key. *Designs and their Codes.* (Cambridge Tracts in Mathematics, Vol. 103, Second printing with corrections, 1993).

[2] A. Björner and J. Karlander. The mod p rank of incidence matrices for connected uniform hyper- graphs. *European J. Combin.*, 14 (1993), 151–155.

[3] Z. R. Bogdanowicz. Pancyclicity of connected circulant graphs. *J. Graph Theory*, Vol. 22, 167–174 (1996).

[4] A. E. Brouwer, A. M. Cohen and A. Neumaier. Distance Regular Graphs. (*Springer-Verlag*, A Series of Modern Surveys in Mathematics).

[5] P. Dankelmann, J. D. Key, and B. G. Rodrigues. Codes from incidence matrices of graphs. *Des. Codes Cryptogr.* (2012) DOI 10. 1007/s10623-011-9594-x.

[6] P. J. Davis. Circulant Matrices. (*John Wiley and sons*, 1979).

[7] D. Ghinellie and J. D. Key. Codes from incidence matrices and line graphs of Paley graphs. *Adv. Math. Commun.* 5, no.1, (2011), 93–108.

[8] M. Grassl. Code Tables. `http://www.codetables.de`

[9] J. D. Key, J. Moori, and B. G. Rodrigues. Codes associated with triangular graphs, and permutation decoding. Int. J. Inf. and Coding Theory 13 (2010), 334–349.

[10] J. D. Key and P. Seneviratne. Binary codes from rectangular lattice graphs and permutation decoding. Discrete Math. 308 (2008), 2862–2867.