New Linear Codes of Dimensions 5 and 6 over GF(8)[1]

T. Aaron Gulliver [1]

Abstract

Let $[n, k, d; q]$-codes be linear codes of length n, dimension k and minimum Hamming distance d over $GF(q)$. Let $d_8(n, k)$ be the maximum possible minimum Hamming distance of a linear $[n, k, d; 8]$-code for given values of n and k. In this paper, twenty-two new linear codes over $GF(8)$ are constructed which improve the bounds on $d_8(n, k)$.

Keywords: linear codes over GF(8)

Let $GF(q)$ denote the Galois field of q elements, and let $V(n, q)$ denote the vector space of all ordered n-tuples over $GF(q)$. A linear code C of length n and dimension k over $GF(q)$ is a k-dimensional subspace of $V(n, q)$. Such a code is called an $[n, k, d; q]$- code if its minimum Hamming distance is d.

A central problem in coding theory is that of optimizing one of the parameters n, k and d for given values of the other two. Two versions are:

[1] This work was supported in part by the Natural Sciences and Engineering Research Council of Canada.

[2] T. Aaron Gulliver is with the Department of Electrical and Computer Engineering, University of Victoria, P.O. Box 3055, MS 8610, Victoria, B.C., Canada V8W 3P6, agullive@ece.uvic.ca

1. Find $d_q(n,k)$, the largest value of d for which there exists an $[n,k,d;q]$-code.

2. Find $n_q(k,d)$, the smallest value of n for which there exists an $[n,k,d;q]$-code.

For $k \leq 3$, $d_8(n,k)$ is known for all n, and for $k = 4$, most have been determined [1]. For $k \geq 5$, there are still many unknown values, and this paper considers codes with dimensions $k = 5 - 6$. Twenty-two codes are presented which improve the bounds on minimum distance.

A stochastic optimization algorithm is used in this paper for code construction. By restricting the search to a particular class of codes, and using this stochastic heuristic, good codes can be found with a reasonable amount of computational effort.

The next section describes the class codes considered in this paper, and Section 3 presents the search algorithm and results.

1 Quasi-cyclic Codes

A code C is said to be quasi-cyclic (QC) if a cyclic shift of any codeword by p positions is also a codeword in C. A cyclic code is a QC code with $p = 1$. The length n of a QC code is a multiple of p, i.e., $n = mp$. With a suitable permutation of coordinates, many QC codes can be characterized in terms of $(m \times m)$ circulant matrices. In this case, a QC code can be transformed into an equivalent code with generator matrix

$$G = [R_0;\ R_1;\ R_2;\ \ldots\ ;\ R_{p-1}], \tag{1}$$

where $R_i, i = 0, 1, \ldots, p-1$ is a circulant matrix of the form

$$R = \begin{bmatrix} r_0 & r_1 & r_2 & \cdots & r_{m-1} \\ r_{m-1} & r_0 & r_1 & \cdots & r_{m-2} \\ r_{m-2} & r_{m-1} & r_0 & \cdots & r_{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ r_1 & r_2 & r_3 & \cdots & r_0 \end{bmatrix}. \tag{2}$$

The algebra of $m \times m$ circulant matrices over $GF(q)$ is isomorphic to the algebra of polynomials in the ring $GF(q)[x]/(x^m - 1)$ if R is mapped onto the polynomial, $r(x) = r_0 + r_1x + r_2x^2 + \cdots + r_{m-1}x^{m-1}$, formed from the entries in the first row of R [5]. The $r_i(x)$ associated with a QC code are called the *defining polynomials* [3].

Let $\{b_i(x)\}$ be the set of all possible defining polynomials where $b_0(x)$ denotes the all-zero polynomial. The number of non-zero polynomials is $M = |\{b_i(x)\} \backslash \{b_0(x)\}|$. A subset of p of these polynomials

$$\{b_{j_0}(x), b_{j_1}(x), \cdots, b_{j_{p-1}}(x)\}, 1 \leq j_i \leq M,$$

($j_a \neq j_b$ when $a \neq b$) defines an $[mp, m]$ QC code.

The problem is to find the subset which gives the largest minimum distance, d. This is considered in the next section.

2 The Construction Algorithm

By imposing a structure on the codes being sought, the search space can be reduced. The stronger the structure is, the smaller the search problem is. There is a trade-off, because good codes may be missed if too much structure is imposed on the code. However, it is often the case that good codes have a lot of structure.

It is not necessary to check the weight of every codeword in a QC code in order to determine d. Only a subset, $N < M$, of the codewords need be considered since the Hamming weight of $i_t(x)b_s(x)$ mod $(x^m - 1)$ is equal to the weight of $i_t(x)\alpha x^l b_s(x)$ mod $(x^m - 1)$ for all $l \geq 0$ and $\alpha \in$GF$(q) \setminus \{0\}$. Note that this argument also applies to the set of defining polynomials. For example, if $q = 8$ and $m = 5$, this subset contains 937 defining polynomials, and with $m = 6$, 6257 polynomials.

To simplify the process of searching for good codes, the weights of the subset of codewords can be stored in an array, and a matrix, D, can be formed from the arrays for the subset of defining polynomials to be considered

$$D = \begin{array}{c|cccccc} & b_1(x) & b_2(x) & \cdots & b_s(x) & \cdots & b_y(x) \\ \hline i_1(x) & w_{11} & w_{12} & \cdots & w_{1s} & \cdots & w_{1y} \\ i_2(x) & w_{21} & w_{22} & \cdots & w_{2s} & \cdots & w_{2y} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ i_t(x) & w_{t1} & w_{t2} & \cdots & w_{ts} & \cdots & w_{ty} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ i_z(x) & w_{z1} & w_{z2} & \cdots & w_{zs} & \cdots & w_{zy}, \end{array}$$

where $i_t(x)$ is the tth information polynomial, $b_s(x)$ is the sth generator polynomial, and w_{ts} is the Hamming weight of $i_t(x)b_s(x)$ mod $(x^m - 1)$. Since $i_t(x)$ and $b_s(x)$ correspond to the same subset of defining polynomials, D is a square $(y = z = N)$, symmetric (by letting $i_t(x) = b_t(x)$ for all $1 \leq t \leq N$) matrix.

The complete weight distribution for a QC code composed of any set of $b_s(x)$ can be constructed from D. The search for a good code consists of finding p columns of D with a large row sum, since the weight of a minimum distance codeword must be contained in these sums.

Having decided on the values of m, and p (and thus also $n = mp$), the entries of the integer matrix D can be calculated and the problem formulated as a combinatorial optimization problem. Namely, find

$$\max_{S} \min_{1 \leq j \leq N} \sum_{s \in S} w_{j,s}, \qquad (3)$$

where $S \subseteq \{1, 2, \ldots, N\}$ and $|S| = p$.

The optimization method used in this work is a greedy local search algorithm, similar to that in [2] and [4]. The algorithm starts from a random initial solution and iterates through new solutions in a search for better codes. Each potential new solution differs only slightly from the previous solution. If a better minimum distance is found, this is chosen as the new solution. Otherwise, one of the potential solutions with the highest minimum distance is chosen randomly. To ensure that the search does not loop on a subset of solutions, recent solutions are stored in a so-called tabu list; and these are not allowed for a certain period of time.

Table 1: QC Codes Over GF(8) with $k = 5$ Which Improve the Lower Bounds on Minimum Distance

code	d	$r_i(x)$
(90,5)	72	116, 1033, 1436, 13, 11415, 1154, 12165, 1433, 1565, 11355, 176 13132, 1062, 11314, 1537, 11336, 1471, 11154
(95,5)	76	103, 1227, 12127, 11646, 104, 12364, 1321, 1757, 11765, 1057 12346, 1625, 11643, 1335, 11135, 126, 11572, 1115, 13135
(100,5)	80	11, 105, 1016, 13135, 1753, 12134, 103, 111, 11526, 1451, 13252 1167, 12176, 11656, 11647, 15432, 1757, 11447, 12625, 11727
(105,5)	85	1075, 1752, 102, 11233, 123, 1255, 1244, 13243, 12453, 1435 11254, 11372, 11657, 11737, 11645, 11612, 11143, 1726, 1137 1413, 1657
(110,5)	89	1522, 11226, 11426, 1647, 11217, 1057, 1622, 111, 1557, 1043 1154, 11656, 13254, 12174, 1762, 11416, 1517, 11762, 104 11447, 13252, 1365
(115,5)	93	1173, 1025, 11245, 17, 1, 11426, 1355, 11523, 12425, 157, 11233 1232, 1444, 11473, 11416, 16532, 1267, 13132, 171, 11435 11546, 14264, 13643
(120,5)	96	15, 144, 11546, 1517, 1762, 11175, 1644, 1577, 115, 13615, 11476 1552, 1321, 11145, 1622, 11463, 1415, 12156, 1373, 1714, 1163 1463, 1276, 11467
(125,5)	101	112, 11757, 1, 13, 14315, 1132, 104, 1131, 11, 1077, 13526, 12373 1315, 11456, 1745, 11756, 13742, 1451, 12542, 11622, 11567 13174, 1735, 11676, 1526
(130,5)	106	1016, 1, 1416, 15, 11372, 12316, 1114, 12726, 1122, 1445, 13135 141, 1732, 12172, 11157, 137, 11643, 1744, 11747, 1667, 11723 12432, 11215, 1364, 166, 14374

The codes obtained are listed in Tables 1 and 2. The defining polynomials are listed with the lowest degree coefficient on the left, i.e., 4321 corresponds to the polynomial $x^3 + \alpha x^2 + \alpha^2 x + \alpha^3$, where α is a root of the binary primitive polynomial $x^3 + x + 1$.

References

[1] A.E. Brouwer, "Bounds on the size of linear codes," in *Handbook of Coding Theory*, eds. V. Pless et al., Elsevier, Amsterdam, 1998, and Linear code bound (server), Eindhoven University of Technology, The Netherlands, http://www.win.tue.nl/win/math/dw/voorlincod.html.

[2] R. N. Daskalov and T. A. Gulliver, "New good quasi-cyclic

Table 2: QC Codes Over GF(8) with $k = 6$ Which Improve the Lower Bounds on Minimum Distance

code	d	$r_i(x)$
(42,6)	30	111114, 13, 1171, 11656, 12431, 1534, 1541
(48,6)	35	117, 1017, 14731, 14115, 1444, 14125, 13462, 13131
(54,6)	40	1445, 117435, 1174, 10154, 12515, 117414, 17362, 113613, 113412
(78,6)	59	115, 116, 12117, 10461, 12431, 1534, 1541, 13654, 14235, 13376 11134, 17547, 111762
(84,6)	64	115, 114, 11531, 10461, 12431, 1534, 1541, 13654, 14235, 13376 11134, 17547, 111762, 14562
(90,6)	69	114, 115, 11542, 10461, 12431, 1534, 1541, 13654, 14235, 13376 11134, 17547, 111762, 14562, 14463
(96,6)	74	11153, 13, 1171, 10461, 12431, 1534, 1541, 13654, 14235, 13376 111117, 17547, 111762, 14562, 14463, 1243
(102,6)	79	111114, 1453, 111226, 13117, 1565, 11177, 10745, 15743, 10547 15371, 1502, 10265, 17126, 12445, 14632, 17243, 11017
(108,6)	84	111112, 151, 12743, 10461, 12431, 1534, 1541, 13654, 14235 13376, 11134, 17547, 111762, 14562, 14463, 1243, 16736, 1021
(114,6)	89	1474, 16, 1053, 16522, 142173, 16652, 12565, 11536, 17467 11545, 14265, 113463, 12152, 11134, 124174, 127214, 113465 11612, 10623
(120,6)	94	111154, 16722, 1171, 10461, 12431, 1534, 1541, 111157, 14235 13376, 11134, 17547, 111762, 14562, 14463, 1243, 16736, 1021 11274, 11655
(126,6)	99	11166, 13, 1171, 11156, 12431, 1534, 1541, 111453, 14235, 13376 11134, 17547, 111762, 14562, 14463, 1243, 16736, 1021, 11274 11655, 111235
(132,6)	104	101, 16, 102, 11472, 111423, 116473, 10222, 16677, 17475, 16265 12431, 121414, 127414, 111352, 111165, 1446, 116267, 1102 12663, 13475, 124 313, 17547

ternary and quaternary linear codes," *IEEE Trans. Inform. Theory*, vol. 43, pp.1647–1650, 1997.

[3] P.P. Greenough and R. Hill, "Optimal ternary quasi-cyclic codes," *Designs, Codes and Crypt.*, vol. 2, pp. 81-91, 1992.

[4] T.A. Gulliver and V.K. Bhargava, "Some best rate 1/p and rate (p-1)/p systematic quasi-cyclic codes over GF(3) and GF(4)," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1369–1374, July 1992.

[5] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Co., New York, NY, 1977.

4-Circulant Graphs

George J. Davis, Gayla S. Domke and Charles R. Garner, Jr.
Department of Mathematics and Statistics
Georgia State University, Atlanta, GA 30303

October 23, 2000

Abstract

A 4-regular graph G is called a 4-circulant if its adjacency matrix $A(G)$ is a circulant matrix. Because of the special structure of the eigenvalues of $A(G)$, the rank of such graphs is completely determined. We show how all disconnected 4-circulants are made up of connected 4-circulants and classify all connected 4-circulants as isomorphic to one of two basic types.

1 Introduction.

In this paper, we consider the class of graphs called circulant graphs. Let S be any subset of $\{1, 2, \ldots, n-1\}$ such that $S = -S \bmod n$. A graph G with vertex set $\{0, 1, 2, \ldots, n-1\}$ is called a *circulant graph* if two vertices i and j are adjacent if and only if $(i-j) \bmod n \in S$. The adjacency matrix $A(G)$ is a *circulant matrix*, i.e., $a_{i,j} = a_{i-1,j-1}$ with the subscript calculation done mod n. In other words, row $(i+1)$ of the matrix is a cyclic right shift one position from row (i).

The study of circulant graphs is an interesting blend of ideas and techniques from linear algebra, number theory, abstract algebra and graph theory. Our study of circulants began with our interest in the rank of $A(G)$ [1, 2, 3, 6, 9]. Much is known about the eigenvalues of the adjacency matrix of a graph in general [5] and circulants in particular [8] that this work is a natural extension.

In what follows, we consider circulant graphs where $|S| = 4$, i.e. the *4-circulant graphs.* Some elementary results reveal when such graphs are connected, and, if not, the number of isomorphic connected components. We provide these results in Section 2. The rank of $A(G)$ for connected circulants turns out to be determined by a formula which we develop in Section 3. Having settled the rank question, we turn to the underlying structure of connected 4-circulant graphs.

ARS COMBINATORIA 65(2002), pp. 97-110

In Section 4 we review the structure of connected 2- and 3-circulants and show how each connected 4-circulant is isomorphic to one of two basic types. In the final section we outline plans for the more general k-circulant case.

2 Connectivity Structure.

The first step in understanding circulant graphs is to understand their connectivity. A result of Broere [4] settles this issue.

Theorem 1 *Let G be a circulant graph with n vertices formed by $S = \{s_1, \ldots, s_k\}$. If $d = \gcd(s_1, \ldots, s_k, n)$, then G has d connected components each isomorphic to a circulant graph on $\frac{n}{d}$ vertices formed by $S' = \{\frac{s_1}{d}, \ldots, \frac{s_k}{d}\}$.*■

Thus, in what follows, we need only consider connected circulants.

For S to be a four-element subset of $\{0, 1, 2, ..., n-1\}$ such that $S = -S$ mod n, it is clear that S must have the form $S = \{a, b, n-b, n-a\}$,with $a \neq b$, $a < \frac{n}{2}$, $b < \frac{n}{2}$. We can then apply the above theorem to the specific 4-circulant case as follows.

Corollary 1 *Let $S = \{a, b, n-b, n-a\}$. If gcd$(a, b, n) = d$, then the circulant graph with n vertices formed by S has d components each isomorphic to the circulant graph on $\frac{n}{d}$ vertices formed by $S' = \{\frac{a}{d}, \frac{b}{d}, \frac{n-b}{d}, \frac{n-a}{d}\}$.* ■

It is clear from the above that although the set S has four elements, it is completely determined by the three values a, b and n. We therefore employ a compact notation for 4-circulant graphs. From now on, we denote the 4-circulant graph on n vertices formed by $S = \{a, b, n-b, n-a\}$ by $4C_n(a, b)$.

A simple example illustrates these ideas (see Figure 1). The figure represents $4C_{12}(2, 4)$. As the gcd(2,4,12) $= 2$, the graph is made up of two connected components, each isomorphic to $4C_6(1, 2)$. These connected components are shown in Figure 2.

3 Rank of $A(G)$.

The eigenvalue structure of circulant matrices is well known [8]. In fact, the p-th eigenvalue λ_p of $4C_n(a, b)$ is given by $\lambda_p = \omega^{ap} + \omega^{bp} + \omega^{(n-b)p} + \omega^{(n-a)p}$, where $\omega = e^{2\pi i/n}$. The number of distinct values of p for which $\lambda_p = 0$ is the dimension of the null space of $A(G)$, i.e. its nullity. Since the sum of

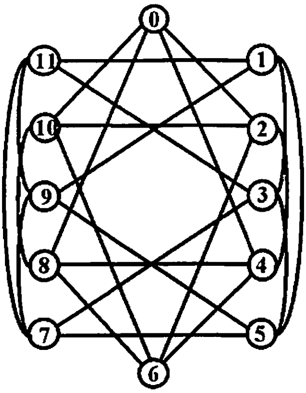

Figure 1: $4C_{12}(2,4)$.

the rank and nullity of a matrix is always equal to the number of columns in it, knowing the nullity uniquely determines the rank.

Exploring the equation of $\lambda_p = 0$, and the number of ways that it can be satisfied, carries us quickly into number theory. The following lemma on the solvability of equations will prove useful in this regard.

Lemma 1 *Let n be a positive integer, $m, k \in \mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$, and d =gcd(m, n). Then $mx \equiv k$ (mod n) has exactly d solutions in $\mathbf{Z}_n$ if and only if d divides k. Furthermore if d does not divide k, then $mx \equiv k$ (mod n) has no solutions in $\mathbf{Z}_n$.* ■

The next lemma gives the conditions under which an eigenvalue will be zero.

Lemma 2 *Let $G = 4C_n(a, b)$. Then the eigenvalue $\lambda_p = \omega^{ap} + \omega^{bp} + \omega^{(n-b)p} + \omega^{(n-a)p} = 0$ if and only if either $2(b-a)p = (2k+1)n$ or $2(n-b-a)p = (2k+1)n$ for some integer k.*

Proof: Suppose $G = 4C_n(a, b)$. Then the eigenvalue $\lambda_p = \omega^{ap} + \omega^{bp} + \omega^{(n-b)p} + \omega^{(n-a)p} = 0$ if and only if $\omega^{ap}(1 + \omega^{(b-a)p} + \omega^{(n-b-a)p} + \omega^{(n-2a)p}) = 0$. Since $\omega^{ap} \neq 0$, then

$$1 + \omega^{(b-a)p} + \omega^{(n-b-a)p} + \omega^{(n-2a)p} = 0. \tag{1}$$

Now, $\omega^k = \cos(\frac{2\pi k}{n}) + i \sin(\frac{2\pi k}{n})$. So, (1) holds if and only if

$$\cos(0) + \cos\frac{(b-a)p \cdot 2\pi}{n} + \cos\frac{(n-b-a)p \cdot 2\pi}{n} + \cos\frac{(n-2a)p \cdot 2\pi}{n} = 0 \tag{2}$$

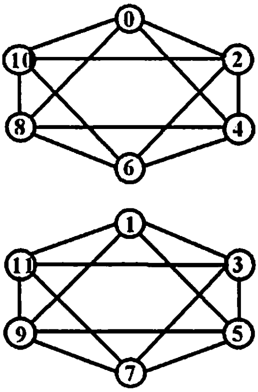

Figure 2: The two connected components of $4C_{12}(2,4)$.

and

$$\sin(0)+\sin\frac{(b-a)p\cdot 2\pi}{n}+\sin\frac{(n-b-a)p\cdot 2\pi}{n}+\sin\frac{(n-2a)p\cdot 2\pi}{n}=0. \quad (3)$$

Define $\alpha \equiv \frac{(b-a)p\cdot 2\pi}{n}$ and $\beta \equiv \frac{(n-b-a)p\cdot 2\pi}{n}$. Then, $\alpha+\beta = \frac{(n-2a)p\cdot 2\pi}{n}$. Hence, (2) and (3) become

$$\cos\alpha+\cos\beta+\cos(\alpha+\beta)=-1 \tag{4}$$

and

$$\sin\alpha+\sin\beta+\sin(\alpha+\beta)=0. \tag{5}$$

Now, from (5)

$$\begin{aligned}\sin\alpha+\sin\beta &= -\sin(\alpha+\beta)\\ \sin^2\alpha+2\sin\alpha\sin\beta+\sin^2\beta &= \sin^2(\alpha+\beta)\end{aligned}$$

$$\begin{aligned}(1-\cos^2\alpha)+2(\cos\alpha\cos\beta-\cos(\alpha+\beta))+(1-\cos^2\beta) &= \\ 1-\cos^2(\alpha+\beta) &\Rightarrow\end{aligned}$$

$$\begin{aligned}\cos^2(\alpha+\beta)-2\cos(\alpha+\beta)+1 &= \\ \cos^2\alpha-2\cos\alpha\cos\beta+\cos^2\beta &\Rightarrow\end{aligned}$$

$$(\cos(\alpha+\beta)-1)^2=(\cos\alpha-\cos\beta)^2$$

This means either

$$\cos(\alpha+\beta) - 1 = \cos\alpha - \cos\beta \tag{6}$$

or

$$\cos(\alpha+\beta) - 1 = -\cos\alpha + \cos\beta \tag{7}$$

Combining (6) and (4) we get

$$\begin{aligned} 2\cos\alpha + 2 &= 0 \\ \cos\alpha &= -1 \\ \alpha &= (2k+1)\pi \qquad \text{where } k \text{ is an integer} \end{aligned}$$

Hence,

$$\frac{(b-a)p \cdot 2\pi}{n} = (2k+1)\pi$$

or

$$2(b-a)p = (2k+1)n.$$

Similarly, combining (7) and (4) we get

$$2(n-b-a)p = (2k+1)n$$

and our result holds.■

As a first application of these properties, we show that 4-circulants on an odd number of vertices always have full rank.

Theorem 2 *Let n be odd and $G = 4C_n(a,b)$. Then rank$(A(G)) = n$.*

Proof: By Lemma 2, if n is odd, then in the equations

$$2(b-a)p = (2k+1)n \qquad \text{and} \qquad 2(n-b-a)p = (2k+1)n$$

the left hand sides are even while the right hand sides are odd. Since this can never happen, none of the eigenvalues can be 0. Therefore, rank$(G) = n$. ■

Combining these ideas with those of the connectivity of G, many "special case" type results can be generated. Typical of this kind of corollary is the following.

Corollary 2 *Let $n \equiv 2 \bmod 4$ and $G = 4C_n(a,b)$. If gcd$(n,a,b) = 2$, then rank$(G) = n$.*

Proof: By Corollary 1, G is isomorphic to two circulants on $\frac{n}{2}$ vertices, where $\frac{n}{2}$ is odd. Then by Theorem 2, they are each full rank.■

We now work toward a formula that will give the rank of any 4-circulant. The following is a necessary and sufficient condition for an eigenvalue to be zero.

Theorem 3 *Let n be even and $G = 4C_n(a,b)$. Then G has an eigenvalue $\lambda_p = 0$ if and only if d_1 =gcd$(b-a,n)$ divides $\frac{n}{2}$ or d_2 =gcd$(n-b-a,n)$ divides $\frac{n}{2}$*

Proof: If $G = 4C_n(a,b)$, then by Lemma 2, the eigenvalue, λ_p, of $A(G)$ equals 0 if and only if

$$2(b-a)p = (2k+1)n \qquad \text{or} \qquad 2(n-b-a)p = (2k+1)n.$$

This is equivalent to

$$(b-a)p = (2k+1)\frac{n}{2} = kn + \frac{n}{2} \equiv \frac{n}{2}(\text{mod} n) \tag{8}$$

or

$$(n-b-a)p = (2k+1)\frac{n}{2} = kn + \frac{n}{2} \equiv \frac{n}{2}(\text{mod} n). \tag{9}$$

By Lemma 1, if gcd$(b-a,n) = d_1$, then $(b-a)p \equiv \frac{n}{2}$ (mod n) has d_1 solutions if and only if d_1 divides $\frac{n}{2}$. Similarly, if gcd$(n-b-a,n) = d_2$, then $(n-b-a)p \equiv \frac{n}{2}$ (mod n) has d_2 solutions if and only if d_2 divides $\frac{n}{2}$.■

Knowing how many solutions exist for each congruence is only part of the story. To precisely determine the rank of $A(G)$, we need to know the number of distinct solutions to the simultaneous system of congruencies. We will need the following generalization of the Chinese Remainder Theorem.

Theorem 4 *(The Generalized Chinese Remainder Theorem) The system of congruencies*
$x \equiv c_1 \, mod \, m_1$
$x \equiv c_2 \, mod \, m_2$
$\vdots$
$x \equiv c_r \, mod \, m_r$
is solvable if and only if gcd(m_i, m_j) divides $c_i - c_j$ for every i andj wherei $\neq j$. If there is a solution, it is unique modulo lcm$(m_1, m_2, ..., m_r)$.■

The following corollary is a special case of the Chinese Remainder Theorem.

Corollary 3 *The system of congruencies*
$rx \equiv \frac{n}{2} \, \text{mod} \, n$
$sx \equiv \frac{n}{2} \, \text{mod} \, n$
for n even, has a solution if and only if gcd$(\frac{n}{d_1}, \frac{n}{d_2})$ divides $\frac{n(d_2-d_1)}{2d_1d_2}$, where d_1 =gcd$(r,\ n)$ and d_2 =gcd$(s,\ n)$. If the system is solvable, there are exactly gcd$(d_1,\ d_2) = d$ solutions.

Proof: Let $d_1 = \gcd(r, n)$ and $d_2 = \gcd(s, n)$. Then by Lemma 1, $rx \equiv \frac{n}{2} \bmod n$ is solvable if and only if d_1 divides $\frac{n}{2}$, and $sx \equiv \frac{n}{2} \bmod n$ is solvable if and only if d_2 divides $\frac{n}{2}$. If one congruence is not solvable, the system is not solvable. So assume that d_1 divides $\frac{n}{2}$ and d_2 divides $\frac{n}{2}$. The goal is to reduce the system of congruencies so that there are no coefficients for x. This will allow the use of Theorem 4.

The claim is that $\frac{n}{2d_1}$ is a solution to $rx \equiv \frac{n}{2} \bmod n$ and $\frac{n}{2d_2}$ is a solution to $sx \equiv \frac{n}{2} \bmod n$. For $\frac{n}{2d_1}$ to be a solution to $rx \equiv \frac{n}{2} \bmod n, n$ must divide $\frac{rn}{2d_1} - \frac{n}{2} = n(\frac{r-d_1}{2d_1})$. This will happen if and only if $\frac{r-d_1}{2d_1}$ is an integer. Thus the investigation turns to the nature of $\frac{r-d_1}{2d_1}$.

By factoring out the highest powers of 2 in n and r it is seen that $n = 2^{\nu}j$ and $r = 2^{\rho}k$, where j and k are odd. Then $d_1 = 2^{\min\{\nu,\rho\}}\gcd(j,k)$. Now since d_1 divides $\frac{n}{2}$, $2^{\min\{\nu,\rho\}}\gcd(j,k)$ divides $2^{\nu-1}j$. Clearly $\gcd(j,k)$ divides j, but since $2^{\min\{\nu,\rho\}}$ divides $2^{\nu-1}$ it must be that $\min\{\nu,\rho\} \leq \nu-1$, implying $\min\{\nu,\rho\} = \rho$. Thus $d_1 = 2^{\rho}\gcd(j,k)$. Also, since $d_1 = \gcd(n.r)$, there exists $q \in \mathbf{Z}$ such that $d_1q = r$. Thus $2^{\rho}\gcd(j,k)q = 2^{\rho}k$, which implies that $\gcd(j,k)q = k$. Therefore q must be odd since both k and $\gcd(j,k)$ are odd. Hence $q = 2m+1$, for some $m \in \mathbf{Z}$, so that $r = d_1(2m+1) = 2d_1m + d_1$, implying $2d_1m = r - d_1$. Therefore $\frac{r-d_1}{2d_1}$ is an integer. This establishes the claim that $\frac{n}{2d_1}$ is a solution to $rx \equiv \frac{n}{2} \bmod n$. Similarly, $\frac{n}{2d_2}$ is a solution to $sx \equiv \frac{n}{2} \bmod n$.

Since the particular solutions $\frac{n}{2d_1}$ and $\frac{n}{2d_2}$ are unique solutions modulo $\frac{n}{d_1}$ and $\frac{n}{d_2}$ respectively, to the original system, these congruencies are equivalent to the following reduced system

$x \equiv \frac{n}{2d_1} \bmod \frac{n}{d_1}$
$x \equiv \frac{n}{2d_2} \bmod \frac{n}{d_2}$.

Each of these reduced congruencies have only one solution modulo $\frac{n}{d_1}$ and $\frac{n}{d_2}$, respectively. On applying Theorem 4, the reduced system has a solution if and only if $\gcd(\frac{n}{d_1}, \frac{n}{d_2})$ divides $\frac{n}{2d_1} - \frac{n}{2d_2} = \frac{n(d_2-d_1)}{2d_1d_2}$, which implies that the original system has a solution if and only if $\gcd(\frac{n}{d_1}, \frac{n}{d_2})$ divides $\frac{n(d_2-d_1)}{2d_1d_2}$.

The number of solutions to the original system of congruencies is shown presently. Assume there is a solution to the reduced system. Then by Theorem 4, the solution is unique modulo $\mathrm{lcm}(\frac{n}{d_1}, \frac{n}{d_2}) = N$. If x_0 is the unique solution modulo N, the general solutions modulo n for the original congruencies are given by $x_0 + jN$, $j = 0, 1, ..., \frac{n}{N} - 1$. Thus, there are exactly $\frac{n}{N} = \frac{n}{\mathrm{lcm}(\frac{n}{d_1}, \frac{n}{d_2})} = \frac{n}{\frac{n}{\gcd(d_1,d_2)}} = \gcd(d_1, d_2) = d$ solutions. ■

Now the theory is in place for the statement and proof of a formula for the rank of 4-circulant graphs with an even number of vertices.

Theorem 5 *Let n be even and $G = 4C_n(a, b)$. Then rank$(A(G)) = n - d_1 - d_2 + d_3$, where*

$$d_1 = \left\{ \begin{array}{ll} \gcd(b-a,n) & \textit{if } \gcd(b-a,n) \textit{ divides } \frac{n}{2} \\ 0 & \textit{otherwise} \end{array} \right\}$$
$$d_2 = \left\{ \begin{array}{ll} \gcd(b+a,n) & \textit{if } \gcd(b+a,n) \textit{ divides } \frac{n}{2} \\ 0 & \textit{otherwise} \end{array} \right\} \textit{ and}$$
$$d_3 = $$
$$\left\{ \begin{array}{ll} \gcd(d_1,d_2) & \textit{if } d_1, d_2 \textit{ are nonzero and } \gcd(\frac{n}{d_1}, \frac{n}{d_2}) \textit{ divides } \frac{n(d_2-d_1)}{2d_1d_2} \\ 0 & \textit{otherwise} \end{array} \right\}$$

Proof. If $G = 4C_n(a, b)$, then by Theorem 3, the eigenvalue, λ_p, of $A(G)$ is zero if and only if

$$(b-a)p \equiv \frac{n}{2} \bmod n \quad \text{or} \quad (b+a)p \equiv \frac{n}{2} \bmod n.$$

Recall that $(b-a)p \equiv \frac{n}{2} \bmod n$ has $\gcd(b-a,n)$ solutions if and only if $\gcd(b-a,n)$ divides $\frac{n}{2}$. Similarly, $(b+a)p \equiv \frac{n}{2} \bmod n$ has $\gcd(b+a,n)$ solutions if and only if $\gcd(b+a,n)$ divides $\frac{n}{2}$. However, the solutions to these congruencies could overlap. This will occur if and only if the system of congruencies

$(b-a)p \equiv \frac{n}{2} \bmod n$
$(b+a)p \equiv \frac{n}{2} \bmod n$

has a solution. Define the following conditional values as follows:

$$d_1 = \left\{ \begin{array}{ll} \gcd(b-a,n) & \text{if } \gcd(b-a,n) \text{ divides } \frac{n}{2} \\ 0 & \text{otherwise} \end{array} \right\} \text{ and}$$
$$d_2 = \left\{ \begin{array}{ll} \gcd(b+a,n) & \text{if } \gcd(b+a,n) \text{ divides } \frac{n}{2} \\ 0 & \text{otherwise} \end{array} \right\}.$$

Then by Corollary 3, the system is solvable if and only if

$$\gcd\left(\frac{n}{d_1}, \frac{n}{d_2}\right) \text{ divides } \frac{n(d_2-d_1)}{2d_1d_2}, \text{ where } d_1 \text{ and } d_2 \text{ are nonzero,}$$

in which case there are $\gcd(d_1, d_2)$ solutions to the system. Finally, the quantity

$$d_3 = $$
$$\left\{ \begin{array}{ll} \gcd(d_1,d_2) & \text{if } d_1, d_2 \text{ are nonzero and } \gcd(\frac{n}{d_1}, \frac{n}{d_2}) \text{ divides } \frac{n(d_2-d_1)}{2d_1d_2} \\ 0 & \text{otherwise} \end{array} \right\}$$

gives the number of overlapping solutions to the system of congruencies. Hence, the number of zero-valued eigenvalues is $d_1 + d_2 - d_3$. Therefore, rank$(A(G)) = n - d_1 - d_2 + d_3$. ■

We have determined the rank of the adjacency matrix for any 4-circulant. We now turn to the problem of classifying these graphs.

4 Classification.

Before classifying all connected 4-circulants, we briefly review the types of connected 2- and 3-circulant graphs. For 2-circulants, there is only one type.

Theorem 6 . *Let G be the connected 2-circulant on n vertices formed by $S = \{a, n-a\}$, i.e., $2C_n(a)$. Then G is isomorphic to the cycle on n vertices C_n.*

Proof. Let $G = 2C_n(a)$. Since G is connected, $\gcd(a, n) = 1$. Thus the cyclic group of $\mathbf{Z}_n$ generated by a is $\mathbf{Z}_n$; in other words, the elements of $\langle a \rangle = \{0, a, 2a, ..., (n-1)a\}$ are all distinct modulo n. Therefore, G is a cycle on n vertices. ■

Now 3-circulants are formed by a three-element set $S = \{a, \frac{n}{2}, n-a\}$. These are the only sets for which $S = -S \bmod n$. We denote a general 3-circulant by $3C_n(a)$. It turns out that all connected 3-circulants are isomorphic to one of two basic types. The primary quantity that distinguishes the two types is $\frac{n}{d}$, where $d = \gcd(a, n)$.

Theorem 7 . *Let $G = 3C_n(a)$, and $d = \gcd(a, n)$.*
If $\frac{n}{d}$ is even, then G has d components, each isomorphic to $3C_{\frac{n}{d}}(1)$.
If $\frac{n}{d}$ is odd, then G has $\frac{d}{2}$ components, each isomorphic to $C_{\frac{n}{2}} \times P_2$.

Proof. [7].

When classifying 4-circulants, the fact that set S has four elements and three parameters makes the situation significantly more complicated. There are still two basic types, but the types are fundamentally different. Some $4C_n(a, b)$ are isomorphic to $4C_n(1, c)$ for some c. Others are isomorphic to graphs called *twisted prismatic graphs* or *twisted towers*[10]. These twisted towers are graphs that have the Cartesian product $C_r \times P_s$ as a subgraph, but they also have an additional r edges that connect the top and bottom cycles in a permutation.

Definition 1 *A graph G is called a* twisted tower with parameters r, s and t, *denoted $G = TT(r, s, t)$ if G has vertex set $V = \{(u, v) : 0 \leq u \leq s-1, 0 \leq v \leq r-1\}$ and the following adjacencies:*
(u, v) is adjacent to:

$(u, (v+1) \bmod r)$	$\forall u$	$\forall v$
$(u, (v-1) \bmod r)$	$\forall u$	$\forall v$
$(u+1, v)$	$0 \leq u \leq s-2$	$\forall v$
$(u-1, v)$	$1 \leq u \leq s-1$	$\forall v$

$(0, v)$ is adjacent to:
$(s-1, (v+t) \bmod r) \quad \forall v$.

Note that the first two lines of adjacencies specify cycles of length r, the second two lines specify paths of length s. Without any further edges this graph would be $C_r \times P_s$. The last line defines the adjacencies of the top cycle to the bottom cycle. If $t = 0$, then the graph is $C_r \times C_s$. Note that in general, such a graph G has rs vertices, and that $TT(r, s, t)$ is isomorphic to $TT(r, s, r - t)$.

For example, consider $G_1 = TT(6, 2, 3)$ (Figure 3), and $G_2 = TT(4, 3, 2)$ (Figure 4) which can both be shown to be isomorphic to $4C_{12}(2, 3)$. Note in each drawing how vertices in the top cycle are connected to vertices in the bottom cycle. This is a good illustration of the notation, and leads us into our first classification theorem.

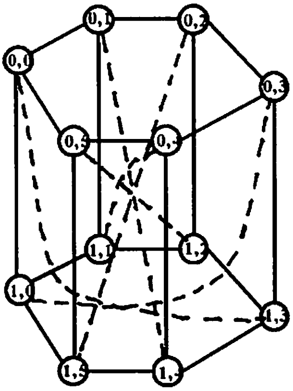

Figure 3: $G_1 = TT(6, 2, 3)$.

Theorem 8 *Let $G = 4C_n(a, b)$. If $\gcd(n, a, b) = 1$, so that G is connected, and $\gcd(n, a) = d \neq 1$, then G is isomorphic to $G' = TT(\frac{n}{d}, d, t)$, where t is a solution of the equation $ta \equiv (n - db) \bmod n$.*

Proof. Since $\gcd(n, a, b) = 1$, the mapping $(bu + av) \bmod n \leftrightarrow (u, v)$ provides a correspondence between the vertices of G and the vertices of a twisted tower. Indeed this is a one-to-one mapping for if $bu + av = 0$, then $bu + av = qn$, or $bu = qn - av$ for some integer q. Now $1 \neq d = \gcd(a, n)$, so $d \mid n$ and $d \mid a$. Now $\gcd(n, a, b) = 1$, and $\gcd(d, b) = 1$ with $d \mid (qn - av)$ implies that $d \mid bu$ and thus $d \mid u$. Since $0 \leq u \leq d - 1$, u must be 0. Similarly $av = 0$ implies $v = 0$ since $0 \leq v \leq \frac{n}{d} - 1$, and the mapping is one-to one. We now show that adjacencies are preserved by this mapping.

We show that vertex (u, v) has the adjacencies indicated by the definition.

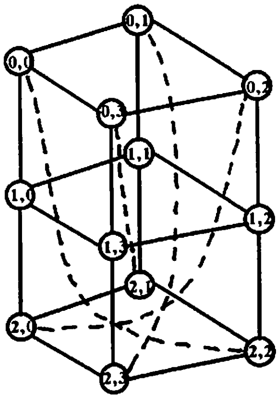

Figure 4: $G_2 = TT(4,3,2)$.

Vertex $v_1 = (u, (v+1) \bmod \frac{n}{d})$ in G' corresponds to $(bu+a((v+1) \bmod \frac{n}{d}))$ in G, which is adjacent to vertex $(bu + av)$, since the difference in vertex numbers is a. Since $(bu + av)$ maps to (u, v) in G', v_1 is adjacent to (u, v).

Similarly, vertex $v_2 = (u, (v-1) \bmod \frac{n}{d})$ in G' corresponds to $(bu+a((v-1) \bmod \frac{n}{d}))$ in G, which is adjacent to vertex $(bu + av)$, since the difference in vertex numbers is again a. Since $(bu + av)$ maps to (u, v) in G', v_2 is adjacent to (u, v).

Now vertex $v_3 = (u + 1, v)$ for $0 \leq u \leq d - 2$ in G' corresponds to $(b(u + 1) + av)$ in G and is adjacent to $(bu + av)$ since the difference in vertex numbers is b. This shows that any such v_3 is adjacent to (u, v).

Similarly, any vertex $v_4 = (u - 1, v)$ for $1 \leq u \leq d - 1$ in G' corresponds to $(b(u - 1) + av)$ in G and is adjacent to $(bu + av)$ since the difference in vertex numbers is b. This shows that any such v_4 is adjacent to (u, v).

Finally, focus on vertex $(0, v)$, which corresponds to vertex av in G. Note that vertex av is adjacent to vertex $(av + (n - b)) \bmod n$. We claim that vertex $(0, v)$ is adjacent to $(d-1, (v+t) \bmod \frac{n}{d})$. Indeed $(d-1, (v+t) \bmod \frac{n}{d})$ in G' corresponds to $(b(d-1)+a((v+t) \bmod \frac{n}{d})) \equiv (b(d-1)+a(v+t\pm k\frac{n}{d}) \equiv (b(d-1)+a(v+t)) \bmod n$ since d divides a. Further, $(b(d-1)+a(v+t)) \equiv (bd-b+av+at) \equiv (bd-b+av+(n-db)) \equiv (av+n-b)$ by the definition of t. This establishes the final adjacency.■

The roles of a and b above are interchangeable, and a similar statement is true using $\gcd(n, b) = d$. That is how in the above example with $n = 12$, it is possible for G to be isomorphic to two very different looking graphs. In one case, $\gcd(12, 2) = 2$, creating 6-cycles; in the other, $\gcd(12, 3) = 3$, creating 4-cycles.

Sometimes the edges connecting the top and bottom cycles line up to create even more structure. In these cases, G is isomorphic to some $C_{a'} \times C_{b'}$.

Theorem 9 *Let $G = 4C_n(a,b)$. If $gcd(a,b) = 1$, $gcd(n,a) = d_1 \neq 1$, $gcd(n,b) = d_2 \neq 1$ and $d_1 d_2 = n$, then the circulant on n vertices formed by S is isomorphic to $C_{d_1} \times C_{d_2}$.*

Proof: We need only show that $t = 0$. Solving $ta \equiv n - d_1 b \bmod n$ gives $ta \equiv n - d_1 b \equiv n - \frac{n}{d_2} b \equiv n - n(\frac{b}{d_2}) \equiv 0$, thus $t = 0$.■

In the above, we have focused on the cases where $\gcd(n,a) \neq 1$ or $\gcd(n,b) \neq 1$ or perhaps both. In these cases, G is always isomorphic to a twisted tower, and sometimes can be drawn in two different ways. We now consider the implications of $\gcd(n,a) = 1$ or $\gcd(n,b) = 1$. As usual, we assume that $\gcd(n,a,b) = 1$ so that G is connected.

Theorem 10 *Let $G = 4C_n(a,b)$. Then G is isomorphic to $4C_n(1,c)$ for some c if and only if* $\gcd(a,n) = 1$ *or* $\gcd(b,n) = 1$.

Proof. ($\Rightarrow$) Let G be isomorphic to $4C_n(1,c)$ for some c. Then there exists an automorphism ϕ from $\mathbf{Z}_n$ to $\mathbf{Z}_n$ such that $\phi(0) = 0$. Then, since ϕ preserves adjacencies, $\phi(0)$ must be adjacent to $\phi(1)$. Hence, $\phi(1) \in \{a, b, n-b, n-a\}$. Thus we have four cases.

(i) If $\phi(1) \equiv a$, then since $\langle 1 \rangle = \mathbf{Z}_n$, $\langle a \rangle = \mathbf{Z}_n$. Therefore $\gcd(a,n) = 1$.
(ii) If $\phi(1) \equiv b$,, then by a similar argument, $\gcd(b,n) = 1$.
(iii) If $\phi(1) \equiv n - b$, then $\gcd(n-b,n) = 1$ which implies $\gcd(b,n) = 1$.
(iv) If $\phi(1) \equiv n - a$, then $\gcd(n-a,n) = 1$, which implies $\gcd(a,n) = 1$.
In any of the four cases, either $\gcd(a,n) = 1$ or $\gcd(b,n) = 1$.

($\Leftarrow$) Let $G = 4C_n(a,b)$ where $\gcd(n,a) = 1$ and $V(G) = \{0,1,2,\ldots,n-1\}$. Also, let $G' = 4C_n(1,c)$, where $c = \frac{b+nq}{a}$ for the smallest positive integer q which makes $\frac{b+nq}{a}$ an integer and $V(G') = \{0',1',2',\ldots,(n-1)'\}$.

We claim that G and G' are isomorphic.

Define a function $\phi : V(G') \to V(G)$ by $\phi(k') \equiv ak$. Since $\gcd(n,a) = 1$, it is easy to see that modulo n, $\{0, a, 2a, \ldots, (n-1)a\} = \{0,1,2,\ldots,n-1\}$. Hence, ϕ is one-to-one and onto. We must now show that ϕ preserves adjacencies.

Let $k' \in V(G')$. Since $S' = \{1, c, n-c, n-1\}$, k' is adjacent to $(k+1)', (k+c)', (k-c)'$, and $(k-1)'$. Now $\phi(k') \equiv ak \in V(G)$ is adjacent to $ak+a, ak+b, ak-b$, and $ak-a$ since $S = \{a, b, n-b, n-a\}$.

Now, $\phi(k+1)' \equiv a(k+1) \equiv ak+a$, $\phi(k+c)' \equiv a(k+c) \equiv ak+ac \equiv ak + a(\frac{b+nq}{a}) \equiv ak+b+nq \equiv ak+b \bmod n$, $\phi(k-c)' \equiv a(k-c) \equiv ak-(b+nq) \equiv ak-b \bmod n$, and $\phi(k-1)' \equiv a(k-1) \equiv ak-a$. Hence, ϕ preserves adjacencies, and G and G' are isomorphic.■

Finally we note when a 4-circulant with a jump of one can be isomorphic to another 4-circulant with a jump of one.

Theorem 11 *Let $G = 4C_n(1, c)$. Then G is isomorphic to $4C_n(1, k)$ for some k if and only if $ck \equiv 1 \bmod n$.*

Proof. ($\Rightarrow$) Let G be isomorphic to $4C_n(1, k)$ for some k. Then by Theorem 10, $k = \frac{1+nq}{c}$ for the smallest $q \in \mathbf{Z}$ that makes k an integer. Then $ck = 1 + nq$ so that $ck - 1 = nq$, which implies $ck \equiv 1 \bmod n$.

($\Leftarrow$) Let $ck \equiv 1 \bmod n$. Note that G is isomorphic to $4C_n(1, c')$ where $c' = \frac{1+nq_1}{c}$, and that $4C_n(1, k)$ is isomorphic to $4C_n(1, k')$ where $k' = \frac{1+nq_2}{c}$. Then $cc' \equiv 1 + nq_1$ and $kk' \equiv 1 + nq_2$, implying $cc' \equiv kk' \equiv 1 \bmod n$. Thus, since $ck \equiv 1 \bmod n$, $cc' \equiv ck \bmod n$ and $kk' \equiv ck \bmod n$. Examining the first congruence, we have $n \mid (cc' - ck)$, implying $n \mid c(c' - k)$. But note that since $ck \equiv 1 \bmod n, c$ is a unit in $\mathbf{Z}_n$; therefore $\gcd(n, c) = 1$, which implies n must divide $c' - k$. Thus $(c' - k) = 0$, so that $c' = k$. Similarly $k' = c$. Therefore $4C_n(1, c)$ is isomorphic to $4C_n(1, k)$. ■

5 Future Directions.

This work, together with [7] establish the rank and the isomorphism structure of the 3- and 4- circulant graphs. Finding the rank is done through examining the eigenvalues of $A(G)$ and determining how many of these are zero. As the eigenvalues of circulant matrices have a formula, determining the rank is mainly an algebraic task. Classifying these graphs and determining their isomorphism structure is a much more challenging problem. Results from the 3-circulant class do not immediately generalize to 4-circulants. Future work will focus on what can be learned of the general k-circulant.

References

[1] J. Bevis, K. Blount, G. Davis, G. Domke, J. Lalani and V. Miller, "Recent Results Involving the Rank of the Adjacency Matrix of a Graph," Congressus Numerantium, 100 (1994), pp. 33-45.

[2] J. Bevis, K. Blount, G. Davis, G. Domke and V. Miller, "The Rank of a Graph After Vertex Addition," Linear Algebra and Its Applications, 265 (1997), pp. 55-69.

[3] J. Bevis, G. Domke and V. Miller, "Ranks of Trees and Grid Graphs," Journal of Combinatorial Mathematics and Combinatorial Computing, 18 (1995), pp. 109-119.

[4] I. Broere, "Every connected circulant is Hamiltonian," Verslagreeks van die Departement Wiskunde, Rand Afrikaans University, no 2/86, May 1986.

[5] D. Cvetkovic, M. Doob and H. Sachs, Spectra of Graphs: Theory and Application, Academic Press, New York, 1979.

[6] G. Davis, "The Rank of a Graph After Edge Insertion or Deletion," Congressus Numerantium, 133 (1998), pp. 31-43.

[7] G. Davis and G. Domke, "3-Circulant Graphs," Journal of Combinatorial Mathematics and Combinatorial Computing, to appear.

[8] P. Davis, Circulant Matrices, John Wiley & Sons, New York, 1979.

[9] M. Ellingham, "Basic Subgraphs and Graph Spectra," Australasian Journal of Combinatorics, 8 (1993), pp. 247-265.

[10] R. Giudici and M. Abreu, "On Generating Cayley's Graphs." Series Preprint, Universidad Simón Bolívar, Departmento do Mathmáticas.