Ultra Scientist Vol. 28(4)A, 197-203 (2016).
www.ultrascientist.org

ISSN 2231-346X (Print)
2319-8044 (Online)

Directed Circulant graphs and Binary Cyclic codes

GEORGE MATHEW

Department of Mathematics, BCM College Kottayam-686001, Kerala (India)
e- mail : gmathew5616x@gmail.com

(Acceptance Date 31st July, 2016, Online Publication date 2nd Sep. 2016)

Abstract

Various papers have been written on the theory of circulant graphs[3,6,8,9,10]. Also graphs with circulant adjacency matrices is discussed in[7]. Circulant graphs have important applications to the theory of designs and error correcting codes[12]. This paper is a study of relationship between circulant graphs and binary linear codes. It establishes a strong connection between directed circulant graphs and binary cyclic codes . Each binary cyclic code corresponds to an equivalence class of directed circulant graphs. Circulant graphs associated with combination of cyclic codes is also discussed.

Key words : Cayley graphs, circulant graphs, adjacency matrix, cyclic codes, generator polynomial, generator matrix.

1. Introduction

Circulant graphs is a special class of Cayley graphs. Various papers have been written on the theory of circulant graphs[3,6,8,9,10]. It is interrelated with many branches of mathematics outside graph theory. For example, for geometers, circulant graphs are known as star polygons[4]. Circulant graphs have been used to solve problems in group theory[1] as well as number theory and analysis[5]. They have important applications to the theory of designs and error correcting codes[12]. This paper is a study of relationship between circulant graphs and binary linear codes. It establishes a strong connection between directed circulant graphs and binary cyclic codes. Each binary cyclic code corresponds to an equivalence class of directed circulant graphs. Circulant graphs associated with combination of cyclic codes is also discussed.

2. Basic Concepts :

A ***graph*** G is a pair G = (V,E) consisting of a finite set V and a set E of 2-element subsets of V. The elements of V are called ***vertices*** and the elements of E are called ***edges***. Two vertices u and v of G are said to be ***adjacent*** if there is an edge e = (u,v) $\in$ E. Two edges are said to be adjacent if they have a common vertex. A ***directed graph*** or ***digraph*** consists of a finite set V of vertices and a set A of ordered pairs of distinct vertices called ***arcs***. If the ordered pair (u,v) is an *arc a* we say that *arc a* is directed from u to v.

2.1. Definition [2] :

Let G be a group and S be a subset of G\{e}. We say that a graph X is a ***Cayley graph*** of G with ***connection set*** S written as X = Cay(G, S) if
(i)V(X) = G
(ii) A(X) = {(g, sg): g $\in$ G & s $\in$ S }

2.2. Definition [1, 10] :

Let Z_n denote the additive group of integers modulo n and let $S\subset Z_n\backslash\{0)$. If X=Cay ($Z_n$, S), then we say X is a ***circulant graph*** of order n.

2.3. Definition [2]:

The ***adjacency matrix*** of a directed graph X is the matrix $\mathbb{A}(X)$ with rows and columns indexed by vertices of X. Each entry $\mathbb{A}_{ij}$ is equal to the number of times the arc (i, j) appears in X.

The adjacency matrix of a circulant graph has a pleasing nature : each row is the cyclic shift of the preceding row. If (a_1, a_2, ………… a_n) is the first row, then (a_n, a_1, ………… a_{n-1}) is the second row (a_{n-1}, a_n, ………… a_{n-2}) is the third row and finally (a_2, a_3, ………, a_1) is the nth row.

If F represents the binary field, thenF^n the set of all n-tuples of F is an n-dimensional vector space over F. A k-dimensional subspace of F^n is called an [n,k] ***binary linear code*** C. A basis of C consists of k linearly independent binary n-tuples. The matrix G formed by the basis vectors is called a ***generator matrix*** of C.The elements of C are called ***code words*** and are linear combinations of the rows of the generator matrix G. Since a vector space can have many basis, a code C has many generator matrices.

2.4. Definition [11]:

An [n,k] code C is called ***cyclic*** if whenever x=(a_0, a_1, ………… a_{n-1}) is in C, so is its first cyclic shift y=(a_{n-1}, a_1, ……… a_{n-2}).

This means that (a_{n-2}, a_{n-1}, …… a_{n-3}) the first cyclic shift of y and all other cyclic shifts of y are also in C. When considering cyclic codes it is useful to let a vector (a_0, a_1,…, a_{n-1}) corresponds to a polynomial a_0+ a_1x + ……+ a_{n-1} x^{n-1}. Then (a_{n-1}, a_0, ….,a_{n-2}) corresponds to a_{n-1}+ a_0x + ……+ $a_{n-2}x^{n-1}$. This polynomial equals the polynomial (a_0+ a_1x + ……+ a_{n-1} x^{n-1})x (modulo x^n-1). Hence the cyclic shift corresponds to multiplication by x. If F[x] represents the ring of polynomials over F, then the set R_n= $\frac{F[x]}{<x^n-1>}$ consists of polynomials over F of degree less than n is a ring. Polynomials in R_n are added co-ordinatewise and multiplication is modulo (x^n – 1). The following theorem give an insight into the structure of cyclic codes.

2.5. Theorem [11] :

A set of elements S inR_n corresponds

to a cyclic code if and only if S is an ideal in R_n.

2.6. Theorem [11] :

R_n is a principal ideal ring. If C is an ideal in R_n and g(x) is the monic polynomial of smallest degree in C, then g(x) is uniquely determined and C = <g(x)>.

The unique monic polynomial g(x) of smallest degree in C is called the ***generator polynomial*** of C. To find the generator polynomial we make use of the following theorem.

2.7. Theorem [11] :

If C is an ideal in R_n, the unique monic generator g(x) of C of smallest degree divides $(x^n – 1)$ and conversely if a polynomial g(x) in C divides $(x^n – 1)$, then g(x) has the lowest degree in <g(x)>.

When considering binary cyclic codes, we here assume that n is of the form 2^m-1. Note that when n is odd x^n -1 has distinct factors. There is a nice relationship between the dimension of a cyclic code and the degree of its generator polynomial.

2.8. Theorem [11] :

If the degree of g(x) is n-k, then the dimension of C = <g(x)> is k. if g(x) = g_0 + g_1x + g_2x^2 + ……… + $g_{n-k}x^{n-k}$, then the generator matrix of C is

$$\begin{pmatrix} g_0 & g_1 & g_2 & g_{n-k} & 0 & 0 \\ 0 & g_0 & g_1 & g_{n-k-1} & g_{n-k} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & . & . & g_{n-k} \end{pmatrix}$$

Thus the generator matrix of C is the matrix whose first row is g(x) and the second row is g(x)x, the third row is $g(x)x^2$………… until the last row $g(x)x^{k-1}$. That is g(x) and its k-1 cyclic shifts. We now establish a relationship between circulant graphs and cyclic codes.

3. Equivalence of circulant graphs and cyclic codes :

As it is stated earlier, the adjacency matrix of a circulant graph is always a cyclic nxn matrix. In fact, if $\mathbb{A}$ is the adjacency matrix of a circulant graph X = Cay(Z_n, S) with its first row r_1 is having 1 in the i_1, i_2,……… i_k th positions and 0 in the remaining positions then the connection set is S = {i_1, i_2,……… i_k} and therefore (1, i_1 + 1), ………, (1, i_k+1)are arcs in X so that i_1 + 1,……..,i_k + 1 th positions of the second row r_2 are 1 and the remaining positions 0. This is clearly the first cyclic shift of r_1. Similarly r_3 is the second cyclic shift of r_1 and so on. Also there is a one to one correspondence between circulant graphs and binary cyclic n x n matrices other than those with leading element 1. We make use of this relationship to prove the equivalence of circulant graphs and cyclic codes.

3.1. Theorem :

If C is a binary cyclic code of length n, then C corresponds to a circulant graph on Z_n. Conversely if X = Cay(Z_n, S) is a circulant graph on Z_n, then X corresponds to a cyclic code.

Proof :

Let C be a cyclic code of length n. If

$g(x)$ is its generator polynomial, then $g(x)/x^n-1$. Let $g(x) = g_0 + g_1x + g_2x^2 + \ldots\ldots. + g_{n-k}x^{n-k}$. To the kxn generator matrix G, adjoin the remaining n-k cyclic shifts to get the nxn matrix

$$A=\begin{pmatrix} g_0 & g_1 & g_2 & g_{n-k} & 0 & 0 \\ 0 & g_0 & g_1 & g_{n-k-1} & g_{n-k} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & g_0 & g_1 & g_{n-k} \\ g_{n-k} & 0 & 0 & 0 & g_0 & g_{n-k-1} \\ \vdots & \vdots & \vdots & & & \vdots \\ g_1 & g_2 & g_3 & 0 & 0 & g_0 \end{pmatrix}$$

Choose any row r_j having its first element 0. Let B be the nxn matrix formed with r_j as the first row and remaining rows the n-1 cyclic shifts of r_j.

Since each row of A is a row of B and vice versa, and that C consists of linear sums of rows of A, it can be generated by B. Now B is a cyclic n x n binary matrix with leading element 0, hence form the adjacency matrix of a circulant graph

Conversely, let there be a circulant graph X = Cay(Z_n, S). If A is the adjacency matrix of X, then A is a cyclic nxn matrix with leading element 0. Let C be the row space of A. The first row r_1 corresponds to a polynomial k(x) of degree $\leq$ n-1. The remaining rows are $xk(x)$, $x^2k(x)$,………,$x^{n-1}k(x)$.. We prove that C is a cyclic code. Let $s(x) \in C$. Then s(x) is a linear combination of these polynomials

$$s(x) = a_0k(x) + a_1xk(x) + a_2\, x^2k(x) + \ldots\ldots\ldots + a_{n-1}\, x^{n-1}k(x).$$

Then

$$xs(x) = a_0\, xk(x) + a_1\, x^2\, k(x) + \ldots\ldots\ldots + a_{n-1}\, k(x) \pmod{(x^n-1)}$$

$$= a_{n-1}\, k(x) + a_0\, x\, k(x) + \ldots\ldots\ldots + a_{n-2}\, x^{n-1}\, k(x)$$

This means that the first cyclic shift of s(x) can be generated by the rows of A. Consequently the second cyclic shift and all the remaining cyclic shifts can be generated using the rows of A. Thus s(x) and all its cyclic shifts belong to C, hence C is a cyclic code ■

Note that the correspondence mentioned in the theorem is not a one to one correspondence. However the relation that 'two circulant graphs are equivalent if and only if the cyclic code representing both are equal' is an equivalence relation.

The following theorem is a useful way to find the generator polynomial of the cyclic code representing a circulant graph.

3.2. Theorem

Suppose X= Cay(Zn, S) be a circulant graph. Let C = <k(x)>be the cyclic code representing X. Then $g(x)=\gcd(k(x), x^n-1)$ is the generator polynomial of C and C =<g(x)>. If g(x) has degree n – k, then dim C = k

Proof :

Let C = <k(x)> be the cyclic code representing X. Then k(x) is the first row of the adjacency matrix of X.We first prove that k(x) is a linear combination of g(x) and its cyclic shifts and that g(x) is a linear combination of k(x) and its cyclic shifts.

Since $g(x)=\gcd(k(x), x^n-1)$, g(x)/ k(x). Therefore k(x)=a(x) g(x) for some $a(x) \in R_n$. If

$$a(x) = a_0 + a_1 x + a_2 x^2 + \ldots\ldots\ldots + a_{n-1} x^{n-1},$$

we have

$$k(x) = a_0 g(x) + a_1 x g(x) + a_2 x^2 g(x) + \ldots\ldots\ldots + a_{n-1} x^{n-1} g(x)$$

Thus $k(x)$ is a linear combination of $g(x)$ and its cyclic shifts.Again, since
$g(x) = \gcd(k(x), x^n - 1)$, by Eclidean algorithm,
$g(x) = b(x)\, k(x) + a(x)\,(x^n - 1)$ in $F[x]$, hence
$g(x) = b(x)\, k(x)$ in R_n. If
$b(x) = b_0 + b_1 x + b_2 x^2 + \ldots\ldots\ldots + b_{n-1} x^{n-1}$, we have

$g(x) = b_0 k(x) + b_1 x k(x) + b_2 x^2 k(x) + \ldots\ldots\ldots + b_{n-1} x^{n-1} k(x)$, thus $g(x)$ is a linear combination of $k(x)$ and its cyclic shifts.Therefore $C = <g(x)>$. Since $g(x) / x^n - 1$, Theorem 2.7 guarantee that $g(x)$ is the generator polynomial of C. Finally, if $g(x)$ has degree $n - k$, by Theorem 2.8, C has dimension k ■

3.3. Example :

Consider the circulant graph $X = \mathrm{Cay}(Z_{7,}\{3,5\})$. The adjacencymatrix of X is

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

The polynomial represented by X is $k(x) = x^3 + x^5 = x^3 (1 + x^2) = x^3 (1 + x)^2$.
We know

$$x^7 - 1 = (1 + x)\,(1 + x + x^3)(\,1 + x^2 + x^3)$$

Therefore $\gcd(k(x), x^7 - 1) = 1 + x$. Hence X corresponds to the cyclic code $C = <1 + x>$. Since the degree of the generator polynomial is 1, dimension of the code is 6 ■

3.4. Example :

Consider the circulant graph $X = \mathrm{Cay}(Z_{15}, \{2,4,7,9\})$. The polynomial represented by X is
$k(x) = x^9 + x^7 + x^4 + x^2$
$\quad = x^2(x + 1)^3\,(x^4 + x^3 + x^2 + x + 1)$
We have
$x^{15} - 1 = (x + 1)(x^2 + x + 1)(x^4 + x^3 + 1)(x^4 + x + 1)\,(x^4 + x^3 + x^2 + x + 1)$. Therefore
$\gcd(k(x), x^{15} - 1) = (x + 1)\,(x^4 + x^3 + x^2 + x + 1)$
$\quad = x^5 + 1$

Thus $g(x) = x^5 + 1$ is the generator polynomial of the corresponding code. Since the degree of $g(x)$ is 5, dimension of the code is 10 ■

We now seek a condition under which the cyclic code corresponding to one circulant graph becomes a subset of another.

3.5. Theorem :

Suppose $X = \mathrm{Cay}(Z_n, k_1(x))$ corresponds to the code C_1 and $Y = \mathrm{Cay}(Z_n, k_2(x))$ corresponds to the code C_2. If $k_2(x) / k_1(x)$, then $C_1 \subset C_2$. The converse is not however true.

Proof :

If g_1 and g_2 are the generator polynomials of C_1 and C_2, then
$g_1(x) = \gcd(k_1(x), x^n - 1)$ and $g_2(x)$

$= \gcd(k_2(x), x^n - 1)$. Suppose $k_2(x) / k_1(x)$, then $k_1(x) = a(x)\, k_2(x)$. Now $\gcd(k_2(x), x^n - 1) / \gcd(k_1(x), x^n - 1)$. That is $g_2(x) / g_1(x)$, hence $C_1 \subset C_2$. The converse is not however true. For example

Let

$X = Cay(Z_7, \{1,2\})$ and $Y = Cay(Z_7, \{2,3,6\})$

Here

$k_1(x) = x + x^2$ and $k_2(x) = x^2 + x^3 + x^6$

$g_1(x) = (1 + x)$ and $g_2(x) = 1$. Therefore $C_1 \subset C_2$ but $k_2(x)$ $k_1(x)$ ■

We shall now investigate the circulant graphs corresponding to the intersection of the cyclic codes and sum of the cyclic codes representing two different circulant graphs. For this we require the use of the following theorem.

3.6. Theorem [11] :

Let C_1 and C_2 be cyclic codes with generator polynomials $g_1(x)$ and $g_2(x)$, then $C_1 \cap C_2$ has generator polynomial $g(x) = \operatorname{lcm}(g_1(x), g_2(x))$ and $C_1 + C_2$ has generator polynomial $\gcd(g_1(x), g_2(x))$.

1.4. Theorem:

Suppose that a cyclic code C_1 corresponds to a circulant graph $x = Cay(Z_n, k_1(x))$ and C_2 corresponds to the circulant graph $Y = Cay(Z_n, k_2(x))$, then $C_1 \cap C_2$ corresponds to $Z = Cay(Z_n, k_1(x)\, k_2(x))$ and $C_1 + C_2$ corresponds to $U = Cay(Z_n, \gcd(k_1(x), k_2(x))$

Proof :

Let g_1 and g_2 be the generator polynomials of X and Y respectively. Then

$g_1(x) = \gcd(k_1(x), x^n - 1)$ and $g_2(x) = \gcd(k_2(x), x^n - 1)$.

Using Theorem 3.6, $C_1 \cap C_2$ has generator polynomial

$g(x) = \operatorname{lcm}(\gcd(k_1(x), x^n - 1), \gcd(k_2(x), x^n - 1))$.

We claim thatthis is equal to $\gcd(k_1(x)k_2(x), x^n - 1)$. Since n is odd, we know all the factors of $x^n – 1$ are distinct. Therefore the factors of $\gcd(k_1(x)k_2(x), x^n - 1)$ are all distinct. They can be classified into 3 groups

u : factors of $x^n - 1$ in $k_1(x)$ but not in $k_2(x)$

v : factors of $x^n - 1$ common to both $k_1(x)$ and $k_2(x)$

w: factors of $x^n - 1$ in $k_2(x)$ but not in $k_1(x)$

Thus

$\gcd(k_1(x)k_2(x), x^n - 1) = u\, v\, w$

Now

$\gcd(k_1(x), x^n - 1) = u\, v$ and $\gcd(k_2(x), x^n - 1) = v\, w$

Since gcd (u, v) = gcd (v, w) = gcd (u, w) = 1 and that each of u, v, w has distinct factors, it follows that

$\operatorname{lcm}(\gcd(k_1(x), x^n - 1), \gcd(k_2(x), x^n - 1)) = u\, v\, w$. Thus

$\operatorname{lcm}(\gcd(k_1(x), x^n - 1), \gcd(k_2(x), x^n - 1)) = \gcd(k_1(x)k_2(x), x^n - 1)$

Hence $C_1 \cap C_2$ corresponds to the circulant graph $Z = Cay(Z_n, k_1(x)\, k_2(x))$.

Again by Theorem 3.6, $C_1 + C_2$ has generator polynomial $\gcd(\gcd(k_1(x), x^n - 1),$

gcd ($k_2(x)$, x^n -1)). We claim that this is equal to gcd ($k_1(x)$, $k_2(x)$, x^n -1). If q(x) divides gcd (gcd ($k_1(x)$, x^n -1), gcd ($k_2(x)$, x^n -1)), then q(x) divides both gcd ($k_1(x)$, x^n -1) andgcd ($k_2(x)$, x^n -1). This implies q(x) divides $k_1(x)$, $k_2(x)$ and x^n – 1, hence divides gcd ($k_1(x)$, $k_2(x)$, x^{n-1}). On the other hand if q(x) divides gcd ($k_1(x)$, $k_2(x)$, x^n -1), then it divides all of $k_1(x)$, $k_2(x)$, and x^n – 1. But then q(x) divides gcd ($k_1(x)$, x^n -1) and gcd ($k_2(x)$, x^n -1), hence divides gcd (gcd ($k_1(x)$, x^n -1), gcd ($k_2(x)$, x^n -1)). Therefore $C_1 + C_2$ has generator polynomial gcd ($k_1(x)$, $k_2(x)$, x^n -1) Since this is equal to gcd (gcd ($k_1(x)$, $k_2(x)$), x^n -1), we conclude that $C_1 + C_2$ corresponds to the circulant graph U = Cay (Z_n, gcd ($k_1(x)$, $k_2(x)$)) ■

3.8. Example :

Suppose X = Cay (Z_{15}, {3,4,5,8} and Y = Cay (Z_{15},{5,6,8,9}). If C_1 and C_2 are the cyclic codes representing these circulant graphs, then $C_1 \cap C_2$ represents the circulant graph Z = Cay (Z_{15} , {1,2,8,13}) and $C_1 + C_2$ represents the circulant graph U = Cay(Z_{15}, {5,3}) ■

References

1. B. Alspach, T. Parsons, Isomorphism of Circulant Graphs and Digraphs, Discrete Mathematics *25*, 97-108 (1979).
2. N. Biggs, Algebraic Graph Theory, Cambridge University Press, London, 1974
3. K. Collins, Circulants and Sequences, SIAM Journal of Discrete Mathematics, *11*, 330-339 (1998).
4. H. S. M. Coxeter, Twelve Geometric Essays, Southern Illinois University Press, Carbondale/Edwardsville, IL, (1968).
5. G. J. Davis, G. S. Domke, C. R. Garner, 4-Circulant Graphs, ArsCombinatoria *65*, 97-110 (2002).
6. P.J. Davis, Circulant Matrices, 2 nd edition, Chelsea Publishing, New York (1994).
7. B. Elspas, J. Turner, Graphs with Circulant Adjacency Matrices, Journal of Combinatorial Theory *9*, 297-307 (1970).
8. E.J. Farrell, E. G. Whitehead, On Matching and Chromatic Properties of Circulants, Journal of Combinatorial Mathematics and Combinatorial Computing *8*, 79-88 (1990).
9. K. W. Lih, D. Der-Fen Liu, X. Zhu, Star Extremal Circulant Graphs, SIAM Journal of Discrete Mathematics *12*, 491-499 (1999).
10. M. Muzychuk, A Solution of the Isomorphism Problem for Circulant Graphs, Proceedings of the London Mathematical Society 88, Volume 1, 1-41 (2004).
11. V. Pless, Introduction to the Theory of Error Correcting Codes, John Wiley & Sons, Inc., New York (1998).
12. V.N. Sachkov, V.E. Tarakanov, Combinatorics of Nonnegative Matrices, Translations of Mathematical Monographs Vol. 213, American Mathematical Society, Providence, (2002).