ISSN 2231-346X (Print)
JUSPS-A Vol. 28(5), 251-258 (2016). Periodicity-Monthly
Section A
(Online) ISSN 2319-8044

JOURNAL OF ULTRA SCIENTIST OF PHYSICAL SCIENCES
An International Open Free Access Peer Reviewed Research Journal of Mathematics
website:- www.ultrascientist.org
Estd. 1989

Equivalent Circulant Graphs associated with a Binary Cyclic Code

GEORGE MATHEW

Department of Mathematics, BCM College Kottayam-686001, Kerala
Email of corresponding author : e- mail : gmathew5616x@gmail.com
http://dx.doi.org/10.22147/jusps-A/280504

Acceptance Date 30th August, 2016, Online Publication Date 2nd Oct. 2016

Abstract

Various papers have been written on the theory of circulant graphs [3, 6, 8, 10, 11]. Also graphs with circulant adjacency matrices is discussed in[7]. Circulant graphs have important applications to the theory of designs and error correcting codes[13]. The relationship between directed circulant graphs and binary linear codes is established in[9]. Each binary cyclic code corresponds to an equivalence class of directed circulant graphs. This paper discusses the method of determining the equivalent circulant graphs associated with a binary cyclic code.

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, 10, 11]. 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[13]. The relationship between circulant graphs and binary linear codes is established in[9]. This paper discusses the method of determining the equivalent circulant graphs associated with a binary cyclic code.

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.If G is a group and S is a subset of G\{e}, we say that a graph X is a ***Cayley graph*****[2]** of G with ***connectionset*** S written as X = Cay(G, S) if (i)V(X) = G (ii) A(X) = { (g, sg): g ∈ G & s ∈ S }. 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.

If F represents the binary field, then F^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.An [n, k] code C is called ***cyclic*** [12] if whenever $x = (a_0, a_1, \ldots\ldots\ldots\ldots, a_{n-1})$ is in C, so is its first cyclic shift $y = (a_{n-1}, a_1, \ldots\ldots\ldots\ldots, a_{n-2})$.

When considering cyclic codes it is useful to let a vector $(a_0, a_1, \ldots, a_{n-1})$ corresponds to a polynomial $a_0 + a_1x + \ldots\ldots + a_{n-1}x^{n-1}$. Then $(a_{n-1}, a_0, \ldots, a_{n-2})$ corresponds to $a_{n-1} + a_0x + \ldots\ldots + a_{n-2}x^{n-1}$. This polynomial equals the polynomial $(a_0 + a_1x + \ldots\ldots + a_{n-1}x^{n-1})x$ (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-ordinate wise and multiplication is modulo $(x^n - 1)$.A set of elements S in R_n corresponds to a cyclic code if and only if S is an ideal in R_n.We here assume that n is of the form 2^m-1. Note that when n is odd, x^n -1 has distinct factors.

The equivalence of circulant graphs and cyclic codes is established in the following theorem.

2.1. Theorem[9]*:*

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.

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

2.2. Theorem[9]*:*

Suppose X= Cay (Zn, S) be a circulant graph. Let C be the cyclic code representing X and k(x) the polynomial determined by S. 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.

3. Equivalence classes of circulant graphs :

The correspondence between circulant graphs and binary cyclic codes was established in Theorem 2.1and that the relation “two circulant graphs are equivalent if and only if both of them represents the same cyclic code” is an equivalence relation. We here develop a method to generate all the members belong to an equivalence class.

Let C be a cyclic code of length n. Let g(x) be its generator polynomial. Then the n x n matrix determined by the column vector

$$\begin{bmatrix} xg(x) \\ x^2g(x) \\ \vdots \\ x^{n-1}g(x) \\ g(x) \end{bmatrix}$$

is the adjacency matrix of a circulant graph which corresponds to C. We shall derive the condition under which

the matrix of sum of its consecutive rows

$$\begin{bmatrix} x(x+1)g(x) \\ x^2(x+1)g(x) \\ \vdots \\ (x^{n-1}+1)g(x) \\ (x+1)g(x) \end{bmatrix}$$

is again the adjacency matrix of another circulant graph which corresponds to C.It is the same as to derive the condition for the two sets Span{g(x), xg(x), x^2g(x),……,x^{n-1}g(x)} and Span {(x+1)g(x), x(x+1)g(x), x^2 (x+1)g(x),……., x^{n-1}(x +1)g(x),} are equal.The second set is clearly a subset of the first. Hence we want to derive the condition that the first set is asubset of the second. Let

u(x) = (x + 1)g(x). Then

Span {x(x+1)g(x), x^2(x+1)g(x),……,(x^{n-1} + 1)g(x), (x+1)g(x)} = Span{xu(x), x^2u(x), ……., x^{n-1}u(x), u(x)}
This is clearly a cyclic code. Therefore if g(x) $\in$ RHS, then xg(x),……,x^{n-1} g(x) are all elements of RHS. Now g(x) $\in$ RHS if we can find scalars $\beta_0, \beta_1, \ldots \ldots, \beta_{n-1}$ such that

$$g(x) = \beta_0 u(x) + \beta_1 x u(x) + \cdots + \beta_{n-1} x^{n-1} u(x)$$

That is

$$(1 + \beta_0(x+1) + \beta_1 x(x+1) + \cdots + \beta_{n-1} x^{n-1}(x+1))g(x) = 0 \ in R_n$$

$$= M(x^n - 1) \text{ in } F[x]$$

Since x^n-1 = g(x)h(x), this is the same as

$$(1 + \beta_0(x+1) + \beta_1 x(x+1) + \cdots + \beta_{n-1} x^{n-1}(x+1)) = M(h(x))$$

That is

$$(\beta_0 + \beta_{n-1}) + (\beta_0 + \beta_1)x + \ldots\ldots + (\beta_{n-2} + \beta_{n-1})x^{n-1} = 1 + M(h(x)) \quad (1)$$

Thus the matrix

$$\begin{bmatrix} x(x+1)g(x) \\ x^2(x+1)g(x) \\ \vdots \\ (x^{n-1}+1)g(x) \\ (x+1)g(x) \end{bmatrix}$$

corresponds C if and only if we can find scalars $\beta_0, \beta_1, \ldots \ldots, \beta_{n-1}$ satisfying condition (1)

3.1. Example :

Consider the length 7 cyclic code corresponding to the circulant graph Cay (Z_7, {1,3,4,6}). The generator polynomial of the code is

$g(x) = \gcd(x + x^3 + x^4 + x^6, x^7 - 1) = 1 + x$

Hence

$h(x) = (1 + x + x^3)(1 + x^2 + x^3)$

$\therefore 1 + h(x) = x + x^2 + x^3 + x^4 + x^5 + x^6$

Substituting this in equation (1) and equating coefficients of like terms on both sides, we get

$\beta_0 + \beta_6 = 0, \beta_0 + \beta_1 = 1, \beta_1 + \beta_2 = 1, \beta_2 + \beta_3 = 1, \beta_3 + \beta_4 = 1, \beta_4 + \beta_5 = 1, \beta_5 + \beta_6 = 1.$

The corresponding matrix equation is

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \\ \beta_4 \\ \beta_5 \\ \beta_6 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

Clearly this matrix equation is consistent, hence solvable. We can therefore apply the above result. By successive application of the result, we get each of the circulant graphs Cay (Z_7 ,{1,3,4,6}), Cay (Z_7 ,{4,5}) Cay (Z_7 ,{4,6}), Cay (Z_7 ,{1,4}), Cay (Z_7 ,{1,2,4,5}) belong to the same equivalence class all of them corresponds to the same cyclic code $C = \langle 1 + x \rangle$

Since consistency of the matrix equation is essential for obtaining a solution, the above result holds if and only if (1 + h(x)) is of even weight. That is h(x) is of odd weight. With the backup of the above discussions, we can now state the following theorem.

3.2. Theorem :

Let X = Cay (Z_n, k(x)) be a circulant graph that corresponds to a cyclic code C. Let g(x) be the generator polynomial of C and that g(x) h(x) = $x^n - 1$. Then Y = Cay (Z_n, (x + 1)k(x)) also corresponds to C if and only if h(x) is of odd weight.

3.3. Example

Let X = Cay (Z_7, {1,2,3})

Here

$g(x) = \gcd(k(x), x^7 - 1)$

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

$\therefore h(x) = x^7 - 1 = 0.$

Since h(x) is of even weight, the above theorem does not hold. In fact X = Cay (Z_7, {1,2,3}) = Cay (Z_7, $x + x^2 + x^3$) $\neq$ Cay (Z_7 , (x +1) ($x + x^2 + x^3$)) = Cay (Z_7, $x + x^4$) = Cay (Z_7, {1,4}) = Y.

Eventhough certain class of equivalent circulant graphs which corresponds to the same cyclic code can be determined by the above result, it will not be applicable in allcases as we have seen earlier. We therefore seek a unified way which brings the members of each class together.

3.4. Theorem

Suppose that the polynomials a(x) and b(x) represent two circulant graphs of length n. If C_1 and C_2 are the cyclic codes they correspond, then $C_1 = C_2$ if and only if there exist polynomials c(x) and d(x) which are respectively relatively prime to the generator polynomials of C_2 and C_1 such that c(x) a(x) = d(x) b(x)

Proof :

Let h(x) and k(x) be the generator polynomials of C_1 and C_2. Then

$h(x) = \gcd(a(x), x^n - 1)$ and $k(x) = \gcd(b(x), x^n - 1)$.

Suppose $C_1 = C_2$. Then h(x) = k(x). We have,

$a(x) = d(x)\, h(x)$ for some $d(x)$ relatively prime to $x^n - 1$. Similarly

$b(x) = c(x)\, k(x)$ for some $c(x)$ relatively prime to $x^n - 1$.

Now

$c(x)\, a(x) = d(x)\, b(x)$.

Since $c(x)$ is relatively prime to $x^n - 1$, it is relatively prime to $k(x)$. Since $d(x)$ is relatively prime to $x^n - 1$, it is relatively prime to $h(x)$.

Conversely suppose that there exist $c(x)$ and $d(x)$ with $\gcd(c(x), k(x)) = 1$ and $\gcd(d(x), h(x)) = 1$ and that $c(x)\, a(x) = d(x)\, b(x)$. Since $h(x) / a(x)$, $h(x) / d(x)\, b(x)$. Since $\gcd(d(x), h(x)) = 1$, $h(x) / b(x)$. At the same time $h(x) / x^n - 1$. Therefore $h(x) / k(x)$. Similarly, since $k(x) / b(x)$, $k(x) / c(x)\, a(x)$. Since $\gcd(c(x), k(x)) = 1$, $k(x) / a(x)$. At the same time $k(x) / x^n - 1$. Therefore $k(x) / h(x)$. Thus $h(x) = k(x)$, hence $C_1 = C_2$. This proves the theorem.

3.5. Corollary :

Let $a(x)$ and $b(x)$ be polynomials that represents two circulant graphs. Let C_1 and C_2 be the cyclic codes they correspond. If $b(x) = c(x)\, a(x)$ for some $c(x)$ relatively prime to $x^n - 1$, then $C_1 = C_2$.

Conversely if $a(x)$ and $b(x)$ represents the same code C, then there exist a polynomial $u(x)$ representing C such that $u(x) = \beta(x)\, a(x) = \alpha(x)\, b(x)$ for some $\alpha(x)$ and $\beta(x)$ relatively prime to $x^n - 1$

Proof :

The first part is an immediate consequence of the pervious theorem simply by taking $d(x) = 1$. Applying the same theorem to the converse part, we have two polynomials $\alpha(x)$ and $\beta(x)$ relatively prime to $x^n - 1$ such that

$\beta(x)\, a(x) = \alpha(x)\, b(x) = u(x)$ (say)

Then $\gcd(u(x), x^n - 1) = \gcd(\alpha(x)\, b(x), x^n - 1) = \gcd(b(x), x^n - 1) = k(x)$ and

$\gcd(u(x), x^n - 1) = \gcd(\beta(x)\, a(x), x^n - 1) = \gcd(a(x), x^n - 1) = h(x)$.

Hence C is also represented by $u(x)$ and that we have

$u(x) = \beta(x)\, a(x)$

$= \alpha(x)\, b(x)$ where $\alpha(x)$ and $\beta(x)$ relatively prime to $x^n - 1$.

3.6. Example :

Consider the circulant graphs $X = Cay(Z_7, \{3,4,5\})$ and $Y = Cay(Z_7, \{1,3,5\})$. The polynomials they represent are $x^3 + x^4 + x^5$ and $x + x^3 + x^5$. Suppose

$(x^3 + x^4 + x^5)(a_0 + a_1 x + \ldots\ldots + a_6 x^6) = x + x^3 + x^5$.

Equating coefficients on both sides

$a_2 + a_3 + a_4 = 0$, $a_3 + a_4 + a_5 = 1$, $a_4 + a_5 + a_6 = 0$, $a_0 + a_5 + a_6 = 1$

$a_0 + a_1 + a_6 = 0$, $a_0 + a_1 + a_2 = 1$, $a_1 + a_2 + a_3 = 0$

The equations are consistent and provide a unique solution

$a_0 = 1$, $a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 0$, $a_5 = 1$, $a_6 = 1$

$\therefore (x^3 + x^4 + x^5)(1 + x^5 + x^6) = x + x^3 + x^5$

Since $(1 + x^5 + x^6)$ is relatively prime to $x^7 - 1$, X and Y corresponds to the same code, Other equivalent circulant graphs are obtained by successively multiplying with $(1 + x^5 + x^6)$

$(x + x^3 + x^5)(1 + x^5 + x^6) = 1 + x^2 + x^4 + x^5 + x^6$

$(1 + x^2 + x^4 + x^5 + x^6)(1 + x^5 + x^6) = x + x^4 + x^5$

$(x + x^4 + x^5)(1 + x^5 + x^6) = 1 + x + x^2 + x^5 + x^6$

$(1 + x + x^2 + x^5 + x^6)(1 + x^5 + x^6) = 1 + x^2 + x^3 + x^5 + x^6$

$(1 + x^2 + x^3 + x^5 + x^6)(1 + x^5 + x^6) = x^5$

$x^5(1 + x^5 + x^6) = (x^3 + x^4 + x^5)$

Thus the circulant graphs $Cay(Z_7, \{3,4,5\})$, $Cay(Z_7, \{1,3,5\})$, $Cay(Z_7, \{1,4,5\})$, $Cay(Z_7, \{5\})$ are equivalent(excluding those containing 0 in the connection set,which are not considered as circulant graphs).

The above theorem is a means of getting a circulant graph equivalent to another and it is by just multiplying it with a polynomial relatively prime to $x^n - 1$. But it may sometimes produce only few equivalent

ones. For example, if n = 15, the polynomial $c(x) = x^7 + x^{10} + x^{13}$ is relatively prime to $x^{15} - 1$.Let $X = Cay(Z_{15}, \{1,2,3\})$. The polynomial it represents is $a(x) = x + x^2 + x^3$, $c(x)\,a(x) = 1 + x + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14}$, $c^2(x)\,a(x) = 1 + x + x^2 + x^6 + x^7 + x^8 + x^{12} + x^{13} + x^{14}$, $c^3(x)\,a(x) = x + x^2 + x^3 = a(x)$, thus produces only 3 different ones of which two are not considered circulant graphs. The following theorem gives us a useful way to bypass this difficulty.

3.7. Theorem :

Let $\beta(x)$ be a polynomial in R_n but not a power of x. If $\beta(x)$ is relatively prime to $x^n - 1$, then there exist a polynomial $\delta(x)$ not a power of x and relatively prime to $x^n - 1$ that generates a multiplicative group of order n.

Proof :

Consider the set G of all polynomials in R_n relatively prime to $x^n - 1$. If $\alpha(x)$ and $\beta(x)$ belong to G, then $\alpha(x)\,\beta(x)$ also belongs to G. Also by Euclidean algorithm, there exist polynomials a(x) and b(x) in F[x] such that $a(x)\,\alpha(x) + b(x)\,(x^n - 1) = 1$.Therefore $a(x)\,\alpha(x) = 1 \pmod{(x^n - 1)}$ and that a(x) is relatively prime to $x^n - 1$. Thus $\alpha(x)$ has inverse in G. Hence G is a group under multiplication modulo $x^n - 1$. We now claim that the order of every element of G is a divisor of n.

Consider the sequence of powers $\{\beta(x), \beta^2(x), \beta^3(x), \ldots\ldots\}$ of an element $\beta(x) \in G$. Since it is a subset of G and G is a finite group, $\beta^i(x) = \beta^j(x)$ for come $j < i$. But then

$\beta^j(x)\,(1 + \beta^{i-j}(x)) = 0$ in R_n, hence

$\beta^j(x)\,(1 + \beta^{i-j}(x)) = M(x^n - 1)$.

Since $\beta^j(x)$ is relatively prime to $x^n - 1$, we get $(1 + \beta^{i-j}(x)) = 0$ in R_n. Therefore $\beta^h(x) = 1$ for some h and the set $\{\beta(x), \beta^2(x), \beta^3(x), \ldots\ldots, \beta^h(x) = 1\}$ is therefore a cyclic subgroup of G. We now prove that $o(\beta)$ is a divisor of n.Let

$\beta(x) = c_0 + c_1x + \ldots\ldots\ldots + c_{n-1}x^{n-1}$. Then

$$\beta^{n+1}(x) = (c_0 + c_1x + \ldots\ldots\ldots + c_{n-1}x^{n-1})^{2^m}$$

$$= c_0 + c_1(x^{2^m}) + \ldots\ldots\ldots + c_{n-1}(x^{2^m})^{n-1}$$

$$= c_0 + c_1x + \ldots\ldots\ldots + c_{n-1}x^{n-1}$$

$$= \beta(x)$$

$\therefore \beta^{n+1}(x) - \beta(x) = 0$ in R_n.

$= M(x^n - 1)$ in F[x]. That is

$\beta(x)\,(\beta^n(x) - 1) = M(x^n - 1)$. Since $\gcd(\beta(x), x^n - 1) = 1$, we get $\beta^n(x) - 1 = 0$ in R_n or $\beta^n(x) = 1$, thus $o(\beta(x))$ is a divisor of n.

We now claim that there is a $\delta \in R_n$ relatively prime to $x^n - 1$, not a power of x but of order n. Suppose $p_1 < p_2 < \ldots\ldots < p_k$ be the prime divisors of n. Choose an $\alpha \in G$ not a power of x but relatively prime to $x^n - 1$. If $o(\alpha) = n$, we take $\delta = \alpha$ and the theorem holds. Suppose $o(\alpha) \neq n$. Since $o(\alpha)$ is a divisor of n, we can take

$$o(\alpha) = p_1^{h_1} \ldots\ldots p_i^{h_i} \ldots\ldots p_k^{h_k}$$

Then

$$\alpha^{p_1^{h_1} \ldots\ldots p_i^{h_i} \ldots\ldots p_k^{h_k}} = 1$$

$$\therefore ((\alpha^{p_2^{h_2} \ldots\ldots p_i^{h_i} \ldots\ldots p_k^{h_k}})^{p_1^{h_1 - 1}})^{p_1} = 1.$$ Let

$\beta = (\alpha^{p_2^{h_2} \ldots\ldots p_i^{h_i} \ldots\ldots p_k^{h_k}})^{p_1^{h_1 - 1}}$. Then $\beta^{p_1} = 1$, hence $o(\beta) = p_1$

Take $\gamma(x) = x\,\beta(x)$. If $o(\gamma) = M(p_1) = z\,p_1$, then $1 = \gamma^{zp_1} = x^{zp_1}\beta^{zp_1}$, hence $x^{zp_1} = 1$. But then $n = z\,p_1$. The theorem therefore holds if we take $\delta = \gamma$. On the other hand, if $o(\gamma) \neq M(p_1)$, then $o(\gamma) = w\,p_j$ for some $j > 1$ and $\gcd(p_1, w) = 1$

Now $\gamma^{wp_j} = 1$. Therefore $x^{wp_j}\beta^{wp_j} = 1$. Hence $x^{wp_1p_j}\beta^{wp_1p_j} = 1$. It follows that $x^{wp_1p_j} = 1$, hence w $p_1p_j = n$. Now $o(\beta) = p_1$, $o(\gamma) = w\, p_j$ and $\gcd(p_1, w\, p_j) = \gcd(p_1, w) = 1$. Therefore $o(\beta\gamma) = w\, p_1p_j = n$. The theorem therefore holds if we take $\delta = \beta\gamma$ and the proof is complete.

3.8. Example :

Consider $R_7 = \frac{F[x]}{<x^7-1>}$

We have

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

The polynomial $\beta(x) = x^2 + x + 1 \in R_7$ is relatively prime to $x^7 - 1$. Since n = 7, $o(\beta) = 7$. In fact, $\beta^2 = x^4 + x^2 + 1$, $\beta^3 = x^6 + x^5 + x^3 + x + 1$, $\beta^4 = x^4 + x + 1$, $\beta^5 = x^6 + x^5 + x^4 + x^3 + 1$, $\beta^6 = x^6 + x^5 + x^3 + x^2 + 1$ and $\beta^7 = 1$

3.9. Example :

$$R_{15} = \frac{F[x]}{< x^{15} - 1 >}$$

We have

$x^{15} - 1 = (x-1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)$

The polynomial $\beta(x) = x^{13} + x^{10} + x^7$ is relatively prime to $x^{15} - 1$

$\beta^4(x) = (x^{13} + x^{10} + x^7)^4 = x^{13} + x^{10} + x^7 = \beta(x)$, therefore $o(\beta) = 3$. Take

$\delta(x) = x\,\beta(x) = x^{14} + x^{11} + x^8$, then $\delta^3(x) \neq 1$, $\delta^5(x) \neq 1$. It follows that $o(\delta) = 15$.

3.10. Example :

Consider the circulant graph $X = Cay(Z_{15}, \{1,2\})$. We shall find all the circulant graph equivalent to X. To do so we take the polynomial $\delta(x) = x^8 + x^{11} + x^{14}$ which is relatively prime to $x^{15} - 1$ and is of order 15. Multiplying the polynomial $k(x) = x + x^2$ represented by X with $\delta(x)$ and its powers, we get the following polynomials.

$1 + x + x^9 + x^{10} + x^{12} + x^{13}$, $1 + x^2 + x^3 + x^8 + x^9 + x^{14}$, $x^4 + x^5$, $1 + x + x^3 + x^4 + x^{12} + x^{13}$, $x^2 + x^3 + x^5 + x^6 + x^{11} + x^{12}$, $x^7 + x^8$, $1 + x + x^2 + x^4 + x^6 + x^7$, $1 + x^5 + x^6 + x^8 + x^9 + x^{14}$, $x^{10} + x^{11}$, $x^3 + x^4 + x^6 + x^7 + x^9 + x^{10}$, $x^2 + x^3 + x^8 + x^9 + x^{11} + x^{12}$, $x^{13} + x^{14}$, $x^6 + x^7 + x^9 + x^{10} + x^{12} + x^{13}$, $1 + x^5 + x^6 + x^{11} + x^{12} + x^{14}$.

This leads to the equivalent circulant graphs $Cay(Z_{15}, \{4,5\})$, $Cay(Z_{15}, \{2,3,5,6, 11,12\})$, $Cay(Z_{15}, \{7,8\})$, $Cay(Z_{15}, \{10,11\})$, $Cay(Z_{15}, \{3,4,6,7,9.10\})$, $Cay(Z_{15}, \{2,3,8,9,11,12\})$, $Cay(Z_{15}, \{13,14\})$, $Cay(Z_{15}, \{6,7,9,10,12,13\})$.

Each one of the above leads a subfamily of equivalent ones. For example $Cay(Z_{15}, \{1,2\})$ leads the subfamily consists of its cyclic shifts namely $Cay(Z_{15}, \{2,3\})$, $Cay(Z_{15}, \{3,4\})$, $Cay(Z_{15}, \{4,5\})$, $Cay(Z_{15}, \{5,6\})$, $Cay(Z_{15}, \{6,7\})$, $Cay(Z_{15}, \{7,8\})$, $Cay(Z_{15}, \{8,9\})$, $Cay(Z_{15}, \{9,10\})$, $Cay(Z_{15}, \{10,11\})$, $Cay(Z_{15}, \{11, 12\})$, $Cay(Z_{15}, \{12, 13\})$ and $Cay(Z_{15}, \{13,14\})$.

4. Use of cyclotomic cosets :

The concept of cyclotomic cosets can be used to determine equivalent circulant graphs when we deal with binary cyclic codes of comparatively higher length.

4.1. Definition[12]*:*

If $0 < s < 2^m - 1$, and r is the smallest number with the property that $2^{r+1}\, s \equiv s \pmod{(2^m - 1)}$ then the set $\{s, 2s, 2^2s, 2^3s, \ldots, 2^rs\}$ where each $2^i s$ is reduced mod $(2^m - 1)$ is called the ***cyclotomic coset*** containing s.

4.2. Example :

Let $X = Cay(Z_{63}, \{1,3,5\})$. The cyclotomic cosets of 63 are

$C_0 = \{0\}$ $C_1 = \{1, 2, 4, 8, 16, 32\}$

$C_3 = \{3, 6, 12, 24, 48, 33\}$ $C_5 = \{5, 10, 20, 40, 17, 34\}$

$C_7 = \{7, 14, 28, 56, 49, 35\}$ $C_9 = \{9, 18, 36\}$
$C_{11} = \{11, 22, 33, 44, 25, 50, 37\}$ $C_{13} = \{13, 26, 52, 41, 19, 38\}$
$C_{15} = \{15, 30, 60, 57, 51, 39\}$ $C_{21} = \{21, 42\}$
$C_{23} = \{23, 46, 29, 58, 53, 43\}$ $C_{27} = \{27,54,45\}$
$C_{31} = \{31,62, 61, 59,55,47\}$

From this computation we can tell that $x^{63} - 1$ is the product of nine irreducible polynomials of degree 6, two irreducible polynomials of degree 3, one irreducible polynomial of degree 2 and one irreducible polynomial of degree 1. Since there is only one binary irreducible polynomial of degree 1 which is $x + 1$ and only one binary irreducible polynomial of degree 2 which is $x^2 + x + 1$ and two binary irreducible polynomials of degree 3 which are $x^3 + x + 1$ and $x^3 + x^2 + 1$ we can infer that $x + 1$, $x^2 + x + 1$, $x^3 + x + 1$ and $x^3 + x^2 + 1$ are factors of $x^{63} - 1$. Hence there are no binary polynomials of degree less than or equal to 3 relatively prime to $x^{63} - 1$. At the same time, $x^{63} - 1$ has no factors of degree 4. Hence every fourth degree irreducible polynomial is relatively prime to $x^{63} - 1$. One among them can therefore be taken as δ.

Let $\delta(x) = x^4 + x + 1$. Since $63 = 3^2 . 7$. The factors of 63 are 3,7 and 9. We have

$\delta^3(x) = x^{12} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1 \neq 1$

$\delta^7(x) = x^{28} + x^{25} + x^{24} + x^{22} + x^{20} + x^{19} + x^{18} + x^{17} + x^{13} + x^{10} + x^9 + x^7 + x^5 + x^3 + x^2 + x + 1 \neq 1$

$\delta^9(x) = x^{20} + x^{17} + x^{16} + x^5 + x^4 + x^2 + 1 \neq 1$

$o(\delta)$ is therefore not equal to 3 or 7 or 9. It follows that $o(\delta) = 63$. Multiplying the polynomial $k(x) = x + x^3 + x^5$ determined by X successively by powers of δ, we get the leaders of the sub families of the equivalent class of circulant graphs corresponds to the binary cyclic code $C = < g(x) >$ where $g(x) = \gcd(k(x), x^{63} - 1) = \gcd(x(x^2 + x + 1)^2, x^{63} - 1) = x^2 + x + 1$. Multiplying each of the subfamily leaders successively by powers of x, we get the members of the subfamily it represents. We can thus find all the members of the equivalent class ■

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, *Ars Combinatoria 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. George Mathew, Directed Circulant Graphs and Binary Cyclic Codes, *J. Ultra Scientist of Physical Sci., 28(4)A*, 197-203 (2016).
10. K. W. Lih, D. Der-Fen Liu, X. Zhu, Star Extremal Circulant Graphs, *SIAM Journal of Discrete Mathematics 12*, 491-499 (1999).
11. M. Muzychuk, A Solution of the Isomorphism Problem for Circulant Graphs, *Proceedings of the London Mathematical Society* 88, Volume *1*, 1-41 (2004).
12. V. Pless, Introduction to the Theory of Error Correcting Codes, John Wiley & Sons, Inc., New York (1998).
13. V. N. Sachkov, V. E. Tarakanov, Combinatorics of Nonnegative Matrices, *Translations of Mathematical Monographs* Vol. 213, American Mathematical Society, Providence, (2002).