Quadratic Residues of Commutative Rings

Shakila Banu P
Assistant professor of Mathematics
Vellalar College for Women,Thindal,
Erode, India
shakimeeran10@gmail.com

Suganthi T
B.T.Assistant of Mathematics
Govt.Hr.Sec.School,Vadugam
Namakkal , Tamilnadu
sugan1306thi@gmail.com

ABSTRACT

The structure of the quadratic residues and non-residues of a ring is introduced in this study as $Z_P+wZ_p+w^2Z_p+\ldots+w^{k-1}Z_p$,$w^k=1$,p=2,3. We discover the universal formula for the ring's total number of quadratic residues. By integrating graph theory with algebraic concepts, certain complete graphs were discovered in the ring.

Keywords: Commutative ring, Quadratic Residues, Complete graph

I. INTRODUCTION

The theory of algebraic integers and the theory of polynomial rings are the roots of ring theory research. Zahlring was first used by David Hilbert in 1897. A set is a ring that has two binary operations and meets certain criteria. If multiplication is commutative, then the ring is as well. Rings that are commutative are simpler to comprehend than those that are not. David S. Dimmit investigated rings and commutative rings [1]. In [1-4], many number kinds and their characteristics were examined.In the seventeenth and eighteenth century, Fermat, Euler, Lagrange, and Legendre investigated the quadratic residues of an integer. For factoring big numbers and acoustical engineering, quadratic residues are used. Finding quadratic residues of an integer and counting them is simple. However, it is not possible to count the quadratic residues of a commutative ring in the same way as an integer. We utilised residue properties of commutative chain or non-chain rings to graphs in order to put the transition from ring theory to graph theory. In [7], graphs and their byproducts, such as cartesian, lexiographic, tensor, and strong products, were investigated. If the squares of vertices a and b under mod n are the same, Rezaei [6] defined graphs whose vertex set is a reduced residue system mod n such that two different vertices a and b are nearby. In [8], graphic code structures were found. The quadratic residues and non-residues of a commutative ring $Z_P+wZ_p+w^2Z_p+\ldots+w^{k-1}Z_p$,$w^k=1$,p=2,3 are studied in this article. We discover the generic formula to count the ring's quadratic residues.We learned about various regular graphs from the ring's residue feature.

II. PRELIMINARIES

In this section, we look into certain basic ring theory and graph theory ideas.

- A *set* is the mathematical representation of a group of different objects. A set's elements or members can be any type of mathematical object, including numbers, symbols, lines, points in space, other geometric structures, variables, or even other sets.

- A *group* is a set S that is nonempty and has the binary operation: $\ast : S\times S \rightarrow S$ satisfying the axioms listed below:
  (i) Closure: if a, b $\in$ S, then $a \ast b \in S$.
  (ii) Associativity: $a \ast (b \ast c)=(a \ast b) \ast c$ for all a, b, c $\in$ S.
  (iii) Identity: there is an element e $\in$ S, such that $a \ast e = e \ast a = a$ for all a $\in$ S.
  (iv) Inverse: for each element a $\in$ S, there is an element b $\in$ S such that $a \ast b = e = b \ast a$.
- A group S is said to be *abelian* (or commutative) if $a \ast b = b \ast a$ for all a, b $\in$ S.

Example: 2.1
$\mathbb{Z}$ is an addition-based abelian group.
A ring is a nonempty set R with two binary operations + and × that satisfy the following operations:
(i)(R, +) is an abelian group.
(ii)(R, ×) is monoid
(iii)(R, ×)hold distributive laws over addition.
Ring R is called a commutative ring if it holds commutative under multiplication.
A commutative ring with unity is field if every element of R has multiplicative inverse.

In order to obtain graphs from commutative ring ,we must to know certain fundamentals of graph theory.

Graph theory is the study of mathematical constructions used to represent pairwise relationship between objects. A graph is a mathematical structure made up of a collection of points called vertices and a set of lines connecting various pairs of vertices, some of which may be empty. There is a chance that the edges will be directed, or orientated. If the lines are directed or undirected, respectively, they are referred to as arcs or edges. Let G=(V,E) be a graph ,where V is the set of all vertices and E={(x is adjacent to y /x and y are vertices of V}.

A simple graph is one in which no two vertices are connected by more than one edge, and no edge begins or finishes at the same vertex. In other words, a simple graph is one that does not contain loops or many edges. If an edge (arc) connects two vertices, they are said to be adjacent by. Each vertex in a directed graph has a direction attached to it, and the vertices have connections by edges.

Arrows indicating in the direction the graph can be traversed are usually utilised to denote edges. The edges in an undirected graph are bidirectional and have no associated direction. As a result, either direction can be used to traverse the graph. The graph is undirected because there isn't an arrow present. A complete graph is one in which there is precisely one edge connecting each pair of vertices.

- The exact number nC_2 of edges are present in a complete graph of 'n' vertices.
- A complete graph with 'n' vertices is denoted as K_n.

Example:2.2

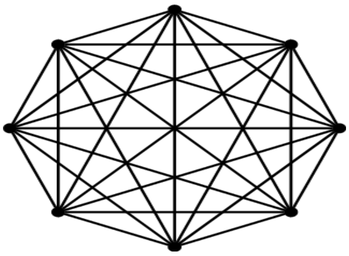


Figure:1 K_8

III. QUADRATIC RESIDUES

In this section,we study the structure of elements of the ring Ṙ = $Z_P+wZ_p+w^2Z_p+\dots.+w^{k-1}Z_p$,w^k=1,p=2,3. Quadratic residues and quadratic non-residues of the ring were discovered of the ring.

In number theory,an integer q is called quadratic residue of n if there exists an integer x such that $x^2 \equiv q$(mod n).otherwise q is called quadratic non-residue of n.

Example:2.3

Let Z_7={0,1,2,3,4,5,6}.

Since all the elements of commutative ring Z_7 has multiplicative inverse , Z_7 is a field.

1^2=1(mod 7), 2^2=4(mod 7)

3^2=2(mod 7), 4^2=2(mod 7), 5^2=4(mod 7), 6^2=1(mod 7)

Therefore, quadratic residues of Z_7={1,2,4}

A.Quadratic Residues over ₿= $Z_2+u\,Z_2+u^2\,Z_2+\dots.+u^{k-1}\,Z_2$,u^k=1

Consider ₿= $Z_2+u\,Z_2+u^2\,Z_2+\dots.+u^{k-1}\,Z_2$,u^k=1 where Z_2={0,1}.

Every element ȝ of ₿ is of the form $a+bu+cu^2+\dots.+ru^{k-1}$,Here a,b,c,r ∈ Z_2.

An element of ₿ is called a quadratic residue if ȝ² ≡ ŋ (mod u^k=1)

Consider the ring, ₿₂ .= Z_2+uZ_2={0,1,u,1+u}, u^2=1.since ₿₂ satisfy the commutative ring properties, ₿₂ is a commutative ring.The set of all quadratic residue of ₿₂ is ṙ₂ ={1,0} and the set of all quadratic non-residues ={u,1+u}. Let ₿₃= $Z_2+uZ_2+u^2Z_2$, u^3=1 is a commutative ring .₿₃= {0,1,u,1+u,u^2,1+ u^2,u+ u^2,1+ u+ u^2}

Quadratic residues ṙ₃ =₿₃.Let ₿₄= $Z_2+uZ_2+u^2Z_2+u^3\,Z_2$, u^4=1.

₿₄={0,1,u,1+u,u^2,1+ u^2,u+ u^2,1+u+u^2,u^3, 1+ u^3,u+ u^3,1+u+u^3,u^2+u^3,1+ u^2+u^3,u+ u^2+u^3,1+ u+ u^2+u^3}

Residues of ₿₄ is ṙ₄={0,1+ u^2, 1+ u+u^2, 1+ u+u^3}

Let ₿₅= $Z_2+uZ_2+u^2Z_2+u^3Z_2+u^4Z_2$, u^5=1.In this ring ṙ₅= ₿₅.

continuing in this way,we obtain all the elements and quadratic residues of the commutative ring $Z_2+uZ_2+u^2\,Z_2+\dots.+u^{k-1}Z_2$ where ,u^k=1.

Theorem:3.1

Let ₿ₙ= $Z_2+u\,Z_2+u^2\,Z_2+\dots.+u^{k-1}\,Z_2$,u^k=1 be a commutative ring.Then the number of quadratic residues of

$$₿n = \begin{cases} k, u^k = 1 \; and\ k\ is\ even\ \ number \\ 2^k, u^k = 1 \; and\ k\ is\ odd\ number \end{cases}$$

B.Quadratic Residues over Ꜩ=$Z_3+vZ_3+v^2Z_3+\dots.+v^{k-1}Z_3$,v^k=1

In this section,we study the structure of elements and quadratic residues and quadratic non-residues of the ring $Z_3+vZ_3+v^2Z_3+\dots.+v^{k-1}Z_3$,v^k=1.

Consider Ꜩ = $Z_3+vZ_3+v^2Z_3+\ldots.+v^{k-1}Z_3$,$v^k=1$ where $Z_3=\{0,1,2\}$.

Every element ꜩ of Ꜩ is of the form $a+bv+cv^2+\ldots.+rv^{k-1}$,Here a,b,c,..r ε Z_3.

Consider the ring, $Ꜩ_2=Z_3+vZ_3$, $v^2=1$.

$Ꜩ_2=\{0,1,v,1+v,2v,1+2v,2,2+v,2+2v\}$

since $Ꜩ_2$ satisfy the commutative ring properties,$Ꜩ_2$ is a commutative ring.The set of all quadratic residue of the ring is $ẗ_2=\{1,2+2v,2+v\}$and the set of all quadratic non-residues $=\{0,v,1+v,2v,1+2v,2\}$.

Let $Ꜩ_3 = Z_3+vZ_3+v^2Z_3$, $v^3=1$ is a commutative ring.

$=\{0,1,2,v,2v,1+v,2+v,1+2v,2+2v,v^2,1+v^2,2+v^2,v+v^2,2v+v^2,1+v+v^2,2+v+v^2,1+2v+v^2,2+2v+v^2,2v^2,$
$1+2v^2,2+2v^2,v+2v^2,2v+2v^2,1+v+2v^2,2+v+2v^2,1+2v+2v^2, 2+2v+2v^2\}$

Quadratic residues $ẗ_3=\{0,1,v^2,1+2v+v^2,2v+2v^2,2+2v, 2+2v^2,1+v+v^2,v,2+v+v^2,1+v+2v^2\}$.

Let $Ꜩ_4 = Z_3+vZ_3+v^2Z_3+v^3Z_3$, $v^4=1$.

$Ꜩ_4 =\{0,1,2,v,2v,1+v,2+v,1+2v,2+2v,v^2,1+v^2,2+v^2, v+v^2,2v+v^2,1+v+v^2,2+v+v^2,1+2v+v^2,2+2v+v^2,2v^2,1+2v^2,2+2v^2,v+2v^2,2v+2v^2,1+v+2v^2,2+v+2v^2,1+2v+2v^2,2+2v+2v^2,v^3,1+v^3,2+v^3,v+v^3,2v+v^3,1+v+v^3,2+v+v^3,1+2v+v^3,2+2v+v^3,v^2+v^3,1+v^2+v^3, 2+v^2+v^3, v+v^2+v^3,2v+v^2+v^3,,1+v+v^2+v^3,2+v+v^2+v^3,1+2v+v^2+v^3,2+2v+v^2+v^3,2v^2+v^3,1+2v^2+v^3,2+2v^2+v^3,v+2v^2+v^3,2v+2v^2+v^3,1+v+2v^2+v^3, 2+v+2v^2+v^3,1+2v+2v^2+v^3,2+2v+2v^2+v^3,2v^3,1+2v^3,2+2v^3,v+2v^3,2v+2v^3,1+v+2v^3,,2+v+2v^3,1+2v+2v^3,2+2v+2v^3, v^2+2v^3,1+v^2+2v^3,2+v^2+2v^3,v+v^2+2v^3,2v+v^2+2v^3,1+v+v^2+2v^3,2+v+v^2+2v^3,1+2v+v^2+2v^3,2+2v+v^2+2v^3,2v^2+2v^3,1+2v^2+2v^3,2+2v^2+2v^3,v+2v^2+2v^3,2v+2v^2+2v^3,1+v+2v^2+2v^3,2+v+2v^2+2v^3,1+2v+2v^2+2v^3,2+2v+2v^2+2v^3\}$

Residues of $Ꜩ_4$ is $ẗ_4=\{v^2,2+2v^2,1+2v^2,1,1+v^2+2v^3, 1+v^2+v^3, 1+2v+v^2, 2v+2v^2+2v^3, 2+2v+2v^2+v^3, 1+v+v^2, v+2v^2+v^3,2+v^2,v+2v^3,2v+v^3,1+2v+v^2,2+2v+2v^3,1+2v+v^2+2v^3,2+v+v^3,1+v+v^2+v^3,2+v+2v^2+2v^3\}$

continuing in this way,we obtain the elements and quadratic residues of the commutative ring $Z_3+vZ_3+v^2Z_3+\ldots.+v^{k-1}Z_3$,$v^k=1$.

Theorem:3.2

Let Ꜩ = $Z_3+vZ_3+v^2Z_3+\ldots+v^{k-1}Z_3$,$v^k=1$ be a commutative ring.Then the number of all quadratic residues of

$$Ꜩ=\begin{cases} 2^k-1, if\ u^k=1, k=2 \\ 2^k+1,\ \ if\ u^k=1, k>2\ and\ k\ is\ positive\ integer \end{cases}$$

IV.QUADRATIC RESIDUE GRAPH OVER Ṙ $=Z_P+w Z_p+w^2 Z_p+\ldots.+w^{k-1} Z_p$,$w^k=1$

A simple graph G is a quadratic residue graph G_n [7] with vertex set V and edge set E where

$V(G_n)=\{a\in Z/(a,n)=1$ and $a<n\}$ and $E(G_n)=\{ab/a,b\in V(G_n)$ and $a^2\equiv b^2 \pmod n\}$

Let $Z_{12}=\{0,1,2,3,4,5,6,7,8,9,10,11\}$

$V(G_{12})=\{0,1,2,3,4,5,6,7,8,9,10,11\}$

Here,$1^2=5^2=7^2=11^2\equiv1$(mod 12),$2^2=4^2=8^2=10^2\equiv4$ (mod 12),$3^2= 9^2\equiv49$(mod 12), $0^2= 6^2\equiv0$(mod 12)

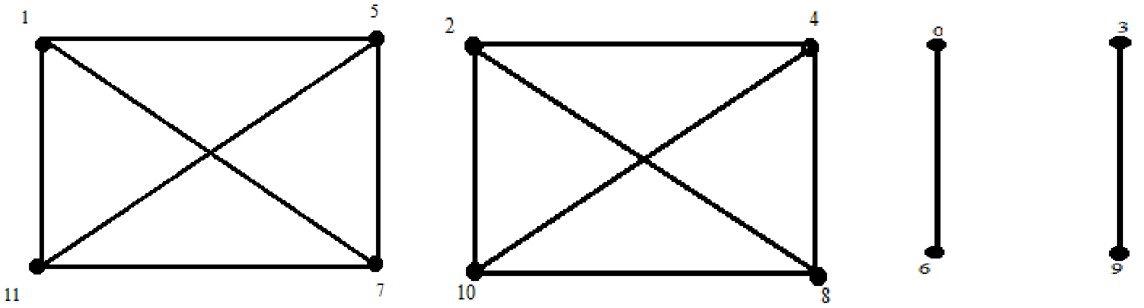


Figure 2: G(Z_{12})

In this section ,we study anbout quadratic residue graph over $Z_P+w Z_p+w^2 Z_p+\ldots.+w^{k-1} Z_p$,$w^k=1$, p=2 or 3.if their vertex sets are reduced residue systems mod $w^k=1$.

V(G)={a ∈ Ṙ}

E(G)={a is adjacent to b/a,b ∈ V(G) and $a^2=b^2$ (mod $w^k=1$)}.Here,w 's are congruent under $w^k=1$ and element of Z_p are congruent under modulo p in the product and addition of polynomials over Ṙ.

Throughout this paper,we consider G is undirected graph only.

Theorem:4.1

Let G($฿_n$)=(V,E), be a quadratic residue graph where n is even .Then the graph is n types of complete graph and $|V|=2^n$.

Example:

Let $฿_4= Z_2+uZ_2+u^2Z_2+u^3Z_2$, $u^4=1$.

This is commutative ring has four quadratic residues twelve quadratic non residues.

The graph generated by the ring $฿_4$ is a Quadratic residue graph which has the following vertices and edges :

$V(G)=\{0,1,u,1+u,u^2,1+u^2,u+u^2,1+u+u^2,u^3, 1+u^3,u+u^3,1+u+u^3,u^2+u^3,1+u^2+u^3,u+u^2+u^3,1+u+u^2+u^3\}$

$E(G)=\{(0,1+u^2),(0,1+u+u^2+u^3),(1+u^2, 1+u+u^2+u^3),(u^2, u+u^2+u^3)(1,1+u+u^3),(1,u^2),(1, u+u^2+u^3),(u+u^2+u^3, 1+u+u^3),(u^2, 1+u+u^3),(u,u^3),(u,1+u^2+u^3), (u,1+u+u^2), (u^3,1+u^2+u^3), (1+u+u^2,1+u^2+u^3),(u^3, 1+u+u^2),(u+u^2,u+u^3),$

$(u+u^2,u^2+u^3),(1+u^3,1+u),(1+u^3,u^2+u^3),(u+u^3,1+u), (u+u^2,1+u^3),(1+u^3,u+u^3),(1+u,u^2+u^3),(u+u^3,u^2+u^3), (u+u^2,1+u)\}$

Quadratic binary Residue graph is given below:

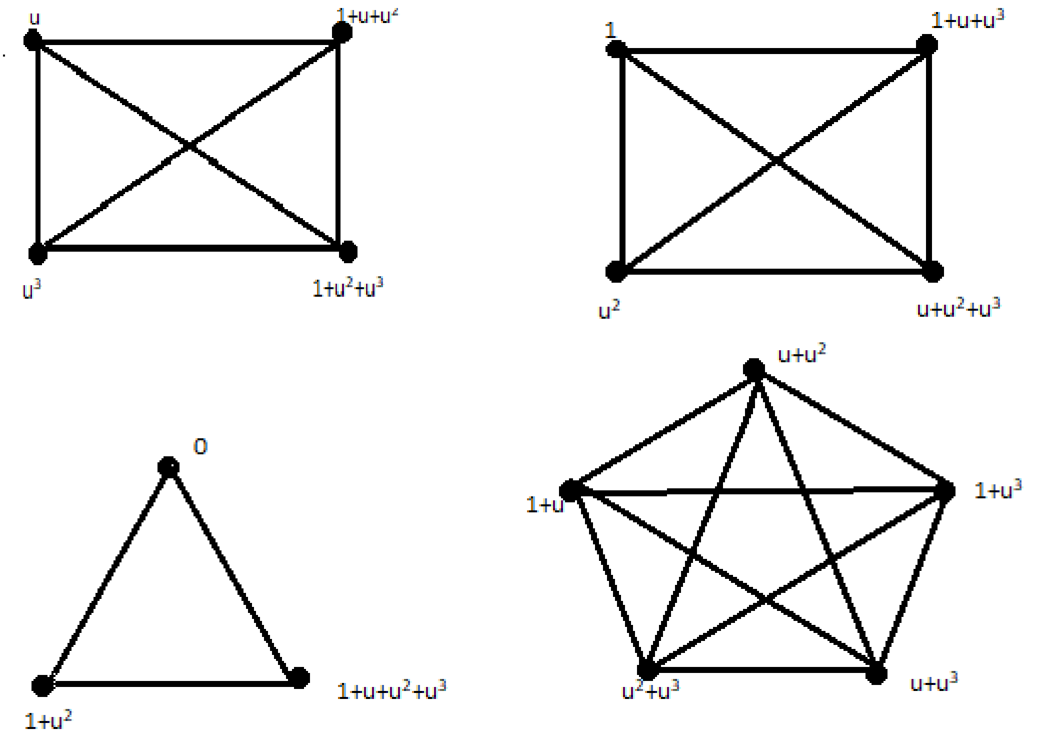


Figure 3: **G(฿₄)**

Theorem:4.2

Let G(₮)=(V,E), be a quadratic residue graph .Then the graph is 3 types of complete graph with $|V|=3^n$

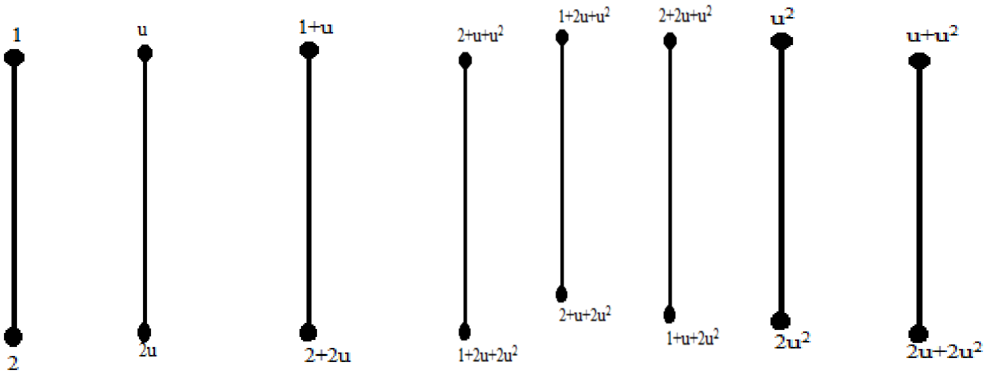
Example:

Let Ꜩ4 = $Z_3+vZ_3+v^2Z_3+ v^3 Z_{3,} v^4=1$.

It is a commutative ternary ring with eighty one elements .Quadratic residue graph obtained from the ring with the following vertices ..

$V(G^*) =\{0,1,2,v,2v,1+v,2+v,1+2v,2+2v,v^2,1+v^2,2+ v^2, v+ v^2,2v+ v^2,1+v+ v^2,2+v+ v^2,1+2v+ v^2,2+2v+ v^2,2v^2,1+2 v^2,2+2 v^2,v+2 v^2,2v+2 v^2,1+v+2 v^2,2+v+2 v^2,1+2v+2 v^2,2+2v+2 v^2 \}$

Quadratic Ternary Residue graph over Ꜩ4 is shown below:



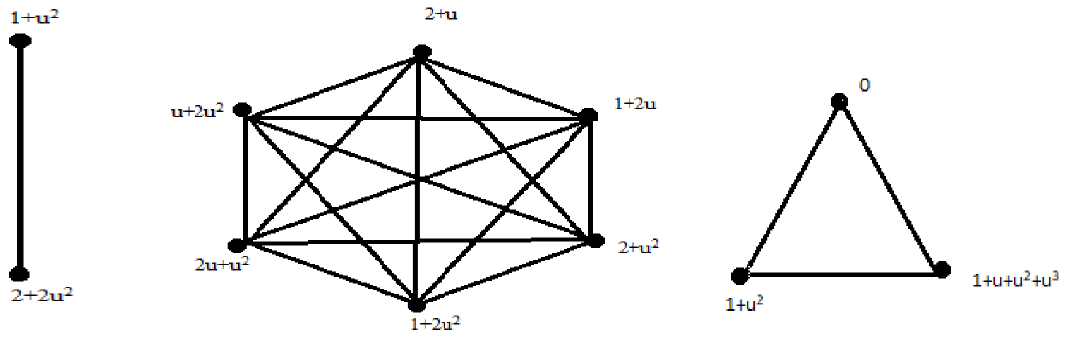


Figure 3: G(Tʒ4)

Conclusion:

We describe the structure of quadratic residues in a commutative ring in this study. Complete graphs were found in the ring by using algebraic ideas to graph theory. The author hopes to expand the work to include the encoding and decoding of commutative rings in future research.

REFERENCES

[1] David S.Dummit,Richard M.Foote,Abstract algebra,third edition,Wiley India Pvt.Ltd.,Delhi,(2014).ISBN:978-81-265-3228-5.

[2] G. H.Hardy,E. M. Wright, An introduction to the theory of numbers (fifth ed,(1980).), Oxford: Oxford University Press.

[3] Ireland, Kenneth, Rosen, and Michael, A classical introduction to modern number theory,(second ed.), New York: Springer (1990).

[4] H. Kenneth, Rosen, Elementary number theory and its application, Addison-Wesley Publishing company,(1984).

[5] Lemmermeyer, Franz, Reciprocity laws: from Euler to Eisenstein, Berlin: Springer, (2000).

[6] F.J.Macwilliams,Theory of error correcting codes,North-Holland Mathematical library,(1983).

[7] Rezaei, Mehdi & Rehman, Shafiq & Khan, Zia & Baig,A, & Farahani, Mohammad, Quadratic residues graphs , International Journal of Pure and Applied Mathematics,vol.113. pp.465-470. 10.12732/ijpam.v113i3.8.(2017).

[8] F.Harray, Graph theory, Addison Wesley,(1969).

[9] El. Rouayheb,Salim &Geroghiades,Costas,Graph theorectic methods in coding Theory, vol.10, 1007/978-1-4419-6624-7-5,(2011).