Mathematics and Statistics 11(2): 434-439, 2023
DOI: 10.13189/ms.2023.110222 http://www.hrpub.org

Cartesian Product of Quadratic Residue Graphs

Shakila Banu.P.[1], **Suganthi.T.**[2,*]

[1]Assistant Professor, Department of Mathematics, Vellalar College for Women, India

[2]B.T.Assistant of Mathematics, Govt. Higher Secondary School, India

Received October 13, 2022; Revised February 17, 2023; Accepted March 12, 2023

Cite This Paper in the following Citation Styles

***(a)**: [1] Shakila Banu.P, Suganthi.T, "Cartesian Product of Quadratic Residue GraphsCartesian Product of Quadratic Residue Graphs," Mathematics and Statistics, Vol.11, No.2, pp. 434-439, 2023. DOI: 10.13189/ms.2023.110222*

***(b)**: Shakila Banu.P, Suganthi.T, (2023). Cartesian Product of Quadratic Residue Graphs. Mathematics and Statistics, 11(2), 434-439. DOI: 10.13189/ms.2023.110222*

Abstract Rezaei [7], who introduced the first simple graph G, defined it as a quadratic residue graph modulo n if its vertex set is reduced, a residue system modulo n such that two different vertices a and b are nearby, and $a^2 \equiv b^2 (\text{mod } n)$. This initiates to study the present article, here we introduce a cartesian product of quadratic residue graphs $F = G_m \circ H_n$, where m and n are either prime or composite, and G_m and H_n are quadratic residue graphs, respectively. The aforementioned work suggests and evaluates the regular graphs that are produced from graph F and its adjacency matrix. In addition, we define and examine their generating matrices with the help of adjacency matrix of F. Also, in this article we define three linear codes that are taken from the graph F and the parameters of codes denotes [N, k, d], where N denotes length, k denotes the dimension which is taken from the number of vertices and d denotes the distance which is taken from the minimum degree. Moreover, we also introduce an encoding and decoding algorithm for the graph using binary bits which is illustrated with a suitable example. Finally, we test the error correction capability of the code by using sphere packing bounds.

Keywords Cartesian Product, Quadratic Residue, Graphs, Regular Graph, Encoding and Decoding

1 Introduction

The origins of coding theory may be traced back to the late 1940s in engineering [5]. It is the branch of communication theory concerned with the mathematical study of codes with the goal of applying them to communication systems, frequently to increase their efficacy and reliability. The focus of error control coding is on methods of conveying information from a source to a destination. The process of translating concepts into language is known as encoding. Decoding is the process of translating verbal communication into cognition. Encoding and decoding are critical in communication. They investigated a few integer properties [1-4]. Graphs and their numerous descendants were investigated in [6-8]. Rezaei [9] constructed networks whose vertex set is a reduced residue system mod n such that two unique vertices, a and b, are adjacent if the squares of vertices a and b under mod n are the same. The author of [10] demonstrated the graphical structures using codes. In this article, we discuss the cartesian product of quadratic residue graphs and present three linear codes produced from the graph. Furthermore, the ability of the codes to repair faults, as well as the encoding and decoding of the graph using binary bits, are both investigated.

2 Preliminaries

According to coding theory, each linear combination of codewords is also a codeword for a linear code, which is an error-correcting code. Linear codes are used in methods for transferring symbols (such as bits) via a communications channel as well as error correction. The vector space

F_{q^n} has a linear subspace C with dimension k that corresponds to a linear code with length n and rank k. One such code is a q-ary code.

A t-error-correcting binary or non-binary linear code of length N containing M codewords must satisfy the sphere packing bound

$$M(1+(q-1)(1^N)+....+(q-1)^t(t^N))\, q^N.$$

In order to derive some linear codes from graphs, we must be aware of some fundamentals of graph theory. A graph with no meaning G = (V, E) is a set of vertices of cardinality n and a collection of edges, each of which is an ordered pair of vertices. If v_i and v_j are adjacent if $\{v_i, v_j\}$ are near together, they

are neighbouring. The degree of a vertex is determined by the number of vertices next to it, v. A graph is said to be a regular of degree d if every vertex in it has the same degree.

If (a,n) = 1 and $x^2 \equiv$ a (mod n), we may say that the integer an is a quadratic residue of n if n is a positive integer. We say that an is a quadratic non-residue of n if there is no solution to the congruence $x^2 \equiv$ a (mod n).

The trivial case q = 0 is generally excluded from lists of quadratic residues. so that the number of quadratic residues (mod m) is taken to be one less than the number of squares (mod n). Assume n$\geq$2 is a fixed positive integer. If two distinct vertices a and b are close together and their vertex sets are reduced residue systems mod n, we call a simple graph G a quadratic residue graph [7] $a^2 \equiv b^2$(mod n). It is symbolised by the symbol G_n.

$V(G_n)=\{a \in Z/(a,n)=1 \text{ and } a<n\}$ and

$E(G_n)=\{ab/a,b \in V(G_n) \text{ and } a^2 \equiv b^2 (\text{mod } n)\}$

Let n=5, $V(G_5)=\{1,2,3,4\}$ and $E(G_5)=\{(1,4)(2,3)\}$.So G_5 is as follows:

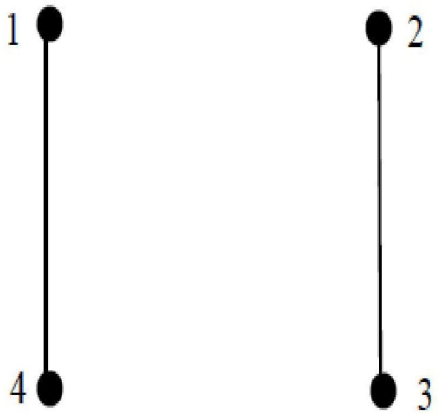

Figure 1. G_5

The adjacency matrix of a simple labeled graph is the matrix A with the element of a_{ij} is a_{ij} either 0 or 1 according to whether the vertex v_i is adjacent to the vertex v_j or not.

2.1 Lemma

(1). Let p be an odd prime, e a positive number, and a a prime number close to p. For the congruence $x^2 \equiv$ a (mod p^e), there are either no solutions or precisely two incongruent solutions.

(ii). The congruence $x^2 \equiv$ a (mod 2^e), where e is an integer, $e \geq 3$. There are either four incongruent responses or no solutions.

3 Cartesian product of Quadratic residue graphs

The Cartesian product of quadratic residue graph F of G_m and H_n and denoted as $F = G_m \circ H_n$, whose vertex set is $V = V(G_m) \circ V(H_n)$. Two vertices (g,h)$\in V(G_m)$ and (g′,h′)$\in V(H_n)$ are adjacent precisely if g=g′ and hh′$\in E(H_n)$ or gg′$\in E(G_m)$ and h=h′. Thus,

$V(G_m \circ H_n)=\{(g,h)/g \in V(G_n)$ and h$\in V(H_n)\}$,

$E(G_m \circ H_n)= \{(g,h)(g'h')/g=g'$ and hh′$\in E(H_n)$ or gg′$\in E(G_m)$,h=h′$\}$. Let, r_1 and r_2 be the numbers of quadratic residues of m and n respectively.

The graphs G_m and H_n are called factors of the product $G_m \circ H_n$. Throughout this paper,we consider F as an undirected graph.

Example 1

Let the quadratic residue graphs G_3 and H_4.

$V(G_3)=\{1,2\}$ and $E(G_3)=\{(1,2)\}$

$V(H_4)=\{1,2,3\}$ and $E(H_4)=\{(1,3)\}$

$G_3 \circ H_4$ is as follows:

$V(G_3 \circ H_4)=\{(1,1)(1,3)(2,1)(2,3)\}$

$E(G_3 \circ H_4)=\{((1,1)(2,1)),\ ((1,1)(1,3)),((1,3)(2,3)),$ $((2,1)(2,3))\}$

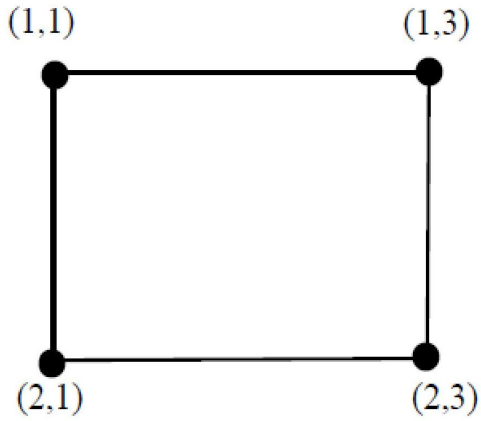

Figure 2. $G_3 \circ H_4$

Theorem 3.1 Let $F = G_{p^{m_1}} \circ H_{q^{n_2}}$ be a cartesian product of two quadratic residue graphs.

If $G_2 \circ H_p$, then F an empty.

If $G_{2^{m_1}} \circ H_{p^{n_2}}$, m_1=2, $n_2 \in \mathbb{N}$ and p is an odd prime, then $F=\frac{\varphi(p^{n_2})}{2} R_2$.

If $G_{2^{m_1}} \circ H_{p^{n_2}}$, $m_1 \geq 3$ and p^{n_2} is powers of an odd prime,$n_2 \mathbb{N}$ then $F=2^{m_1-4}\varphi(p^{n_2})R_4$.

If $G_{2^{n_1}} \circ H_{2^{n_2}}$, where $n_1, n_2 \geq 3$, then $F=2^{m_1+n_2-6} R_6$.

If $G_{p^{m_1}} \circ H_{q^{n_2}}$, p$\neq$q are distinct odd primes, then $F=\frac{\varphi(p^{m_1})\varphi(q^{n_2})}{4} R_2$.

Proof (i)Since G_2 has only one vertex, F=$G_2 \circ H_p$ is empty.

(ii)Let $G_{2^{m_1}} \circ H_{p^{n_2}}$, m_1=2, $n_2 \in$N and p be an odd prime. G_{2^2} has two vertices and one quadratic residue. $H_{p^{n_2}}$ has $p^{n_2-1} \times$(p-1) vertices. By Lemma:2.1, the congruence $x^2 \equiv a \pmod{p^{n_2}}$, has either no solutions or exactly two incongruent solutions modulo p^{n_2}, there are $\varphi(p^{n_2})=p^{n_2-1} \times$ (p-1) squares to be considered in p^{n_2} and there must be $\frac{(p^{n_2-1})(p-1)}{2}$ number of quadratic residues existing for p^{n_2}. Therefore, there exist (1) $\times \frac{(p^{n_2-1})(p-1)}{2}$ numbers of two regular graphs. Hence,$F=\frac{\varphi(p^{n_2})}{2}$ R_2.

(iii) The graph $G_{2^{m_1}}$ has $\varphi(2^{m_1})$)=2^{m_1-1} vertices. By Lemma 2.2, $x^2 \equiv a \pmod{2^{m_1}}$ has either no solutions or exactly 4 incongruent solutions. Therefore, there must be $\frac{(2^{m_1-1})}{4}$ number of quadratic residues. $H_{p^{n_2}}$ has $p^{n_2-1} \times$(p-1) vertices. By Lemma 2.1, the congruence $x^2 \equiv a \pmod{p^{n_e}}$ has either no solutions or exactly 2 incongruent solutions. Then there are $\frac{\varphi(p^{n_2})}{2}$ number of quadratic residues existing for p^{n_2}. Therefore, we get $\frac{(2^{m_1-1})}{4}$ $p^{n_2-1} \times$(p-1) four regular graphs. $F=2^{m_1-4}\varphi(p^{n_2})R_4$.

We can prove the (iv) and (v) in a similar manner.

Theorem 3.2

Let F=$G_{p^{m_1}} \circ H_{q^{n_2}}$, $m_1 \geq 2$ and p^{m_1}, q^{n_2} be powers of an odd prime, $n_2 \in \mathbb{N}$. If F is a group R_i,i=2,4,6 regular graph which has z vertices for all the cases of Theorem 3.1, then the adjacency matrix of every R_i's of F is skew-symmetry matrix and

$$A(R_i\text{'s})= \begin{pmatrix} B_{z/2\times z/2} & M_{z/2\times z/2} \\ M_{z/2\times z/2} & B_{z/2\times z/2} \end{pmatrix}$$

Proof

Let F have v vertices. Every R_i ,i=2,4,6 regular graph of F has z=v/r vertices where r= $r_1 \times r_2$, where r_1 and r_2 are the numbers of quadratic residues of p^{m_1} and q^{m_2} respectively. Since R_i's are regular graphs, every vertex of R_i is adjacent to z vertices. Therefore, we get the adjacency matrix in the form $\begin{pmatrix} B_{z/2\times z/2} & M_{z/2\times z/2} \\ M_{z/2\times z/2} & B_{z/2\times z/2} \end{pmatrix}$ Here, the diagonal entries of the matrix $A(R_i)$ are zero and the order of matrix is z$\times$ z. The proof is trivial.

3.1 Properties of the adjacency matrix of R_i,i=2,4,6 of F

- Diagonal entries of the adjacency matrix all zero.
- There are no self-loops.
- $A(R_i)$ are Skew-symmetric matrix.

Theorem 3.3

Let F = $G_m o H_n$ where m = $p_1^{\alpha_1}.p_2^{\alpha_2}.....p_{m_1}^{\alpha_{m_1}}$, $p_i^{'s}$ are distinct odd primes and n=$q_1^{\beta_1}$. $q_2^{\beta_2}.....q_{m_2}^{\beta_{m_2}}$, $q_i^{'s}$ are distinct odd primes. Then F = $\frac{\varphi(mn)}{2^{m_1+m_2}}$ $R_{2^{m_1+2^{m_2}-2}}$.

Proof

G_m has φ(m) vertices and H_n has φ(n) vertices. By Lemma 2.1,m and n has 2^{m_1} and 2^{m_2} incongruent solutions respectively. Therefore F is a $\frac{\varphi(mn)}{2^{m_1+m_2}}$ number of 2^{m_1}+2^{m_2}-2 regular graphs.

corollary 1

Let F= $G_m o H_n$, where m=2^r. $p_1^{\alpha_1}$. $p_2^{\alpha_2}$....$p_{m_1}^{\alpha_{m_1}}$, n=2^r. $q_1^{\beta_1}$. $q_2^{\beta_2}$...$q_{m_2}^{\beta_{m_2}}$. Then

$$F = \begin{cases} \frac{\varphi(mn)}{2^{m_1+m_2}} R_{2^{m_1}+2^{m_2}-2}, & ifr = 0 or 1 \\ \frac{\varphi(mn)}{2^{m_1+m_2+1}} R_{2^{m_1}+2^{m_2}-1}, & ifr = 2 \\ \frac{\varphi(mn)}{2^{m_1+m_2+2}} R_{2^{m_1}+2^{m_2}}, & ifr \geq 3 \end{cases} \quad (1)$$

4 Codes over F

In this section, we specify the code over F's parameters. A non-empty subset C of F_{q^n} is defined as a q-ary code of length N. One of the components of code C is a codeword. A q-ary linear code with length N, dimension k=number of vertices, and minimum distance d=degmin will be represented by the notation $[N, k, d]_q$. F is linear codes that are used to define all codes. A generator matrix G for a linear code C is an adjacency matrix of F.

Theorem 4.1

Let F = $G_{p^{n_1}} o H_{q^{n_2}}$, p and q be primes, $n_1, n_2 \in \mathbb{N}$.

Then the parameters of the code generated by the adjacency matrix of the graph are,

$[N = c(xy, 2), k = xy, d = degmin]$ where x = number of incongruent solutions of p^{n_1} and y = number of incongruent solutions of q^{n_2}.

Proof

Let F = $G_{p^{n_1}} o H_{q^{n_2}}$. F has $v = \varphi(p^{n_1}) \times \varphi(q^{n_2})$ vertices. By Lemma 2.1, p^{n_1}, q^{n_2} has either no solutions or exactly x and y incongruent solutions respectively. By Theorem 3.1, F is a $\frac{(p^{n_1}-1)(p-1)(q^{n_2}-1)(q-1)}{xy}$ number of R_i,i=2,4,6 regular graphs. Total number of vertices of every R_i graph = $\frac{v}{\frac{v}{xy}} = xy$. Hence, k = xy, N =c(xy,2)=xy(xy-1)/2 and d = deg min of R_i, i=2,4,6.

Example 2

Consider,G_3o H_4.

By Theorem:4.1, x = 2, y = 4,K=xy=8=z. Here, the Cartesian product of quadratic residue graph F is a 2-regular graph which has 4 vertices.

Then the adjacency matrix of every 2-regular graph of F is

$$A = \left(\begin{array}{cc|cc} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array}\right)$$

Eigen-values of this matrix are $\lambda_1 = 2$, $\lambda_2 = 2$, $\lambda_3 = \lambda_4 = 0$.

Therefore, there exists a code C with parameters [N=6, k=4, d=2] for R_2.

Example 3 Consider, G_7o H_2^3.

By Theorem:4.1, x=2, y=4, k=xy=8. Here, the Cartesian product of quadratic residue graph F is a group of 4-regular graph

which has twenty-four vertices.
V($G_7 \circ H_8$)={(1,1)(1,3)(1,5)(1,7)(2,1)(2,3)(2,5)(2,7)(3,1)
(1,3)(3,5)(3,7)(4,1)(4,3)(4,5)(4,7)(5,1)(5,3)(5,5)(5,7)(6,1)(6,3)
(6,5)(6,7)}

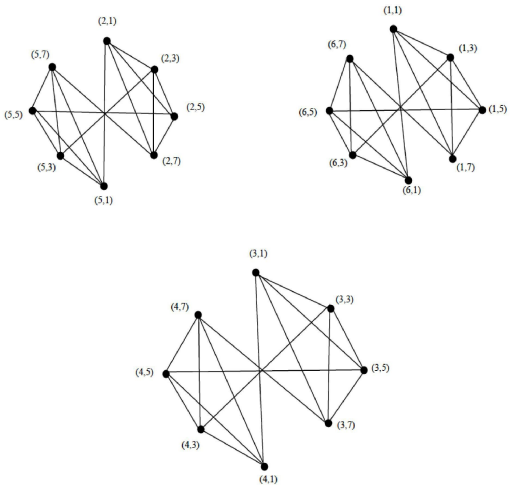

Figure 3. $G_7 \circ H_8$

Then the adjacency matrix of every 4-regular graph of F is

$$\mathbf{A} = \left(\begin{array}{cccc|cccc} 0&1&1&1&1&0&0&0\\ 1&0&1&1&0&1&0&0\\ 1&1&0&1&0&0&1&0\\ 1&1&1&0&0&0&0&1\\ \hline 1&0&0&0&0&1&1&1\\ 0&1&0&0&1&0&1&1\\ 0&0&1&0&1&1&0&1\\ 0&0&0&1&1&1&1&0 \end{array}\right)$$

Therefore, there exists a code C with parameters [N =28,k =8,d=4] for R_4.

5 Encoding and decoding of cartesian product of quadratic residue graphs in binary

Encoding Algorithm:
Step:1

Let N=c(z,2) be a code length, with z=the number of vertices of R_i and i=2,4,6.
Step:2

Write the entries of the adjacency matrix above the diagonal of R_i, i=2,4,6 of F.

Using this algorithm, we can encode the graph R_i, i=2,4,6 in bits 0's and 1's.

Decoding Algorithm:
step:1

The first k-1 bits represent the number of vertices in a graph.
step:2

Form a skew - symmetric matrix using the given code with k-1 rows and k-1 columns and write the received code above the diagonal and also below.
step:3

(i)In the first row, non-zero elements indicate, corresponding vertices adjacent to the vertex z_1.

(ii) In the second row, non-zero elements indicate, corresponding entries adjacent to the vertex z_2.
etc.,
(iii) Non-zero elements in the k-th row indicate corresponding vertices adjacent to the vertex z_k.
step:4
There should be,deg(z_1)= deg(z_2) =...=deg(z_k)=d.
step:5

If deg(z_i)=d, i=1,2,..,k and every vertex has a symmetric adjacency, then there is no error in the graph's received code. Otherwise, go to step 6.
step:6

If deg(z_i)=d-1 or d+1, then the received code has one error.
step:7

Choose the two vertices. Have a degree that equals d-1.Replace a '0' bit with a '1' bit where the adjacency symmetric is missing. Then go to step 5. Otherwise, go to the next step.
step:8

If any two vertices have a degree equal to d+1, then replace '1' with '0', where the adjacency symmetric is missing. Go to step 5. Otherwise, go to step 7.
step:9

If any two vertices have a degree that is equal to neither d-1 nor d+1, then declare the received code of the graph has more than one error.
step:10

End.

5.1 Codes over F_1=$G_{2^{m_1}}$ o $H_{p^{n_2}}$,$m_1 \geq$3,p be an odd prime

By theorem 3.1, (iii) result,$G_{2^{m_1}}$ o $H_{p^{n_2}}$ is a group of four regular graphs. The parameters of a code generated by the adjacency matrix of every four regular graphs are [N=28, K=8, d=6].

x=4, y=2, k=xy=8. $F_1=2^{3-1}\varphi(3)$ R_4=8R_4.

Then the adjacency matrix of one R_4 graph is

$$\mathbf{A} = \left(\begin{array}{cccc|cccc} 0&1&1&0&1&0&1&0\\ 1&0&0&1&0&1&0&1\\ 1&0&0&1&1&0&1&0\\ 0&1&1&0&0&1&0&1\\ \hline 1&0&1&0&0&1&1&0\\ 0&1&0&1&1&0&0&1\\ 1&0&1&0&1&0&0&1\\ 0&1&0&1&0&1&1&0 \end{array}\right)$$

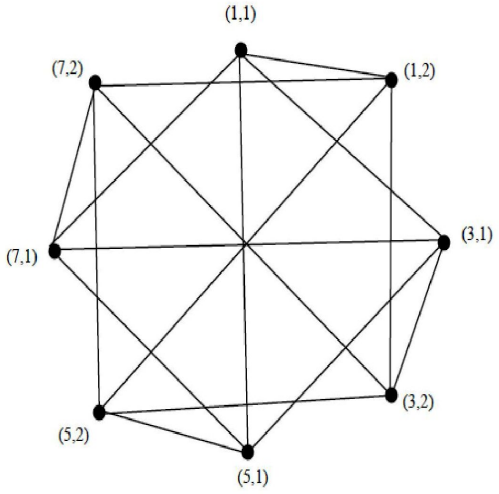

Figure 4. $G_2 \circ H_3$.

ρ[A(R_4)]=5.

Eigen values are λ_1 = 4, λ_2 = -2, λ_3 = -2, λ_4 = -2, λ_5 = -2, $\lambda_6 = \lambda_7 = \lambda_8 = 0$.

Here, d = 4. E($G_{2^{m_1}}$ o $H_{p^{n_2}}$) = 12.

Therefore, there exists, [N=28, k=8, d=4] linear code for the graph G_2^3 o H_3. We can detect and correct one error.

5.2 Codes over F_2=$G_{2^{n_1}} o H_{2^{n_2}}$, n_1,$n_2 \geq 3$

Let F_2= $G_{2^{n_1}} o G_{2^{n_2}}$, x = 4, y = 4. code length N= c(xy,2)=120. dimension K=xy=16=z. By Theorem 3.1, F_2 contains $2^{n_1+n_2-6}$ number of 6-regular graphs. The parameters of code generated by the adjacency matrix A(R_6) are [N=120, 16, 6]. This code can correct $\frac{d-2}{2}$ = 2 errors.

Example 4

Let, F_2=G_{2^3} o H_{2^3}. By Theorem 3.1,F_2 =2^{3+3-6}=(1) R_6. there exists,[N=c(16,2)=120, k=8, d=6] linear code for the graph F_2. This code detects 2 errors and corrects one error.

Then the adjacency matrix of every R_6 of F_2 is,

A =

$$\left(\begin{array}{cccccccc|cccccccc}
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
\hline
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0
\end{array}\right)$$

ρ[A(R_6)]=8.

Eigen values are λ_1 = 6, $\lambda_2 = -2$, $\lambda_3 = -2$, $\lambda_4 = \lambda_5 = \lambda_6 = \lambda_7 = \lambda_8 = \lambda_9 = \lambda_{10} = \lambda_{11} = \lambda_{12} = \lambda_{13} = \lambda_{14} = \lambda_{15} = \lambda_{16} = 0$.

E(G_{2^3} o H_{2^3})=10.

5.3 Codes over F_3=$G_{3^{n_1}} o H_{3^{n_2}}$, n_1, $n_2 \in$ N

By Lemma 2.1, 3^{n_1} and 3^{n_2} have either no solution or exactly two incongruent solutions, $x = 2$, $y = 2$. Therefore, code length= c(4,2)=6, message length k=z=4, by the (v) th statement of theorem 3.1, d=2. Therefore, the parameters of the code generated by the adjacency matrix of the graph F= $G_{3^{n_1}} o H_{3^{n_2}}$ is [N=6, k=4,2].

Example 5

Consider, G_{3^2}o H_{3^2}.

since 3^2 has either no solutions or exactly two incongruent solutions, $x = 2$, $y = 2$. Therefore, code length= c(4,2)=6, message length k = 4. By Theorem 3.1, the Cartesian product of quadratic residue graph F is the nine 2-regular graphs which have 36 vertices and d=2.

$$\text{A}(R_2)= \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

Since d= 2, we can detect and correct only one error. Here, F_3 is a group of two regular graphs; we just encode and decode R_2 only.

Using encoding algorithm of a R_2 of F is C(R_2) =110011. Let the received graph be r(R_2)=010011.

The decoding algorithm states that the first k bits denote the number of vertices the i-regular graph. By using the encoding method frame, a matrix,

i.e.,

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

This matrix shows that

(i)vertex z_1 of R_2 is adjacent to z_3.

(ii)z_2 is adjacent to z_1, z_4.
(iii)z_3 is adjacent to z_1, z_4.
(iv)z_4 is adjacent to z_2, z_3.
i.e.,$z_2 \sim z_4$, $z_1 \sim z_3$, $z_3 \sim z_4$, $z_1 \nsim z_2$.
Here, degree of z_1 is not equal to d=2. If we replace a_{14} with '1', it increases the degree of z_4.
If we return a_{11} by '1', it gives self loops. Therefore the error is in a_{12}. By putting the adjacency between the vertices 1 to 2 we can correct the error of graph.

5.4 Sphere-packing bound of codes over F

We know that, the sphere packing bound for binary code is

$$M(1+\binom{N}{1}+.....+\binom{N}{t}) \leq 2^N.$$

$$2^{16}\,(1+\binom{16}{1}+.....+\binom{16}{2}) \leq 2^{120}.$$

Therefore, code [N=120, k=16, d=6] is a linear code.
Similarly,

The code [28,8,4] satisfies the sphere - packing bound; it is also a linear code . Hence, these two codes are linear and one error correction code.

6 Conclusions

In this article, the authors introduce an encoding and decoding algorithm for detecting and correcting one error for the cartesian product of quadratic residue graphs. Further, the authors will be interested in extending their work from more than one error in the specified graph.

REFERENCES

[1] Frei G. The Reciprocity Law from Euler to Eisenstein, The Intersection of History and Mathematics, vol.15, pp.67-90, 1994.

[2] Hardy G H., Wright E.M. Congruences and Residues, An Introduction to the Theory of Numbers, fifth ed, Oxford University Press, pp.48-91, 1980.

[3] Ireland., Kenneth., Rosen and Michael. Congruence, A Classical Introduction to Modern Number Theory, second ed, New York: Springer, pp.29-73, 1990.

[4] Kenneth H., Rosen. Primes and Greatest Common Divisors, Elementary Number Theory and its Application, Addison-Wesley Publishing company, pp.86-99, 1984.

[5] Macwilliams F.J., Sloane N.J.A.Linear Codes, The Theory of Error correcting codes, 1 st ed, North-Holland, Amsterdam, pp.01-37, 1983.

[6] Nouri M., Talatahari S., Salimi Shamloo A. Graph Products and Its Applications in Mathematical Formulation of Structures, Journal of Applied Mathematics, vol.2012, Article ID 510180, 16 pages, 2012.

[7] Ravi.J et. al., A robust measure of pair wise distance estimation approach: RD-RANSAC, International Journal of Statistics and Applied Mathematics, vol.2, pp.31-34, 2017.

[8] Ravi.J et. al., An Optimal Solution for Transportation problem-DFSD, Journal of Computational Mathematica, vol.3, pp.43-51, 2019.

[9] Rezaei., Mehdi., Rehman., Shafiq., Khan., Zia., Baig A., Farahani., Mohammad. Quadratic Residues Graphs, International Journal of Pure and Applied Mathematics, vol.113, no.3, pp.465-470, 2017.

[10] Rouayheb S.E., Georghiades C.N. Graph Theoretic Methods in Coding Theory, Classical, Semi-classical and Quantum Noise, pp.53-62, 2012.