Science and Technology Indonesia
e-ISSN:2580-4391 *p*-ISSN:2580-4405
Vol. 11, No. 3, July 2026

Research Paper

Construction of Binary Linear Codes from Zero Divisor Graphs

Vira Hari Krisnawati[1], Ardi Nur Hidayat[1], Muhammad Husnul Khuluq[2*]

[1]*Department of Mathematics, Faculty of Mathematics and Natural Sciences, Brawijaya University, Malang, East Java, 65145, Indonesia*
[2]*Department of Mathematics, Faculty of Mathematics and Natural Sciences, State University of Surabaya, Surabaya, East Java, 60231, Indonesia*
***Corresponding author**: muhammadkhuluq@unesa.ac.id*

Abstract
Binary linear codes play an essential role in communication systems by ensuring reliable data transmission. One approach to constructing binary linear codes is through graph theory. In this paper, we study the construction of binary linear codes derived from the incidence matrices of zero divisor graphs of the rings $Z_{(p^\alpha)}$ and $Z_{(p^\alpha q^\beta)}$, where p, q are prime numbers and α, $\beta \geq 1$ are integers. We analyze the parameters of the resulting binary linear codes, such as their length, dimension, and minimum distance. Furthermore, we investigate some examples of the constructed codes. To justify their theoretical and practical relevance, we perform an optimality analysis comparing the constructed codes with classical bounds. All evaluated codes strictly satisfy the Hamming sphere-packing bound. This work offers a new contribution to the study of linear codes by combining ideas from algebra, graph theory, and coding theory.

Keywords
Incidence Matrix, Hamming Bound, Linear Codes, Zero Divisor Graphs

Received: 18 January 2026, Accepted: 26 March 2026
https://doi.org/10.26554/sti.2026.11.3.784-794

1. INTRODUCTION

Graph-theoretic methods have become an effective approach for studying algebraic structures. Among various constructions, the zero divisor graph offer a natural representation of the multiplicative relationships among zero divisors in a ring through a graphical structure. This representation allows algebraic properties of rings to be explored using graph invariants such as chromatic number, connectivity, diameter, and others. A nonzero element x of a commutative ring R is said to be a zero divisor if there exists a nonzero element $y \in R$ such that $y \cdot x = 0_R$. The set $Z^*(R)$ denotes the set of all nonzero zero divisors of R (Herstein, 1995). A zero divisor graph of R is a simple graph with vertex set $Z^*(R)$ and the edges xy satisfying $x \cdot y = 0_R$, and it is denoted by $\Gamma(R)$. This concept was introduced by Beck (1988); Anderson and Livingston (1999). This graph is connected with diameter at most 3. For the ring Z_n, the structure of $\Gamma(Z_n)$ depends strongly on the prime factorization of n. For every positive integer n, the order of $\Gamma(Z_n)$ is $n - \varphi(n) - 1$, where φ is Euler's totient function. In particular, the size of $\Gamma(Z_n)$ was given by Mukhtar et al. (2020). Further results on zero divisor graphs can be found in Singh and Bhat (2020).

Meanwhile, coding theory plays an important role in information transmission and storage systems, with the main purpose of identifying and correcting errors that occur in the course of data communication. Among various classes of codes, linear codes form one of the most fundamental and widely studied families due to their rich algebraic structure and efficient encoding and decoding procedures. In particular, a linear code can be characterized as a subspace of a finite-dimensional vector space over a finite field, which makes it amenable to analysis using techniques from linear algebra and finite field theory. Several researchers have attempted to construct linear codes from the adjacency matrix of connected graphs (Saranya and Durairajan, 2021, 2022). Although this approach offers a direct representation of vertex connectivity, it has limited capability in systematically representing edge–vertex relationships and in deriving meaningful algebraic properties for code construction. However, the construction of linear codes using the incidence matrix of a graph has been explored more extensively and shown to be more effective. This approach has been widely studied in coding theory because incidence matrices offer a clearer algebraic framework and support the systematic determination of code parameters, as illustrated in Key and Seneviratne (2008); Fish et al. (2010). Dankelmann et al. (2011) further provided code parameters for linear codes constructed from connected graphs. These studies highlight the advantage of incidence-matrix-based constructions in producing well-structured linear codes with desirable parameters. The strong interest in these constructions is driven by

the crucial role of linear codes in improving the security of communication systems, particularly in improving resistance to hardware Trojans, side-channel attacks, and data tampering. Moreover, the inherent properties of linear codes support the design of secure and fault-tolerant circuits, as discussed by Ngo et al. (2015); Nachmani et al. (2018).

Recent studies on graph-based linear code constructions over rings have considered several types of graphs associated with the ring Z_n. Several works have extensively investigated linear codes derived from unit graphs for many cases of Z_n, such as in articles Annamalai and Durairajan (2021); Jain et al. (2023); Shaikh et al. (2024). They provided a relatively broad development of code constructions from unit graphs. In contrast to the relatively extensive development based on unit graphs, research on linear code constructions derived from zero divisor graphs remains very limited. In particular, Annamalai and Durairajan (2022) constructed linear codes from the graph $\Gamma(Z_n)$ for $n = p_1p_2, \ldots, p_k$, showing that zero divisor graphs can also serve as a systematic structure to generate codes with well-defined parameters. However, this construction is restricted to specific forms of integers, and a more general framework for constructing linear codes from zero divisor graphs has not yet been fully developed.

Motivated by these limitations, in this research, we study the construction of binary linear codes from the graph $\Gamma(Z_n)$ for broader classes of integers, namely $n = p^\alpha$ and $n = p^\alpha q^\beta$, where p and q are primes and $\alpha, \beta \geq 1$ are integers. The motivation of this work is to extend existing results to wider ring families and to provide a simple and systematic way to obtain binary linear codes from zero divisor graphs. We also determine the parameters of the resulting linear codes and their corresponding dual codes and give concrete examples to illustrate construction. Moreover, we perform an optimality analysis by comparing the constructed codes with the classical bound. Finally, we conclude the paper and present some open problems for future research.

2. EXPERIMENTAL SECTION

In this section, we restate the main definitions and preliminary results related to the zero divisor graph of Z_n and linear codes are restated. We begin with the basic notions of graph theory and then proceed to the definition of the zero divisor graph together with several fundamental properties needed in the subsequent discussion.

Let $G = (V(G), E(G))$ be a simple graph. The order and size of G are denoted by $|V(G)|$ and $|E(G)|$, respectively. The incidence matrix of G, denoted by $M(G)$, is the $|V(G)|\times|E(G)|$ matrix $M(G) = [m_{ij}]$, where $m_{ij} = 1$ whenever the vertex v_i is incident with the edge e_j, and $m_{ij} = 0$ otherwise. The diameter of G, denoted by $\text{diam}(G)$, is the maximum distance between any two vertices of G. If G is connected, then an edge-cut of G is a set $S \subseteq E(G)$ for which $G - S = (V(G), E(G) - S)$ is disconnected. The minimum cardinality of an edge-cut is called the edge-connectivity of G, denoted by $\lambda(G)$. In addition, the girth of G, denoted by $g_r(G)$, is the length of a shortest cycle in G. Further notation and terminology may be found in Diestel (2024); Chartrand et al. (2024).

Definition 2.1. (Anderson and Livingston, 1999)
The zero divisor graph of a commutative ring R, denoted by $\Gamma(R)$, is a simple graph with $V(\Gamma(R)) = Z^*(R) = Z(R) \setminus \{0_R\}$, the set of all nonzero zero divisors of R, and two distinct vertices $x, y \in Z^*(R)$ are adjacent if and only if $x \cdot y = 0_R$.

Theorem 2.2. (Anderson and Livingston, 1999)
For any commutative ring R, the graph $\Gamma(R)$ is connected with $\text{diam}(\Gamma(R)) \leq 3$. Moreover, if $\Gamma(R)$ contains a cycle, then $g_r(\Gamma(R)) \leq 7$.

Throughout this paper, we consider the ring Z_n and its associated zero divisor graph. The order and size of $\Gamma(Z_n)$ are given in the following theorem.

Theorem 2.3. (Phillips et al., 2004)
For any integer $n \geq 1$, the graph $\Gamma(Z_n)$ has order

$$|V(\Gamma(Z_n))| = n - \varphi(n) - 1,$$

where $\varphi(n)$ is Euler's totient function.

Theorem 2.4. (Mukhtar et al., 2020)
For any integer $n \geq 1$, the graph $\Gamma(Z_n)$ has size

$$|E(\Gamma(Z_n))| = \frac{1}{2}\left(\left(\sum_{m|n} m\,\varphi\left(\frac{n}{m}\right)\right) - \omega_n - 2n + 2\right),$$

where ω_n denotes the number of elements $x \in Z_n$ such that $x^2 = 0$.

The following theorem states the edge-connectivity of $\Gamma(Z_n)$.

Theorem 2.5. (Reddy et al., 2020)
For every positive integer $n = p_1^{n_1}p_2^{n_2}\cdots p_m^{n_m}$, the graph $\Gamma(Z_n)$ has edge-connectivity

$$\lambda(\Gamma(Z_n)) = \min\{p_i - 1 \mid i = 1, 2, \ldots, m\},$$

and for $n = p^2$, the edge-connectivity of $\Gamma(Z_{p^2})$ is $\lambda = p-2$.

The girth plays an important role in determining the minimum distance of the corresponding dual codes. The following theorem characterizes the girth of $\Gamma(Z_n)$.

Theorem 2.6. (Pi et al., 2019)

The girth of $\Gamma(Z_n)$ is given as follows:

- $g_r(\Gamma(Z_n)) = 0$ iff $n = 4, 8, 9$ or $n = 2q$ for some prime $q \geq 3$.
- $g_r(\Gamma(Z_n)) = 4$ iff $n = pq$ or $n = 4q$ for some distinct primes $p, q \geq 3$.
- $g_r(\Gamma(Z_n)) = 3$ in all other cases.

Meanwhile, the following theorem establishes the girth for the specific class of the graph $\Gamma(Z_{p^\alpha})$. For more properties of the zero divisor graph, we refer the reader to the survey (Singh and Bhat, 2020).

Corollary 2.7. (Magi et al., 2020)
Let p be an odd prime and $\alpha \geq 3$ be an integer. Then, the girth of the graph $\Gamma(Z_{p^\alpha})$ is given by

$$g_r(\Gamma(Z_{p^\alpha})) = 3.$$

We next review the concept of linear codes, along with the basic definitions and properties needed in this paper. Let $\mathbb{F}_q$ denote the finite field of order q. A linear code C_q of length n over $\mathbb{F}_q$ (q-ary linear code) is a subspace of $\mathbb{F}_q^n$, and each element of C_q is called the codeword. The dimension of C_q, denoted by $\dim(C_q)$, is the dimension of C_q as a vector space over $\mathbb{F}_q$. The dual code of C_q, denoted by $C_q^\perp$, is defined as the orthogonal complement of the subspace C_q in $\mathbb{F}_q^n$ (Ling and Xing, 2004).

Theorem 2.8. (Vanstone and Van Oorschot, 2013)
For any linear code C_q of length n, the dual code $C_q^\perp$ is also a linear code of length n, and its dimension satisfies:

$$\dim(C_q^\perp) = n - \dim(C_q).$$

Let $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ be elements of $\mathbb{F}_q^n$. The Hamming distance between x and y, denoted by $d(x, y)$, is the number of coordinates at which they differ. The Hamming weight of x is defined by $\mathrm{wt}(x) = d(x, 0)$. For a linear code C_q, let

$$\mathrm{wt}(C_q) = \min\{\mathrm{wt}(x) \mid x \in C_q, x \neq 0\}$$
$$d(C_q) = \min\{d(x, y) \mid x, y \in C_q, x \neq y\}$$

Clearly, $d(C_q) = \mathrm{wt}(C_q) = d$. A linear code C_q with length n, dimension k, and minimum distance d is called an $[n, k, d]_q$ code. Therefore, the dual code $C_q^\perp$ is an

$$[n, n-k, d^\perp]_q \quad \text{code},$$

where $d^\perp$ denotes the minimum distance of $C_q^\perp$. A generator of $C_q = [n, k, d]_q$ is a $k \times n$ matrix G of rank k in which every codeword x can be represented as

$$x = yG,$$

where $y \in \mathbb{F}_q^k$ (Roth, 2006).

The fundamental purpose of algebraic coding theory is to facilitate reliable data transmission over noisy channels. The error-detecting and correcting capabilities of a q-ary linear code C_q with parameters $[n, k, d]_q$ depend strictly on its minimum distance d. The code C_q can detect up to s errors if $s \leq d - 1$, and correct up to t errors if $t = \lfloor (d-1)/2 \rfloor$. The efficiency of C_q is evaluated using fundamental theoretical bounds. The Singleton bound states that the parameters of C_q must satisfy the inequality $d \leq n - k + 1$. If C_q achieves equality ($d = n - k + 1$), it is called a Maximum Distance Separable (MDS) code. Additionally, the Hamming bound (or sphere-packing bound) restricts the size of the code. A t-error-correcting code C_q must satisfy

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq q^{n-k}.$$

For a binary code C_2, this simplifies to

$$\sum_{i=0}^{t} \binom{n}{i} \leq 2^{n-k}.$$

If a code achieves strict equality in this bound, it is classified as a perfect code (Vanstone and Van Oorschot, 2013).

Furthermore, the incidence matrix of a graph can be employed to construct a linear code, where several code properties are related to the structural characteristics of the graph. The following theorems explain this construction.

Theorem 2.9. (Dankelmann et al., 2011)
For any simple connected graph $G = (V(G), E(G))$, the binary linear code generated by $M(G)$ is

$$C_2 = [\, |E(G)|,\ |V(G)| - 1,\ \lambda(G)\,]_2.$$

Theorem 2.10. (Dankelmann et al., 2011)
For any simple connected graph G with girth $g_r(G)$, if C_2 is a binary linear code generated by $M(G)$, then

$$C_2^\perp = [\, |E(G)|,\ |E(G)| - |V(G)| + 1,\ g_r(G)\,]_2.$$

3. RESULTS AND DISCUSSION

3.1 Binary Linear Codes from Incidence Matrices of $\Gamma(Z_{p^\alpha})$

In this subsection, we give the parameters of the binary linear code constructed from the incidence matrix of the graph $\Gamma(Z_{p^\alpha})$. This construction starts from a simple case to the general case.

Lemma 3.1. For every prime $p > 2$, the binary linear code generated by $M(\Gamma(Z_{p^2}))$ is

$$C_2 = \left[\frac{(p-1)(p-2)}{2},\ p-2,\ p-2\right]_2.$$

Proof. Consider $Z^*(\Gamma(Z_{p^2})) = \{p, 2p, \ldots, (p-1)p\}$. Observe that for every $ap, bp \in Z^*(\Gamma(Z_{p^2}))$ holds $ap \cdot bp = 0$, thus all distinct elements in $Z^*(\Gamma(Z_{p^2}))$ are adjacent. We obtain $\Gamma(Z_{p^2}) \cong K_{p-1}$ and it has order $p-1$ and size $\frac{(p-1)(p-2)}{2}$. Thus, by **Theorem 2.5**, we have $\lambda(\Gamma(Z_{p^2})) = p-2$. Therefore, according to **Theorem 2.9**, the binary linear code generated by $M(\Gamma(Z_{p^2}))$ is

$$C_2 = \left[\frac{(p-1)(p-2)}{2},\ p-2,\ p-2\right]_2.$$

Lemma 3.2. For every prime p, the binary linear code generated by $M(\Gamma(Z_{p^3}))$ is

$$C_2 = \left[p^3 - \frac{3p^2}{2} - \frac{p}{2} + 1,\ p^2 - 2,\ p-1\right]_2.$$

Proof. All nonzero zero divisors of Z_{p^3} are $A_1 = \{p^2, 2p^2, \ldots, (p-1)p^2\}$ and $A_2 = \{p, 2p, \ldots, (p^2-1)p\} \setminus A_1$, such that $V(\Gamma(Z_{p^3})) = A_1 \cup A_2$. Observe that every two distinct elements in A_1 are adjacent and every pair of elements from A_1 and A_2 is adjacent. Thus, the size of $\Gamma(Z_{p^3})$ is $\frac{(p-1)(p-2)}{2} + (p-1)(p^2-p) = p^3 - \frac{3p^2}{2} - \frac{p}{2} + 1$.

By **Theorem 2.5**, we have $\lambda(\Gamma(Z_{p^3})) = p-1$. Therefore, according to **Theorem 2.9**, the binary linear code generated by $M(\Gamma(Z_{p^3}))$ is

$$C_2 = \left[p^3 - \frac{3p^2}{2} - \frac{p}{2} + 1,\ p^2 - 2,\ p-1\right]_2.$$

Lemma 3.3. For every prime p, the binary linear code generated by $M(\Gamma(Z_{p^4}))$ is

$$C_2 = \left[\frac{3p^4}{2} - 2p^3 - \frac{p^2}{2} + 1,\ p^3 - 2,\ p-1\right]_2.$$

Proof. Let A_1, A_2, A_3 be all nonzero zero divisors of Z_{p^4} such that $V(\Gamma(Z_{p^4})) = A_1 \cup A_2 \cup A_3$, where

$$A_1 = \{p^3, 2p^3, \ldots, (p-1)p^3\}, \quad |A_1| = p-1,$$

$$A_2 = \{p^2, 2p^2, \ldots, (p^2-1)p^2\} \setminus A_1, \quad |A_2| = p^2 - p,$$

$$A_3 = \{p, 2p, \ldots, (p^3-1)p\} \setminus (A_1 \cup A_2), \quad |A_3| = p^3 - p^2.$$

Observe that every two distinct elements in A_1 are adjacent, as well as in A_2. Also, every pair of elements in A_1 and A_2 is adjacent, as well as every pair of elements in A_1 and A_3. Thus, the size of $\Gamma(Z_{p^4})$ is

$$\frac{(p-1)(p-2)}{2} + \frac{(p^2-p)(p^2-p-1)}{2} + (p-1)(p^3-p) = \frac{3p^4}{2} - 2p^3 - \frac{p^2}{2} + 1.$$

By **Theorem 2.5**, we have $\lambda(\Gamma(Z_{p^4})) = p-1$. Therefore, according to **Theorem 2.9**, the binary linear code generated by $M(\Gamma(Z_{p^4}))$ is

$$C_2 = \left[\frac{3p^4}{2} - 2p^3 - \frac{p^2}{2} + 1,\ p^3 - 2,\ p-1\right]_2.$$

Then, by **Theorem 2.5**, we have $\lambda(\Gamma(Z_{p^4})) = p-1$. Therefore, according to **Theorem 2.9**, the binary linear code generated by $M(\Gamma(Z_{p^4}))$ is $C_2 = \left[\frac{3p^4}{2} - 2p^3 - \frac{p^2}{2} + 1,\ p^3 - 2,\ p-1\right]_2$.

Lemma 3.4. For every prime p, the binary linear code generated by $M(\Gamma(Z_{p^5}))$ is

$$C_2 = \left[2p^5 - \frac{5p^4}{2} - \frac{p^2}{2} + 1,\ p^4 - 2,\ p-1\right]_2.$$

Proof. Let A_1, A_2, A_3, and A_4 be all nonzero zero divisors of Z_{p^5} such that $V(\Gamma(Z_{p^5})) = A_1 \cup A_2 \cup A_3 \cup A_4$, where

$$\begin{aligned}
A_1 &= \{p^4, 2p^4, \ldots, (p-1)p^4\}, && |A_1| = p-1,\\
A_2 &= \{p^3, 2p^3, \ldots, (p^2-1)p^3\} \setminus A_1, && |A_2| = p^2 - p,\\
A_3 &= \{p^2, 2p^2, \ldots, (p^3-1)p^2\} \setminus (A_1 \cup A_2), && |A_3| = p^3 - p^2,\\
A_4 &= \{p, 2p, \ldots, (p^4-1)p\} \setminus (A_1 \cup A_2 \cup A_3), && |A_4| = p^4 - p^3.
\end{aligned}$$

The connectivity between each pair of vertices is given as follows:

1. Every two distinct elements in A_1 are adjacent, as well as in A_2.
2. Every pair of elements in A_1 and A_2 is adjacent, as well as every pair of elements in A_1 and A_3, and A_1 and A_4.
3. Every pair of elements in A_2 and A_3 is adjacent.

Thus, the size of $\Gamma(Z_{p^5})$ is

$$\frac{(p-1)(p-2)}{2} + \frac{(p^2-p)(p^2-p-1)}{2} + (p-1)(p^4-p) + (p^2-p)(p^3-p^2)$$
$$= 2p^5 - \frac{5p^4}{2} - \frac{p^2}{2} + 1$$

Then, by Theorem 3.5, we have $\lambda(\Gamma(Z_{p^5})) = p-1$. Therefore, according to **Theorem 2.9**, the binary linear code generated by $M(\Gamma(Z_{p^5}))$ is

$$C_2 = \left[2p^5 - \frac{5p^4}{2} - \frac{p^2}{2} + 1,\ p^4 - 2,\ p-1\right]_2.$$

To further clarify the construction, we present a simple illustrative example as a representative case of the result stated in **Lemma 3.2.**

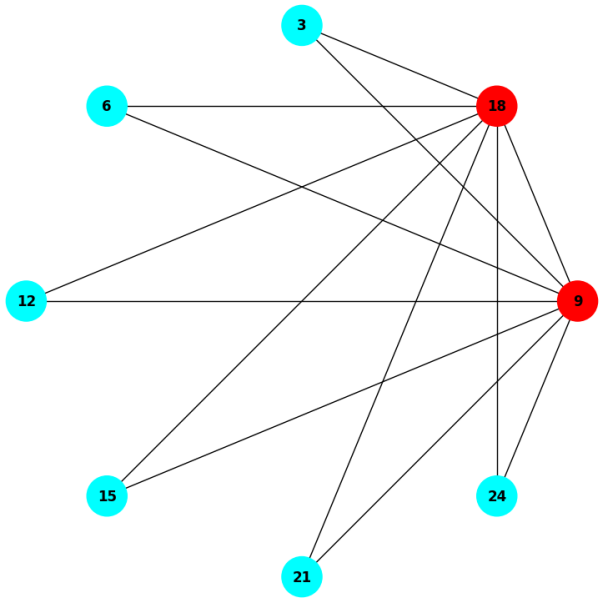

Figure 1. The Graph $\Gamma(Z_{27})$

Example 3.5. Consider the graph $\Gamma(Z_{27})$.

The incidence matrix of $\Gamma(Z_{27})$ is

$$M = \begin{bmatrix} 0&1&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&1&0&0&0&0 \\ 1&1&1&1&1&1&1&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0&1&0&0 \\ 1&0&0&0&0&0&1&1&1&1&1&1&1 \\ 0&0&0&0&0&1&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&1 \end{bmatrix}.$$

Since there are 7 linearly independent rows in the matrix M, the rank of M is 7. Then, the linear code over $\mathbb{F}_2$ generated by M is $C_2 = [13, 7, 2]_2$.

Based on **Lemma 3.2-3.4**, linear codes can be constructed from the incidence matrices of $\Gamma(Z_{p^\alpha})$. In general, the parameters of these codes are given as follows.

Theorem 4.6. For every prime p and integer $\alpha > 2$, the binary linear code generated by $M(\Gamma(Z_{p^\alpha}))$ is

$$C_2 = \begin{cases} \left[\frac{1}{2}\left(\Delta - p^{(\alpha-1)/2}\right),\ p^{\alpha-1} - 2,\ p-1\right]_2 & \text{if } \alpha \text{ is odd}, \\ \left[\frac{1}{2}\left(\Delta - p^{\alpha/2}\right),\ p^{\alpha-1} - 2,\ p-1\right]_2 & \text{if } \alpha \text{ is even}. \end{cases}$$

where $\Delta = (\alpha-1)p^\alpha - \alpha p^{\alpha-1} + 2$.

Proof. By **Theorem 2.9**, the binary linear code C_2 generated by $M(\Gamma(Z_{p^\alpha}))$ has parameters

$$[\,|E(\Gamma(Z_{p^\alpha}))|,\ |V(\Gamma(Z_{p^\alpha}))| - 1,\ \lambda(\Gamma(Z_{p^\alpha}))\,]_2.$$

Hence, determining the parameters of C_2 reduces to evaluating the order, the size, and the edge-connectivity of $\Gamma(Z_{p^\alpha})$. Using the standard property of Euler's totient function, we obtain

$$|V(\Gamma(Z_{p^\alpha}))| = p^\alpha - \varphi(p^\alpha) - 1 = p^\alpha - (p^\alpha - p^{\alpha-1}) - 1 = p^{\alpha-1} - 1.$$

By **Theorem 2.4**,

$$|E(\Gamma(Z_{p^\alpha}))| = \frac{1}{2}\left(\sum_{m|p^\alpha} m\varphi\left(\frac{p^\alpha}{m}\right) - \omega_{p^\alpha} - 2p^\alpha + 2\right).$$

Since the positive divisors of p^α are $1, p, p^2, \ldots, p^\alpha$, we obtain

$$\sum_{m|p^\alpha} m\varphi\left(\frac{p^\alpha}{m}\right) = \sum_{i=0}^{\alpha} p^i \varphi(p^{\alpha-i}) = \sum_{i=0}^{\alpha-1} p^i \left(p^{\alpha-i} - p^{\alpha-i-1}\right) + p^\alpha \varphi(1).$$

$$= \sum_{i=0}^{\alpha-1} (p^\alpha - p^{\alpha-1}) + p^\alpha = \alpha(p^\alpha - p^{\alpha-1}) + p^\alpha = (\alpha+1)p^\alpha - \alpha p^{\alpha-1}.$$

Now, $x^2 = 0$ in Z_{p^α} if and only if $p^\alpha \mid x^2$. Indeed, if $x = p^k u$, where u is not divisible by p, then $x^2 = p^{2k}u^2$, so $p^\alpha \mid x^2$ holds if and only if $2k \geq \alpha$, that is, $k \geq \lceil \alpha/2 \rceil$. Therefore,

$$\omega_{p^\alpha} = p^{\alpha - \lceil \alpha/2 \rceil} = p^{\lfloor \alpha/2 \rfloor} = \begin{cases} p^{(\alpha-1)/2}, & \text{if } \alpha \text{ is odd}, \\ p^{\alpha/2}, & \text{if } \alpha \text{ is even}. \end{cases}$$

Substituting these into the formula for $|E(\Gamma(Z_{p^\alpha}))|$, we get

$$|E(\Gamma(Z_{p^\alpha}))| = \frac{1}{2}\left((\alpha+1)p^\alpha - \alpha p^{\alpha-1} - \omega_{p^\alpha} - 2p^\alpha + 2\right),$$

that is,

$$|E(\Gamma(Z_{p^\alpha}))| = \frac{1}{2}\left((\alpha-1)p^\alpha - \alpha p^{\alpha-1} + 2 - \omega_{p^\alpha}\right).$$

If we write

$$\Delta = (\alpha-1)p^\alpha - \alpha p^{\alpha-1} + 2,$$

then

$$|E(\Gamma(Z_{p^\alpha}))| = \begin{cases} \frac{1}{2}\left(\Delta - p^{(\alpha-1)/2}\right), & \text{if } \alpha \text{ is odd}, \\ \frac{1}{2}\left(\Delta - p^{\alpha/2}\right), & \text{if } \alpha \text{ is even}. \end{cases}$$

Finally, by Theorem 3.5, we obtain

$$\lambda(\Gamma(Z_{p^\alpha})) = p - 1.$$

Combining the obtained values of $|E(\Gamma(Z_{p^\alpha}))|$, $|V(\Gamma(Z_{p^\alpha}))|$ and $\lambda(\Gamma(Z_{p^\alpha}))$, we obtain the parameters of C_2 as

$$C_2 = \begin{cases} \left[\frac{1}{2}\left(\Delta - p^{(\alpha-1)/2}\right),\ p^{\alpha-1} - 2,\ p - 1\right]_2, & \text{if } \alpha \text{ is odd,} \\ \left[\frac{1}{2}\left(\Delta - p^{\alpha/2}\right),\ p^{\alpha-1} - 2,\ p - 1\right]_2, & \text{if } \alpha \text{ is even.} \end{cases}$$

where $\Delta = (\alpha - 1)p^\alpha - \alpha p^{\alpha-1} + 2$.

Table 1 systematically evaluates the optimality of the linear codes generated by $M(\Gamma(Z_{p^\alpha}))$ based on the parameters established in **Theorem 2.6**. To provide a clearer understanding of the structural evolution of these codes, the table is divided into two distinct sections: the first explores the effect of increasing the base prime p while keeping the exponent fixed, and the second examines the impact of increasing the exponent α while holding the prime base constant. The optimality is assessed using the Singleton defect ($\sigma = n-k+1-d$) and the theoretical Hamming bound.

The rows 1–5 maintains a fixed exponent of $\alpha = 5$ and incrementally increases the prime base $p \in \{2, 3, 5, 7, 11\}$. As p grows, the order of the ring expands, leading to a substantial increase in both the length n and the dimension k of the code. Importantly, since the minimum distance is solely determined by the prime ($d = p - 1$), increasing p directly enhances the minimum distance and subsequently improves the error-correcting capability t. However, because the length of the code n increases significantly faster than the dimension k and the distance d, the Singleton defect δ widens rapidly. Despite drifting further from the Singleton bound, all generated codes in this section still satisfy the Hamming bound.

The rows 6–10 fix the prime base at $p = 5$ and increment the exponent α from 3 to 7. Higher exponents drastically increase the density of the zero divisor graph due to the rapid proliferation of zero divisors, causing an exponential increase in both n and k. Interestingly, because the minimum distance is independent of α, it remains constant at $d = 4$ across all these variations. Consequently, the error-correcting capability remains fixed at $t = 1$, regardless of how large the graph becomes. This structural limitation causes the Singleton defect to escalate dramatically (reaching $\sigma = 164000$ for $\alpha = 7$), indicating a high degree of redundancy. Nevertheless, these highly redundant codes theoretically remain valid, since they still satisfy the Hamming sphere-packing bound.

Having established the parameters of the linear code C_2 generated by $M(\Gamma(Z_{(p^\alpha)}))$ in **Theorem 3.6**, our next objective is to derive the precise parameters of its corresponding dual code, $C_2^\perp$. To construct this dual code, we systematically apply two foundational theorems that bridge coding theory and algebraic graph theory.

First, by **Theorem 2.8**, the dimension of a dual code, denoted as $k^\perp$, is intrinsically linked to the original code through the fundamental relation $k^\perp = n - k$. Since the length n and the dimension k of C_2 are explicitly defined in **Theorem 3.6**, evaluating $k^\perp$ is a direct algebraic substitution. Second, determining the minimum distance of the dual code requires an analysis of the structural properties of the zero divisor graph itself. As established in **Theorem 2.10**, the minimum distance of a dual code generated by an incidence matrix corresponds exactly to the girth (the shortest cycle length) of the graph. For the specific class of zero divisor graphs $\Gamma(Z_{(p^\alpha)})$, where $p > 2$ is a prime and $\alpha \geq 3$, by **Theorem 2.7** the girth is invariably 3. Consequently, the minimum distance of the dual code is precisely $d^\perp = 3$.

By integrating the calculated dimension and the fixed minimum distance derived from the girth of the graph, we systematically obtain the complete parameters for the dual code $C_2^\perp$, as formalized in the following corollary.

Corollary 3.7. Let C_2 be a binary linear code generated by $M(\Gamma(Z_{(p^\alpha)}))$, where $p > 2$ is a prime and $\alpha \geq 3$. The dual code $C_2^\perp$ is given by:

$$C_2^\perp = \begin{cases} \left[\frac{1}{2}(\Delta - p^{(\alpha-1)/2}),\ \frac{1}{2}(\Omega - p^{(\alpha-1)/2}),\ 3\right]_2 & \text{if } \alpha \text{ is odd,} \\ \left[\frac{1}{2}(\Delta - p^{\alpha/2}),\ \frac{1}{2}(\Omega - p^{\alpha/2}),\ 3\right]_2 & \text{if } \alpha \text{ is even.} \end{cases}$$

where $\Delta = (\alpha - 1)p^\alpha - \alpha p^{\alpha-1} + 2$, and $\Omega = \Delta - 2(p^{\alpha-1} - 2)$.

As an illustration of **Corollary 3.7**, by **Example 3.5**, we obtain

$$C_2^\perp = [13, 6, 2]_2.$$

3.2 Binary Linear Codes from Incidence Matrices of $\Gamma(Z_{(p^\alpha q^\beta)})$

In this subsection, we give parameter codes from the linear code constructed from the incidence matrix of $\Gamma(Z_{(p^\alpha q^\beta)})$. Unlike **Theorem 3.6**, in this part we directly examine $M(\Gamma(Z_{(p^\alpha q^\beta)}))$ to obtained its code parameters. This approach is taken because analyzing the cases with small values of α and β would be more complex.

Theorem 3.8. For every distinct prime p and q, and positive integers α and β, the binary linear code generated by $M(\Gamma(Z_{(p^\alpha q^\beta)}))$ is

$$C_2 = \begin{cases} \left[\frac{1}{2}\left(\Theta - p^{(\alpha-1)/2}q^{(\beta-1)/2}\right), k^*, d^*\right]_2 & \alpha, \beta \text{ odd,} \\ \left[\frac{1}{2}\left(\Theta - p^{(\alpha-1)/2}q^{\beta/2}\right), k^*, d^*\right]_2 & \alpha \text{ odd, } \beta \text{ even,} \\ \left[\frac{1}{2}\left(\Theta - p^{\alpha/2}q^{(\beta-1)/2}\right), k^*, d^*\right]_2 & \alpha \text{ even, } \beta \text{ odd,} \\ \left[\frac{1}{2}\left(\Theta - p^{\alpha/2}q^{\beta/2}\right), k^*, d^*\right]_2 & \alpha, \beta \text{ even.} \end{cases}$$

where

$$\Theta = \left((\alpha+1)p^\alpha - \alpha p^{\alpha-1}\right)\left((\beta+1)q^\beta - \beta q^{\beta-1}\right) - 2p^\alpha q^\beta + 2,$$

Table 1. Code Parameters from $\Gamma(Z_{p^\alpha})$ and Classical Bounds Comparison

Graph	p	α	$[n, k, d]$ – code	t	σ	Remark
$\Gamma(Z_{32})$	2	5	$[23, 14, 1]_2$	0	9	Satisfies Hamming bound, not MDS
$\Gamma(Z_{243})$	3	5	$[280, 79, 2]_2$	0	200	Satisfies Hamming bound, not MDS
$\Gamma(Z_{3125})$	5	5	$[4676, 623, 4]_2$	1	4050	Satisfies Hamming bound, not MDS
$\Gamma(Z_{16807})$	7	5	$[27588, 2399, 6]_2$	2	25184	Satisfies Hamming bound, not MDS
$\Gamma(Z_{161051})$	11	5	$[285440, 14639, 10]_2$	4	270792	Satisfies Hamming bound, not MDS
$\Gamma(Z_{125})$	5	3	$[86, 23, 4]_2$	1	60	Satisfies Hamming bound, not MDS
$\Gamma(Z_{625})$	5	4	$[676, 123, 4]_2$	1	550	Satisfies Hamming bound, not MDS
$\Gamma(Z_{3125})$	5	5	$[4676, 623, 4]_2$	1	4050	Satisfies Hamming bound, not MDS
$\Gamma(Z_{15625})$	5	6	$[29626, 3123, 4]_2$	1	26500	Satisfies Hamming bound, not MDS
$\Gamma(Z_{78125})$	5	7	$[179626, 15623, 4]_2$	1	164000	Satisfies Hamming bound, not MDS

$$k^* = p^\alpha q^\beta - p^{\alpha-1}q^{\beta-1}(p-1)(q-1) - 2, \quad d^* = \min\{p-1, q-1\}.$$

Proof. By **Theorem 2.9**, the binary linear code C_2 generated by $M(\Gamma(Z_{(p^\alpha q^\beta)}))$ has parameters

$$\left[|E(\Gamma(Z_{(p^\alpha q^\beta)}))|,\ |V(\Gamma(Z_{(p^\alpha q^\beta)}))| - 1,\ \lambda(\Gamma(Z_{(p^\alpha q^\beta)}))\right]_2.$$

Hence, determining the parameters of C_2 reduces to evaluating the order, the size, and the edge-connectivity of the graph $\Gamma(Z_{(p^\alpha q^\beta)})$.

We first determine the number of vertices. Using the standard property of Euler's totient function, we have

$$\begin{aligned} |V(\Gamma(Z_{(p^\alpha q^\beta)}))| &= p^\alpha q^\beta - \varphi(p^\alpha q^\beta) - 1 \\ &= p^\alpha q^\beta - p^\alpha q^\beta \left(1 - \tfrac{1}{p}\right)\left(1 - \tfrac{1}{q}\right) - 1 \\ &= p^\alpha q^\beta - p^{\alpha-1}q^{\beta-1}(p-1)(q-1) - 1. \end{aligned}$$

Consequently, the dimension of the code equals $|V(\Gamma(Z_{(p^\alpha q^\beta)}))| - 1$. Denoting this quantity by k^* gives

$$k^* = p^\alpha q^\beta - p^{\alpha-1}q^{\beta-1}(p-1)(q-1) - 2.$$

Next, we compute the number of edges of the graph, which determines the length of the code.

Next, we compute the number of edges of the graph, which determines the length of the code. By **Theorem 2.4**, the number of edges satisfies

$$|E(\Gamma(Z_{(p^\alpha q^\beta)}))| = \tfrac{1}{2}\left(\left(\sum_{m|p^\alpha q^\beta} m\,\varphi\left(\tfrac{p^\alpha q^\beta}{m}\right)\right) - \omega_{p^\alpha q^\beta} - 2p^\alpha q^\beta + 2\right). \quad (1)$$

To evaluate the divisor sum, consider first the divisors of p^α. For every divisor p^k with $k = 0, 1, \ldots, \alpha - 1$, we obtain

$$p^k \varphi\left(\tfrac{p^\alpha}{p^k}\right) = p^k p^{\alpha-k}\left(\tfrac{p-1}{p}\right) = p^{\alpha-1}(p-1) = p^\alpha - p^{\alpha-1},$$

and for $k = \alpha$

$$p^k \varphi\left(\tfrac{p^\alpha}{p^k}\right) = p^\alpha \varphi(1) = p^\alpha.$$

Therefore,

$$\sum_{p^k|p^\alpha} p^k \varphi\left(\tfrac{p^\alpha}{p^k}\right) = (\alpha+1)p^\alpha - \alpha p^{\alpha-1}. \quad (2)$$

Similarly, for the divisors q^l of q^β with $l = 0, 1, \ldots, \beta$, we obtain

$$\sum_{q^l|q^\beta} q^l \varphi\left(\tfrac{q^\beta}{q^l}\right) = (\beta+1)q^\beta - \beta q^{\beta-1}. \quad (3)$$

Since the arithmetic function $f(x) = x\varphi(n/x)$ is multiplicative, the Chinese Remainder Theorem allows the divisor sum over $p^\alpha q^\beta$ to be expressed as the product of the sums in (2) and (3). Hence,

$$\begin{aligned} \sum_{d|p^\alpha q^\beta} d\,\varphi\left(\tfrac{p^\alpha q^\beta}{d}\right) &= \left(\sum_{p^k|p^\alpha} p^k \varphi\left(\tfrac{p^\alpha}{p^k}\right)\right)\left(\sum_{q^l|q^\beta} q^l \varphi\left(\tfrac{q^\beta}{q^l}\right)\right) \\ &= \left((\alpha+1)p^\alpha - \alpha p^{\alpha-1}\right)\left((\beta+1)q^\beta - \beta q^{\beta-1}\right). \end{aligned} \quad (4)$$

Furthermore, by **Theorem 2.4**, the quantity $\omega_{p^\alpha q^\beta}$ depends on the parity of α and β and is given by

$$\omega_{p^\alpha q^\beta} = \begin{cases} p^{(\alpha-1)/2} q^{(\beta-1)/2} & \alpha, \beta \text{ odd}, \\ p^{(\alpha-1)/2} q^{\beta/2} & \alpha \text{ odd}, \beta \text{ even}, \\ p^{\alpha/2} q^{(\beta-1)/2} & \alpha \text{ even}, \beta \text{ odd}, \\ p^{\alpha/2} q^{\beta/2} & \alpha, \beta \text{ even}. \end{cases} \quad (5)$$

Substituting (4) and (5) into (1), and letting

$$\Theta = \big((\alpha+1)p^{\alpha} - \alpha p^{\alpha-1}\big)\big((\beta+1)q^{\beta} - \beta q^{\beta-1}\big) - 2p^{\alpha}q^{\beta} + 2,$$

we obtain

$$|E(\Gamma(Z_{(p^{\alpha}q^{\beta})}))| = \begin{cases} \frac{1}{2}\big(\Theta - p^{(\alpha-1)/2}q^{(\beta-1)/2}\big) & \alpha, \beta \text{ odd}, \\ \frac{1}{2}\big(\Theta - p^{(\alpha-1)/2}q^{\beta/2}\big) & \alpha \text{ odd}, \beta \text{ even}, \\ \frac{1}{2}\big(\Theta - p^{\alpha/2}q^{(\beta-1)/2}\big) & \alpha \text{ even}, \beta \text{ odd}, \\ \frac{1}{2}\big(\Theta - p^{\alpha/2}q^{\beta/2}\big) & \alpha, \beta \text{ even}. \end{cases}$$

Finally, by **Theorem 2.5**, we obtain

$$\lambda(\Gamma(Z_{(p^{\alpha}q^{\beta})})) = \min\{p-1, q-1\}.$$

Let $d^* = \min\{p-1, q-1\}$ denote the minimum distance of the code.

Combining the obtained values of $|E(\Gamma(Z_{(p^{\alpha}q^{\beta})}))|$, k^*, and d^* with the parameter formula from **Theorem 2.9**, we conclude that the binary linear code C_2 has parameter

$$C_2 = \begin{cases} \left[\frac{1}{2}\big(\Theta - p^{(\alpha-1)/2}q^{(\beta-1)/2}\big), k^*, d^*\right]_2 & \alpha, \beta \text{ odd}, \\ \left[\frac{1}{2}\big(\Theta - p^{(\alpha-1)/2}q^{\beta/2}\big), k^*, d^*\right]_2 & \alpha \text{ odd}, \beta \text{ even}, \\ \left[\frac{1}{2}\big(\Theta - p^{\alpha/2}q^{(\beta-1)/2}\big), k^*, d^*\right]_2 & \alpha \text{ even}, \beta \text{ odd}, \\ \left[\frac{1}{2}\big(\Theta - p^{\alpha/2}q^{\beta/2}\big), k^*, d^*\right]_2 & \alpha, \beta \text{ even}. \end{cases}$$

where

$$\Theta = \big((\alpha+1)p^{\alpha} - \alpha p^{\alpha-1}\big)\big((\beta+1)q^{\beta} - \beta q^{\beta-1}\big) - 2p^{\alpha}q^{\beta} + 2,$$

$$k^* = p^{\alpha}q^{\beta} - p^{\alpha-1}q^{\beta-1}(p-1)(q-1) - 2, \quad d^* = \min\{p-1, q-1\}.$$

Next, we aim to determine the parameters of the dual code $C_2^{\perp}$ corresponding to the linear code C_2 obtained in **Theorem 3.8.** To achieve this, we rely on two fundamental theoretical results. First, by **Theorem 2.8**, the dimension of the dual code, denoted as $k^{\perp}$, is simply given by the relation $k^{\perp} = n - k$, where n and k are the length and dimension of the original code C_2 explicitly derived in **Theorem 3.8.** Second, by **Theorem 2.10**, the minimum distance of the dual code generated by an incidence matrix is equal to the girth of its corresponding graph.

Therefore, to establish the minimum distance, our immediate task is to evaluate the girth of the zero divisor graph $\Gamma(Z_{(p^{\alpha}q^{\beta})})$. According to **Theorem 2.6** in their work, the girth $g_r(\Gamma(Z_n))$ is determined exclusively by the prime factorization of n. Restricting their theorem to our domain where $n = p^{\alpha}q^{\beta}$ (with $p < q$ being distinct primes, and positive integers α, β), the condition $n \in \{4, 8, 9\}$ is naturally excluded. Consequently, the girth can only take values from the set $\{0, 3, 4\}$ under the following specific conditions:

- $g_r(\Gamma(\mathbb{Z}_{p^{\alpha}q^{\beta}})) = 0$ if $n = 2q$ (i.e., $p = 2$, $\alpha = 1$, $\beta = 1$).
- $g_r(\Gamma(\mathbb{Z}_{p^{\alpha}q^{\beta}})) = 4$ if $n = pq$ for $p \geq 3$ (i.e., $p \geq 3$, $\alpha = 1$, $\beta = 1$) or $n = 4q$ (i.e., $p = 2$, $\alpha = 2$, $\beta = 1$).
- $g_r(\Gamma(\mathbb{Z}_{p^{\alpha}q^{\beta}})) = 3$ in all other cases.

By combining the dimension $k^{\perp} = n - k$ and the minimum distance $d^{\perp} = 3$ derived from the girth calculation, we obtain the exact parameters of the dual code $C_2^{\perp}$ as presented in the following corollary.

Corollary 3.9. Let C_2 be a binary linear code generated by $M(\Gamma(Z_{(p^{\alpha}q^{\beta})}))$, where p and q are distinct primes ($p < q$), positive integers α and β. The parameters of the dual codes $C_2^{\perp} = [n, k^{\perp}, d^{\perp}]_2$ are classified into the following cases:

$$C_2^{\perp} = \begin{cases} [(p-1)(q-1),\ (p-2)(q-2),\ 4]_2 & \text{if } \alpha = 1, \beta = 1, p > 2, \\ [4(q-1),\ 2(q-2),\ 4]_2 & \text{if } \alpha = 2, \beta = 1, p = 2, \\ \left[\frac{1}{2}\big(\Theta - p^{(\alpha-1)/2}q^{(\beta-1)/2}\big),\ \frac{1}{2}\big(\Theta - p^{(\alpha-1)/2}q^{(\beta-1)/2}\big) - k^*,\ 3\right]_2 & \text{if } \alpha, \beta \text{ odd with } \alpha + \beta \geq 4, \\ \left[\frac{1}{2}\big(\Theta - p^{(\alpha-1)/2}q^{\beta/2}\big),\ \frac{1}{2}\big(\Theta - p^{(\alpha-1)/2}q^{\beta/2}\big) - k^*,\ 3\right]_2 & \text{if } \alpha \text{ odd}, \beta \text{ even}, \beta \geq 2, \\ \left[\frac{1}{2}\big(\Theta - p^{\alpha/2}q^{(\beta-1)/2}\big),\ \frac{1}{2}\big(\Theta - p^{\alpha/2}q^{(\beta-1)/2}\big) - k^*,\ 3\right]_2 & \text{if } \alpha \text{ even}, \beta \text{ odd}, \alpha \geq 2, \\ p > 2, & \\ \left[\frac{1}{2}\big(\Theta - p^{\alpha/2}q^{\beta/2}\big),\ \frac{1}{2}\big(\Theta - p^{\alpha/2}q^{\beta/2}\big) - k^*,\ 3\right]_2 & \text{if } \alpha, \beta \text{ even}, \alpha, \beta \geq 2. \end{cases}$$

where the auxiliary parameter Θ and the dimension of the primary code k^* are defined as follows:

$$\Theta = \big((\alpha+1)p^{\alpha} - \alpha p^{\alpha-1}\big)\big((\beta+1)q^{\beta} - \beta q^{\beta-1}\big) - 2p^{\alpha}q^{\beta} + 2,$$

$$k^* = p^{\alpha}q^{\beta} - p^{\alpha-1}q^{\beta-1}(p-1)(q-1) - 2.$$

Remark 3.10. In **Corollary 3.9** for the case $p = 2$, $\alpha = 1$, $\beta = 1$, the zero divisor graph $\Gamma(Z_{2q})$ is acyclic. By standard graph theory conventions Diestel (2024), the girth of an acyclic graph is defined as 0. Since the dual code $C^{\perp}$ generated by an incidence matrix corresponds precisely to the cycle space of the graph (Diestel, 2024), the absence of cycles yields a trivial cycle space $\{\vec{0}\}$ with dimension $k^{\perp} = 0$. Because the generated code has dimension 0, its minimum distance is technically undefined.

To clarify the construction of the linear code described in **Theorem 3.8**, we present **Example 3.11.** This example serves as a simple illustration of the results given in **Theorem 3.8** and **Corollary 3.9** for a specific case.

Example 3.11. For $p = 2$, $q = 3$, and $\alpha = \beta = 2$ the graph $\Gamma(Z_{36})$ is as in Figure 2.

Then, the binary linear codes generated by $M(\Gamma(Z_{36}))$ is

$$C_2 = [46, 22, 1]_2 \quad \text{and its dual} \quad C_2^{\perp} = [46, 24, 3]_2.$$

To evaluate the practical efficiency of the binary linear codes constructed in **Theorem 3.8**, we compute their parameters for various instances of the graph $\Gamma(Z_{(p^{\alpha}q^{\beta})})$. Since the theoretical framework of the Singleton and Hamming bounds has been

Table 2. Code Parameters from $\Gamma(Z_{pq^{\alpha\beta}})$ and Classical Bounds Comparison

Graph	p	q	α	β	$[n,k,d]_2$	t	δ	Remark
$\Gamma(Z_6)$	2	3	1	1	$[2,2,1]_2$	0	0	MDS and perfect code
$\Gamma(Z_{10})$	2	5	1	1	$[4,4,1]_2$	0	0	MDS and perfect code
$\Gamma(Z_{14})$	2	7	1	1	$[6,6,1]_2$	0	0	MDS and perfect code
$\Gamma(Z_{15})$	3	5	1	1	$[8,5,2]_2$	0	2	Satisfies Hamming bound
$\Gamma(Z_{21})$	3	7	1	1	$[12,7,2]_2$	0	4	Satisfies Hamming bound
$\Gamma(Z_{22})$	2	11	1	1	$[10,10,1]_2$	0	0	MDS and perfect code
$\Gamma(Z_{23})$	3	11	1	1	$[20,11,2]_2$	0	8	Satisfies Hamming bound
$\Gamma(Z_{35})$	5	7	1	1	$[24,9,4]_2$	1	8	Satisfies Hamming bound
$\Gamma(Z_{55})$	5	11	1	1	$[40,13,4]_2$	1	24	Satisfies Hamming bound
$\Gamma(Z_{77})$	7	11	1	1	$[60,15,6]_2$	2	40	Satisfies Hamming bound
$\Gamma(Z_{12})$	2	2	3	1	$[8,6,1]_2$	0	2	Satisfies Hamming bound
$\Gamma(Z_{18})$	2	3	3	1	$[13,10,1]_2$	0	3	Satisfies Hamming bound
$\Gamma(Z_{24})$	2	4	3	1	$[18,13,2]_2$	0	5	Satisfies Hamming bound
$\Gamma(Z_{36})$	2	3	2	2	$[46,22,11]_2$	0	24	Satisfies Hamming bound
$\Gamma(Z_{48})$	2	3	3	2	$[71,30,11]_2$	0	41	Satisfies Hamming bound
$\Gamma(Z_{72})$	2	3	3	3	$[136,46,11]_2$	0	90	Satisfies Hamming bound
$\Gamma(Z_{108})$	2	3	3	4	$[214,70,11]_2$	0	144	Satisfies Hamming bound
$\Gamma(Z_{144})$	2	3	3	5	$[355,99,11]_2$	0	256	Satisfies Hamming bound
$\Gamma(Z_{216})$	2	3	3	6	$[592,142,11]_2$	0	450	Satisfies Hamming bound
$\Gamma(Z_{288})$	2	3	5	2	$[883,190,11]_2$	0	693	Satisfies Hamming bound

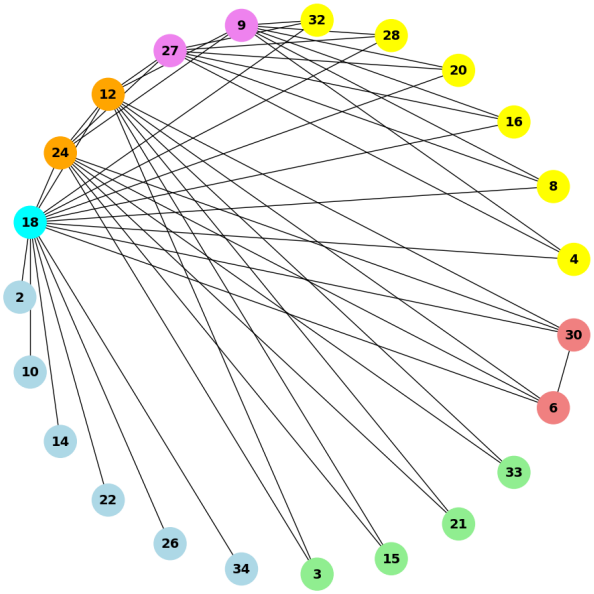

Figure 2. The Graph $\Gamma(Z_{36})$

established in the preliminaries, we can directly compute the Singleton defect, denoted as

$$\sigma = (n - k + 1) - d,$$

and verify the Hamming bound condition to determine the relative optimality of these codes, as summarized in Table 2.

Table 2 is systematically divided into two sections to analyze the structural behavior of the constructed codes. The first section (rows 1–10) investigates the influence of the base primes p and q by restricting the exponents to $\alpha = \beta = 1$. As the primes p and q increase, the order and size of the zero divisor graph expand proportionally, leading to a steady growth in both the length n and dimension k of the linear code. Since the minimum distance depends strictly on the primes ($d = \min\{p-1, q-1\}$), larger prime pairs naturally yield a higher minimum distance, which subsequently enhances the error-correcting capability t. Notably, when one of the primes is $p = 2$, the codes achieve perfect optimality with a Singleton defect of $\sigma = 0$, making them Maximum Distance Separable (MDS) codes. However, as both p and q become larger odd primes, the Singleton defect gradually increases, reflecting a deviation from the Singleton bound.

The second section (rows 11–20) explores the impact of the exponents α and β by fixing the base primes to $p = 2$ and $q = 3$. Higher exponents generate a significantly denser zero divisor graph due to the abundance of nilpotent elements and intersecting divisors. This structural density drastically increases both the code length and dimension. Interestingly, for these specific cases, the minimum distance remains strictly constant at $d = 1$ (bounded by $\min\{2-1, 3-1\} = 1$). Consequently, the error-correcting capability is restricted to $t = 0$ in all variations. Furthermore, with exponential growth of the size of the graph, the Singleton defect σ increases significantly (up to $\sigma = 693$). This highlights that the complex combinato-

rial structure introduced by higher prime powers deteriorates the relative optimality of the code in terms of the Singleton bound. Despite this, all evaluated instances strictly satisfy the Hamming bound, confirming their robust theoretical validity.

4. CONCLUSIONS

This study presents the construction of binary linear codes from $M(\Gamma(Z_n))$, for $n = p^\alpha$ and $n = p^\alpha q^\beta$, where distinct prime numbers p and q, and positive integers α and β. The parameters and duals of the resulting codes over the binary field $\mathbb{F}_2$ have been determined and analyzed. Our analysis demonstrates that generating optimal Maximum Distance Separable (MDS) codes from these graphs is achievable, although this occurs only in specific cases involving small primes. As the prime bases or their exponents increase, the structural density of the zero divisor graphs naturally leads to highly redundant codes with a large Singleton defect and limited error-correcting capabilities. However, the primary theoretical contribution of this work lies in providing an exact mathematical characterization of the length, dimension, and dual distance of these codes for the broader classes of rings $Z_{(p^\alpha)}$ and $Z_{(p^\alpha q^\beta)}$, which have not been fully explored in the previous literature. Future work may explore analogous constructions over finite fields $\mathbb{F}_q$ with $q > 2$. Another direction is the investigation of modified graph matrices, such as weighted incidence matrices or specific subgraphs, to mitigate the high redundancy and obtain codes with optimal or near-optimal parameters. These investigations may contribute to the development of new classes of codes with potential applications in secure communication systems.

5. ACKNOWLEDGMENT

The author gratefully acknowledges the anonymous reviewers for their careful reading, valuable comments, and insightful suggestions, all of which have contributed significantly to the improvement of this manuscript. The author also extends sincere thanks to the editorial team for their thoughtful consideration and support throughout the publication process.

REFERENCES

Anderson, D. F. and P. S. Livingston (1999). The Zero-Divisor Graph of a Commutative Ring. *Journal of Algebra*, **217**; 434–447

Annamalai, N. and C. Durairajan (2021). Linear Codes from Incidence Matrices of Unit Graphs. *Journal of Information and Optimization Sciences*, **42**(8); 1943–1950

Annamalai, N. and C. Durairajan (2022). Codes from the Incidence Matrices of Zero-Divisor Graphs. *Journal of Discrete Mathematical Sciences and Cryptography*; 1–9

Beck, I. (1988). Coloring of Commutative Rings. *Journal of Algebra*, **116**; 208–226

Chartrand, G., H. Jordon, V. Vatter, and P. Zhang (2024). *Graphs and Digraphs*. Chapman and Hall/CRC

Dankelmann, P., J. D. Key, and B. G. Rodrigues (2011). Codes from Incidence Matrices of Graphs. *Designs, Codes and Cryptography*, **68**; 1–21

Diestel, R. (2024). *Graph Theory*. Springer

Fish, W., J. D. Key, and E. Mwambene (2010). Binary Codes from the Line Graph of the n-Cube. *Journal of Symbolic Computation*, **45**(7); 800–812

Herstein, I. N. (1995). *Abstract Algebra*. John Wiley & Sons

Jain, R. S., B. S. Reddy, and W. M. Shaikh (2023). Construction of Linear Codes from the Unit Graph $G(Z_n)$. Asian-European Journal of Mathematics. 2350213

Key, J. D. and R. Seneviratne (2008). Permutation Decoding for Binary Codes from Lattice Graphs. *Discrete Mathematics*, **308**(13); 2862–2867

Ling, S. and C. Xing (2004). *Coding Theory: A First Course*. Cambridge University Press

Magi, P., S. M. Jose, and A. Kishore (2020). Spectrum of the Zero-Divisor Graph on the Ring of Integers Modulo n. *Journal of Mathematical and Computational Science*, **10**(4); 1285–1297

Mukhtar, A., R. Murtaza, S. U. Rehman, S. Usman, and A. Q. Baig (2020). Computing the Size of Zero Divisor Graphs. *Journal of Information and Optimization Sciences*, **41**(4); 855–864

Nachmani, E., E. Marciano, L. Lugosch, W. J. Gross, D. Burshtein, and Y. Be'ery (2018). Deep Learning Methods for Improved Decoding of Linear Codes. *IEEE Journal of Selected Topics in Signal Processing*, **12**(1); 119–131

Ngo, X. T., S. Bhasin, J.-L. Danger, S. Guilley, and Z. Najm (2015). Linear Complementary Dual Code Improvement to Strengthen Encoded Circuit Against Hardware Trojan Horses. In *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. pages 82–87

Phillips, A., J. Rogers, K. Tolliver, and F. Worek (2004). Uncharted Territory of Zero Divisor Graphs and Their Complements. SUMSRI, Miami University

Pi, S. J., S. H. Kim, and J. W. Lim (2019). The Zero-Divisor Graph of the Ring of Integers Modulo n. *Kyungpook Mathematical Journal*, **59**(4); 591–601

Reddy, B. S., R. S. Jain, and N. Laxmikanth (2020). Vertex and Edge Connectivity of the Zero Divisor Graph $\Gamma(Z_n)$. *Communications in Mathematics and Applications*, **11**(2); 253–258

Roth, R. (2006). *Introduction to Coding Theory*. Cambridge University Press

Saranya, R. and C. Durairajan (2021). Codes from Incidence Matrix of Some Regular Graphs. *Discrete Mathematics, Algorithms and Applications*, **13**(4); 2150035

Saranya, R. and C. Durairajan (2022). Codes from Incidence Matrices of (n,1)-Arrangement Graphs and (n,2)-Arrangement Graphs. *Journal of Discrete Mathematical Sciences and Cryptography*, **25**(2); 373–393

Shaikh, W. M., R. S. Jain, and B. S. Reddy (2024). Construction of Linear Codes from the Unit Graph $G(Z_n \oplus Z_n)$. arXiv preprint

Singh, P. and V. K. Bhat (2020). Zero-Divisor Graphs of Finite

Commutative Rings: A Survey. *Surveys in Mathematics & Its Applications*, **15**

Vanstone, S. A. and P. C. Van Oorschot (2013). *An Introduction to Error Correcting Codes with Applications*. Springer Science & Business Media