On the Probability and Graph of Some Finite Rings of Matrices

Nurhidayah Zaid[1,a)], Nor Haniza Sarmin[1,b)] and Sanhan Muhammad Salih Khasraw[2,c)]

[1]*Department of Mathematical Sciences, Faculty of Science, Universiti Teknologi Malaysia, 81310 Skudai, Johor Bahru, Johor, Malaysia.*
[2]*Department of Mathematics, College of Basic Education, Salahaddin University-Erbil, Kurdistan Region, Iraq.*

[a)]Corresponding author: nurhidayah57@graduate.utm.my
[b)]nhs@utm.my
[c)]sanhan.khasraw@su.edu.krd

Abstract. The study on probability theory in finite rings has been an interest of various researchers. One of the probabilities that has caught their attention is the probability that two elements of a ring have product zero. In this study, the probability is determined for a finite ring R of matrices over integers modulo four. First, the annihilators of R are determined with the assistance of Groups, Algorithms and Programming (GAP) software and then the probability is calculated using the definition. Next, by using the results obtained, the zero divisor graph of the ring R is constructed. A zero divisor graph is defined as a graph in which the zero divisors of R are its vertices and two vertices are connected by an edge if their product is zero.

INTRODUCTION

A ring R is a set which is an abelian group by addition, associative by multiplication and also satisfy the distributive law [1]. Interesting features of rings have lead to numerous researches in various fields, such as in cryptography, physics and computer science. In this paper, finite rings are particularly applied in probability and graph theory. In probability theory, the probability that two elements of a finite ring have product zero is determined for some finite rings of matrices. Meanwhile, in graph theory, this paper focuses on constructing the zero divisor graph of the same ring of matrices.

Probability theory has been widely applied in groups, as well as in rings. One of the probabilities which is commonly known in this field is the commutativity degree of a group which is used to determine the abelianness of a group. The commutativity degree of a group is introduced by Gustafson [2] in 1973 and is defined as in the following.

Definition 1 *Let G be a finite group with order n. The probability that two elements selected at random from G are commutative is $\frac{|C|}{n^2}$ where $C = \{(x, y) \in G \times G | xy = yx\}$.*

From the definition, it is clear that the commutativity degree of a group is one if and only if all elements of the group commute. This notion has been generalized in many ways, such as the relative commutativity degree [3], conjugation degree [4] and autocommuting probability [5] of a finite group.

The notion of commutativity degree in groups has also attracted various mathematicians to apply it in rings. This has been started by MacHale [6] in 1976, where a study is done to determine the probability that a pair of elements in a finite ring R commute. The author has defined the probability as

$$P(R) = \frac{\sum_{r\in R} |C_R(r)|}{|R|^2} \ ,$$

Proceedings of the 27th National Symposium on Mathematical Sciences (SKSM27)
AIP Conf. Proc. 2266, 060010-1–060010-6; https://doi.org/10.1063/5.0018067
Published by AIP Publishing. 978-0-7354-2029-8/$30.00

where $C_R(r)$ is the subring $\{x \in R | xr = rx\}$. In addition, in the article, MacHale has studied the probability in subrings of finite rings and found that $P(R) \leq P(S)$ whenever S is a subring of R.

This concept has welcomed numerous generalizations and extensions of probability in rings. For example, recently in 2014, Buckley *et al*. [7] has formally defined the commuting probability in R to be

$$\Pr(R) = \frac{|\{(x, y) \in R \times R | xy = yx\}|}{|R|^2},$$

where R is a finite ring, and $|R|$ is the order of the ring R.

Another recent study which involves probability in finite rings includes the study on the relative commuting probability of a subring in a finite ring which has been done by Dutta *et al*. [8] in 2017. Later in 2018, Khasraw [9] introduced a new type of probability in rings, where the author studied the probability that a pair of elements of a finite ring have product zero.

Meanwhile, a graph is a mathematical object which consists of vertices and edges, and is commonly used to show the relation between two objects. Throughout this paper, discussions are made on the zero divisor graph. This graph is initially introduced by Beck [10] in 1988. Beck's interest was mainly on the coloring of commutative rings. In the study, Beck has considered a simple graph whose vertices are the elements of a finite commutative ring R, such that two different elements a and b are adjacent if $ab = 0$. The graph has later been introduced formally by Anderson and Livingston [11] in 1999, where it is named the zero divisor graph.

In 2002, Redmond [12] extended the research on zero divisor graph to noncommutative rings. Redmond has found that for a noncommutative ring, the zero divisor graph must be a directed graph. In the paper, Redmond has also proved that the graph need not to be a connected graph in finite noncommutative rings. As a result, a lot of extensions have been done to the research on zero divisor graph, which include the ideal based zero divisor graph [13] and the compressed zero divisor graph [14].

This article contains four sections. The first section provides the introduction of the research. Next, some preliminaries of the research are provided in the second section. The third section presents the results and discussions. Lastly, the conclusion of the study is given in the fourth section.

PRELIMINARIES

Some definitions and fundamental concepts related to this study are provided in this section. The methodology of the study is also described.

The finite ring R considered in this study is the ring of 2×2 matrices over the set of integers modulo four, $M_2(\mathbb{Z}_4)$. The ring R is applied in probability and graph theory. In probability theory, the probability that two elements of R have product zero is determined. The definition is given in the following.

Definition 2 [9] *The probability $P(R)$ that a pair of elements chosen at random (with replacement) from a ring R have product zero is*

$$P(R) = \frac{|Ann|}{|R \times R|},$$

where $Ann = \{(p, q) \in R \times R | pq = 0\}$.

Another probability related to Definition 2 is newly defined and is determined for the ring R, which is stated in the following.

Definition 3 *The probability $\tilde{P}(R)$ that a pair of commuting elements chosen at random (with replacement) from a ring R have product zero is*

$$\tilde{P}(R) = \frac{\{(p, q) \in R \times R | pq = qp = 0\}}{|R \times R|}.$$

After determining the probabilities, the zero divisor graph is constructed for the ring R. To construct the graph, the zero divisors of R are firstly determined. The definition of the zero divisor of a finite ring is stated as follows.

Definition 4 [1] *Let p and q be two nonzero elements of a finite ring R. If $pq = 0$, then p and q are the zero divisors of R. The set of all zero divisors in R is denoted as $Z(R)$.*

After determining the zero divisors of R, the zero divisor graph of R, which is denoted as $\Gamma(R)$ is constructed based on the following definition.

Definition 5 [11] *Let R be a commutative ring and $Z(R)$ be the set of zero divisors in R. Then, the zero divisor graph, denoted as $\Gamma(R)$ is a simple graph of R where the vertices are $Z(R)$. For distinct $p, q \in Z(R)$, the vertices p and q are adjacent if and only if $pq = 0$.*

Lastly, another type of zero divisor graph, where commuting elements are considered, is constructed for R. The definition of the graph, which is denoted as $\tilde{\Gamma}(R)$, is given as follows.

Definition 6 *The commuting zero divisor graph, $\tilde{\Gamma}(R)$ is a simple graph of R where its vertices are the set of zero divisors of R, $Z(R)$. An arc is constructed between two vertices, say p and q in $Z(R)$ if and only if $pq = qp = 0$.*

RESULTS AND DISCUSSIONS

In this section, the results obtained in this study are given in the form of propositions. The ring considered is the finite ring of 2×2 matrices over the set of integers modulo four, $M_2(\mathbb{Z}_4)$. Definition 2 to Definition 6 are used in obtaining the results.

Proposition 1 *Let $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}_4 \right\}$. Then, the probability that a pair of elements of R have product zero, $P(R) = \frac{77}{2048}$.*

Proof Let $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}_4 \right\}$. The number of elements in R, $|R| = |\mathbb{Z}^4|^4 = 4^4 = 256$. By Definition 2, the annihilator, $Ann = \{(p, q) \in R \times R | pq = 0\}$. For example, when $p = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \in R$, the annihilator of p is

$$\begin{aligned} Ann(p) &= \{q \in R | pq = 0\} \\ &= \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 2 & 2 \end{pmatrix} \right\}. \end{aligned}$$

Since the ring R has a large order, a programming code is constructed in Groups, Algorithms and Programming (GAP) software to assist the computations of the annihilators of R. The GAP algorithm can be found in Appendix A. From the calculations, it was found that the ring R has a total of 2464 pairs of annihilators. Therefore, by using Definition 2,

$$P(R) = \frac{|Ann|}{|R \times R|} = \frac{2464}{256 \times 256} = \frac{77}{2048}. \blacksquare$$

Proposition 2 *Let $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}_4 \right\}$. Then, the probability that a pair of commuting elements of R have product zero, $\tilde{P}(R) = \frac{299}{32768}$.*

Proof Let $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}_4 \right\}$ and $|R| = 256$. In this case, pairs of commuting elements that have product zero are considered. For example, when $p = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \in R$, the annihilator,

$$\begin{aligned} Ann(p) &= \{q \in R | pq = qp = 0\} \\ &= \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix} \right\}. \end{aligned}$$

A GAP algorithm has been created to compute the annihilators and can be found in Appendix B. From the calculations, it was found that there are 598 pairs of commuting elements which have product zero. Therefore, the probability that two commuting elements of R have product zero,

$$\tilde{P}(R) = \frac{598}{256 \times 256} = \frac{299}{32768}. \blacksquare$$

Proposition 3 *Let* $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}_4 \right\}$. *Then, the zero divisor graph of R,* $\Gamma(R)$ *is a directed graph of 159 vertices and 1928 arcs.*

Proof Let $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}_4 \right\}$. From the annihilators found in Proposition 1 and by using Definition 4, the zero divisors of R are determined. It has been found that the ring R has 159 zero divisors. Some of the elements of $Z(R)$ includes $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$. Since $|Z(R)| = 159$, from Definition 5, it is clear that the zero divisor graph of R, $\Gamma(R)$ has 159 vertices. Then, an arc is constructed between two vertices, $p \to q$ if and only if $pq = 0$. By using the calculations of annihilators that have been made earlier in Proposition 1, the pairs where $pp = 0$ are eliminated since $\Gamma(R)$ is a simple graph. Thus, it has been found that the graph $\Gamma(R)$ has 1928 arcs. Therefore, $\Gamma(R)$ is a directed graph with 159 vertices and 1928 arcs. $\blacksquare$

Proposition 4 *Let* $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}_4 \right\}$. *Then, the commuting zero divisor graph of R,* $\tilde{\Gamma}(R)$ *is a directed graph of 159 vertices and 314 arcs.*

Proof Let $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}_4 \right\}$. The proof for this proposition is similar to the previous proposition. Since $|Z(R)| = 159$, then the commuting zero divisor graph $\tilde{\Gamma}(R)$ clearly has 159 vertices. In this case, only commuting elements of R which has product zero are considered, therefore from the annihilators which have been determined in Proposition 2, it has been found that the graph $\tilde{\Gamma}(R)$ has a total of 314 arcs. Therefore, $\tilde{\Gamma}(R)$ is a directed graph of 159 vertices and 314 arcs. $\blacksquare$

CONCLUSION

In this study, the probability that a pair of elements of a finite ring have product zero has been determined for a ring R of 2×2 matrices over the set of integers modulo four, $M_2(\mathbb{Z}_4)$. Two cases have been considered which are $pq = 0$ and $pq = qp = 0$, where p and q are elements of R. The results have shown that $P(R) = \frac{77}{2048}$ and $\tilde{P}(R) = \frac{299}{32768}$.

Other than that, the zero divisor graphs have been constructed for the ring R, considering the same two cases. It has been found that both $\Gamma(R)$ and $\tilde{\Gamma}(R)$ have 159 vertices. However, $\Gamma(R)$ has a total of 1928 arcs, while $\tilde{\Gamma}(R)$ has 314 arcs.

ACKNOWLEDGEMENTS

This research is funded by Universiti Teknologi Malaysia (UTM) Fundamental Research Grant, cost center code 20H70. In addition, we would also like to acknowledge UTM for the financial funding through UTM Zamalah Scholarship.

REFERENCES

[1] J. Fraleigh and V. Katz, *A first course in abstract algebra*, 7th ed. (Addison-Wesley, 2003).
[2] W. H. Gustafson, The American Mathematical Monthly **80**, 1031–1034 (1973).
[3] A. Erfanian, R. Rezaei, and P. Lescot, Communications in Algebra **35**, 4183–4197 (2007).
[4] S. Zamri, N. H. Sarmin, H. I. Mat Hassim, and M. A. El-sanfaz, "On the conjugation degree of a metacyclic 3-group," (2017), preprint.
[5] P. Dutta and R. K. Nath, Communications in Algebra **46**, 961–969 (2018).
[6] D. MacHale, The American Mathematical Monthly **83**, 30–32 (1976).
[7] S. M. Buckley, D. Machale, and N. S. Aine, "Finite rings with many commuting pairs of elements," (2014), preprint.
[8] J. Dutta, D. K. Basnet, and R. K. Nath, Indagationes Mathematicae **28**, 372–382 (2017).
[9] S. M. S. Khasraw, "What is the probability that two elements of a finite ring have product zero?" (2018), preprint.
[10] I. Beck, Journal of Algebra **116**, 208–226 (1988).
[11] D. F. Anderson and P. S. Livingston, Journal of Algebra **217**, 434–447 (1999).
[12] S. Redmond, International Journal of Commutative Rings **1**, 203–211 (2002).
[13] S. P. Redmond, Communications in Algebra **31**, 4425–4443 (2003).
[14] X. Ma, D. Wang, and J. Zhou, Journal of the Korean Mathematical Society **53**, 519–532 (2016).

APPENDICES

This section provides the algorithms constructed in GAP software that assist in the computations of results in this study.

Appendix A

This GAP algorithm is constructed to compute the annihilators and the probability that two elements of a ring have product zero for 2×2 matrices over integers modulo four, $M_2(\mathbb{Z}_4)$.

```
A:=[];;
n:=4;
s:=0;
r:=Integers mod n;;
m1:=[ [ One(r), Zero(r) ],
      [ Zero(r), Zero(r) ]];
m2:=[ [ Zero(r), One(r)  ],
      [ Zero(r), Zero(r) ]];
m3:=[ [ Zero(r), Zero(r) ],
      [ One(r), Zero(r)  ]];
m4:=[ [ Zero(r), Zero(r) ],
      [ Zero(r), One(r)  ]];
rm:=Ring(m1, m2, m3, m4);
e:=Elements(rm);
for i in [1..Size(e)] do
 a:=e[i];
```

```
  for j in [1..Size(e)] do
   b:=e[j];
   if a*b=Zero(rm) then
    s:=s+1;
    Print(s,"\n");
    Display(a);
    Print("--------","\n");
    Display(b);
    Print("-----------------------------","\n");
    Add(A, 1);
   fi;
  od;
od;
p:=Size(A)/Size(rm)^2;
Print("P(rm",n,") = ",p,"\n");
```

Appendix B

This GAP algorithm is constructed to compute the annihilators and the probability that two commuting elements of a ring have product zero for 2×2 matrices over integers modulo four, $M_2(\mathbb{Z}_4)$.

```
A:=[];;
n:=4;
r:=Integers mod n;;
m1:=[ [ One(r), Zero(r) ],
      [ Zero(r), Zero(r) ]];
m2:=[ [ Zero(r), One(r)  ],
      [ Zero(r), Zero(r) ]];
m3:=[ [ Zero(r), Zero(r) ],
      [ One(r), Zero(r) ]];
m4:=[ [ Zero(r), Zero(r) ],
      [ Zero(r), One(r) ]];
rm:=Ring(m1, m2, m3, m4);
e:=Elements(rm);
for i in [1..Size(e)] do
  a:=e[i];
  for j in [i..Size(e)] do
   b:=e[j];
   if a*b=Zero(rm) and b*a=Zero(rm) then
    Display(a);
    Print("--------", "and","\n");
    Display(b);
    Print("-----------------------------","\n");
    Print("-----------------------------","\n");
    Add(A, 1);
   fi;
  od;
od;
p:=Size(A)/Size(rm)^2;
Print("P(rm",n,") = ",p,"\n");
```