MJFAS MALAYSIAN JOURNAL OF FUNDAMENTAL AND APPLIED SCIENCES
PRINT ISSN: 2289-5981 | ONLINE ISSN: 2289-599X

RESEARCH ARTICLE

What is the probability that two elements of a finite ring have product zero?

Sanhan Muhammad Salih Khasraw*

Department of Mathematics, College of Education, Salahaddin University-Erbil, Erbil, Kurdistan Region Iraq

*Corresponding author: *sanhan.khasraw@su.edu.krd*

Article history
Received 23 March 2020
Revised 21 April 2020
Accepted 14 May 2020
Published Online 27 August 2020

Abstract

In this paper, the probability that two elements of a finite ring have product zero is considered. The bounds of this probability are found for an arbitrary finite commutative ring with identity 1. An explicit formula for this probability in the case of Z_n, the ring of integers modulo n, is obtained.

***Keywords*:** Zero-divisor, zero-divisor graph, probability.

INTRODUCTION

In a previous research, the problem of finding the probability that two elements of a finite group G commute, $P(G)$ was considered by Gustafson [1], where he showed that $P(G) \le 5/8$. For more studies about probability and group theory, see [2, 3]. Beck in [4] introduced the notion of zero-divisor graphs of a commutative ring. The zero-divisor graph is a graph with non-zero zero-divisors vertices, in which two vertices are adjacent if their product is zero. Zero-divisor graph of a commutative ring has been studied by many authors, see [6, 5, 7]. The idea of the study of zero-divisor graph of rings helps to study the probability that two elements of a finite ring R have product zero in which for both cases depend on the products of elements of a ring which results in zero.

In this paper, the probability that two elements chosen at random (with replacement) from a ring R have product zero which is $P(R) = \frac{|Ann|}{|R \times R|}$, where $Ann = \{(x,y) \in R \times R \mid xy = 0\}$ is considered. This idea has been considered in [8] where the authors found the structures of rings R having maximum or minimum value of $P(R)$ among all rings with identity of the same size. Also, they found $P(R)$ for the case of R is a PIR local ring.

For each $x \in R$, the number of elements of Ann of the form (x,y) is $|Ann(x)|$, where $Ann(x)$ is the annihilator of x in R. Hence $|Ann| = \sum_{x \in R} |Ann(x)|$, where the sum is taken over all $x \in R$. Note that if $xy = 0$, then both (x,y) and (y,x) are elements of Ann.

Throughout this paper, all rings are assumed to be finite and commutative with identity 1 to establish lower and upper bounds of $P(R)$. Furthermore, the identity element 1 is assumed different from 0, as the zero ring is a finite commutative ring with identity (namely 0 since $0 \cdot 0 = 0$) and the corresponding probability that two elements multiply to 0 is 1. Also in the case where a ring R does not have an identity element, the probability that two elements multiply to 0 can be 1, for instance, if R is a ring such that $ab = 0$ for all $a, b \in R$, then $P(R) = 1$. These two cases are exempted throughout this paper in order to investigate the minimum and maximum values of $P(R)$.

Bounds for P(R)

In this section, the general lower and upper bounds for $P(R)$ will be determined.

Theorem 2.1 Suppose $|R| = n$. Then

$P(R) \ge \frac{2n + |Z(R)| - 1}{n^2}$, where $Z(R)$ is the set of non-zero zero-divisors of R.

Proof. It is clear that $|Ann(0)| = n$. Suppose $Z(R)$ be the set of non-zero zero-divisors of R. For every $x \in Z(R)$ we have that $|Ann(x)| \ge 2$, and $|Ann(x)| = 1$ for each $0 \ne x \notin Z(R)$. Thus,

$$|Ann| = |Ann(0)| + \sum_{x \in Z(R)} |Ann(x)| + \sum_{0 \ne x \notin Z(R)} |Ann(x)|$$

$$\geq n+2\cdot|Z(R)|+(n-1-|Z(R)|)\cdot 1 = 2n+|Z(R)|-1.$$

Therefore, $P(R)=\frac{|Ann|}{n^2}\geq\frac{2n+|Z(R)|-1}{n^2}$.

Theorem 2.2 Suppose $|R|=n$. Then

$P(R)\leq\frac{2n+(m-1)|Z(R)|-1}{n^2}$, where $Z(R)$ is the set of non-zero zero-divisors of R, and $m=\max\{|Ann(x)|:x\in Z(R)\}$.

Proof. Suppose $|R|=n$. Again, $|Ann(0)|=n$, and let the number of non-zero zero-divisors of R be k, that is, $k:=|Z(R)|$. Suppose that $m:=\max\{|Ann(x)|:x\in Z(R)\}$. Note that k and m vary as n varies. Thus,

$$|Ann|=|Ann(0)|+\sum_{x\in Z(R)}|Ann(x)|+\sum_{0\neq x\notin Z(R)}|Ann(x)|$$

$$\leq n+m\cdot k+(n-1-k)\cdot 1=2n+(m-1)k-1.$$

So, $P(R)\leq\frac{2n+(m-1)k-1}{n^2}$.

Corollary 2.3 If R is a finite ring with $|R|=n$, then

$P(R)\leq\frac{3}{4}$.

Proof. Since $Ann(x)$ is an ideal of R for any $x\in R$, it must be the case that $m=\max\{|Ann(x)|:x\in Z(R)\}\leq\frac{1}{2}n$ and, in general, $k=|Z(R)|\leq n-2$, for then, by Theorem 2.2, $P(R)\leq\frac{2n+(\frac{1}{2}n-1)(n-2)-1}{n^2}=\frac{1}{2}+\frac{1}{n^2}$ which is decreasing as n increases. If $n=2$, then $P(R)\leq\frac{3}{4}$.

From Theorem 2.1 and Theorem 2.2, the following corollaries can be deduced.

Corollary 2.4 If R is an integral domain and $|R|=n$, then

$P(R)=\frac{2n-1}{n^2}$.

Proof. Since R is an integral domain, then $|Z(R)|=0$. Thus, $\frac{2n-1}{n^2}\leq P(R)\leq\frac{2n-1}{n^2}$. The result follows.

For the non-integral domain case, if all annihilators have size m, then the inequalities of Theorem 2.1 and Theorem 2.2 lead to the following.

Corollary 2.5 If R is a non-integral domain, $|R|=n$ and $|Ann(x)|=m$ for all $x\in Z(R)$, then $P(R)=\frac{2n+(m-1)k-1}{n^2}$.

Next, the following theorem of computing the probability of direct product of rings is needed for the following section.

Theorem 2.6 Let $R=R_1\times R_2$, where R_1 and R_2 are rings. Then $P(R)=P(R_1)P(R_2)$.

Proof. Recall that $P(R)=\frac{|Ann|}{|R\times R|}$, where

$Ann=\{((r_1,s_1),(r_2,s_2))\in R\times R\,|\,(r_1r_2,s_1s_2)=(0,0)\}$.

Rewrite Ann in terms of $Ann(R_1)$ and $Ann(R_2)$, where

$Ann(R_1):=\{(r_1,r_2)\in R_1\times R_1\,|\,r_1r_2=0\}$ and

$Ann(R_2):=\{(s_1,s_2)\in R_2\times R_2\,|\,s_1s_2=0\}$, as follows:

$$Ann=\{((r_1,s_1),(r_2,s_2))\in R\times R\,|\,(r_1r_2,s_1s_2)=(0,0)\}=$$
$$\{(r_1,r_2)\in R_1\times R_1\,|\,r_1r_2=0\}\times$$
$$\{(s_1,s_2)\in R_2\times R_2\,|\,s_1s_2=0\}=Ann(R_1)\times Ann(R_2)$$

Thus,

$$P(R)=\frac{|Ann|}{|R\times R|}=\frac{|Ann(R_1)||Ann(R_2)|}{|R_1\times R_1||R_2\times R_2|}=P(R_1)P(R_2).$$

The probability that two elements of Z_n have product zero

In this section $P(Z_n)$ will be found, where Z_n is the ring of integers modulo n. It is well known that if $n=p_1^{k_1}\cdot p_2^{k_2}\cdots p_r^{k_r}$, then $Z_n\cong Z_{p_1^{k_1}}\times Z_{p_2^{k_2}}\times\cdots\times Z_{p_r^{k_r}}$. By Theorem 2.6, and by finding $P(Z_{p^k})$, for some positive integer k, the following holds.

Theorem 3.1 $P(Z_{p^k})=\frac{(k+1)p-k}{p^{k+1}}$, where p is a prime and $k\geq 1$.

Proof. It is clear that the set of nonzero zero divisors of Z_{p^k} is $S:=\{p,\ 2p,\ 3p,\ \cdots,\ (p^{k-1}-1)p\}$ with size $p^{k-1}-1$.

Rewrite the set S as the union of $k-1$ disjoint sets S_i, $i=1,2,\cdots,k-1$, that is, $S=\bigcup_{i=1}^{k-1}S_i$, such that S_i contains mp^i, $m\neq lp$, the multiple of p, and $m=1,2,\cdots,p^{k-i}-1$.

Thus, the size of each S_i is

$(p^{k-i}-1)-(p^{k-(i+1)}-1)=p^{k-i}-p^{k-(i+1)}$. One can see that the product of any element of S_i with every element of $\bigcup_{j=1}^{i} S_{k-j}$ is zero. So, the annihilator of each element of S_i has size p^i. Hence

$$|\mathrm{Ann}|=|\mathrm{Ann}(0)|+\sum_{x\in S}|\mathrm{Ann}(x)|+\sum_{0\neq x\notin S}|\mathrm{Ann}(x)|=$$
$$p^k+\sum_{i=1}^{k-1}p^i(p^{k-i}-p^{k-(i+1)})+(p^k-1-(p^{k-1}-1))=$$
$$p^k+\sum_{i=1}^{k-1}(p^k-p^{k-1})+(p^k-p^{k-1})=(k+1)p^k-kp^{k-1}.$$

Therefore,

$$P(Z_{p^k})=\frac{|\mathrm{Ann}|}{(p^k)^2}=\frac{p^{k-1}((k+1)p-k)}{p^{2k}}=\frac{(k+1)p-k}{p^{k+1}}.$$

Corollary 3.2 If $n=p_1^{k_1}\cdot p_2^{k_2}\cdots p_r^{k_r}$, then

$$P(Z_n)=\prod_{i=1}^{r}\frac{(k_i+1)p_i-k_i}{p_i^{k_i+1}}.$$

Proof. It is well known that if $n=p_1^{k_1}\cdot p_2^{k_2}\cdots p_r^{k_r}$, then $Z_n\cong Z_{p_1^{k_1}}\times Z_{p_2^{k_2}}\times\cdots\times Z_{p_r^{k_r}}$. By Theorem 2.6, $P(Z_n)=\prod_{i=1}^{r}P(Z_{p_i^{k_i}})$. From Theorem 3.1, the result follows.

CONCLUSION

In this paper, the probability $P(R)$ of two elements of a finite ring R have product zero has been introduced. The bounds of $P(R)$ have been found. Also, the general formula of $P(R)$ has been found in the case when R is the ring of integers modulo n.

ACKNOWLEDGEMENT

The authors would like to thank the referee for his/her valuable comments.

REFERENCES

[1] Gustafson, W. H. 1973. What is the probability that two group elements commute? *The American Mathematical Monthly*. 80, 1031–1034.
[2] Rusin, D. 1979. What is the probability that two elements of a finite group commute? *Pacific Journal of Mathematics*. 82, 237–247.
[3] Lescot, P., de, D. 1988. Commutativité et structure d'un groupe fini (2). *Rev. Math. Spéciales*. 8, 276–279.
[4] Beck, I. 1988. Coloring of commutative rings. *Journal of Algebra*. 116(1), 208–226.
[5] Anderson, D. F., Livingston, P. S. 1999. The zero-divisor graph of a commutative ring. *Lecture Notes in Pure and Appl. Math.* 217(2), 434–447.
[6] Anderson, D. F., Levy, R. and Shapiro, J. 2003. Zero-divisor graphs, von Neumann regular rings, and Boolean algebras. *Journal of Pure and Applied Algebra*. 180(3), 221–241.
[7] Livingston, P. S. 1997. Structure in zero-divisor graphs of commutative rings. Master's Thesis, University of Tennessee.
[8] Esmkhani, M. A., Jafarian Amiri, S. M. 2018. The probability that the multiplication of two ring elements is zero. *Journal of Algebra and Its Applications*. 17(3), 1850054(9 pages).