Miskolc Mathematical Notes
Vol. 20 (2019), No. 1, pp. 225–232
HU e-ISSN 1787-2413
DOI: 10.18514/MMN.2019.2274

ON RELATIVE COMMUTING PROBABILITY OF FINITE RINGS

PARAMA DUTTA AND RAJAT KANTI NATH

Received 11 March, 2017

Abstract. In this paper we study the probability that the commutator of a randomly chosen pair of elements, one from a subring of a finite ring and other from the ring itself is equal to a given element of the ring.

2010 *Mathematics Subject Classification:* 16U70; 16U80.

Keywords: finite ring, commuting probability, $\mathbb{Z}$-isoclinism of rings

1. INTRODUCTION

Let S be a subring of a finite ring R. The relative commuting probability of S in R denoted by $\Pr(S,R)$ is the probability that a randomly chosen pair of elements one from S and the other from R commute. That is

$$\Pr(S,R) = \frac{|\{(x,y) \in S \times R : xy = yx\}|}{|S||R|}.$$

This ratio $\Pr(S,R)$ can also be viewed as the probability that the commutator of a randomly chosen pair of elements, one from the subring S and the other from R, equals the zero of R. We write $[x,y]$ to denote the commutator $xy - yx$ of $x, y \in R$. The study of $\Pr(S,R)$ was initiated in [2]. Note that $\Pr(R,R)$, also denoted by $\Pr(R)$, is the probability that a randomly chosen pair of elements of R commute. The ratio $\Pr(R)$ is called the commuting probability of R and it was introduced by MacHale [6] in the year 1976. It is worth mentioning that the commuting probability of algebraic structures was originated from the works of Erdös and Turán [4] in the year 1968.

In this paper we consider the probability that the commutator of a randomly chosen pair of elements, one from the subring S and the other from R, equals a given element r of R. We write $\Pr_r(S,R)$ to denote this probability. Therefore

$$\Pr_r(S,R) = \frac{|\{(x,y) \in S \times R : [x,y] = r\}|}{|S||R|}. \tag{1.1}$$

Clearly $\Pr_r(S,R) = 0$ if and only if $r \notin K(S,R) := \{[x,y] : x \in S, y \in R\}$. Therefore we consider r to be an element of $K(S,R)$ throughout the paper. Also $\Pr_0(S,R) = \Pr(S,R)$ where 0 is the zero of R. It may be mentioned here that the case when

$S = R$ is already considered in [3] by the authors. Interchanging S and R one may define $\Pr_r(R, S)$ for $r \in R$.

The aim of this paper is to obtain some computing formulas and bounds for $\Pr_r(S, R)$. We also discuss an invariance property of $\Pr_r(S, R)$ under $\mathbb{Z}$-isoclinism. The motivation of this paper lies in [7] where analogous generalization of commuting probability of finite group is studied.

We write $[S, R]$ and $[x, R]$ for $x \in S$ to denote the additive subgroups of $(R, +)$ generated by the sets $K(S, R)$ and $\{[x, y] : y \in R\}$ respectively. Note that $[x, R] = \{[x, y] : y \in R\}$. Let $Z(S, R) := \{x \in S : xy = yx \,\forall\, y \in R\}$. Then $Z(R) := Z(R, R)$ is the center of R. Further, if $r \in R$ then the set $C_S(r) := \{x \in S : xr = rx\}$ is a subring of S and $\underset{r\in R}{\cap} C_S(r) = Z(S, R)$. We write $\frac{R}{S}$ and $|R : S|$ to denote the additive quotient group and the index of S in R respectively.

2. Computing formula for $\Pr_r(S, R)$

In this section, we derive some computing formulas for $\Pr_r(S, R)$. We begin with the following useful lemmas.

Lemma 1 (Lemma 2.1 in [3])**.** *Let R be a finite ring. Then*

$$|[x, R]| = |R : C_R(x)| \text{ for all } x \in R.$$

Lemma 2. *Let S be a subring of a finite ring R and $T_{x,r}(S, R) = \{y \in R : [x, y] = r\}$ for $x \in S$ and $r \in R$. Then we have the followings*

(1) *$T_{x,r}(S, R) \neq \phi$ if and only if $r \in [x, R]$.*
(2) *If $T_{x,r}(S, R) \neq \phi$ then $T_{x,r}(S, R) = t + C_R(x)$ for some $t \in T_{x,r}(S, R)$.*

Proof. Part (1) follows from the fact that $y \in T_{s,r}(S, R)$ if and only if $r \in [s, R]$. Let $t \in T_{x,r}(S, R)$ and $p \in t + C_R(x)$. Then $[x, p] = r$ and so $p \in T_{x,r}(S, R)$. Therefore, $t + C_R(x) \subseteq T_{x,r}(S, R)$. Again, if $y \in T_{x,r}(S, R)$ then $(y - t) \in C_R(x)$ and so $y \in t + C_R(x)$. Therefore, $T_{x,r}(S, R) \subseteq t + C_R(x)$. Hence part (2) follows. □

Now we state and prove the following main result of this section.

Theorem 1. *Let S be a subring of a finite ring R. Then*

$$\Pr_r(S, R) = \frac{1}{|S||R|} \sum_{\substack{x\in S \\ r\in[x,R]}} |C_R(x)| = \frac{1}{|S|} \sum_{\substack{x\in S \\ r\in[x,R]}} \frac{1}{|[x, R]|}.$$

Proof. Note that $\{(x, y) \in S \times R : [x, y] = r\} = \underset{x\in S}{\cup} (\{x\} \times T_{x,r}(S, R))$. Therefore, by (1.1) and Lemma 2, we have

$$|S||R|\Pr_r(S, R) = \sum_{x\in S} |T_{x,r}(S, R)| = \sum_{\substack{x\in S \\ r\in[x,R]}} |C_R(x)|. \tag{2.1}$$

The second part follows from (2.1) and Lemma 1. □

Proposition 1. *Let S be a subring of a finite ring R and $r \in R$. Then* $\Pr_r(S,R) = \Pr_{-r}(R,S)$. *However, if* $2r = 0$ *then* $\Pr_r(S,R) = \Pr_r(R,S)$.

Proof. Let $X = \{(x,y) \in S \times R : [x,y] = r\}$ and $Y = \{(y,x) \in R \times S : [y,x] = -r\}$. It is easy to see that $(x,y) \mapsto (y,x)$ defines a bijective mapping from X to Y. Therefore, $|X| = |Y|$ and the result follows from (1.1).

Second part follows from the fact that $r = -r$ if $2r = 0$. □

Proposition 2. *Let S_1 and S_2 be two subrings of the finite rings R_1 and R_2 respectively. If $(r_1,r_2) \in R_1 \times R_2$ then*

$$\Pr_{(r_1,r_2)}(S_1 \times S_2, R_1 \times R_2) = \Pr_{r_1}(S_1,R_1)\Pr_{r_2}(S_2,R_2).$$

Proof. Let $X_i = \{(x_i,y_i) \in S_i \times R_i : [x_i,y_i] = r_i\}$ for $i = 1,2$ and

$$Y = \{((x_1,x_2),(y_1,y_2)) \in (S_1 \times S_2) \times (R_1 \times R_2) : [(x_1,x_2),(y_1,y_2)] = (r_1,r_2)\}.$$

Then $((x_1,y_1),(x_2,y_2)) \mapsto ((x_1,x_2),(y_1,y_2))$ defines a bijective map from $X_1 \times X_2$ to Y. Therefore, $|Y| = |X_1||X_2|$ and hence the result follows from (1.1). □

Using Proposition 1 in Theorem 1, we get the following corollary.

Corollary 1. *Let S be a subring of a finite ring R. Then*

$$\Pr(R,S) = \Pr(S,R) = \frac{1}{|S||R|}\sum_{x \in S}|C_R(x)| = \frac{1}{|S|}\sum_{x \in S}\frac{1}{|[x,R]|}.$$

We conclude this section with the following corollary.

Corollary 2. *Let S be a subring of a finite non-commutative ring R. If* $|[S,R]| = p$*, a prime, then*

$$\Pr_r(S,R) = \begin{cases} \frac{1}{p}\left(1 + \frac{p-1}{|S:Z(S,R)|}\right), & \text{if } r = 0 \\ \frac{1}{p}\left(1 - \frac{1}{|S:Z(S,R)|}\right), & \text{if } r \neq 0. \end{cases}$$

Proof. For $x \in S \setminus Z(S,R)$, we have $\{0\} \subsetneq [x,R] \subseteq [S,R]$. Since $|[S,R]| = p$, it follows that $[S,R] = [x,R]$ and hence $|[x,R]| = p$ for all $x \in S \setminus Z(S,R)$.

If $r = 0$ then by Corollary 1, we have

$$\begin{aligned}\Pr_r(S,R) &= \frac{1}{|S|}\left(|Z(S,R)| + \sum_{x \in S \setminus Z(S,R)}\frac{1}{|[x,R]|}\right) \\ &= \frac{1}{|S|}\left(|Z(S,R)| + \frac{1}{p}(|S| - |Z(S,R)|)\right) \\ &= \frac{1}{p}\left(1 + \frac{p-1}{|S:Z(S,R)|}\right).\end{aligned}$$

If $r \neq 0$ then $r \notin [x, R]$ for all $x \in Z(S, R)$ and $r \in [x, R]$ for all $x \in S \setminus Z(S, R)$. Therefore, by Theorem 1, we have

$$\begin{aligned}\Pr_r(S, R) &= \frac{1}{|S|} \sum_{x \in S \setminus Z(S,R)} \frac{1}{|[x, R]|} = \frac{1}{|S|} \sum_{x \in S \setminus Z(S,R)} \frac{1}{p} \\ &= \frac{1}{p}\left(1 - \frac{1}{|S : Z(S, R)|}\right).\end{aligned}$$

Hence, the result follows. □

3. Bounds for $\Pr_r(S, R)$

If S is a subring of a finite ring R then it was shown in [2, Theorem 2.16] that

$$\Pr(S, R) \geq \frac{1}{|K(S, R)|}\left(1 + \frac{|K(S, R)| - 1}{|S : Z(S, R)|}\right). \tag{3.1}$$

Also, if p is the smallest prime dividing $|R|$ then by [2, Theorem 2.5] and [2, Corollary 2.6] we have

$$\Pr(S, R) \leq \frac{(p - 1)|Z(S, R)| + |S|}{p|S|} \text{ and } \Pr(R) \leq \frac{(p - 1)|Z(R)| + |R|}{p|R|}. \tag{3.2}$$

In this section, we obtain several bounds for $\Pr_r(S, R)$ and show that some of our bounds are better than the bounds given in (3.1) and (3.2). We begin with the following upper bound.

Proposition 3. *Let S be a subring of a finite ring R. If p is the smallest prime dividing $|R|$ and $r \neq 0$ then*

$$\Pr_r(S, R) \leq \frac{|S| - |Z(S, R)|}{p|S|} < \frac{1}{p}.$$

Proof. Since $r \neq 0$ we have $S \neq Z(S, R)$. If $x \in Z(S, R)$ then $r \notin [s, R]$. If $x \in S \setminus Z(S, R)$ then $C_R(x) \neq R$. Therefore, by Lemma 1, we have $|[x, R]| = |R : C_R(x)| > 1$. Since p is the smallest prime dividing $|R|$ we have $|[x, R]| \geq p$. Hence the result follows from Theorem 1. □

Proposition 4. *Let S be a subring of a finite ring R. Then $\Pr_r(S, R) \leq \Pr(S, R)$ with equality if and only if $r = 0$.*

Proof. By Theorem 1 and Corollary 1, we have

$$\Pr_r(S, R) = \frac{1}{|S||R|} \sum_{\substack{x \in S \\ r \in [x, R]}} |C_R(x)| \leq \frac{1}{|S||R|} \sum_{x \in S} |C_R(x)| = \Pr(S, R).$$

The equality holds if and only if $r = 0$. □

Proposition 5. *If $S_1 \subseteq S_2$ are two subrings of a finite ring R then*

$$\Pr_r(S_1, R) \leq |S_2 : S_1| \Pr_r(S_2, R).$$

Proof. By Theorem 1, we have

$$\begin{aligned}|S_1||R|\Pr_r(S_1, R) &= \sum_{\substack{x \in S_1 \\ r \in [x,R]}} |C_R(x)| \\ &\leq \sum_{\substack{x \in S_2 \\ r \in [x,R]}} |C_R(x)| = |S_2||R|\Pr_r(S_2, R).\end{aligned}$$

Hence the result follows. □

Note that equality holds in Proposition 5 if and only if $r \notin [x, R]$ for all $x \in S_2 \setminus S_1$. If $r = 0$ then the condition of equality reduces to $S_1 = S_2$. Putting $S_1 = S$ and $S_2 = R$ in Proposition 5 we have the following corollary.

Corollary 3. *If S is a subring of a finite ring R then*

$$\Pr_r(S, R) \leq |R : S| \Pr_r(R).$$

For any subring S of R, let $m_S = \min\{|[x, R]| : x \in S \setminus Z(S, R)\}$ and $M_S = \max\{|[x, R]| : x \in S \setminus Z(S, R)\}$. In the following theorem we give bounds for $\Pr(S, R)$ in terms of m_S and M_S.

Theorem 2. *Let S be a subring of a finite ring R. Then*

$$\frac{1}{M_S}\left(1 + \frac{M_S - 1}{|S : Z(S, R)|}\right) \leq \Pr(S, R) \leq \frac{1}{m_S}\left(1 + \frac{m_S - 1}{|S : Z(S, R)|}\right).$$

The equality holds if and only if $m_S = M_S = |[x, R]|$ for all $x \in S \setminus Z(S, R)$.

Proof. Since $m_S \leq |[x, R]|$ and $M_S \geq |[x, R]|$ for all $x \in S \setminus Z(S, R)$, we have

$$\frac{|S| - |Z(S, R)|}{M_S} \leq \sum_{x \in S \setminus Z(S,R)} \frac{1}{|[x, R]|} \leq \frac{|S| - |Z(S, R)|}{m_S}. \tag{3.3}$$

Again, by Corollary 1, we have

$$\Pr(S, R) = \frac{1}{|S|}\left(|Z(S, R)| + \sum_{x \in S \setminus Z(S,R)} \frac{1}{|[x, R]|}\right). \tag{3.4}$$

Hence, the result follows from (3.3) and (3.4). □

Note that for any two integers $m \geq n$, we have

$$\frac{1}{n}\left(1 + \frac{n - 1}{|S : Z(S, R)|}\right) \geq \frac{1}{m}\left(1 + \frac{m - 1}{|S : Z(S, R)|}\right). \tag{3.5}$$

Clearly equality holds in (3.5) if $Z(S,R) = S$. Further, if $Z(S,R) \neq S$ then equality holds if and only if $m = n$. Since $|K(S,R)| \geq M_S$, by (3.5), it follows that

$$\frac{1}{M_S}\left(1 + \frac{M_S - 1}{|S : Z(S,R)|}\right) \geq \frac{1}{|K(S,R)|}\left(1 + \frac{|K(S,R)| - 1}{|S : Z(S,R)|}\right).$$

Therefore, the lower bound obtained in Theorem 2 is better than the lower bound given in (3.1) for $\Pr(S,R)$. Again, if p is the smallest prime divisor of $|R|$ then $p \leq m_S$ and hence, by (3.5), we have

$$\frac{1}{m_S}\left(1 + \frac{m_S - 1}{|S : Z(S,R)|}\right) \leq \frac{(p-1)|Z(S,R)| + |S|}{p|S|}.$$

This shows that the upper bound obtained in Theorem 2 is better than the upper bound given in (3.2) for $\Pr(S,R)$.

Putting $S = R$ in Theorem 2 we have the following corollary.

Corollary 4. *Let R be a finite ring. Then*

$$\frac{1}{M_R}\left(1 + \frac{M_R - 1}{|R : Z(R)|}\right) \leq \Pr(R) \leq \frac{1}{m_R}\left(1 + \frac{m_R - 1}{|R : Z(R)|}\right).$$

The equality holds if and only if $m_R = M_R = |[x,R]|$ for all $x \in R \setminus Z(R)$.

We conclude this section noting that the lower bound obtained in Corollary 4 is better than the lower bound obtained in [2, Corollary 2.18]. Also, if p is the smallest prime divisor of $|R|$ then the upper bound obtained in Corollary 4 is better than the upper bound given in (3.2) for $\Pr(R)$.

4. $\mathbb{Z}$-ISOCLINISM AND $\Pr_r(S,R)$

The idea of isoclinism of groups was introduced by Hall [5] in 1940. Years after in 2013, Buckley et al. [1] introduced $\mathbb{Z}$-isoclinism of rings. Recently, Dutta et al. [2] have introduced $\mathbb{Z}$-isoclinism between two pairs of rings, generalizing the notion of $\mathbb{Z}$-isoclinism of rings. Let S_1 and S_2 be two subrings of the rings R_1 and R_2 respectively. Recall that a pair of mappings (α,β) is called a $\mathbb{Z}$-isoclinism between (S_1,R_1) and (S_2,R_2) if $\alpha : \frac{R_1}{Z(S_1,R_1)} \to \frac{R_2}{Z(S_2,R_2)}$ and $\beta : [S_1,R_1] \to [S_2,R_2]$ are additive group isomorphisms such that $\alpha\left(\frac{S_1}{Z(S_1,R_1)}\right) = \frac{S_2}{Z(S_2,R_2)}$ and $\beta([x_1,y_1]) = [x_2,y_2]$ whenever $x_i \in S_i$, $y_i \in R_i$ for $i = 1,2$; $\alpha(x_1 + Z(S_1,R_1)) = x_2 + Z(S_2,R_2)$ and $\alpha(y_1 + Z(S_1,R_1)) = y_2 + Z(S_2,R_2)$. Two pairs of rings are said to be $\mathbb{Z}$-isoclinic if there exists a $\mathbb{Z}$-isoclinism between them.

In [2, Theorem 3.3], Dutta et al. proved that $\Pr(S_1,R_1) = \Pr(S_2,R_2)$ if the rings R_1 and R_2 are finite and the pairs (S_1,R_1) and (S_2,R_2) are $\mathbb{Z}$-isoclinic. We conclude this paper with the following generalization of [2, Theorem 3.3].

Theorem 3. *Let S_1 and S_2 be two subrings of the finite rings R_1 and R_2 respectively. If (α, β) is a $\mathbb{Z}$-isoclinism between (S_1, R_1) and (S_2, R_2) then*

$$\mathrm{Pr}_r(S_1, R_1) = \mathrm{Pr}_{\beta(r)}(S_2, R_2).$$

Proof. By Theorem 1, we have

$$\mathrm{Pr}_r(S_1, R_1) = \frac{|Z(S_1, R_1)|}{|S_1||R_1|} \sum_{\substack{x_1 + Z(S_1,R_1) \in \frac{S_1}{Z(S_1,R_1)} \\ r \in [x_1, R_1]}} |C_{R_1}(x_1)|$$

noting that $r \in [x_1, R_1]$ if and only if $r \in [x_1 + z, R_1]$ and $C_{R_1}(x_1) = C_{R_1}(x_1 + z)$ for all $z \in Z(S_1, R_1)$. Now, by Lemma 1, we have

$$\mathrm{Pr}_r(S_1, R_1) = \frac{|Z(S_1, R_1)|}{|S_1|} \sum_{\substack{x_1 + Z(S_1,R_1) \in \frac{S_1}{Z(S_1,R_1)} \\ r \in [x_1, R_1]}} \frac{1}{|[x_1, R_1]|}. \tag{4.1}$$

Similarly, it can be seen that

$$\mathrm{Pr}_{\beta(r)}(S_2, R_2) = \frac{|Z(S_2, R_2)|}{|S_2|} \sum_{\substack{x_2 + Z(S_2,R_2) \in \frac{S_2}{Z(S_2,R_2)} \\ \beta(r) \in [x_2, R_2]}} \frac{1}{|[x_2, R_2]|}. \tag{4.2}$$

Since (α, β) is a $\mathbb{Z}$-isoclinism between (S_1, R_1) and (S_2, R_2) we have $\frac{|S_1|}{|Z(S_1,R_1)|} = \frac{|S_2|}{|Z(S_2,R_2)|}$, $|[x_1, R_1]| = |[x_2, R_2]|$ and $r \in [x_1, R_1]$ if and only if $\beta(r) \in [x_2, R_2]$. Hence, the result follows from (4.1) and (4.2). □

ACKNOWLEDGEMENT

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

REFERENCES

[1] S. M. Buckley, D. MacHale, and A. Ní Shé, "Finite rings with many commuting pairs of elements." *Preprint*.

[2] J. Dutta, D. K. Basnet, and R. K. Nath, "On commuting probability of finite rings." *Indag. Math.*, vol. 28, no. 2, pp. 372–382, 2017, doi: 10.1016/j.indag.2016.10.002.

[3] P. Dutta and R. K. Nath, "On r-commuting probability of finite rings." *Preprint*.

[4] P. Erdös and P. Turán, "On some problems of a statistical group-theory. IV." *Acta. Math. Acad. Sci. Hungar.*, vol. 19, pp. 413–435, 1968, doi: 10.1007/BF01894517.

[5] P. Hall, "The classification of prime power groups." *J. Reine Angew. Math.*, vol. 182, pp. 130–141, 1940, doi: 10.1515/crll.1940.182.130.

[6] D. MacHale, "Commutativity in Finite Rings." *Amer. Math. Monthly*, vol. 83, pp. 30–32, 1976, doi: 10.1080/00029890.1976.11994032.

[7] R. K. Nath and M. K. Yadav, “Some results on relative commutativity degree.” *Rend. Circ. Mat. Palermo*, vol. 64, no. 2, pp. 229–239, 2015, doi: 10.1007/s12215-015-0194-x.

Authors' addresses

Parama Dutta
Tezpur University, Department of Mathematical Sciences, Napaam-784028, Sonitpur, Assam, India.
E-mail address: parama@gonitsora.com

Rajat Kanti Nath
Tezpur University, Department of Mathematical Sciences, Napaam-784028, Sonitpur, Assam, India.
E-mail address: rajatkantinath@yahoo.com