CORA Cork Open Research Archive
Cartlann Taighde Oscailte Chorcaí

Title	Commuting probability for subrings and quotient rings
Authors	Buckley, Stephen M.;MacHale, Desmond
Publication date	2016-02-25
Original Citation	Buckley, S. M. and MacHale, D. (2016) 'Commuting probability for subrings and quotient rings', Journal of Algebra Combinatorics Discrete Structures and Applications, 4(2), pp. 189-196. doi:10.13069/jacodesmath.284962
Type of publication	Article (peer-reviewed)
Link to publisher's version	http://jacodesmath.com/index.php/jacodesmath/index - 10.13069/jacodesmath.284962
Rights	© 2016, the Authors. Journal of Algebra Combinatorics Discrete Structures and Applications is licensed under a Creative Commons Attribution 4.0 International License. - https://creativecommons.org/licenses/by/4.0/
Download date	2026-11-04 10:16:32
Item downloaded from	https://hdl.handle.net/10468/3730


UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

J. Algebra Comb. Discrete Appl.
4(2) • 189–196

Received: 12 June 2015
Accepted: 25 February 2016

Journal of Algebra Combinatorics Discrete Structures and Applications

Commuting probability for subrings and quotient rings

Research Article

Stephen M. Buckley, Desmond MacHale

Abstract: We prove that the commuting probability of a finite ring is no larger than the commuting probabilities of its subrings and quotients, and characterize when equality occurs in such a comparison.

2010 MSC: 05E15

Keywords: Commuting probability, Subring, Quotient ring

1. Introduction

Suppose R is a finite (possibly nonunital) ring. The *commuting probability of* R is

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

where $|\cdot|$ denotes cardinality.

There has been much written on the commuting probability of a finite group: see for instance [5], [7], [8], [10], [4], and [6]. The commuting probability of a ring has been discussed in [9], [3], [2], and [1].

Work on the commuting probability of rings R has so far mainly concentrated on the possible values of $\Pr(R)$. However, it was shown in [9] that $\Pr(R)$ is no larger than $\Pr(S)$ whenever S is a subring of R. Our first result gives a new proof of this result, one that allows us to characterize when equality occurs.

Theorem 1.1. *Suppose S is a subring of a finite ring R. Then $\Pr(R) \leq \Pr(S)$. Equality holds if and only if $[x,S] = [x,R]$ for all $x \in R$.*

Our second result is similar, but involves a comparison with quotient rings.

Stephen M. Buckley (Corresponding Author); Department of Mathematics and Statistics, Maynooth University, Maynooth, Co. Kildare, Ireland (email: stephen.buckley@maths.nuim.ie).
Desmond MacHale; School of Mathematical Sciences, University College Cork, Cork, Ireland (email: d.machale@ucc.ie).

Proposition 1.2. *Suppose I is an ideal in a finite ring R. Then $\Pr(R) \leq \Pr(R/I)$. Equality holds if and only if $[x, R] \cap I = \{0\}$ for all $x \in R$.*

In the above results, $[x, S] = \{[x, s] : s \in S\}$, and $[x, s] = xs - sx$ is the *commutator of x and s*.

After some preliminaries in Section 2, we prove generalizations of the above results in Section 3. In Section 4, we give various counterexamples which rule out seemingly plausible variants of the above conditions for equality.

2. Preliminaries

Given a set S of finite cardinality, and a function $f : S \to \mathbb{R}$, we write $|S|$ for the cardinality of S, and define the arithmetic mean

$$\sum_{x \in S} f(x) = \frac{1}{|S|} \sum_{x \in S} f(x) .$$

In this paper, a *ring* is not necessarily unital. Our results do not use associativity either and, to emphasize this, we sometimes talk of *PN rings* (where "PN" stands for "possibly nonassociative"). In the absence of the "PN" qualifier, rings and algebras are assumed to be associative. However, an ideal in a PN ring is not assumed to be associative.

Suppose R is a PN ring and $x \in R$. The *annihilator* $\mathrm{Ann}(R)$, *center* $\mathrm{Z}(R)$, and *centralizer* $C_R(x)$ are defined by

$$\begin{aligned} \mathrm{Ann}(R) &:= \{u \in R \,:\, uv = vu = 0 \text{ for all } v \in R\} , \\ \mathrm{Z}(R) &:= \{u \in R \,:\, [u, v] = 0 \text{ for all } v \in R\} , \\ C_R(x) &:= \{u \in R \,:\, [u, x] = 0\} . \end{aligned}$$

If A and B are finite subsets of a PN ring R, then we define the *commuting probability for the triple* $(A, B; R)$ to be

$$\Pr_R(A, B) := \frac{|\{(x, y) \in A \times B \,:\, xy = yx\}|}{|A| \cdot |B|} ,$$

where juxtaposition indicates multiplication in R. We also write $\Pr_R(A) := \Pr_R(A, A)$ and $\Pr(R) := \Pr_R(R)$.

If x, y are elements of a PN ring R, and S is an additive subgroup of R, then we define the commutator $[x, y] := xy - yx$, and we write $[x, S] := \{[x, s] : s \in S\}$. Note that $[x, S]$ is always an additive subgroup of R. If T is another additive subgroup of R, we define $[S, T]$ to be the additive subgroup of R given by the set of finite sums of commutators $[s, t]$, $s \in S$, $t \in T$. $A + B$ denotes the additive subgroup $\{a + b \,:\, a \in A,\ b \in B\}$ whenever A, B are additive subgroups of a PN ring R, and $\operatorname{span} S$ is the subspace of finite linear combinations of elements of a subset S of an algebra R.

If a PN ring R is the direct sum of PN rings R_1 and R_2, it follows easily that $\Pr(R) = \Pr(R_1) \Pr(R_2)$.

3. Proofs

Theorem 1.1 follows immediately from the following more general result.

Theorem 3.1. *Suppose a PN ring R has finite additive subgroups A_1, A_2, B_1, B_2 satisfying $A_1 \subseteq A_2$ and $B_1 \subseteq B_2$. Then $\Pr_R(A_2, B_2) \leq \Pr_R(A_1, B_1)$. Furthermore, the following conditions are equivalent:*

(AB1) $\Pr_R(A_1, B_1) = \Pr_R(A_2, B_2)$.

(AB2) $[x, A_1] = [x, A_2]$ *and* $[y, B_1] = [y, B_2]$, *for all* $x \in B_1$, $y \in A_2$.

(AB3) $[x, A_1] = [x, A_2]$ *and* $[y, B_1] = [y, B_2]$, *for all* $x \in B_2$, $y \in A_2$.

Proof. Note that for any finite subsets A, B of R, we have

$$\Pr_R(A, B) = \sum_{x \in B} \sum_{y \in A} f(y, x)\,,$$

where $f : R \times R \to \{0, 1\}$ is the function defined by $f(y, x) = 1$ if $xy = yx$, and $f(x, y) = 0$ otherwise.

We first prove the result in the special case $B_1 = B_2$. For each $x \in B_2$, define a surjective homomorphism of additive groups, $\phi_x : A_2 \to [x, A_2]$, by

$$\phi_x(y) = [x, y]\,, \qquad y \in A_2\,.$$

For $x \in B_2$, $y \in A_2$, and f as in the previous paragraph, we have $f(x, y) = 1$ if and only if $y \in \ker \phi_x$. By the first isomorphism theorem, it follows that

$$\sum_{y \in A_2} f(y, x) = \frac{|\ker \phi_x|}{|A_2|} = \frac{1}{|[x, A_2]|}\,.$$

and so

$$\Pr_R(A_2, B_2) = \sum_{x \in B_2} \frac{1}{|[x, A_2]|}\,.$$

By the same argument, we have

$$\Pr_R(A_1, B_2) = \sum_{x \in B_2} \frac{1}{|[x, A_1]|}\,.$$

It follows readily that $\Pr_R(A_2, B_2) \le \Pr_R(A_1, B_2)$, with equality if and only if $[x, A_1] = [x, A_2]$ for all $x \in B_2$. This proves the equivalence of (AB1)–(AB3) in the special case $B_1 = B_2$.

We wish to employ symmetry between the A- and B-subgroups. For this, we note that (AB2) can be written in a simpler form in our special case $B_1 = B_2$:

(AB2′) $[x, A_1] = [x, A_2]$, for all $x \in B_2$.

Moreover, let us say that (AB2′) has data $(A_1, A_2; B_2)$.

By symmetry, we can now handle the special case $A_1 = A_2$. In fact, we have $\Pr_R(A_2, B_2) \le \Pr_R(A_2, B_1)$, with equality if and only if $[y, B_1] = [y, B_2]$ for all $y \in A_2$, and we deduce the equivalence of (AB1)–(AB3) as before. For the special case $A_1 = A_2$, (AB2) can be written in the simpler form

(AB2″) $[y, B_1] = [y, B_2]$, for all $y \in A_2$.

Moreover, let us say that (AB2″) has data $(B_1, B_2; A_2)$.

We now consider the general case. By the two special cases considered above, we have

$$\Pr_R(A_2, B_2) \le \Pr_R(A_2, B_1) \le \Pr_R(A_1, B_1)\,, \tag{1}$$

as required. Moreover, $\Pr_R(A_1, B_1) = \Pr_R(A_2, B_2)$ if and only if both of inequalities in (1) are equalities, which is equivalent to the conjunction of (AB2′) with data $(A_1, A_2; B_1)$, and (AB2″) with data $(B_1, B_2; A_2)$. This conjunction is just the required general form of (AB2).

Thus, (AB1) is equivalent to (AB2). Because of the symmetry between the A- and B-subgroups in (AB1) that is lacking in (AB2), we get a version of (AB2) where the equations are instead true for all $y \in A_1$ and all $x \in B_2$. Putting this together with the original form of (AB2), we derive the formally stronger (AB3). Thus, all three conditions (AB1)–(AB3) are mutually equivalent. □

Next, we tackle Proposition 1.2. In fact we prove a slight generalization of it in the context of PN rings.

Proposition 3.2. *Suppose I is an ideal in a finite PN ring R. Then $\Pr(R) \leq \Pr(R/I)$, with equality if and only if $[x, R] \cap I = \{0\}$ for all $x \in R$.*

Proof. Take $x + I, y + I \in R/I$, where $x, y \in R$. Since $[x + I, y + I] = [x, y] + I$ is independent of the representatives x, y of these elements in R/I, it follows that

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

It is now clear that $\Pr(R) \leq \Pr(R/I)$. Furthermore, we have equality if and only if the condition $xy - yx \in I$ is equivalent to $xy = yx$ for all $x, y \in R$. This is equivalent to the desired condition. □

4. Counterexamples

Here we pose three questions and give a negative answer in each case. Together, these answers show that our results cannot be simplified or improved in any obvious way.

Question 4.1. *Can we improve Theorem 3.1 by dropping one equation from (AB2) or (AB3), or by significantly restricting the set of elements for which the equations hold, and still obtaining a condition equivalent to (AB1)?*

Question 4.2. *Can we strengthen the first conclusion of Theorem 3.1 by dropping one of the assumptions that A_i, B_i are additive subgroups of R?*

Question 4.3. *Can we strengthen the statement of either Theorem 3.1 or Proposition 1.2 by replacing the necessary and sufficient condition for equality of commuting probabilities by a simpler quantifier-free commutator subgroup property?*

We will see that the first two questions are easily answered, but that the third one is rather more interesting (although we will need to make clearer what we have in mind by this question separately for each of the two results to which it refers).

Our first proposition gives a negative answer to Question 4.1.

Proposition 4.4. *Neither of the following conditions are equivalent to conditions (AB1)–(AB3) in Theorem 3.1.*

(AB4) $[x, A_1] = [x, A_2]$ *and* $[y, B_1] = [y, B_2]$, *for all* $x \in B_1$, $y \in A_1$.

(AB5) $[x, A_1] = [x, A_2]$ *for all* $x \in B_2$.

Proof. We get counterexamples in an arbitrary finite noncommutative ring R. In (AB4), let $A_1 = B_1 = \mathrm{Z}(R)$ and $A_2 = B_2 = R$. Then $[x, A_1] = [x, A_2] = [y, B_1] = [y, B_2] = \{0\}$ for all $x \in B_1$, $y \in A_1$. However, $\Pr_R(A_1, B_1) = 1 > \Pr_R(A_2, B_2)$.

For (AB5), let $B_1 = \mathrm{Z}(R)$ and $A_1 = A_2 = B_2 = R$. Trivially, $[x, A_1] = [x, A_2]$ for all $x \in B_2$. However, $\Pr_R(A_1, B_1) = 1 > \Pr_R(A_2, B_2)$. □

The following proposition gives a negative answer to Question 4.2.

Proposition 4.5. *If we drop any one of the assumptions that A_i, B_i are additive subgroups of R in Theorem 3.1, then the main inequality $\Pr_R(A_2, B_2) \leq \Pr_R(A_1, B_1)$ may fail.*

Proof. By symmetry, it suffices to show that the inequality may fail if either B_1 or B_2 is not an additive subgroup. Below, p is any prime number.

Let R be the $\mathbb{Z}_p$-algebra with basis $\{u, v\}$, where $u^2 = vu = u$ and $v^2 = uv = v$. Let $B_2 = A_1 = A_2 = R$, and let $B_1 = \{u\}$. It is clear that $\Pr_R(A_1, B_1) = 1/p$, whereas it is well known and straightforward to verify (see [3, Theorem 5.1]) that

$$\Pr_R(A_2, B_2) = \Pr(R) = \frac{p^2 + p - 1}{p^3} > \frac{1}{p}.$$

Next, let S be the ring of order p^3 given by an internal direct sum of $\mathbb{Z}_p$ and the ring R of the previous paragraph. Let $A_1 = A_2 = B_1 = R$, and let B_2 be any subset of S such that $B_2 = R \cup \{z\}$ where $z \in Z(S) \setminus \{0\}$; note that $|Z(S) \setminus \{0\}| = p - 1$ and $Z(S) \setminus \{0\}$ does not intersect R. Then $\Pr_R(A_1, B_1) = \Pr(R) = (p^2 + p - 1)/p^3$ as before, but

$$\Pr_R(A_2, B_2) = \frac{(p^3 + p^2 - p) + p^2}{p^2(p^2 + 1)} = \frac{p^2 + 2p - 1}{p^3 + p} > \frac{p^2 + p - 1}{p^3}.$$

since $(p^2 + 2p - 1)/(p^3 + p)$ is a weighted mean of $\Pr(R)$ and 1. □

Remark 4.6. *The counterexamples in Proposition 4.5 do not immediately imply that the assumption that S is a subring in Theorem 1.1 is essential. However, this is easily shown. For instance, if R is any finite non-commutative ring and $S = \{a, b\}$, where $a, b \in R$ do not commute, then $\Pr(S) = 0 < \Pr(R)$.*

We next address Question 4.3 in relation to Theorem 3.1. Assume that the hypotheses of Theorem 3.1 are in effect and that (AB1)–(AB3) hold. Suppose $u \in [A_2, B_2]$. By definition, u is a finite sum of terms of the form $[y, x]$, $y \in A_2$, $x \in B_2$. By (AB2), we may assume that $x \in B_1$ for each such term, and so $[A_2, B_2] = [A_2, B_1]$. By symmetry, it is also true that $[A_2, B_2] = [A_1, B_2]$. If we restrict y to A_1 then, by essentially the same argument, it follows that $[A_1, B_1] = [A_1, B_2]$. Thus, (AB1)–(AB3) imply the following quantifier-free condition:

(AB6) $[A_1, B_1] = [A_1, B_2] = [A_2, B_1] = [A_2, B_2]$.

If (AB6) were equivalent to (AB1)–(AB3), then we could weaken the condition for equality in Theorem 1.1 to $[S, S] = [R, R]$. However, we will see that this is false. In fact, we can say more.

Let us consider the following four conditions for a subring S of a ring R.

(S1) $S + \mathrm{Z}(R) = R$.

(S2) $\Pr(R) = \Pr(S)$.

(S3) $[S, S] = [R, R]$.

(S4) $[R, S] = [R, R]$.

If (S1) holds, then R is a disjoint union of cosets of the form $z+S$, $z \in \mathrm{Z}(R)$. Since $[z_1+s_1, z_2+s_2] = [s_1, s_2]$ for $s_1, s_2 \in S$, $z_1, z_2 \in \mathrm{Z}(R)$, it follows readily that (S2) holds. Since (AB1) implies (AB6), it follows in particular that (S2) implies (S3), and trivially (S3) implies (S4).

The above implications cannot be reversed. First, it is easy to see that (S4) does not imply (S3): just take R to be a two-dimensional non-commutative $\mathbb{Z}_p$-algebra (as in the proof of Proposition 4.5), where p is a prime, and let S be a one-dimensional subalgebra. Then $[R, S] = [R, R]$ has order p, but $[S, S] = \{0\}$. The following pair of results show that the other two reverse implications also fail.

Proposition 4.7. *For each prime p, there exists a 5-dimensional $\mathbb{Z}_p$-algebra R with a subalgebra S of codimension 1 such that $[S, S] = [R, R]$ and $\Pr(R) < \Pr(S)$.*

Theorem 4.8. *There exists a 7-dimensional $\mathbb{Z}_2$-algebra R with a subalgebra S of codimension 1 such that $\Pr(S) = \Pr(R)$ and $S + \mathrm{Z}(R) \neq R$.*

In the proofs of the above pair of results and the proof of one subsequent result, R will in each case be a finite nilpotent $\mathbb{Z}_p$-algebra. In each proof, we list a basis $\mathcal{B}$ of R and define xy for all $x, y \in \mathcal{B}$. By distributivity, this defines R uniquely as a PN $\mathbb{Z}_p$-algebra. However the products of basis elements will be of a special type that in each case allows us to drop the "PN" qualifier: for $x, y \in \mathcal{B}$, we will either have $xy = 0$ or $xy = z$ for some $z \in B \cap \operatorname{Ann}(R)$. By distributivity, it follows that $(uv)w = u(vw) = 0$ for all $u, v, w \in R$, and so in particular R is associative. We will in each proof denote elements of $\mathcal{B} \cap \operatorname{Ann}(R)$ as z_i (or simply z if there is only one such element).

Proof of Proposition 4.7. Let R be the $\mathbb{Z}_p$-algebra with basis $\{x_1, x_2, y_1, y_2, z\}$, where the only nonzero products of basis elements are $x_1y_1 = x_2y_2 = z$. Letting S be the 4-dimensional subalgebra of R with basis $\{x_1, x_2, y_1, z\}$, it is clear that $[S, S] = [R, R] = \operatorname{span}\{z\}$.

Next, let T be the 3-dimensional subalgebra of S with basis $\{x_1, y_1, z\}$. Thus, $S = T \oplus \operatorname{span}\{x_2\}$ is isomorphic to a direct sum of T and $\mathbb{Z}_p$, and so it is readily verified that

$$\Pr(S) = \Pr(T)\Pr(\mathbb{Z}_p) = \frac{p^2+p-1}{p^3} \cdot 1 = \frac{p^2+p-1}{p^3}\,.$$

The ring R is what we call an *augmentation of* T in [3, Section 4], so it follows from that paper, or by direct calculation, that

$$\Pr(R) = \frac{p^4+p-1}{p^5} < \Pr(S)\,. \qquad \square$$

Proof of Theorem 4.8. Let R be the algebra with basis

$$\mathcal{B} = \{u_1, u_2, v_1, v_2, w, z_1, z_2\}\,,$$

where the only nonzero products of basis elements are $v_1v_2 = z_1$ and $u_iv_i = u_iw = z_2$ for $i = 1, 2$. Let S be the codimension 1 subalgebra with basis $\mathcal{B}' := \mathcal{B} \setminus \{w\}$.

Let $A_i := \operatorname{span}\mathcal{B}_i$ for $i = 1, 2$, where $\mathcal{B}_1 := \{u_1, u_2, v_1, v_2, w\}$ and $\mathcal{B}_2 := \{z_1, z_2\}$. It is clear that $(R, +)$ is a direct sum of A_1 and A_2. We claim that $\mathrm{Z}(R) = A_2$. Clearly $A_2 \subseteq \operatorname{Ann}(R) \subseteq \mathrm{Z}(R)$, so we need only show that $\mathrm{Z}(R) \subseteq A_2$. First, note that $\dim[v_1, R] = \dim A_2 = 2$, so $C_R(v_1)$ has codimension 2, and we easily deduce that

$$C_R(v_1) = \operatorname{span}\{u_2, v_1, w, z_1, z_2\}\,.$$

By symmetry, $C_R(v_2) = \operatorname{span}\{u_1, v_2, w, z_1, z_2\}$. Now

$$A_2 \subseteq \mathrm{Z}(R) \subseteq C_R(v_1) \cap C_R(v_2) = \operatorname{span}\{w, z_1, z_2\}\,.$$

Moreover, w is not central, so we deduce that $\mathrm{Z}(R) = A_2$, as claimed. Since $A_2 = \mathrm{Z}(R) \subset S \subset R$, we have also proved that $S + \mathrm{Z}(R) \neq R$.

The fact that $\Pr(S) = \Pr(R)$ is a routine exercise, but we indicate how to carry out the required work efficiently. We need to show that $[x, S] = [x, R]$ for all $x \in R$. Since $A_2 = \mathrm{Z}(R)$, it suffices to examine $x \in A_1$. Let us write $Z_2 := \operatorname{span}\{z_2\}$. Since $R = \operatorname{span}(S \cup \{w\})$ and $[w, R] = Z_2$, we have

$$[x, S] \subseteq [x, R] \subseteq [x, S] + Z_2\,, \qquad x \in R\,.$$

Consequently, $[x, S] = [x, R]$ if either $z_2 \in [x, S]$ or $x \in C_R(w)$. We claim that one of these two conditions holds for all $x \in A_1$.

Let

$$x = a_1u_1 + a_2u_2 + b_1v_1 + b_2v_2 + cw\,, \qquad \text{where} \quad a_1, a_2, b_2, b_2, c \in \mathbb{Z}_2\,.$$

Now, $[x, u_1] = (b_1+c)z_2$, so $z_2 \in [x, S]$ if $b_1 + c = 1$. Thus, without loss of generality, it suffices to consider the case $b_1 = c$ and, by symmetry, we may also assume that $b_2 = c$. It follows that $[x, v_1+v_2] = (a_1+a_2)z_2$ so, again without loss of generality, it suffices to consider the case $a_1 = a_2$. Since $u_1 + u_2$, v_1, v_2, and w all lie in $C_R(w)$, our claim is proved, and we have shown that $[x, S] = [x, R]$. $\square$

Finally, we address Question 4.3 in relation to Proposition 1.2. The quantifier-free condition $[R,R]\cap I=\{0\}$ certainly implies that $[x,R]\cap I=\{0\}$ for $x\in R$. However, the next result shows that this quantifier-free condition is not necessary for $\Pr(R)=\Pr(R/I)$.

Theorem 4.9. *There exists a 15-dimensional $\mathbb{Z}_2$-algebra R containing a nontrivial ideal I such that $\Pr(R)=\Pr(R/I)$ and $I\subset[R,R]$.*

Proof. Let R be the $\mathbb{Z}_2$-algebra with basis

$$\mathcal{B}=\{x_i,y_i\mid i=1,2,3\}\cup\{z_{i,j}:(i,j)\in S\}\,,$$

where

$$S=\{(i,j)\mid 1\le i,j\le 3\}\,,$$

and the only nonzero products of basis elements are

$$x_iy_j=z_{i,j}\,,\qquad (i,j)\in S\,.$$

It is readily verified that

$$\operatorname{Ann}(R)=R^2=\operatorname{span}\{z_{i,j}:(i,j)\in S\}\,.$$

Let $I=\operatorname{span}\{s\}$, where $s:=z_{1,1}+z_{2,2}+z_{3,3}$. Since $I\subset\operatorname{Ann}(R)$, I is an ideal.

We claim that s is not a commutator in R. Suppose that $c:=[u,u']$ is a sum of the form $\sum_{i,j=1}^3 c_{i,j}z_{i,j}$ for some $u,u'\in R$, where $c_{i,j}\in\mathbb{Z}_2$ and $c_{i,i}=1$ for $1\le i\le 3$. We claim at least one of the coefficients $c_{i,j}$, $i\ne j$, equals 1, regardless of the choice of u,u'; note that it follows from this claim that s is not a commutator.

It suffices to assume that both u and u' are linear combinations of the six basis elements that lie outside $\operatorname{Ann}(R)$:

$$\left.\begin{aligned}u&:=\sum_{i=1}^3(a_ix_i+b_iy_i)\\ u'&:=\sum_{i=1}^3(a_i'x_i+b_i'y_i)\end{aligned}\right\}\,,\qquad a_i,b_i,a_i',b_i'\in\mathbb{Z}_2\,,\quad i=1,2,3\,.$$

Note that $c_{i,j}=a_ib_j'+a_i'b_j$.

Since $z_{i,i}$ occurs as a term in c, it follows that exactly one of a_ib_i' and $a_i'b_i$ is nonzero for each $i\in\{1,2,3\}$. By swapping u and u' if necessary, we may assume that $a_ib_i'=1$ and $a_i'b_i=0$ for at least two indices i. In fact, by symmetry of the indices, we may assume that these two equations hold for $i\in\{1,2\}$ and, in particular, $a_1=a_2=b_1'=b_2'=1$. Because

$$0=(a_1'b_1)(a_2'b_2)=(a_2'b_1)(a_1'b_2)\,,$$

it also follows that either $a_1'b_2=0$ or $a_2'b_1=0$. Thus, either $a_1b_2'+a_1'b_2=1$ or $a_2b_1'+a_2'b_1=1$, and so either $c_{1,2}=1$ or $c_{2,1}=1$, as claimed.

We have shown that $[x,R]\cap I=\{0\}$ for all $x\in R$ and so, by Proposition 1.2, $\Pr(R)=\Pr(R/I)$. However, $s\in[R,R]$ because $s=[x_1,y_1]+[x_2,y_2]+[x_3,y_3]$, and so $I\subset[R,R]$. □

References

[1] S. M. Buckley, Distributive algebras, isoclinism, and invariant probabilities, Contemp. Math. 634 (2015) 31–52.

[2] S. M. Buckley, D. MacHale, Commuting probabilities of groups and rings, preprint.
[3] S. M. Buckley, D. MacHale, Á. Ní Shé, Finite rings with many commuting pairs of elements, preprint.
[4] J. D. Dixon, Probabilistic group theory, C. R. Math. Acad. Sci. Soc. R. Can. 24(1) (2002) 1–15.
[5] P. Erdös, P. Turán, On some problems of a statistical group–theory, IV, Acta Math. Acad. Sci. Hung. 19(3) (1968) 413–435.
[6] R. M. Guralnick, G. R. Robinson, On the commuting probability in finite groups, J. Algebra 300(2) (2006) 509–528.
[7] K. S. Joseph, Commutativity in non–abelian groups, PhD thesis, University of California, Los Angeles, 1969.
[8] D. MacHale, How commutative can a non–commutative group be? Math. Gaz. 58(405) (1974) 199–202.
[9] D. MacHale, Commutativity in finite rings, Amer. Math. Monthly 83(1) (1976) 30–32.
[10] D. Rusin, What is the probability that two elements of a finite group commute?, Pacific J. Math. 82(1) (1979) 237–247.