Contrasting the commuting probabilities of groups and rings

STEPHEN M. BUCKLEY AND DESMOND MACHALE

Abstract. We contrast the set of commuting probabilities of all finite rings with the set of commuting probabilities of all finite groups.

1. Introduction

Suppose F is an algebraic system of finite cardinality, closed with respect to a multiplication operation denoted by juxtaposition. We define the *commuting probability of* F to be

$$\Pr(F) := \frac{|\{(x,y) \in F \times F \ : \ xy = yx\}|}{|F|^2} \tag{1}$$

where $|S|$ denotes cardinality of a set S.

Much has been written on $\Pr(G)$ when G is a group, and its possible values: see for instance [9], [14], [12], [16], [22], [8], [11], and [7]. Less has been written on the corresponding concepts for rings and semigroups: the only papers on this topic of which we are aware are [17] and [5] for rings, and [18], [10], [1], [21], and [4] for semigroups.

Before proceeding, we introduce a little notation. Let $\mathfrak{G}$, $\mathfrak{S}$, and $\mathfrak{R}$ be the set of values of $\Pr(F)$ as F ranges over all finite groups, finite semigroups, and (possibly non-unital) finite rings, respectively. For each prime p, we define $\mathfrak{G}_p$ and $\mathfrak{R}_p$ similarly, except that we are considering commuting probabilities of *p-groups* and *p-rings*, meaning finite groups and rings whose orders are a power of p.

Trivially, $\mathfrak{G}$, $\mathfrak{S}$, and $\mathfrak{R}$ are all subsets of $(0,1] \cap \mathbb{Q}$. All values in $\mathfrak{G} \cap (11/32, 1]$ were explicitly listed in [22], while all values in $\mathfrak{R} \cap [11/32, 1]$ were explicitly listed in [5]. Despite the very different methods involved in finding the two sets of values exceeding 11/32, both sets are surprisingly similar: in fact both $\mathfrak{G} \cap (11/32, 1]$ and $\mathfrak{R} \cap (11/32, 1]$ are infinite sets, and the only difference between them is the presence of four additional values in the former. By contrast, the situation for semigroups is both very different and completely understood: $\mathfrak{S} = (0,1] \cap \mathbb{Q}$ [21]. In this paper, we concentrate on the differences between groups and rings, rather than the above similarities.

One basic observation for groups, made by Erdös and Turán [9], is that $\Pr(G) = k/|G|$, where k is the number of conjugacy classes in G. There is no equivalent result for rings R and in fact, the following result says that $|R|\Pr(R)$ often fails to be an integer.

Theorem 1. *Suppose R_t is a ring of minimal order among the finite rings satisfying $\Pr(R) = t$ for any t in the infinite set $\mathfrak{R} \cap [11/32, 1)$. Then $t|R_t|$ is not an integer.*

We do not know of any element of $\mathfrak{R}$ that fails to lie in $\mathfrak{G}$, but the following result tells us that $\mathfrak{G} \setminus \mathfrak{R}$ contains infinitely many elements.

2010 *Mathematics Subject Classification.* 20P99, 15A21, 16U99.

Theorem 2. *For all $n \in \mathbb{N}$, $1/n \in \mathfrak{G}$. However, $1/n \notin \mathfrak{R}$ if n is congruent to 2 mod 4, or if $n > 1$ is square-free with at most 69 prime factors.*

After some preliminaries in Section 2, we prove the above theorems and some related results in Section 3, and discuss some conjectures in Section 4.

2. Preliminaries and background

Let us first list the basic terminology and notation used in this paper. All groups and rings are implicitly assumed to be finite. Rings are not necessarily unital[1], but are always associative. We speak of *possibly nonassociative rings* when we want to drop the associativity assumption.

$\mathbb{Z}_n$ denotes the ring of integers mod n, $\mathbb{Z}_n^*$ is the set of units in $\mathbb{Z}_n$, and C_n denotes a cyclic group of order n.

Suppose R is a ring. A *commutator* in R always means an additive commutator and is denoted $[x, y] = xy - yx$. We write $[x, R]$ for the subgroup of $(R, +)$ consisting of all elements of the form $[x, y]$, $y \in R$. The *commutator subgroup* $[R, R]$ is the subgroup of $(R, +)$ generated by the set of all commutators $[x, y]$, $x, y \in R$.

If G is a group, we employ mostly similar notation: $Z(G)$ is the center of G, $C_G(x)$ is the centralizer of $x \in G$, a commutator is $[x, y] = x^{-1}y^{-1}xy$, the commutator subgroup $[G, G]$ is generated by all such commutators, and $x^y = y^{-1}xy$ is the conjugate of x by y.

Each of the sets $\mathfrak{R}$, $\mathfrak{G}$, $\mathfrak{R}_p$, and $\mathfrak{G}_p$, where p is prime, is a monoid under multiplication. Certainly it is clear that each of these sets includes 1 (since abelian groups and commutative rings of all finite orders exist). As for closure under multiplication, this follows from the fact that $\Pr(G) = \Pr(G_1)\Pr(G_2)$ and $\Pr(R) = \Pr(R_1)\Pr(R_2)$, whenever a group G is a direct product of finite groups G_1, G_2, and a ring R is a direct sum of finite rings R_1, R_2; both of these equations follow from the fact that two elements in a direct product/sum commute if and only if both pairs of factors/summands commute. It follows that 0 is an accumulation point of each of these sets.

One difference between groups and rings is that finite rings are direct sums of rings of prime power order, and so it follows that the numbers in $\mathfrak{R}$ are precisely the set of all products $\prod_{i=1}^n t_i$, where $n \in \mathbb{N}$, $t_i \in \mathfrak{R}_{p_i}$, and each p_i is prime. This difference is quite significant: indeed the only numbers we know of in $\mathfrak{G} \setminus \mathfrak{R}$ arise from groups that are not direct products of groups of prime power order, i.e. non-nilpotent groups.

In the absence of the previously-mentioned conjugacy class identity $\Pr(G) = k/|G|$ for groups, we have to make do with the following identity for rings.

$$\Pr(R) = \frac{1}{|R|^2} \sum_{x \in R} |C_R(x)| = \frac{1}{|R|} \sum_{x \in R} \frac{1}{|R/C_R(x)|}\,. \tag{2}$$

Above, $R/C_R(x)$ denotes an additive factor group.

The following are important values of $\Pr(R)$ and $\Pr(G)$, so we give them the following names throughout this paper:

$$\alpha_p = \frac{p^2 + p - 1}{p^3}, \quad \beta_p = \frac{2p^2 - 1}{p^4}, \quad \text{and} \quad \gamma_p = \frac{p^3 + p^2 - 1}{p^5}\,.$$

[1] The set $\mathfrak{R}$ is unchanged if we use only unital rings: see [5, Remark 2.8].

Note that $\gamma_2 = 11/32$. It is straightforward to verify (see [5, Section 2]) that

$$\gamma_p < \alpha_p^2 < \beta_p < \frac{1}{p} < \alpha_p\,, \qquad p \geq 2\,.$$

We will need the following characterization of large $\mathrm{Pr}(R)$ values, which combines two results from [5] (namely, Theorem 1.1 and a consequence of Theorem 1.2).

Theorem A. *For all primes p,*

$$\mathfrak{R}_p \cap [\gamma_p, 1] = \left\{ \frac{p^{2k}+p-1}{p^{2k+1}} \;\middle|\; k \in \mathbb{N} \right\} \cup \left\{1, \beta_p, \alpha_p^2, \gamma_p\right\}\,.$$

Moreover

$$\mathfrak{R} \cap [\gamma_2, 1] = (\mathfrak{R}_2 \cap [\gamma_2, 1]) \cup \{\alpha_3\} = \left\{ \frac{2^{2k}+1}{2^{2k+1}} \;\middle|\; k \in \mathbb{N} \right\} \cup \left\{1, \frac{7}{16}, \frac{11}{27}, \frac{25}{64}, \frac{11}{32}\right\}\,.$$

Moreover in both of the following situations, the equation $\mathrm{Pr}(R) = t$ uniquely determines the isomorphism type of the additive group $R/Z(R)$ where R is a ring in the indicated class S of finite rings:

(a) *$t \in \mathfrak{R}_p \cap (\gamma_p, 1]$, and S is the class of all p-rings for some prime p.*
(b) *$t \in \mathfrak{R} \cap (\gamma_2, 1]$, and S is the class of all finite rings.*

We also state a characterization of $\mathfrak{R}_{\mathrm{odd}} \cap [\gamma_3, 1]$, where $\mathfrak{R}_{\mathrm{odd}}$ is the set of values of $\mathrm{Pr}(R)$ as R ranges over all finite rings of odd order.

Theorem B ([5, Theorem 5.7])**.**

$$\begin{aligned}\mathfrak{R}_{odd} \cap [\gamma_3, 1] &= (\mathfrak{R}_3 \cap [\gamma_3, 1]) \cup (\mathfrak{R}_5 \cap [\gamma_3, 1]) \cup \{\alpha_7\} \\ &= \left\{ \frac{3^{2k}+2}{3^{2k+1}} \;\middle|\; k \in \mathbb{N} \right\} \cup \left\{ \frac{5^{2k}+4}{5^{2k+1}} \;\middle|\; k \in \mathbb{N} \right\} \cup \left\{1, \frac{17}{81}, \frac{121}{729}, \frac{55}{343}, \frac{35}{243}\right\}\,.\end{aligned}$$

The largest values in $\mathfrak{G}$ and in $\mathfrak{R}$ coincide, and the same is true of $\mathfrak{G}_p$ and $\mathfrak{R}_p$ for any given prime p. For a finite non-abelian group G, Gustafson [12] proved that $\mathrm{Pr}(G) \leq \alpha_2$, and Joseph [14] showed that if p is the smallest prime divisor of $|G|$, then $\mathrm{Pr}(G) \leq \alpha_p$, with equality if and only if $|G/Z(G)| = p^2$. By [22, p.246] and [7, Remark 4.4(a)], we see that the elements in $\mathfrak{G} \cap (11/32, 1]$ are precisely the same as the elements in $\mathfrak{R} \cap (11/32, 1]$ as given in Theorem A, plus four additional values, namely 1/2, 2/5, 3/8, and 5/14. We do not know of any explicit listing of the elements of $\mathfrak{G}$ below 11/32, but recently Hegarty [13] gleaned some information about the structure of $\mathfrak{G} \cap (2/9, 1]$.

Nilpotent groups will be used in Section 4; in view of our finiteness assumption, nilpotent groups coincide with the class of groups that are direct products of their Sylow p-subgroups. We are particularly interested in *class 2 nilpotent groups*, namely those noncommutative groups for which $[G,G] \subseteq Z(G)$. In particular, we note the class 2 group identities $[x,y][x,w] = [x,yw]$ and $[y,x][w,x] = [yw,x]$, which in turn imply that $[x^n, y] = [x,y]^n = [x, y^n]$ for all $n \in \mathbb{N}$.

We now state a proposition that gives a pair of identities that are equivalent to nilpotency of class at most 2; we leave the proof to the reader.

Proposition 3. *The following conditions are equivalent for a group G:*

(a) *G is nilpotent of class at most 2.*
(b) *$[y,x][w,x] = [yw,x]$, for all $x, y, w \in G$.*
(c) *$[x,y][x,w] = [x,yw]$, for all $x, y, w \in G$.*

3. Proofs of main results

It follows immediately from Theorem A that $\mathfrak{R} \cap [11/32, 1)$ and $\mathfrak{R}_p \cap [\gamma_p, 1)$ are infinite for all primes p. Thus part (b) of the following result is equivalent to Theorem 1.

Theorem 4. *Suppose R_t is a finite ring such that $\operatorname{Pr}(R_t) = t$ for some $t < 1$. Then $t|R_t|$ fails to be an integer in each of the following cases:*

(a) *$t \geq \gamma_p$ for some prime p, and R_t has minimal order among finite p-rings with commuting probability t.*
(b) *$t \geq \gamma_2$ and R_t has minimal order among finite rings with commuting probability t.*

Note that the choice of a ring of minimal order with a particular commuting probability is crucial in Theorem 4: if R' is the direct sum of any finite ring R and a commutative ring of order $|R|$, then $\operatorname{Pr}(R') = \operatorname{Pr}(R)$, and so $|R'| \operatorname{Pr}(R') = |R|^2 \operatorname{Pr}(R)$ is an integer by (1).

Proof of Theorem 4. Suppose first that R_t has minimal order among p-rings with commuting probability t. By the proof of Theorem A in [5, Theorem 1.1], we see that there is a ring R of order p^{2k} with $\operatorname{Pr}(R) = (p^{2k} + p - 1)/p^{2k+1}$. Also by the case $k = 1$, we see that if R is a direct sum of two noncommutative rings of order p^2, then $\operatorname{Pr}(R) = \alpha_p^2$. In all these cases, we have a ring $R \in \mathfrak{R}_p$ such that $|R| \operatorname{Pr}(R)$ is not an integer. This is already enough to imply that $t|R_t|$ is not an integer, since $|R_t|$ is a divisor of $|R|$ if $\operatorname{Pr}(R) = \operatorname{Pr}(R_t)$. In fact though, it is easily seen that the rings given here are the minimal order rings. To see this, note first that according to Theorem A, each $t > \gamma_p$ uniquely determines $R/Z(R)$ among p-rings satisfying $\operatorname{Pr}(R) = t$. A table of these isomorphism types is given in [5, Figure 2], and in each case the order of the ring R given above for this value of t equals the order of the uniquely determined central factor group $R/Z(R)$.

As for γ_p, it follows from [5, Theorem 5.1] that the ring

$$M(p^2) = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z}_{p^2} \right\} .$$

satisfies $\operatorname{Pr}(M(p^2)) = \gamma_p$. Since $|M(p^2)| = p^4$, we deduce that $|R_t| \operatorname{Pr}(R_t)$ is not an integer for $t = \gamma_p$.

The one value remaining in part (a) is β_p. In this case, we consider the vector space A over $\mathbb{Z}_p$ with basis $\{u, v, w\}$. We define a multiplication on A by first defining it on all ordered pairs of basis elements (x, y): let $xy = x$ if $y = w$ and $xy = 0$ otherwise. We then extend multiplication to all of A by distributivity. This clearly makes A into a possibly nonassociative ring. To check that A is in fact a ring, it suffices to check that $(xy)z = x(yz)$ when x, y, z are basis elements. From the definition of products of basis elements, we see that the only nonzero products involve w as the right-hand factor. Thus $(xy)z = x(yz) = 0$ unless $y = z = w$, in which case $(xw)w = x(ww) = x$ for $x \in \{u, v, w\}$, so A is indeed associative.

Now let $x = x_0 w + x_1 u + x_2 v$, where $x_i \in \mathbb{Z}_p$, $i = 0, 1, 2$. If $x_0 \neq 0$, then $[x, A]$ has dimension 2, since it includes $[u, x] = x_0 u$ and $[v, x] = x_0 v$. Thus $|C_R(x)| = p$ for the $p^3 - p^2$ elements x for which $x_0 \neq 0$. If $x_0 = 0$ but $x \neq 0$, then x commutes with u and v but not with w, so $|C_R(x)| = p^2$ for the $p^2 - 1$ elements of this type.

Finally, $|C_0(0)| = p^3$. Since $|A| = p^3$, it follows from (2) that

$$\Pr(A) = \frac{1}{p^6}\left((p^3 - p^2)(p) + (p^2-1)(p^2) + (1)(p^3)\right) = \frac{2p^2-1}{p^4} = \beta_p\,.$$

Thus $|A|\Pr(A)$ is not an integer, and so $t|R_t|$ is not an integer for $t = \gamma_p$. In fact, $|A|$ is again of minimal order because [5, Figure 2] tells us that $|R/Z(R)| = p^3$ if R is a p-ring with $\Pr(R) = \beta_p$.

We next consider $t \geq \gamma_2$ and now R_t has minimal order among rings in $\mathfrak{R}$ with commuting probability t. If $t > \gamma_2$, then Theorem A tells us that $t \in \mathfrak{R}_p$ for $p = 2$ or $p = 3$. Now arguing as in the proof of (a), we readily deduce that $t|R_t|$ is not an integer. There remains $t = \gamma_2$. Among 2-rings, it follows from [5, Figure 3] that a ring R with $\Pr(R) = \gamma_2$ has central factor group of order 8, 16, or 32. The ring $M(4)$ given above has order 16, so the minimal order ring R_t either has order 8 or 16. In either case, $t|R_t|$ is not an integer. □

The above proof demonstrates the difficulty or perhaps the impossibility of defining any satisfactory analogue of group theoretic conjugacy classes in rings.

Remark 5. The above proof reveals that when $t > \gamma_p$ (or $t > \gamma_2$), the minimal order p-ring (or minimal order ring, respectively) R_t has the property that $|Z(R_t)| = 1$, and so $|R_t|$ equals the uniquely determined number $|R/Z(R)|$ for rings R satisfying $\Pr(R) = t$. The situation for $t = \gamma_p$ is rather different. The example of a ring R with $\Pr(R) = \gamma_p$ that we gave was $M(p^2)$, and $|M(p^2)| = p^4$. There is not a unique isomorphism type of $|R/Z(R)|$ for p-rings R satisfying $\Pr(R) = \gamma_p$, but [5, Figure 3] tells us that p^3 is the minimal order for $|R/Z(R)|$ in this case. One might therefore wonder if there exists such a ring R of order p^3. However, this is impossible by the following result, because [5, Figure 3] also tells us that $|[R,R]| = p^3$ if R is a p-ring such that $\Pr(R) = \gamma_p$ and $|R/Z(R)| = p^3$.

Proposition 6. *If R is a finite nontrivial ring, then $[R,R]$ is a proper subgroup of $(R,+)$.*

Proof. Suppose for the sake of contradiction that R is a finite ring with $[R,R] = R$. Writing $J(R)$ for the Jacobson radical of R, it is straightforward to verify that $R' := R/J(R)$ has the property $[R',R'] = R'$. By Jacobson's structure theory and Wedderburn's little theorem, R' is a direct sum of full matrix rings over finite fields.

Recall the well-known trace identity

$$\operatorname{tr}(AB - BA) = 0, \qquad A, B \in M_n(F)\,,$$

where $M_n(F)$ is the ring of $n \times n$ matrices over a field F, and $n \in \mathbb{N}$. It follows that the trace of all matrices in $[M_n(F), M_n(F)]$ must be zero: in particular, the identity matrix does not lie in $[M_n(F), M_n(F)]$. Consequently, R' must be trivial and so $R = J(R)$, i.e. R is a finite radical ring.

But finite radical rings are nilpotent. We do not have a direct reference for this, so let us prove it. First, suppose $n \in \mathbb{N}$ is such that $nR = \{0\}$; we could take $n = |R|$. Now let S be a Dorroh extension of R defined as follows: $(S,+) = \mathbb{Z}_n \oplus R$, and multiplication is defined by $(i,x)\cdot(j,y) = (ij, xy+iy+jx)$. Then $J(R) = R \cap J(S)$ by [19, Lemma 12]. Moreover the radical of a left Artinian unital ring is nilpotent [2, 15.19], so it follows that $J(R)$ is nilpotent. However, $[R,R] = R$ implies that $R^2 = R$, which is incompatible with nilpotency. □

We now state three theorems which together imply Theorem 2. The first lists some elements of $\mathfrak{G}$; part (a) is known and can be found for instance in [20, Theorem 1.7.4] or [6, Section 5.3]. The other parts may also be known but appear to be unpublished, so we include a proof of the full theorem for completeness. The second and third theorems show that many of these elements of $\mathfrak{G}$ are not in $\mathfrak{R}$.

Theorem 7.
(a) $1/n \in \mathfrak{G}$ *for all* $n \in \mathbb{N}$.
(b) $2/n \in \mathfrak{G}$ *if* $n \equiv 5 \pmod 8$ *or* $n \equiv 7 \pmod 8$.
(c) $1/q + (q-1)/p^2q \in \mathfrak{G}$ *if* p, q *odd primes and* $q \equiv 1 \pmod p$.

Theorem 8. *Below,* $k, m, n \in \mathbb{N}$, $k < n$, *and* k *is coprime to* m *and* n.
(a) $k/n \notin \mathfrak{R}$, *if* k *is even, or if* k *is odd and* $n = 2m$ *for some odd* m.
(b) $k/4m \notin \mathfrak{R}$, *if* $k/m \notin \mathfrak{R}$ *and* k, m *are odd.*

Theorem 9. *Suppose* $n \in \mathbb{N}$ *is square-free, and* $k \in \mathbb{N}$ *is less than, and coprime to,* n. *Then* $k/n \notin \mathfrak{R}$ *if any of the following additional assumptions hold:*
(a) n *is divisible by* 2;
(b) n *is divisible by* 3 *and has at most 410 distinct prime factors;*
(c) n *has at most 69 prime factors.*

Let us now prove Theorem 7. Note that the restriction on n in (b) cannot be dropped: for instance, it follows from Gustafson's main result in [12] that $2/3 \notin \mathfrak{G}$.

Proof of Theorem 7. We first prove (a). Certainly $1 \in \mathfrak{G}$ (abelian groups) and $1/2 \in \mathfrak{G}$ (the symmetric group S_3), so suppose inductively that $1/m \in \mathfrak{G}$ for all $m < n$, where $n \geq 3$. If $n = 2n'$ is even, then $1/n \in \mathfrak{G}$ because of the semigroup property of $\mathfrak{G}$ and the fact that $1/2$ and $1/n'$ both lie in $\mathfrak{G}$. Suppose therefore that n is odd.

The dihedral group with $4k$ elements is known to have $k+3$ conjugacy classes for all $k > 1$. Thus $(k+3)/4k \in \mathfrak{G}$ for all $k > 1$ (and trivially for $k = 1$). If n is congruent to 1 mod 4, then by the inductive hypothesis we have $4/(n+3) \in \mathfrak{G}$, and so

$$\frac{1}{n} = \frac{n+3}{4n} \cdot \frac{4}{n+3} \in \mathfrak{G}\,.$$

If instead n is congruent to 3 mod 4, then the dihedral group with $12n$ elements shows that $(n+1)/4n = (3n+3)/4(3n) \in \mathfrak{G}$, and the inductive hypothesis now allows us to deduce that $1/n = [(n+1)/4n][4/(n+1)] \in \mathfrak{G}$.

The proof of (b) is similar to that of (a), except now we need that either $8/(n+3)$ or $8/(n+1)$ lie in $\mathfrak{G}$. Because of the form of n, this follows from (a).

Finally, (c) follows immediately from the fact that there is a (unique) non-abelian group of order pq when p, q are as hypothesized, and this group has $p + (q-1)/p$ conjugacy classes. □

In preparation for the proof of Theorem 8, we need the following lemma concerning the *p-adic valuation* defined by $\nu_p(r) = k$ whenever $r = ip^k/j$, $i, j, k \in \mathbb{Z}$, and ij is not divisible by the prime p.

Lemma 10. *Suppose* $0 < t < 1$ *and* $t \in \mathfrak{R}_p$ *for some prime* p.
(a) $\nu_2(t) \leq -2$ *if* $p = 2$, *and* $\nu_2(t) = 0$ *if* $p \neq 2$.
(b) $\nu_3(t) \leq -2$ *if* $p = 3$, *and* $\nu_3(t) = 0$ *if* $p \neq 3$ *and* $t \geq \gamma_p$.

Proof. Suppose R is a p-ring with $\Pr(R) = t < 1$. We first prove (a). Since $1/2 \notin \mathfrak{R}_2$, it follows from (1) that if $p = 2$, then $\nu_2(t) \le -2$. On the other hand if $p > 2$, then $|C_R(x)|$ is odd for all $x \in R$, and so (2) implies that $\nu_2(\Pr(R)) = 0$.

We next prove (b). Since $1/3, 2/3 \notin \mathfrak{R}_3$, it follows from (1) that if $p = 3$, then $\nu_3(R) \le -2$. The fact that $\nu_3(t) = 0$ whenever $p \ne 3$, $t \in \mathfrak{R}_p$, $t \ge \gamma_p$, follows by an examination of the values that arise in Theorem A. Calculating mod 3, $p^{2k} + p - 1 \equiv p \not\equiv 0$, and this also shows that $\nu_3(\alpha_p^2) = 0$. Next $\nu_3(\beta_p) = \nu_3(2p^2-1)$ and $2p^2-1 \equiv 1 \pmod 3$. Finally, $\nu_3(\gamma_p) = \nu_3(p^3+p^2-1) = 0$ because $p^3 + p^2 - 1 \equiv p^3 \equiv p \pmod 3$. □

Proof of Theorem 8. We first prove (a). Suppose for the sake of contradiction that R is a finite ring with $\Pr(R) = k/n$. By hypothesis, either $\nu_2(k/n) > 0$ or $\nu_2(k/n) = -1$. We write R in the form $R_1 \oplus R_2$, where $|R_1|$ is odd and R_2 is a 2-ring, and so $\Pr(R) = \Pr(R_1)\Pr(R_2)$. Applying Lemma 10(a) to R_2, we see that either $\Pr(R_2) = 1$ or $\nu_2(\Pr(R_2)) \le -2$. On the other hand, $\Pr(R_1)$ is a product of numbers $t_p \in \mathfrak{R}_p$ for some finite collection of odd primes p, and $\nu_2(t_p) = 0$ for all of these primes by Lemma 10(a). Thus $\nu_2(\Pr(R_1)) = 0$, and so either $\nu_2(k/n) = 0$ or $\nu_2(k/n) \le -2$, both of which are incompatible with our hypotheses.

We now prove (b). Suppose $\Pr(R) = k/4m$. Following the proof of (a), we see that R can be written in the form $R_1 \oplus R_2$, where R_1, R_2 are as before. We get a contradiction as before unless $\Pr(R_2) = 1/4$ (since $2/4$ and $3/4$ do not lie in $\mathfrak{R}$). But $\Pr(R_2) = 1/4$ forces $\Pr(R_1) = k/m$, so $k/m \in \mathfrak{R}$. □

In preparation for the proof of Theorem 9, we now show that the numbers α_p, β_p, and γ_p are decreasing as functions of p. These numbers are only of interest when p is prime, but we allow p to take on real values in $[2, \infty)$ in the following lemma in order to use calculus.

Lemma 11. *$p\alpha_p$, β_p/α_p and γ_p/α_p are all strictly decreasing functions of p, for $p \in [2, \infty)$.*

Proof. Let $f(p) := p\alpha_p$. Then $f'(p) = (2-p)/p^3 < 0$ for all $p > 2$. Consequently, $f(p)$ is strictly decreasing on $[2, \infty)$.

Let $g(p) := \alpha_p/\beta_p = (p^3 + p^2 - p)/(2p^2 - 1)$. Differentiating, we get $g'(p) = (2p^4 - p^2 - 2p + 1)/(2p^2 - 1)^2$, and it is clear that $g'(p) > 0$ for all $p \ge 2$. Consequently, $g(p)$ is strictly increasing on $[2, \infty)$.

Let $h(p) := \alpha_p/\gamma_p = (p^4 + p^3 - p^2)/(p^3 + p^2 - 1)$. Differentiating, we get

$$h'(p) = \frac{p(p^2 - 1)(p^3 + 2p^2 + 3p - 2)}{(p^3 + p^2 - 1)^2},$$

and it is clear that $h'(p) > 0$ for all $p \ge 2$. Consequently, $h(p)$ is strictly increasing on $[2, \infty)$. □

Proof of Theorem 9. Part (a) follows from Theorem 8(a). We next prove (b), so suppose that n is divisible by 3. In view of part (a), we may assume that n is odd. We write n as a product $\prod_{i=1}^{s} p_i$ of distinct prime factors, with $p_1 = 3$. We may assume that $s > 1$ since $1/3, 2/3 \notin \mathfrak{R}_{\mathrm{odd}}$ by Theorem B. Suppose for the sake of contradiction that R is a finite ring with $\Pr(R) = k/n$, and $s \le 410$.

First we note that R must be a direct sum of a commutative ring and a finite set of noncommutative p-rings R_p, where the set S of such primes p includes p_i

for all $1 \le i \le s$. Thus $\Pr(R) = \prod_{p\in S} \pi_p$, where $\pi_p := \Pr(R_p) \le \alpha_p$ (because α_p is the largest number in $\mathbb{R}_p \setminus \{1\}$).

Since $\nu_3(k/n) = -1$ and $\nu_3(\pi_3) \le -2$ (Lemma 10), we must have $\nu_3(\pi_p) > 0$ for some $p \in S \setminus \{3\}$. By Lemma 10, we deduce that $\pi_q < \gamma_q$ for some $q \in S$, $q \ge 5$. Since $p\alpha_p$ and γ_p/α_q are both decreasing functions of p (Lemma 11), and since α_p is the largest element in $\mathfrak{R}_p \setminus \{1\}$, it follows that

$$k = n \Pr(R) < \frac{\gamma_q}{\alpha_q} \prod_{i=1}^{s} p_i \alpha_{p_i} \le \frac{\gamma_5}{\alpha_5} P_3(410)\,,$$

where $P_t(s)$ is the product of $p\alpha_p$, as p ranges over the smallest s primes that equal or exceed t; here $s, t \in \mathbb{N}$. A computation shows that

$$P_3(410) < 4.8652 < 4.8657 < \frac{\alpha_5}{\gamma_5}\,,$$

so $k < 1$, giving a contradiction.

Finally, we prove (c). We write n as a product $\prod_{i=1}^{s} p_i$ of distinct prime factors, where $s \le 69$. By (a) and (b), we may assume that $p_i \ge 5$ for all i. Suppose for the sake of contradiction that R is a finite ring with $\Pr(R) = k/n$, and $s \le 69$.

Arguing as before, we again see that R must be a direct sum of a commutative ring and a finite set of noncommutative p-rings R_p, where the set S of such primes p includes at least p_i for all $1 \le i \le s$. Thus $\Pr(R) = \prod_{p\in S} \pi_p$, where $\pi_p := \Pr(R_p) \le \alpha_p$.

Suppose first that $\pi_p \le 1/p$ for some divisor p_i of n. Using Lemma 11, it follows that

$$k = n \Pr(R) \le \frac{\beta_5}{\alpha_5} P_5(69)\,.$$

But a computation shows that

$$P_5(69) < 2.9586 < 2.9591 < \frac{\alpha_5}{\beta_5}\,,$$

so $k < 1$, giving a contradiction. We may therefore suppose that $\pi_{p_i} > 1/p_i$, $1 \le i \le s$.

Suppose now that S includes at least one prime p that is not a factor of n. If $p \ge 5$, then it follows that

$$k = n \Pr(R) \le \alpha_p P_5(69)\,.$$

We get a contradiction as before because $1/\alpha_p \ge 1/\alpha_5 > 4 > P_5(69)$. If instead $p = 3$, then $\nu_3(\pi_3) \le -2$ while $\nu_3(\pi_{p_i}) = 0$ for all i (by Lemma 10(b)). Since $\nu_3(k/n) \ge 0$, S must contain a prime q that does not divide $3n$, and we are back to the previous case.

We conclude that S contains the prime factors of n and no other primes, and that $\pi_{p_i} > 1/p$ for all p, so

$$k = n \Pr(R) = \prod_{i=1}^{s} p_i \pi_{p_i} > 1\,.$$

But as in the proof of Theorem 8(a), we see that $\nu_2(\Pr(R)) = 0$, and $\nu_3(\Pr(R)) = 0$ by Lemma 10(b). Thus k cannot be a multiple of 2 or 3, so $k \ge 5$. But $k \le P_5(69) < 5$, giving a contradiction. □

Remark 12. Das and Nath [7, Theorem 4.3] find all values $\mathfrak{G}_{\text{odd}}$ of $\Pr(G) \geq 11/75$ among odd order groups. An examination of these values reveals some additional elements of $\mathfrak{G} \setminus \mathfrak{R}$. Comparing their results with the values of $\mathfrak{R}_{\text{odd}} \cap [11/75]$, as given in Theorem B, we see that $\mathfrak{G}_{\text{odd}} \cap [11/75]$ contains all of $\mathfrak{R}_{\text{odd}} \cap [11/75]$, plus five additional values, namely 5/21, 7/39, 3/19, 29/189, and 11/75.

4. Conjectures

In view of Theorem 9 and the considerable constraints on the equation $\Pr(R) = 1/n$ that become apparent when one examines various special cases, it seems highly likely that the following conjecture is true.

Conjecture 13. $1/n \notin \mathfrak{R}$ *when* $n \in \mathbb{N}$ *is square-free.*

Our second conjecture is quite a natural one in view of what we know about $\mathfrak{R}$ and $\mathfrak{G}$, but we have no other evidence in its favor.

Conjecture 14. $\mathfrak{R} \subset \mathfrak{G}$.

The groups G of which we know with the property that $\Pr(G) \notin \mathfrak{R}$ all have orders involving at least two distinct prime factors: for instance, dihedral groups and their direct products featured in Theorem 7, and $\Pr(A_4) = 1/3$, where A_4 is the alternating group on four symbols, and the five additional values in Remark 12 arise as commuting probabilities only of groups G for which $|G/Z(G)|$ has two distinct prime factors. We know of no number that lies in either $\mathfrak{R}_p \setminus \mathfrak{G}_p$ or $\mathfrak{G}_p \setminus \mathfrak{R}_p$. This leads us to the following two-part conjecture, where we cannot rule out any possibility: logically, it is possible that either, both, or neither of these two parts might be true.

Conjecture 15.

(a) $\mathfrak{R}$ *coincides with the set of values of* $\Pr(G)$ *as* G *ranges over all finite nilpotent groups.*

(b) $\mathfrak{R}$ *coincides with the set of values of* $\Pr(G)$ *as* G *ranges over all finite nilpotent groups of class at most* 2.

Since a finite ring is a direct sum of finite rings of prime power order, it is arguable that the best group theoretic analogue of a finite ring is a finite nilpotent group rather than a general finite group, leading us to Conjecture 15(a).

There is some suggestive evidence that class 2 nilpotent groups are the “right” group theoretic analogues of noncommutative rings, and it is such thoughts that lead us to Conjecture 15(b). By Proposition 3, class 2 nilpotent groups satisfy the identities $[x, yw] = [x, y][x, w]$ and $[yw, x] = [y, x][w, x]$, and so $[x^n, y] = [x, y]^n = [x, y^n]$, $n \in \mathbb{N}$. These equations mirror the ring theoretic identities $[x, y + w] = [x, y] + [x, w]$ and $[nx, y] = n[x, y] = [x, ny]$.

A second analogy between these concepts involves isoclinism. Since $\Pr(\cdot)$ is an isoclinic invariant for groups, a p-group G satisfies $\Pr(G) = \Pr(H)$, where H is a *stem group*, meaning a group of minimal order in the isoclinism family of G. Equivalently, stem groups H satisfy the condition $Z(H) \subseteq [H, H]$ [3, p.287]. Since it is clear that isoclinism preserves nilpotency class, it follows that if a p-group G is of class 2, then any stem group H of G satisfies $Z(H) = [H, H]$.

For a p-ring R, we do not in general have any containment relation between $Z(R)$ and $[R, R]$. However, according to the results of [5], there exists a p-ring S such that $\Pr(R) = \Pr(S)$ and $Z(S) = [S, S]$. Thus all elements of $\mathfrak{R}$ are products over a finite set of primes p of numbers of the form $\Pr(R)$ for some p-ring R such that $Z(R) = [R, R]$. Note also that $[x, G]$ is a subgroup of a group G if $x \in G$

and G is class 2 nilpotent, and that this mirrors the fact that $[x, R]$ is a subring of a ring R for all $x \in R$.

As further justification for Conjecture 15, we note that Theorem 8 remains true if $\mathfrak{R}$ is replaced by $\mathfrak{G}_{\mathrm{nilp}}$, the set of commuting probabilities of finite nilpotent groups (or *a fortiori* if we replace $\mathfrak{R}$ by the set of commuting probabilities of finite nilpotent groups of class at most 2). The proof follows immediately once we have an analogue of Lemma 10(a) for p-groups. Such an analogue holds because the analogue of (2) for groups holds and $1/2 \notin \mathfrak{G}_2$ (see [16]).

It seems likely that a similar analogue of Theorem 9 holds for nilpotent groups but this would require a classification of the set $\mathfrak{G}_p \cap [\gamma_p, 1]$, and this does not appear to have been carried out. However, we can at least show that the values in $\mathfrak{G} \setminus \mathfrak{R}$ exceeding 11/32 and the five exceptional values in Remark 12 all fail to be associated with nilpotent groups. This rules out “large” probabilities as counterexamples to Conjecture 15.

Proposition 16. *If G is a finite nilpotent group then*

$$\Pr(G) \notin \{1/2, 2/5, 3/8, 5/14, 5/21, 7/39, 3/19, 29/189, 11/75\}.$$

The proof is by examination of the possible isomorphism types of $G/Z(G)$ for finite groups attaining each of these values, as given in [22] and [7]. In each case the only possible isomorphism types of $G/Z(G)$ are non-nilpotent, and so G must also be non-nilpotent. This proof is however suspect for $\Pr(G) = 5/14$, since this value was missed by Rusin but mentioned in Das and Nath in [7, Remark 4.4(a)] with the comment that $G/Z(G)$ is isomorphic to the dihedral group of order 14. This group is of course non-nilpotent, but no proof is given that it is the only possible isomorphism type of $G/Z(G)$ in this case. Fortunately the nilpotent group analogue of Theorem 8 comes to our rescue and rules out $\Pr(G) = 5/14$.

An alternative proof of Proposition 16 avoiding the deeper results of Rusin and Das-Nath can be given for all listed values t except 3/8. It relies mostly on the following facts:

(a) If G is a noncommutative finite nilpotent group, then $\Pr(G) = \prod_p \Pr(G_p)$, where we take a product over one or more primes p, and each G_p is a noncommutative Sylow p-subgroup of G.

(b) Writing $\Pr(G) = m/n$ for coprime $m, n \in \mathbb{N}$, only G_p can give rise to any particular prime factor p of n.

(c) $\Pr(G_p) \le \alpha_p < 2/p$ [15].

For instance in the case $t = 2/5$, (b) tells us that we would need a G_5, but then $\Pr(G) \le \alpha_5 < 2/5$. For five of the values, all that is needed is an estimate using (c) for a single prime. For two other values, namely the last two listed numbers, we need to use two primes: for instance, $\Pr(G) \le \alpha_3\alpha_7 < 29/189$ for $t = 29/189$. The two remaining values are 1/2 and 3/8. Now $\Pr(G) = 1/2$ would require that we have a G_2 with $\Pr(G_2) = 1/2$, but $1/2 \notin \mathfrak{G}_2$ [16]. Finally, $\Pr(G) = 3/8$ is easily seen to imply that there is a G_2 with $\Pr(G_2) = 3/8$. However, the only proof we know of that this value is not attained by a 2-group is that of Rusin [22].

Our last conjecture is inspired by Joseph’s three conjectures for groups [15].

Conjecture 17.

(a) *Every accumulation point of $\mathfrak{R}$ is rational.*

(b) *For each $0 < t \le 1$, there exists $\epsilon_t > 0$ such that $\mathfrak{R} \cap (t - \epsilon_t, t) = \emptyset$.*

(c) *$\mathfrak{R}$ does not contain any of its accumulation points.*

Here, (a) and (b) are direct analogues of Joseph's first and second conjectures: we have merely replaced $\mathfrak{G}$ by $\mathfrak{R}$. By contrast, (c) negates as strongly as possible the natural analogue of Joseph's third conjecture, which states that $\mathfrak{G}$ contains all of its positive accumulation points.

The one piece of evidence that we can offer in favor of (a) is that we know how to construct positive limits of elements in $\mathfrak{R}$ only by repeated augmentation (or by generalized variants of such a process) as described in [5, Section 4], and such processes always give rational limits.

Our evidence in favor of (b) is limited to the fact that limits of sequences drawn from $\mathfrak{R}_p \cap (\gamma_p, 1]$ have this property for each prime p (and hence the same is true of $\mathfrak{R} \cap (\gamma_2, 1]$), as follows immediately from Theorem A. Note that if (b) is true then $\mathfrak{R}$ is a well-ordered set, so we could ask what is its order type: it is routine to see that it must be at least ω^ω.

As evidence for (c), we note that the limits of $\mathfrak{R}_p \cap [\gamma_p, 1]$ do not lie in $\mathfrak{R}_p$, and hence the same is true of $\mathfrak{R} \cap [\gamma_2, 1]$. Also note that $1/p$ is an accumulation point of $\mathfrak{R}_p$ (by Theorem A), and so $1/n$ is an accumulation point of $\mathfrak{R}$ for all n, whereas Theorem 8 shows that $1/n \notin \mathfrak{R}$ for many values of n.

References

[1] K. Ahmadidelir, C.M. Campbell, and H. Doostie, *Almost commutative semigroups*, Alg. Colloq. **18** (2011), 881–888.

[2] F.W. Anderson and K.R. Fuller, *Rings and categories of modules*, Springer, Berlin, 1992.

[3] Y. Berkovich, *Groups of prime power order. Vol. 1*, de Gruyter Expositions in Mathematics, 46, Walter de Gruyter, Berlin, 2008; doi:10.1515/9783110208221.285.

[4] S.M. Buckley, *Minimal order semigroups with speci?ed commuting probability*, Semigroup Forum, 2013, (DOI) 10.1007/s00233-013-9530-7.

[5] S.M. Buckley, D. MacHale, and Á. Ní Shé, *Finite rings with many commuting pairs of elements*, preprint.

[6] A. Castelaz, *Commutativity degree of finite groups*, M.A. thesis, Wake Forest University (2010).

[7] A.K. Das and R.K. Nath, *A characterisation of certain finite groups of odd order*, Math. Proc. R. Ir. Acad. **111A** (2011), 69–78; doi:10.3318/pria.2011.111.1.8.

[8] J. Dixon, *Probabilistic group theory*, C.R. Math. Rep. Acad. Sci. Canada **24** (2002), 1–15.

[9] P. Erdös and P. Turán, *On some problems of a statistical group-theory, IV*, Acta Math. Acad. Sci. Hung. **19** (1968), 413–435.

[10] B. Givens, *The probability that two semigroup elements commute can be almost anything*, College Math. J. **39** (2008), 399–400.

[11] R.M. Guralnick and G.R. Robinson, *On the commuting probability in finite groups*, J. Algebra **300** (2006), 509-528; doi:10.1016/j.jalgebra.2005.09.044.

[12] W.H. Gustafson, *What is the probability that two group elements commute?*, Amer. Math. Monthly **80** (1973), 1031–1034.

[13] P. Hegarty, *Limit points in the range of the commuting probability function on finite groups*, J. Group Theory **16** (2013), 235–247.

[14] K.S. Joseph, *Commutativity in non-abelian groups*, PhD thesis, University of California, Los Angeles, 1969.

[15] K.S. Joseph, *Several conjectures on commutativity in algebraic structures*, Amer. Math. Monthly **84** (1977), 550-551.

[16] D. MacHale, *How commutative can a non-commutative group be?*, Math. Gaz. **LVIII** (1974), 199–202; doi:10.2307/3615961.

[17] D. MacHale, *Commutativity in finite rings*, Amer. Math. Monthly **83** (1976), 30–32.

[18] D. MacHale, *Probability in finite semigroups*, Irish Math. Soc. Bull. **25** (1990), 64–68.

[19] Z. Mesyan, *The ideals of an ideal extension*, J. Algebra Appl. **9** (2010), 407–431.

[20] A. Ní Shé, *Commutativity and generalisations in finite groups*, PhD thesis, University College Cork (2000).

[21] V. Ponomarenko and N. Selinski, *Two semigroup elements can commute with any positive rational probability*, College Math. J. **43** (2012), 334–336.

[22] D.J. Rusin, *What is the probability that two elements of a finite group commute?*, Pac. J. Math. **82** (1979), 237–247.

S.M. Buckley:
Department of Mathematics and Statistics, National University of Ireland Maynooth, Maynooth, Co. Kildare, Ireland.
E-mail address: stephen.buckley@maths.nuim.ie

D. MacHale:
School of Mathematical Sciences, University College Cork, Cork, Ireland.
E-mail address: d.machale@ucc.ie