Finite rings with many commuting pairs of elements

STEPHEN M. BUCKLEY, DESMOND MACHALE, AND ÁINE NÍ SHÉ

ABSTRACT. We investigate the set of values attained by $\Pr(R)$, the probability that a random pair of elements in a finite ring R commute. A key tool is a new notion of isoclinism for rings, and an associated canonical form for rings. In particular, we show that $\Pr(R)$ is an isoclinic invariant, and characterize all possible values of $\Pr(R) \geq 11/32$, and the associated isoclinism families.

1. INTRODUCTION

There has been much written on the possible values attained by the probability that a random pair of elements in a finite group commute: see for instance [5], [11], [7], [14], [17], [13], [4], [6], [3], and [9]. In this paper, we examine the corresponding question for finite rings. This topic, by contrast, has attracted little attention: indeed [15] is the only contribution of which we are aware.

To be precise, we define the *commuting probability* to be

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

where R is a finite ring, and $|S|$ denotes cardinality of a set S. Let $\mathfrak{R}$ be the set of values of $\Pr(R)$ as R ranges over all (possibly non-unital) finite rings. Trivially, $\mathfrak{R} \subset (0,1] \cap \mathbb{Q}$. For each prime p, we define $\mathfrak{R}_p$ similarly, except that R is allowed to range only over *p-rings*, meaning rings whose order is a power of p.

Throughout the paper, we write

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

We will see later that

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

We determine in particular all $t \in \mathfrak{R}$ such that $t \geq \gamma_2 = 11/32$, and all $t \in \mathfrak{R}_p$, $t \geq \gamma_p$, where p is prime. Additionally, we will see that each such $t \in (\gamma_2, 1)$ uniquely characterizes the ring in a certain sense.

Theorem 1.1. *For all primes p,*

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

Date: 04.02.2014.

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

Moreover,

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

Our second main result deals with uniqueness. This involves the concept of the *Z-family* of a ring R, defined as the equivalence class of R with respect to Z-isoclinism, a new notion of isoclinism for rings that we introduce. Isomorphic rings are always Z-isoclinic but the converse fails: for instance, a ring R is always Z-isoclinic to the direct sum of R and a commutative ring.

There are existing notions of isoclinism for rings and Lie algebras (see [12, Chapter 3] and [16]), but Z-isoclinism is rather different in nature from these: it is built around additive group isomorphisms rather than ring isomorphisms. However, the two associated additive groups $R/Z(R)$ and $[R, R]$ of a ring R in a particular Z-family are nevertheless uniquely determined; here, $Z(R)$ is the center of R, and $[R, R]$ is the subgroup of $(R, +)$ generated by all commutators $[x, y] = xy - yx$.

Theorem 1.2. *The equation* $\Pr(R) = t$ *uniquely determines the Z-family of* $R \in S$*, where* S *is a class of finite rings, in both of the following situations:*

(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.*

The lower bounds for t in the above theorem are best possible. In fact, we have the following result at the endpoint value.

Theorem 1.3. *Suppose* p *is a prime. The equation* $\Pr(R) = \gamma_p$ *does not uniquely identify the Z-family of* R *among the class of* p*-rings. In fact, among all* p*-rings satisfying this equation, the total numbers of various types of equivalence classes are as follows: five Z-families of* R*, four* $R/Z(R)$ *group isomorphism types, and three* $[R, R]$ *group isomorphism types.*

After some preliminaries in Section 2, we develop a basic theory of Z-isoclinism in Section 3, and compare it with other notions of isoclinism. We also discuss a general ring construction which we use in particular to define a canonical form for rings associated with Z-isoclinism. Next, in Section 4, we discuss another ring construction which we call augmentation. Finally, we prove our main results in Section 5, where we also explicitly list the various Z-isoclinism and associated group isomorphism types that occur among p-rings R satisfying $\Pr(R) \geq \gamma_p$.

2. Preliminaries

We will briefly discuss nonassociative rings and Lie algebras in Section 3 but, unless so qualified, rings and algebras are assumed to be associative. We do not assume that rings are unital. We will occasionally make use of possibly nonassociative rings R, and we extend the definition of $\Pr(R)$ given in the introduction to this context in the obvious manner.

We use standard notation. Throughout this paragraph, R is a possibly nonassociative ring. $\mathbb{Z}_n$ 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. 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 $[x, y]$, $x, y \in R$, while R^2 is the possibly nonassociative subring of R

generated by the set of all pairwise products xy, $x, y \in R$. $C_R(x)$ is the centralizer of x in R. $R/Z(R)$ and $R/C_R(x)$ always refer to the relevant additive factor groups; we call $R/Z(R)$ the *central factor group of* R. We write $A \cong B$ when A and B are isomorphic (as groups, rings, or Lie algebras, depending on the context). We use the terms *monomorphism* and *epimorphism* in the algebraic sense, so they refer to homomorphisms that are injective or surjective, respectively.

We will need to deal with direct sums of rings, but also direct sums of abelian groups, and sometimes the groups involved in the latter are additive groups of associated rings. To distinguish between the two concepts, we write $A \oplus B$ for a direct sum of rings, and $A \boxplus B$ for a direct sum of abelian groups.

If R is the direct sum of subrings R_1 and R_2, then $\Pr(R) = \Pr(R_1)\Pr(R_2)$: this follows easily from the fact that two elements in a direct sum commute if and only if both pairs of summands commute. Thus $\mathfrak{R}$ is closed under products, and 0 is an accumulation point of $\mathfrak{R}$. Since a finite ring is a direct sum of rings of prime power order, 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. To understand the structure of $\mathfrak{R} \cap (a, 1]$ for any given $0 < a < 1$, it therefore suffices to understand $\mathfrak{R}_p \cap (a, 1]$ for all primes p. Thus in our search for elements of $\mathfrak{R}$, it suffices to examine only p-rings.

Observation 2.1. If $a, b, a', b' \in R$, with $a - a', b - b' \in Z(R)$, then $[a, b] = [a', b']$.

Thus we can view $[\cdot, \cdot]$ as a bilinear map from $(R/Z(R)) \times (R/Z(R))$ to R.

We now discuss the key role played by centralizers $C_R(x)$ in the calculation of $\Pr(R)$.

Observation 2.2. For each x in a ring R, the additive group $R/C_R(x)$ is isomorphic to $[x, R]$. In particular, if R is a $\mathbb{Z}_p$-algebra, then the dimension of $R/C_R(x)$ equals the dimension of $[x, R]$.

It follows easily from the definition of $\Pr(\cdot)$ that

$$\Pr(R) = \frac{1}{|R|^2} \sum_{x \in R} |C_R(x)| = \frac{1}{|R|} \sum_{x \in R} \frac{1}{|R/C_R(x)|}\,. \tag{2.1}$$

Note that $C_R(x) = C_R(x + z)$ for any $z \in Z(R)$. Consequently,

$$\Pr(R) = \frac{1}{|R/Z(R)|} \sum_{x + Z(R) \in R/Z(R)} \frac{1}{|R/C_R(x)|}\,, \tag{2.2}$$

where this last sum involves a term for a single representative x of each coset.

If R is a p-ring, it follows from (2.2) that

$$\Pr(R) = \frac{1}{|R/Z(R)|} \sum_{k=0}^{K} \frac{n_k}{p^k}$$

where n_k is the number of cosets $x + Z(R) \in R/Z(R)$ such that $|R/C_R(x)| = p^k$ and $|R/Z(R)| = p^K$. By Observation 2.2, this last equation for $\Pr(R)$ can be rewritten as:

$$\Pr(R) = \sum_{k=0}^{K} \frac{a_k(R)}{p^k}\,. \tag{2.3}$$

where we define $a_k(R)$ to be the proportion of cosets $x + Z(R) \in R/Z(R)$ such that $[x, R]$ has order p^k.

Lemma 2.3. *If R is a finite noncommutative ring, then $\Pr(R) > 1/|[R,R]|$. Moreover, both $N := |[R,R]| \cdot |R/Z(R)| \cdot \Pr(R)$ and $M := |R/Z(R)|^2 \Pr(R)$ are integers.*

Proof. Since $|[R,R]| \geq |[u,R]| = |R/C_R(u)|$ for all $u \in R$, the inequality $\Pr(R) \geq 1/|[R,R]|$ follows from (2.2). Equality would require that $|[R,R]| = |[u,R]|$ for all $u \in R$, but this fails when $u = 0$. To see that N is an integer, note that $[u,R]$ is a subgroup of $[R,R]$, and so $|R/C_R(u)|$ is a divisor of $|[R,R]|$ for all $u \in R$. Similarly, M is an integer because $R/C_R(u)$ is a factor group of $R/Z(R)$, and so $|R/C_R(u)|$ divides $|R/Z(R)|$. □

Remark 2.4. One might hope to reverse partially the inequality in Lemma 2.3 and prove that $\Pr(R) \leq f(|[R,R]|)$ for some $f : \mathbb{N} \to (0,1]$ such that $f(n) \to 0$ as $n \to \infty$. However, no such inequality is possible. To see this, we let R be the $\mathbb{Z}_p$-algebra with basis $\{u_0, u_1, \ldots, u_n, z_1, \ldots, z_n\}$, where the only nonzero products of basis elements are $u_0 u_i = z_i$ for $1 \leq i \leq n$, and $n \in \mathbb{N}$. Then $Z(R)$ has basis $\{z_1, \ldots, z_n\}$, $|R/Z(R)| = p^{n+1}$, and $|[R,R]| = p^n$. It is also clear that if $x = \sum_{i=0}^{n} x_i u_i$, where each $x_i \in \mathbb{Z}_p$, then $\dim R/C_R(x) = n$ if $x_0 \neq 0$, and $\dim R/C_R(x) = 1$ if $x_0 = 0$ but $x \neq 0$. Consequently,

$$\Pr(R) = \frac{p^{n+1} - p^n}{p^{(n+1)+n}} + \frac{p^n - 1}{p^{(n+1)+1}} + \frac{1}{p^{n+1}} = \frac{p^n + p^2 - 1}{p^{n+2}} > \frac{1}{p^2}\,.$$

(Note that the cases $n = 1, 2, 3$ of this example already give us rings with $\Pr(R) = \alpha_p, \beta_p, \gamma_p$, respectively.)

By the fundamental theorem of finitely generated groups, a finite abelian p-group $(A, +)$ can be decomposed as a direct sum $\boxplus_{i=1}^{m} C_{p^{k_i}}$ in essentially one way. This leads to the following definition.

Definition 2.5. If $(A, +)$ is a finite abelian p-group of the form $\boxplus_{i=1}^{m} C_{p^{k_i}}$ with more than one element, we denote its isomorphism type as $(k_1, k_2, \ldots, k_m; p)$, where each k_i is an integer and $k_1 \geq k_2 \geq \cdots \geq 1$. We define the *noncommutative type of a finite ring* R to be the isomorphism type of $R/Z(R)$, so if R is a p-ring and $|R| > 1$, we denote this type as $(k_1, k_2, \ldots, k_m; p)$.

Sometimes it will be useful to write the invariant factors k_i as "functions" which take a finite abelian p-group A or a p-ring R as a parameter, writing $k_i(A)$ or $k_i(R)$, $m(A)$ or $m(R)$, etc.

Lemma 2.6. *Let R be a nonabelian p-ring with $k := k_1(R)$. There exist elements $a, b \in R$ such that $p^{k-1}[a,b] \neq 0$. Consequently $m(R) \geq 2$ and $k_1(R) = k_2(R)$.*

Proof. Choose $a \in R$ such that $p^{k-1}a \notin Z(R)$. Then there exists $b \in R$ such that $p^{k-1}a$ does not commute with b, so $p^{k-1}[a,b] \neq 0$, and also a does not commute with $p^{k-1}b$. It follows that $a + Z(R)$ and $b + Z(R)$ generate distinct subgroups of $R/Z(R)$ of order p^k, and that they have trivial intersection. Thus $k_2(R) = k$. □

Suppose $(A,+)$ is an abelian group of order p^M for some M. We say that a set of elements $B = \{b_1, \ldots, b_N\}$ is linearly independent if all elements in the span of B can be written as a linear combination of elements of B in a "unique" way. By unique, we mean that if $\sum_{i=1}^N n_i b_i = \sum_{i=1}^N m_i b_i$, then $n_i b_i = m_i b_i$ for all $1 \leq i \leq N$. We say that $B = \{b_1, \ldots, b_N\}$ is a basis if it is linearly independent and it spans A. Equivalently, B is a basis if and only if A is an internal direct sum of the cyclic subgroups generated by each of the elements of B. Every finite abelian group has a basis, and in fact any linearly independent collection of elements of maximal order in such a group A is a subset of a basis: this follows by a straightforward modification of the proof of [10, Theorem 2.14.1].

Remark 2.7. It is readily verified that if $B = \{b_1, \ldots, b_N\}$ is a basis of a finite abelian p-group A and $B' = \{b'_1, \ldots, b'_N\}$ has the "lower triangular form" $b'_i = \sum_{j \leq i} c_{ij} b_j$ with every $c_{ij} \in \mathbb{N}$, then B' is also a basis as long as c_{ii} is not divisible by p, and p^k divides c_{ij} whenever $o(b_j) = p^k o(b_i)$ for some $k \in \mathbb{N}$; here $o(x)$ denotes the order of the element x.

An *ordered basis* just means a tuple $(b_1, \ldots, b_N)$ such that $\{b_1, \ldots, b_N\}$ is a basis.

Whenever p is a prime, we define a *p-value* to be any number in $\mathfrak{R}_p$, and a *value* is any number in $\mathfrak{R}$. Further, we call a p-value t a *small p-value* if $t \leq \gamma_p$, and we call it a *large p-value* otherwise, where γ_p is as in Theorem 1.1. A *large value* is a value larger than γ_2, and all other values are *small*. Thus the main results in the introduction give in particular all large p-values and all large values, and state that each such value is associated with a unique Z-family.

Let us now verify that α_p, β_p, and γ_p satisfy the inequalities mentioned in the introduction for $p \geq 2$. The inequalities $\beta_p \leq 1/p \leq \alpha_p$ are immediate. As for $\alpha_p^2 < \beta_p$, this amounts to the statement that $2p^4 - p^2 - (p^2+p-1)^2 > 0$, which follows by algebra:

$$2p^4 - p^2 - (p^2+p-1)^2 = p^4 - 2p^3 + 2p - 1 = (p-1)^2(p^2-1) > 0\,, \qquad p \geq 2\,.$$

Likewise, the inequality $\gamma_p < \alpha_p^2$ can be verified as follows:

$$(p^2+p-1)^2 - (p^4+p^3-p) = p^3 - p^2 - p + 1 = (p-1)(p^2-1) > 0\,, \qquad p \geq 2\,.$$

Remark 2.8. Throughout the paper, we allow rings to be non-unital. Perhaps surprisingly, however, there is no difference in the set of values in $\mathfrak{R}$ if we restrict to finite rings with unity. To see this, suppose $t = \Pr(R)$ for a possibly non-unital finite ring R. Choosing n such that $nx = 0$ for all $x \in R$, we can embed R in a unital ring R', where $(R',+)$ is the direct sum of R and $\mathbb{Z}_n$, and multiplication is defined by the rule $(i+r)(j+s) = ij + (is + jr + rs)$ whenever $i,j \in \mathbb{Z}_n$ and $r,s \in R$. Then it is readily verified that the additive groups $R'/C_{R'}(i+r)$ and $R/C_R(r)$ are isomorphic whenever $i \in \mathbb{Z}_n$, $r \in R$, and so (2.2) implies that $\Pr(R) = \Pr(R')$.

3. Isoclinism, joins, and Z-canonical form

In this section, we introduce the concept of Z-isoclinism, as mentioned in the introduction. This is analogous to the concept of isoclinism for groups introduced by Hall [8] and used widely in the literature of group theory; for more on group isoclinism, see for instance [1]. It was used to investigate the commuting probability of groups by Lescot [13]. There is also an existing concept

of isoclinism for rings and Lie algebras due to Kruse and Price [12] and Moneyhun [16], respectively, but these are different from Z-isoclinism, as we discuss below.

We also define a general method for constructing a noncommutative ring by "joining" two abelian groups via a "join function" or "join form" that suggests how we might define multiplication of elements in order to define canonical representatives of Z-families, and it will also be used later to construct various rings important to our arguments.

As motivation for the concept of Z-isoclinism, consider a finite ring S which is the direct sum of another ring R with some commutative ring. It follows from (2.2) that $\Pr(R) = \Pr(S)$. We would therefore like a relation that treats these two rings as being equivalent. Observation 2.2 and (2.2) suggest that such an equivalence should preserve the isomorphism type of both the central factor group and the commutator subgroup. However, even if rings R, S have isomorphic central factor groups and isomorphic commutator subgroups, it does not necessarily follow that $\Pr(R) = \Pr(S)$—see Propositions 4.6(c) and 4.7(b)—so we also need to preserve how elements of R (or $R/Z(R)$, in view of Observation 2.1) give rise to elements of $[R, R]$. This leads us to the following definition; in this definition, we are mostly interested in (associative) rings, but it is useful to employ the context of possibly nonassociative rings.

Definition 3.1. A pair of possibly nonassociative rings, R and S, are said to be *Z-isoclinic* if there are additive group isomorphisms $\phi : R/Z(R) \to S/Z(S)$ and $\psi : [R, R] \to [S, S]$ such that $\psi([u, v]) = [u', v']$ whenever $\phi(u + Z(R)) = u' + Z(S)$ and $\phi(v + Z(R)) = v' + Z(S)$. We call (ϕ, ψ) a *Z-isoclinism from R to S*.

$$\begin{array}{ccc} (R/Z(R))^{\otimes 2} & \xrightarrow[\cong]{\phi^{\otimes 2}} & (S/Z(S))^{\otimes 2} \\ \Big\downarrow{\scriptstyle [\cdot,\cdot]} & & \Big\downarrow{\scriptstyle [\cdot,\cdot]} \\ [R, R] & \xrightarrow[\cong]{\psi^{\otimes 2}} & [S, S] \end{array}$$

FIGURE 1. Z-isoclinism: horizontal maps are group isomorphisms

Equivalently, Definition 3.1 says that the diagram in Figure 1 commutes. Here the top spaces are tensor squares, and $[\cdot, \cdot]$ denotes the universal map from each tensor square induced by the bilinear commutator map (which is well-defined on $T/Z(T) \times T/Z(T)$, $T \in \{R, S\}$, by Observation 2.1).

The following result shows that $\Pr(\cdot)$ is a Z-isoclinic invariant, which mirrors the situation for groups.

Lemma 3.2. *If (ϕ, ψ) is a Z-isoclinism from one finite ring R to another S, then $[x, R]$ and $[x', S]$ are isomorphic whenever $x \in R$, $\phi(x + Z(R)) = x' + Z(S)$, and $\Pr(R) = \Pr(S)$.*

Proof. The desired isomorphism for any given $x \in R$ is simply $\psi' := \psi|_{[x,R]}$. Since ψ is an isomorphism, it is clear that ψ' is at least a monomorphism. Suppose $x \in R$ and $x', y' \in S$, with $\phi(x + Z(R)) = x' + Z(S)$. There exists $y \in R$ such that

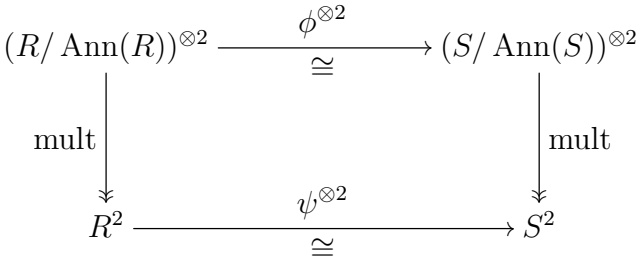

FIGURE 2. R- and G-isoclinism: horizontal maps are ring isomorphisms

$\phi(y + Z(R)) = y' + Z(S)$, and now $\psi'([x, y]) = [x', y']$. Thus $\psi' : [x, R] \to [x', S]$ is actually an isomorphism. The fact that $\Pr(R) = \Pr(S)$ now follows from Observation 2.2 and (2.2). □

We now pause to compare Z-isoclinism with other notions of isoclinism. It is best to begin by recasting Z-isoclinism as a special case of a more general type of isoclinism on possibly nonassociative rings. Suppose therefore that R is a possibly nonassociative ring, and let $\operatorname{Ann}(R)$ be the *two-sided annihilator of* R, i.e. the ideal of all $x \in R$ such that $xR = Rx = \{0\}$. Let $\operatorname{mult} : (R/\operatorname{Ann}(R))^{\otimes 2} \to R^2$ be the additive group epimorphism defined by $\operatorname{mult}(x \otimes y) = xy$. We say that two such possibly nonassociative rings R and S are *G-isoclinic* if Figure 2 is a commutative diagram with the horizontal maps being group isomorphisms. We say that R and S are *R-isoclinic* if in fact the horizontal maps are ring isomorphisms.

Note that Z-isoclinism for an (associative) ring R coincides with G-isoclinism for R_{Lie}, the Lie ring obtained from R by replacing the original multiplication of R by the commutator operation. Z- and G-isoclinism appear to be new concepts, but R-isoclinism has appeared previously, at least in special cases: Kruse and Price [12, Chapter 3] define it for (associative) rings and Moneyhun [16] defines it for Lie algebras. Note that G-isoclinism is a coarser notion than R-isoclinism, and so Z-isoclinism of rings R is a coarser notion than R-isoclinism of R_{Lie}.

We now compare and contrast the notions of group-, G-, and R-isoclinisms. To begin with, we list some basic properties of G- and R-isoclinisms that are natural analogues of the corresponding properties for group isoclinism; these properties *a fortiori* imply the corresponding properties for Z-isoclinism (where we change *possibly nonassociative ring* to *ring*, $\operatorname{Ann}(R)$ to $Z(R)$, and *null ring* to *commutative ring*).

Observation 3.3.

(a) G- and R-isoclinism are both equivalence relations on the class of all possibly nonassociative rings.
(b) Isomorphic possibly nonassociative rings are R-isoclinic (and so G-isoclinic): a ring isomorphism $\Phi : R \to S$ induces an R-isoclinism (ϕ, ψ), where $\phi : R/\operatorname{Ann}(R) \to S/\operatorname{Ann}(S)$ is a factor map of Φ, and $\psi = \Phi|_{R^2}$ is a restriction of Φ.
(c) R-isoclinic (and so also G-isoclinic) possibly nonassociative rings are not necessarily isomorphic: indeed, all null rings (meaning rings where all products are zero) are R-isoclinic.

(d) If R_i is G-isoclinic (or R-isoclinic) to S_i, $i = 1, 2$, then $R_1 \oplus R_2$ is G-isoclinic (or R-isoclinic, respectively) to $S_1 \oplus S_2$.

A *Z-family* is an equivalence classes of possibly nonassociative rings with respect to Z-isoclinism.

We now contrast the different sorts of isoclinism. The following example of a pair of Lie algebras that are G-isoclinic but not R-isoclinic is a useful starting point.

Example 3.4. Suppose R is the 2-dimensional $\mathbb{Z}_p$-algebra with basis $\{u, v\}$, where $xy = x$ for all choices of basis elements x, y, and suppose S is the 3-dimensional $\mathbb{Z}_p$-algebra with basis $\{u, v, z\}$, where the only nonzero product of basis elements is $uv = z$. Then $Z(R) = \{0\}$, $Z(S)$ has basis $\{z\}$, and so the monomorphism $\mu : R \to S$ defined by $\mu(iu + jv) = iu + jv$, $i, j \in \mathbb{Z}_p$, induces a group isomorphism $\phi : R/Z(R) \to S/Z(S)$. It can also be verified that μ induces a group isomorphism $[R, R] \to [S, S]$ (an isomorphism between these two groups of order p), and that (ϕ, ψ) is a Z-isoclinism from R to S, or equivalently (ϕ, ψ) is a G-isoclinism from R' to S', where these last two objects are the Lie rings associated with R and S, respectively. Note though that R' and S' are not R-isoclinic: in fact, $R'/\operatorname{Ann}(R')$ is isomorphic as a Lie algebra to R', whereas $S'/\operatorname{Ann}(S')$ is a commutative Lie algebra. (In this example, $[R', R']$ and $[S', S']$ are isomorphic as Lie algebras, but it is not hard to construct an example where that too fails.)

In the following result, R^{op} is the opposite (possibly nonassociative) ring, i.e. $(R, +)$ and $(R^{\mathrm{op}}, +)$ are the same group, while the multiplication $*$ of R^{op} is related to the multiplication $\cdot$ of R by the rule $x * y = y \cdot x$.

Proposition 3.5. *If R is a ring, then R is Z-isoclinic to R^{op}.*

Proof. By symmetry of their definitions, $Z(R) = Z(R^{\mathrm{op}})$ and $[R, R] = [R^{\mathrm{op}}, R^{\mathrm{op}}]$. Taking ϕ to be the identity map and $\psi(x) = -x$, we get the desired Z-isoclinism. □

Kruse and Price [12, p. 30] define the notion of a *stem ring* to be a ring R such that $R^2 \supset Z(R)$. Similarly Moneyhun [16] defines a *stem algebra* to be a Lie algebra L such that $[L, L] \supset Z(L)$. In both cases, they show that every finite ring (or Lie algebra) is R-isoclinic to a stem ring (or stem algebra) which, for an R-isoclinism family containing a finite order ring (or Lie algebra) can alternatively be defined as a ring (or Lie algebra) of minimal order. These statements are all direct analogues of what is true for stem groups and group isoclinism families that contain groups of finite order.

Kruse and Price [12, 3.2.7] further show that all algebras over a field F that lie in a single R-isoclinism family are R-isoclinic to the direct sum of some minimal dimension algebra and a null algebra. The corresponding result for Lie algebras was later proven by Moneyhun [16]. In particular, R-isoclinic stem algebras (either among associative algebras or Lie algebras) are isomorphic.

By contrast, if we were to define a Z-isoclinic stem ring to be a ring R with the property that $Z(R) \subset [R, R]$, then both R and S of Example 3.4 would be stem rings in the same Z-family even though they are not of the same order. Furthermore, it is well known that the two non-isomorphic noncommutative rings of order p^2 are this ring R and its opposite ring, so they both belong to the same Z-family by Proposition 3.5.

Note that the situation regarding groups is intermediate between that regarding R- and Z-isoclinism. On the one hand, stem groups can be defined as groups G such that $Z(G) \subset [G, G]$, and for finite groups this is consistent with being a group of minimal order in its isoclinism family. In particular if two stem groups are in the same isoclinism family and one is of finite order, then they are of the same order. On the other hand, there is no simple direct product characterization of isoclinism for finite groups. In fact, isoclinic stem groups are not necessarily isomorphic: it is well known that the two non-isomorphic nonabelian groups of order p^3 are isoclinic for any given prime p. Roughly speaking, we could say that R-isoclinism is much more restrictive than group isoclinism, which in turn is a little more restrictive than G-isoclinism (if it makes sense to compare groups and rings!).

Since the natural definition of a stem ring is not restrictive enough to tie down even the order of a ring in a Z-family of finite rings, we replace it by the following notion which at least achieves this much.

Definition 3.6. A ring R is said to have *Z-canonical form* if:

(a) $(R, +)$ is the internal direct sum of subgroups A_1 and A_2.
(b) $xy \in A_2$ for all $x, y \in R$, and $xy = 0$ if either x or y lies in A_2.
(c) $[R, R] = Z(R) = A_2$.

We say that a ring S is a *Z-canonical relative* of a ring R if R and S are Z-isoclinic and S has Z-canonical form. (It follows from (b) and (c) above that we also have $\mathrm{Ann}(R) = A_2$.)

Note that in Example 3.4, S is a Z-canonical relative of R. It is perhaps not immediately clear that every finite ring has a Z-canonical relative, but we will prove that this is so (Proposition 3.10). In fact, we will see that a ring R might have several (ring-isomorphism classes of) Z-canonical relatives (Example 3.13). However, the choice of Z-canonical relative will not be important for our analysis. In general, separating the central factor group and the commutator subgroup will greatly aid our analysis of $\mathfrak{R}$.

To prove that Z-canonical relatives always exist, we need a certain join construction which we now define.

Definition 3.7. Suppose we have the following data:

(a) A pair of abelian groups $(A_1, +)$ and $(A_2, +)$.
(b) A *join form* $J : A_1 \times A_1 \to A_2$ which is bilinear over $\mathbb{Z}$.

We define the ring $R = \mathrm{Join}(A_1, A_2, J)$ as follows. First, $(R, +)$ is the (internal) direct sum $A_1 \boxplus A_2$. Multiplication in R is defined by the following equations and distributivity:

(a) $xy = J(x, y)$ if $x, y \in A_1$.
(b) $xy = yx = 0$ if $x \in A_2$ and $y \in R$.

Note that in the above definition, associativity of R is trivial since all triple products are zero. Distributivity follows readily from the bilinearity of J.

When R is finitely generated, we can replace the join form J by a multiplication defined only on basis elements.

Definition 3.8. Suppose we have the following data:

(a) A pair of abelian groups $(A_1, +)$ and $(A_2, +)$.
(b) A basis $B = \{b_1, \ldots, b_N\}$ of A_1.

(c) A *join function* $f : B \times B \to A_2$ such that $|f(b, b')|_2$ divides both $|b|_1$ and $|b'|_1$, where $|x|_k$ denotes the order of $x \in A_k$, $k = 1, 2$ (and all orders divide infinity).

Then $\mathrm{join}(A_1, A_2, B, f) = \mathrm{Join}(A_1, A_2, J)$, where $J : A_1 \times A_1 \to A_2$ is defined by

$$J\left(\sum_{i=1}^{N} x_i b_i,\ \sum_{j=1}^{N} y_j b_j\right) = \sum_{i,j=1}^{N} x_i y_j f(b_i, b_j)\,, \qquad \text{where } x_i, y_j \in \mathbb{Z}\,.$$

It is a routine matter to verify that J is bilinear over $\mathbb{Z}$.

Observation 3.9. Let $R = \mathrm{join}(A_1, A_2, B, f)$, as above. Then:

(a) $Z(R)$ consists of all elements of the form $z + x$, where $x \in A_2$, and $z \in A_1$ is any element that commutes in R with all elements of A_1.
(b) $[b, b'] = f(b, b') - f(b', b)$ for $b, b' \in B$.
(c) $[R, R]$ is the subgroup of A_2 generated by $[b, b']$, $b, b' \in B$.

Our first use of the join construction is to prove that Z-canonical relatives often exist. Below and in later sections, we at times slightly abuse terminology by saying that $\{r_1, \ldots, r_m\} \subset R$ is a *basis of* $R/Z(R)$ when we mean that $\{r_1 + Z(R), \ldots, r_m + Z(R)\} \subset R/Z(R)$ is a basis of $R/Z(R)$.

Proposition 3.10. *A ring R has a Z-canonical relative if either*

(a) *the factor group $R/Z(R)$ is finitely generated, or*
(b) *$g(x) := 2x$ defines a (group) automorphism of $[R, R]$.*

Proof. We first prove (a). Let $B := (b_1, \ldots, b_N) \in R^N$ be a finite ordered basis of coset representatives of $A_1 := R/Z(R)$. Let $A_2 := [R, R]$. Define $f(b_i, b_j) = c_{ij} := [b_i, b_j]$ if $i < j$, and $f(b_i, b_j) = 0$ otherwise. It is readily verified that $\mathrm{join}(A_1, A_2, B, f)$ is a Z-canonical relative of R. We write $\mathrm{Can}(R; B)$ for $\mathrm{join}(A_1, A_2, B, f)$ in this construction. Note that the consistency condition follows from the basic properties of R.

We now prove (b). Let $A_1 = R/Z(R)$ and $A_2 = [R, R]$. Let $J : A_1 \times A_1 \to A_2$ be defined by $J(u + Z(R), v + Z(R)) = [u, v]$ for all $u, v \in R$: this is well defined by Observation 2.1, and is bilinear over $\mathbb{Z}$. Let $S = \mathrm{Join}(A_1, A_2, J)$. Using Observation 3.9(a) and the fact that g is injective, it is straightforward to verify that $Z(S) = A_2$, so we can identify the abelian groups $S/Z(S)$ and $R/Z(R)$. It is also clear that $[S, S] = 2A_2 = [R, R]$. Taking ϕ to be the identity map on $R/Z(R)$, and ψ to be g, we see that R is Z-isoclinic to S. It follows readily that S is a Z-canonical relative of R. □

Note that any canonical relative S of a finite ring R is a member of the Z-isoclinism class of R with "reasonably small" order. Indeed, Z-isoclinism preserves the group isomorphism types of the central factor group $R/Z(R)$ and of the commutator subgroup $[R, R]$, so a given finite ring R determines the order of its Z-canonical relatives: $|S| = |R/Z(R)| \cdot |[R, R]|$. Thus $|S| \le |R|$ if and only if $|[R, R]| \le |Z(R)|$.

It is now easy to deduce the following analogue for Z-isoclinism of a result for isoclinism of groups [2, Proposition 2.10].

Corollary 3.11. *The following are equivalent for a ring R:*

(a) *R has a finite Z-canonical relative.*
(b) *R is Z-isoclinic to a finite ring;*

(c) $R/Z(R)$ *is finite;*

Proof. It is trivial that (a) implies (b). If R is Z-isoclinic to a finite ring S, then $R/Z(R) \cong S/Z(S)$, so certainly $R/Z(R)$ is finite. Thus (b) implies (c). Finally, suppose (c) holds. By Observation 2.1, R contains only finitely many commutators. Since $[R, R]$ consists of all finite sums of commutators, this also is of finite size. By Proposition 3.10, R has a Z-canonical relative, and it has order $|R/Z(R)| \cdot |[R, R]|$. Thus (c) implies (a). □

Observation 3.12. If $R/Z(R)$ is a vector space over $\mathbb{Z}_p$, and S is a canonical relative of R, then S is a $\mathbb{Z}_p$-algebra.

Z-canonical relatives S of a ring R are quite closely related. Not only are they all in the same Z-family, but they also have features that set them apart from most members of this Z-family: they satisfy the nilpotency condition $S^3 = 0$, and they satisfy $[S, S] = Z(S)$. However, the following example shows that the isomorphism type of a Z-canonical relative of a ring R is not uniquely determined.

Example 3.13. Suppose A_1 is a $\mathbb{Z}_p$-vector space with ordered basis $B := (u_0, \ldots, u_n)$, and A_2 a $\mathbb{Z}_p$-vector space with basis $\{z_1, \ldots, z_n\}$. Let $f(u_0, u_j) = z_j$ for $1 \le j \le n$, and $f(u_i, u_j) = 0$ for all other pairs (i, j). Defining $R := \mathrm{join}(A_1, A_2, B, f)$, we can identify $R/Z(R)$ with A_1, and $Z(R)$ with A_2. Next let $R_j := \mathrm{Can}(R; B_j)$ for $0 \le j \le n$, where $B_j := (u_1, \ldots, u_j, u_0, u_{j+1}, \ldots, u_n)$ and $\mathrm{Can}(R; B_j)$ is in the proof of Proposition 3.10(a). We write $\cdot_j$ for the multiplication of R_j to distinguish distinct multiplications. Then

(a) $R = R_0$, and $(R_j, +)$ is the same group for all $0 \le j \le n$.
(b) The commutator of x and y in R_j is independent of j, so we denote it by $[x, y]$ in all cases.
(c) Defining the subset S of R_j to consist of all $u = z + \sum_{i=0}^{n} c_i u_i$ such that $z \in A_2$ and $c_i \in \mathbb{Z}_p$ for all i with $c_0 \neq 0$, we see that S has the following isomorphism-invariant property: $\dim[x, R_j] = n$ for $x \in S$ and $\dim[x, R_j] = 1$ otherwise.

Because of the form of S, the right ideal $x \cdot_j R_j$ contains $\mathrm{span}\{z_{j+1}, \ldots, z_n\}$, and so has dimension at least $n - j$ for all $x \in S$. Furthermore this minimum is achieved for $x = x_0$. Thus $m_j := \min\{\dim x \cdot_j R_j \mid x \in S\}$ equals $n - j$ for each $0 \le j \le n$. Since S is defined by an isomorphism-invariant property, the number m_j is also isomorphism invariant. It follows that no two of the Z-canonical relatives R_j of R are isomorphic.

We now use Z-isoclinism to define a weaker notion of decomposability for p-rings.

Definition 3.14. A ring is said to be *decomposable* if it can be written as a direct sum of two nontrivial rings, and *Z-decomposable* if it is Z-isoclinic to a ring that can be written as a direct sum of two noncommutative rings. We use the terms *indecomposable* and *Z-indecomposable* to refer to rings where these conditions fail.

Since $\Pr(R)$ is a Z-isoclinism invariant, it follows that if a finite ring R is Z-decomposable with R being Z-isoclinic to $R_1 \oplus R_2$, then $\Pr(R) = \Pr(R_1) \Pr(R_2)$. To characterize all p-values no less than γ_p, it therefore suffices to characterize $\Pr(R)$ for all Z-indecomposable p-rings R.

Lemma 3.15. *A finitely generated ring R is Z-decomposable if and only if it has a Z-canonical relative S of the form $S = S_1 \oplus S_2$, where S_1, S_2 are both noncommutative.*

Proof. Suppose that R is Z-isoclinic to $R_1 \oplus R_2$, where R_1, R_2 are noncommutative. By Observation 3.3(d), R is Z-isoclinic to $S := S_1 \oplus S_2$, where S_i is a Z-canonical relative of R_i, $i = 1, 2$. It readily follows that S is a Z-canonical relative of R, as desired. The converse is trivial. □

It is tempting to conjecture that perhaps all Z-canonical relatives of a Z-decomposable ring R can be decomposed as direct sums of noncommutative rings. However, this is false.

Proposition 3.16. *There exists a ring in Z-canonical form which is Z-decomposable, but cannot itself be decomposed as a direct sum of two noncommutative rings.*

Proof. Suppose p is a prime. Consider the $\mathbb{Z}_p$-algebra R with basis

$$B = \{u_1, u_2, u_3, u_4, z_{13}, z_{24}\},$$

where the only nonzero products of basis elements are $u_1u_3 = z_{13}$ and $u_2u_4 = z_{24}$. Then R is in Z-canonical form and it is Z-decomposable: in fact $R = R_1 \oplus R_2$, where R_i is the noncommutative ring generated by u_i and u_{i+2}, $i = 1, 2$.

Let S be the $\mathbb{Z}_p$-algebra S with the same basis B as above, but now the only nonzero products of basis elements are $u_1u_3 = z_{13}$ and $u_2u_4 = u_1^2 = z_{24}$. Certainly S is in Z-canonical form, and it is readily verified that S is Z-isoclinic to R, using identity maps for both ϕ and ψ in Definition 3.1. We claim that S is not decomposable as a direct sum of two noncommutative rings.

Suppose for the sake of contradiction that $S = S_1 \oplus S_2$, where S_1, S_2 are noncommutative ideals of S. Let Z be the ideal with basis $\{z_{13}, z_{24}\}$. We write a general element of S in the form $x = z_x + \sum_{i=1}^{4} x_i u_i$, where $x_i \in \mathbb{Z}_p$ and $z_x \in Z$. Suppose without loss of generality that S_1 contains some x with $x_1 \neq 0$. Then $xu_1 = x_1 z_{24}$ and $xu_3 = x_1 z_{13}$ both lie in S_1, so S_1 contains Z. Since $S_1 \cap S_2 = \{0\}$ and $[S, S] = Z$, this forces S_2 to be commutative, giving the required contradiction. □

4. Augmentation

In this section, we study a construction that we call augmentation. We are interested in this mainly for (associative) rings but, in the absence of an added assumption (see below), the augmentation of an (associative) ring might be nonassociative. Since we want to repeatedly augment a ring, it is therefore best to develop the theory in the context of possibly nonassociative rings.

Whenever R is a possibly nonassociative ring, and $c \in [R, R]$ is an element of order p, we define the *p-augmentation R' of R (via c)* to be a specific possibly noncommutative ring of order $p^2|R|$. Addition in R' is defined by the requirement that $(R', +)$ is a direct sum of $(R, +)$ and $(T, +)$, where $(T, +)$ equals $C_p \boxplus C_p$. To define multiplication in R', we view R as being embedded in R' and write a general element of R' as $iu + jv + r$, where $r \in R$, u, v are the basis elements of T, and $i, j \in \mathbb{Z}_p$. We multiply elements in $R \subset R'$ as in the original ring R, define $ur = ru = vr = rv = 0$ for all $r \in R$, and define $uv = c$, $vu = 0$. Multiplication can now be extended to all of R' by distributivity.

Clearly the p-augmentation R' of a finite possibly nonassociative ring R via c is a possibly nonassociative ring of order $p^2|R|$. If in fact R is a ring and

$c \in [R,R] \cap \mathrm{Ann}(R)$, then R' is also an (associative) ring. To prove associativity, we first use distributivity to reduce the required proof to a proof that $(xy)z = x(yz)$ for all $x, y, z \in R \cup S$, where $S := \{u, v\}$. Assume therefore that $x, y, z \in R \cup S$. If $x, y, z \in R$, then the desired equation follows from associativity of R. In all remaining cases, we claim that $(xy)z = x(yz) = 0$. Let us denote either $(xy)z$ or $x(yz)$ as t, and so t equals either ab or ba, where a is a parenthesized product (either xy or yz) and b is the remaining factor (either z or x). Now $a \in R$ for all $x, y, z \in R \cup S$, so $t = 0$ if $b \in S$. If instead $b \in R$, and one of the factors of a lies in S, then $a \in \{0, c\} \subset \mathrm{Ann}(R)$, and again $t = 0$. The claim is proved.

An equivalent way of defining the above p-augmentation R', assuming $c \in [R,R] \cap \mathrm{Ann}(R)$, is to write $R' := (R \oplus S)/I$, where S is the three-dimensional $\mathbb{Z}_p$-algebra S with basis $\{u, v, z\}$ in which the only nonzero product of basis elements is $uv = z$, and I is the ideal generated by $z - c$. If we also assume that R is in Z-canonical form, then $c \in Z(R)$, and it becomes clear that this is a rather special ring theoretic analogue of a central product in group theory. A reasonable general ring theoretic analogue of a central product would be $(R \oplus S)/I$, where R, S are arbitrary Z-canonical form rings and I is an arbitrary ideal defined by identifying two isomorphic central additive subgroups of R and S (which are necessarily ideals because of the Z-canonical form). However, we do not require such a general "central sum", and we look only at the special case of augmentations.

A *p-augmented ring* is any ring that is a p-augmentation of some other ring. A ring is *augmented* if it is p-augmented for some p, and otherwise it is *unaugmented*. A ring is *Z-augmented* if it is Z-isoclinic to an augmented ring, and otherwise we say that R is *Z-unaugmented*.

We write $R' = \mathrm{Aug}_p(R, c)$ if R' is the p-augmentation of R via c. For $n \in \mathbb{N}$, we write $R_n = \mathrm{Aug}_p^n(R, c)$ if R_n is the n-fold p-augmentation of R via c, meaning that R_n is defined by the equations $R_0 = R$ and $R_i = \mathrm{Aug}_p(R_{i-1}, c)$ for $1 \leq i \leq n$.

We now record some properties of augmentation; for these, we assume that $R' = \mathrm{Aug}_p(R, c)$ and $S' = \mathrm{Aug}_p(S, d)$ are p-augmentations of rings R and S.

Observation 4.1.

(a) $R'/Z(R')$ can be identified naturally with $(R/Z(R)) \boxplus T$, and so is isomorphic to the direct sum $(R/Z(R)) \boxplus C_p \boxplus C_p$.
(b) $[R', R']$ is isomorphic to $[R, R]$.
(c) If $\phi : R \to S$ is a ring isomorphism and $\phi(c) = d$, then R' and S' are also isomorphic.
(d) If (ϕ, ψ) is a Z-isoclinism from R to S such that $\psi(c) = d$, then R' and S' are Z-isoclinic.
(e) The isomorphism type of $\mathrm{Aug}_p(R, c)$ remains unchanged if we change the basis $\{u, v\}$ of T, or if we replace c by ic, $i \in \mathbb{Z}_p^*$.
(f) If R is a Z-canonical form ring, then so is R'.

Parts (a)–(c) above are rather obvious, so we leave the verifications to the reader. We now prove (d). Let us assume that (ϕ, ψ) is a Z-isoclinism from R to S. Writing general elements x_1, x_2 of R' in the form $x_i = r_i + t_i$, where $r_i \in R$ and $t_i \in T$, we define the Z-isoclinism (Φ, Ψ) from R' to S' by the equations $\Phi(x_i + Z(R')) = \phi(r_i + Z(R)) + t_i$ and $\Psi([x_1, x_2]) = \psi([r_1, r_2]) + [t_1, t_2]$. Note that on the right-hand side of these equations, each t_i is to be interpreted as an element of $\{0\} \boxplus T \subset S'$ and $[t_1, t_2]$ is given by the augmentation process in S'.

We leave to the reader the verification that (Φ, Ψ) is indeed a Z-isoclinism. The first part of (e) follows because any change of basis induces an automorphism of T, while the isomorphism from $\mathrm{Aug}_p(R, c)$ to $\mathrm{Aug}_p(R, ic)$ is a consequence of the T-automorphism $f(au + bv) = aiu + bv$, $a, b \in \mathbb{Z}_p$. Finally, it is clear that if R has Z-canonical form with data (A_1, A_2), as in Definition 3.6, then R' has Z-canonical form with data isomorphic to $(A_1 \boxplus C_p \boxplus C_p, A_2)$.

Despite Observation 4.1(e), and the fact that $R'/Z(R')$ and $[R', R']$ are independent of c, we will see in Proposition 4.6 that the p-augmentation $R' := \mathrm{Aug}_p(R, c)$ may depend on the choice of c. Indeed, by changing c, we can change not only the ring-isomorphism class of R', but also its Z-family and the value of $\Pr(R')$.

We will use augmentation to create rings with new commuting probabilities from rings with a given commuting probability. Since $\Pr(R)$ is a Z-isoclinic invariant (Lemma 3.2), and since augmentation interacts well with isoclinism (Observation 4.1(d)), we get the same new commuting probabilities whether we augment R or one of its Z-isoclinic relatives S. Since a finite ring is Z-isoclinic to a Z-canonical form ring (Proposition 3.10), it follows that if we want to find all commuting probabilities of rings that can be obtained from any given class $\mathcal{C}$ of finite rings, and if all finite rings isoclinic to $R \in \mathcal{C}$ also lie in $\mathcal{C}$, then it suffices to consider augmentations of Z-canonical form rings $R \in \mathcal{C}$. Note that, since $[R, R] = \mathrm{Ann}(R)$ in a Z-canonical form ring, using only such rings ensures that all p-augmentations are associative.

We call a number $t \in \mathfrak{R}$ an *augmented* or an *unaugmented value* if $t = \Pr(R)$ for an augmented or an unaugmented ring R, respectively; a value could potentially be both augmented and unaugmented. Once we discover an unaugmented value $t = \Pr(R)$, where R is a Z-canonical form ring with a commutator of order p, we get a sequence of associated augmented values in $\mathfrak{R}$ by repeatedly p-augmenting R. This process depends on R and c, not just on t. To get a formula for $\Pr(\mathrm{Aug}_p(R, c))$, we first define

$$\Pr_c^+(R) = \frac{1}{|R|} \sum_{\substack{x \in R \\ c \in [x,R]}} \frac{1}{|R/C_R(x)|}\,,$$

$$\Pr_c^-(R) = \frac{1}{|R|} \sum_{\substack{x \in R \\ c \notin [x,R]}} \frac{1}{|R/C_R(x)|}\,,$$

Note that $\Pr(R) = \Pr_c^+(R) + \Pr_c^-(R)$. Also $\Pr_c^+(R) > 0$ (since $c = [x, y]$ for some $x, y \in R$) and $\Pr_c^-(R) > 0$ (since $c \notin [0, R]$).

Lemma 4.2. *Suppose R is a finite possibly nonassociative ring, and let $R_n := \mathrm{Aug}_p^n(R, c)$, where $n \in \mathbb{N}$ and $c \in R$ is a commutator of order p. Then*

$$\Pr(R_n) = \Pr_c^+(R) + \frac{(p^{2n} + p - 1)\Pr_c^-(R)}{p^{2n+1}}\,. \tag{4.1}$$

This sequence of values is strictly decreasing, with positive limit $\Pr_c^+(R) + \Pr_c^-(R)/p$, as $n \to \infty$.

Proof. Throughout this proof, we write $(R_n, +) = W \boxplus R$, where W is the direct sum of $2n$ copies of C_p. Letting e_i be a generator of the ith copy of C_p in W, we assume that these basis elements are ordered so that $\{e_1, e_2\}$ is a basis of what

we called $(T,+)$ for the first augmentation, $\{e_3,e_4\}$ is a basis of $(T,+)$ for the second augmentation, etc. Thus $e_{2i-1}e_{2i}=c$ for all $1\le i\le n$.

We write a general element $x\in R_n$ as $x=w+r$, where $w\in W$ and $r\in R$. Now $[x,R_n]$ contains c whenever $w\neq 0$. Indeed, if $w=\sum_{i=1}^{2n} w_ie_i$, where $w_i\in\mathbb{Z}_p$, and $w_j\neq 0$ for some $1\le j\le 2n$, then either $[x,e_{j+1}]$ or $[x,e_{j-1}]$ is a nonzero multiple of c, depending on whether j is odd or even, respectively. It is similarly clear that $[x,R_n]$ contains $[r,R]$, and hence that $[x,R_n]$ is generated as an additive group by $[r,R]$ and c when $w\neq 0$. It is also clear that $[x,R_n]=[r,R]$ when $w=0$.

We now fix $r\in R$, and let x range over all elements of the form $w+r$, $w\in W$. Suppose first that $c\in[r,R]$. For all such x, we have

$$|R_n/C_{R_n}(x)| = |[x,R_n]| = |[r,R]| = |R/C_R(r)|\,,$$

and so the contribution to $\Pr(R_n)$ corresponding to this r is the same as its contribution to $\Pr(R)$ because the single term in (2.1) for $r\in R$ has been replaced by p^{2n} equal terms for $x\in R_n$, a change that compensates exactly for the fact that we now multiply our sum by $1/|R_n| = p^{-2n}(1/|R|)$.

Suppose instead that $c\notin[r,R]$. For $p^{2n}-1$ of p^{2n} possible elements $x=w+r\in R_n$, we see that $|R_n/C_{R_n}(x)| = p|R/C_R(r)|$. For the remaining element, $|R_n/C_{R_n}(x)| = |R/C_R(r)|$. Thus the contribution to $\Pr(R_n)$ corresponding to r is a times the corresponding contribution towards $\Pr(R)$, where

$$a=\frac{p^{2n}-1}{p^{2n+1}}+\frac{1}{p^{2n}}=\frac{p^{2n}+p-1}{p^{2n+1}}\,.$$

Summing the contributions towards $\Pr(R_n)$ above separately over all $r\in R$ for which $c\in[x,R]$, and over all $r\in R$ for which $c\notin[x,R]$, we get (4.1). Finally, the limit statement is clear. □

Corollary 4.3. *Suppose R is a finite possibly nonassociative ring, and suppose $R_n=\mathrm{Aug}_p^n(R,c)$, where $n\in\mathbb{N}$ and $c\in R$ is a commutator of order p. Then*

$$\Pr(R_n)\le\Pr(R)-\left(1-\frac{p^{2n}+p-1}{p^{2n+1}}\right)a_0(R)\,, \tag{4.2}$$

where $a_0(R)=1/|R/Z(R)|$, with equality if and only if $c\in[x,R]$ for all $x\in R\setminus Z(R)$. The upper bound in (4.2) is strictly decreasing to the positive limit $\Pr(R)-(p-1)a_0(R)/p$ as $n\to\infty$.

Proof. Note that $\Pr_c^-(R)\ge a_0(R)$, so (4.2) follows immediately from (4.1). The condition for equality is equally clear, as is the limit statement; note that positivity of the limit follows from positivity of the limit in Lemma 4.2. □

An important special case of augmentation is when $[R,R]$ is of order p. In this case, we omit c from our notation and terminology because it follows from Observation 4.1(e) that the choice of c is unimportant. We also obtain the following special case of Corollary 4.3.

Corollary 4.4. *Suppose R is a finite possibly nonassociative ring and that $[R,R]$ is of order p. Writing $R_n=\mathrm{Aug}_p^n(R)$, $n\in\mathbb{N}$, and $a_0(R)=1/|R/Z(R)|$, we have*

$$\Pr(R_n)=\Pr(R)-\left(1-\frac{p^{2n}+p-1}{p^{2n+1}}\right)a_0(R)\,, \tag{4.3}$$

Thus $\Pr(R_n)$ decreases to the positive limit $\Pr(R)-(p-1)a_0(R)/p$ as $n\to\infty$.

Once we find all the unaugmented large p-values, and we understand the structure of the associated rings, we can use Lemma 4.2 or one of its corollaries to gain information about all augmented large p-values. Consequently, we may restrict our attention initially to unaugmented rings in Z-canonical form if we wish.

It remains to give examples showing that for $R' = \mathrm{Pr}(\mathrm{Aug}_p(R, c))$, $\mathrm{Pr}(R')$ may depend on the chosen c. Because of Lemma 3.2, such examples automatically imply that the Z-isoclinism class of R' may also depend on c. The following ring, which will be important later, is one where there is no such dependence, but we will use it to construct an example where there is such dependence.

Example 4.5. Let $R = \mathrm{join}(A_1, A_2, B, f)$, where A_1 is a vector space over $\mathbb{Z}_p$ with ordered basis $B := (u_1, u_2, u_3)$, A_2 is a vector space over $\mathbb{Z}_p$ with basis $\{c_{12}, c_{23}\}$, and f is the join function defined by $f(u_1, u_2) = c_{12}$, $f(u_2, u_3) = c_{23}$, and $f(u_i, u_j) = 0$ otherwise. As usual, we view $\{u_1, u_2, u_3\}$ as being a basis of $R/Z(R)$. Examining the p^3 representatives $x = \sum_{i=1}^{3} x_i u_i$ of $R/Z(R)$, where $x_i \in \mathbb{Z}_p$ for $i = 1, 2, 3$, we see that $[x, R] = [R, R]$ is two-dimensional for the $p^3 - p^2$ elements with $x_2 \neq 0$. For the remaining $p^2 - 1$ nonzero representatives, $[x, R]$ is one-dimensional, and each of the $p + 1$ one-dimensional subspaces of $[R, R] = A_2$ occurs for $p - 1$ of these representatives. Finally, $[0, R]$ is zero-dimensional. It follows that, regardless of the choice of nonzero commutator c, we have $\mathrm{Pr}_c^+(R) = (p^2 - 1)/p^4$ and $\mathrm{Pr}_c^-(R) = 1/p^2$. Applying Lemma 4.2, we see that if $R_1 := \mathrm{Aug}_p(R, c)$, then

$$\mathrm{Pr}(R_1) = \frac{p^2 - 1}{p^4} + \frac{p^2 + p - 1}{p^5} = \frac{p^3 + p^2 - 1}{p^5} = \gamma_p\,, \tag{4.4}$$

Augmentation was independent of c in the above example because R was symmetrical with respect to all nonzero commutators. However, augmentation breaks this symmetry so if we carry out a second augmentation via d, it matters whether or not $d \in \mathrm{span}\{c\}$, as we now see.

Proposition 4.6. *Suppose R, p are as in Example 4.5, and let c, d be nonzero commutators in R. Let $R_i := \mathrm{Aug}_p^i(R, c)$ and let $R_{1,1} := \mathrm{Aug}_p(R_1, d)$.*

(a) *R_2 and $R_{1,1}$ have isomorphic central factor groups and isomorphic commutator subgroups.*
(b) *R_2 and $R_{1,1}$ are Z-isoclinic, and even isomorphic, if $d = ic$ for some $i \in \mathbb{Z}_p^*$*
(c) *If $\dim \mathrm{span}\{c, d\} = 2$, then R_2 and $R_{1,1}$ are not Z-isoclinic. Moreover, $\mathrm{Pr}(R_{1,1}) < \mathrm{Pr}(R_2)$.*

Proof. Parts (a) and (b) follow immediately from parts (a), (b) and (e) of Observation 4.1.

It remains to prove (c), so we assume that $\dim \mathrm{span}\{c, d\} = 2$. It suffices to prove that $\mathrm{Pr}(R_{1,1}) < \mathrm{Pr}(R_2)$, since this implies that $R_{1,1}$ and R_2 cannot be Z-isoclinic. By the analysis of Example 4.5, Lemma 4.2 implies that

$$\mathrm{Pr}(R_2) = \frac{p^2 - 1}{p^4} + \frac{p^4 + p - 1}{p^7} = \frac{p^5 + p^4 - p^3 + p - 1}{p^7}\,.$$

Let (u_1, u_2, u_3) be the ordered basis of A_1 used to construct R, and let $\{u_4, u_5\}$ be a basis of the copy of T used to construct R_1 from R. The only nonzero products of

elements of $\{u_1, \ldots, u_5\}$ are $u_1u_2 = c_{12}$, $u_2u_3 = c_{23}$, and $u_4u_5 = c \in \operatorname{span}\{c_{12}, c_{23}\}$. We identify R with the subring $R \oplus \{0\}$ of R_1.

Note that $\dim[R_{1,1}, R_{1,1}] = \dim[R, R] = 2$. In order to compute $\Pr(R_{1,1})$, we first compute $\Pr_d^+(R_1)$, which we rewrite as an average over cosets as we did for the definition of $\Pr(R)$:

$$\Pr_d^+(R_1) = \frac{1}{|R_1/Z(R_1)|} \sum_{\substack{x+Z(R_1) \in R_1/Z(R_1) \\ d \in [x, R_1]}} \frac{1}{|R_1/C_{R_1}(x)|}\,, \tag{4.5}$$

It suffices to sum over elements of the form $x = \sum_{i=1}^5 x_i u_i$, where $x_i \in \mathbb{Z}_p$ for all i, since there is one such element in each coset of $Z(R_1) = A_2$. We also write $x = X_1 + X_2$, where $X_1 = \sum_{i=1}^3 x_i u_i$ and $X_2 = \sum_{i=4}^5 x_i u_i$.

As in the proof of Lemma 4.2, $[x, R_1]$ is the subspace of R_1 generated by $[x, R] = [X_1, R]$, and possibly c: we include c as a generator exactly when $X_2 \neq 0$. We break the sum in (4.5) into three pieces. First, there are those elements with $\dim[x, R] = 2$: this condition corresponds exactly to the inequality $x_2 \neq 0$. Then $d \in [x, R] \subset [x, R_1]$ irrespective of the other coefficients, so these elements give a contribution of $(p^5 - p^4)/p^{5+2}$ to $\Pr_d^+(R_1)$. Next, there are the elements with $\dim[x, R] = 1$ but $\dim[x, R_1] = 2$. This happens when the following two conditions are satisfied:

- $[x, R]$ is any one-dimensional subspace of A_2 other than the one containing c (as happens for $p(p-1)$ choices of X_1);
- $X_2 \neq 0$ (as happens for $p^2 - 1$ choices of X_2).

Thus these elements give a contribution of $p(p-1)(p^2-1)/p^{5+2}$ to $\Pr_d^+(R_1)$. Finally, there are those elements x such that $d \in [x, R]$ and $\dim[x, R] = 1 = \dim[x, R_1]$. This happens for $p-1$ choices of X_1 and one choice of X_2, so these elements give a contribution of $(p-1)/p^{5+1}$ to $\Pr_d^+(R_1)$. Summing the contributions, we get

$$\Pr_d^+(R_1) = \frac{(p^5 - p^4) + (p^4 - p^3 - p^2 + p) + (p^2 - p)}{p^7} = \frac{p^2 - 1}{p^4}\,.$$

Combining this equation with (4.4), we get

$$\Pr_d^-(R_1) = \frac{p^3 + p^2 - 1}{p^5} - \frac{p^2 - 1}{p^4} = \frac{p^2 + p - 1}{p^5}\,.$$

Now using (4.1), we deduce that

$$\Pr(R_{1,1}) = \frac{p^2 - 1}{p^4} + \frac{(p^2 + p - 1)^2}{p^8} = \frac{p^6 + 2p^3 - p^2 - 2p + 1}{p^8}\,.$$

Finally,

$$\begin{aligned}\Pr(R_2) - \Pr(R_{1,1}) &= \frac{(p^6 + p^5 - p^4 + p^2 - p) - (p^6 + 2p^3 - p^2 - 2p + 1)}{p^8} \\ &= \frac{(p-1)^3(p+1)^2}{p^8}\,,\end{aligned}$$

which is positive for all primes p. Since R_2 and $R_{1,1}$ have different commuting probabilities, they cannot be Z-isoclinic. □

We give one more example which will be important later.

Proposition 4.7. *Suppose the ring R can be written in the form $S \oplus S$, where S is the Z-canonical form $\mathbb{Z}_p$-algebra with basis $\{u, v, z\}$, in which the only nonzero product of basis elements is $uv = z$. Let $R' := \mathrm{Aug}_p(R, c)$ for some nonzero $c \in [R, R]$, and let us write $c = c_1 + c_2$, where $c_1 \in S \oplus \{0\}$ and $c_2 \in \{0\} \oplus S$.*

(a) *If $c_1 = 0$ or $c_2 = 0$, then $\Pr(R') = P_1 := (p^2 + p - 1)(p^4 + p - 1)/p^8$.*
(b) *If $c_1 \neq 0$ and $c_2 \neq 0$, then $\Pr(R') = P_2 < P_1$.*

Proof. Note that S has Z-canonical form with data $A_1 := \mathrm{span}\{u, v\}$ and $A_2 := \mathrm{span}\{z\}$. We first examine the augmentations of S. It is readily verified that $|S/C_S(x)| = p$ for all nonzero elements of A_1, and that $|[S, S]| = p$. It follows readily that for every nonzero $c \in [S, S]$, $\Pr_c^+(S) = (p^2 - 1)/p^3$, $\Pr_c^-(S) = 1/p^2$, and so $\Pr(S) = \Pr_c^+(S) + \Pr_c^-(S) = \alpha_p$. Defining $S' = \mathrm{Aug}_p(S)$, we see using Lemma 4.2 that

$$\alpha_p' := \Pr(S') = \frac{p^2 - 1}{p^3} + \frac{p^2 + p - 1}{p^5} = \frac{p^4 + p - 1}{p^5}\,.$$

From now on, we write elements of R as a sum of direct sum components using subscripts, e.g. given $x \in R$, we implicitly write $x = x_1 + x_2$, where $x_1 \in S \oplus \{0\}$ and $x_2 \in \{0\} \oplus S$. If $c \neq 0$ but $c_i = 0$ for $i = 1$ or $i = 2$, then the augmented ring R' is of the form $S \oplus S'$ or $S' \oplus S$, so $\Pr(R') = \Pr(S)\Pr(S') = \alpha_p \alpha_p'$, as desired for (a).

Suppose instead that $c_1 \neq 0$ and $c_2 \neq 0$. Note that $c = [x, y]$ if and only if $c_i = [x_i, y_i]$ for $i \in \{1, 2\}$. It suffices to consider $x, y \in A_1 \boxplus A_1$. It follows that there are $2p^2 - 1$ such elements with $c \notin [x, R]$, namely all $x \in A_1 \boxplus A_1$ with either $x_1 = 0$ or $x_2 = 0$. We deduce that

$$\Pr_c^+(R) = \frac{p^4 - 2p^2 + 1}{p^6} \quad \text{and} \quad \Pr_c^-(R) = \frac{2p^2 - 2}{p^5} + \frac{1}{p^4} = \frac{2p^2 + p - 2}{p^5}\,.$$

By Lemma 4.2,

$$\begin{aligned} P_2 := \Pr(R') &= \frac{p^4 - 2p^2 + 1}{p^6} + \frac{(p^2 + p - 1)(2p^2 + p - 2)}{p^8} \\ &= \frac{p^6 + 3p^3 - 2p^2 - 3p + 2}{p^8}\,. \end{aligned}$$

It could be shown directly that $P_2 < P_1$ for all primes p, but let us prove this in a way that sheds light on the underlying reason. Note that $\Pr(R) = \Pr_c^+(R) + \Pr_c^-(R) = \alpha_p^2$ for both (a) and (b), so Lemma 4.2 implies that the inequality $P_2 < P_1$ holds if and only if $\Pr_c^-(R)$ is larger in case (b) than in case (a). In either case, the contributions to $\Pr_c^-(R)$ come from 0 and from those nonzero elements $x \in A_1 \boxplus A_1$ such that $c \notin [x, R]$: the former gives the same contribution regardless of c, and each $x \in A_1 \boxplus A_1$ with $c \notin [x, R]$ contributes $1/p|R|$ to $\Pr_c^-(R)$. Thus a larger value of $\Pr_c^-(R)$ corresponds to there being more elements $x \in A_1 \boxplus A_1$ such that $c \notin [x, R]$. In case (a), $c \in [x, R]$ if $x_j \neq 0$ (where c_j is the nonzero component of c), so there are p^2 elements $x \in A_1 \boxplus A_1$ with $c \notin [x, R]$. By contrast in case (b), we saw that there are $2p^2 - 1$ elements with $c \notin [x, R]$. □

5. Proof of main results

In the results in this section, we are interested in finite rings only up to Z-isoclinism. Thus we may always assume that R has Z-canonical form, in which case $R/Z(R)$ can be viewed as a subgroup of $(R,+)$ and it makes sense to talk about a basis of $R/Z(R)$ with elements drawn from R. When discussing spans of subsets in such a ring R, we indicate by a subscript whether we are working in R or $R/Z(R)$.

In the proofs of several results, we aim to understand rings that are *Z-atomic*, meaning that they are both Z-unaugmented and Z-indecomposable.

We begin with a theorem which gives a general upper bound for $\Pr(R)$ when R is noncommutative. In this result and its proof, $M(n)$ denotes the matrix ring over $\mathbb{Z}_n$ defined by

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

Theorem 5.1. *Let R be a finite noncommutative p-ring, with $k := k_1(R)$. Then*

$$\Pr(R) \le P(k;p) := \frac{p^{k+1} + p^k - 1}{p^{2k+1}} .$$

Equality is attained if and only if R is Z-isoclinic to the ring $M(p^k)$, as defined in the preceding paragraph. Furthermore, $P(1;p) = \alpha_p$, $P(2;p) = \gamma_p$, and $P(k;p)$ is strictly decreasing as a function of k.

Proof. By Lemma 2.6, we have elements $a, b \in R$ such that $p^{k-1}c \neq 0$, where $c = [a,b]$. We can find a basis $B = \{u_1, u_2, u_3, \ldots, u_m\} \subset R$ for $R/Z(R)$, where $u_1 = a$ and $u_2 = b$. Since c is an element of maximal order in $[R,R]$, there exists a basis $F = \{c_1, \ldots, c_m\}$ of $[R,R]$, with $c_1 = c$.

Suppose that for some $i > 2$, $[u_1, u_i] = n_1 c_1 + u$ and $[u_2, u_i] = n_2 c_1 + v$, where $u, v \in \operatorname{span} F'$, where $F' := \{c_2, \ldots, c_m\}$. Replacing u_i by $u_i' := u_i + n_2 u_1 - n_1 u_2$, a simple calculation shows that $[u_1, u_i'] = u$ and $[u_2, u_i'] = v$. Furthermore if u_i has order p^j for some $j < k$, then n_1 and n_2 must be divisible by p^{k-j}, so it follows from Remark 2.7 that B remains a basis after these replacements. We may therefore assume that the basis F of $[R,R]$ is such that

$$\{[u_1, u_i], [u_2, u_i]\} \subset \operatorname{span} F' , \qquad i > 2 . \tag{5.1}$$

A set of coset representatives of $R/Z(R)$ is given by $\sum_{i=1}^{n} x_i u_i$, where the integers x_i satisfy $0 \le x_i < p^{k_i(R/Z(R))}$. It follows from (5.1) that $[x, u_1] = \sum_i n_i c_i$ with $n_1 = -x_2$ and $[x, u_2] = \sum_i m_i c_i$ with $m_1 = x_1$. Thus $[x,R]$ includes an element of order p^k if either x_1 or x_2 is not divisible by p, and so the proportion of elements in the ring for which $|R/C_R(x)| \ge p^k$ is at least $(p^2-1)/p^2$.

If $k > 1$ and both x_1 and x_2 are divisible by p, but at least one is not divisible by p^2, we similarly deduce that an additional proportion at least $(p^2-1)/p^4$ of these representatives satisfy $|R/C_R(x)| \ge p^{k-1}$. For $k > 2$, we make a similar estimate when both x_1 and x_2 are divisible by p^2, but at least one is not divisible by p^3. We continue in this fashion until eventually we simply estimate that the probability that a second element will commute with x when both x_1 and x_2 are

divisible by p^k is 1. Adding up the various contributions, we get that

$$\Pr(R) \le \frac{1}{p^{2k}} + \sum_{i=0}^{k-1} \frac{p^2-1}{p^{k+2+i}} = \frac{p^{k+1}+p^k-1}{p^{2k+1}},$$

as required.

It is not hard to see that for each of the estimates above, we get equality if $R = M(p^k)$, and consequently we get equality in the overall bound for this ring, i.e. $\Pr(M(p^k)) = P(k;p)$.

Conversely the equality $\Pr(R) = P(k;p)$ requires that we have equality for each of the upper bounds in the above estimation. In particular, x must be central if x_1 and x_2 are zero. This forces $m = 2$, and so $R/Z(R)$ must have type $(k,k;p)$ in view of Lemma 2.6. Moreover, the commutator group must be a C_{p^k}, the same as for $M(p^k)$, and it is now straightforward to verify that R is Z-isoclinic to $M(p^k)$.

The equations in the last statement are immediate, and the decreasing nature of $P(k;p)$ amounts to the inequality $p^{k+1} - 1 < p^{k+2} - p^2$. Once we rewrite this inequality as $p^{k+2} - p^{k+1} - p^2 + 1 > 0$, it is clear that it holds for all $p \ge 2$ and $k \in \mathbb{N}$. □

Lemma 5.2. *Suppose R is a noncommutative $\mathbb{Z}_p$-algebra with $\dim[x,R] \ge 2$ for all $x \in R \setminus Z(R)$. Then $\Pr(R) \le (p^n + p^2 - 1)/p^{n+2} \le \gamma_p$, where $n = \dim R/Z(R)$.*

Proof. Since $\dim[x,R] \ge 2$ for at least one x, $R/Z(R)$ must have dimension $n \ge 3$. Consequently

$$\Pr(R) \le \frac{1-p^{-n}}{p^2} + \frac{1}{p^n} = \frac{p^n + p^2 - 1}{p^{n+2}}.$$

This bound is a strictly decreasing function of n, so it is maximal when $n = 3$, in which case it simply says that $\Pr(R) \le \gamma_p$. □

Lemma 5.3. *Suppose R is a $\mathbb{Z}_p$-algebra such that $R/Z(R)$ has dimension at least 3 and $\dim[u_1,R] = \dim[u_2,R] = 1$, for some $u_1, u_2 \in R$ such that $[u_1,u_2] \ne 0$. Then R is not Z-atomic.*

Proof. The hypotheses are invariant under Z-isoclinism, so we may assume that R has Z-canonical form, with $(R,+) = A_1 \boxplus A_2$ as in Definition 3.6. We may also assume that $T := \{u_1, u_2\} \subset A_1$, since if this is not the case, then certainly $u_i' = u_i + z_i \in A_1$ for some $z_i \in A_2$, and u_1', u_2' satisfy the same assumptions as u_1, u_2 since $A_2 = Z(R)$.

Let $V_1 = \operatorname{span}(T)$. By Observation 2.2, $C_R(u_1)$ and $C_R(u_2)$ both have codimension 1 in R. Writing $U := C_R(u_1) \cap C_R(u_2)$, it follows that $\operatorname{codim} U \le 2$. Every nontrivial linear combination of u_1 and u_2 fails to commute with one or other of these two elements, so $(R,+) = U \boxplus V_1$. Now U is a subring of R, and $u \in U$ if and only if $u + z \in U$ for all $z \in A_2$, so $(U,+) = U_1 \boxplus A_2$ for some $U_1 \subset A_1$. Note that U_1 and V_1 are complementary subspaces of A_1. We define the abelian groups $U_2 = [U_1, U_1]$, $V_2 = [V_1, V_1]$, and $V = V_1 + V_2$. Since R has Z-canonical form, we have $R^2 = [R,R] = A_2$, and the definitions of U_1, V_1 then ensure that $A_2 = U_2 + V_2$. Let us write a general element $x \in R$ in the form $x = u_x + v_x + z_x$, where $u_x \in U_1$, $v_x \in V_1$, and $z_x \in A_2$. Note that $xy = (u_x + v_x)(u_y + v_y)$ and $[x,y] = [u_x, u_y] + [v_x, v_y]$.

Suppose first that $U_2 \cap V_2 = \{0\}$, and so $A_2 = U_2 \boxplus V_2$. Let $P : A_2 \to U_2$ and $Q : A_2 \to V_2$ be the ring epimorphisms defined by $P(u+v) = u$ and $Q(u+v) = v$

for all $u \in U_2$, $v \in V_2$. Let S be the ring which coincides as an additive group with R, but where multiplication $*$ is defined by $x * y = P(u_x u_y) + Q(v_x v_y)$, and let us denote by $[\cdot,\cdot]'$ commutators in S. It follows that $[x,y]' = [x,y]$, so $Z(S) = Z(R) = A_2$, and we readily deduce that R is Z-isoclinic to S. It is also clear that $S = S' \oplus S''$, where S' is the subring of S generated by U_1, and S'' is the subring of S generated by V_1. Thus R is Z-decomposable.

Suppose instead that $U_2 \cap V_2 \neq \{0\}$. Since V_2 is one-dimensional, $V_2 \subset U_2$. It follows readily that R is a p-augmentation of the subring R' generated by U_1. $\square$

In the next three theorems, we will classify up to Z-isoclinism all Z-atomic $\mathbb{Z}_p$-algebras R with $\Pr(R) \geq \gamma_p$ and $\dim R/Z(R) > 2$. Since Z-isoclinism depends only on the Lie ring R_{Lie} associated with a ring R, it suffices in the proofs to consider only all possible commutators rather than all possible products. However, since we wish to fully specify associative rings in each Z-family in the statements of the theorems, we define the relevant products for each ring in these theorems.

Theorem 5.4. *Suppose R is a $\mathbb{Z}_p$-algebra such that $\dim R/Z(R) = 3$. Then R is Z-atomic, and it is Z-isoclinic to one of the following pair of rings:*

(a) *$R_{3,1}$ has basis $\{u_1, u_2, u_3, c_{12}, c_{23}\}$ and the only nonzero products of basis elements are $u_1u_2 = c_{12}$ and $u_2u_3 = c_{23}$.*
(b) *$R_{3,2}$ has basis $\{u_1, u_2, u_3, c_{12}, c_{13}, c_{23}\}$ and the only nonzero products of basis elements are $u_1u_2 = c_{12}$, $u_1u_3 = c_{13}$, and $u_2u_3 = c_{23}$.*

Furthermore, $\Pr(R_{3,1}) = \beta_p$ and $\Pr(R_{3,2}) = \gamma_p$.

Theorem 5.5. *Suppose R is a Z-atomic $\mathbb{Z}_p$-algebra such that $\dim R/Z(R) = 4$ and $\Pr(R) \geq \gamma_p$. Then R is Z-isoclinic to one of the following pair of rings:*

(a) *$R_{4,1}$ has basis $\{u_1, u_2, u_3, u_4, c_{12}, c_{24}\}$, and the only nonzero products of basis elements are $u_1u_2 = c_{12}$, $u_2u_4 = c_{24}$, and $u_3u_4 = c_{12}$.*
(b) *$R_{4,2}$ has basis $\{u_1, u_2, u_3, u_4, c_{12}, c_{23}, c_{24}\}$, and the only nonzero products of basis elements are $u_1u_2 = c_{12}$, $u_2u_3 = c_{23}$, and $u_2u_4 = c_{24}$.*

Furthermore, $\Pr(R_{4,1}) = \Pr(R_{4,2}) = \gamma_p$.

Theorem 5.6. *Suppose R is a Z-atomic $\mathbb{Z}_p$-algebra such that $\dim R/Z(R) = n \geq 5$. Then $\Pr(R) \leq \delta_{p,n} := (p^{n-1} + p^{n-2} - p^{n-3} + p - 1)/p^{n+1} < \gamma_p$.*

Proof of Theorem 5.4. Note that $R_{3,1}$ and $R_{3,2}$ are joins. The fact that the central factor group in both cases has dimension 3, and so both rings are in Z-canonical form, now follows from Observation 3.9(a).

The Z-atomicity of R follows easily from Lemma 2.6. We assume without loss of generality that R has Z-canonical form, with data (A_1, A_2) as in Definition 3.6. In particular, we can identify $R/Z(R)$ with A_1.

Suppose first that R has an element u_1 such that $\dim[u_1, R] = 1$. We may assume that $u_1 \in A_1$. By Lemma 5.3, $\dim[u_2, R] \geq 2$ whenever $[u_1, u_2] \neq 0$. But $\dim[x, R] \leq \dim(R/Z(R)) - 1 = 2$, so we must have $\dim[u_2, R] = 2$ for all u_2 such that $[u_1, u_2] \neq 0$. We pick such an element $u_2 \in A_1$.

Since $\operatorname{codim} C_R(u_1) = 1$, there exists $u_3 \in C_R(u_1) \cap A_1$ such that

$$\dim \operatorname{span}_{A_1}\{u_1, u_3\} = 2\,.$$

Since $u_2 \notin C_R(u_1)$, $\{u_1, u_2, u_3\}$ is a basis of A_1. Furthermore $[u_2, u_3] \neq 0$, lest u_3 be central. Since $[u_1, u_2]$ and $[u_2, u_3]$ span $[u_2, R]$, they cannot be collinear. In summary, A_1 has basis $\{u_1, u_2, u_3\}$, the commutators $[u_i, u_j]$, $i < j$, are nonzero

only for $(i,j) = (1,2)$ and $(i,j) = (2,3)$, and these two commutators are not collinear. It follows readily that R is Z-isoclinic to $R_{3,1}$.

Let us calculate $\Pr(R_{3,1})$. It suffices to consider sums of the form $x = \sum_{i=1}^{3} x_i u_i$, where $x_i \in \mathbb{Z}_p$. If $x_2 \neq 0$, then $[x,u_1]$ and $[x,u_3]$ are non-collinear, so $\dim[x,R] = 2$. If $x_2 = 0$, but at least one of x_1 and x_3 is nonzero, then it is clear that $\dim[x,R] = 1$ is one-dimensional. Finally, $x = 0$ commutes with everything. Thus

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

It remains to consider the case where $\dim[x,R] = 2$ for all noncentral x. Let $\{u_1,u_2,u_3\} \subset R$ be a basis of A_1, and let us write $c_{ij} = [x_i,x_j]$. We claim that the commutators $\{c_{12},c_{23},c_{13}\}$ form an independent set. Suppose that this is false, and so by symmetry we can assume that $c_{23} = sc_{12} + tc_{13}$, for some $s,t \in \mathbb{Z}_p$. Letting $u_2' := u_2 - tu_1$ and $u_3' := u_3 + su_1$, we see that $[u_2',u_3'] = 0$. But u_2', u_3' are not in the same coset of $Z(R)$, so $\dim[u_i',R] \leq 1$ for $i = 2,3$, contradicting our assumptions. It is now easy to deduce that R is Z-isoclinic to $R_{3,2}$.

Finally, we calculate $\Pr(R_{3,1})$. It again suffices to consider sums of the form $x = \sum_{i=1}^{3} x_i u_i$, where $x_i \in \mathbb{Z}_p$. Now $\dim[x,R] = 2$ for all nonzero sums x, so

$$\Pr(R) = \frac{p^3 - 1}{p^{3+2}} + \frac{1}{p^3} = \gamma_p \,. \qquad \square$$

Proof of Theorem 5.5. Note that $R_{4,1}$ and $R_{4,2}$ are joins. The fact that the central factor group in both cases has dimension 4, and so both rings are in Z-canonical form, now follows from Observation 3.9(a).

We assume without loss of generality that R has Z-canonical form, with data (A_1,A_2) as in Definition 3.6. In particular, we can identify $R/Z(R)$ with A_1. By Lemma 5.2 with $n = 4$, we see that there must exist $u_1 \in R$ with $\dim[u_1,R] = 1$. Without loss of generality, $u_1 \in A_1$. By Z-atomicity and Lemma 5.3, we have the dimensional bound $\dim[u_2,R] \geq 2$ whenever $u_2 \in A_1$ is such that $[u_1,u_2] \neq 0$. We now split the analysis into two main cases depending on whether this dimensional bound is always strict or not.

Case 1: *There exist* $u_1,u_2 \in A_1$ *such that* $[u_1,u_2] \neq 0$, $\dim[u_1,R] = 1$, *and* $\dim[u_2,R] = 2$.

We fix u_1,u_2 with the specified properties. Since $C_R(u_1)/Z(R)$ and $C_R(u_2)/Z(R)$ have codimensions 1 and 2, respectively, in $R/Z(R)$, their intersection has codimension at most 3 (in fact, exactly 3 because $u_2 \in C_R(u_2) \setminus C_R(u_1)$), and so there exists a nonzero element $u_3 \in A_1$ which commutes with both u_1 and u_2. Note that

$$\dim \operatorname{span}_{A_1}\{u_1,u_2,u_3\} = 3 \,,$$

since $(C_R(u_1) \cap C_R(u_2))/Z(R)$ has trivial intersection with the vector space generated by $u_1 + Z(R)$ and $u_2 + Z(R)$. Choose any $u_4 \in A_1$ such that $\{u_1,\ldots,u_4\}$ is a basis of A_1, and define $c_{ij} := [u_i,u_j] \in A_2$, $1 \leq i,j \leq 4$.

Below, we change the values of u_i for a specific i in various ways to achieve various reductions. In each such case, $c_{ij} := [u_i,u_j]$ is changed accordingly for each j.

We assume as we may that $c_{14} = 0$, since if this fails, then $c_{14} = \lambda c_{12}$, and we get the desired property if we replace u_4 by $u_4 - \lambda u_2$. Since $u_i \in C_R(u_3)$ for $i \leq 3$, we see that $\dim[u_3,R] = 1$, and so $c_{34} \neq 0$. Our unaugmented assumption now

forces $\dim[u_4, R] = 2$. Thus $\dim \operatorname{span}\{c_{12}, c_{24}\} = 2$, $\dim \operatorname{span}\{c_{24}, c_{34}\} = 2$, and $A_2 = \operatorname{span} S$, where $S := \{c_{12}, c_{24}, c_{34}\}$ has dimension 2 or 3.

We next perform some reductions for the case $\dim A_2 = 2$. We must have $c_{12} = a_2c_{24} + a_3c_{34}$, for some $a_2, a_3 \in \mathbb{Z}_p$. If $a_2 \neq 0$, then $u := a_2u_2 + a_3u_3 \in Q$ fails to commute with u_1 and also $[u, R] = \operatorname{span}\{c_{12}\}$. Thus $\dim[u, R] = \dim[u_1, R] = 1$ and $[u, u_1] \neq 0$. By Lemma 5.3, this contradicts the hypothesis that R is Z-atomic. Thus $c_{12} = a_3c_{34}$ for some $a_3 \in \mathbb{Z}_p$. We must have $a_3 \neq 0$, since if $a_3 = 0$, then u_1 would be central, and $\dim R/Z(R) < 4$. Replacing u_3 by $a_3^{-1}u_3$, we reduce to the case where $c_{12} = c_{34}$, and so $R = R_{4,1}$.

We have therefore essentially reduced Case 1 to two possible Z-canonical form rings: either A_2 has basis S, or it has basis $\{c_{24}, c_{34}\}$ and $c_{12} = c_{34}$. We can begin the analysis of both of these rings together.

Let us write $x := \sum_{i=1}^{4} x_iu_i$, where $x_i \in \mathbb{Z}_p$. If $x_2 \neq 0$ or $x_4 \neq 0$, we claim that $\dim[x, R] \geq 2$. By symmetry, it suffices to verify this for $x_2 \neq 0$. Then $[x, u_1] = -x_2c_{12}$ and $[x, u_4] = x_2c_{24} + x_3c_{34}$ are non-collinear, so the claim is verified. Thus

(i) $\dim[x, R] \geq 2$ for all x with $x_2 \neq 0$ or $x_4 \neq 0$, and
(ii) $\dim[x, R] \geq 1$ for all $x \neq 0$ with $x_2 = x_4 = 0$.

and so

$$\Pr(R) \leq \frac{p^4 - p^2}{p^{4+2}} + \frac{p^2 - 1}{p^{4+1}} + \frac{1}{p^4} = \frac{p^3 + p^2 - 1}{p^5} = \gamma_p\,, \tag{5.2}$$

with equality in (5.2) if and only if the inequalities in both (i) and (ii) always hold with equality.

Suppose now that $\dim A_2 = 3$. Taking $u := u_2 + u_3 + u_4$, we see that $[u, R]$ contains $[u, u_1] = -c_{12}$, $[u, u_2] = -c_{24}$ and $[u, u_3] = -c_{34}$, so $\dim[u, R] = 3$. Thus equality fails for $x = u$ in (i), and we do not get equality in (5.2).

There remains only the case $\dim A_2 = 2$, and so $R = R_{4,1}$. In this case, it is readily verified that the inequalities in (i) and (ii) above holds with equality, and so $\Pr(R_{4,1}) = \gamma_p$, as required.

Case 2: *Whenever* $u_1, u_2 \in A_1$ *satisfy* $\dim[u_1, R] = 1$ *and* $[u_1, u_2] \neq 0$*, we have* $\dim[u_2, R] = 3$*.*

We fix u_1 with $\dim[u_1, R] = 1$. Because $\dim[u_1, R] = 1$, there are exactly $p^4 - p^3$ elements $u \in A_1$ with $[u_1, u] \neq 0$ and $\dim[u, R] = 3$ for all such u. It follows that

$$\Pr(R) \leq \frac{p^4 - p^3}{p^{4+3}} + \frac{p^3 - 1}{p^{4+1}} + \frac{1}{p^4} = \frac{p^3 + p^2 - 1}{p^5} = \gamma_p\,, \tag{5.3}$$

Equality above requires that $\dim[u, R] = 1$ for the $p^3 - 1$ nonzero elements $u \in A_1$ that commute with u_1. In this case, it follows that $C_R(x) = C_R(y)$ for any distinct pair x, y of these elements, since otherwise $C_R(x) \cap C_R(y)$ has codimension at least 2, and so $R \setminus (C_R(x) \cap C_R(y))$ would include at least $p^4 - p^2$ elements of A_1. By our hypothesis, we would then have $|R/C_R(w)| = p^3$ for at least $p^4 - p^2$ elements $w \in A_1$, preventing equality in (5.3). Thus $C_R(u_1)$ is a commutative subring of R, with $|R/C_R(u_1)| = p$, and there is a basis $\{u_1, u_3, u_4\} \subset R$ of $C_R(u_1)/Z(R)$ such that u_i, u_j commute if $i, j \neq 2$. It follows that R is Z-isoclinic to $R_{4,2}$, and that $R = R_{4,2}$ satisfies the requirements for equality in (5.3).

Note that, in view of Lemma 5.3 and the Z-atomic assumption, Cases 1 and 2 cover all possibilities that can arise.

Finally, we show that both $R_{4,1}$ and $R_{4,2}$ are Z-atomic. Suppose R is a $\mathbb{Z}_p$-algebra such that $\dim R/Z(R) = 4$. If R is Z-decomposable, then it follows from Lemma 2.6 that it is Z-isoclinic to a ring $S = S_1 \oplus S_2$, where each $S_i/Z(S_i)$ is two-dimensional. It is then easily deduced that S_i is Z-isoclinic to the ring $M(p)$ of Theorem 5.1 for $i = 1, 2$, and so $\Pr(R) = \alpha_p^2 \neq \gamma_p$. If instead R is Z-augmented, then $[R, R]$ is forced to be one-dimensional, whereas we have seen above that there are elements x of $R_{4,i}$, $i = 1, 2$, such that $\dim[x, R_{4,i}] > 1$. □

Proof of Theorem 5.6. If $\dim[x, R] < 2$ for at most p^{n-2} of the cosets $x + Z(R) \in R/Z(R)$, then

$$\Pr(R) \leq \frac{p^n - p^{n-2}}{p^{n+2}} + \frac{p^{n-2} - 1}{p^{n+1}} + \frac{1}{p^n} = \delta_{p,n} < \frac{p^{n-1} + p^{n-2} - p^{n-4}}{p^{n+1}} = \gamma_p \,.$$

Thus we may assume that there are at least $p^{n-2} + 1$ of the cosets $x + Z(R)$ with $\dim[x, R] < 2$. Letting S be the union of all of such cosets, and $V = \operatorname{span}(S)$, we see that V has codimension at most 1 in R.

Lemma 5.3 tells us that $[x, y] = 0$ if $x, y \in S$, so the elements of V all commute with each other. It follows that $\operatorname{codim} V = 1$, and that $V = C_R(x)$ for all $x \in S \setminus Z(R)$. Since V is a commutative subring of R, every $y \notin V$ must fail to commute with all non-central elements of V. Thus $\dim R/C_R(y) = n - 1$ whenever $y \notin V$, and it follows that

$$\Pr(R) = \frac{p^n - p^{n-1}}{p^{n+(n-1)}} + \frac{p^{n-1} - 1}{p^{n+1}} + \frac{1}{p^n} = \frac{p^{n-1} + p^2 - 1}{p^{n+1}} < \delta_{p,n} < \gamma_p \,.$$

□

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1. We first investigate $\mathfrak{R}_p$. By Theorem 5.1, $\Pr(M(p^2)) = \gamma_p$, so γ_p is a p-value. This reduces the task to the determination of all large p-values and all large values. But again by Theorem 5.1, p-rings R with $k_1(R) > 1$ lead only to small p-values, so we may assume that R is a p-ring with $k_1(R) = 1$. Thus $R/Z(R)$ has the form $\boxplus_{i=1}^m C_p$ and, in view of Observation 3.12, we may also assume that R is a $\mathbb{Z}_p$-algebra. If $m = 2$, R is easily seen to be Z-isoclinic to $M(p)$, giving the value α_p. Theorems 5.4, 5.5, and 5.6 tell us that β_p is the only other large p-value associated with a Z-atomic $\mathbb{Z}_p$-algebra R of dimension at least 3.

We next consider augmentation. According to Theorem 5.1, the only p-rings giving rise to the p-value α_p are Z-isoclinic to $M(p)$, so we may use a Z-canonical relative R of $M(p)$ for augmentation. Now, $[R, R]$ has order p. Additionally, $\Pr(R) = (p^2 + p - 1)/p^3$ and $a_0(R) = 1/p^2$. Thus if we define $R_k := \operatorname{Aug}_p^k(R)$ for all $k \in \mathbb{N}$, then Corollary 4.4 yields

$$\Pr(R_k) = \frac{p^{2k+2} + p - 1}{p^{2k+3}} \,.$$

It also follows from our analysis that there is a unique Z-atomic Z-family associated with β_p, namely that of $R_{3,1}$ in Theorem 5.4. But we already analyzed this algebra in Example 4.5, where we found that $\Pr(\operatorname{Aug}_p(R, c)) = \gamma_p$. Thus we get no additional large p-values in this case, and there remain no other ways of getting large p-values by augmentation of Z-atomic rings.

We next consider rings that are Z-decomposable, with summands of the types that we have already obtained. This reduces to considering products of the p-values that we have already obtained. Since α_p is a p-value, we see that α_p^n is also a p-value for all $n \in \mathbb{N}$. Now $\alpha_p^2 > \gamma_p$, but $\alpha_p^n < \gamma_p$ for all $n \geq 3$, since

$$p^9(\gamma_p - \alpha_p^3) = (p^7 + p^6 - p^4) - (p^2 + p - 1)^3 = (p-1)^3(p+1)(p^3 + 2p^2 + p - 1)\,,$$

and it is clear that this last expression is positive for $p \geq 2$. If we take the product of two distinct p-values that we have already obtained, then we obtain at most $\gamma_p' := (p^2 + p - 1)(p^4 + p - 1)/p^8$ and this is smaller than γ_p because for $p \geq 2$,

$$p^8(\gamma_p - \gamma_p') = (p^6 + p^5 - p^3) - (p^2 + p - 1)(p^4 + p - 1) = (p-1)^3(p+1) > 0\,.$$

Now that we have considered augmentation followed by direct sums, we need to iterate this pair of processes until we get no additional large p-values. This happens at the very next step: the only new p-value obtained above by taking direct sums was α_p^2, and if we now augment the associated Z-canonical form ring, it follows from Proposition 4.7 that the largest p-value obtained is γ_p' of the last paragraph. But $\gamma_p' < \gamma_p$, so we are done.

We obtain all large values by taking products of p-values for distinct primes p. Any nontrivial product of this type gives a value at most equal to $\alpha_2\alpha_3$, which is smaller than γ_2. Thus we obtain all large values simply by taking the union of all p-values that are larger than γ_2 for some prime p. We already know the 2-values in this set. As for the 3-values, we get only α_3 because $(3^4 + 3 - 1)/3^5 < \gamma_2$. Finally, $\alpha_p < \gamma_2$ for $p \geq 5$, so we get no additional large values by using such primes. □

Proof of Theorem 1.2. An examination of the proof of Theorem 1.1 shows that each large p-value is associated with a unique Z-family of p-rings, and each large value is associated with a unique Z-family of finite rings. □

Proof of Theorem 1.3. We first define rings S_i, $1 \leq i \leq 5$:

(a) $S_1 = M(p^2)$.

(b) $S_2 = \mathrm{Aug}_p^c(R_0)$ where $\Pr(R_0) = \beta_p$, and c is any nonzero commutator.

(c) S_3 is the ring $R_{3,2}$ of Theorem 5.4.

(d) S_4 is the ring $R_{4,1}$ of Theorem 5.5.

(e) S_5 is the ring $R_{4,2}$ of Theorem 5.5.

Theorem 5.1 tells us that $\Pr(S_1) = \gamma_p$, and it follows from Example 4.5 that $\Pr(S_2) = \gamma_p$. The fact that $\Pr(S_i) = \gamma_p$ for $i = 3, 4, 5$ follows from Theorems 5.4 and 5.5.

Next we consider the central factor groups. It is readily verified that $Z(S_1) = \{0\}$, so $S_1/Z(S_1) \cong C_{p^2} \boxplus C_{p^2}$. For all other i, $S_i/Z(S_i)$ must be of the form $\boxplus_{i=1}^d C_p$ for some d. Specifically for $i = 2$, we have $d = 5$: for the unaugmented algebra R, we have $\dim R/Z(R) = 3$, and augmentation increases this dimension by 2 (Observation 4.1(a)). According to Theorems 5.4 and 5.5, we have $d = 3$ for $i = 3$, and $d = 4$ for $i \in \{4, 5\}$.

It is readily verified that $[S_1, S_1] \approx C_{p^2}$ and, for all $i > 1$, $[S_i, S_i]$ must be a $\mathbb{Z}_p$-vector space of the form $\boxplus_{i=1}^d C_p$ for some d. When $i = 2$, we have $d = 2$, since $\dim[R, R] = 2$ for the unaugmented ring, and augmentation always leaves

the commutator subgroup unchanged. When $i = 3$, $d = 3$ and $[S, S]$ has basis $\{c_{12}, c_{23}, c_{13}\}$. When $i = 4$, $d = 2$ and $[S, S]$ has basis $\{c_{12}, c_{24}\}$. When $i = 5$, $d = 3$ and $[S, S]$ has basis $\{c_{12}, c_{23}, c_{24}\}$.

The above calculations show that the rings S_i provide us with four central factor group isomorphism classes, three commutator subgroup group isomorphism classes, and five Z-families (since no two of these rings have both isomorphic central factor groups and isomorphic commutator subgroups).

It remains to prove that there are no other Z-families of p-rings R for which $\Pr(R) = \gamma_p$, so suppose R is such a ring. We assume initially that R is a Z-atomic p-ring. For $k_1(R) > 1$, the proof of Theorem 1.1 reveals that we get $\Pr(R) = \gamma_p$ if and only if R is Z-isoclinic to S_1. We may consequently suppose, as in the proof of Theorem 1.1 that R is a $\mathbb{Z}_p$-algebra, with $\dim R/Z(R) = m > 1$: in fact $m > 2$ since $m = 2$ forces a $\mathbb{Z}_p$-algebra to be Z-isoclinic to $M(p)$ and $\Pr(M(p)) \neq \gamma_p$. Now Theorems 5.4, 5.5, and 5.6 tell us that the only Z-atomic options are S_3, S_4, and S_5.

There remains the task of considering augmentations and direct sums. The proof of Theorem 1.1 reveals that an augmented ring R satisfies $\Pr(R) = \gamma_p$ if and only if R is Z-isoclinic to S_2, and that we cannot obtain $\Pr(R) = \gamma_p$ by taking the direct sum of two noncommutative p-rings. □

By explicitly giving $\mathfrak{R}_p \cap [\gamma_p, 1]$ together with the possible Z-families, we were easily able to deduce an explicit form for $\mathfrak{R} \cap [\gamma_2, 1]$, together with the possible Z-families. This mirrors fairly closely the characterization in the group setting of all commuting probabilities strictly larger than γ_2, together with the possible types of $[G, G]$ and $G/Z(G)$ for the associated groups G: see [17] and Remark 4.4 of [3].

In the group setting, the set of all commuting probabilities greater than or equal to $11/75$ for *odd order* groups G, together with the possible types of $[G, G]$ and $G/Z(G)$, has also been explicitly given in [3]. In view of this, we record the corresponding result for $\mathfrak{R}_{\text{odd}} \cap [\gamma_3, 1]$, where $\mathfrak{R}_{\text{odd}}$ is the set of values of $\Pr(R)$ as R ranges over all finite rings of odd order. Note that $\gamma_3 = 0.1440\cdots < 0.1466\cdots = 11/75$.

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 value γ_3 is associated with exactly five Z-families and all other values are associated with a unique Z-family.

Proof. Since $\alpha_3\alpha_5 < \gamma_3$, the only values in $S := \mathfrak{R}_{\text{odd}} \cap [\gamma_3, 1]$ are p-values for some p. Now $\alpha_{11} < \gamma_3$, so we need only examine $p = 3, 5, 7$. The 3-values are already given by Theorem 1.1, so it remains only to examine $p = 5, 7$. The full set of augmentations of α_5 lie in S because $1/5 > \gamma_3$, but there are no other 5-values in S because $\beta_5 < \gamma_3$. As for $p = 7$, we see that $\alpha_7 > \gamma_3$, but all other values in $\mathfrak{R}_7$ are smaller than γ_3. □

Finally, we gather together in Figure 3 all possible Z-families and group isomorphism types among p-rings R for which $\Pr(R) \geq \gamma_p$: the R-column gives a representative of the Z-family, and the last two columns give group isomorphism

classes. $M(p)$ is as in Theorem 5.1, $R_{3,1}$ is as in Theorem 5.4, and the rings S_i are as in the proof of Theorem 1.3.

$\Pr(R)$	R	$R/Z(R)$	$[R,R]$
1	commutative	C_1	C_1
$\dfrac{p^{2k}+p-1}{p^{2k+1}}$, $k \in \mathbb{N}$	$\mathrm{Aug}_p^{k-1}(M(p))$	$\boxplus_{i=1}^{2k} C_p$	C_p
β_p	$R_{3,1}$	$\boxplus_{i=1}^{3} C_p$	$C_p \boxplus C_p$
α_p^2	$M(p) \oplus M(p)$	$\boxplus_{i=1}^{4} C_p$	$C_p \boxplus C_p$
	S_1	$C_{p^2} \boxplus C_{p^2}$	C_{p^2}
	S_2	$\boxplus_{i=1}^{5} C_p$	$C_p \boxplus C_p$
γ_p	S_3	$\boxplus_{i=1}^{3} C_p$	$\boxplus_{i=1}^{3} C_p$
	S_4	$\boxplus_{i=1}^{4} C_p$	$C_p \boxplus C_p$
	S_5	$\boxplus_{i=1}^{4} C_p$	$\boxplus_{i=1}^{3} C_p$

FIGURE 3. Equivalence classes for $\mathfrak{R}_p \cap [\gamma_p, 1]$

The corresponding table for $\mathfrak{R} \cap [\gamma_2, 1]$ is identical to Figure 3 for $p = 2$, except for the addition of a line for α_3, given by the second row of Figure 3 for $(p, k) = (3, 1)$. The possible Z-families in Theorem 5.7, and associated isomorphism types for $R/Z(R)$ and $[R, R]$, can also be readily understood from Figure 3.

Note that similar tables for groups given in [17] and [3] also include a column for $[G, G] \cap Z(G)$. However, we do not give a $[R, R] \cap Z(R)$ column because this is not a Z-isoclinic invariant. Indeed, a noncommutative ring R of order p^2 has trivial center, so $|R/Z(R)| = p^2$, and it is also clear that $|[R, R]| = p$. However, the Z-canonical relative S of R satisfies the equation $[S, S] \cap Z(S) = [S, S] = Z(S)$—as do all Z-canonical form rings—so $|[S, S] \cap Z(S)| = p$ has order p.

REFERENCES

[1] 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.

[2] F.R. Beyl, *Isoclinisms of group extensions and the Schur Multiplicator*, in "Groups — St Andrews 1981", Ed. C.M. Campbell and E.F. Robertson, Cambridge University Press, Cambridge, 1982.

[3] 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.

[4] J. Dixon, *Probabilistic group theory*, C.R. Math. Rep. Acad. Sci. Canada **24** (2002), 1–15.
[5] P. Erdös and P. Turán, *On some problems of a statistical group-theory, IV*, Acta Math. Acad. Sci. Hung. **19** (1968), 413–435.
[6] 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.
[7] W.H. Gustafson, *What is the probability that two group elements commute?*, Amer. Math. Monthly **80** (1973), 1031–1034.
[8] P. Hall, *The classification of prime-power groups*, J. reine angew. Math. **182** (1940), 130–141; doi:10.1515/crll.1940.182.130.
[9] P. Hegarty, *Limit points in the range of the commuting probability function on finite groups*, J. Group Theory **16** (2013), 235–247.
[10] I.N. Herstein, *Topics In Algebra*, 2nd edition. John Wiley and sons, New York, 1975.
[11] K.S. Joseph, *Commutativity in non-abelian groups*, PhD thesis, University of California, Los Angeles, 1969.
[12] R.L. Kruse and D.T. Price, *Nilpotent rings*. Gordon and Breach, New York, 1969.
[13] P. Lescot, *Isoclinism classes and commutativity degrees of finite groups*, J. Algebra **177** (1995), 847–869.
[14] D. MacHale, *How commutative can a non-commutative group be?*, Math. Gaz. **LVIII** (1974), 199–202; doi:10.2307/3615961.
[15] D. MacHale, *Commutativity in finite rings*, Amer. Math. Monthly **83** (1976), 30–32.
[16] K. Moneyhun, *Isoclinisms in Lie algebras*, Algebras Groups Geom. **11** (1994), 9–22.
[17] 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

A. Ní Shé:
Department of Mathematics, Cork Institute of Technology, Cork, Ireland.
E-mail address: aine.nishe@cit.ie