Finite rings with large anticommuting probability

S.M. BUCKLEY, D. MACHALE, AND YU. ZELENYUK

ABSTRACT. We investigate the set of values attained by $\Pr_{\mathrm{ac}}(R)$, the probability that a random ordered pair of elements in a finite ring R has zero Jordan product. In particular, we find all possible values of $\Pr_{\mathrm{ac}}(R)$ in $[15/32, 1]$.

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], [9], [7], [10], [12], [4], [6], [3], and [8]. The corresponding question for finite rings was examined in [11] and [2]. In this paper, we examine the probability that a random pairs of elements in a finite ring anticommute.

Let $f(X,Y) = aXY + bYX$ be a formal noncommutative polynomial in the unknowns X and Y, where $a, b \in \mathbb{Z}$. We use f as a symbol of the function $f^R : R \times R \to R$, defined by $f^R(x,y) := axy + byx$, on an arbitrary ring R. For such a symbol f, and a ring R of finite cardinality, let

$$\Pr_f(R) := \frac{|\{(x,y) \in R \times R : \ f^R(x,y) = 0\}|}{|R|^2}\,, \tag{1.1}$$

where $|S|$ denotes the cardinality of a set S. Whenever $\mathcal{C}$ is a class of finite rings, we define the associated *f-spectrum* $\mathfrak{S}_f(\mathcal{C}) \subseteq \mathbb{Q} \cap (0,1]$ by

$$\mathfrak{S}_f(\mathcal{C}) := \{\Pr_f(R) \mid R \in \mathcal{C}\}\,.$$

We give $\Pr_f(R)$ and $\mathfrak{S}_f(\mathcal{C})$ special terminology and notation in three important cases: the *commuting probability* and *commuting spectrum*, $\Pr_{\mathrm{c}}(R)$ and $\mathfrak{S}_{\mathrm{c}}(\mathcal{C})$, correspond to $f(X,Y) := XY - YX$; the *anticommuting probability* and *anticommuting spectrum*, $\Pr_{\mathrm{ac}}(R)$ and $\mathfrak{S}_{\mathrm{ac}}(\mathcal{C})$, correspond to $f(X,Y) := XY + YX$; and the *annihilating probability* and *annihilating spectrum*, $\Pr_{\mathrm{ann}}(R)$ and $\mathfrak{S}_{\mathrm{ann}}(\mathcal{C})$, correspond to $f(X,Y) := XY$.

The commuting spectrum was investigated in [2], where all sufficiently large spectral values were given explicitly, both for the class $\mathcal{C}_{\mathrm{fin}}$ of all finite rings and for the class $\mathcal{C}_p$ of all rings of order a power of a given prime p. In [1], some relationships between the various spectra were discussed: in particular, it was shown that the annihilating spectrum of various classes of finite rings contains the f-spectrum of the same class for each f as above. However [1] does not discuss any particular values that lie in any of these spectra, so in this paper we carry out such an investigation for anticommuting spectra (and annihilating spectra for commutative rings), although some of our results apply equally well to f-spectra for a general symbol f.

Date: 03.08.2013.

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

We use three parametrized proportions in our main results:

$$\alpha(k;p) := \frac{p^k + p - 1}{p^{k+1}}, \quad \delta(p) := \frac{3p-2}{p^3}, \quad \epsilon(p) := \frac{2p^3 + p^2 - 3p + 1}{p^5},$$

where p is a prime and $k \in \mathbb{N}$. For comparison with the results of [2], we also define $\gamma(p) := (p^3 + p^2 - 1)/p^5$. We will see in Section 2 that for all primes p and $k \in \mathbb{N}$,

$$\gamma(p) < \epsilon(p) < \delta(p) \le \frac{1}{p} < \alpha(k+1;p) < \alpha(k;p), \tag{1.2}$$

with all inequalities being strict for $p > 2$.

Let $\mathcal{C}_{\text{fin}}$ and $\mathcal{C}_p$ be as above. In [2], all elements of $\mathfrak{S}_{\text{c}}(\mathcal{C}_p) \cap [\gamma(p), 1]$ and $\mathfrak{S}_{\text{c}}(\mathcal{C}_{\text{fin}}) \cap [\gamma(2), 1]$ are explicitly listed for all primes p. In the following theorem, we explicitly list all elements of $\mathfrak{S}_{\text{ac}}(\mathcal{C}_p) \cap [\epsilon(p), 1]$ and $\mathfrak{S}_{\text{ac}}(\mathcal{C}_{\text{fin}}) \cap [\epsilon(2), 1]$; note that $\epsilon(2) = 15/32$.

Theorem 1.1. *For all primes p,*

$$\mathfrak{S}_{\text{ac}}(\mathcal{C}_p) \cap [\epsilon(p), 1] = \{\alpha(k;p) \mid k \in \mathbb{N}\} \cup \left\{1, \alpha(1;p)^2, \delta(p), \epsilon(p)\right\}.$$

The above values are all distinct except for the equation $\alpha(1;2)^2 = \alpha(3;2)$. Moreover,

$$\mathfrak{S}_{\text{ac}}(\mathcal{C}_{\text{fin}}) \cap [\epsilon(2), 1] = \{\alpha(k;2) \mid k \in \mathbb{N}\} \cup \{1, 5/9, 1/2, 15/32\}.$$

Comparing the above result with [2, Theorem 1], we see that

$$\mathfrak{S}_{\text{c}}(\mathcal{C}_p) \cap [\epsilon(p), 1] = \{\alpha(2k;p) \mid k \in \mathbb{N}\} \subsetneq \mathfrak{S}_{\text{ac}}(\mathcal{C}_p) \cap [\epsilon(p), 1],$$
$$\mathfrak{S}_{\text{c}}(\mathcal{C}_{\text{fin}}) \cap [\epsilon(2), 1] = \{\alpha(2k;2) \mid k \in \mathbb{N}\} \subsetneq \mathfrak{S}_{\text{ac}}(\mathcal{C}_{\text{fin}}) \cap [\epsilon(2), 1].$$

Not only are there more large anticommuting values than large commuting values, but the isomorphism types associated with large anticommuting values are considerably more diverse than those associated with large commuting values; see Theorem 4.6. It is because of this extra complexity that we chose a larger cutoff value than that employed in [2]; note that $\gamma(2) = 11/32$ but $\epsilon(2) = 15/32$.

After some preliminaries in Section 2, we characterize all values of $\Pr_f(R)$ for p-rings R (meaning rings in $\mathcal{C}_p$) satisfying $|f(R,R)| = p$ in Section 3; here $f(R,R)$ is the additive subgroup of R generated by all elements of the form $f(x,y)$, $x, y \in R$. There are two key ideas introduced in that section to accomplish this characterization: reductions to rings of a simpler form (split and canonical forms), and an augmentation process that produces a sequence of values of $\Pr_f(\cdot)$ once we find a single value $\Pr_f(R) < 1$. Split form also allows us to prove that the anticommuting spectrum for all finite rings, or all p-rings, equals the annihilating spectrum for all finite commutative rings, or all commutative p-rings, respectively.

Finally in Section 4, we prove Theorem 1.1. We also list there all possible isomorphism types of canonical-form commutative p-rings R with the property $\Pr_{\text{ann}}(R) \ge \epsilon(p)$.

2. Preliminaries

Rings and algebras are always assumed to be associative, but are not necessarily unital. The classes $\mathcal{C}_{\text{fin}}$ and $\mathcal{C}_p$ are as defined in the introduction; we call a ring in $\mathcal{C}_p$ a *p-ring*. We also define $\mathcal{C}_{\text{c}}$ to be the class of all finite commutative rings, and $\mathcal{C}_{\text{ac}}$ to be the class of all finite anticommutative rings. If R is a ring, then R^2 will always denotes the additive subgroup generated by all products xy, rather than the cartesian product which will be denoted $R \times R$. A *null ring* is a ring R with $R^2 = 0$.

$\mathbb{Z}_n$ 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. The *p-adic valuation* $\nu_p : \mathbb{Z} \setminus \{0\} \to \{0, 1, 2, \dots\}$ is defined by $\nu_p(n) = k$ whenever $n = ip^k$, $i, k \in \mathbb{Z}$, and i is not divisible by the prime p. If S is a subset of a vector space V, we write $\operatorname{span} S$ for the subspace spanned by S; usually V will be the additive group of a $\mathbb{Z}_p$-algebra.

$f(X, Y) := aXY + bYX$ is a *symbol*, with $a, b \in \mathbb{Z}$. Given a symbol f and a ring R, $f^R : R \times R \to R$ is defined by $f^R(x, y) := axy + byx$. Suppose R is a ring. For $x \in R$, we write $f(x, R)$ for the additive subgroup $\{f^R(x, y) \mid y \in R\}$ of $(R, +)$, and $f(R, R)$ is the additive subgroup generated by $f^R(x, y)$, $x, y \in R$. The *right f-annihilator of $x \in R$* is

$$\text{r-Ann}_{f,R}(x) := \{y \in R \mid f^R(x, y) = 0\},$$

and the *right f-annihilator of R* is

$$\text{r-Ann}_f(R) := \{z \in R \mid f^R(x, z) = 0 \text{ for all } x \in R\}.$$

The left-handed variants $\text{l-Ann}_{f,R}(x)$ and $\text{l-Ann}_f(R)$ are defined analogously. The *(two-sided) f-annihilator of R* is $\text{Ann}_f(R) := \text{r-Ann}_f(R) \cap \text{l-Ann}_f(R)$. These various annihilators are not in general ideals, so $R/\text{r-Ann}_f(R)$, $R/\text{ l-Ann}_f(R)$, $R/\text{ Ann}_f(R)$ always refer to factor groups of $(R, +)$. If $f(X, Y) = XY$, we drop references to f in the above terminology and notation, so $\text{r-Ann}_R(x)$ is the *right annihilator of $x \in R$*, $\text{Ann}(R)$ is the *annihilator of R*, etc.

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 a ring R equals $R_1 \oplus R_2$, then $\Pr_f(R) = \Pr_f(R_1) \Pr_f(R_2)$: this follows easily from the fact that the kernel of f^R is precisely the cartesian product of the kernels of f^{R_1} and f^{R_2}. Thus $\mathfrak{S}_f(\mathcal{C})$ is a monoid under multiplication, with 0 as an accumulation point, whenever $\mathcal{C}$ is a class of finite rings closed under direct sums that contains at least one commutative ring and at least one noncommutative ring.

Since a finite ring is a direct sum of rings of prime power order, it follows that the numbers in $\mathfrak{S}_f(\mathcal{C}_{\text{fin}})$ are precisely the set of all products $\prod_{i=1}^n t_i$, where $n \in \mathbb{N}$, $t_i \in \mathfrak{S}_f(\mathcal{C}_{p_i})$, and each p_i is prime. To understand the structure of $\mathfrak{S}_f(\mathcal{C}_{\text{fin}}) \cap [a, 1]$ for any given $0 < a < 1$, it therefore suffices to understand $\mathfrak{S}_f(\mathcal{C}_p) \cap [a, 1]$ for all primes p. For this reason, we mostly concentrate on investigating the spectra $\mathfrak{S}_f(\mathcal{C}_p)$.

By considering the surjective group homomorphism $f_x^R : R \to f(x, R)$, $f_x(y) = f(x, y)$, we make the following observation; note that $\ker f_x^R = \text{r-Ann}_{f,R}(x)$.

Observation 2.1. For each x in a ring R, the additive groups $R/\text{r-Ann}_{f,R}(x)$ and $f(x,R)$ are isomorphic.

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

$$\begin{aligned}\Pr_f(R) &= \frac{1}{|R|^2}\sum_{x\in R}|\,\text{r-Ann}_{f,R}(x)| = \frac{1}{|R|}\sum_{x\in R}\frac{1}{|R/\text{r-Ann}_{f,R}(x)|}\\ &= \frac{1}{|R|}\sum_{x\in R}\frac{1}{|f(x,R)|}\,.\end{aligned} \tag{2.1}$$

Since $\text{r-Ann}_{f,R}(x) = \text{r-Ann}_{f,R}(x+z)$, $z\in \text{l-Ann}_f(R)$, we can alternatively write

$$\Pr(R) = \frac{1}{|R/A|}\sum_{[x]\in R/A}\frac{1}{|f(x,R)|}\,, \tag{2.2}$$

whenever A is a subgroup of $(\text{l-Ann}_f(R),+)$; the sum above involves one term for each coset $[x]$ of A.

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

$$\Pr_f(R) = \sum_{k=0}^{\infty}\frac{q_k}{p^k} = (p-1)\sum_{k=0}^{\infty}\frac{Q_k}{p^{k+1}}\,, \tag{2.3}$$

where q_k is the proportion of cosets $x+\text{l-Ann}_f(R)$ in $R/\,\text{l-Ann}_f(R)$ such that $|f(x,R)| = p^k$, and $Q_k := \sum_{j=0}^{k} q_j$. Note that the series involving q_k is really a finite sum, but the one involving Q_k is always an infinite series: in fact $Q_k = 1$ for all sufficiently large k.

Related to the above discussion, we make the following useful observation.

Observation 2.2. If $a,b,a',b'\in R$, with $a-a', b-b'\in \text{Ann}_f(R)$, then $f^R(a,b) = f^R(a',b')$, so f^R induces a bilinear map $\tilde{f}^R : (R/\,\text{Ann}_f(R))\times(R/\,\text{Ann}_f(R))\to R$.

By the fundamental theorem of finite abelian groups, a finite abelian p-group $(A,+)$ can be decomposed as a direct sum

$$\boxplus_{i=1}^{m} C_{p^{k_i}}, \qquad k_1\ge k_2\ge \ldots k_m > 0,\ m\ge 0\,,$$

We call k_i the *i-th invariant of A*; these invariants and m are uniquely determined. A *basis of A* is a set $\{u_1,\ldots,u_m\}\subset A$, where each u_i is a generator of the ith summand $C_{p^{k_i}}$ (when we view A as an internal direct sum of such summands). Equivalently, a basis of A is a spanning set of A with the property that a sum of the form $\sum_{i=1}^{m} n_i u_i$, $n_i\in\mathbb{N}$, equals 0 only if each term $n_i u_i$ equals 0.

Finally in this section, we justify (1.2). The inequalities $1/p < \alpha(k+1;p) < \alpha(k;p)$ are obvious, once we write $\alpha(k;p) = p^{-1}+p^{-k-1}(p-1)$. Next, $\delta(2) = 1/2$, and the inequality $\delta(p) < 1/p$ is clear for $p\ge 3$. The inequality $\epsilon(p) < \delta(p)$ holds because

$$p^5(\delta(p)-\epsilon(p)) = (3p^3-2p^2)-(2p^3+p^2-3p+1) = (p-1)^3 > 0\,,$$

Finally, the inequality $\gamma(p) < \epsilon(p)$ holds because

$$p^5(\epsilon(p)-\gamma(p)) = (2p^3+p^2-3p+1)-(p^3+p^2-1) = (p+2)(p-1)^2 > 0\,.$$

It is noteworthy also that $\epsilon(p) = \alpha(1;p)\alpha(2;p)$.

3. Split form, canonical form, and augmentation

In this section, we discuss the concept of split- (and canonical-) form rings. Split-form rings are easier to handle than general rings for $\Pr_f$, and provide a useful reduction because for every finite ring R, there is a split-form ring S with $\Pr_f(R) = \Pr_f(S)$. This concept is an outgrowth of the concept of canonical form developed as part of the theory of isoclinism and isologism for certain universal algebras in [1], but here we develop the concept without reference to that theory.

We then define a process of augmentation that allows us to use existing values of $\mathfrak{S}_f(\mathcal{C}_p)$ to find new ones. In particular, we use this process for a general symbol f to help us characterize the set of values of $\Pr_f(R)$ for rings satisfying $|f(R,R)| = p$. Our augmentation process is related to that discussed in [2, Section 4]: in fact the earlier process roughly corresponds to the case where $f(X,Y) := XY - YX$ and S is a split-form noncommutative ring of order p^3 in the following definition.

3.1. **Split form and canonical form.**

Definition 3.1. A ring (or algebra) R has *split form (with data (R_1, R_2))* if it satisfies the following conditions:

(a) $(R,+)$ is an internal direct sum of two abelian groups R_1 and R_2, and we write elements $x \in S$ as $x_1 + x_2$, where $x_i \in R_i$, $i = 1, 2$.
(b) R_1 has an associated multiplication that makes it into a ring, and such that multiplication in R is then given by the equation

$$(x_1 + x_2)(y_1 + y_2) = 0 + x_1 y_1 \in R_2 \,.$$

Part (b) above can be rewritten as

$$R^2 \subseteq R_2 \subseteq \operatorname{Ann}(R) = \text{l-Ann}(R) \cap \text{r-Ann}(R) \,. \tag{3.1}$$

It is sometimes useful to replace these containments by equations, if possible.

Definition 3.2. A split-form ring (or algebra) R with data (R_1, R_2) is said to have *canonical form* if $\text{l-Ann}(R) = \text{r-Ann}(R) = R^2 = R_2$.

Given a split-form ring R, there may be more than one choice of data (R_1, R_2), although the split-form data are uniquely defined if R has canonical form, as is clear from (3.1).

We now describe the *split construction* which defines a split-type ring S associated with a given ring R. First, $(S,+)$ equals the internal direct sum of the abelian groups S_1 and S_2, where $S_1 := (R,+)$ and $S_2 := R^2$. Writing a general element of S as $x = x_1 + x_2$, $x_i \in A_i$, $i = 1, 2$, we define multiplication on S by the equation $(x_1 + x_2)(y_1 + y_2) = 0 + x_1 y_1 \in S_2$, where $x_1 y_1$ is an R-product.

The utility of the split construction is tied to the fact that it preserves several features of a ring R, as summarized below. These features imply that if we wish to investigate $\mathfrak{S}_f(\mathcal{C})$ for some class $\mathcal{C}$ of finite rings, then it often suffices to consider split-form rings. In the following observations, f can be any symbol, and we use the notation of the split construction above.

Observations 3.3.

(a) If R is a p-ring, or is commutative, or anticommutative, then S has the same property.
(b) $f(S,S)$ can be identified with $f(R,R)$.
(c) $A(S) = A(R) \boxplus S_2$, where $A(\cdot)$ stands for $\text{r-Ann}_f(\cdot)$, $\text{l-Ann}_f(\cdot)$, or $\operatorname{Ann}_f(\cdot)$.
(d) S has split form, with data (S_1, S_2).

(e) If R is finite, then $\Pr_f(R) = \Pr_f(S)$ (as follows from (2.2)).
(f) $S^3 = 0$.

We now give the *canonical construction* which defines a canonical-type ring S associated with a split-form ring R with data (R_1, R_2) that satisfies l-Ann(R) = r-Ann(R). Let $(S, +)$ be the internal direct sum of $S_1 := R_1/\operatorname{Ann}(R_1)$ and $S_2 = R^2$, and we write a general $x \in S$ as $x_1 + x_2$, where $x_1 \in S_1$ and $x_2 \in S_2$. Multiplication on S is defined by the rule $(x_1 + x_2)(y_1 + y_2) = 0 + u_1v_1 \in S_2$, where u_1v_1 is an R-product, and $u_1, v_1 \in R_1$ are such that $x_1 = u_1 + \operatorname{Ann}(R_1)$ and $y_1 = v_1 + \operatorname{Ann}(R_1)$.

We now state some readily verified properties of the canonical construction of S from a given split-form ring R, with notation as in the previous paragraph.

Observations 3.4.

(a) Observations 3.3 all hold (since canonical form is a special type of split form).
(b) $S^2 = S_2 = R^2$.
(c) $\operatorname{Ann}(S) = S_2$.
(d) S has canonical form, with data (S_1, S_2).
(e) The first invariant of $(S, +)$ equals the first invariant of both S_1 and S_2. In particular, S is a $\mathbb{Z}_p$-algebra if and only if S_1 is an elementary p-group.

Split form is of interest for all rings and all symbols f, while canonical form will mostly be of interest for $f(X, Y) = XY$ in the case of commutative and anticommutative rings. However we will see that it will be useful by extension when working with symbols of the form $f(X, Y) = a(XY \pm YX)$, $a \in \mathbb{N}$.

Given a split-form ring R, we can always define a new split-form ring with the same data $R' := (R, +, \circ)$, where $x \circ y := f^R(x, y)$; associativity follows from the split-form assumption. It is clear that $\Pr_{\text{ann}}(R') = \Pr_f(R)$. Since split-form rings give all possible values of $\Pr_f(\cdot)$, we deduce that $\mathfrak{S}_f(\mathcal{C}) \subseteq \mathfrak{S}_{\text{ann}}(\mathcal{C})$ if $\mathcal{C} = \mathcal{C}_{\text{fin}}$ or if $\mathcal{C} = \mathcal{C}_p$ for some prime p; these containments were originally proved in [1].

The containment $\mathfrak{S}_f(\mathcal{C}) \subseteq \mathfrak{S}_{\text{ann}}(\mathcal{C})$ might not be an equality: for instance, $\Pr_{\text{ann}}(\mathbb{Z}_2) = 3/4 \notin \mathfrak{S}_{\text{c}}(\mathcal{C}_{\text{fin}})$ according to the results of [2] or [11]. However we do have the following result.

Theorem 3.5. *Suppose p is a prime.*

(a) $\mathfrak{S}_{\text{ac}}(\mathcal{C}_{\text{fin}}) = \mathfrak{S}_{\text{ann}}(\mathcal{C}_{\text{c}})$ *and* $\mathfrak{S}_{\text{ac}}(\mathcal{C}_p) = \mathfrak{S}_{\text{ann}}(\mathcal{C}_{\text{c}} \cap \mathcal{C}_p)$.
(b) $\mathfrak{S}_{\text{c}}(\mathcal{C}_{\text{fin}}) = \mathfrak{S}_{\text{ann}}(\mathcal{C}_{\text{ac}})$ *and* $\mathfrak{S}_{\text{c}}(\mathcal{C}_p) = \mathfrak{S}_{\text{ann}}(\mathcal{C}_{\text{ac}} \cap \mathcal{C}_p)$.

Proof. We prove only (a) since the proof of (b) is similar. Since finite rings are direct sums of rings of prime power order, it suffices to prove that $\mathfrak{S}_{\text{ac}}(\mathcal{C}_p) = \mathfrak{S}_{\text{ann}}(\mathcal{C}_{\text{c}} \cap \mathcal{C}_p)$. When $f(x, y) = xy + yx$, the new multiplication for $x \circ y := f^R(x, y)$ considered above is commutative (and associative as long as R has split form, as mentioned above). Thus $\mathfrak{S}_{\text{ac}}(\mathcal{C}_p) \subseteq \mathfrak{S}_{\text{ann}}(\mathcal{C}_{\text{c}} \cap \mathcal{C}_p)$.

Conversely, if R is a commutative p-ring for some odd prime p, then $\Pr_{\text{ann}}(R) = \Pr_{\text{ac}}(R')$, where $R' := (R, +, *)$ and $x * y = 2^{-1}xy$. Thus $\mathfrak{S}_{\text{ann}}(\mathcal{C}_{\text{c}} \cap \mathcal{C}_p) = \mathfrak{S}_{\text{ac}}(\mathcal{C}_p)$ for all $p > 2$.

This argument can be modified to work also for $p = 2$. First, we assume as we may that the commutative ring R has split form with data (R_1, R_2). Write R_2 as an internal direct sum of groups U_i, $1 \le i \le m$, where each U_i is a cyclic group of order 2^{k_i} with generator u_i. Let S_2 be the abelian group which is an internal

direct sum of cyclic groups V_i of order 2^{k_i+1} with generators v_i, $1 \le i \le m$. We define an injective homomorphism $\mu_2 : R_2 \to S_2$ by the equations $\mu_2(u_i) = 2v_i$, $1 \le i \le m$. Let S be the commutative split-form ring with data (R_1, S_2) whose multiplication $*_S$ is defined by $x *_S y = \mu_2(xy) \in S_2$ for all $x, y \in R_1$, where xy is an R-product. Given $x, y \in R_1$ we have $xy = 0$ in R if and only if $x *_S y = 0$, and so $\Pr_{\text{ann}}(R) = \Pr_{\text{ann}}(S)$.

We choose a basis $\mathfrak{B} := \{u_1, \dots, u_m\}$ of R_1. Since $u_i *_S u_j \in 2S_2$ for all $u_i, u_j \in \mathfrak{B}$, we can define a function $F : \mathfrak{B} \times \mathfrak{B} \to S_2$ with the properties that $F(u_i, u_j) = F(u_j, u_i)$ and $2F(u_i, u_j) = u_i *_S u_j$ for all $1 \le i, j \le m$. Using bilinearity, we then define a new multiplication $*'_S$ on S such that $S' := (S, +, *')$ is a split-form commutative ring with data (R_1, S_2) satisfying $u_i *' u_j = F(u_i, u_j)$. By bilinearity, we deduce that $2x *' y = x *_S y$ for all $x, y \in S$. It follows that $\Pr_{\text{ac}}(S') = \Pr_{\text{ann}}(S)$, as required. □

Remark 3.6. The above theorem makes canonical form useful for studying $\Pr_{\text{c}}$ and $\Pr_{\text{ac}}$: we first transform the study of $\Pr_{\text{c}}(R)$ or $\Pr_{\text{ac}}(R)$ for p-rings R to the study of $\Pr_{\text{ann}}(S)$ for anticommutative or commutative p-rings S, respectively. By applying the canonical construction if necessary, we can then assume that S has canonical form (bearing in mind Observations 3.4).

Remark 3.7. For the benefit of someone who has read [1], we mention that replacing a ring R by a related canonical-form ring when investigating $\Pr_{\text{c}}$ or $\Pr_{\text{ac}}$ corresponds in the language of [1] to replacing R by a canonical-form ring for isologism with respect to the variety of commutative or anticommutative rings, respectively. Furthermore two rings are isologic in this sense if and only if the associated canonical-form rings are isomorphic; see [1, Theorem 4.16(b)]. Thus subsequent statements in this paper concerning isomorphism types of canonical-form rings with certain properties can be reworded as statements about the isologism types of rings with those properties.

We have the following variant of (2.2) for split-form rings R with data (R_1, R_2):

$$\Pr_f(R) = \frac{1}{|R_1|} \sum_{x_1 \in R_1} \frac{1}{|f(x_1, R)|}\,. \tag{3.2}$$

A *split ring homomorphism* h is a ring homomorphism between split-form rings R, S such that $h(R_i) \subseteq S_i$, $i = 1, 2$, where (R_1, R_2) and (S_1, S_2) are the data of R and S, respectively. *Split ring isomorphisms* are then defined in the natural way.

3.2. **Augmentation.**

Definition 3.8. Suppose R and S are split-form rings with data (R_1, R_2) and (S_1, S_2), respectively. Given an injective homomorphism $\mu : S_2 \to R_2$, we define $R \oplus_\mu S$, the *augmentation of R by S (via μ)*, to be the unique ring T with the following properties:

(a) $(T, +)$ equals the internal direct sum $R_1 \boxplus R_2 \boxplus S_1$.
(b) Write a general element $x \in T$ as $x = x_1 + x_2 + x_3$, where $x_1 \in R_1$, $x_2 \in R_2$, and $x_3 \in S_1$, multiplication in T is defined by

$$(x_1 + x_2 + x_3)(y_1 + y_2 + y_3) = 0 + [x_1 y_1 + \phi(x_3 y_3))] + 0 \in R_2\,.$$

It is convenient below to have an alternative notation for split-form data: if R has data (R_1, R_2), we write $\Delta_1(R) := R_1$ and $\Delta_2(R) := R_2$. In the following observations, we use the notation of Definition 3.8.

Observations 3.9.

(a) If R, S are both p-rings, or commutative, or anticommutative, then $R \oplus_\mu S$ has the same property.
(b) T has split form with data (T_1, T_2), where $T_1 := R_1 \boxplus S_1$ and $T_2 := R_2$, and T has canonical form if R and S both have canonical form.
(c) Writing $\mathrm{Ann}_f(R) = R_1' \boxplus R_2$ and $\mathrm{Ann}_f(S) = S_1' \boxplus S_2$ for some subgroups R_1' of R_1, and S_1' of S_1, we have $\mathrm{Ann}_f(T) = R_1' \boxplus R_2 \boxplus S_1'$.
(d) $f(T,T)$ can naturally be identified with $f(R,R) + f(S,S)$. If R has canonical form, then T^2 can be identified with R^2.
(e) If $\phi_R : R \to R'$ and $\phi_S : S \to S'$ are split ring isomorphisms between split-form rings R, S, then $R \oplus_\mu S$ is isomorphic to $R' \oplus_{\mu'} S'$, where $\mu' = \phi_R \circ \mu \circ (\phi_S^{-1})|_{S_2'}$ and $S_2' = \Delta_2(S')$.
(f) If a ring R is an internal direct sum of split-form rings R' and R'', and $\mu : S_2 \to \Delta_2(R')$, then $R \oplus_\mu S$ is isomorphic to $(R' \oplus_\mu S) \oplus R''$.
(g) Both R and S can naturally be viewed as ideals in T.

The proofs of the above observations are all rather obvious, and are left to the reader. As we will see, the choice of μ can affect the isomorphism type of an augmentation, so the definition of μ' in Observation 3.9(e) is essential.

We now discuss the relationship between $\mathrm{Pr}_f(R \oplus_\mu S)$, and $\mathrm{Pr}_f(R), \mathrm{Pr}_f(S)$, concentrating mostly on the case where $\Delta_2(S)$ is cyclic of order p, and R is a p-group for some prime p; even here, the choice of μ is important. We begin with a preparatory lemma.

Lemma 3.10. *If S is a p-ring with $|f(S,S)| = p$, then $\mathrm{Pr}_f(S) = \alpha(m;p)$, where $m = \dim S/\,\text{l-Ann}_f(S) > 0$.*

Proof. Since $|f(S,S)| = p$, $S/\,\text{l-Ann}_f(S)$ is necessarily a vector space over $\mathbb{Z}_p$ of positive dimension m. It follows from (2.2) that

$$\mathrm{Pr}_f(S) = \frac{1}{|S/\,\text{l-Ann}_f(S)|}\left(\frac{p^m - 1}{p} + 1\right) = \frac{p^m + p - 1}{p^{m+1}} = \alpha(m;p)\,,$$

as required. □

Remark 3.11. Given a ring S, it is clear that $\mathrm{Pr}_f(S) = \mathrm{Pr}_f(S^{\mathrm{op}})$, where S^{op} is the opposite ring with multiplication $x * y = yx$, and yx is an S-product. Since $\dim S/\,\text{l-Ann}_f(S)$ determines $\mathrm{Pr}_f(S)$ in the above lemma, we see that $|S/\,\text{l-Ann}_f(S)| = |S/\,\text{r-Ann}_f(S)|$ under the assumption that $|f(S,S)| = p$. This equation can fail if $|f(S,S)| > p$. For instance, let $f(X,Y) = XY$, and let S be the four-dimensional $\mathbb{Z}_p$-algebra with basis $\{u, v, w, z\}$ where the only nonzero products of basis elements are $u^2 = uv = w$ and $v^2 = vu = z$. We see that S has split form with data (S_1, S_2), where $S_1 := \mathrm{span}\{u, v\}$ and $S_2 := \mathrm{span}\{w, z\}$, Moreover $\text{l-Ann}_f(S) = S_2$ has dimension 2, while $\text{r-Ann}_f(S) = \mathrm{span}\{u - v, w, z\}$ has dimension 3.

We write $\Pr_f(R) = \Pr_f^+(R) + \Pr_f^-(R)$, where

$$\Pr_f^+(R) = \frac{1}{|R|} \sum_{\substack{x \in R \\ \mu(S_2) \subseteq f(x,R)}} \frac{1}{|f(x,R)|}\,,$$

$$\Pr_f^-(R) = \frac{1}{|R|} \sum_{\substack{x \in R \\ \mu(S_2) \not\subseteq f(x,R)}} \frac{1}{|f(x,R)|}\,.$$

If R has split form with data (R_1, R_2), we could equivalently write

$$\Pr_f^+(R) = \frac{1}{|R_1|} \sum_{\substack{x \in R_1 \\ \mu(S_2) \subseteq f(x,R)}} \frac{1}{|f(x,R)|}\,,$$

$$\Pr_f^-(R) = \frac{1}{|R_1|} \sum_{\substack{x \in R_1 \\ \mu(S_2) \not\subseteq f(x,R)}} \frac{1}{|f(x,R)|}\,.$$

Lemma 3.12. *Suppose R, S are split-form p-rings with data (R_1, R_2) and (S_1, S_2), respectively, for some prime p. Suppose also that $|S_2| = p$ and $\dim S/\,\text{l-Ann}_f(S) = m \in \mathbb{N}$. With the notation of the previous paragraph, we have*

$$\Pr_f(R \oplus_\mu S) = \Pr_f^+(R) + \Pr_f^-(R)\Pr_f(S) = \Pr_f^+(R) + \alpha(m;p)\Pr_f^-(R)\,. \tag{3.3}$$

In particular, $\Pr_f(R)\Pr_f(S) \le \Pr_f(R \oplus_\mu S) < \Pr_f(R)$.

Proof. Let $T := R \oplus_\mu S$. As before, we write a general element $x \in T$ as $x = x_1 + x_2 + x_3$, where $x_1 \in R_1$, $x_2 \in R_2$, and $x_3 \in S_1$. We say that $x \in T$ is of *Type A* if $\mu(S_2) \subseteq f(x_1, R)$, and of *Type B* otherwise. Since $m > 0$, we have $1 < |f(S,S)| \le |S_2| = p$, and so necessarily $|f(S,S)| = p$.

It is clear that $f(x,T)$ is the sum of the subgroups $f(x_1,R)$ and $f(x_3,S)$. Thus if x is Type A, then $f(x,T) = f(x_1,R)$, and the total contribution to $\Pr_f(T)$ of all Type A elements is precisely $\Pr_f^+(R)$.

Suppose instead that x is of Type B. Now $|f(x_3,S)|$ is either p or 1, depending on whether or not $x_3 \in \text{l-Ann}_f(S)$. In either case, we see that

$$|f(x,T)| = |f(x_1,R)| \cdot |f(x_3,S)|\,. \tag{3.4}$$

It follows that

$$\begin{aligned}\frac{1}{|T|} \sum_{x_3 \in S_3} \frac{1}{|f(x_1+x_2+x_3,T)|} &= \frac{1}{|R| \cdot |f(x_1,R)|} \left(\frac{1}{|S_3|} \sum_{x_3 \in S_3} \frac{1}{|f(x_3,S)|} \right) \\ &= \frac{\Pr_f(S)}{|R| \cdot |f(x_1,R)|} = \frac{\alpha(m;p)}{|R| \cdot |f(x_1,R)|}\,,\end{aligned}$$

where the last equation follows from Lemma 3.10. Summing these terms over all $x \in R$ of Type B, we get $\alpha(m;p)\Pr_f^-(R)$. Adding this to the Type A contribution, we deduce (3.3). Finally, the inequalities

$$\Pr_f(R)\Pr_f(S) \le \Pr_f(R \oplus_\mu S) < \Pr_f(R)$$

follow immediately from (3.3) because $\Pr_f^-(R) > 0$. □

We now prove a variation of Lemma 3.12 dealing with repeated augmentations using the same homomorphism μ, under the natural embedding of R in $R \oplus_\mu S$. We denote the n-fold repeated augmentation as $R \oplus_\mu^n S$, i.e. $R \oplus_\mu^0 S = R$, and $R \oplus_\mu^n S = (R \oplus_\mu^{n-1} S) \oplus_\mu S$ for all $n \in \mathbb{N}$.

Lemma 3.13. *Suppose R, S are p-rings of split form with data (R_1, R_2) and (S_1, S_2), respectively, for some prime p. Suppose also that $|S_2| = p$ and that $\dim S/\,\text{l-Ann}_f(S) = m$ for some $m \in \mathbb{N}$. With the same notation as in Lemma 3.12, we have*

$$\Pr(R \oplus_\mu^n S) = \Pr_f^+(R) + \alpha(mn; p) \Pr_f^-(R)\,, \qquad n \in \mathbb{N}\,. \tag{3.5}$$

Proof. Let $T_n := R \oplus_\mu^n S$. We view $(T_n, +)$ as an internal direct sum of R_1, R_2, and n distinct copies of S_1, and write a general element of T in the form $x = x_1 + x_2 + \sum_{i=3}^{n+2} x_i$, where x_{i+2} lies in the ith copy of S_1. Arguing as in the proof of Lemma 3.12, we see that if $\mu(S_2) \subseteq f(x_1, R)$, then $f(x, T) = f(x_1, R)$, and so the total contribution to $\Pr_f(T)$ of all such points is $\Pr_f^+(R)$. For all other points, we see that if $x_{i+2} \in \text{l-Ann}_f(S)$ for all $i > 2$ (a condition that corresponds to $\sum_{i=3}^{n+2} x_i$ representing the zero element of $\boxplus_{i=3}^{n+2} S/\,\text{l-Ann}_f(S)$), then $|f(x, T)| = |f(x_1, R)|$, and otherwise $|f(x, T)| = p\,|f(x_1, R)|$. Consequently, we see that

$$\begin{aligned}\frac{1}{|T_n|} \sum_{(x_3,\ldots,x_{n+2}) \in \boxplus_{i=3}^{n+2} S} \frac{1}{|f\left(\sum_{i=1}^{n+2} x_i, T_n\right)|} &= \frac{1}{|R| \cdot |f(x_1, R)|} \left(\frac{1}{p^{mn}} + \frac{1}{p} \cdot \frac{p^{mn} - 1}{p^{mn}}\right) \\ &= \frac{\alpha(mn; p)}{|R| \cdot |f(x_1, R)|}\,,\end{aligned}$$

and the lemma follows as before. □

Remark 3.14. Taking $R = S$ in Lemma 3.13, it is readily verified that

$$\Pr(S \oplus_{\text{Id}}^{n-1} S) = \alpha(mn; p)\,, \qquad n \in \mathbb{N}\,,$$

where $\text{Id} : S_2 \to S_2$ is the identity map. Thus, once we find a single number in the spectrum $\mathfrak{S}_f(\mathcal{C}_p)$ corresponding to a ring S as in the above lemmas, we immediately get an infinite sequence of elements of $\mathfrak{S}_f(\mathcal{C}_p)$. For future reference, we write $\text{Aug}(S, n) = S \oplus_{\text{Id}}^{n-1} S$.

Theorem 3.15. *Suppose $f(X, Y) = aXY + bYX$ is a symbol for some $a, b \in \mathbb{Z}$, and that at least one of a, b is nonzero. Suppose also that p is a prime. Then the elements of $\mathfrak{S}_f(\mathcal{C}_p)$ obtained by rings $R \in \mathcal{C}_p$ for which $|f(R, R)| = p$ are precisely:*

(a) *all numbers of the form $\alpha(n; p)$, $n \in \mathbb{N}$, if $a + b \neq 0$;*
(b) *all numbers of the form $\alpha(2n; p)$, $n \in \mathbb{N}$, if $a + b = 0$.*

Furthermore to achieve these values, it suffices to use commutative rings in (a), and anticommutative rings in (b).

Proof. Suppose first that $a + b \neq 0$, and let $k = \nu_p(a + b)$. It is readily verified that $R := \mathbb{Z}_{p^{k+1}}$ satisfies $|f(R, R)| = p$ and $\dim R/\,\text{l-Ann}_f(R) = 1$. This is not a split-form ring but we can apply the split construction to get the commutative ring S such that $(S, +)$ is isomorphic to $C_{p^{k+1}} \boxplus C_{p^{k+1}}$ and has basis $\{u, v\}$, with multiplication being defined by $u^2 = v$ and $uv = v^2 = 0$. Then

$|f(S,S)| = p$ and $\dim S/\,\text{l-Ann}_f(S) = 1$. By Lemma 3.10 and Remark 3.14, we have $\Pr_f(\text{Aug}(S,n)) = \alpha(n;p)$ for all $n \in \mathbb{N}$, and no other values of $\Pr_f(R)$ can occur for p-rings R satisfying $|f(R,R)| = p$. Since S is commutative, so is $\text{Aug}(S,n)$.

It remains to consider $f(X,Y) := a(XY - YX)$, $a \in \mathbb{N}$; in this case, we have $\text{l-Ann}_f(S) = \text{r-Ann}_f(S)$. Let $k = \nu_p(a)$ and assume $p > 2$. As an abelian group, we take $(S,+)$ to be $\boxplus_{i=1}^{3} C_{p^{k+1}}$, with basis $\mathfrak{B} := \{u,v,w\}$. Multiplication is defined by taking $uv = -vu = w$, and $xy = 0$ for all other pairs (x,y) of basis elements. It is readily verified that S is an anticommutative split-form $\mathbb{Z}_p$-algebra with data (S_1,S_2), where S_1 is the additive group generated by u and v, and S_2 the additive group generated by w. Also $f(S,S)$ is generated by $p^k w$, so $|f(S,S)| = p$. Since $\text{Ann}_f(S)$ is generated by $p^k u$, $p^k v$, and w, we have $|S/\,\text{Ann}_f(S)| = p^2$. Thus by Lemma 3.10, we have $\Pr_f(S) = \alpha(2;p)$, and so $\mathfrak{S}_f(\mathcal{C}_p)$ contains $\alpha(2n;p)$ for all $n \in \mathbb{N}$. Since S is anticommutative, so is the augmented ring $\text{Aug}(S,n)$ that gives rise to $\alpha(2n;p)$ for all $n \in \mathbb{N}$.

When $p = 2$, this construction needs to be tweaked. We instead take $(S,+)$ to be $\oplus_{i=1}^{3} C_{2^{k+2}}$. Then the rest of the proof is as before, except that $f(S,S)$ is generated by $2^{k+1}w$, and $\text{Ann}_f(S)$ is generated by $2^{k+1}u$, $2^{k+1}v$, and w.

Suppose conversely that $|f(R,R)| = p$ for some p-ring R. Without loss of generality, R has split form with data (R_1,R_2). We first define a new ring R', where $(R',+) = (R,+)$ and the multiplication $\circ$ of R' is defined by $x \circ y = f(x,y)$. Then R' is also a split-form ring with data (R_1,R_2), and by construction $\Pr_{\text{ann}}(R') = \Pr_f(R)$. Because of the form of f, R' is anticommutative and $\text{r-Ann}(R') = \text{l-Ann}(R')$. We now carry out the canonical construction to get an anticommutative canonical-form $\mathbb{Z}_p$-algebra S with data (S_1,S_2), where $S_1 = R_1/\,\text{Ann}(R_1)$, $S_2 = (R')^2$, and $\Pr_{\text{ann}}(S) = \Pr_{\text{ann}}(R')$.

To finish the proof of (b), it suffices by Lemma 3.10 to prove that $\dim S_1$ is even. This amounts to the claim that if S is a finite-dimensional anticommutative canonical-form $\mathbb{Z}_p$-algebra with data (S_1,S_2) such that $\dim S_2 = 1$, then S_1 has even dimension. For the sake of contradiction, we assume that this is false, and that $\dim S_1$ is minimal for such a counterexample.

Because S_2 is nontrivial, we can select nonzero $u,v \in S_1$ such that $uv \neq 0$. Since S is anticommutative, u and v are non-collinear. Moreover, $uS = vS = S_2$ is a vector space of dimension 1, so $\text{Ann}_S(u)$ and $\text{Ann}_S(v)$ both have codimension 1 in S. Since $v \in \text{Ann}_S(v) \setminus \text{Ann}_S(u)$, we see that $\text{Ann}_S(u)$ and $\text{Ann}_S(v)$ are distinct, and $U := \text{Ann}_S(u) \cap \text{Ann}_S(v)$ has codimension 2. It is also clear that U is of the form $U_1 \boxplus S_2$ for some subspace U_1 of S_1. Neither u nor v lie in U_1 since each fails to annihilate the other. It follows that u and U generate $\text{Ann}_S(u)$, that v and U generate $\text{Ann}_S(v)$, and that u, v, and U generate S. Thus $\dim U = \dim S - 2$.

We are done if $\dim S = 2$, so suppose $\dim S > 2$, and thus U is a nontrivial split-form $\mathbb{Z}_p$-algebra. Since $U_1 \subset S_1$, wS_1 is nontrivial for all nonzero $w \in U_1$. But U annihilates u and v, so in fact wU must be nontrivial. It follows that $U^2 = S_2$, and that $\text{Ann}(U) = S_2$. Thus U has canonical form and it satisfies the same assumptions as S, with data (U_1,S_2). Since $\dim U < \dim S$, $\dim U_1$ must be even. Now $\dim S_1 = \dim U_1 + 2$, and the claim follows. □

As previously claimed, the choice of μ can affect the isomorphism type of $R \oplus_\mu S$ even if $|\Delta_2(S)| = p$. We now verify this fact by giving an example where the choice of μ affects the annihilating probability of the augmented ring.

Proposition 3.16. *For each prime p, there exist canonical-type $\mathbb{Z}_p$-algebras R and S, with $\dim R = 5$, $\dim S = 2$, and $\dim \Delta_2(S) = 1$ such that $\Pr_{\text{ann}}(R \oplus_\mu S)$ can take on two distinct values depending on the choice of μ.*

Proof. Let R be the $\mathbb{Z}_p$-algebra with basis $\{u_1, u_2, u_3, z_1, z_2\}$, where $u_1^2 = u_2^2 = z_1$, $u_3^2 = z_2$, and all other products of basis elements are zero, and let S be the subalgebra of R with basis $\{u_1, z_1\}$. It is readily verified that R and S both have canonical type with data (R_1, R_2) and (S_1, S_2), respectively, where $R_1 := \text{span}\{u_1, u_2, u_3\}$, $R_2 := \text{span}\{z_1, z_2\}$, $S_1 := \text{span}\{u_1\}$, and $S_2 := \text{span}\{z_1\}$. Moreover it is clear that $\text{span}\{u_1, u_2, z_1\}$ is isomorphic to $\text{Aug}(S, 2)$, and so R is isomorphic to $\text{Aug}(S, 2) \oplus S$. Also let $S_2' := \text{span}\{z_1\}$ and $S_2'' := \text{span}\{z_2\}$.

We now augment R by (another copy of) S in two ways, namely via isomorphisms $\mu' : S \to S_2'$ and $\mu'' : S \to S_2''$. By Observation 3.9(f), $R \oplus_{\mu'} S$ is isomorphic to $\text{Aug}(S, 3) \oplus S$ and $R \oplus_{\mu''} S$ is isomorphic to $\text{Aug}(S, 2) \oplus \text{Aug}(S, 2)$. In view of Lemma 3.10, we see that

$$P_1 := \Pr_{\text{ann}}(R \oplus_{\mu'} S) = \Pr_{\text{ann}}(\text{Aug}(S, 3)) \cdot \Pr_{\text{ann}}(S) = \alpha(3; p) \cdot \alpha(1; p)$$

while

$$P_2 := \Pr_{\text{ann}}(R \oplus_{\mu''} S) = (\Pr_{\text{ann}}(\text{Aug}(S, 2)))^2 = \alpha(2; p)^2 .$$

Now $P_1 > P_2$ for all primes p since

$$p^6(P_1 - P_2) = (p^3 + p - 1)(2p - 1) - (p^2 + p - 1)^2 = p(p - 1)^3 .$$

Thus we have obtained two distinct values of $\Pr(R \oplus_\mu S)$ by varying μ. □

4. Large probability values

In this section, we find all possible values of $\mathfrak{S}_{\text{ac}}(\mathcal{C}_p)$ in the interval $[\epsilon(p), 1]$. However we begin by obtaining an upper bound on $\Pr_f(R)$ dependent on the largest order of elements in $R/\text{r-Ann}_f(R)$; for this result, f can be any symbol.

Theorem 4.1. *Suppose $f(X, Y) := aXY + bYX$ is a symbol, where $a, b \in \mathbb{Z}$ are not both zero. Let R be a finite p-ring for some prime p. Suppose the first invariant of $R/\text{r-Ann}_f(R)$ is $k \in \mathbb{N}$.*

(a) $\Pr_f(R) \le M(k; p) := (k(p - 1) + p)/p^{k+1}$.
(b) *Equality in (a) is attained if and only if $R/\text{r-Ann}_f(R)$ is isomorphic to C_{p^k}, and this is possible for a given symbol f if and only if $a + b$ is nonzero.*
(c) *$M(k; p)$ is strictly decreasing as a function of k, with $M(1; p) = \alpha(1; p)$, $M(2; p) = \delta(p)$, and $M(3; p) < \epsilon(p)$.*
(d) *In the case $k = 2$, if $R/\text{r-Ann}_f(R)$ is not isomorphic to C_{p^2}, then $\Pr_f(R) < \epsilon(p)$.*

Proof. Let us fix a p-ring R, and write $A := R/\text{r-Ann}_f(R)$. We also write $[x]$ for the A-coset containing $x \in R$, and $o_f(x)$ for the order of $[x]$ in A. We assume that k is the first invariant of A, i.e. p^k is the maximal value of $o_f(x)$.

Let A_j be the set of elements in A of order at most p^j, $j \ge 0$. Then $|A_j/A_{j-1}| \ge p$ for each $1 \le j \le k$. Thus if we define $R_j := |A_j|/|A|$ and $r_j := R_j - R_{j-1}$ for all $0 \le j$, then $R_j = 1$ for $j \ge k$ and $r_j \ge (p - 1)R_j/p$ for all $1 \le j \le k$. Iterating downwards from $j = k$, we see that $R_j \le p^{j-k}$ for all $0 \le j \le k$.

Since $|f(x,R)| \geq p^j$ whenever $[x] \in A$ has order p^j, it follows from (2.3) that

$$\Pr_f(R) \leq (p-1)\sum_{j=0}^{\infty} \frac{R_j}{p^{j+1}}\,,$$

Thus to maximize $\Pr_f(R)$ we should maximize every R_j. Equivalently, we should take $r_j = (p-1)/p^{k+1-j}$ for $1 \leq j \leq k$ and $r_0 = 1/p^k$. With these proportions, the q_k-form of the bound in (2.3) gives

$$\Pr_f(R) \leq \sum_{j=0}^{k} \frac{r_j}{p^j} = \frac{1}{p^k} + \sum_{j=1}^{k} \frac{p-1}{p^{k+1-j+j}} = M(k;p)\,, \tag{4.1}$$

thus finishing the proof of (a).

It is clear that equality in (4.1) can occur only if $R/\text{r-Ann}_f(R)$ is a cyclic group (of order p^k): in fact in this case we see that $|f(x,R)| = p^j$ whenever $[x] \in A$ has order p^j, so we get equality if and only if $R/\text{r-Ann}_f(R)$ is cyclic.

Suppose $a+b$ is nonzero, and let $m = \nu_p(a+b)$. Given $k \in \mathbb{N}$, it is readily verified that $R := \mathbb{Z}_{p^{k+m}}$ is such that $R/\text{r-Ann}_f(R)$ has elements of order p^k and $\Pr_f(R) = M(k;p)$.

Suppose instead that $a+b=0$ and that the first invariant of $R/\text{r-Ann}_f(R)$ is $k \in \mathbb{N}$. Now $a \neq 0$ and R is non-commutative. Note also that $\text{r-Ann}_f(R) = \text{Ann}_f(R)$. Since $f(x,x) = 0$ for all $x \in R$, and since there are elements x, y with $axy \neq ayx$, $R/\operatorname{Ann}_f(R)$ cannot be cyclic: in fact its first two invariants must be equal. Thus we cannot have $\Pr_f(R) = M(k;p)$, and we have finished the proof of (b).

Part (c) is rather easily proved. First, the proof that $M(k;p)$ is a strictly decreasing function of k is straightforward (or alternatively can be deduced from the discussion of the upper bound on $\Pr_f(R)$ above). The equations $M(1;p) = \alpha(1;p)$ and $M(2;p) = \delta(p)$ are trivial. The inequality $M(3;p) < \epsilon(p)$ holds because

$$p^5(\epsilon(p) - M(3;p)) = (2p^3 + p^2 - 3p + 1) - (4p^2 - 3p) = (2p+1)(p-1)^2 > 0\,.$$

Lastly we prove (d). Arguing as in (a), we see that we still have $Q_1 \leq p^{-1}$. However we now have $|A| \geq p^3$, so $Q_0 \leq p^{-3}$, and to maximize the upper bound on $\Pr_f(R)$, we take $Q_1 = p^{-1}$ and $Q_0 = p^{-3}$, or equivalently $q_2 = (p-1)/p$, $q_1 = (p^2-1)/p^3$, and $q_0 = 1/p^3$. With these values of q_i, we get

$$\Pr_f(R) \leq \frac{p-1}{p^{1+2}} + \frac{p^2-1}{p^{3+1}} + \frac{1}{p^3} = \frac{2p^2-1}{p^4}\,,$$

and this upper bound $\beta(p)$ is less than $\epsilon(p)$ because

$$p^5(\epsilon(p) - \beta(p)) = (2p^3 + p^2 - 3p + 1) - (2p^3 - p) = (p-1)^2\,. \tag{4.2}$$

□

If we want to find all elements of the set $\mathfrak{S}_f(\mathcal{C}_p) \cap [\epsilon(p), 1]$, then Theorem 4.1 says that rings R for which $R/\text{r-Ann}_f(R)$ fails to be a p-group are relevant only for $\Pr_f(R) = \delta(p)$, and it tells us when such examples exist. Thus it remains only to investigate the case where $R/\text{r-Ann}_f(R)$ is an elementary p-group.

Below, we carry out this analysis for the anticommuting symbol $f(X,Y) := XY + YX$. As a first step, we appeal to Theorem 3.5(a) to transform the problem into an investigation of $\mathfrak{S}_{\mathrm{ann}}(\mathcal{C}_{\mathrm{c}} \cap \mathcal{C}_p) \cap [\epsilon(p), 1]$. Since the rings of interest are commutative, it suffices to consider canonical-form rings R with data (R_1, R_2). Now R_1 is isomorphic to the elementary p-group $R/\operatorname{Ann}(R)$ and so, by Observation 3.4(e), R is a $\mathbb{Z}_p$-algebra.

Thus the task at hand is to compute all annihilating probabilities no less than $\epsilon(p)$ for commutative canonical-form $\mathbb{Z}_p$-algebras. Initially we will assume that R is *atomic*: by this we mean that R is both *unaugmented* (meaning that it is not the augmentation $U \oplus_\mu V$ for a canonical-form $\mathbb{Z}_p$-algebra V with $\dim V^2 = 1$) and *indecomposable* (i.e. it is not a direct sum of two nontrivial $\mathbb{Z}_p$-algebras). The following result will be useful.

Lemma 4.2. *Suppose R is an atomic canonical-form commutative $\mathbb{Z}_p$-algebra for some prime p, with data (R_1, R_2) where $\dim R_1 > 1$. Then $u^2 = 0$ whenever $u \in R$ is such that $\dim uR = 1$. More generally, we have $uv = 0$ for all pairs $u, v \in R$ for which $\dim uR = \dim vR = 1$ under either of the following additional assumptions:*

(a) $\dim R_1 > 2$*;*
(b) $p > 2$*.*

Proof. Suppose for the sake of contradiction that $u^2 \neq 0$ even though $\dim uR = 1$. We may assume that $u \in R_1$, since $R_2 = \operatorname{Ann}(R)$. Now $A' := \operatorname{Ann}_R(u)$ has codimension 1, and it has the form $A_1 \boxplus R_2$ for some $A_1 \subset R_1$. Since $u \notin A'$, we see that R_1 is the direct sum of $U_1 := \operatorname{span}\{u\}$ and A_1. Both $U_2 := \operatorname{span}\{u^2\}$ and $A_2 := A_1^2$ are subspaces of R_2, and both of the subspaces $U := U_1 \boxplus U_2$ and $A := A_1 \boxplus A_2$ of R are canonical-form subrings of R. Either U_2 is a subset of A_2, in which case R is an augmentation of A by U, or it is not a subset, in which case R is an internal direct sum of A and U. In either case, we get a contradiction to the atomicity hypothesis.

The proof that $uv = 0$ when $\dim uR = \dim vR = 1$ and $\dim R_1 > 2$ is similar. From (a), we already know that $u^2 = v^2 = 0$. Suppose for the sake of contradiction that $uv \neq 0$, and without loss of generality we assume that $u, v \in R_1$. Now $A' := \operatorname{Ann}_R(u) \cap \operatorname{Ann}_R(v)$ has codimension 2, and it has the form $A_1 \boxplus R_2$. The codimension-1 subspace $\operatorname{Ann}_R(u)$ is spanned by A' and u (since $u \notin \operatorname{Ann}_R(v)$), and R is spanned by u, v, and A' (since $v \notin \operatorname{Ann}_R(u)$). Letting $U_1 := \operatorname{span}\{u, v\}$, $U_2 := \operatorname{span}\{uv\}$, and $A_2 := A_1^2$, we can then finish the proof as before.

Finally, suppose that $\dim R_1 = 2$, $p > 2$, and $\dim uR = \dim vR = 1$. We know that $u^2 = v^2 = 0$, so suppose for the sake of contradiction that $uv = z$ is nonzero. Then $u' := u + v$ and $v' := u - v$ span R_1, $(u')^2 = 2z \neq 0$, and $u'v' = 0$. Thus $\dim u'R = 1$, and the fact that $(u')^2 \neq 0$ gives a contradiction. □

The condition $\dim uR = \dim vR = 1$ does not imply that $uv = 0$ when R is an atomic canonical-form commutative $\mathbb{Z}_2$-algebra, with data (R_1, R_2) where $\dim R_1 = 2$, as the following example shows.

Example 4.3. Consider the commutative $\mathbb{Z}_2$-algebra R with basis $\{u, v, z\}$, where $uv = vu = z$ and $u^2 = v^2 = 0$. Then R has canonical form with data (R_1, R_2), where $R_1 := \operatorname{span}\{u, v\}$ and $R_2 := \operatorname{span}\{z\}$, and $\dim xR = 1$ for all nonzero $x \in R_1$, since $(u + v)u = z$. However R is indecomposable because it has only four nontrivial proper ideals—one is R_2, while the other three are spanned by R_2

and a single nonzero element of R_1—and all contain R_2. It is also unaugmented because all of these ideals are null algebras so if we use them for augmentation we can only get other null algebras.

We now separately examine the cases where $R/\operatorname{Ann}(R)$ has dimension 2, or dimension at least 3. For dimension 2, we examine all possibilities regardless of whether or not $\Pr_{\text{ann}}(R) \geq \epsilon(p)$.

Theorem 4.4. *Suppose p is a prime, and R is a commutative atomic canonical-form $\mathbb{Z}_p$-algebra with data (R_1, R_2) such that $\dim R_1 = 2$. Writing $m = \dim R_2$, one of the following situations must occur:*

(a) *$m = 1$, $p = 2$, and $\Pr_{\text{ann}}(R) = \alpha(2;2)$.*
(b) *$m = 2$ and $\Pr_{\text{ann}}(R) = \delta(p)$.*
(c) *$m \in \{2, 3\}$ and $\Pr_{\text{ann}}(R) = (2p^2 - 1)/p^4 < \epsilon(p)$.*

Furthermore (a) is possible only for $p = 2$, in which case there is a unique isomorphism type, while for each prime p there is a unique isomorphism type giving (b). Finally for each prime p, there is a unique isomorphism type giving the $m = 3$ subcase of (c), and at least one isomorphism type giving the subcase $m = 2$ of (c), with uniqueness at least when $p = 2$.

Proof. The only possible values of $\dim xR$, for a nonzero element x of R_1 are 1 and 2.

Case 1: $\dim xR = 1$ *for all nonzero* $x \in R_1$.

Lemma 4.2 tells us that $x^2 = 0$ for all $x \in R$. Thus if $\{u, v\}$ is any basis of R_1, then $z := uv$ must be nonzero (lest R be a null ring, contradicting the canonical-form assumption), and it is clear that $R^2 = \operatorname{span}\{z\}$, so $m = 1$. Applying Lemma 4.2 again, we must have $p = 2$. The equation $\Pr_{\text{ann}}(R) = \alpha(2;2)$ now follows from Lemma 3.10. This possibility does occur, as we saw in Example 4.3. Since multiplication is fully specified, this case corresponds to a unique isomorphism type.

Case 2: $\dim xR$ *takes on both the values* 1 *and* 2 *for different choices of* $x \in R_1$.

We select $u, v \in R_1$ such that $\dim uR = 1$ and $\dim vR = 2$. By Lemma 4.2, $u^2 = 0$. The equation $\dim vR = 2$ forces the products $z_1 := uv$ and $z_2 := v^2$ to be non-collinear. Given that $R_2 = \operatorname{span}\{z_1, z_2\}$, this fully specifies multiplication on R, so we have shown that there is exactly one isomorphism type for each prime p. It is readily verified that if $x = au + bv$ for $a, b \in \mathbb{Z}_p$, then $\dim xR = 2$ whenever $b \neq 0$, and $\dim xR = 1$ whenever $b = 0$ and $a \neq 0$. We therefore deduce from (3.2) that

$$\Pr_{\text{ann}}(R) = \frac{1}{p^2}\left(\frac{p^2 - p}{p^2} + \frac{p-1}{p} + 1\right) = \delta(p)\,.$$

It remains to verify that R is atomic. Suppose for the sake of contradiction that R is of the form $U \oplus_\mu V$, where V is a canonical-form $\mathbb{Z}_p$-algebra V with $\dim V^2 = 1$. Let (U_1, U_2) and (V_1, V_2) be the data of U and V, respectively, and so $V_2 = V^2$. Since $\mu : V_2 \to U_2$, $\dim U_2 \geq 1$. Thus $\dim U_1 \geq \dim U/\operatorname{Ann}(U) \geq 1$ and $\dim V_1 = \dim V/\operatorname{Ann}(V) \geq 1$. But it follows from Observation 3.9(c) with $f(X, Y) := XY$ that $2 = \dim R_1 = \dim U/\operatorname{Ann}(U) + \dim V/\operatorname{Ann}(V)$, so we must have $\dim U_1 = 1$ and so $\dim U^2 = 1$. But now by Observation 3.9(d), $\dim R^2 = 1$, contradicting the fact that $\dim R^2 = 2$.

Suppose instead that R is a direct sum of nontrivial algebras U and V. It is clear that $\operatorname{Ann}(R) = \operatorname{Ann}(U) \boxplus \operatorname{Ann}(V)$ and $R^2 = U^2 \boxplus V^2$, so we have $\operatorname{Ann}(U) = U^2$ and $\operatorname{Ann}(V) = V^2$. Also

$$R/\operatorname{Ann}(R) = (U/\operatorname{Ann}(U)) \boxplus (V/\operatorname{Ann}(V))$$

so

$$\dim U/\operatorname{Ann}(U) + \dim V/\operatorname{Ann}(V) = 2\,.$$

If one of these factor spaces has dimension 2, say $\dim U/\operatorname{Ann}(U) = 2$, then $\dim V/\operatorname{Ann}(V) = 0$. But then V would be a null ring, so $V = \operatorname{Ann}(V)$ and also $\operatorname{Ann} V = V^2 = 0$, so V would be trivial, contradicting our hypotheses. Thus $\dim U/\operatorname{Ann}(U) = \dim V/\operatorname{Ann}(V) = 1$, and so $\dim U^2 = \dim V^2 = 1$. By Lemma 3.10, $\Pr_{\text{ann}}(U) = \Pr_{\text{ann}}(V) = \alpha(1;p)$, forcing the equation $\delta(p) = \alpha(1;p)^2$. But this equation fails for all primes p since

$$p^4(\alpha(1;p)^2 - \delta(p)) = (2p-1)^2 - (3p^2 - 2p) = (p-1)^2 > 0\,. \tag{4.3}$$

This concludes the proof that R is atomic.

Case 3: $\dim xR = 2$ *for all nonzero* $x \in R_1$.

It readily follows from (3.2) that $\Pr_{\text{ann}}(R) = (2p^2-1)/p^4$, and this is less than $\epsilon(p)$ by (4.2). It is readily verified that this occurs if $m = 3$, $\{u, v\}$ is a basis of R_1, $\{z_1, z_2, z_3\}$ is a basis of R_2, and $u^2 = z_1$, $v^2 = z_2$, and $uv = vu = z_3$.

Conversely, the condition $\dim uR = \dim vR = 2$ requires that $z_1 := u^2$ and $z_3 := uv$ are non-collinear, and that $z_2 := v^2$ and z_3 are non-collinear. If $\{z_1, z_2, z_3\}$ is a linearly independent set, then we are in the $m = 3$ situation above, and the isomorphism type of R is uniquely specified. However we claim that even in the absence of independence, it is possible that $\dim xR$ may equal 2 for all $x \in R_1$.

For $p = 2$, we take $z_3 = z_1 + z_2$. Then $(u+v)^2 = z_1 + z_2$ and $(u+v)u = z_1 + z_3 = z_2$, giving $\dim(u+v)R = 2$ and so $\dim xR = 2$ for all nonzero $x \in R$. It is readily verified that if we instead chose $z_3 \in \{z_1, z_2\}$, then we would get $\dim(u+v)R = 1$, so there is a unique isomorphism type giving $m = 2$ when $p = 2$.

Suppose instead that $p > 2$. Let $s \in \mathbb{Z}_p$ be a quadratic nonresidue mod p, and let $c \in \mathbb{Z}_p$ be defined by $c := 4^{-1}(1-s)$. Then $1 - 4c = s$, so it follows that the quadratic $g(a) := a^2 + a + c$ has no roots in $\mathbb{Z}_p$. Let R be the canonical-type $\mathbb{Z}_p$-algebra with data (R_1, R_2) where $\{u, v\}$ is a basis of R_1, $\{z_1, z_2\}$ is a basis of R_2, and $u^2 = z_1$, $v^2 = z_2$, and $uv = vu = cz_1 + z_2$. Certainly $\dim uR = 2$, so to prove that $\dim xR = 2$ for all $x \in R_1$, it suffices to prove this when $x = au + v$ for some $a \in \mathbb{Z}_p$. For such an element x, we have $xu = (a+c)z_1 + z_2$ and $xv = acz_1 + (1+a)z_2$. Thus $\dim xR = 2$ if (and only if) the associated matrix

$$M := \begin{pmatrix} a+c & 1 \\ ac & 1+a \end{pmatrix}$$

is nonsingular. But $\det M = (a+c)(1+a) - ac = g(a)$ has no roots, so our claim is proved.

We have shown that this case yields exactly two isomorphism types when $p = 2$, and at least two when $p > 2$. We will not investigate whether or not there are more than one isomorphism type corresponding to $m = 2$ for $p > 2$.

It remains to show that these rings are atomic. The proof that they are unaugmented is exactly as in Case 2, as is the proof that the $m = 2$ ring is indecomposable. The proof for the $m = 3$ ring starts in a similar fashion, but

we get a contradiction from the fact that $\dim S/\operatorname{Ann}(S) = \dim T/\operatorname{Ann}(T) = 1$, whereas one of S^2 and T^2 must have dimension 2. □

We now consider atomic algebras R with $\dim R/\operatorname{Ann}(R) \geq 3$.

Theorem 4.5. *If R is a commutative atomic canonical-form $\mathbb{Z}_p$-algebra with data (R_1, R_2) and $\dim R_1 \geq 3$, then $\Pr_{\text{ann}}(R) < \epsilon(p)$.*

Proof. Suppose first that $\dim xR \leq 1$ for at most p of the elements of R_1. By (3.2),

$$\Pr_{\text{ann}}(R) \leq \frac{1}{p^3}\left(\frac{p^3-p}{p^2} + \frac{p-1}{p} + 1\right) = \frac{p^2+2p-2}{p^4}\,.$$

This bound is less than $\epsilon(p)$ because

$$p^5\epsilon(p) - p(p^2+2p-2) = (p+1)(p-1)^2\,.$$

Thus we may assume that $\dim xR \leq 1$ for more than p elements of R_1, and so there exists a two-dimensional subspace T of R_1 spanned by elements u_1, u_2 such that $\dim u_1R = \dim u_2R = 1$. By Lemma 4.2 and distributivity, $xy = 0$ for all $x, y \in T$. Letting $w \in R_1 \setminus T$, we deduce that u_1w and u_2w must both be nonzero, since otherwise u_1 or u_2 would be an element of $\operatorname{Ann}(R)$, contradicting the canonical-form assumption. Furthermore u_1w and u_2w must be non-collinear, since otherwise some linear combination of u_1 and u_2 would similarly contradict the canonical-form assumption. We deduce that if x is a linear combination of u_1, u_2, and w, with the w-coefficient being nonzero (in $\mathbb{Z}_p$), then $\dim xR \geq 2$. Thus

$$\Pr_{\text{ann}}(R) \leq \frac{1}{p^3}\left(\frac{p^3-p^2}{p^2} + \frac{p^2-1}{p} + 1\right) = \frac{2p^2-1}{p^4}\,,$$

which is less than $\epsilon(p)$ according to (4.2). □

Proof of Theorem 1.1. As discussed above, the task of finding all possible values in $\mathfrak{S}_{\text{ac}}(\mathcal{C}_p) \cap [\epsilon(p), 1]$ is reduced to finding all possible values of $\Pr_{\text{ann}}(R) \geq \epsilon(p)$ when R is a commutative canonical-form p-ring. The data of R will be denoted (R_1, R_2) as usual, and we write $m_i := \dim R_i$, $i = 1, 2$.

Based on our work above, it is straightforward to calculate the values that occur when R is an atomic canonical-form $\mathbb{Z}_p$-algebra; we call these *atomic values*. If $m_1 = 0$, then necessarily $m_2 = 0$, so R is the trivial ring and $\Pr_{\text{ann}}(R) = 1$. If $m_1 = 1$, then necessarily $m_2 = 1$, and $\Pr_{\text{ann}}(R) = \alpha(1; p)$ now follows from Lemma 3.10. Both of these rings are clearly atomic. Theorems 4.4 and Theorem 4.5 tell us that the only possible atomic values in $[\epsilon(p), 1]$ corresponding to $m_1 \geq 2$ are $\alpha(2; 2)$ and $\delta(p)$.

The value $\delta(p)$ also occurs for commutative p-rings R that are not $\mathbb{Z}_p$-algebras according to Theorem 4.1, but such rings give no other values in $[\epsilon(p), 1]$. Since $R/\operatorname{Ann}(R)$ is cyclic and R has canonical form, we see that R can only have one isomorphism type: for $i = 1, 2$, R_i is isomorphic to C_{p^2} and has generator u_i, with $u_1^2 = u_2$ and $u_iu_j = 0$ for all other choices of i, j.

It remains to investigate what can be found by augmentation of the (nontrivial) atomic $\mathbb{Z}_p$-algebras above by a canonical-form $\mathbb{Z}_p$-algebra V with $\dim V^2 = 1$, or by direct sums of non-null algebras (since a null ring direct summand leaves the annihilating probability unchanged). Both of these processes strictly decrease the annihilating probability—in the case of augmentation because of (3.3)—so it

suffices to apply these processes iteratively to the atomic algebras R above for which $\mathrm{Pr}_{\mathrm{ann}}(R) = \alpha(1;p)$, $\mathrm{Pr}_{\mathrm{ann}}(R) = \alpha(2;2)$, or $\mathrm{Pr}_{\mathrm{ann}}(R) = \delta(p)$.

The algebras with $\mathrm{Pr}_{\mathrm{ann}}(R) = \alpha(1;p)$ or $\mathrm{Pr}_{\mathrm{ann}}(R) = \alpha(2;2)$ both satisfy $|R^2| = p$, so augmentation yields only algebras R' with $\mathrm{Pr}_{\mathrm{ann}}(R') = \alpha(k;p)$ for some $k \in \mathbb{N}$. Repeated augmentation of the algebra R with $\mathrm{Pr}_{\mathrm{ann}}(R) = \alpha(1;p)$ yields all numbers $\alpha(k;p)$, $k \in \mathbb{N}$ by Remark 3.14.

Next we consider augmenting the algebra R in Theorem 4.4(b) for which $\mathrm{Pr}_{\mathrm{ann}}(R) = \delta(p)$. Since the contribution to $\mathrm{Pr}^-_{\mathrm{ann}}(R)$ always includes the contributions of all elements of R_2, we see that $\mathrm{Pr}^-_{\mathrm{ann}}(R) \geq 1/p^2$, and so $\mathrm{Pr}^+_{\mathrm{ann}}(R) \leq \delta(p) - 1/p^2$. If $R \oplus_\mu V$ is any augmentation with $|V^2| = p$, then (3.3) and (4.2) together imply that

$$\mathrm{Pr}_{\mathrm{ann}}(R \oplus_\mu V) \leq \frac{2p-2}{p^3} + \frac{2p-1}{p^2} \cdot \frac{1}{p^2} = \frac{2p^2-1}{p^4} < \epsilon(p)\,,$$

so these algebras give no new values.

For direct sums applied to the above atomic algebras and their augmentations, we must consider products of values that we already have. We first recall that $\alpha(1;p)\alpha(2;p) = \epsilon(p)$, so this gives us one new value. In view of (1.2), it follows that it remains only to consider powers of $\alpha(1;p)$. But

$$p^4(\alpha(2;p) - \alpha(1;p)^2) = (p-1)^3 > 0\,,$$

so $\alpha(1;p)^3 < \epsilon(p)$. Thus we need only consider $\alpha(1;p)^2$, a number that by (4.3) exceeds $\delta(p)$. Now $\alpha(k;p) > 1/p$ for all $k \in \mathbb{N}$, whereas $\alpha(1;3)^2 < 1/3$ and for $p \geq 5$, $\alpha(1;p)^2 \leq (2/p)^2 < 1/p$. Thus $\alpha(1;p)^2$ is a new value for all $p > 2$, but $\alpha(1;2)^2 = \alpha(3;2)$.

The next step is to augment the one new canonical-form algebra R with $\mathrm{Pr}_{\mathrm{ann}}(R) > \epsilon(p)$ that we obtained by a direct sum. This is a $\mathbb{Z}_p$-algebra with $\mathrm{Pr}_{\mathrm{ann}}(R) = \alpha(1;p)^2$, with basis $\{u_1, u_2, z_1, z_2\}$, where $u_i^2 = z_i$, $i = 1, 2$, and all other products of basis elements are zero. We write $R_1 := \mathrm{span}\{u_1, u_2\}$ and $R_2 := \mathrm{span}\{z_1, z_2\}$ as usual, and write a general element $x \in R$ in the form $x = a_1u_1 + a_2u_2 + b_1z_1 + b_2z_2$ for $a_i, b_i \in \mathbb{Z}_p$. We also denote by $\{v, w\}$ the basis of the $\mathbb{Z}_p$-algebra S that we use for augmentation; here $v^2 = w$ and $vw = wv = w^2 = 0$, and the data of S is (S_1, S_2), where $S_1 := \mathrm{span}\{v\}$ and $S_2 := \mathrm{span}\{w\}$.

If a_1 and a_2 are both nonzero, then it is readily verified that $xR = R_2$, so x contributes to $\mathrm{Pr}^+_{\mathrm{ann}}(R)$ in (3.3) regardless of the augmentation function μ. By contrast, if $a_1 = a_2 = 0$, then x contributes to $\mathrm{Pr}^-_{\mathrm{ann}}(R)$ in (3.3). However elements x with one but not both of a_1 and a_2 nonzero satisfy $\dim xR = 1$, and so the choice of μ affects whether such elements x contribute towards $\mathrm{Pr}^+_{\mathrm{ann}}(R)$ or $\mathrm{Pr}^-_{\mathrm{ann}}(R)$. As is clear from (3.3), maximizing $\mathrm{Pr}_{\mathrm{ann}}(R \oplus_\mu S)$ for a given S is equivalent to maximizing the number of such elements that contribute to $\mathrm{Pr}^+_{\mathrm{ann}}(R)$. Since for such elements, xR is either $\mathrm{span}\{z_1\}$ or $\mathrm{span}\{z_2\}$, $\mathrm{Pr}_{\mathrm{ann}}(R \oplus_\mu S)$ is maximized when $\mu : S_2 \to R_2$ is the homomorphism with the property $\mu(w) = z_1$. By construction, R is a direct sum of two isomorphic copies of S, and the condition $\mu(w) = z_1$ means that Observation 3.9(f) is applicable. Thus $R \oplus_\mu S$ is isomorphic to $\mathrm{Aug}(S, 2) \oplus S$ and

$$\mathrm{Pr}_{\mathrm{ann}}(R \oplus_\mu S) = \alpha(1;p)\alpha(2;p) = \epsilon(p)\,.$$

This is a value that we already have, and in fact $\mathrm{Aug}(S,2) \oplus S$ is the same canonical-form isomorphism type that gave that value in the previous direct sum stage of this proof. We have now completed the proof that $\mathfrak{S}_{\mathrm{ac}}(\mathcal{C}_p) \cap [\epsilon(p), 1]$ is as stated.

Finally to compute $\mathfrak{S}_{\mathrm{ac}}(\mathcal{C}_{\mathrm{fin}}) \cap [\epsilon(2), 1]$, we need to take products of elements in $\mathfrak{S}_{\mathrm{ac}}(\mathcal{C}_p)$ for distinct primes p. First we have all the values in $\mathfrak{S}_{\mathrm{ac}}(\mathcal{C}_2) \cap [\epsilon(2), 1]$. These give 1, $\alpha(k;2)$ for all $k \in \mathbb{N}$, $9/16 = \alpha(1;2)^2 = \alpha(3;2)$, $1/2 = \delta(2)$, and $15/32 = \epsilon(2)$. We get nothing additional from primes $p > 5$ because in this case $(2p-1)/p^2 < 2/p < 15/32$. Taking $p = 3$ does give one additional value, namely $\alpha(1;3) = 5/9$, but it gives no other new values because $\alpha(2;3) = 11/27$ and $\alpha(1;2)\alpha(1;3) = 5/12$ are both less than $15/32$. □

Although we did not explicitly state it in Theorem 1.1, we can read off all isomorphism types of canonical-form commutative p-rings R satisfying $\Pr_{\mathrm{ann}}(R) \geq \epsilon(p)$ from the above proofs. These types consist of the trivial ring, a one-parameter of algebras giving $\Pr(R) = \alpha(k;p)$ for all $k \in \mathbb{N}$, and either six (for $p = 2$) or four (for $p > 2$) other types, as detailed in the following theorem.

Theorem 4.6. *The following list gives all possible isomorphism types of canonical-form commutative p-rings R with $\Pr_{\mathrm{ann}}(R) \geq \epsilon(p)$ for a given prime p.*

(a) $\Pr_{\mathrm{ann}}(R) = 1$ *for the trivial algebra R.*
(b) $\Pr_{\mathrm{ann}}(R) = \alpha(k;p)$, $k \in \mathbb{N}$, *for the algebra R with basis $\{u_1, \ldots, u_k, z\}$, where $u_i^2 = z$ for all $1 \leq i \leq k$, and all other products of basis elements are zero.*
(c) $\Pr_{\mathrm{ann}}(R) = \alpha(2;2)$ *for the atomic algebra R of Theorem 4.4(a).*
(d) $\Pr_{\mathrm{ann}}(R) = \alpha(1;p)^2$ *for a direct sum algebra R constructed in the proof of Theorem 1.1.*
(e) $\Pr_{\mathrm{ann}}(R) = \delta(p)$ *for the algebra R of Theorem 4.4(b).*
(f) $\Pr_{\mathrm{ann}}(R) = \delta(p)$ *for the canonical construction applied to a ring R given by Theorem 4.1(b) for $k = 2$.*
(g) $\Pr_{\mathrm{ann}}(R) = \epsilon(p)$ *for the algebra $R := \mathrm{Aug}(S,2) \oplus S$, where S is the unique canonical-form commutative $\mathbb{Z}_p$-algebra with $\Pr_{\mathrm{ann}}(S) = \alpha(1;p)$.*
(h) $\Pr_{\mathrm{ann}}(R) = \epsilon(2)$ *for the algebra $R := T \oplus S$, where S is as in (g) for $p = 2$, and T is the algebra in (c).*

All rings listed above give distinct isomorphism types, but note that (c) and (h) are for $p = 2$ only.

We omit most of the proof of Theorem 4.6, since it is contained in our earlier proofs. The fact that the isomorphism type in (f) is unique follows from the fact that $R/\operatorname{Ann}(R)$ is cyclic, as discussed in the proof of Theorem 1.1. The one other aspect of the proof upon which we should comment is the fact that the various isomorphism types listed are distinct. For $p > 2$, this follows from the fact that there is only one isomorphism type for each value of $\Pr_{\mathrm{ann}}(R)$, with the exception of $\delta(p)$ which is associated with both an algebra and a non-algebra.

For $p = 2$, there are three other duplicate sets of $\Pr_{\mathrm{ann}}(R)$ values. First, $\alpha(2;2)$ is given by an augmented algebra in (b) and an atomic algebra in (c), so these are necessarily distinct. Also, $\alpha(3;2) = \alpha(1;2)^2$ is associated with an augmented algebra R in (b) and a direct product algebra in (d), and these are distinguished by the dimension of R^2. The algebras in (g) and (h) are distinguished by the number of elements x with $x^2 \neq 0$: there are two such elements in (g) and none in (h).

The set of types given in Theorem 4.6 is considerably more diverse than the set of types of canonical-form p-rings with $\Pr_c(R) \geq \epsilon(p)$, which can be deduced from [2, Theorem 1.2]. For the latter problem and any given prime p, we get a null algebra for $\Pr_c(R) = 1$, one algebra for $\Pr_c(R) = \alpha(2k; p)$, $k \in \mathbb{N}$, and nothing else. The extra complexity is a direct result of the fact that x^2 can be nonzero in a commutative ring, in contrast to the fact that it must equal zero in an anticommutative ring.

References

[1] S.M. Buckley, *Distributive algebras, isoclinism, and invariant probabilities*, preprint.

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

[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. Hegarty, *Limit points in the range of the commuting probability function on finite groups*, J. Group Theory, to appear.

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

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

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

[12] 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

Yu. Zelenyuk:
School of Mathematics, University of the Witwatersrand, Wits 2050, Johannesburg, South Africa.
E-mail address: yuliya.zelenyuk@wits.ac.za