Odd order rings with many idempotents

STEPHEN M. BUCKLEY AND DESMOND MACHALE

ABSTRACT. Let $\mathrm{Pr_I}(R)$ be the proportion of idempotents in a ring R, and suppose p is an odd prime. We find all values of $\mathrm{Pr_I}(R) \in [1/p, 1]$ when R is a (finite) p-ring, and all values of $\mathrm{Pr_I}(R) \in [1/3, 1]$ when R is a ring of odd order. Additionally, we characterize all the possible isomorphism types of R with $\mathrm{Pr_I}(R) > 1/p$. Rings can be replaced by the larger class of possibly nonassociative rings R without affecting the sets of values of $\mathrm{Pr_I}(R) > 1/p$ that occur; in this case, we characterize all possible Jordan isomorphism types of R.

1. INTRODUCTION

The *idempotent proportion* $\mathrm{Pr_I}(R)$ of a finite possibly nonassociative ring R is defined by $\mathrm{Pr_I}(R) = m/|R|$, where m is the number of idempotents in R. In this paper, we study the sets

$$\mathcal{I}_{\mathrm{odd}} = \{\mathrm{Pr_I}(R) \mid R \text{ is a (possibly non-unital) ring of odd order}\},$$
$$\mathcal{I}_p = \{\mathrm{Pr_I}(R) \mid R \text{ is a (possibly non-unital) } p\text{-ring}\},$$

where p is an odd prime and a *p-ring* means a ring of order p^n for some $n \geq 0$. We also study the corresponding sets $\mathcal{I}_{\mathrm{odd,na}}$ and $\mathcal{I}_{p,\mathrm{na}}$ defined in terms of possibly nonassociative rings, so trivially $\mathcal{I}_{\mathrm{odd}} \subset \mathcal{I}_{\mathrm{odd,na}}$ and $\mathcal{I}_p \subset \mathcal{I}_{p,\mathrm{na}}$. The sets $\mathcal{I}_p$ and $\mathcal{I}_{p,\mathrm{na}}$ for $p = 2$ are studied in [3].

Let us first recall a result of the second author [8, Theorem 3].

Theorem A. *For each odd prime p, $\mathcal{I}_p \cap (1/(p-1), 1] = \{1, 2/p\}$, and the only p-rings R with $\mathrm{Pr_I}(R)$ in this range are the ring of order 1, and $\mathbb{Z}_p$.*

It is conjectured in [8] that the number $1/(p-1)$ in Theorem A could be replaced by the strictly smaller value $(p+1)/p^2$. Our first main result explicitly lists all elements of $\mathcal{I}_p \cap [1/p, 1]$, thereby implying this conjecture *en passant*.

Let us first define, for all primes p, the set $\mathfrak{A}_p := \{a(n,p) \mid 0 \leq n \leq \infty\}$, where

$$a(n,p) := \begin{cases} 1, & n = 0\,, \\ (p^{n-1}+1)/p^n, & n \in \mathbb{N}\,, \\ 1/p, & n = \infty\,. \end{cases}$$

Also let $N(n,p)$ be the number of isomorphism types of p-rings for which $\mathrm{Pr_I}(R) = a(n,p)$, and let $N_J(n,p)$ and $N_{J,\mathrm{na}}(n,p)$ be the number of Jordan isomorphism types of p-rings and possibly non-associative p-rings, respectively,

Date: 22.11.2013.

2010 *Mathematics Subject Classification.* 16U99.

Key words and phrases. rings, nonassociative rings, idempotent proportion, Jordan isomorphism.

for which $\Pr_{\mathrm{I}}(R) = a(n,p)$. Jordan isomorphisms are defined in Section 2; we consider them in this paper because idempotent proportion is a Jordan isomorphism invariant for rings of odd order.

Theorem 1.1. *Suppose p is an odd prime.*

(a) If R is a possibly nonassociative p-ring with $\Pr_{\mathrm{I}}(R) > 2/p^2$, then R is a possibly nonassociative $\mathbb{Z}_p$-algebra.
(b) $\mathcal{I}_p \cap [1/p, 1] = \mathcal{I}_{p,\mathrm{na}} \cap [1/p, 1] = \mathfrak{A}_p$.
(c) other than the exceptional values $N_J(2,3) = N_{J,\mathrm{na}}(2,3) = 2$, we have $N_J(n,p) = N_{J,\mathrm{na}}(n,p) = 1$, $n \in \mathbb{N} \cup \{0\}$.

The crucial reason for considering nonassociative rings in Theorem 1.1 is that our method of proof makes use of nonassociative rings even if we wish to prove the result only for (associative) rings, and so there is no extra work involved in extending the result to possibly nonassociative rings. Additionally, the fact that we get no additional $\Pr_{\mathrm{I}}(R)$ values when R is allowed to be nonassociative seems noteworthy.

Once we understand the large values that arise for all odd primes p, it is easy to deduce what large values occur for all rings of odd order, leading to the following result. Below, the parenthetical use of "possibly nonassociative" means that the result is true whether this word is included in all cases, or omitted in all cases.

Theorem 1.2. $\mathcal{I}_{\mathrm{odd}} \cap [1/3, 1] = \mathcal{I}_{\mathrm{odd,na}} \cap [1/3, 1] = \mathfrak{A}_3 \cup \{2/5\}$. *Moreover if R is a finite (possibly nonassociative) ring with $\Pr_{\mathrm{I}}(R) \geq 1/3$, then either*

(a) $R \cong \mathbb{Z}_5$ and $\Pr_{\mathrm{I}}(R) = 2/5$, or
(b) R is a (possibly nonassociative) $\mathbb{Z}_3$-algebra and $\Pr_{\mathrm{I}}(R) \in \mathfrak{A}_3$.

We also classify the p-rings with $\Pr_{\mathrm{I}}(R) > 1/p$ up to isomorphism. The following theorem indicates how many types occur for each possible value of $\Pr_{\mathrm{I}}(R) \in (1/p, 1)$; the omission of the case $\Pr_{\mathrm{I}}(R) = 1$ in this result is harmless, since for odd p that value occurs only when $|R| = 1$; we will give details of the precise types that arise later.

Theorem 1.3. *Suppose p is an odd prime, $n \geq 0$, and R is a p-ring with $\Pr_{\mathrm{I}}(R) = a(n,p)$. Then*

(a) R is a $\mathbb{Z}_p$-algebra of order p^n, and
(b) other than the exceptional value $N(2,3) = 3$, we have $N(n,p) = n$.

After some preliminaries in Section 2, we characterize the Jordan isomorphism types of nonassociative rings R satisfying $\Pr_{\mathrm{I}}(R) > 1/p$ in Section 3, thus yielding proofs of Theorems 1.1 and 1.2. Finally in Section 4, we assume associativity and characterize all isomorphism types of rings for which $\Pr_{\mathrm{I}}(R) > 1/p$, yielding a proof in particular of Theorem 1.3.

2. Preliminaries

We first list the basic terminology and notation used in this paper, other than what was already given in the introduction. Throughout the rest of the paper, p is an odd prime; we will state this fact explicitly in all formal results, but leave it implicit elsewhere.

A *ring* is required to be associative, but is not necessarily unital. A *p-ring* is a ring of order p^n for some $n \geq 0$. A $\mathbb{Z}_p$-algebra means a ring R in which $pR = \{0\}$. Each of these concepts will be prefixed with the phrase *possibly*

nonassociative whenever associativity is dropped as an assumption. To avoid awkward terminology, we will not however include this phrase when describing objects derived from a given possibly nonassociative ring or algebra: thus subrings, opposite rings, etc., are not in general assumed to be associative.

By a *basis* of a possibly nonassociative ring R, we mean a basis of $(R, +)$, which always exists by the fundamental theorem of finite abelian groups.

$\mathbb{Z}_n$ is the ring of integers mod n, $\mathbb{Z}_n^*$ is the group of units in $\mathbb{Z}_n$, and $\mathbb{Z}_n^m$ is the direct sum of m copies of $\mathbb{Z}_n$. O_p is the ring of order p in which all products are zero.

Given a possibly nonassociative ring R, we define two other possibly nonassociative rings R^{op} and R^{sym} that both have the same additive structure as R but have a different multiplication whenever R is noncommutative. In the definitions that follow, the new multiplication is denoted by $\circ$ and the original multiplication is denoted by juxtaposition.

- In the *opposite ring* R^{op}, $x \circ y = yx$.
- The *symmetrized ring* R^{sym} is defined only if we can divide by 2 in R (for instance if $nR = 0$ for some odd n). Then $x \circ y = (xy + yx)/2$.

A *Jordan subring of* R is an additive subgroup S of R such that $xy + yx \in S$ whenever $x, y \in S$. If R is associative, then R^{sym} is usually called a *special Jordan ring*, but there appears to be no existing name for the construction in the nonassociative case (which merely yields a commutative nonassociative ring).

An *idempotent* of a ring R is an element x satisfying $x^2 = x$.

We now record two simple lemmas whose proofs we omit.

Lemma 2.1. *Suppose $x := x_1 \oplus x_2 \in R_1 \oplus R_2$, where R_1, R_1 are possibly nonassociative rings. Then x is idempotent if and only if x_1, x_2 are idempotent. Thus if R_1, R_2 are finite, then $\Pr_{\text{I}}(R_1 \oplus R_2) = \Pr_{\text{I}}(R_1) \Pr_{\text{I}}(R_2)$.*

Lemma 2.2. *If x, y are both idempotent elements in a possibly nonassociative ring, then $x + y$ is idempotent if and only if $xy + yx = 0$.*

Suppose R, S are possibly nonassociative rings and $f : R \to S$ is an additive group isomorphism. We call f a *Jordan isomorphism* if it satisfies the identity $f(xy + yx) = f(x)f(y) + f(y)f(x)$ on R, or a *square isomorphism* if it satisfies the identity $f(x^2) = (f(x))^2$; we call these identities the *Jordan* and *square* identities, respectively. Jordan isomorphisms have been studied extensively, beginning with the papers [1], [2], [7], [5], [6], [4]. Note that a Jordan isomorphism between possibly nonassociative rings R, S is merely an isomorphism between R^{sym} and S^{sym}.

We have no specific reference for square isomorphisms, but they are closely related to Jordan isomorphisms. It is clear that every square isomorphism is a Jordan isomorphism (consider $f(x^2)$ with $x = u + v$). In the converse direction, a Jordan isomorphism clearly satisfies $2f(x^2) = 2(f(x))^2$, so Jordan and square isomorphisms are equivalent concepts for possibly nonassociative rings of odd order, the only algebraic systems of concern in this paper.

Although for us they are equivalent, the bilinear nature of Jordan isomorphisms is useful, yielding in particular the following useful observation.

Observation 2.3. If $f : R \to S$ is an additive group isomorphism between possibly nonassociative rings whose additive groups are finitely generated, and if $\mathcal{B}$ is a basis of R, then f is a Jordan isomorphism if and only if the Jordan identity holds for all $x, y \in \mathcal{B}$.

The point of considering square isomorphisms $f : R \to S$ between possibly nonassociative rings is that it follows immediately from the definition that $f(x)$ is idempotent if and only if $x \in R$ is idempotent. This allows us to make the following observation.

Observation 2.4. If $f : R \to S$ is a Jordan isomorphism of odd order possibly nonassociative rings, then $f(x)$ is a nonzero idempotent if and only if x is a nonzero idempotent. Consequently, idempotent proportion is a Jordan isomorphism invariant when restricted to the class of possibly nonassociative rings of odd order.

Note that the above observation fails in rings of even order: for instance, all commutative $\mathbb{Z}_2$-algebras R of dimension n are Jordan isomorphic, but these include at one extreme the Boolean algebra $R = \mathbb{Z}_2^n$ (with $\Pr_{\mathrm{I}}(R) = 1$) and at the other extreme the algebra R in which all products are zero (with $\Pr_{\mathrm{I}}(R) = 2^{-n}$).

Suppose $n \in \mathbb{N} \cup \{0\}$. Throughout the rest of the paper, $A_{n,p}$ will denote the n-dimensional $\mathbb{Z}_p$-algebra with idempotent basis $\{u_1, \ldots, u_n\}$ in which multiplication of basis elements is defined by $u_i u_j = u_i$; multiplication is extended to all of $A_{n,p}$ by distributivity. This multiplication clearly gives the basis a semigroup structure, and so the associated $\mathbb{Z}_p$-vector space becomes an algebra.

We now compute the idempotent proportion of $A_{n,p}$.

Lemma 2.5. *Given a prime p and $n \in \mathbb{N}$, let $A_{n,p}$ be defined with basis $\{u_1, \ldots, u_n\}$, as above. Let $x := \sum_{i=1}^n x_i u_i \in A_{n,p}$, where the coefficients x_i all lie in $\mathbb{Z}_p$. Writing $s := \sum_{i=1}^n x_i \in \mathbb{Z}_p$, the following are equivalent:*

(a) $s = 1$.
(b) x is a right unity.
(c) x is a nonzero idempotent.
(d) $xy + yx = x + y$ whenever y is a nonzero idempotent.

Consequently, $\Pr_{\mathrm{I}}(A_{n,p}) = a(n,p)$. This last equation holds also for $n = 0$.

Proof. Defining $y := \sum_{i=1}^n y_i u_i$, where $y_i \in \mathbb{Z}_p$ for all i, a simple calculation shows that $yx = sy$. With this in hand, the equivalence of (a)–(c) follows easily. In view of (b), part (d) is equivalent to the condition $yx = y$ whenever y is a nonzero idempotent. Since in general $yx = sy$, and since nonzero idempotents exist, this is again equivalent to $s = 1$.

The set of all x with $s = 1$ can be identified with a coset of the surjective group homomorphism $\phi : \mathbb{Z}_p^n \to \mathbb{Z}_p$ given by $\phi(x_1, \ldots, x_n) = \sum_{i=1}^n x_i$, so there are p^{n-1} such elements and $\Pr_{\mathrm{I}}(A_{n,p}) = a(n,p)$.

The case $n = 0$ is of course trivial. □

Since all nonzero idempotents in $A_{n,p}$ are right unities, it follows that the linear map induced by a bijection between any two idempotent bases of $A_{n,p}$ is an automorphism.

$A_{n,p}$ and $(A_{n,p})^{\mathrm{op}}$ are Jordan isomorphic, since trivially every possibly nonassociative ring R is Jordan isomorphic to R^{op} via the identity map. However for $n > 1$, $A_{n,p}$ and $(A_{n,p})^{\mathrm{op}}$ are non-isomorphic because the former has p^{n-1} right unities and the latter has no right unities.

We will not need the following simple result, but we state it because it indicates a striking difference between odd orders and the situation for $p = 2$ in which nontrivial subgroups of idempotents exist (e.g. Boolean rings).

Proposition 2.6. *If R is a ring of odd order and S is the set of idempotents in R, then the only subgroup of $(R,+)$ contained in S is the trivial subgroup.*

Proof. Suppose G is a subgroup contained in S, and $x \in G$. Then $-x = (-x)^2 = x^2 = x$. Thus $2x = 0$, and so $x = 0$ because $|R|$ is odd. □

Despite Proposition 2.6, note that the idempotents in $A_{n,p}$ are closely connected to a subgroup, since the set of all nonzero idempotents is a coset of a subspace G with codimension 1 in $A_{n,p}$.

3. Classification up to Jordan isomorphism

Since $\Pr_{\mathrm{I}}(R)$ is a Jordan isomorphism invariant, it is natural to attempt to characterize possibly nonassociative rings R with a given value of $\Pr_{\mathrm{I}}(R)$ up to Jordan isomorphism. The following set of three results exhibit all values of $\Pr_{\mathrm{I}}(R) \geq 1/p$ among possibly nonassociative p-rings R, and also characterize the Jordan isomorphism types that give rise to values of $\Pr_{\mathrm{I}}(R)$ strictly exceeding $1/p$.

Lemma 3.1. *Suppose R is a ring of order p^n for some prime p and $n \geq 0$, and $(R,+)$ is cyclic with generator u. Then R has either one or two idempotents, depending on whether or not $u^2 \in pR$. Moreover if $\Pr_{\mathrm{I}}(R) \geq 1/p$, then*

$$\Pr_{\mathrm{I}}(R) \in \{a(0,p),\ a(1,p),\ a(\infty,p)\} = \{1,\ 2/p,\ 1/p\}\,,$$

and each of these possibilities is associated with a single isomorphism class of rings of order at most p, namely the ring of order 1, $\mathbb{Z}_p$, and O_p.

Theorem 3.2. *Let p be an odd prime, and let R be a possibly nonassociative p-ring such that $\Pr_{\mathrm{I}}(R) > 2/p^2$. Then R is a possibly nonassociative $\mathbb{Z}_p$-algebra.*

The cutoff for $\Pr_{\mathrm{I}}(R)$ in the above theorem cannot be improved, as evidenced by $\Pr_{\mathrm{I}}(\mathbb{Z}_{p^2}) = 2/p^2$.

Theorem 3.3. *Suppose p is an odd prime, $n \geq 0$, and R is a possibly nonassociative ring of order p^n such that $\Pr_{\mathrm{I}}(R) > 1/p$. Then*

(a) If $(n,p) = (2,3)$, then R is Jordan isomorphic to either $A_{2,3}$ or $\mathbb{Z}_3^2$.
(b) If $(n,p) \neq (2,3)$, then R is Jordan isomorphic to $A_{n,p}$.
(c) $\Pr_{\mathrm{I}}(R) = a(n,p)$.

Using the above results, it is not hard to prove Theorems 1.1 and 1.2.

Proof of Theorem 1.1. The fact that $\mathcal{I}_p \cap [1/p, 1]$ contains $\mathfrak{A}_p$ follows from Lemmas 2.5 and 3.1. Conversely, the fact that $\mathcal{I}_{p,\mathrm{na}} \cap [1/p, 1]$ is contained in $\mathfrak{A}_p$ follows from Theorem 3.3. Parts (a) and (c) follow from Theorems 3.2 and 3.3. □

The following lemma follows in the same manner as for finite rings, a context in which the conclusion is well known. For completeness, we sketch the proof.

Lemma 3.4. *A finite possibly nonassociative ring R is a direct sum of possibly nonassociative p-rings.*

Proof. For each prime p dividing $|R|$, we define $R_p := m_p R$, where $m_p := |R|/p^{k_p}$ and k_p is the largest number $k \in \mathbb{N}$ such that p^k divides $|R|$. The fact that the possibly nonassociative rings R_p have trivial intersection follows from distributivity, and the fact that every $x \in R$ can be written as a sum of elements of the form $m_p x$ follows from Bézout's identity. □

Proof of Theorem 1.2. Writing R as a direct sum of nontrivial p-rings R_p, we see from Theorem 1.1 that only $p = 3$ and $p = 5$ can arise, since $2/7 < 1/3$. If $|R|$ is divisible by 5, then R must be a 5-ring because $(2/5)(2/3) < 1/3$. Also $a(2, 5) = 6/25 < 1/3$, so we must have $\Pr_{\mathrm{I}}(R) = 2/5$. The one isomorphism type of a 5-ring with $\Pr_{\mathrm{I}}(R) = 2/5$ is $R = \mathbb{Z}_5$, again by Theorem 1.1. If instead R is a 3-ring, then R is a $\mathbb{Z}_3$-algebra and $\Pr_{\mathrm{I}}(R) \in \mathfrak{A}_3$ by Theorem 1.1. □

Proof of Theorem 3.2. We suppose for the sake of contradiction that R is not a $\mathbb{Z}_p$-algebra. Let $|R| = p^n$ and denote by $N(A)$ the number of idempotents in a subset A of R. Let S_+, S_2, and S_1 be the collection of elements in R of order exceeding p^2, equal to p^2, or equal to p, respectively. Then $|S_+| = p^n - p^k$, $|S_2| = p^k - p^j$, and $|S_1| = p^j - 1$, where $j \geq 1$ and $n \geq k \geq 2$.

Suppose first that S_+ is nonempty, and so $n > k$. Let T be the collection of integers $1 \leq i < p^3$ that are coprime to p. For each $x \in S_+$, it follows readily that ix is idempotent for at most one integer $i \in T$. Consequently, $m_+ \leq |S_+|$, where m_+ is the number of pairs $(x, i) \in S_+ \times T$ such that ix is idempotent. However $y \mapsto iy$ is a bijection on S_+ for each $i \in T$, so the mapping $f(x, i) := ix$ from $S_+ \times T$ to S_+ takes on each value $|T| = p^2(p - 1)$ times. It follows that

$$N(S_+) = \frac{m_+}{|T|} \leq \frac{|S_+|}{p^2(p-1)} = \frac{p^n - p^k}{p^2(p-1)}\,.$$

In a similar fashion, we see that

$$N(S_2) \leq \frac{|S_2|}{p(p-1)} = \frac{p^k - p^j}{p(p-1)}\,.$$

The analogous estimate for S_1 is not good enough for our purposes, so we work a little harder to improve it. By the fundamental theorem of finite abelian groups, $(R, +)$ can be written as an internal direct sum $A' \oplus A_1$, where A' is a direct sum of one or more cyclic groups of order p^2 or larger, and A_1 is an elementary abelian group. Note that $|S_1| + 1$, the number of elements of order dividing p, is at least $p|A_1|$. Now $x = x' \oplus x_1 \in A' \oplus A_1$ has order dividing p if and only if x' has order dividing p, in which case distributivity implies that $(x')^2 = x'x_1 = x_1x' = 0$, and so $x^2 = x_1^2 \in A_1$. It follows that $N(S_1) \leq N(A_1 \setminus \{0\})$. Moreover if $x \in A_1$, then at most one of the elements ix, $1 \leq i < p$, can be idempotent, so

$$N(S_1) \leq \frac{|A_1| - 1}{p - 1} \leq \frac{(|S_1| + 1) - p}{p(p-1)} = \frac{p^j - p}{p(p-1)}\,.$$

Adding the estimates for the number of idempotents of different orders, and not forgetting the zero idempotent, we see that

$$N(R) \leq \frac{p^n - p^k + p^{k+1} - p^{j+1} + p^{j+1} - p^2 + p^3 - p^2}{p^2(p-1)}\,.$$

We claim that $N(R) \leq 3p^{n-3}$, or equivalently

$$D := p^2(p-1)(3p^{n-3} - N(R)) \geq 0\,.$$

Now $k < n$ and

$$D \geq D_{n,k} := 3p^n - 3p^{n-1} - p^n - p^{k+1} + p^k - p^3 + 2p^2\,.$$

Since $D_{n,k}$ is decreasing as a function of k, we have

$$D_{n,k} \geq D_{n,n-1} = p^n - 2p^{n-1} - p^3 + 2p^2\,,$$

Since $p > 2$, this last expression is increasing as a function of n, and

$$D_{n,n-1} \geq D_{3,2} = 0\,,$$

as claimed.

Consequently, $N(R) \leq 3p^{n-3} \leq p^{n-2}$ and $\Pr_{\mathrm{I}}(R) \leq p^{-2}$. This rules out all rings with elements of order exceeding p^2.

Thus we may assume that S_+ is empty, $|S_2| = p^n - p^j$, and $|S_1| = p^j - 1$, where $n \geq j + 1 \geq 2$. As before,

$$N(S_2) \leq \frac{|S_2|}{p(p-1)} = \frac{p^n - p^j}{p(p-1)}\,.$$

Now $(R, +)$ is of the form $A_2 \oplus A_1$, where A_2 is a direct sum of one or more cyclic groups of order p^2, and A_1 is an elementary abelian group. If A_1 is trivial then, arguing as before, we see that there are no nonzero idempotents outside S_2, and so

$$\Pr_{\mathrm{I}}(R) \leq E_{n,j} := p^{-n} + \frac{1 - p^{j-n}}{p(p-1)}\,.$$

Now $E_{j,n}$ is decreasing as a function of j, so

$$E_{n,j} \leq E_{n,1} = \frac{1 + p^{2-n} - 2p^{1-n}}{p(p-1)}\,.$$

It is clear from this last expression that $E_{n,1}$ is strictly decreasing as a function of n, and so $E_{n,1} \leq E_{2,1} = 2/p^2$, with equality only if $n = 2$. Thus $\Pr_{\mathrm{I}}(R) \leq 2/p^2$, with equality possible only if $j = 1$ and $n = 2$ (and equality does occur for $\mathbb{Z}_{p^2}$). In any case, we get a contradiction.

Finally, we consider the case where A_1 and A_2 are both nontrivial, and so $n \geq j + 1 \geq 3$. As before,

$$N(S_1) \leq \frac{|A_1| - 1}{p - 1} \leq \frac{p^j - p}{p(p-1)}\,,$$

and so

$$N(R) \leq \frac{p^n - p^j + p^j - p + p^2 - p}{p(p-1)} = \frac{p^n + p^2 - 2p}{p(p-1)}\,.$$

To finish the proof, we show that $N(R) < 2p^{n-2}$, or equivalently

$$F := p(p-1)(2p^{n-2} - N(R)) > 0\,.$$

Now

$$F \geq F_n := p^n - 2p^{n-1} - p^2 + 2p\,,$$

and F_n is an increasing function of n, so

$$F_n \geq F_3 = p^3 - 3p^2 + 2p = p(p-1)(p-2) > 0\,. \qquad \square$$

Remark 3.5. It follows from the proof that for any odd prime p, there is only one p-ring with $\Pr_{\mathrm{I}}(R) = 2/p^2$ that is not a $\mathbb{Z}_p$-algebra, namely $R = \mathbb{Z}_{p^2}$.

Proof of Theorem 3.3 for $n = 2$.
Because $\mathrm{Pr_I}(R) > 1/p$, there are at least four idempotents. By Lemma 3.1, these idempotents cannot all be contained in a single cyclic subgroup of $(R, +)$. It follows that R has an idempotent basis $\{u, v\}$. We write $uv + vu = \lambda u + \mu v$, $\lambda, \mu \in \mathbb{Z}_p$.

Let $x := iu + jv$, $i, j \in \mathbb{Z}_p$. Then

$$x^2 = (iu + jv)^2 = i(i + j\lambda)u + j(j + i\mu)v\,. \tag{3.1}$$

The equation $x^2 = x$ has at least three solutions, namely 0, u, and v. In any other case $i, j \neq 0$, and so

$$i + j\lambda = 1 \qquad \text{and} \qquad j + i\mu = 1\,. \tag{3.2}$$

Solving for i in the first equation of (3.2), and substituting into the second yields

$$j(1 - \lambda\mu) = 1 - \mu\,. \tag{3.3}$$

Note that (3.2) is a system of linear equations in the unknowns i, j with augmented matrix

$$\left(\begin{array}{cc|c} 1 & \lambda & 1 \\ \mu & 1 & 1 \end{array}\right)$$

By Lemma 2.5 and Observation 2.3, if $(\lambda, \mu) = (1, 1)$ then R is Jordan isomorphic to $A_{2,p}$, so we may suppose that $(\lambda, \mu) \neq (1, 1)$. But then the augmented matrix has rank 2, and so there is at most one pair (i, j) satisfying (3.2). Thus there are at most four idempotents in total, which is inconsistent with $\mathrm{Pr_I}(R) > 1/p$ when $p > 3$.

Suppose therefore that $p = 3$. The condition $\mathrm{Pr_I}(R) > 1/3$ means that the fourth idempotent must exist. If $\mu = 1$, then since $j \neq 0$, (3.3) would force $\lambda = 1$, a case that we already considered.

Suppose instead that $\mu = -1$. Then $j(1 + \lambda) = 2$ and $i = 1 - j\lambda$. Now $\lambda = 1$ would force $i = 0$ which we do not allow, while $\lambda = -1$ is inconsistent with the equation $j(1 + \lambda) = 2$, so we eliminate both possibilities. The remaining possibility is that $\lambda = 0$ and so $uv + vu = -v$, and the last idempotent is $u - v$. Taking $x = v$ and $y = u - v$, we see that $xy + yx = 0$, and so R is Jordan isomorphic to $\mathbb{Z}_3^2$.

Lastly suppose $\mu = 0$. Now (3.3) implies that $j = 1$ and (3.2) gives $i = 1 - \lambda$. We get the desired final idempotent if either $\lambda = 0$ or $\lambda = -1$. If $\lambda = 0$, then $uv + vu = 0$ and R is Jordan isomorphic to $\mathbb{Z}_3^2$. The final case $(\mu, \lambda) = (0, -1)$ is by symmetry equivalent to the previously considered case $(\mu, \lambda) = (-1, 0)$, so again R is Jordan isomorphic to $\mathbb{Z}_3^2$.

We have proven parts (a) and (b). As for (c), since idempotent proportion is a Jordan isomorphism invariant for rings of odd order, this follows from the equations $\mathrm{Pr_I}(A_{2,p}) = a(2, p)$ and $\mathrm{Pr_I}(\mathbb{Z}_3) = a(1, 3)$ proven in Lemmas 2.5 and 3.1, together with Lemma 2.1. □

Remark 3.6. Let us record a noteworthy consequence of the above proof: if R is a possibly nonassociative ring of order p^2 with more than four idempotents, then it is Jordan isomorphic to $A_{2,p}$ and has $p + 1$ idempotents (with $p > 3$).

We now prove the remaining parts of Theorem 3.3.

Proof of Theorem 3.3 (b), (c), for $n \neq 2$.
Since $\mathrm{Pr_I}(A_{n,p}) = a(n,p)$ and idempotent proportion is a Jordan isomorphism invariant for rings of odd order, it suffices to prove (b).

The cases $n \in \{0,1\}$ follow from Lemma 3.1, since $A_{0,p}$ is isomorphic to the trivial ring, and $A_{1,p}$ is isomorphic to $\mathbb{Z}_p$. We therefore suppose that R is a n-dimensional possibly nonassociative $\mathbb{Z}_p$-algebra for some $n \geq 3$, and $\mathrm{Pr_I}(R) > 1/p$. We may also suppose that R has a nonzero idempotent e, and we let $E = \mathrm{span}\{e\}$ be the associated subring.

Let x be an element of $R \setminus E$, and let $U_x := \mathrm{span}\{x, e\}$. Let V_x be a complementary subspace in R to U_x, and let $\pi_x : R \to U_x$ be projection on the U_x-subspace, so that $u - \pi_x(u) \in V_x$ for all $u \in R$. Now define a multiplication $*$ on U_x by the equation $u * v = \pi_x(uv)$ for all $u, v \in R$. We call u a *$*$-idempotent* if $u * u = u$, and reserve the unqualified term *idempotent* for the original multiplication of R. Then $(U_x, +, *)$ is a two-dimensional possibly nonassociative $\mathbb{Z}_p$-algebra (note that it may be nonassociative even if R itself is associative), and so it has at most $p+1$ $*$-idempotents by the previously proved case $n = 2$. Consequently $W_x := U_x \setminus E$ has at most $p-1$ $*$-idempotents, and hence at most $p-1$ idempotents, since the equation $u^2 = u$ implies $u * u = u$.

The subsets W_x partition $R \setminus E$ into subsets of size $p^2 - p$, and the proportion of idempotents in each is at most $(p-1)/(p^2-p) = 1/p$. Thus the same is true of $R \setminus E$ as a whole, and so there are at most $p^{n-1} - 1$ idempotents in $R \setminus E$. Since exactly two elements of E are idempotent, it follows that the number of idempotents in R is at most $p^{n-1} + 1$, and so

$$\mathrm{Pr_I}(R) \leq \frac{p^{n-1}+1}{p^n} = a(n,p)\,. \tag{3.4}$$

Equality in (3.4) means having $p^{n-1}+1$ idempotents in R. Thus in the absence of equality, we have $\mathrm{Pr_I}(R) \leq 1/p$, contradicting our hypothesis. Thus $a(n,p)$ is the only value of $\mathrm{Pr_I}(R)$ consistent with the condition $\mathrm{Pr_I}(R) > 1/p$ for an n-dimensional possibly nonassociative $\mathbb{Z}_p$-algebra.

It remains to prove that R is Jordan isomorphic to $A_{n,p}$. In the above argument, the condition $\mathrm{Pr_I}(R) > 1/p$ requires the equality $\mathrm{Pr_I}(R) = a(n,p)$, which in turn requires that there are exactly $p+1$ idempotents in every ring set U_x above, and so every $*$-idempotent in U_x must be an idempotent. Moreover, there must exist an idempotent $u \in U_x \setminus E$, and so $\{e, u\}$ is a basis for U_x, and we must have $ue + eu \in U_x$ (since otherwise $0, e, u$ are the only idempotents in U_x). It follows by distributivity that U_x is a Jordan subring of R. Note also that the Jordan structures defined on U_x by $\cdot$ and by $*$ are the same, i.e. $vw + wv = v * w + w * v$ for all $u, v \in U_x$: this follows by linearity of π_x and the fact that $\pi_x|_{U_x}$ is the identity map. It is convenient to denote this Jordan product on R by $\circ$, i.e. $v \circ w = vw + wv$ for all $v, w \in R$; note that v is an idempotent if and only if $v \circ v = 2v$.

We call the argument in the preceding paragraph a *projection argument*: the input to this argument is (e, x), where e is a nonzero idempotent and $x \notin E := \mathrm{span}\{e\}$. The output is a nonzero idempotent $u \in U_x := \mathrm{span}\{e, x\}$ such that $\mathrm{span}\{e, u\} = U_x$. Additionally, U_x is a Jordan subring; this is a very strong restriction that will enable us to rule out most of the remaining possibilities, so we record it as a formal fact.

Fact 3.7. *Every two-dimensional subspace of R containing a nonzero idempotent is a Jordan subring of R.*

If we start off with a basis $\{x_1, \ldots, x_n\}$ of R where $e_1 := x_1$ is an idempotent, and we apply projection arguments with input (e_1, x_j) for each $2 \le j \le n$, then we get outputs e_j such that $\mathcal{B} = \{e_1, \ldots, e_n\}$ is an idempotent basis of R. Also by Fact 3.7, $R_{ij} := \operatorname{span}\{e_i, e_j\}$ is a Jordan subalgebra for each pair of distinct indices $1 \le i, j \le n$.

Suppose first that $p > 3$. By the case $n = 2$ and Observation 2.3, each R_{ij} is Jordan isomorphic to $A_{2,p}$. It follows from Lemma 2.5 that any bijection from an idempotent basis of $A_{n,p}$ to $\mathcal{B}$ satisfies the Jordan identity on this basis, and so R is Jordan isomorphic to $A_{n,p}$ by Observation 2.3.

Suppose instead that $p = 3$. In this case, we have to rule out the possibility that some of the Jordan subalgebras R_{ij} are Jordan isomorphic to $\mathbb{Z}_3^2$. If, for a set of three distinct indices i, j, k, R_{ij} is Jordan isomorphic to $\mathbb{Z}_3^2$, and R_{jk} is Jordan isomorphic to $A_{2,3}$, then there exist idempotent bases $\{u_i, u_j\}$ of R_{ij}, and $\{u_j, u_k\}$ of R_{jk} satisfying the equations $u_i \circ u_j = mu_i$ and $u_j \circ u_k = u_j + u_k$, where m is either 2 or 0, depending on whether or not u_j maps to the identity element under the Jordan isomorphism $R_{ij} \to \mathbb{Z}_3^2$. Thus

$$u_j \circ (u_i + u_k) = mu_i + u_j + u_k \,.$$

Whether $m = 0$ or $m = 2$, the element $mu_i + u_j + u_k$ is not in the two-dimensional subspace spanned by u_j and $u_i + u_k$, so this subspace is not a Jordan subring of R even though it contains a nonzero idempotent u_j. This contradicts Fact 3.7. It follows that either every R_{ij} is Jordan isomorphic to $A_{2,3}$, or every one is Jordan isomorphic to $\mathbb{Z}_3^2$. If all are Jordan isomorphic to $A_{2,3}$, then R is Jordan isomorphic to $A_{n,p}$, again by Observation 2.3.

Suppose instead that every R_{ij} is Jordan isomorphic to $\mathbb{Z}_3^2$. This implies that $e_i \circ e_j \in \{0, 2e_i, 2e_j\}$ for each i, j. Let us take three distinct indices i, j, k and rule out all possible options for the values of the resulting Jordan products.

Suppose first that $e_i \circ e_j = 2e_j$ and that $e_i \circ e_k \ne 2e_k$. Thus $e_i \circ e_k = me_i$, where $m \in \{0, 2\}$. Then e_i and $e_j + e_k$ both lie in $S := \operatorname{span}\{e_i, e_j + e_k\}$, but $e_j \circ (e_i + e_k) = 2e_j + me_i \notin S$, contradicting Fact 3.7. It follows that either $e_i \circ e_j = 0$ for all pairs of distinct integers $1 \le i, j \le n$, or that there is a distinguished idempotent, which we can take to be e_1 without loss of generality, such that $e_1 \circ e_j = 2e_j$ for all $2 \le j \le n$ and $e_i \circ e_j = 0$ for all $2 \le i \le n$. We claim that this second case reduces to the first if we replace e_1 by $e_1' := e_1 - \sum_{i=2}^n e_i$.

Assume that we are in the second case. First, we use distributivity of $\circ$ to expand $e_1' \circ e_1'$, discarding all zero terms:

$$\begin{aligned} e_1' \circ e_1' &= e_1 \circ e_1 - 2\sum_{i=2}^n e_1 \circ e_i + \sum_{i=2}^n e_i \circ e_i \\ &= 2e_1 - 2\sum_{i=2}^n 2e_i + \sum_{i=2}^n 2e_i = 2e_1' \,, \end{aligned}$$

and so e_1' is an idempotent. Also, for all $2 \le j \le n$,

$$e_1' \circ e_j = e_1 \circ e_j - \sum_{i=2}^n e_i \circ e_j = 0 \,.$$

It is now clear that $\{e_1'\} \cup \{e_j \mid 2 \leq j \leq n\}$ is an idempotent basis of R such that the Jordan product of any two distinct elements is 0. This gives the claimed reduction.

It remains to derive a contradiction under the assumption that $e_i \circ e_j = 0$ for all distinct indices i, j. Replace e_1 by $e'' := e_1 + e_2$. By distributivity, as before, we see that e'' is idempotent, so $\mathcal{B}'' := \{e''\} \cup \{e_j \mid 2 \leq j \leq n\}$ is an idempotent basis of R. Also $e'' \circ e_2 = 2e_2$, but $e'' \circ e_j = 0$ for all $j > 2$. Earlier, we saw that such a configuration contradicts Fact 3.7, so we are done. □

Remark 3.8. Although Fact 3.7 tells us that many two-dimensional subspaces of R are closed under the symmetrized operation, these are not necessarily closed under the original multiplication of R. For instance, whenever $l, r \in \mathbb{N}$, the algebras $B_{l,r,p}$ of Definition 4.1 below have two-dimensional subspaces with basis given by a pair of idempotents that nevertheless fail to be closed under multiplication.

4. Classification up to isomorphism

The characterization of possibly nonassociative p-rings R satisfying $\Pr_{\mathrm{I}}(R) > 1/p$ up to Jordan isomorphism given in the previous section can readily be used to give a characterization up to isomorphism. For instance the main case where R is Jordan isomorphic to $A_{n,p}$ corresponds to R being an n-dimensional $\mathbb{Z}_p$-algebra with idempotent basis $\{u_1, \ldots, u_n\}$ where $u_i u_j$ is defined as follows for distinct indices i, j:

(a) $u_i u_j = v_{ij}$ if $i < j$; here $v_{ij} \in R$ is arbitrary.
(b) $u_i u_j = u_i + u_j - v_{ij}$ if $i > j$.

Multiplication is then extended to all of R by distributivity.

Of course in most cases R as defined above is nonassociative. So there remains the problem of classifying p-rings R such that $\Pr_{\mathrm{I}}(R) > 1/p$. We carry out such a classification in this final section.

Definition 4.1. Suppose p is a prime, l, r are non-negative integers, and $n := l + r + 1$. Let V be the n-dimensional vector space over $\mathbb{Z}_p$ with basis $\mathcal{B} := \{u_i \mid -l \leq i \leq r\}$. Define a bilinear map $\psi_{\mathcal{B}} : V \times V \to V$ by the equations

$$\psi_{\mathcal{B}}(u_i, u_j) = \begin{cases} u_i, & 0 \leq i, j \leq r, \\ u_j, & -l \leq i, j \leq 0, \\ u_0, & -l \leq i < 0 \leq j \leq r, \\ u_i + u_j - u_0, & -l \leq j < 0 \leq i \leq r. \end{cases} \tag{4.1}$$

Denote by $B_{l,r,p}$ the vector space V equipped with multiplication $xy := \psi_{\mathcal{B}}(x, y)$, and define $R_-(\mathcal{B}) := \operatorname{span}\{u_i \mid -l \leq i < 0\}$, $R_+(\mathcal{B}) := \operatorname{span}\{u_i \mid 0 < i \leq r\}$, and $R_0(\mathcal{B}) := \operatorname{span}\{u_0\}$. The above multiplication depends on the basis, so we refer to *$\mathcal{B}$-multiplication* whenever we need to indicate the basis.

There is some overlap between the cases in the above definition, so we need to verify that these overlapping cases are consistent. Specifically the cases $i, j \geq 0$ and $i, j \leq 0$ overlap when $i = j = 0$, and $i, j \leq 0$ overlaps with the final two cases if $i < 0 = j$ or if $j < 0 = i$. In the first two cases, both parts of the definition say that $u_i u_j = u_0$, while in the last case, both parts say that $u_i u_j = u_j$. Thus the definition is consistent, and bilinearity of $\psi_{\mathcal{B}}$ implies that $B_{l,r,p}$ is a possibly

nonassociative $\mathbb{Z}_p$-algebra. Note also that $B_{0,n-1,p}$ is isomorphic to $A_{n,p}$, and $B_{n-1,0,p}$ is isomorphic to $(A_{n,p})^{\mathrm{op}}$.

The following theorem establishes some important properties of $B_{l,r,p}$.

Theorem 4.2. *Suppose p is an odd prime, l, r are non-negative integers, and $n = l + r + 1$. Let $B_{l,r,p}$, $\mathcal{B}$, $R_- := R_-(\mathcal{B})$, $R_+ := R_+(\mathcal{B})$, and $R_0 := R_0(\mathcal{B})$ be as in Definition 4.1.*

(a) $\mathcal{B}$ is an idempotent basis of $B_{l,r,p}$.
(b) R_+, R_-, and R_0 are subrings isomorphic to $A_{r,p}$, $(A_{l,p})^{\mathrm{op}}$, and $A_{1,p}$, respectively.
(c) $B_{l,r,p}$ is Jordan isomorphic to $A_{n,p}$.
(d) $\mathrm{Pr}_{\mathrm{I}}(B_{l,r,p}) = a(n,p)$.
(e) $B_{l,r,p}$ is a $\mathbb{Z}_p$-algebra.
(f) If $\mathcal{B}' := \{u'_i \mid -l \le i \le r\}$ is another idempotent basis of $B_{l,r,p}$, such that $R_-(\mathcal{B}) = R_-(\mathcal{B}')$, $R_+(\mathcal{B}) = R_+(\mathcal{B}')$, and $R_0(\mathcal{B}) = R_0(\mathcal{B}')$, then $\mathcal{B}'$-multiplication coincides with $\mathcal{B}$-multiplication.
(g) $B_{l,r,p}$ is isomorphic to $B_{l',r',p'}$ if and only if $l = l'$, $r = r'$, and $p = p'$.
(h) $B_{l,r,p}$ has a right unity if and only if $l = 0$, and a left unity if and only if $r = 0$.

By the above theorem, there are n distinct isomorphism classes of $B_{l,r,p}$ with $l + r + 1 = n$ for any given n and p, and in each case $\mathrm{Pr}_{\mathrm{I}}(B_{l,r,p}) = a(n,p) > 1/p$.

Definition 4.3. We call a ring R a *special ring* if $\mathrm{Pr}_{\mathrm{I}}(R) > 1/p$ and R is not isomorphic to any of the rings $B_{l,r,p}$.

Bearing in mind Theorem 4.2(d), the following result gives the desired classification of p-rings satisfying $\mathrm{Pr}_{\mathrm{I}}(R) > 1/p$ up to isomorphism.

Theorem 4.4. *Suppose p is an odd prime, $n \in \mathbb{N}$, and R is a p-ring of order p^n with $\mathrm{Pr}_{\mathrm{I}}(R) > 2/p^2$.*

(a) R is a $\mathbb{Z}_p$-algebra.
(b) If in fact $\mathrm{Pr}_{\mathrm{I}}(R) > 1/p$, then $\mathrm{Pr}_{\mathrm{I}}(R) = a(n,p)$.
(c) The only special ring is $\mathbb{Z}_3^2$.

The main new part of Theorem 4.4 is implied by the following result.

Theorem 4.5. *Suppose p is an odd prime and $n \in \mathbb{N}$.*

(a) A ring R is Jordan isomorphic to $\mathbb{Z}_p^n$ if and only if it is isomorphic to $\mathbb{Z}_p^n$.
(b) A ring R is Jordan isomorphic to $A_{n,p}$ if and only if it is isomorphic to $B_{l,r,p}$ for some $l, r \ge 0$ such that $l + r + 1 = n$.

We pause to give a couple of lemmas. The first is very simple but will be used repeatedly, mostly without explicit reference. The second shows that most of Lemma 2.5 extends to algebras that are merely Jordan isomorphic to $A_{n,p}$.

Lemma 4.6. *Suppose R is a $\mathbb{Z}_p$-algebra for some prime p, and suppose a particular pair of idempotents $u, v \in R$ satisfy $uv + vu = u + v$. Then $uvu = u$, and uv is idempotent.*

Proof. Multiplying $uv + vu$ on the left by u, we get $uv + uvu = u + uv$, so $uvu = u$. Now multiplying on the right by v, we see that uv is idempotent. □

Lemma 4.7. *Suppose R is a possibly nonassociative $\mathbb{Z}_p$-algebra for some odd prime p, and $\phi : A_{n,p} \to R$ is a Jordan isomorphism for some $n \in \mathbb{N}$. Then:*

(a) R has an idempotent basis.
(b) $\mathrm{Pr}_{\mathrm{I}}(R) = a(n,p)$.
(c) If $\{v_1, \ldots, v_n\}$ is any idempotent basis of R, $x := \sum_{i=1}^n x_i v_i \in R$, and $s := \sum_{i=1}^n x_i \in \mathbb{Z}_p$, with $x_i \in \mathbb{Z}_p$ for $1 \leq i \leq n$, then the following are equivalent:
  (i) $s = 1$;
  (ii) x is a nonzero idempotent;
  (iii) $xy + yx = x + y$ whenever y is a nonzero idempotent.
(d) Every set S of independent idempotents in R is a subset of an idempotent basis.

Proof. By definition, $A_{n,p}$ has an idempotent basis, and it is clear by Observation 2.4 that ϕ sends an idempotent basis to an idempotent basis. This gives (a). Part (b) follows from Lemma 2.5 and the fact that idempotent proportion is a Jordan isomorphism invariant on the class of odd order rings.

We now prove (c). Let $v_i = \phi(u_i)$ for $1 \leq i \leq n$, so that $\{u_1, \ldots, u_n\}$ is an idempotent basis of $A_{n,p}$. The equivalence of (i) and (ii) follow immediately from Lemma 2.5 and Observation 2.4. In a similar fashion, the equivalence of (ii) and (iii) follows from Observation 2.4 and the equivalence of parts (c) and (d) of Lemma 2.5.

Finally, (d) is a straightforward consequence of (a): given an idempotent basis $\mathcal{B} := \{v_1, \ldots, v_n\}$ and an independent set of idempotents S containing $k \leq n$ elements, we define a chain of independent sets $S_0 \subset S_1 \subset \cdots$, where $S_0 := S$ and S_{i+1} is obtained from S_i by adding an element of $\mathcal{B}$ to S_i. This process can be continued until we obtain an idempotent basis S_{n-k} containing S. □

Proof of Theorem 4.2. Part (a) follows immediately from Definition 4.1, and part (b) is obvious. For (c), it suffices to check that $u_i u_j + u_j u_i = u_i + u_j$ for all indices i, j, and this is routine. Part (d) now follows from Lemma 4.7(b). Let us also write $A_+ := R_+ + R_0$, $A_- := R_- + R_0$, and note that A_+ and A_- are subalgebras isomorphic to $A_{r+1,p}$ and $(A_{l+1,p})^{\mathrm{op}}$, respectively.

For (e), we need to verify associativity, and for this it suffices to check that $u_i(u_j u_k) = (u_i u_j)u_k$ in all cases. If i, j, k are all non-negative or all nonpositive, then these basis elements either lie in A_+ or A_-, subrings that are isomorphic to $A_{r+1,p}$ or $(A_{l+1,p})^{\mathrm{op}}$, respectively, and associativity follows immediately. There are six other cases to be checked: three with two non-negative indices and one negative index, and three with two negative indices and one non-negative index. By the left-right symmetry of the definition the last three cases reduce either to the previous three cases or to the case of all non-negative indices. Thus there remain only three cases to be checked.

If $i < 0$ and $j, k \geq 0$, then

$$u_i(u_j u_k) = u_i u_j = u_0 = u_0 u_k = (u_i u_j)u_k \,.$$

If $j < 0$ and $i, k \geq 0$, then

$$u_i(u_j u_k) = u_i u_0 = u_i = u_i + u_0 - u_0 = (u_i + u_j - u_0)u_k = (u_i u_j)u_k \,.$$

Finally, if $k < 0$ and $i, j \geq 0$, then

$$u_i(u_j u_k) = u_i(u_j + u_k - u_0) = u_i + (u_i + u_k - u_0) - u_i \\ = u_i + u_k - u_0 = u_i u_k = (u_i u_j) u_k \,.$$

We now prove (f). Let us write $\psi := \psi_{\mathcal{B}}$ and $\psi' := \psi_{\mathcal{B}'}$, using the notation of Definition 4.1. We assume that $R_+(\mathcal{B}') = R_+$, $R_-(\mathcal{B}') = R_-$, and $R_0(\mathcal{B}') = R_0$. (The last equation just means that $u'_0 = u_0$.) Let $u'_i = \sum_{\alpha=-l}^{r} c_{i\alpha} u_\alpha$, where $c_{i\alpha} \in \mathbb{Z}_p$. Then $c_{i\alpha} = 0$ for all $\alpha \leq 0$ if $i > 0$, and $c_{i\alpha} = 0$ for all $\alpha \geq 0$ if $i < 0$. It follows from Lemma 2.5 that $\sum_{\alpha=-l}^{r} c_{i\alpha} = 1$ regardless of the sign of i, and that u'_i is a left unity in A_- when $i \leq 0$ and a right unity in A_+ when $i \geq 0$. This already gives $\psi(u'_i, u'_j) = u'_i = \psi'(u'_i, u'_j)$ when $i, j \geq 0$, and $\psi(u'_i, u'_j) = u'_j = \psi'(u'_i, u'_j)$ when $i, j \leq 0$. If $i < 0 \leq j$, then

$$\psi(u'_i, u'_j) = \sum_{\alpha=-l}^{-1} \sum_{\beta=0}^{r} c_{i\alpha} d_{j\beta} u_\alpha u_\beta = \sum_{\alpha=-l}^{-1} \sum_{\beta=0}^{r} c_{i\alpha} d_{j\beta} u_0 = u_0 = \psi'(u'_i, u'_j) \,,$$

because $\sum_{\alpha=-l}^{-1} c_{i\alpha} = \sum_{\beta=0}^{r} d_{i\alpha} = 1$. Similarly if $j < 0 \leq i$, then

$$\begin{aligned} \psi(u'_i, u'_j) &= \sum_{\alpha=0}^{r} \sum_{\beta=-l}^{-1} c_{i\alpha} d_{j\beta} u_\alpha u_\beta \\ &= \sum_{\alpha=0}^{r} \sum_{\beta=-l}^{-1} c_{i\alpha} d_{j\beta} (u_\alpha + u_\beta - u_0) \\ &= \left(\sum_{\alpha=0}^{r} c_{i\alpha} u_\alpha \right) + \left(\sum_{\beta=-l}^{-1} d_{j\beta} u_\beta \right) - u_0 \\ &= u'_i + u'_j - u'_0 = \psi'(u'_i, u'_j) \,. \end{aligned}$$

We next prove (g). We identify isomorphism invariants of $B_{l,r,p}$ that allow us to distinguish between any two such algebras. The parameter p itself is one obvious invariant, so it suffices to find invariants from which we can determine l and r. (Actually it would suffice to be able to determine one of l and r, since $n = l + r + 1$ is the dimension, but it is just as easy to determine both simultaneously.)

We write $R := B_{l,r,p}$ for given l, r, and define the vector space projection $P_+ : R \to R_+$:

$$P_+ \left(\sum_{i=-l}^{r} c_i u_i \right) = \sum_{i=1}^{r} c_i u_i \,.$$

For each idempotent $x \in R$, we define the subspace $L_x := \{y \in R \mid xy = y\}$ of R. We write $y := \sum_{i=-l}^{r} y_i u_i$, where the coefficients y_i lie in $\mathbb{Z}_p$, and let $s_y := \sum_{i=-l}^{r} y_i$, $x_+ := P_+(x)$, and $y_+ := P_+(y)$.

Now $P_+(xy) = s_y x_+$, so $y_+ = s_y x_+$ for all $y \in L_x$. If $x_+ = 0$ then the equation $y_+ = s_y x_+$ requires that $y_+ = 0$ also. But A_- is isomorphic to $(A_{l+1,p})^{\mathrm{op}}$, so all of its idempotents are left unities, and thus in this case $L_x = A_-$ has dimension $l+1$. Note that this case does occur, e.g. $x := u_0$ is an idempotent with $x_+ = 0$.

Suppose instead that $x_+ \neq 0$. In this case, y_+ lies in the one-dimensional subspace $X := \mathrm{span}\{x_+\}$. The condition $s_y x_+ = y_+$ implies that L_x is contained in a subspace of $X + A_-$ of codimension 1. Thus $\dim L_x \leq l + 1$.

We conclude that $M_L := \max_x(\dim L_x) = l + 1$, where x ranges over all idempotents in R. By symmetry, if we define $R_x := \{y \in R \mid yx = y\}$, then $M_R := \max_x(\dim R_x) = r + 1$, where again x ranges over all idempotents in R.

We assumed that $l, r > 0$ in the above argument. But if either l or r equals 0, then R is either $A_{n,p}$ or $(A_{n,p})^{\mathrm{op}}$, respectively, and the above formulae for M_L and M_R follow immediately.

The numbers M_L and M_R are the desired isomorphism invariants that allow us to recover the parameters l and r, and hence to deduce that different choices of the parameters l, r, p always lead to distinct isomorphism types for $B_{l,r,p}$.

Finally, we note that the invariants M_L and M_R automatically imply (h). □

Proof of Theorem 4.5. We first prove (a). Suppose R is Jordan isomorphic to $\mathbb{Z}_p^n$, and so it has an idempotent basis $\{u_1, \ldots, u_n\}$ with $u_i u_j + u_j u_i = 0$ whenever i, j are distinct indices. Now

$$u_i u_j = u_i^2 u_j = u_i(u_i u_j) = u_i(-u_j u_i) = (-u_i u_j)u_i = (u_j u_i)u_i = u_j u_i^2 = u_j u_i \,.$$

Thus $2u_i u_j = 0$, and so $u_i u_j = 0$ since $|R|$ is odd. Since this holds for all distinct indices i, j, it follows that $R = \mathbb{Z}_p^n$, as desired.

We now prove (b). One direction follows from Theorem 4.2(c), so it remains to prove that if a ring R is Jordan isomorphic to $A_{n,p}$ for some $n \in \mathbb{N}$, then it is isomorphic to some $B_{l,r,p}$, where $l + r + 1 = n$. In fact we prove that R has a chain of subalgebras S_m of dimension m for each $1 \leq m \leq n$ that are of the form $B_{l_m,r_m,p}$, such that $l_m + r_m + 1 = m$ for all $1 \leq m \leq n$. An idempotent basis $\mathcal{B}_m$ of S_m will always be given by $\{u_i \mid -l_m \leq i \leq r_m\}$, and there will be an associated bilinear map $\psi_m : S_m \times S_m \to S_m$ defined on $\mathcal{B}_m \times \mathcal{B}_m$ by the equations $\psi_m(u_i, u_j) := u_i u_j$, $-l_m \leq i, j \leq r_m$. Moreover this function ψ_m will always satisfy (4.1) (with $l, r, \psi_{\mathcal{B}}$ replaced by l_m, r_m, ψ_m), and $\mathcal{B}_{m+1}$ will be formed from $\mathcal{B}_m$ by adjoining a single element u_{-l_m-1} or u_{r_m+1}, and so $l_{m+1} \in \{l_m, l_m + 1\}$ and $r_{m+1} \in \{r_m, r_m + 1\}$.

We begin by selecting any nonzero idempotent u_0, and let $S_1 = \mathrm{span}\{u_0\}$. Because u_0 is an idempotent, S_1 is a subalgebra. Suppose we have defined S_m for some $m < n$, and that $S_m = B_{l_m,r_m,p}$. There remain idempotents outside of S_m, since S_m has only p^{m-1} nonzero idempotents, whereas R has p^{n-1} of them. Let us therefore select a nonzero idempotent $v \in R \setminus S_m$. By the Jordan isomorphism property, $u_0 v + v u_0 = u_0 + v$, so at least one of $u_0 v$ and $v u_0$ lies outside S_m. By symmetry, it suffices to consider only the case $u := u_0 v \notin S_m$. We exploit the identity $xyx = x$ for nonzero idempotents $x, y \in R$ (as follows from Lemma 4.6 for rings that are Jordan isomorphic to $A_{n,p}$). For $j < 0$,

$$u u_j = (u_0 v)(u_0 u_j) = (u_0 v u_0)u_j = u_0 u_j = u_j \,.$$

For $j \geq 0$,

$$u u_j = (u_0 u_j v)u_j = u_0(u_j v u_j) = u_0 u_j = u_0 \,.$$

The products $u_j u$ are then calculated via the Jordan isomorphism property, giving $u_j u = u$ when $j < 0$ and $u_j u = u_j + u - u_0$ when $j \geq 0$. Thus if we define $u_{-l_m-1} := u$, and write $\mathcal{B}_{m+1} = \mathcal{B}_m \cup \{u_{-l_m-1}\}$, then the bilinear map $\psi_{m+1} : S_{m+1} \times S_{m+1} \to S_{m+1}$ defined on $\mathcal{B}_{m+1} \times \mathcal{B}_{m+1}$ by the equations $\psi_{m+1}(u_i, u_j) := u_i u_j$ for all $-l_m - 1 \leq i, j \leq r_m$, satisfies (4.1) as required. □

Proof of Theorem 4.4. Parts (a) and (b) are just restatements of Theorems 3.2 and 3.3(c). Part (c) follows from Theorems 3.3 and 4.5. □

Proof of Theorem 1.3. Part (a) follows from Theorems 3.2 and 3.3, and Part (b) follows from Theorems 4.2 and 4.4. □

References

[1] G. Ancochea, *Le Théorème de von Staudt en géométrie projective quaternionienne*, J. Reine Angew. Math. **184** (1942) pp. 193–198.
[2] G. Ancochea, *On semi-automorphisms of division algebras*, Ann. of Math. (2) **48** (1947), 147–153.
[3] S.M. Buckley and D. MacHale, *Finite rings with many idempotents*, preprint. (Available at `http://www.maths.nuim.ie/staff/sbuckley/Papers/idem_2.pdf`)
[4] I.N. Herstein, *Jordan homomorphisms*, Trans. Amer. Math. Soc. **81** (1956), 331–341.
[5] N. Jacobson, *Isomorphisms of Jordan Rings*, Amer. J. Math., *70* (1948), 317–326.
[6] N. Jacobson and C.E. Rickart, *Jordan homomorphisms of rings*, Trans. Amer. Math. Soc. **69** (1950), 479–502.
[7] I. Kaplansky, *Semi-automorphisms of rings*, Duke Math. J. **14** (1947), 521–525.
[8] D. MacHale, *Idempotents in finite rings*, Proc. R. Ir. Acad. Sect. A **82** (1982), 9–12.

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`