Finite rings with many idempotents

STEPHEN M. BUCKLEY AND DESMOND MACHALE

ABSTRACT. Let $\mathrm{Pr}_{\mathrm{I}}(R)$ be the proportion of idempotents in a ring R. We find all values of $\mathrm{Pr}_{\mathrm{I}}(R) \in [1/2, 1]$ when R is a finite ring or a 2-ring. Replacing the class of rings by the larger class of possibly nonassociative rings does not affect the sets of values of $\mathrm{Pr}_{\mathrm{I}}(R)$ that occur, and neither does the restriction to unital rings. We also discuss the types of rings that give rise to these values of $\mathrm{Pr}_{\mathrm{I}}(R)$.

1. Introduction

Given a finite possibly nonassociative (and possibly non-unital) ring R containing exactly m idempotent elements, we define its *idempotent proportion* to be $\mathrm{Pr}_{\mathrm{I}}(R) := m/|R|$. We also define the sets

$$\mathcal{I} = \{\mathrm{Pr}_{\mathrm{I}}(R) \mid R \text{ is a finite ring}\},$$
$$\mathcal{I}_p = \{\mathrm{Pr}_{\mathrm{I}}(R) \mid R \text{ is a } p\text{-ring}\},$$

where $p \in \mathbb{N}$ is a prime number, a *p-ring* means a ring of order p^n for some $n \geq 0$, and rings are not assumed to be unital. Corresponding sets $\mathcal{I}_{\mathrm{na}}$ and $\mathcal{I}_{p,\mathrm{na}}$ are defined using possibly nonassociative rings in place of rings, so trivially $\mathcal{I} \subset \mathcal{I}_{\mathrm{na}}$ and $\mathcal{I}_p \subset \mathcal{I}_{p,\mathrm{na}}$. In this paper we study these sets for $p = 2$. The sets $\mathcal{I}_p$ and $\mathcal{I}_{p,\mathrm{na}}$ for odd p are studied in [6].

Let us first recall a result of the second author [15, Theorem 4].

Theorem A. *If R is a finite ring with $\mathrm{Pr}_{\mathrm{I}}(R) > 3/4$, then R is a Boolean ring.*

In this paper, we extend this theorem by listing all possible values of $\mathrm{Pr}_{\mathrm{I}}(R) \geq 1/2$ when R is a finite ring, or a finite 2-ring. The values of $\mathrm{Pr}_{\mathrm{I}}(R) \geq 1/2$ involve the set $\mathfrak{A} := \{a(n) \mid 1 \leq n \leq \infty)$, where

$$a(n) := \begin{cases} (2^{n-1}+1)/2^n, & n \in \mathbb{N}, \\ 1/2, & n = \infty. \end{cases}$$

Our first main result concerns 2-rings.

Theorem 1.1.

(a) *If $\mathrm{Pr}_{\mathrm{I}}(R) > 1/2$ for a possibly nonassociative 2-ring R, then R is a $\mathbb{Z}_2$-algebra.*

(b) *$\mathcal{I}_2 \cap [1/2, 1] = \mathcal{I}_{2,\mathrm{na}} \cap [1/2, 1] = \mathfrak{A}$.*

(c) *The equations in (b) remain valid if we restrict to unital rings.*

Date: 04.11.2013.

2010 *Mathematics Subject Classification.* 16U99.

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

(d) *Whether R is assumed to be a finite ring or just a finite possibly nonassociative ring, we can find R of order 2^N with* $\mathrm{Pr}_{\mathrm{I}}(R) = a(n)$ *if and only if $N \ge g(n)$, where*

$$g(n) = \begin{cases} 0, & n = 1, \\ n, & 1 < n < \infty, \\ 1, & n = \infty. \end{cases}$$

The proof of the corresponding result for odd p in [6] involves the consideration of nonassociative rings even if we wish to handle only (associative) rings. The proof for $p = 2$ is quite different and, if we restrict our conclusions to rings, then nonassociative rings are not required in the proof. However we deal with all possibly nonassociative rings for consistency of analysis with [6], and because the results extend naturally to this setting without extra effort. It is also noteworthy and perhaps a little surprising that we get no additional $\mathrm{Pr}_{\mathrm{I}}(R)$ values when R is not required to be associative.

Using the above result, we can deduce a result for all finite possibly nonassociative rings R satisfying $\mathrm{Pr}_{\mathrm{I}}(R) > 1/2$.

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

(a) $\mathrm{Pr}_{\mathrm{I}}(R) = 2/3$ *and R is the direct sum of $\mathbb{Z}_3$ and a possibly nonassociative Boolean algebra, or*

(b) $\mathrm{Pr}_{\mathrm{I}}(R) \in \mathfrak{A}$ *and R is a possibly nonassociative $\mathbb{Z}_2$-algebra.*

After some preliminaries in Section 2, we investigate $\mathcal{I}_{\mathrm{na}}$ in Section 3 and prove the above results. Finally in Section 4, we explore the class of rings R of order 2^k, $k \le 4$, that satisfy $\mathrm{Pr}_{\mathrm{I}}(R) > 1/2$. The lesson that we draw from this exploration is that it would appear to be much harder to characterize all p-rings satisfying the condition $\mathrm{Pr}_{\mathrm{I}}(R) > 1/p$ when $p = 2$ than it was to do so for odd p in [6].

2. Preliminaries

We first list the basic terminology and notation used in this paper, other than what was already given in the introduction. A *ring* is required to be associative, but is not necessarily unital. A *2-ring* is a ring of order 2^n for some $n \ge 0$. A $\mathbb{Z}_2$-algebra means a ring R in which $2R = \{0\}$. Each of these concepts will be prefixed with the phrase *possibly nonassociative* whenever associativity is dropped as an assumption.

An *idempotent* of a possibly nonassociative ring R is an element x satisfying $x^2 = x$. An *idempotent basis* of an algebra will simply mean a basis consisting only of idempotents. A *possibly nonassociative Boolean ring* is a possibly nonassociative ring in which all elements are idempotent. Boolean rings are well known, but nonassociative Boolean rings also exist: see for instance Example 9 in Section II.12 of [4]. The fact that $2x = 0$ in a Boolean ring is well known; we note that the same proof works in a nonassociative Boolean ring: $-x = (-x)^2 = x^2 = x$.

$\mathbb{Z}_n$ 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 $\mathbb{Z}_n$. The *null algebra* O_{2^n} is the $\mathbb{Z}_2$-algebra of order 2^n in which all products are zero. $\mathrm{GF}(2^n)$ is the finite field of order 2^n, $n \in \mathbb{N}$.

Given a possibly nonassociative ring R, its *opposite ring* is R^{op}: $(R^{\mathrm{op}}, +) = (R, +)$, and multiplication $\circ$ in R^{op} is related to multiplication in R (denoted by juxtaposition) via the identity $x \circ y = yx$. (To avoid awkward terminology, we use the simple term "opposite ring" even when R and R^{op} are non-associative.) We say that R is *self-opposite* if it is isomorphic to its opposite ring.

Suppose R, S are possibly nonassociative rings and $\phi : R \to S$ is an additive group isomorphism. We call ϕ a *Jordan isomorphism* if it satisfies the identity $\phi(xy + yx) = \phi(x)\phi(y) + \phi(y)\phi(x)$ on R, or a *square isomorphism* if it satisfies the identity $\phi(x^2) = (\phi(x))^2$.

Jordan isomorphisms have been studied extensively, beginning with the papers [1], [2], [12], [10], [11], [9]. We have no specific reference for square isomorphisms, but they are of interest in this paper because idempotent proportion is an obvious square isomorphism invariant.

By expanding $\phi((x + y)^2)$, we see that every square isomorphism is a Jordan isomorphism. In the converse direction, a Jordan isomorphism clearly satisfies $2\phi(x^2) = 2(\phi(x))^2$, so Jordan and square isomorphisms are equivalent concepts for possibly nonassociative rings of odd order, but not for possibly nonassociative rings of even order. For instance all commutative possibly nonassociative $\mathbb{Z}_2$-algebras are trivially Jordan isomorphic, but they need not be square isomorphic; indeed, such possibly nonassociative algebras of dimension n have idempotent proportion ranging from 2^{-n} (for O_{2^n}) to 1 (for $\mathbb{Z}_2^n$).

The following simple lemma will be useful for verifying that an additive group isomorphism is a square isomorphism.

Lemma 2.1. *Suppose $\phi : R \to S$ is an additive group isomorphism, where R, S are possibly nonassociative rings. Suppose also that the subset $B \subset R$ generates $(R, +)$. Then ϕ is a square isomorphism if and only if:*

$$\left.\begin{aligned} \phi(x^2) = (\phi(x))^2\,, \\ \phi(xy + yx) = \phi(x)\phi(y) + \phi(y)\phi(x)\,. \end{aligned}\right\}\,, \qquad x, y \in B\,. \tag{2.1}$$

Proof. Because a square isomorphism is a Jordan isomorphism, it satisfies (2.1). The converse follows easily by distributivity. □

Observation 2.2. If R_i is square isomorphic to S_i for $i = 1, 2$, then $R_1 \oplus R_2$ is square isomorphic to $S_1 \oplus S_2$.

To prove that a pair of rings are not square isomorphic, we need some square isomorphism invariants. Fortunately, several can easily be discovered.

Observation 2.3. For rings of finite order the following are square isomorphism invariants: idempotent proportion, number of elements that are squares of other elements, number of elements in the ring whose square is zero.

Finally in this section, we make one observation and record two simple lemmas whose proofs we omit.

Observation 2.4. If x, y are both idempotent elements in a possibly nonassociative ring, then $x + y$ is idempotent if and only if $xy + yx = 0$.

Lemma 2.5. *Suppose R_1, R_1 are finite possibly nonassociative rings, and $x := x_1 \oplus x_2 \in R_1 \oplus R_2$. Then x is idempotent if and only if x_1, x_2 are both idempotent. Thus* $\mathrm{Pr}_{\mathrm{I}}(R_1 \oplus R_2) = \mathrm{Pr}_{\mathrm{I}}(R_1)\,\mathrm{Pr}_{\mathrm{I}}(R_2)$.

Lemma 2.6. *Suppose R is a ring of order 2^n for some $n \geq 0$, and $(R,+)$ is cyclic with generator u. Then R has either one or two idempotents, depending on whether or not $u^2 \in 2R$. Moreover if $\mathrm{Pr_I}(R) \geq 1/2$, then*

$$\mathrm{Pr_I}(R) \in \{a(1),\ a(\infty)\} = \{1,\ 1/2\}\,.$$

If $(R,+)$ is cyclic and $\mathrm{Pr_I}(R) = 1$, then R is either the ring of order 1 or $\mathbb{Z}_2$. If $(R,+)$ is cyclic and $\mathrm{Pr_I}(R) = 1/2$, then R is either O_2 or $\mathbb{Z}_4$.

3. Proofs of main results

The proof of Theorem 1.1(a) is similar to, but shorter than, that of [6, Theorem 3.2] which concerns p-rings for odd p, but we include a proof for completeness. Note that the condition $\mathrm{Pr_I}(R) > 1/2$ is best possible since $\mathrm{Pr_I}(\mathbb{Z}_4) = 1/2$.

Proof of Theorem 1.1(a).
Let $|R| = 2^n$. Suppose for the sake of contradiction that R is not an algebra. Let S_+, S_- be the collection of elements in R of (additive) order at least 4, or at most 2, respectively, and let $N(A)$ denote the number of idempotents in any subset A of R. Let m_+ be the number of pairs $(i,x) \in \{1,-1\} \times S_+$ such that ix is idempotent.

Since x and $-x$ cannot both be idempotent for $x \in S_+$, we have $m_+ \leq |S_+|$. However $y \mapsto iy$ is a bijection from S_+ to S_+ for both $i = 1$ and $i = -1$, so the mapping $f(i,x) := ix$ from $\{-1,1\} \times S_+$ to S_+ takes on each value twice. Consequently,

$$N(S_+) = \frac{m_+}{2} \leq \frac{|S_+|}{2}\,.$$

By the fundamental theorem of finite abelian groups, $(R,+)$ is an internal direct sum $A_+ \oplus A_-$, where A_+ is a direct sum of one or more cyclic groups of order at least 4, and A_- is an elementary abelian 2-group. Now $x_+ \oplus x_- \in A_+ \oplus A_-$ has order dividing 2 if and only if x_+ has order dividing 2, in which case distributivity implies that $x_+^2 = x_+x_- = x_-x_+ = 0$, and so $(x_+ \oplus x_-)^2 = x_-^2$. Thus $N(S_-) \leq |A_-| \leq |S_-|/2$; the latter inequality holds because A_+ is nontrivial. But R is the disjoint union of S_+ and S_-, so combining the estimates for $N(S_+)$ and $N(S_-)$, we get $N(R) \leq |R|/2$, contradicting the assumption that $\mathrm{Pr_I}(R) > 1/2$. □

Whenever R is a possibly nonassociative ring satisfying $nR = 0$ for some $n \in \mathbb{N}$, the *$\mathbb{Z}_n$-Dorroh extension $D_n(R)$* (introduced for rings in [7] and [5]) is the possibly nonassociative ring S, where $(S,+) = \mathbb{Z}_n \oplus R$ and multiplication is defined by $(i \oplus x)(j \oplus y) = ij \oplus (iy + jx + xy)$. Then S is a unital possibly nonassociative ring with unity $1 \oplus 0$, and we identify R with $\{0\} \oplus R$; also S is associative if and only if R is associative.

Lemma 3.1. *Suppose R, S are finite possibly nonassociative $\mathbb{Z}_2$-algebras.*

(a) $\mathrm{Pr_I}(D_2(R)) = \mathrm{Pr_I}(R)$.
(b) *$D_2(R)$ is square isomorphic to the ring direct sum $\mathbb{Z}_2 \oplus R$.*
(c) *If R and S are isomorphic (or square isomorphic), then $D_2(R)$ and $D_2(S)$ are isomorphic (or square isomorphic, respectively).*

Proof. We first prove (b). Let S be the (internal) ring direct sum $\mathbb{Z}_2 \oplus R$, so that S and $D_2(R)$ are equal as sets, with R being a subring of each. The desired square isomorphism $\phi : S \to D_2(R)$ is the identity map: although multiplication is different in S and $D_2(R)$, it is readily verified that squares match up.

Since idempotent proportion is a square isomorphism invariant, (a) follows immediately from (b). Lastly, the isomorphism part of (c) is as usual trivial. The square isomorphism part follows by using the fact that $D_2(R)$ and $D_2(S)$ are square isomorphic to $\mathbb{Z}_2 \oplus R$ and $\mathbb{Z}_2 \oplus S$, respectively, and then appealing to Observation 2.2. □

Suppose $n \in \mathbb{N} \cup \{0\}$. Throughout the rest of the paper, A_n will denote the n-dimensional $\mathbb{Z}_2$-algebra with idempotent basis $\mathcal{B} = \{u_0, \dots, u_{n-1}\}$ in which multiplication of basis elements is defined by $u_i u_j = u_i$; multiplication is extended to all of A_n by distributivity. It is clear that multiplication gives a semigroup structure to $\mathcal{B}$, and so the associated $\mathbb{Z}_2$-vector space becomes an algebra.

The following definition is a special case of Definition 4.1 in [6].

Definition 3.2. Suppose l, r are non-negative integers and $n := l + r + 1$. Let V be the n-dimensional vector space over $\mathbb{Z}_2$ with basis $\mathcal{B} := \{u_i \mid -l \le i \le r\}$. Define a bilinear map $\phi_{\mathcal{B}} : V \times V \to V$ by the equations

$$\phi_{\mathcal{B}}(u_i, u_j) = \begin{cases} u_i, & 0 \le i, j \le r, \\ u_j, & -l \le i, j \le 0, \\ u_0, & -l \le i < 0 \le j \le r, \\ u_i + u_j - u_0, & -l \le j < 0 \le i \le r. \end{cases} \tag{3.1}$$

$B_{l,r}$ is the vector space V equipped with multiplication $xy := \phi_{\mathcal{B}}(x, y)$. We define $R_-(\mathcal{B}) := \operatorname{span}\{u_i \mid -l \le i < 0\}$, $R_+(\mathcal{B}) := \operatorname{span}\{u_i \mid 0 < i \le r\}$, 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.

It is simple to verify that $B_{l,r}$ is a possibly nonassociative $\mathbb{Z}_2$-algebra of dimension $l + r + 1$, and it is clear that $B_{0,n-1} = A_n$ for all $n \in \mathbb{N}$. The importance of $B_{l,r}$ is tied to the following result.

Theorem 3.3. *Suppose l, r are non-negative integers and $n = l+r+1$. Let $B_{l,r}$, $\mathcal{B}$, $R_+ := R_+(\mathcal{B})$, $R_- := R_-(\mathcal{B})$, and $R_0 := R_0(\mathcal{B})$ be as in Definition 3.2.*

- *(a) $\mathcal{B}$ is an idempotent basis of $B_{l,r}$.*
- *(b) R_+, R_-, and R_0 are subrings isomorphic to A_r, $(A_l)^{\mathrm{op}}$, and A_1, respectively.*
- *(c) $B_{l,r}$ is square isomorphic to A_n.*
- *(d) $\mathrm{Pr}_{\mathrm{I}}(B_{l,r}) = a(n)$.*
- *(e) $B_{l,r}$ is a $\mathbb{Z}_2$-algebra.*
- *(f) If $\mathcal{B}' := \{u'_i \mid -l \le i \le r\}$ is another idempotent basis of $B_{l,r}$, 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) $B_{l,r}$ is isomorphic to $B_{l',r'}$ if and only if $l = l'$ and $r = r'$.*
- *(h) $B_{l,r}$ has a right unity if and only if $l = 0$, and a left unity if and only if $r = 0$.*

Theorem 3.3 is an analogue of Theorem 4.2 in [6], a result that deals with similarly defined $\mathbb{Z}_p$-algebras for odd primes p. We omit the proof because most of it follows exactly like the earlier result. The one exception is part (c), which follows readily from Lemma 2.1.

Proof of Theorem 1.1, parts (b)–(d).
Theorem 3.3 says that $\mathrm{Pr}_\mathrm{I}(B_{l,r}) = a(n)$ whenever l, r are non-negative integers with $l + r + 1 = n$, while Lemma 2.6 tells us that $\mathrm{Pr}_\mathrm{I}(O_2) = a(\infty)$. The fact that these rings are of minimal order follows readily from the condition that $|R| \, \mathrm{Pr}_\mathrm{I}(R)$ is always an integer. Rings of any larger order with the same idempotent proportion as these rings are obtained simply by taking direct sums with Boolean rings $\mathbb{Z}_2^m$ of the appropriate order. This proves (d). It remains to prove that $\mathcal{I}_{2,\mathrm{na}} \cap [1/2, 1] \subset \mathfrak{A}$: once we prove this, we have (b), and then (c) follows using Lemma 3.1(a).

It thus remains to show that if R is a finite possibly nonassociative ring of order 2^n with $\mathrm{Pr}_\mathrm{I}(R) > 1/2$, then $\mathrm{Pr}_\mathrm{I}(R) \in \mathfrak{A}$. By (a), R is a possibly nonassociative $\mathbb{Z}_2$-algebra. Let T be the set of all idempotents in R, and we assume without loss of generality that $|T| > 1$: otherwise $|R| = 1$ and the result is trivial. Let M be an additive subgroup of T of maximal order, so certainly $|M| > 1$.

For each subset S of R, we define the number $d(S) := N_1 - N_2$, where N_1 is the number of idempotents in S, and N_2 is the number of non-idempotents in S. By our hypotheses, we have $d(R) > 0$, and the desired conclusion is equivalent to the statement that $d(R)$ is a power of 2.

We now consider cosets of M in R of three different types. *Type A cosets* are those satisfying $M + x \neq M$ but $(M + x) \cap T \neq \emptyset$, allowing us to assume without loss of generality that $x \in T$. Observation 2.4 implies that $u + x \in T$ if and only if $ux + xu = 0$, and so $(M + x) \cap T$ is a coset of the subgroup M_x of M consisting of all elements that anticommute with x. Moreover $M_x \neq M$, since otherwise the subgroup generated by M and x would be a subgroup of idempotents, contradicting the maximality of M. So $|M_x|/|M| \leq 1/2$, and $d(M + x) \leq 0$.

The sole *Type B coset* is M itself: in this case $d(M) = |M|$. Finally *Type C cosets* are those whose intersection with T is empty: in this case $d(M) = -|M|$. Since $d(R) > 0$ is the sum of $d(M + x)$ over all cosets, we see that there are no type C cosets.

Consider now three separate cases, depending on the sizes of the subgroups M_x of M for various Type A cosets.

Suppose first that $|M_x|/|M| = 1/2$ for each Type A coset $M + x$. Then $d(M + x) = 0$ for every type A coset, and by summing over all cosets we get $d(R) = d(M) = |M|$. This is a power of 2, as required.

Suppose next that for a single Type A coset $M + y$, we have $|M_y|/|M| = 1/2^j$ for some $j > 1$, while for all other Type A cosets we have $|M_x|/|M| = 1/2$. Summing over all cosets we see that

$$d(R) = d(M + y) + d(M) = -|M|(1 - 2^{-j+1}) + |M| = 2^{-j+1}|M| \, ,$$

as desired.

Finally suppose that for at least two distinct Type A cosets $M + y$, $y \in \{u, v\}$, we have $|M_y|/|M| \leq 1/4$. Then

$$d(R) \leq d(M + u) + d(M + v) + d(M) \leq -\frac{|M|}{2} - \frac{|M|}{2} + |M| \leq 0 \, ,$$

contradicting the assumption that $d(R) > 0$. □

Proof of Theorem 1.2.
A finite nontrivial ring R is a direct sum of nontrivial rings R_p of order a power of p for some finite set of primes p, and so the elements of $\mathcal{I} \cap [1/2, 1]$ consist of products of elements in $\mathcal{I}_p \cap [1/2, 1]$ for a finite collection of primes p. But for odd p, the largest elements of $\mathcal{I}_p$ are 1 (attained only by the trivial p-ring), $2/p$ (attained only by $\mathbb{Z}_p$), and $(p+1)/p^2$, according to the results of [6]. Of these, the only numbers exceeding $1/2$ are 1 and $2/3$. Since $(2/3)(3/4)$ does not exceed $1/2$, we see that $\mathcal{I} \cap [1/2, 1] = \mathfrak{A}_2 \cup \{2/3\}$ and that, with one exception, these values occur only for 2-rings. The one exception is that the direct sum of $\mathbb{Z}_3$ and a Boolean ring has idempotent proportion $2/3$. Since $\mathcal{I}_{p,\mathrm{na}} \cap [1/p, 1] = \mathcal{I}_p \cap [1/p, 1]$, and since among possibly non-associative p-rings, the equations $\mathrm{Pr}_{\mathrm{I}}(R) = 1$ and $\mathrm{Pr}_{\mathrm{I}}(R) = 2/p$ occur only for the trivial p-ring and $\mathbb{Z}_p$, respectively, we get the same conclusions for possibly nonassociative rings as for rings. □

There are both similarities and differences between Theorem 1.1 and [6, Theorem 1.1] which is a roughly analogous result dealing with p-rings for odd primes p. The values that arise for odd p are denoted in [6] as $a(n, p)$ for $0 \le n \le \infty$, and they are natural analogues of the numbers $a(n)$, $0 < n \le \infty$, that arise for $p = 2$. Parts (a) and (b) of the two results are natural analogues of each other, although the proofs of the two parts (b) are very different: Theorem 1.1(b) is based on classical group theoretic methods (used in [16], [13], and [14]), while the proof of [6, Theorem 1.1(b)] is more combinatorial in nature. In terms of the statements of the results though, Theorem 1.1(c) is the first significant indication that the condition $\mathrm{Pr}_{\mathrm{I}}(R) > 1/p$ is a much less restrictive condition on a p-ring R when $p = 2$ than when $p > 2$, since if p is an odd prime there are no unital p-rings R with $\mathrm{Pr}_{\mathrm{I}}(R) > 1/p$ other than $\mathbb{Z}_p$ and the exceptional ring $\mathbb{Z}_3^2$; see Theorems 4.2 and 4.4 of [6].

[6, Theorem 1.1(c)] provides further evidence of how much more restrictive $\mathrm{Pr}_{\mathrm{I}}(R) > 1/p$ is for odd p: it indicates that, with one exception, all possibly nonassociative p-rings R for which $\mathrm{Pr}_{\mathrm{I}}(R) = a(n, p)$ must be Jordan isomorphic (or equivalently, square isomorphic). Furthermore if we insist on associativity, then [6, Theorem 4.4] says that with one exception, each value $a(n, p)$ of $\mathrm{Pr}_{\mathrm{I}}(R) > 1/p$ gives rise to exactly n isomorphism types of p-rings: these types are the $\mathbb{Z}_p$-analogues of what we here call $B_{l,r}$ for $l + r + 1 = n$. The one exceptional case in both of these results occurs when $(p, n) = (3, 2)$, and is represented by $\mathbb{Z}_3^2$.

By contrast, no such result is possible when $p = 2$ for the simple reason that if a finite ring R_1 is the direct sum of a ring R_0 and a Boolean ring, then $\mathrm{Pr}_{\mathrm{I}}(R_1) = \mathrm{Pr}_{\mathrm{I}}(R_0)$, and so the equation $\mathrm{Pr}_{\mathrm{I}}(R) = a(n)$ does not even tie down the order of R, let alone its square isomorphism type. Nevertheless one might hope for a characterization of all possible isomorphism types, or at least square isomorphism types of 2-rings R satisfying $\mathrm{Pr}_{\mathrm{I}}(R) > 1/2$. Unfortunately achieving this would appear not to be straightforward, based on the evidence for rings of order 2^k, $k \le 4$, presented in the next section.

4. Rings of small order with many idempotents

In this section, we discuss rings R of order 2^k, $k \le 4$, that satisfy $\mathrm{Pr}_{\mathrm{I}}(R) > 1/2$. The cases $k = 0, 1$ are handled by Lemma 2.6, so let us begin by considering rings of order 4. Since it is not hard to do so in this case, we also consider the endpoint condition $\mathrm{Pr}_{\mathrm{I}}(R) = 1/2$.

Theorem 4.1. *Suppose R is a ring of order 4, and $\mathrm{Pr}_{\mathrm{I}}(R) \ge 1/2$. Then one of the following holds:*

(a) $\mathrm{Pr}_{\mathrm{I}}(R) = a(1) = 1$, *and* $R = \mathbb{Z}_2^2$.
(b) $\mathrm{Pr}_{\mathrm{I}}(R) = a(2)$, *and R is isomorphic to either A_2 or $(A_2)^{\mathrm{op}}$.*
(c) $\mathrm{Pr}_{\mathrm{I}}(R) = a(\infty) = 1/2$, *and R is isomorphic to one of the following four rings: $\mathbb{Z}_4$, $\mathrm{GF}(4)$, $\mathbb{Z}_2 \oplus O_2$, and the Dorroh extension $D_2(O_2)$.*
(d) The above rings fall into five distinct square isomorphism classes. The only square isomorphic pairs are the two in (b), and the pair $\mathbb{Z}_2 \oplus O_2$ and $D_2(O_2)$.

Proof. If R is not an algebra, then $(R, +)$ is cyclic, and the condition $\mathrm{Pr}_{\mathrm{I}}(R) \ge 1/2$ implies that R is isomorphic to $\mathbb{Z}_4$ since the other two rings R with cyclic additive group and $|R| = 4$ are nil. Suppose therefore that R is an algebra. There are eight algebras of order 4, as found for instance in [8], and (a)–(c) follow by a routine examination of these types.

It remains to prove (d). The fact that the indicated pairs are square isomorphic follows from Theorem 3.3(c) and Lemma 3.1(b). Since idempotent proportion is a square isomorphism invariant, it remains only to prove that there are no other square isomorphisms between the rings in (c). The additive structure of $\mathbb{Z}_4$ distinguishes it from the others. We distinguish $\mathrm{GF}(4)$ from the other two algebras in (c) by the number of squares that they contain: $\mathrm{GF}(4)$ has four, while the other algebras have only two. □

Remark 4.2. The fact that for $p = 2$, the condition $\mathrm{Pr}_{\mathrm{I}}(R) > 1/p$ for rings of order p^2 corresponds to two square isomorphism types and three isomorphism types is not so different from the situation for odd primes p. In fact, an analysis of the isomorphism types given in [8] shows that the numbers of square isomorphism types and isomorphism types are the same for $p = 3$ as for $p = 2$, and they are both smaller by one for $p > 3$ since then $\mathrm{Pr}_{\mathrm{I}}(\mathbb{Z}_p^2) < 1/p$. However this same analysis reveals a large difference between $p > 2$ and $p = 2$ for the condition $\mathrm{Pr}_{\mathrm{I}}(R) = 1/p$: there are no such rings of order p^2 when $p > 2$ in contrast to the four obtained when $p = 2$.

Theorem 4.3. *Rings of order 8 with $\mathrm{Pr}_{\mathrm{I}}(R) > 1/2$ consist of exactly three square isomorphism types and seven isomorphism types.*

Proof. Consider first the rings that are directly decomposable: by Lemma 2.5, it follows that these are each of the form $S = \mathbb{Z}_2 \oplus R$, where R is one of the rings in parts (a), (b) of Theorem 4.1. Of these $\mathbb{Z}_2 \oplus A_2$ and $\mathbb{Z}_2 \oplus (A_2)^{\mathrm{op}}$ are square isomorphic by Theorem 3.3(c) and Observation 2.2, but they are not isomorphic because the former has right unities, whereas the latter does not. $\mathbb{Z}_2 \oplus \mathbb{Z}_2^2$ is not even square isomorphic to the other two because it has a different idempotent proportion. Thus we get two square isomorphism types and three isomorphism types.

We next consider the indecomposable rings. Theorem 3.3 gives three non-isomorphic but square isomorphic $\mathbb{Z}_2$-algebras R of order 8 with $\mathrm{Pr}_{\mathrm{I}}(R) > 1/2$, namely $R = B_{2-r,r}$ for $r \in \{0, 1, 2\}$. These must be indecomposable, since otherwise they would have the same idempotent proportion as one of the earlier decomposable rings. However this is not the case, since $\mathrm{Pr_I}(R) = a(3)$ in all cases.

Another ring to consider is the Dorroh extension $R_8 := D_2(A_2)$, with idempotent basis $\mathcal{B} := \{e, f, 1\}$, where $ef = e$ and $fe = f$. By Lemma 3.1(a), $\mathrm{Pr_I}(R_8) = \mathrm{Pr_I}(A_2) = a(2)$. Now R_8 is self-opposite since it is isomorphic to the Dorroh extension $D_2((A_2)^{\mathrm{op}})$, as we see by considering the basis $\mathcal{B}' := \{e', f', 1\}$ of R_8, where $e' := 1 + e$, $f' := 1 + f$. There are only two other rings of order eight considered in this proof that have the same idempotent proportion, namely $S_8 := \mathbb{Z}_2 \oplus A_2$ and $S'_8 := \mathbb{Z}_2 \oplus (A_2)^{\mathrm{op}}$. These last two rings are not self-opposite—in fact, $S'_8 = (S_8)^{\mathrm{op}}$—so R_8 is not isomorphic to either of them. However R_8, S_8, and S'_8 are all square isomorphic by Lemma 3.1.

It remains to prove that no other isomorphism types are possible for indecomposable rings of order 8 satisfying $\mathrm{Pr_I}(R) > 1/2$. By Theorem 1.1, it suffices to consider $\mathbb{Z}_2$-algebras. We examine separately the various cases according to the order of the Jacobson radical $J(R)$. If $|J(R)| = 1$, then by the Artin-Wedderburn theorem, $R = \mathrm{GF}(8)$, so R has only two idempotents and we eliminate this case. We also eliminate the case $|J(R)| = 8$, because then R is nil.

There remain the cases $|J(R)| \in \{2, 4\}$. For these cases, we appeal to the classification of rings of order p^3 given in [3], and refer to rings as Numbers 17–24, according to their numbers in [3, pp. 461–462].

Number 17 is the only indecomposable $\mathbb{Z}_2$-algebra R of order 8 with $|J(R)| = 2$, and we claim that this is R_8. The presentation of Number 17 in [3] involves a basis $\{e_1, e_2, a\}$, where e_1, e_2 are orthogonal idempotents, $e_1a = ae_2 = a$, and $a^2 = ae_1 = e_2a = 0$. We get these equations in R_8 by taking $e_1 := 1 + e$, $e_2 := e$, and $a := e + f$, so the claim is true.

Numbers 18–24 are the only indecomposable $\mathbb{Z}_2$-algebras R of order 8 with $|J(R)| = 4$. Numbers 18 and 19 are commutative rings, and each has a basis consisting of the unity plus two nilpotent elements, so they only have one nonzero idempotent, and we discard them. After some calculation, we see that numbers 21 and 22 each has three idempotents so we can discard them. (It is easier to see that there are at most 4 idempotents in both cases, and this is already enough to discard them: this holds when R is number 21 because R^2 is a subset of $\mathrm{span}\{e, b\}$, and it holds for number 22 because it has a basis $\mathcal{B} := \{a, e, b\}$ and both x^2 and $xy + yx$ lie in $\{e, b\}$ for all choices of $x, y \in \mathcal{B}$.) The three remaining rings are of the form $B_{2-r,r}$: number 20 is $B_{0,2}$ (take $\{u_0, u_1, u_2\} := \{e, e + a, e + b\}$), number 23 is $B_{1,1}$ (take $\{u_{-1}, u_0, u_1\} := \{e + b, e, e + a\}$), and number 24 is $B_{2,0}$ (take $\{u_{-2}, u_{-1}, u_0\} := \{e + a, e + b, e\}$). □

Remark 4.4. Theorem 4.3 should be contrasted with the situation for rings R of order p^3 that satisfy $\mathrm{Pr_I}(R) > 1/p$ for some odd prime p. According to Theorems 1.1 and 4.4 of [6] there are just one square isomorphism type and three isomorphism types for such rings: each is a $\mathbb{Z}_p$-algebra of type analogous to $B_{2-r,r}$.

Theorem 4.5. *Rings of order* 16 *with* $\mathrm{Pr_I}(R) > 1/2$ *include at least five square isomorphism types and at least sixteen isomorphism types.*

Proof. Consider first the decomposable rings. Among these are the direct sums $S = R \oplus \mathbb{Z}_2$, where R is any of the seven rings occurring in Theorem 4.3: arguing as in the proof of that theorem, we see that no two of these seven rings S

are isomorphic, and that they are square isomorphic only if the corresponding summands R are square isomorphic.

Next we consider direct sums of two rings of order 4. The only ones of these that are different from the previous seven are $R_1 := A_2 \oplus A_2$, $R_2 := A_2 \oplus (A_2)^{\mathrm{op}}$, and $R_3 := (A_2)^{\mathrm{op}} \oplus (A_2)^{\mathrm{op}}$, which all give idempotent proportion $a(4)$. By virtue of having a different idempotent proportion from any of the first seven, they cannot be square isomorphic to any of the earlier ones, but they are square isomorphic to each other by Theorem 4.1(d). No two of them are isomorphic since by Theorem 3.3(h), R_1 has only right unities, R_3 has only left unities, and R_2 has neither left nor right unities. Thus the decomposable rings of order 16 yield exactly four square isomorphism types and ten isomorphism types.

Next we have the four rings $B_{3-r,r}$. Certainly no two of these rings are isomorphic by Theorem 3.3. They all have the same idempotent proportion $a(4)$ as R_i, $i = 1, \dots, 3$, and those are the only decomposable rings with that idempotent proportion. Each $B_{3-r,r}$ is square isomorphic to A_4, and so it has eight elements with square zero since A_4 has eight such elements (namely $\sum_{i=0}^{3} a_i u_i$, where each a_i lies in $\mathbb{Z}_2$ with $\sum_{i=0}^{3} a_i = 0$, and the elements $u_0, \dots, u_3$ form an idempotent basis of A_4, as in Definition 3.2). By contrast, A_2 has two elements with square zero, and so $R_1 = A_2 \oplus A_2$ has four elements with square zero. Since R_i, $i = 1, \dots, 3$, are all square isomorphic, they all have four elements with square zero. Thus $B_{3-r,r}$ is not square isomorphic to the rings R_i, $i = 1, 2, 3$, and so it must be indecomposable since we have ruled out it being isomorphic to any of the decomposable examples.

Lastly we define the Dorroh extensions $R_{16} = D_2(A_3)$ and $S_{16} = D_2(B_{1,1})$. Thus R_{16} has idempotent basis $\{u_0, u_1, u_2, 1\}$ with $u_i u_j = u_i$ for all i, j, and S_{16} has idempotent basis $\{u_{-1}, u_0, u_1, 1\}$ with $u_i u_j$ as defined in Definition 3.2. We call $\{0, 1, 2\}$ the *index set of* R_{16}, and $\{-1, 0, 1\}$ the index set of S_{16}.

Then S_{16} is self-opposite because $B_{1,1}$ is self-opposite, and R_{16} is self-opposite because $R_{16} = D_2((A_3)^{\mathrm{op}})$, as we can see by considering multiplication for the basis $\{1+u_0, 1+u_1, 1+u_2, 1\}$. By Lemma 3.1, $\mathrm{Pr_I}(R_{16}) = \mathrm{Pr_I}(S_{16}) = a(3)$. This is the same idempotent proportion as the three rings $B_{2-r,r} \oplus \mathbb{Z}_2$, but each of these latter rings is non-unital because each $B_{2-r,r}$ is non-unital, and so it cannot be isomorphic to either of the unital rings R_{16} and S_{16}.

Since A_3 and $B_{1,1}$ are square isomorphic, it follows from Lemma 3.1(c) that R_{16} and S_{16} are square isomorphic. However we claim that R_{16} and S_{16} are not isomorphic. Each has three nonzero nilpotents, namely elements of the form $z := u_i + u_j$ for distinct indices i, j, and eight idempotents that are different from 0 and 1. In both rings, we partition the set of idempotents into two subsets, $E := \{u_i \mid i \in I\} \cup \{\sum_{i \in I} u_i\}$, and $F := \{1 + x \mid x \in E\}$, where I is the index set for the ring in question. For the ring R_{16} and a nilpotent z, $ez = 0$ whenever $e \in E$, and $ez = z$ whenever $e \in F$. However for the ring S_{16}, if we choose the nilpotent $z := u_1 + u_{-1}$ and the idempotent $e := u_0$, we see that $ez = u_0 + u_{-1}$ is a nonzero idempotent different from z. The claim follows.

Lastly, it follows from Theorem 3.3(c) and Lemma 3.1(c) that both R_{16} and S_{16} are square isomorphic to each of the rings $B_{2-r,r} \oplus \mathbb{Z}_2$. □

Remark 4.6. Theorem 4.5 should be contrasted with the situation for rings R of order p^4 that satisfy $\mathrm{Pr_I}(R) > 1/p$ for some odd prime p. According to Theorems 1.1 and 4.4 of [6] there is just one square isomorphism type and four isomorphism types for such rings: each is a $\mathbb{Z}_p$-algebra of type analogous to $B_{3-r,r}$.

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] V.G. Antipkin and V.P. Elizarov, *Rings of order p^3*, Sib. Math. J. **23** (1982), 457–464.

[4] G. Birkhoff, *Lattice Theory*, Corrected reprint of the 1967 third edition, American Mathematical Society Colloquium Publications 25, American Mathematical Society, Providence, R.I., 1979.

[5] B. Brown and N.H. McCoy, *Rings with unit element which contain a given ring*, Duke Math. J. **13** (1946), 9–20.

[6] S.M. Buckley and D. MacHale, *Odd order rings with many idempotents*, preprint. (Available at `http://www.maths.nuim.ie/staff/sbuckley/Papers/idem_1.pdf`)

[7] J.L. Dorroh, *Concerning Adjunctions to Algebras*, Bull. Amer. Math. Soc. 38 (1932) 85–88.

[8] B. Fine, *Classification of finite rings of order p^2*, Math. Mag. **66** (1993), 248–252.

[9] I.N. Herstein, *Jordan homomorphisms*, Trans. Amer. Math. Soc. **81** (1956), 331–341.

[10] N. Jacobson, *Isomorphisms of Jordan Rings*, Amer. J. Math., *70* (1948), 317–326.

[11] N. Jacobson and C.E. Rickart, *Jordan homomorphisms of rings*, Trans. Amer. Math. Soc. **69** (1950), 479–502.

[12] I. Kaplansky, *Semi-automorphisms of rings*, Duke Math. J. **14** (1947), 521–525.

[13] H. Liebeck and D. MacHale, *Groups with automorphisms inverting most elements*, Math. Z. **124** (1972), 51–63.

[14] H. Liebeck and D. MacHale, *Groups of odd order with automorphisms inverting many elements*, J. London Math. Soc. (2) **6** (1973), 215–223.

[15] D. MacHale, *Rings that are nearly Boolean*, Proc. R. Ir. Acad. Sect. A **80** (1980), 41–46.

[16] G.A. Miller, *Isomorphisms of a group whose order is a power of a prime*, Trans. Amer. Math. Soc. **12** (1911), 387–402.

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`