QUASISHEFFER OPERATIONS AND k-PERMUTABLE ALGEBRAS

CLIFFORD BERGMAN

ABSTRACT. A well known theorem of Murskiĭ's asserts that almost every finite, nonunary algebra is idemprimal. We derive an analagous result under the assumption that all basic operations are idempotent. If the algebra contains a basic ℓ-ary idempotent operation with $\ell > 2$ then the algebra is idemprimal with probability 1. However, for an algebra with a single basic binary operation, the probability of idemprimality is only $e^{-2} \approx 0.14$.

These observation are applied to show that for any $k > 2$, a finite algebra generating a congruence k-permutable variety will, with probability 1, generate a congruence 2-permutable variety.

This investigation arose from the observation that we know few examples of varieties that are congruence 3-permutable but not 2-permutable, 4-permutable but not 3-permutable, etc. (Definitions of these terms appear in Sections 1 and 2.) On the face of it, it ought to be easy to create such varieties. The Hagemann-Mitschke terms provide a recipe for constructing a k-permutable variety. By choosing the remaining values of those operations randomly, one would expect that the resulting variety would fail to satisfy any other identities (such as $(k-1)$-permutability).

As we discovered, that turns out not to be the case. A random, finite, k-permutable algebra almost surely generates a 2-permutable variety. In fact, as we shall demonstrate below, a random, idempotent, ternary operation on a finite set will be quasisheffer with probability 1. The resulting algebra is not only 2-permutable, but also rigid, and quasiprimal, so it generates a variety that is congruence distributive, semisimple, and equationally complete.

These results are not surprising in light of Murskiĭ's theorem: almost every nonunary operation on a finite set is quasisheffer. The only new wrinkle here is the requirement that the operation be idempotent. But note that Murskiĭ's theorem applies even to binary operations. As we show in Theorem 2.13, the probability that an idempotent binary operation be quasisheffer is quite small.

1. Background and definitions

Basic concepts of universal algebra as well as explanations for the notation used in this paper can be found in [1]. Let A be a set, α, β binary relations on A. The

---

Date: August 2017.

2010 *Mathematics Subject Classification.* Primary: 08A40; Secondary: 08B05, 60A99.

Key words and phrases. congruence permutable, idemprimal, Murskiĭ, quasisheffer, relative product.

Research partially supported by NSF grant no. 1500235 and the Barbara J. Janson Professorship in Mathematics.

relative product of α *and* β is the binary relation

$$\alpha \circ \beta = \{\, (x, z) : (\exists y \in A)\ (x, y) \in \alpha \text{ and } (y, z) \in \beta \,\}\,.$$

We define an iterated version of relative product recursively as follows.

$$\alpha \circ^{0} \beta = \alpha;$$

$$\alpha \circ^{k+1} \beta = \alpha \circ (\beta \circ^{k} \alpha), \text{ for } k \geq 0.$$

Let k be an integer, $k > 1$. A variety, $\mathcal{V}$, is *congruence k-permutable* if, for every algebra, $\mathbf{A}$, in $\mathcal{V}$, and every $\alpha, \beta \in \mathrm{Con}(\mathbf{A})$ we have $\alpha \circ^{k-1} \beta = \beta \circ^{k-1} \alpha$. In particular, congruence 2-permutability is generally called "congruence permutability" in the literature. Congruence k-permutability is important because it provides a bound on the construction of the join of two congruences in the congruence lattice. Finally, since no confusion is likely to result, we will drop the word "congruence" and simply say k-permutable instead of congruence k-permutable.

Definition 1.1. Let k be an integer, $k > 2$. A variety, $\mathcal{V}$, is *sharply k-permutable* if it is k-permutable and not $(k-1)$-permutable.

The initial stimulus for this project was the search for sharply 3- and 4-permutable varieties. A few examples are well-known. Implication algebras are sharply 3-permutable, and Polin's variety is sharply 4-permutable. Both E. T. Schmidt [8] and K. Kearnes [5, Example 3.8] have constructed a tower of varieties containing, for each k, a sharply k-permutable member. These examples are somewhat contrived, rather than typical. In particular, with the exception of Polin's variety, they are all congruence-distributive.

Since we are primarily interested in finitely generated varieties, we frequently use these notions in the context of a single algebra. Thus an algebra, $\mathbf{A}$, is k-permutable (sharply k-permutable) if $\mathbf{A}$ generates a variety that is k-permutable (sharply k-permutable). Our original goal was to construct random, finite, sharply k-permutable algebras for small values of k.

For every $k > 1$, congruence k-permutability is a strong Maltsev condition. This was established by Hagemann and Mitschke [3] in 1973.

Theorem 1.2. *Let k be an integer,* $k > 1$*. A variety,* $\mathcal{V}$*, is congruence k-permutable if and only if there are ternary terms* $p_1, \dots, p_{k-1}$ *such that* $\mathcal{V}$ *satisfies the identities*

$$(\mathrm{HM}_k) \qquad \begin{aligned} y &\approx p_1(x, x, y) \\ p_i(x, y, y) &\approx p_{i+1}(x, x, y), \quad \textit{for } 1 \leq i < k-1 \\ p_{k-1}(x, y, y) &\approx x. \end{aligned}$$

It follows from the equations in (HM_k) that each of the terms $p_1, \dots, p_{k-1}$ is idempotent. Consequently, a variety $\mathcal{V}$ is k-permutable if and only if the idempotent reduct of $\mathcal{V}$ is also k-permutable. For this reason, we restrict our attention to idempotent algebras throughout this paper.

Theorem 1.2 gives us a straightforward recipe for constructing a finite, random k-permutable algebra. Fix a finite set $A = \{0, 1, \dots, n-1\}$ and randomly choose basic ternary operations $p_1, \dots, p_{k-1}$ satisfying (HM_k). For example, one could proceed as follows.

1. Choose $p_1, \dots, p_{k-1}$ to be random ternary operations.
2. For each $x, y \in A$ redefine $p_1(x, x, y)$ to be y.
3. Working successively with $i = 1, 2, \dots, k-2$, for every $x, y \in A$, redefine $p_{i+1}(x, x, y)$ to be $p_i(x, y, y)$.
4. Finally for every $x, y \in A$ redefine $p_{k-1}(x, y, y)$ to be x.

This algorithm will indeed yield an algebra $\mathbf{A} = \langle A, p_1, p_2, \dots, p_{k-1} \rangle$ that is k-permutable. However, as a little experimentation will show, the resulting algebras is seldom *sharply* k-permutable. In fact, in hundreds of trials performed by this author, every single algebra turned out to be 2-permutable. The results in this paper constitute our efforts to understand this phenomenon.

2. Idemprimal algebras and quasisheffer operations

Let A be a finite set. We write $\mathrm{Op}_k(A)$ for the set of all k-ary operations on A, and set $\mathrm{Op}(A) = \bigcup_k \mathrm{Op}_k(A)$. The *clone generated by* f is denoted $\mathrm{Clo}(f)$ while $\mathrm{Clo}(\mathbf{A})$ is the clone of *term operations* of the algebra $\mathbf{A}$, equivalently, the clone generated by all of the basic operations of $\mathbf{A}$. A set Θ of relations on A induces a clone, $\mathrm{Pol}(\Theta)$, the clone of operations that preserve the members of Θ.

Recall that an operation, f, on a set A is called *idempotent* if $f(x, x, \dots, x) = x$, for all $x \in A$. The set of idempotent operations forms a clone, $\mathrm{Idem}(A)$. Lastly, we set $\mathcal{S}_A$ equal to $\{ \{a\} : a \in A \}$. Consider $\mathcal{S}_A$ to be a set of unary relations on A. Then $\mathrm{Idem}(A) = \mathrm{Pol}(\mathcal{S}_A)$.

The algebra $\mathbf{A}$ is called *primal* if $\mathrm{Clo}(\mathbf{A})$ contains $\mathrm{Op}_k(A)$ for every $k > 0$. An operation, f, on A, is *Sheffer* if the algebra $\langle A, f \rangle$ is primal. Similarly, $\mathbf{A}$ is *idemprimal* if $\mathrm{Clo}(\mathbf{A})$ contains $\mathrm{Idem}(A)$, and f is *quasisheffer* if $\langle A, f \rangle$ is idemprimal.

Since the discriminator is idempotent, every finite idemprimal algebra is quasiprimal, hence generates an arithmetical variety. It is not hard to see that an idemprimal algebra is simple, rigid, and has no proper nontrivial subalgebras. It is worth noting that if $\mathbf{A}$ is an idempotent algebra then to say that $\mathbf{A}$ is idemprimal is to assert that $\mathrm{Clo}(\mathbf{A}) = \mathrm{Idem}(A)$. A similar observation applies to quasisheffer operations.

In 1975, Murskiĭ proved that with probability 1, a randomly chosen k-ary operation (with $k > 1$) on a finite set will be quasisheffer. Our objective in this section is to prove a similar result under the assumption that the random operation is idempotent. We first make precise the notion of probability that we shall use.

In this context, by a finite set we shall mean one of the form $\{0, 1, \dots, n-1\}$ for some natural number, n. We shall write $\mathrm{Op}_k(n)$ in place of $\mathrm{Op}_k(\{0, 1, \dots, n-1\})$. Note that $|\mathrm{Op}_k(n)| = n^{(n^k)}$. Suppose that $\mathcal{P}$ is some collection of k-ary operations (a "property") on finite sets, and write $\mathcal{P}(n) = \mathcal{P} \cap \mathrm{Op}_k(n)$. Then we define the probability that a random k-ary operation has property $\mathcal{P}$ to be

$$\mathrm{Prob}(\mathcal{P}) = \lim_{n \to \infty} \frac{|\mathcal{P}(n)|}{|\mathrm{Op}_k(n)|}.$$

It is easy to see that this yields a finitely additive probability measure on the set of k-ary operations. For a further discussion of this idea see [2].

We can restrict this notion to idempotent operations. The probability that an operation will have $\mathcal{P}$ given that it is chosen randomly from the set of idempotent operations is simply the conditional probability

$$\mathrm{Prob}(\mathcal{P}|\,\mathrm{Idem}) = \lim_{n\to\infty} \mathrm{Prob}\big(\mathcal{P}(n)|\,\mathrm{Idem}_k(n)\big) = \lim_{n\to\infty} \frac{\big|\mathcal{P}(n)\cap \mathrm{Idem}_k(n)\big|}{\big|\mathrm{Idem}_k(n)\big|}$$

where $\mathrm{Idem}_k(n)$ denotes the set of idempotent k-ary operations on $\{0, 1, \dots, n-1\}$. This set has cardinality $n^{(n^k-n)}$.

Now let $\mathcal{QS}_k$ be the property that a k-ary operation is quasisheffer. In [6] Murskiĭ proved that for any $k > 1$ we have $\mathrm{Prob}(\mathcal{QS}_k) = 1$. Our objective is to establish analogous results for idempotent operations. In this section we shall prove

(1) $$\mathrm{Prob}(\mathcal{QS}_k|\,\mathrm{Idem}) = 1, \quad \text{for } k > 2$$

(2) $$\mathrm{Prob}(\mathcal{QS}_2|\,\mathrm{Idem}) = e^{-2} \approx 0.14.$$

There seems to be no way to directly derive equations (1) and (2) from the statement of Murskiĭ's theorem. However, we can imitate his proof. And, in fact, idempotence considerably simplifies the argument. Moreover, the single most difficult step in the proof, a particular combinatorial limit (Lemma 2.8), can be reused unchanged.

Let A be a finite set of cardinality greater than 2. In [9] (see also [10]), Á. Szendrei described the lower covers of $\mathrm{Idem}(A)$ in the lattice of clones. They are the clones $\mathrm{Pol}(\mathcal{S}_A \cup R)$, where R is one of the following relations:

(1) a proper nontrivial subset of A;
(2) a permutation of A of prime order containing at most one fixed point;
(3) a relation $X_a = \big(\{a\} \times A\big) \cup \big(A \times \{a\}\big)$, for some $a \in A$.

(On a 2-element set there are two additional choice for the relation R, namely the two linear orders.) In the terminology of [4], the relations of the form X_a are called 2-dimensional, thin, symmetric crosses. We shall just call them crosses. We can restate Szendrei's result as follows.

Theorem 2.1 (Szendrei)**.** *A finite idempotent algebra* $\mathbf{A}$*, of cardinality greater than 2, is idemprimal if and only if it has no proper nontrivial subalgebras, is rigid, and has no compatible crosses.*

We introduce one special-purpose notion. Let f be an idempotent ℓ-ary operation on a set A, I a proper nonempty subset of $\{1, 2, \dots, \ell\}$, and $a \in A$. Then $f_{I,a}(x)$ denotes the unary operation obtained from f by inserting the value a at the positions indicated by I and x in the remaining positions. For example, if $\ell = 3$ then for $I = \{1\}$ and $J = \{1, 3\}$ we have $f_{I,a}(x) = f(a, x, x)$ and $f_{J,a}(x) = f(a, x, a)$.

If the operation $f_{I,a}$ turns out to be constant, it will be called a *special translation* of f. Note that by idempotence, the constant value must be a. The relationship between special translations and crosses is captured by the following observation.

Lemma 2.2. *Let g be an idempotent binary operation on a set A, $a \in A$, and suppose that X_a is a cross compatible with g. Then either $g(a,-)$ or $g(-,a)$ is a* *constant unary operation on A. Put another way, either $g_{\{1\},a}$ or $g_{\{2\},a}$ is a special translation.*

Proof. For any $x, y \in A$, the pairs (a, x) and (y, a) lie in X_a. By the compatibility of this cross, $\big(g(a, y),\ g(x, a)\big) \in X_a$, hence

$$(\forall x, y \in A)\ \ g(a, y) = a \text{ or } g(x, a) = a.$$

Suppose that the unary operation $g(a, -)$ is not constant. Then there is some $b \in A$ with $g(a, b) \neq a$. Then for any x, (with $y = b$) we have $g(x, a) = a$, i.e., $g(-, a)$ is constant. □

Theorem 2.3. *Let* **A** *be a finite idempotent (nonunary) algebra of cardinality greater than 2. If* **A** *is not idemprimal then (at least) one of the following holds.*

(a) **A** *has a proper nontrivial subalgebra;*
(b) **A** *has a nontrivial automorphism;*
(c) Some basic operation of **A** *has a special translation.*

Proof. Suppose that **A** is not idemprimal, but that neither condition (a) nor (b) hold. By Theorem 2.1, **A** must have a compatible cross, X_a, for some $a \in A$. Choose some basic ℓ-ary operation, f, and set $I = \{2, 3, \dots, \ell\}$ and $J = \{1\}$. Then by Lemma 2.2, one of the operations $f_{I,a}$ or $f_{J,a}$ is constant, hence a special translation. □

Note. On a 2-element set there are two idempotent ternary operations that are not quasisheffer, but fail to satisfy any of the three conditions of Theorem 2.3.

In light of Theorem 2.3, we can establish the equality in (1) by determining the probability that each of the three conditions in the statement of the theorem holds. The second and third are quite easy, so we tackle those first.

Lemma 2.4. *Let f be an idempotent ℓ-ary operation on a finite set, A, with $\ell > 1$. Then the probability that $\langle A, f\rangle$ has a nontrivial automorphism is 0.*

Proof. Let $g(x, y) = f(x, y, y, \dots, y)$. Every automorphism of $\langle A, f\rangle$ is also an automorphism of $\langle A, g\rangle$. Notice that as f ranges uniformly over all idempotent ℓ-ary operations of A, g ranges uniformly over all idempotent binary operations. Thus it is enough to establish the lemma for an idempotent binary operation, g. We may as well write $x \cdot y$ in place of $g(x, y)$.

So suppose that $|A| = n$ and σ is a nontrivial automorphism of $\langle A, g\rangle$. There must be $a, b \in A$ with $\sigma(b) = a \neq b$. For every $x \in A$ we have $\sigma(b \cdot x) = \sigma(b) \cdot \sigma(x) = a \cdot \sigma(x)$. Hence $b \cdot x = \sigma^{-1}(a \cdot \sigma(x))$. Similarly, for every x, $x \cdot b = \sigma^{-1}(\sigma(x) \cdot a)$. Therefore, in the Cayley table for g, the row for b is completely determined by the row for a together with σ, and similarly for the b column. Thus we can choose $(n-1)\times(n-1)$ table entries randomly—except for the $(n-1)$ entries on the diagonal, which are determined by idempotence.

There are $n! - 1$ choices for σ. The proportion of n-element idempotent binars with a nontrivial automorphism is at most

$$\frac{n! \cdot n^{[(n-1)^2-(n-1)]}}{n^{[n^2-n]}} = \frac{n!}{n^w} \leq \frac{n^{(n-1)}}{n^{2(n-1)}} = \frac{1}{n^{n-1}}$$

where $w = (n^2 - n) - [(n-1)^2 - (n-1)] = 2(n-1)$. Since this fraction tends to 0 as n tends to infinity, the claim is established. □

Lemma 2.5. *Let f be an idempotent ℓ-ary operation on a finite set, with $\ell > 1$. Then the probability that f has a special translation is 0.*

Proof. First consider the case that f is binary on a set of cardinality n. Suppose that $f(a, x)$ has constant value a. Then the table for f has $n-1$ rows each of which has $n-1$ entries that can be chosen arbitrarily (all but the entry on the diagonal), and the remaining row contains nothing but the value a. There are n choices for a itself. Thus the proportion of idempotent binars with this property is

$$\frac{n \cdot n^{(n-1)^2}}{n^{n^2-n}} = \frac{n}{n^{n-1}}$$

which clearly tends to 0 as n tends to infinity. Obviously the same computation holds for the other special translation, $f(x, a)$.

Now suppose that $\ell > 2$. Let $\emptyset \subsetneq I \subsetneq A$ and $a \in A$. Define $g(y, x)$ by putting y in all positions indicated by I, and x in the remaining spots. Then $f_{I,a}$ will be a special translation if and only if $g(a, x)$ is constant. As f and I range uniformly over their respective domains, g will range uniformly over all idempotent binars. Then from the previous paragraph, the probability that f has a special translation is 0. □

Now we turn to the first condition in Theorem 2.3. The combinatorics are somewhat more complex. We are able to utilize Lemma 2.8 (below) which comes directly from Murskiĭ's original paper.

Lemma 2.6. *Let n, k be positive integers with $1 < k < n$ and f a random, idempotent ℓ-ary operation on $A = \{0, 1, \dots, n-1\}$, with $\ell > 1$. Then the probability that $\langle A, f\rangle$ has a subalgebra of cardinality k is at most $\binom{n}{k} \cdot \left(\frac{k}{n}\right)^{k^\ell - k}$.*

Proof. Let S be a subset of cardinality k. Of course $\left|S^\ell\right| = k^\ell$. In order for f to preserve S, all members of S^ℓ must be mapped back into S. The value of f on k of these ℓ-tuples is predetermined by idempotence. The remaining $(k^\ell - k)$ tuples can be chosen in n ways, k of which lie in S. Thus the probability that f maps all k^ℓ tuples back into S is $\left(\frac{k}{n}\right)^{k^\ell - k}$. Finally, there are $\binom{n}{k}$ choices for S. Since these subsets overlap, the best we can say is that $\binom{n}{k} \cdot \left(\frac{k}{n}\right)^{k^\ell - k}$ is an upper bound on the desired probability. □

Corollary 2.7. *Let f be a random, idempotent, ternary operation on a finite set A. Then the probability that $\langle A, f\rangle$ has a subalgebra of cardinality 2 is 0.*

Proof. By Lemma 2.6, with $|A| = n$, the probability that $\langle A, f\rangle$ has a subalgebra of cardinality 2 is at most $32(n^{-4} - n^{-5})$. This fraction clearly approaches 0 as n tends to infinity. □

The most difficult step in Murskiĭ's original argument is the following combinatorial limit. See [1, Lemma 6.22] for a proof.

Lemma 2.8. *Let* $\psi_n(k) = \binom{n}{k}^2 \cdot \left(\frac{k}{n}\right)^{k^2}$*. Then*

$$\lim_{n\to\infty} \sum_{k=3}^{n-1} \psi_n(k) = 0 \tag{3}$$

Lemma 2.9. *Let f be a random, idempotent, ternary operation on a finite set, A. Then the probability that $\langle A, f\rangle$ has a proper nontrivial subalgebra is* 0*.*

Proof. Corollary 2.7 addresses 2-element subalgebras, so we consider subalgebras of cardinality greater than 2. By Lemma 2.6, the probability we seek is bounded above by

$$\lim_{n\to\infty} \sum_{k=3}^{n-1} \binom{n}{k} \cdot \left(\frac{k}{n}\right)^{k^3-k}$$

But for $k > 1$ we have $k^3 - k > k^2$, so (since $k < n$), $\left(\frac{k}{n}\right)^{k^3-k} < \left(\frac{k}{n}\right)^{k^2}$. Since $\binom{n}{k} < \binom{n}{k}^2$ the result follows from Lemma 2.8. □

Theorem 2.10. *let f be a random, idempotent, ternary operation on a finite set. the the probability that f is quasisheffer is 1.*

Proof. Combine Theorem 2.3 with Lemmas 2.4, 2.5, and 2.9. □

It follows from Theorem 2.10 that if g is a random, idempotent, ℓ-ary operation with $\ell > 3$, then g is almost surely quasisheffer. Define $f(x, y, z) = g(x, y, z, z, \dots)$. As g ranges uniformly over all idempotent ℓ-ary operations, f ranges uniformly over all idempotent ternary operations. So with probability 1, f is quasisheffer. Since $\mathrm{Clo}(f) \subseteq \mathrm{Clo}(g)$, g must be quasisheffer as well.

We have established equation (1). Let us turn to (2). Unfortunately, Lemma 2.6 is no help here. Instead we shall use a special property of two element sets. Let $S = \{a, b\}$. An idempotent binary operation, f, preserves S if and only if f maps the set $S^* = S^2 - \{(a, a), (b, b)\}$ back into S. But if S and T are *distinct* 2-element subsets then S^* and T^* are *disjoint*. Consequently the events "f preserves S" and "f preserves T" are independent. (There is nothing special here about f being binary. This observation holds for idempotent ℓ-ary operations as well.)

Lemma 2.11. *Let f be a random, idempotent binary operation on a finite set $A = \{0, 1, \dots, n-1\}$. Then with probability* $1 - e^{-2} \approx 0.86$*, $\langle A, f\rangle$ has a subalgebra of cardinality 2.*

Proof. Using the argument in Lemma 2.6 (with $k = 2$), for any two-element subset, S, the probability that f does not preserve S is $1-(4/n^2)$. Since there are $\binom{n}{2}$ such subsets and their preservation is pairwise independent, the probability that no 2-element subset is preserved is $\left(1 - \frac{4}{n^2}\right)^{\binom{n}{2}}$. But

$$\lim_{n\to\infty} \left(1 - \frac{4}{n^2}\right)^{(n^2-n)/2} = e^{-2}.$$

This limit can be computed either by l'Hôpital's rule or by using the approximation $1 - x \approx e^{-x}$, for $x = 4/n^2$ very small. □

Note that Lemma 2.11 is an exact value and not simply an upper bound. This value turns out to be the correct probability for an idempotent binary operation to be quasisheffer, as we now show.

Lemma 2.12. *Let* **A** *be a finite idempotent binar. The probability of each of the following is 0.*

(1) **A** *has a proper subalgebra of cardinality greater than 2;*
(2) **A** *has a nontrivial automorphism;*
(3) **A** *has a compatible cross.*

Proof. The claim about automorphisms follows from lemma 2.4.

Let $a \in A$ and suppose that X_a is a compatible cross. By Lemma 2.2, either $a \cdot x$ or $x \cdot a$ is a special translation of **A**. But Lemma 2.5 asserts that almost no algebra has a special translation. Consequently, the probability that a finite algebra has a compatible cross is 0.

Finally, let $|A| = n$. From Lemma 2.6 the probability that **A** has a subalgebra of cardinality k is at most $\phi_n(k) = \binom{n}{k} \cdot \left(\frac{k}{n}\right)^{k^2-k}$. We shall show that $\phi_n(k) \leq \psi_n(k)$. Condition (1) of the lemma will follow from this inequality and Lemma 2.8.

Observe first that for $1 \leq j < k < n$, we have $\frac{n-j}{k-j} > \frac{n}{k}$. Hence

$$\binom{n}{k} = \left(\frac{n}{k}\right)\left(\frac{n-1}{k-1}\right)\left(\frac{n-2}{k-2}\right)\cdots\left(\frac{n-k+1}{1}\right) \geq \left(\frac{n}{k}\right)^k. \tag{4}$$

Now we compute

$$\frac{\phi_n(k)}{\psi_n(k)} = \frac{\binom{n}{k}\left(\frac{k}{n}\right)^{k^2-k}}{\binom{n}{k}^2\left(\frac{k}{n}\right)^{k^2}} = \frac{\left(\frac{k}{n}\right)^{-k}}{\binom{n}{k}} = \frac{\left(\frac{n}{k}\right)^{k}}{\binom{n}{k}} \leq 1$$

with the final inequality coming from (4). □

Theorem 2.13. *The probability that a random, finite, idempotent binar is idemprimal is precisely* $e^{-2} \approx 0.14$.

Proof. Let $\mathcal{E}$ be the event that a random, finite, idempotent binar has *none* of the properties in Lemma 2.12, and write $\overline{\mathcal{E}}$ for the complement of $\mathcal{E}$. That lemma shows that $\mathrm{Prob}(\overline{\mathcal{E}}) = 0$. Let $\mathcal{T}$ be the event that such a binar has no 2-element subalgebra. By Lemma 2.11, $\mathrm{Prob}(\mathcal{T}) = e^{-2}$. According to Theorem 2.1, $\mathcal{E} \cap \mathcal{T}$ is precisely the class of finite idempotent idemprimal binars.

Since $(\mathcal{E} \cap \mathcal{T}) \cup (\overline{\mathcal{E}} \cap \mathcal{T}) = \mathcal{T}$, and $\overline{\mathcal{E}} \cap \mathcal{T} \subseteq \overline{\mathcal{E}}$ has probability 0, it follows that $\mathrm{Prob}(\mathcal{E} \cap \mathcal{T}) = e^{-2}$. □

It may also be useful to consider algebras with 2 (independently chosen) idempotent binary operations. No new ideas are required here.

Theorem 2.14. *Let f and g be independently chosen idempotent binary operations on a finite set A. Then with probability 1, the algebra* $\mathbf{A} = \langle A, f, g\rangle$ *is idemprimal.*

Proof. For any pair of distinct elements a, b, the probability that both f and g preserve $\{a, b\}$ is $(4/n^2)^2$. Using the same argument as in Lemma 2.11, the probability that $\mathbf{A}$ has a 2-element subalgebra is 0. Consequently, by Theorem 2.1 and Lemma 2.12, $\mathbf{A}$ is idemprimal. □

3. SHARPLY k-PERMUTABLE ALGEBRAS

Let us return to the initial question: what is the probability that a random k-permutable algebra is actually 2-permutable? We provide a reasonably satisfying answer in the following theorem.

Theorem 3.1. *Let $k > 2$ and $p_1, \dots, p_{k-1}$ be random ternary operations on a finite set, A, that satisfy the identities in* (HM_k)*. With probability 1, the algebra $\mathbf{A} = \langle A, p_1, \dots, p_{k-1}\rangle$ is 2-permutable, in fact, idemprimal.*

Proof. We first treat the case $k > 3$. Consider the following minor variation on the algorithm presented in Section 1.

1. Choose random, idempotent, ternary operations $p_1, \dots, p_{k-1}$.
2. For each $x, y \in A$, redefine $p_1(x, x, y)$ to be y and $p_1(x, y, y)$ to be $p_2(x, x, y)$.
3. Working successively with $i = 2, 3, \dots, k-2$, for every $x, y \in A$, redefine $p_{i+1}(x, x, y)$ to be $p_i(x, y, y)$.
4. Finally, for every $x, y \in A$, redefine $p_{k-1}(x, y, y)$ to be x.

Any sequence $\langle p_1, \dots, p_{k-1}\rangle$ satisfying (HM_k) can be obtained by this algorithm with equal probability. Unlike the version in Section 1, this algorithm does not ever modify p_2 after its initial definition. Thus any idempotent ternary operation occurs as p_2 with equal probability. Then by Theorem 2.10, p_2 is quasisheffer with probability 1. This certainly implies that $\mathbf{A}$ is idemprimal, hence 2-permutable.

Now suppose that $k = 3$. The above algorithm does not work in this case, so we argue directly from Theorem 2.3. Let $\mathbf{A} = \langle A, p_1, p_2\rangle$ be a finite algebra satisfying (HM_3). By Lemma 2.4, $\mathbf{A}$ is almost surely rigid, and by 2.5, the probability that either p_1 or p_2 has a special translation is 0. We need only show that with probability 0, $\mathbf{A}$ has a proper, nontrivial subalgebra.

Let $n = |A|$ and $1 < m < n$. The probability that $\mathbf{A}$ has a m-element subalgebra is

$$\sigma_n(m) = \binom{n}{m}\left(\frac{m}{n}\right)^{2m^3-3m^2+m} \tag{5}$$

To see this, consider a subset $S = \{a_1, \dots, a_m\}$ of A. The operation p_1 will preserve S with probability $\left(\frac{m}{n}\right)^{m^3-m^2}$ since there are m^3 positions in the table that must be mapped back into S, but m^2 of them are predetermined by the condition $p_1(x, x, y) = y$. (This already accounts for the idempotence of p_1.) Now, p_2 will preserve S with probability $\left(\frac{m}{n}\right)^{m^3-2m^2+m}$. Again, there are m^3 entries in the table for p_1 that must be mapped back into S. m^2 of those entries are determined by the condition $p_2(x, y, y) = x$, and another $m(m-1)$ are determined by $p_2(x, x, y) = p_1(x, y, y)$. (In this last tally, we must avoid $x = y$ so we don't double-count.) Thus the probability that S is a subalgebra of $\mathbf{A}$ is $\left(\frac{m}{n}\right)^w$ with $w = (m^3 - m^2) + (m^3 - 2m^2 + m) = (2m^3 - 3m^2 + m)$. Finally, there are $\binom{n}{m}$ choices for S.

Observe that $\sigma_n(2) = \binom{n}{2}\left(\frac{2}{n}\right)^6 = 32n(n-1)/n^6$ which clearly tends to 0 as n tends to infinity. We are left with demonstrating that

$$\lim_{n\to\infty} \sum_{m=3}^{n-1} \sigma_n(m) = 0. \tag{6}$$

We can accomplish this by showing that $\sigma_n(m) \leq \psi_n(m)$ and applying Lemma 2.8. This is an easy verification that we leave to the reader. □

It follows from Theorem 3.1 that almost no algebra is sharply k-permutable for any $k > 2$. To complete our discussion, we determine the probability that a random Maltsev operation is quasisheffer. By a Maltsev operation, we mean one that satisfies (HM_2).

Theorem 3.2. *Let f be a random Maltsev operation on a finite set. Then f is quasisheffer with probability e^{-2}.*

Proof. Let f be a random ternary operation satisfying the identities $f(x, x, y) \approx f(y, x, x) \approx y$ on a finite set. Define $g(x, y) = f(y, x, y)$. The operation g is uniformly distributed over the space of all idempotent binary operations. Since g lies in the clone generated by f, By Theorem 2.13,

$$\mathrm{Prob}(f \in \mathcal{QS}) \geq \mathrm{Prob}(g \in \mathcal{QS}) = e^{-2}.$$

On the other hand, it is easy to see that a 2-element subset is preserved by f if and only if it is preserved by g. Therefore, by Lemma 2.11, the probability that f has no 2-element subalgebra is e^{-2}. Since this is a necessary condition for f to be quasisheffer, the theorem is proved. □

4. Families of quasisheffer operations

In 1936, Webb [11] proved that for any $n > 1$ the binary operation

$$h(x, y) = \big(\min(x, y) + 1\big) \bmod n \tag{7}$$

is a Sheffer operation on $\{0, 1, \dots, n-1\}$. Thus we have an infinite family of Sheffer operations with an elegant and uniform definition. This suggests the question of whether a similar definition exists for idempotent quasisheffer operations. Á. Szendrei discovered such a family.

Theorem 4.1. *Let $n > 2$ and define*

$$g(x, y) = \begin{cases} y + 1 \bmod n & \text{if } x < y \\ x & \text{if } x = y \\ x - 1 \bmod n & \text{if } x > y. \end{cases}$$

Then g is quasisheffer on $\{0, 1, \dots, n-1\}$.

	0	1	2	3
0	0	2	3	0
1	0	1	3	0
2	1	1	2	0
3	2	2	2	3

	0	1	2	3	4
0	0	2	3	4	0
1	0	1	3	4	0
2	1	1	2	4	0
3	2	2	2	3	0
4	3	3	3	3	4

FIGURE 1. The operation g of Theorem 4.1 for $n = 4$ and $n = 5$

For example, the multiplication tables for g in the cases $n = 4$ and $n = 5$ are given in Figure 1.

Proof. We shall apply Theorem 2.1. Suppose that S is a nontrivial subalgebra, say $a, b \in S$ with $a < b$. Since $g(a, b) = b+1$, $g(a, b+1) = b+2, \ldots, g(a, n-2) = n-1$, $g(a, n-1) = 0$, we see that S contains both 0 and $n-1$. But then $g(n-1, 0) = n-2$, $g(n-2, 0) = n-3, \ldots$, so that S is an improper subalgebra.

By Lemma 2.2, if X_a is a cross, then we either have that $g(x, a) = a$ for all x or $g(a, x) = a$ for all x. But according to the definition of g, this is impossible.

Finally, suppose f is an automorphism of the algebra. Among the n^2 entries of the multiplication table for g, there are $n+1$ appearances of 0, 3 appearances of 1, 5 appearances of 2,..., $(2n-3)$ appearances of $n-2$, and $n-1$ appearances of $n-1$. Hence, if n is odd, distinct elements differ in the number of occurrences in the table, so f must be the identity map. If n is even there will be two elements which occur $n-1$ times and two which occur $n+1$ times, while the remaining $n-4$ elements have a pairwise distinct number of appearances. Hence, the number of fixed points of f must be at least $n-4$. But the set of fixed points forms a subalgebra, which will be proper and nontrivial (which we have just shown is impossible), unless $n = 4$. The case $n = 4$ can be checked by direct inspection of the table in Figure 1. □

We have one additional observation on the subject.

Theorem 4.2. *Let h be a binary Sheffer operation on a finite set A of cardinality greater than 2. Define the ternary operation*

$$\hat{h}(x, y, z) = \begin{cases} x & \text{if } x = y = z \\ h(x, y) & \text{otherwise.} \end{cases} \tag{8}$$

Then $\hat{h}$ is an idempotent quasisheffer operation on A.

Proof. We again use Theorem 2.1. Let X be a proper, nontrivial subset of A. Since h is Sheffer, X is not a subalgebra of $\langle A, h\rangle$. Thus there are $a, b \in X$ such that $h(a, b) \notin X$. Since X is nontrivial, there is $c \in X$ with $c \neq a$. Then from (8), $\hat{h}(a, b, c) = h(a, b) \notin X$ proving that X is not a subalgebra of $\langle A, \hat{h}\rangle$.

Now suppose that f is a nonidentity permutation of A. It must be the case that f does not preserve h. Therefore there are $a, b \in A$ such that $f\big(h(a, b)\big) \neq h\big(f(a), f(b)\big)$. Since $|A| > 1$, there is an element $c \in A$ with $c \neq a$. Note that we must have $f(c) \neq f(a)$ since f is a permutation. Then

$$f\big(\hat{h}(a,b,c)\big) = f\big(h(a,b)\big) \neq h\big(f(a),\ f(b)\big) = \hat{h}\big(f(a),\ f(b),\ f(c)\big).$$

Thus $\langle A, \hat{h}\rangle$ is rigid.

Finally, let $a \in A$ and consider X_a. We wish to show that X_a is not invariant under $\hat{h}$. Since h is Sheffer, it has no idempotent elements. Hence $h(a,a) = a' \neq a$. Moreover, h fails to preserve X_a. Thus there are $b, c \in A$ such that $h\big(\,(a,b),\ (c,a)\,\big) = \big(h(a,c),\ h(b,a)\big) \notin X_a$. Equivalently

$$h(a,c) = c' \neq a \text{ and } h(b,a) = b' \neq a. \tag{9}$$

Suppose that there are b, c satisfying (9) with $b \neq a$. Then

$$\hat{h}\big(\,(a,b),(a,a),(b,a)\,\big) = \big(\hat{h}(a,a,b), \hat{h}(b,a,a)\big) = \big(h(a,a), h(b,a)\big) = (a', b') \notin X_a$$

verifying that $\hat{h}$ does not preserve X_a. An analogous argument works if $c \neq a$. Thus we may assume that the only pair b, c satisfying (9) has $b = c = a$. In this case $b' = c' = a' \neq a$ and

$$(\forall x \neq a)\ \ h(a,x) = h(x,a) = a.$$

Since $a' \neq a$ we must have $h(a,a') = h(a',a) = a$. If $h(a',a') \in \{a,a'\}$ then $\{a,a'\}$ forms a 2-element subalgebra of $\langle A, h\rangle$, which is false. Thus we must have $h(a',a') = a'' \notin \{a,a'\}$. Then we compute

$$\hat{h}\big(\,(a,a'),\ (a,a'),\ (a',a)\,\big) = \big(\hat{h}(a,a,a'),\ \hat{h}(a',a',a)\big) = \\ \big(h(a,a),\ h(a',a')\,\big) = (a', a'') \notin X_a.$$

Thus X_a is not preserved by $\hat{h}$. Therefore by Theorem 2.1, $\hat{h}$ is quasisheffer. □

Remark. The author is indebted to Ágnes Szendrei for several helpful suggestions regarding this material.

References

1. Clifford Bergman, *Universal algebra. Fundamentals and selected topics*, Pure and Applied Mathematics (Boca Raton), vol. 301, CRC Press, Boca Raton, FL, 2012. MR 2839398 (2012k:08001)
2. R. Freese, *On the two kinds of probability in algebra*, Alg. Univ. **27** (1990), no. 1, 70–79.
3. J. Hagemann and A. Mitschke, *On n-permutable congruences*, Alg. Univ. **3** (1973), no. 1, 8–12.
4. K. Kearnes and Á. Szendrei, *Cube term blockers without finiteness*, arXiv:1609.02605, September 2016.
5. K. A. Kearnes, *Congruence permutable and congruence* 3*-permutable locally finite varieties*, J. Algebra **156** (1993), no. 1, 36–49. MR 1213783
6. V. L. Murskiĭ, *The existence of a finite basis of identities, and other properties of "almost all" finite algebras*, Problemy Kibernet. (1975), no. 30, 43–56. MR 0401606 (53 #5433)
7. R. Quackenbush, *Random finite groupoids and Murskiĭ's theorem*, unpublished.
8. E. T. Schmidt, *On n-permutable equational classes*, Acta Sci. Math. (Szeged) **33** (1972), 29–30. MR 0302539
9. Á. Szendrei, *Idempotent algebras with restrictions on subalgebras*, Acta. Sci. Math. **51** (1987), 251–268.

10. ______, *A classification of strictly simple algebras with trivial subalgebras*, Demonstratio Math. **24** (1991), no. 1-2, 149–173, Universal algebra, quasigroups and related systems (Jadwisin, 1989). MR 1142886
11. D. L. Webb, *Definition of Post's Generalized Negative and Maximum in Terms of One Binary Operation*, Amer. J. Math. **58** (1936), no. 1, 193–194. MR 1507143

E-mail address: `cbergman@iastate.edu`

DEPARTMENT OF MATHEMATICS, IOWA STATE UNIVERSITY, AMES, IOWA 50011, USA