2-3-2020

# Random Models of Idempotent Linear Maltsev Conditions. I. Idemprimality

Clifford Bergman
*Iowa State University*, cbergman@iastate.edu

Agnes Szendrei
*University of Colorado, Boulder*

# Random Models of Idempotent Linear Maltsev Conditions. I. Idemprimality


## Abstract

We extend a well-known theorem of Murski\v{\i} to the probability space of finite models of a system M of identities of a strong idempotent linear Maltsev condition. We characterize the models of M in a way that can be easily turned into an algorithm for producing random finite models of M, and we prove that under mild restrictions on M, a random finite model of M is almost surely idemprimal. This implies that even if such an M is distinguishable from another idempotent linear Maltsev condition by a finite model A of M, a random search for a finite model A of M with this property will almost surely fail.



## Keywords

Maltsev condition, idemprimal, Murskii

## Disciplines

Discrete Mathematics and Combinatorics | Mathematics

## Comments

This is a post-peer-review, pre-copyedit version of an article published in *Algebra universalis*. The final authenticated version is available online at DOI: 10.1007/s00012-019-0636-y. Posted with permission.

# RANDOM MODELS OF IDEMPOTENT LINEAR MALTSEV CONDITIONS. I. IDEMPRIMALITY

CLIFFORD BERGMAN AND ÁGNES SZENDREI

Abstract. We extend a well-known theorem of Murskiĭ to the probability space of finite models of a system $\mathcal{M}$ of identities of a strong idempotent linear Maltsev condition. We characterize the models of $\mathcal{M}$ in a way that can be easily turned into an algorithm for producing random finite models of $\mathcal{M}$, and we prove that under mild restrictions on $\mathcal{M}$, a random finite model of $\mathcal{M}$ is almost surely idemprimal. This implies that even if such an $\mathcal{M}$ is distinguishable from another idempotent linear Maltsev condition by a finite model $\mathbf{A}$ of $\mathcal{M}$, a random search for a finite model $\mathbf{A}$ of $\mathcal{M}$ with this property will almost surely fail.

## 1. Introduction

This investigation arose from efforts by the first author to construct random finite algebras that generate a variety that is congruence 3-permutable, but not 2-permutable. On the face of it, it ought to be easy to create such varieties. The Hagemann–Mitschke terms provide a recipe for constructing a 3-permutable variety. By choosing the remaining values of those operations randomly, one would expect that the resulting variety would fail to satisfy any stronger identities (such as 2-permutability).

It turns out that this is not the case: a random, finite, 3-permutable algebra almost surely generates a 2-permutable variety. Similar relationships can be sought among other Maltsev conditions. If a random finite algebra has a Maltsev term, will it have (with probability 1) a majority term? Will a random finite algebra lying in a congruence semidistributive variety almost surely generate one that is congruence distributive?

Now we want to make these questions and claims more precise. As we will discuss below, there is a range of possible interpretations. Our aim with the discussion is to

*Date*: January 21, 2019.

2010 *Mathematics Subject Classification.* 08B05, 08A40.

*Key words and phrases.* Maltsev condition, idemprimal, Murskiĭ.

This material is based upon work supported by the National Science Foundation grants no. DMS 1500218 and DMS 1500254. The second author acknowledges the support of the Hungarian National Foundation for Scientific Research (OTKA) grant no. K115518.

clarify and motivate our interpretation. First recall that a strong Maltsev condition is a condition of the form

(1.1) "there exist terms $f_1, \dots, f_m$ which satisfy the identities in $\Sigma$"

where $\mathcal{L} = \{f_1, \dots, f_m\}$ is a finite algebraic language and $\Sigma$ is a finite set of $\mathcal{L}$-identities. We will refer to (1.1) as the Maltsev condition defined by the pair $\mathcal{M} = (\mathcal{L}, \Sigma)$, and will denote it by $\mathcal{C}_\mathcal{M}$. A variety $\mathcal{V}$ satisfies the Maltsev condition $\mathcal{C}_\mathcal{M}$ in (1.1) if and only if there exist terms $f_1, \dots, f_m$ in the language of $\mathcal{V}$ such that for every member $\mathbf{C}$ of $\mathcal{V}$, the $\mathcal{L}$-algebra $(C; f_1^\mathbf{C}, \dots, f_m^\mathbf{C})$ satisfies the identities in $\Sigma$. Similarly, an algebra $\mathbf{A}$ satisfies $\mathcal{C}_\mathcal{M}$ if and only if there exist terms $f_1, \dots, f_m$ in the language of $\mathbf{A}$ such that the $\mathcal{L}$-algebra $(A; f_1^\mathbf{A}, \dots, f_m^\mathbf{A})$ satisfies the identities in $\Sigma$. It is easy to see that $\mathbf{A}$ satisfies $\mathcal{C}_\mathcal{M}$ if and only if the variety generated by $\mathbf{A}$ does.

A number of important properties of a variety are known to be characterized by strong Maltsev conditions, including congruence permutability, arithmeticity, and "having a Taylor term". A rich supply of strong Maltsev conditions arise also in parametrized sequences which define Maltsev conditions characterizing properties of varieties like congruence distributivity and congruence modularity. For further examples, see Section 6. In most cases, the strong Maltsev conditions obtained in this way are both linear and idempotent. Therefore, we will assume throughout this paper that $\mathcal{M}$ is linear and idempotent (see the definitions in Section 2). To avoid some degenerate cases, we will also assume that $\mathcal{M}$ is satisfiable (i.e., satisfiable by some algebra of size $> 1$).

Given a finite set $A$ and a finite algebraic language $\overline{\mathcal{L}}$, a random finite $\overline{\mathcal{L}}$-algebra $\mathbf{A}$ with universe $A$ can be obtained by randomly filling out the tables of all operations $g^\mathbf{A}$ interpreting the symbols $g$ in $\overline{\mathcal{L}}$. This way we get a discrete probability space on the set of all $\overline{\mathcal{L}}$-algebras with universe $A$, where all algebras have the same probability. For an abstract property $P$ of algebras (i.e., for a property that depends only on the isomorphism types of algebras) we define the *probability that a finite $\overline{\mathcal{L}}$-algebra has property $P$* to be the limit, as $n \to \infty$, of the probability that an $n$-element $\overline{\mathcal{L}}$-algebra has property $P$ (see Section 3). This is the approach called *labeled probability* by Freese [6].

Now let's return to the sort of questions alluded to in the opening paragraphs. They have the form

(†) "How likely is it that a random finite algebra which satisfies the Maltsev condition $\mathcal{C}_\mathcal{M}$ will also satisfy [will fail to satisfy] the Maltsev condition $\mathcal{C}_{\mathcal{M}'}$?"

where $\mathcal{M}$ and $\mathcal{M}'$ are two systems of identities which are linear, idempotent, and satisfiable.

Question (†), in its most straightforward interpretation, considers all random finite algebras $\mathbf{A}$ (in a specified finite language $\overline{\mathcal{L}}$) which satisfy $\mathcal{C}_\mathcal{M}$, and asks for the probability, in the sense discussed above, that such an $\mathbf{A}$ satisfies [fails to satisfy] $\mathcal{C}_{\mathcal{M}'}$.

By Murskiĭ's Theorem [19], if $\overline{\mathcal{L}}$ contains a symbol of arity $\geq 2$, then a random finite $\overline{\mathcal{L}}$-algebra is almost surely (i.e., with probability 1) *idemprimal*. Since the defining property of an idemprimal algebra is that its term operations include all idempotent operations on its universe, such an algebra satisfies every satisfiable strong, idempotent, linear Maltsev condition (see Corollary 3.8). Thus, we get that a random finite algebra which satisfies $\mathcal{C}_{\mathcal{M}}$ will satisfy $\mathcal{C}_{\mathcal{M}'}$ with probability 1 [and hence will fail to satisfy $\mathcal{C}_{\mathcal{M}'}$ with probability 0], independently of the choice of $\mathcal{M}$ and $\mathcal{M}'$.

This approach to question (†) is unsatisfying, not because the answer is trivial, but because it is easy to pinpoint the weakness of this approach. If one wants to construct an algebra $\mathbf{A}$ which satisfies a Maltsev condition $\mathcal{C}_{\mathcal{M}}$ and fails to satisfy another, $\mathcal{C}_{\mathcal{M}'}$, then one would arrange the satisfaction of $\mathcal{C}_{\mathcal{M}}$ with as few operations as possible; the more 'unnecessary' operations are added to $\mathbf{A}$, the less likely it is that it will fail to satisfy $\mathcal{C}_{\mathcal{M}'}$. The most 'optimal' satisfaction of $\mathcal{C}_{\mathcal{M}}$ is achieved by requiring that $\mathbf{A}$ satisfies $\mathcal{C}_{\mathcal{M}}$ with its basic operations (and $\mathbf{A}$ has no other basic operations). This is equivalent to requiring that, if $\mathcal{M} = (\mathcal{L}, \Sigma)$, then $\mathbf{A}$ is an $\mathcal{L}$-algebra satisfying the identities in $\Sigma$. Such an algebra will be called a *model of* $\mathcal{M}$.

This motivates us to adopt the following interpretation of the kind of questions alluded to at the beginning of the introduction:

(‡) "How likely is it that a random finite model of $\mathcal{M}$ will satisfy [will fail to satisfy] the Maltsev condition $\mathcal{C}_{\mathcal{M}'}$?"

where $\mathcal{M}$ and $\mathcal{M}'$ are two finite systems of identities which are linear, idempotent, and satisfiable. However, it should be noted that there is a price to pay for considering only random models of $\mathcal{M}$ instead of random algebras satisfying the corresponding Maltsev condition $\mathcal{C}_{\mathcal{M}}$: in Section 6 we will see examples showing there exist different systems $\mathcal{M}_1, \mathcal{M}_2$ that describe equivalent Maltsev conditions, but the random finite models of $\mathcal{M}_1$ and the random finite models of $\mathcal{M}_2$ have essentially different properties, and hence question (‡) might have different answers for $\mathcal{M} = \mathcal{M}_1$ and $\mathcal{M} = \mathcal{M}_2$.

Our main result in this paper, Theorem 5.1, is a characterization of those finite, satisfiable systems $\mathcal{M}$ of idempotent linear identities for which a random finite model is almost surely idemprimal. As shown in Section 6, these include many of the familiar strong Maltsev conditions. For these systems $\mathcal{M}$, question (‡) has the same answer as question (†): A random finite model of $\mathcal{M}$ almost surely satisfies every satisfiable strong, idempotent, linear Maltsev condition $\mathcal{C}_{\mathcal{M}'}$.

To obtain this result, we first study syntactic properties of finite systems $\mathcal{M}$ of idempotent linear identities (Section 2), which we then apply to analyze random finite models of $\mathcal{M}$ (Section 3). We show in Theorem 3.5 how one can construct all finite models of $\mathcal{M}$ by randomly (and independently) filling out well-chosen parts of the operation tables, and then by completing the remaining parts of the tables (which are uniquely determined) so that all required identities are satisfied. This

result is crucial for the counting arguments we need for determining the probability of idemprimality for random models of $\mathcal{M}$. In Section 4 we prove that for every finite, satisfiable systems $\mathcal{M}$ of idempotent linear identities the random models of $\mathcal{M}$ have only small proper subalgebras, where 'small' depends on some parameters of $\mathcal{M}$. Section 5 is devoted to the proof of our main result, and in the final Section 6 we apply our results to some familiar strong idempotent linear Maltsev conditions, and answer the specific questions in the opening paragraphs above.

## 2. Systems of Idempotent Linear Identities

Let $\mathcal{L}$ be an algebraic language with no constant symbols, and let $V := \{v_1, v_2, \dots\}$ be a set of distinct variables indexed by positive integers. We form $\mathcal{L}$-terms using these variables only, but for convenience, we may use other notation like $x, y, z$ or $x_i, y_j, z_k$, etc. for these variables. An $\mathcal{L}$-term is called *linear* if it contains at most one operation symbol. An $\mathcal{L}$-identity or a set of $\mathcal{L}$-identities is called *linear* if all terms involved are linear. If $s$ is an $\mathcal{L}$-term and $X$ is a set of variables that contains all variables occurring in $s$, then for any function $\gamma\colon X \to X$, $s[\gamma]$ will denote the term obtained from $s$ by replacing each variable $x \in X$ with $\gamma(x) \in X$. In the special case in which $X$ is precisely the set of variables occurring in $s$, a term of this form $s[\gamma]$ will be called an *identification minor* of $s$. In particular, $s[\gamma]$ is a *proper identification minor* of $s$ if $\gamma$ is not injective. Thus, the linear $\mathcal{L}$-terms are the variables and all terms of the form $f[\gamma]$ in which $f \in \mathcal{L}$ and $\gamma\colon X \to X$ for some $X \subseteq V$ containing $\{v_1, \dots, v_{\mathrm{arity}(f)}\}$. In this context we also use the symbol $f$ as shorthand for the term $f(v_1, \dots, v_{\mathrm{arity}(f)})$. For any set $X$ of variables, the set of all linear $\mathcal{L}$-terms with variables in $X$ will be denoted by $\mathsf{LT}_X^{\mathcal{L}}$.

As usual, if $\Sigma \cup \{\varphi\}$ is a set of identities in the language $\mathcal{L}$, we write $\Sigma \models \varphi$ to denote that every $\mathcal{L}$-algebra that satisfies all identities in $\Sigma$ also satisfies $\varphi$. We may call two terms, $s$ and $t$, $\Sigma$-*equivalent* if $\Sigma \models s \approx t$. We will say that a set $\Sigma$ of $\mathcal{L}$-identities is *unsatisfiable*, if it has no model of size greater than 1, or equivalently, if $\Sigma \models x \approx y$ for distinct variables $x, y$; otherwise we will say that $\Sigma$ is *satisfiable*. If $\Sigma$ is a set of linear $\mathcal{L}$-identities, we might call the pair $\mathcal{M} = (\mathcal{L}, \Sigma)$ a *linear system*.

If $\Sigma \cup \varphi$ is a set of linear identities, then there is a simple syntactic characterization for the relation $\Sigma \models \varphi$, due to David Kelly [16], which we state in Theorem 2.1 below[1], after introducing some terminology and notation.

Let $\mathcal{M} = (\mathcal{L}, \Sigma)$ be a linear system. For any set $X$ of variables, let

$$\mathsf{E}_X^{\mathcal{M}} := \{(s, t) \in \mathsf{LT}_X^{\mathcal{L}} \times \mathsf{LT}_X^{\mathcal{L}} : \Sigma \models s \approx t\},$$

[1]Kelly's Theorem is slightly more general than Theorem 2.1: it allows constant symbols in $\mathcal{L}$ and in the substitutions $\gamma$. The theorem is a restriction of Birkhoff's completeness theorem for equational logic to the set of so-called 'basic' identities, but it shows that there is a simple algorithm that decides for every set $\Sigma \cup \varphi$ of basic identities whether $\Sigma \models \varphi$.

the restriction of 'Σ-equivalence of terms' to $\mathsf{LT}_X^{\mathcal{L}}$. Clearly, this is an equivalence relation on $\mathsf{LT}_X^{\mathcal{L}}$.

If $X$ is a set of variables that contains all variables occurring in $\Sigma$, we will use $\equiv_X^{\mathcal{M}}$ to denote the least equivalence relation on $\mathsf{LT}_X^{\mathcal{L}}$ satisfying the following conditions:

(i) $\equiv_X^{\mathcal{M}}$ contains $\Sigma$, i.e., $s \equiv_X^{\mathcal{M}} t$ for every identity $s \approx t$ in $\Sigma$, and
(ii) $\equiv_X^{\mathcal{M}}$ is closed under substitutions of variables, i.e., whenever $s \equiv_X^{\mathcal{M}} t$ holds for some $s, t \in \mathsf{LT}_X^{\mathcal{L}}$, we also have $s[\gamma] \equiv_X^{\mathcal{M}} t[\gamma]$ for all functions $\gamma\colon X \to X$.

Thus, the pairs in $\equiv_X^{\mathcal{M}}$ are obtained from the identities in $\Sigma$ by applying the closure conditions induced by reflexivity, symmetry, transitivity, and the condition in (ii). To emphasize that these closure conditions are simple rules of inference for identities, we may write $\Sigma \vdash_X s \approx t$ to indicate that $s \equiv_X^{\mathcal{M}} t$.

Finally, we will say that $X$ is *large enough for* $\Sigma$ (or for $\mathcal{M}$) if

- $|X| \geq 2$ and $X$ contains all variables occurring in $\Sigma$,
- $|X| \geq \mathrm{arity}(f)$ for every $f \in \mathcal{L}$, and
- $|X|$ is at least as large as the number of distinct variables occurring in each identity in $\Sigma$.

**Theorem 2.1** (Kelly [16]; for a published proof, see [13])**.** *Let $X$ be a set of variables, and let $\mathcal{M} = (\mathcal{L}, \Sigma)$ be a linear system in an algebraic language $\mathcal{L}$ without constant symbols.*

(1) *If $X$ is large enough for $\Sigma$, then $\Sigma$ is unsatisfiable if and only if $\Sigma \vdash_X x \approx y$ for distinct variables $x, y \in X$.*
(2) *Assume $\Sigma$ is satisfiable and $s \approx t$ is a linear $\mathcal{L}$-identity. If $X$ is large enough for $\Sigma \cup \{s \approx t\}$, then for any $s, t \in \mathsf{LT}_X^{\mathcal{L}}$ we have that*

$$\Sigma \models s \approx t \qquad \textit{iff} \qquad \Sigma \vdash_X s \approx t.$$

Let $\mathcal{M} = (\mathcal{L}, \Sigma)$ be linear and $X$ large enough for $\mathcal{M}$. The equivalence class of a term $t \in \mathsf{LT}_X^{\mathcal{L}}$ in the equivalence relation $\mathsf{E}_X^{\mathcal{M}}$ (or, equivalently, $\equiv_X^{\mathcal{M}}$) will be denoted by $\mathsf{E}_X^{\mathcal{M}}[t]$. If $X$, $\mathcal{L}$, $\mathcal{M}$ are clear from the context, we may write $\mathsf{LT}$, $\mathsf{E}$, and $\equiv$ for $\mathsf{LT}_X^{\mathcal{L}}$, $\mathsf{E}_X^{\mathcal{M}}$, and $\equiv_X^{\mathcal{M}}$, respectively.

From now on we will focus on the case when $\mathcal{M} = (\mathcal{L}, \Sigma)$ is also *idempotent*, that is, $\Sigma \models f(x, \ldots, x) \approx x$ holds for all operation symbols $f$ in $\mathcal{L}$. Lemmas 2.2–2.3 below establish basic properties of the equivalence relation $\mathsf{E}_X^{\mathcal{M}}$ which will be used later on in the paper.

**Lemma 2.2.** *Assume $\mathcal{M} = (\mathcal{L}, \Sigma)$ is idempotent, linear, and satisfiable, and let $X$ be a large enough set of variables for $\mathcal{M}$. For every equivalence class $C$ of $\mathsf{E} = \mathsf{E}_X^{\mathcal{M}}$ there exists a unique nonempty set $X_C \subseteq X$ such that*

- *$X_C$ is the set of variables of some term in $C$, and*
- *every variable in $X_C$ occurs in all terms in $C$.*

*Moreover, we have that*

- *the terms $t \in C$ are independent, relative to $\Sigma$, of their variables not in $X_C$; i.e., $\Sigma \models t(X_C, \overline{z}) \approx t(X_C, \overline{z}')$ for arbitrary lists of variables $\overline{z}, \overline{z}'$ in $X$.*

*Proof.* Let $C$ be any equivalence class of $\mathsf{E}$, and let $s \in C$ be such that the set $V_s$ of variables occurring in $s$ is minimal (with respect to $\subseteq$) among the members of $C$. For the first claim it suffices to show that all variables in $V_s$ occur in every member of $C$. Suppose not, and let $t \in C$ be a witness to this fact. Thus, the set $V_t$ of variables occurring in $t$ is incomparable to $V_s$. It cannot be that $V_s \cap V_t = \emptyset$, because then $(s,t) \in \mathsf{E}$ — i.e., $\Sigma \models s \approx t$ — would imply $\Sigma \models s(x, \dots, x) \approx t(y, \dots, y)$ for any distinct $x, y \in X$. By idempotence this would yield $\Sigma \models x \approx y$, contradicting our assumption that $\Sigma$ is satisfiable. Thus $V_s \cap V_t \neq \emptyset$. Let $s = s(\overline{x}, \overline{y})$ and $t = t(\overline{x}, \overline{z})$ where $\overline{x} = (x_1, \dots, x_\ell)$ ($\ell \geq 1$) lists the variables in $V_s \cap V_t$, and $\overline{y}$, $\overline{z}$ list the variables in $V_s \setminus V_t$ and $V_t \setminus V_s$ respectively. By the choice of $s$ and $t$, $\overline{y}$ and $\overline{z}$ are both nonempty. Now $(s,t) \in \mathsf{E}$ — or equivalently, $\Sigma \models s(\overline{x}, \overline{y}) \approx t(\overline{x}, \overline{z})$ — implies that $\Sigma \models s(\overline{x}, \overline{y}) \approx t(\overline{x}, x_1, \dots, x_1) \approx s(\overline{x}, x_1, \dots, x_1)$. Thus, $s(\overline{x}, x_1, \dots, x_1) \in C$ and the set of variables occurring in this term, $V_s \cap V_t$, is a proper subset of $V_s$. This contradicts the minimality property of $s$, and hence proves the first claim.

For an arbitrary $t \in C$ the same argument as above shows that $t = t(X_C, \overline{y})$ for some (possibly empty) list $\overline{y}$ of variables which is disjoint from $X_C$, and $\Sigma \models t(X_C, \overline{y}) \approx t(X_C, x_1, \dots, x_1)$ for any $x_1 \in X_C$. Thus,

$$\Sigma \models t(X_C, \overline{z}) \approx t(X_C, x_1, \dots, x_1) \approx t(X_C, \overline{z}')$$

for arbitrary lists of variables $\overline{z}, \overline{z}'$ in $X$, as claimed. □

Under the same assumptions on $\mathcal{M}$ and $X$ as in Lemma 2.2, it is easy to see that the equivalence relation $\mathsf{E} = \mathsf{E}_X^{\mathcal{M}}$ is invariant under all permutations of the variables in $X$; that is, for every permutation $\gamma \in S_X$ and for arbitrary terms $s, t \in \mathsf{LT} = \mathsf{LT}_X^{\mathcal{L}}$, we have

$$(s,t) \in \mathsf{E} \qquad \text{if and only if} \qquad (s[\gamma], t[\gamma]) \in \mathsf{E}.$$

Hence, the symmetric group $S_X$ has an induced action on the set of blocks of $\mathsf{E}$ defined by

$$\gamma \cdot \mathsf{E}[t] = \mathsf{E}[t[\gamma]] \qquad \text{for all } t \in \mathsf{LT} \text{ and } \gamma \in S_X.$$

**Lemma 2.3.** *Assume $\mathcal{M} = (\mathcal{L}, \Sigma)$ is idempotent, linear, and satisfiable, and let $X$ be a large enough set of variables for $\mathcal{M}$. The following statements hold for arbitrary equivalence classes $B$ and $C$ of $\mathsf{E} = \mathsf{E}_X^{\mathcal{M}}$:*

- *If $B$ and $C$ are in the same orbit of $\mathsf{E}$ under the action of $S_X$, say $\gamma \cdot B = C$, then $\gamma$ restricts to a bijection $X_B \to X_C$, and $\gamma' \cdot B = C$ for all $\gamma' \in S_X$ satisfying $\gamma'(x) = \gamma(x)$ for all $x \in X_B$.*
- *In particular, $S_{X_C}$ has a unique subgroup $G_C$ such that for any $\gamma \in S_X$ we have $\gamma \cdot C = C$ if and only if $\gamma(X_C) = X_C$ and $\gamma{\restriction}X_C \in G_C$.*

- *Moreover, for any $t \in C$ whose variables are exactly the variables in $X_C$, and for any permutation $\pi \in S_{X_C}$,*

$$\Sigma \models t \approx t[\pi] \qquad \textit{iff} \qquad (t, t[\pi]) \in \mathsf{E} \qquad \textit{iff} \qquad \pi \in G_C.$$

*Proof.* All three claims are straightforward consequences of Lemma 2.2 and the definition of the action of $S_X$. □

**Definition 2.4.** Let $\mathcal{M} = (\mathcal{L}, \Sigma)$ be idempotent, linear, and satisfiable, and let $X$ be a large enough set of variables for $\mathcal{M}$. For any equivalence class $C$ of $\mathsf{E} = \mathsf{E}^{\mathcal{M}}_X$,

- we will refer to the set $X_C$ (see Lemma 2.2) as *the set of essential variables* of the terms in $C$, and if $t \in C$, we may write $X_t$ in place of $X_C$, and call it *the set of essential variables* of $t$;
- we will refer to the group $G_C$ (see Lemma 2.3) as *the symmetry group* of the terms in $C$, and if $t \in C$, we may write $G_t$ for $G_C$ and call it *the symmetry group* of $t$.

If we want to emphasize the dependence of these notions on $\mathcal{M}$ we may talk about essential variables or symmetry groups of terms *relative to* $\mathcal{M}$.

**Example 2.5.** Let $\mathcal{L}$ consist of a single ternary operation symbol, $f$, and take $\mathcal{M} = (\mathcal{L}, \Sigma)$ where

$$\Sigma = \{f(x, x, y) \approx y,\ f(x, y, z) \approx f(z, y, x)\}.$$

Since $\Sigma \models f(x, x, x) \approx x$, we see that $\mathcal{M}$ is idempotent and linear. It is clear from the definition that the set $X = \{x, y, z\}$ of variables is large enough for $\mathcal{M}$. There are a total of 30 linear terms in $\mathsf{LT} = \mathsf{LT}^{\mathcal{L}}_X$: 27 terms containing $f$, plus the 3 variables. One can easily determine the equivalence relation $\mathsf{E} = \mathsf{E}^{\mathcal{M}}_X$, using Theorem 2.1; it turns out that $\mathsf{E}$ partitions $\mathsf{LT}$ as shown in the first two columns of Table 1. Hence, in particular, it follows that $\mathcal{M}$ is satisfiable.

The action of the symmetric group $S_X$ induces three orbits on the blocks of $\mathsf{E}$: $\{B_1, B_2, B_3\}$, $\{C_1, C_2, C_3, C_4, C_5, C_6\}$, and $\{D_1, D_2, D_3\}$. The symmetry groups of the blocks $B_i$ and $C_i$ are all trivial. The symmetry group of each $D_i$ has order 2. For example, $G_{D_1}$ contains the permutation transposing $x$ and $z$. The last two columns of Table 1 display the sets of essential variables and the symmetry groups of all equivalence classes of $\mathsf{E}$. ◇

Returning to our general discussion, let again $\mathcal{M}$ and $X$ be as in Lemmas 2.2–2.3, and for any positive integer $n$, let $[n]$ denote the set $\{1, \ldots, n\}$. Consider a linear term $r = r(x_1, \ldots, x_k)$ in $\mathsf{LT} = \mathsf{LT}^{\mathcal{L}}_X$ where the variables $x_1, \ldots, x_k \in X$ are distinct. We have $r(x_1, \ldots, x_k) = f(x_{\varphi(1)}, \ldots, x_{\varphi(d)})$ for some $f \in \mathcal{L}$ with $d = \mathrm{arity}(f)$ and some onto function $\varphi\colon [d] \to [k]$. It is easy to see that if $f(y_1, \ldots, y_d) \in \mathsf{LT}$ is another linear term, then under the action of $S_X$ by permuting variables, $f(y_1, \ldots, y_d) \in \mathsf{LT}$ lies in the same orbit as $r$ — that is, $f(y_1, \ldots, y_d) = r[\gamma]$ for some $\gamma \in S_X$ — if

| $C$ | Members | $X_C$ | $G_C\ (\leq S_{X_C})$ |
|---|---|---|---|
| $B_1$ | $x,\ f(x,x,x),\ f(y,y,x),\ f(x,y,y),\ f(z,z,x),\ f(x,z,z)$ | $\{x\}$ | $\{\mathrm{id}\}$ |
| $B_2$ | $y,\ f(y,y,y),\ f(x,x,y),\ f(y,x,x),\ f(z,z,y),\ f(y,z,z)$ | $\{y\}$ | $\{\mathrm{id}\}$ |
| $B_3$ | $z,\ f(z,z,z),\ f(x,x,z),\ f(z,x,x),\ f(y,y,z),\ f(z,y,y)$ | $\{z\}$ | $\{\mathrm{id}\}$ |
| $C_1$ | $f(x,y,x)$ | $\{x,y\}$ | $\{\mathrm{id}\}$ |
| $C_2$ | $f(y,x,y)$ | $\{x,y\}$ | $\{\mathrm{id}\}$ |
| $C_3$ | $f(x,z,x)$ | $\{x,z\}$ | $\{\mathrm{id}\}$ |
| $C_4$ | $f(z,x,z)$ | $\{x,z\}$ | $\{\mathrm{id}\}$ |
| $C_5$ | $f(y,z,y)$ | $\{y,z\}$ | $\{\mathrm{id}\}$ |
| $C_6$ | $f(z,y,z)$ | $\{y,z\}$ | $\{\mathrm{id}\}$ |
| $D_1$ | $f(x,y,z),\ f(z,y,x)$ | $\{x,y,z\}$ | $\langle(x\ z)\rangle$ |
| $D_2$ | $f(y,x,z),\ f(z,x,y)$ | $\{x,y,z\}$ | $\langle(y\ z)\rangle$ |
| $D_3$ | $f(x,z,y),\ f(y,z,x)$ | $\{x,y,z\}$ | $\langle(x\ y)\rangle$ |

TABLE 1. Equivalence classes under $\mathsf{E}$ for Example 2.5

and only if the $d$-tuples of variables $(x_{\varphi(1)},\dots,x_{\varphi(d)})$ and $(y_1,\dots,y_d)$ have the same 'pattern' in the following sense.

**Definition 2.6.** For any set $U$ and $d$-tuple $\overline{u}=(u_1,\dots,u_d)\in U^d$ we define the *pattern of* $\overline{u}$ to be the equivalence relation $\varepsilon(\overline{u}):=\{\,(i,j)\in[d]^2 : u_i=u_j\,\}$ on $[d]$. Two $d$-tuples, $\overline{u},\overline{v}\in U^d$ are said to *have the same pattern* if $\varepsilon(\overline{u})=\varepsilon(\overline{v})$. We might refer to equivalence relations on $[d]$ as *patterns on* $[d]$. Given a pattern $\mu$ on $[d]$, we define

$$U^{(\mu)}=\{\overline{u}\in U^d : \varepsilon(\overline{u})=\mu\}.$$

We shall write $U^{(d)}$ in place of $U^{(\mu)}$ when $\mu$ is the equality relation on $[d]$.

In this terminology, the pattern of the variables $(x_{\varphi(1)},\dots,x_{\varphi(d)})$ of the term $r=f(x_{\varphi(1)},\dots,x_{\varphi(d)})$ is the kernel of the function $\varphi$. Furthermore, if a term, $s\in\mathsf{LT}$, exhibits a pattern $\mu$ in its variables, then for any $\gamma\in S_X$, the term $s[\gamma]$ also has pattern $\mu$. Thus, if a term appears in an equivalence class, $C$, of $\mathsf{E}$, then a similar term, with the same pattern of variables, appears in every block of the orbit of $C$, and in no other orbits.

We now introduce another concept which will be useful in the forthcoming sections, and is related to the equivalence classes of $\mathsf{E}$ and the orbits of the action of $S_X$ on the set of equivalence classes.

**Definition 2.7.** Let $\mathcal{M}=(\mathcal{L},\Sigma)$ be idempotent, linear, and satisfiable, and let $X$ be a large enough set of variables for $\mathcal{M}$. We will say that two terms $s,t\in\mathsf{LT}=\mathsf{LT}_X^{\mathcal{L}}$

are *essentially different for* $\mathcal{M}$ if in the equivalence relation $\mathsf{E} = \mathsf{E}_X^{\mathcal{M}}$, the equivalence classes $\mathsf{E}[s]$ and $\mathsf{E}[t]$ of $s$ and $t$ belong to different orbits of $S_X$.

Equivalently, $s$ and $t$ are essentially different for $\mathcal{M}$ if and only if $\Sigma \not\models s[\gamma] \approx t[\delta]$ for any $\gamma, \delta \in S_X$. Lemma 2.3 implies that, if $s, t \in \mathsf{LT}$ have different numbers of essential variables (relative to $\mathcal{M}$), then $s, t$ are essentially different for $\mathcal{M}$. Furthermore, if $s = s(x_1, \dots, x_d) \in \mathsf{LT}$ and $t = t(x_1, \dots, x_d) \in \mathsf{LT}$ are two linear terms such that $\{x_1, \dots, x_d\}$ is the set of essential variables of both, then they are essentially different for $\mathcal{M}$ if and only if $\Sigma \not\models s(x_1, \dots, x_d) \approx t\big(\pi(x_1), \dots, \pi(x_d)\big)$ for any permutation $\pi$ of $\{x_1, \dots, x_d\}$.

In the remainder of this section we will discuss minimal terms for $\mathcal{M}$, which we now define.

**Definition 2.8.** Let $\mathcal{M} = (\mathcal{L}, \Sigma)$ be idempotent and linear, and let $t = t(x_1, \dots, x_d)$ be a linear $\mathcal{L}$-term (where the variables $x_1, \dots, x_d$ are distinct). We will say that

(1) $t$ is a *trivial term for* $\mathcal{M}$ if $\Sigma \models t \approx z$ for some variable $z$, and
(2) $t$ is a *minimal term for* $\mathcal{M}$ if
   - $\Sigma \not\models t \approx z$ for any variable $z$, but
   - $\Sigma \models t[\gamma] \approx z_\gamma$ for some variable $z_\gamma$, whenever $\gamma\colon \{x_1, \dots, x_d\} \to \{x_1, \dots, x_d\}$ is a non-injective function.

In other words, $t$ is a trivial term for $\mathcal{M}$ iff $t$ is $\Sigma$-equivalent to a variable, while $t$ is a minimal term for $\mathcal{M}$ iff $t$ is non-trivial, but every proper identification minor of $t$ is trivial.

Notice that a minimal term exists for $\mathcal{M}$ only if $\mathcal{M}$ is satisfiable. Moreover, if $t = t(x_1, \dots, x_d)$ is a minimal term for $\mathcal{M}$, then $X_t = \{x_1, \dots, x_d\}$, that is, all variables $x_1, \dots, x_d$ of $t$ are essential.

**Theorem 2.9.** *Assume $\mathcal{M} = (\mathcal{L}, \Sigma)$ is idempotent, linear, and satisfiable. For every $f \in \mathcal{L}$, either the term $f = f(x_1, \dots, x_{\mathrm{arity}(f)})$ (where $x_1, \dots, x_{\mathrm{arity}(f)}$ are distinct variables) is trivial for $\mathcal{M}$, or it has an identification minor that is a minimal term for $\mathcal{M}$. Moreover, every minimal term $t$ of $\mathcal{M}$ satisfies one of the following conditions, up to a permutation of its variables:*

(1) *$t$ is a nontrivial binary term for $\mathcal{M}$, that is, $t = t(x, y)$ such that*
$$\Sigma \not\models t \approx x \quad \text{and} \quad \Sigma \not\models t \approx y.$$
(2) *$t$ is a minority term for $\mathcal{M}$, that is, $t = t(x, y, z)$ with*
$$\Sigma \models t(x, y, y) \approx t(y, x, y) \approx t(y, y, x) \approx x.$$
(3) *$t$ is a $\frac{2}{3}$-minority term for $\mathcal{M}$, that is, $t = t(x, y, z)$ with*
$$\Sigma \models t(x, y, y) \approx t(x, y, x) \approx t(y, y, x) \approx x.$$

(4) *$t$ is a majority term for $\mathcal{M}$, that is, $t = t(x, y, z)$ with*

$$\Sigma \models t(x, y, y) \approx t(y, x, y) \approx t(y, y, x) \approx y.$$

(5) *$t$ is a semiprojection term for $\mathcal{M}$, that is, $t = t(x_1, \dots, x_d)$ $(d \geq 3)$,*

$\Sigma \not\models t(x_1, \dots, x_d) \approx x_1$, *but*

$\Sigma \models t(y_1, \dots, y_d) \approx y_1$ *for any variables $y_1, \dots, y_d$ with $|\{y_1, \dots, y_d\}| < d$.*

*Proof.* Let $f \in \mathcal{L}$ be such that the term $f = f(v_1, \dots, v_{\mathrm{arity}(f)})$ is nontrivial for $\mathcal{M}$. To see that $f$ has an identification minor that is a minimal term for $\mathcal{M}$, let $X$ be a set of variables that is large enough for $\mathcal{M}$ and contains $v_1, \dots, v_{\mathrm{arity}(f)}$, and consider all identification minors $t = f[\gamma] \in \mathsf{LT}$ of the term $f = f(v_1, \dots, v_{\mathrm{arity}(f)})$. These include the term $t = f$, which is nontrivial for $\mathcal{M}$ by assumption, and they also include the terms $t = f(x, \dots, x)$ $(x \in X)$ which are trivial for $\mathcal{M}$, as $\mathcal{M}$ is idempotent. Therefore, among all identification minors of $f$, there exists a term $t$ such that $t$ is nontrivial for $\mathcal{M}$ and $d = |X_t|$ is as small as possible. Clearly, $d > 1$. We may assume without loss of generality that $X_t$ is exactly the set of variables that occur in $t$. Thus, $t = t(x_1, \dots, x_d)$ with $\{x_1, \dots, x_d\} = X_t$. By the choice of $t$, the conditions defining a minimal term for $\mathcal{M}$ hold for $t$.

Now let $t = t(x_1, \dots, x_d)$ be any minimal term for $\mathcal{M}$. Then $\Sigma \not\models t(x_1, \dots, x_d) \approx z$ for any variable $z$, but $\Sigma \models t(y_1, \dots, y_d) \approx y$ for some variable $y$ whenever $|\{y_1, \dots, y_d\}| < d$. Were $y \notin \{y_1, \dots, y_d\}$, we would get (by substituting $z$ for $y$) $\Sigma \models y \approx z$ for distinct variables $y, z$, which contradicts our assumption that $\mathcal{M}$ is satisfiable. Thus $y = y_i$ for some $i$. If $d \leq 3$, then the only possibilities, up to permutations of variables, are those described in (1)–(5). If $d \geq 4$, then by Świerczkowski's Lemma [24], the only possibility, up to permutations of variables, is (5). □

## 3. Random Models

Let $\mathcal{M} = (\mathcal{L}, \Sigma)$ where $\Sigma$ is a finite system of idempotent linear identities in a finite language $\mathcal{L}$. For every finite set $A$, let $\mathrm{Mod}_A(\mathcal{M})$ denote the set of all models of $\mathcal{M}$ on $A$. Clearly, $\mathrm{Mod}_A(\mathcal{M})$ is a finite set. Motivated by our discussion in the introduction, we will stipulate that every member of $\mathrm{Mod}_A(\mathcal{M})$ has the same probability, so we get a discrete probability space on $\mathrm{Mod}_A(\mathcal{M})$ with uniform distribution. Accordingly, for every property $P$ of algebras on $A$, the probability that a random model $\mathbf{A}$ of $\mathcal{M}$ on $A$ has property $P$ is

$$\Pr_A(\mathbf{A} \text{ has property } P) := \frac{|\{\mathbf{A} \in \mathrm{Mod}_A(\mathcal{M}) : \mathbf{A} \text{ has property } P\}|}{|\mathrm{Mod}_A(\mathcal{M})|}. \tag{3.1}$$

Note that we add a subscript $A$ to Pr to indicate the base set of the models we are considering. In contrast, $\mathcal{M}$ is suppressed in the notation, because $\mathcal{M}$ will usually be fixed and clear from the context when we apply the notation $\Pr_A$.

We will call a property $P$ of algebras an *abstract property* (of finite algebras) if for any two isomorphic (finite) algebras $\mathbf{A}$ and $\mathbf{B}$, $\mathbf{A}$ has property $P$ if and only if $\mathbf{B}$ does. It follows that if $A$, $B$ are finite sets of the same cardinality and $P$ is an abstract property, then in the probability spaces of all models of $\mathcal{M}$ on $A$ and $B$, respectively, we have

$$\Pr_A(\mathbf{A} \text{ has property } P) = \Pr_B(\mathbf{B} \text{ has property } P).$$

Therefore, our main concept below is well-defined.

**Definition 3.1.** Let $P$ be an abstract property of finite algebras. We will say that *a random finite model of $\mathcal{M}$ has property $P$ with probability $p$* if

$$p = \lim_{n\to\infty} \Pr_{[n]}(\mathbf{A} \text{ has property } P). \tag{3.2}$$

Clearly, this limit is not affected by disregarding the values of $\Pr_{[n]}(\mathbf{A}$ has property $P)$ on the right hand side for finitely many $n$'s. Therefore, when computing these probabilities, we may, and we often will, restrict to models $\mathbf{A}$ of $\mathcal{M}$ whose universe $[n]$ has large enough cardinality.

If every linear $\mathcal{L}$-term is trivial for $\mathcal{M}$ (i.e., $\Sigma$-equivalent to a variable), then either $\mathcal{M}$ is satisfiable and $\mathcal{M}$ has exactly one model of the form $\mathbf{A} = \langle [n]; \mathcal{L}\rangle$ for every positive integer $n$, or $\mathcal{M}$ is unsatisfiable and $\mathcal{M}$ has exactly one model of the form $\mathbf{A} = \langle [n]; \mathcal{L}\rangle$ for $n = 1$ and none for $n > 1$. Hence, every probability on the right hand side of (3.2) is 0 or 1. This degenerate case is not interesting, and excluding it from our considerations will make our theorems easier to state. Therefore, for the rest of the paper we adopt the following assumption on $\mathcal{M}$:

**Global Assumption 3.2.** We assume that $\mathcal{M} = (\mathcal{L}, \Sigma)$ where

- $\mathcal{L}$ is a finite algebraic language and
- $\Sigma$ is a finite system of idempotent linear $\mathcal{L}$-identities such that
- there exists a nontrivial linear $\mathcal{L}$-term for $\mathcal{M}$.

In this section our goal is to analyze the finite models of $\mathcal{M}$, and show how the operations of each such model can be constructed from a family of independently chosen functions with certain symmetry properties. The significance of this result is twofold: (i) it will provide an algorithm for choosing, with probability $\frac{1}{|\operatorname{Mod}_A(\mathcal{M})|}$, a random model of $\mathcal{M}$ on a fixed finite set $A$; (ii) it will allow us to do counting arguments to find probabilities of the form (3.1).

The intuitive idea for this description of the finite models of $\mathcal{M}$ is quite simple. Every linear $\mathcal{L}$-term $t$ induces a term operation $t^{\mathbf{A}}$ on the universe $A$ of every model $\mathbf{A}$ of $\mathcal{M}$, which can be further restricted to subsets of the domain of $t^{\mathbf{A}}$. It turns out that for a well-chosen family $(t_i)$ of terms, which depends on $\mathcal{M}$, the term operations $t_i^{\mathbf{A}}$ of the models $\mathbf{A}$ of $\mathcal{M}$ restrict to appropriately chosen subsets of their domains as independent functions $h_i$ with certain symmetries. Conversely, any family $(h_i)$ of

independently chosen functions with these symmetry properties (see Definition 3.4) gives rise to a model of $\mathcal{M}$. Unfortunately, nailing down all the details in complete generality is somewhat tedious, therefore we start by illustrating the method with an example.

**Example 3.3.** Let $\mathcal{M} = (\mathcal{L}, \Sigma)$, $X$, and $\mathsf{E}$ be as defined in Example 2.5, and let $A$ be a nonempty set. We want to describe how to construct all models $\mathbf{A} = \langle A; f^{\mathbf{A}} \rangle$ of $\mathcal{M}$, equivalently, how to construct all operations $f^{\mathbf{A}}$ on the set $A$ which obey the identities in $\Sigma$. We will use Table 1, which shows the blocks $B_1, \dots, D_3$ of $\mathsf{E}$, split into orbits $\{B_1, B_2, B_3\}$, $\{C_1, \dots, C_6\}$, and $\{D_1, D_2, D_3\}$ of $S_X$. From this, we can read off all linear identities $r \approx s$ in the variables $x, y, z$ which are consequences of $\Sigma$; namely, $r \approx s$ is such an identity if and only if $r$ and $s$ are in the same block of $\mathsf{E}$ (i.e., appear in the same row of the table). Each one of these identities forces the desired operation $f^{\mathbf{A}}$ to satisfy a condition of the following form:

- "$f^{\mathbf{A}}$ applied to a triple $(a, b, c) \in A^3$ of some pattern has to equal $f^{\mathbf{A}}$ applied to a triple $(a', b', c') \in A^3$ of another pattern", or
- "$f^{\mathbf{A}}$ applied to a triple $(a, b, c) \in A^3$ of some pattern has to equal one of the arguments".

Identities that come from blocks of $\mathsf{E}$ in the same orbit of $S_X$ contain the same information, therefore we will choose and fix a transversal $\mathcal{C}$ for the orbits of $S_X$; say $\mathcal{C} := \{B_1, C_1, D_1\}$. Let us also choose and fix a representative from each of these blocks; say we choose the term $t_{B_1} = t_{B_1}(x) := x$ from $B_1$, $t_{C_1} = t_{C_1}(x, y) := f(x, y, x)$ from $C_1$, and $t_{D_1} = t_{D_1}(x, y, z) := f(x, y, z)$ from $D_1$. Thus, $\{t_{B_1}, t_{C_1}, t_{D_1}\}$ is a maximal family of essentially different linear terms for $\mathcal{M}$. Notice also that $t_{B_1}, t_{C_1}, t_{D_1}$ were chosen so that all of their variables are essential.

First, we want to deduce some necessary conditions for $f^{\mathbf{A}}$ to obey the identities in $\Sigma$. So, suppose $f^{\mathbf{A}}$ obeys the identities in $\Sigma$. Then it also obeys all identities that come from the blocks $B_1, C_1, D_1$. We can use these identities to express $f^{\mathbf{A}}(a, b, c)$, for triples $(a, b, c) \in A^3$ of various patterns, in terms of three functions: $h_{B_1} := t_{B_1}^{\mathbf{A}} = x^{\mathbf{A}}$ (the identity function on $A = A^{(1)}$), $h_{C_1} := t_{C_1}^{\mathbf{A}} \restriction A^{(2)}$, and $h_{D_1} := t_{D_1}^{\mathbf{A}} \restriction A^{(3)}$. Namely, we have

$$f^{\mathbf{A}}(a, b, c) = \begin{cases} h_{B_1}(a) = a & \text{if } a = b = c \text{ or } a \neq b = c, \\ h_{B_1}(c) = c & \text{if } a = b \neq c, \\ h_{C_1}(a, b) & \text{if } a = c \neq b, \\ h_{D_1}(a, b, c) & \text{if } a \neq b \neq c \neq a. \end{cases} \tag{3.3}$$

This show that if $f^{\mathbf{A}}$ obeys the identities in $\Sigma$, then there exist functions $h_{B_1} \colon A \to A$, $h_{C_1} \colon A^{(2)} \to A$, and $h_{D_1} \colon A^{(3)} \to A$ such that (3.3) holds and the functions $h_{B_1}, h_{C_1}, h_{D_1}$ satisfy the following conditions:

(i) $h_{B_1}$ is the identity function on $A = A^{(1)}$, and

(ii) $h_{D_1}$ is invariant under permuting its first and third variables; or equivalently, $h_{D_1}$ is constant on the orbits of $G_{D_1} = \langle (x, z) \rangle$, as $G_{D_1}$ acts on $A^{(3)}$ by permuting coordinates.

The last condition holds, because $f(z, y, x) \in D_1$ implies that the identity $t_{D_1}(x, y, z) = f(x, y, z) \approx f(z, y, x) = t_{D_1}(z, y, x)$ is entailed by $\Sigma$, so $t^{\mathbf{A}}_{D_1}(a, b, c) = t^{\mathbf{A}}_{D_1}(c, b, a)$ for all $(a, b, c) \in A^3$.

Conversely, we will now show that if we are given three functions $h_{B_1} \colon A \to A$, $h_{C_1} \colon A^{(2)} \to A^{(2)}$, and $h_{D_1} \colon A^{(3)} \to A^{(3)}$ satisfying conditions (i)–(ii) above, then the ternary operation $f^{\mathbf{A}}$ defined by (3.3) obeys the identities in $\Sigma$. It is clear from the construction of $f^{\mathbf{A}}$ that it obeys the first identity, $f(x, x, y) \approx y$, in $\Sigma$. For the other identity, $f(x, y, z) \approx f(z, y, z)$, in $\Sigma$ we can check

$$f^{\mathbf{A}}(a, b, c) = f^{\mathbf{A}}(c, b, a) \quad \big((a, b, c) \in A^3\big) \tag{3.4}$$

separately for each possible pattern of $(a, b, c)$. If $(a, b, c) \in A^{(3)}$, then the equality in (3.4) follows from the last line of the definition in (3.3) and property (ii) of $h_{D_1}$. If $a = c$, then the equality in (3.4) is trivial. Finally, if $a = b$ or $b = c$ (including the possibility that $a = b = c$), then the equality in (3.4) follows from the first two lines of the definition in (3.3).

This proves that there is a one-to-one correspondence between the models of $\mathbf{A}$ of $\mathcal{M}$ with universe $A$ and the triples of functions $h_{B_1} \colon A \to A$, $h_{C_1} \colon A^{(2)} \to A$, and $h_{D_1} \colon A^{(3)} \to A$ satisfying conditions (i)–(ii) above. Given such a triple of functions, the operation $f^{\mathbf{A}}$ of $\mathbf{A}$ is obtained by formula (3.3). ◇

Now we give a precise description of the construction of all models for any $\mathcal{M} = (\mathcal{L}, \Sigma)$ satisfying Global Assumption 3.2. As in Example 3.3, we will work with a maximal family of essentially different linear terms for $\mathcal{M}$, where the terms have essential variables only. Throughout this discussion we will use the notation and the facts established in Theorem 2.1, Lemmas 2.2–2.3, and Definition 2.4 without further reference.

Let $X = \{x_1, \dots, x_m\}$ be a large enough set of variables for $\mathcal{M}$ where $x_1, \dots, x_m$ are all distinct, and the subscripts $1, \dots, m$ fix an ordering of these variables. Furthermore, let $\mathcal{C}$ be a transversal for the $S_X$-orbits of equivalence classes of $\mathsf{E} := \mathsf{E}^{\mathcal{M}}_X$ such that for each $C \in \mathcal{C}$, the set of essential variables of the terms in $C$ is $X_C = \{x_1, \dots, x_{m_C}\}$. Clearly, such a transversal exists, and since $\mathcal{M}$ is idempotent, there is a unique $C \in \mathcal{C}$ with $m_C = 1$, namely the $\mathsf{E}$-class containing the term $x_1$. Now choose for every $C \in \mathcal{C}$ a term $t_C = t_C(x_1, \dots, x_{m_C})$ in $C$ so that $t_C$ includes precisely the variables in $X_C$ (i.e., all variables of $t_C$ are essential). Moreover, assume that for the unique $C \in \mathcal{C}$ with $m_C = 1$ we choose $t_C = x_1$.

We wish to argue that every model $\mathbf{A}$ of $\mathcal{M}$ is determined by the following indexed family of functions:

$$(t^{\mathbf{A}}_C \restriction A^{(m_C)} : C \in \mathcal{C}). \tag{3.5}$$

Note that the indexed family (3.5) depends on the choice of $\mathcal{C}$, however, it does not depend on the choice of the terms $t_C(x_1, \dots, x_{m_C}) \in C$, because for any other term $t'_C(x_1, \dots, x_{m_C}) \in C$ (whose variables are all essential) we have that $\Sigma \models t_C(x_1, \dots, x_{m_C}) \approx t'_C(x_1, \dots, x_{m_C})$.

Let $\mathbf{A}$ be a model of $\mathcal{M}$. To show that $\mathbf{A}$ is determined by the family (3.5), let $f \in \mathcal{L}$ be a $d$-ary operation symbol. A complete specification of $f^{\mathbf{A}}$ can be obtained by defining it separately on each set $A^{(\mu)}$ as $\mu$ ranges over all patterns on $[d]$. Let $\mu$ be a pattern and choose any $d$-tuple $(z_1, \dots, z_d)$ of variables in $X$ such that $(z_1, \dots, z_d)$ has pattern $\mu$. The linear term $f(z_1, \dots, z_d)$ lies in some equivalence class of $\mathsf{E}$, and hence it lies in the $S_X$-orbit of exactly one $C \in \mathcal{C}$. Thus, $f\big(\gamma(z_1), \dots, \gamma(z_d)\big) \in C$ for some $\gamma \in S_X$. Since $(z_1, \dots, z_d)$ and $\big(\gamma(z_1), \dots, \gamma(z_d)\big)$ have the same pattern, we may assume without loss of generality that $(z_1, \dots, z_d)$ was chosen so that $f(z_1, \dots, z_d) \in C \in \mathcal{C}$. Thus

$$\Sigma \vDash f(z_1, \dots, z_d) \approx t_C(x_1, \dots, x_{m_C}).$$

Note that by the definition of $X_C$ each of the $x_i$'s must appear in the list $(z_1, \dots, z_d)$. Thus there is a function $\sigma\colon [m_C] \to [d]$ with $x_i = z_{\sigma(i)}$ for all $i \in [m_C]$. Since $\mathbf{A}$ is a model of $\Sigma$, it must be the case that for every $(a_1, \dots, a_d) \in A^{(\mu)}$ we have that $f^{\mathbf{A}}(a_1, \dots, a_d) = t_C^{\mathbf{A}}(a_{\sigma(1)}, \dots, a_{\sigma(m_C)})$.

**Definition 3.4.** For a fixed $\mathcal{C}$ and for any nonempty set $A$, let us call an indexed family $(h_C : C \in \mathcal{C})$ of functions an *$\mathcal{M}$-family on $A$* (suppressing reference to the choice of $\mathcal{C}$, for simplicity) if, for each $C \in \mathcal{C}$

(1) $h_C$ is a function $A^{(m_C)} \to A$;
(2) $h_C$ is invariant under all permutations $\pi \in G_C$ of its variables $x_1, \dots, x_{m_C}$; equivalently, $h_C$ is constant on the orbits of the symmetry group $G_C = G_{t_C}$ of $t_C$ as $G_C$ acts on $A^{(m_C)}$ by permuting coordinates;
(3) if $m_C = 1$ then $h_C(a_1) = a_1$ for all $a_1 \in A^{(1)} = A$.

The discussion preceding Definition 3.4 and the idempotence of $\mathcal{M}$ imply that, if $\mathbf{A}$ is a model of $\mathcal{M}$ then the indexed family $(h_C : C \in \mathcal{C})$ of functions defined by $h_C := t_C^{\mathbf{A}} \restriction A^{(m_C)}$ for every $C \in \mathcal{C}$ is an $\mathcal{M}$-family on $A$. Moreover, the operations of $\mathbf{A}$ can be obtained from this $\mathcal{M}$-family as follows:

(3.6) For every $f \in \mathcal{L}$ with arity $d$, for every pattern $\mu$ on $[d]$, and for every $(a_1, \dots, a_d) \in A^{(\mu)}$ we have

$$f^{\mathbf{A}}(a_1, \dots, a_d) = h_C(a_{\sigma(1)}, \dots, a_{\sigma(m_C)})$$

where $C$ is the unique member of $\mathcal{C}$ such that $f(z_1, \dots, z_d) \in C$ for some tuple $(z_1, \dots, z_d)$ of variables with pattern $\mu$, and $t_C(z_{\sigma(1)}, \dots, z_{\sigma(m_C)})$ is the chosen representative of $C$ with $X_C = \{x_1, \dots, x_{m_C}\}$ and $x_i = z_{\sigma(i)}$ for all $i \in [m_C]$.

To summarize, every model $\mathbf{A}$ of $\mathcal{M}$ is determined by the $\mathcal{M}$-family (3.5) associated to $\mathbf{A}$.

We now consider the converse: every $\mathcal{M}$-family induces an algebraic structure on its underlying set. Moreover, that algebra will be a model of $\mathcal{M}$. This is the content of the following theorem.

**Theorem 3.5.** *Let $X = \{x_1, \dots, x_m\}$ be a set of $m$ distinct variables that is large enough for $\mathcal{M}$, and choose a transversal $\mathcal{C}$ for the $S_X$-orbits of equivalence classes of $\mathsf{E} = \mathsf{E}_X^{\mathcal{M}}$ such that for each $C \in \mathcal{C}$ the set of essential variables is $X_C = \{x_1, \dots, x_{m_C}\}$. Furthermore, for each $C \in \mathcal{C}$, choose a term $t_C = t_C(x_1, \dots, x_{m_C})$ in $C$ with essential variables only. Then the following hold for every nonempty set $A$.*

(1) *The mapping*

$$\mathbf{A} \mapsto (t_C^{\mathbf{A}} \restriction A^{(m_C)} : C \in \mathcal{C}) \tag{3.7}$$

*is a one-to-one correspondence between the models of $\mathcal{M}$ with universe $A$ and the $\mathcal{M}$-families of functions on $A$.*

(2) *For any $\mathcal{M}$-family $(h_C : C \in \mathcal{C})$ on $A$, the member functions $h_C$ with $m_C > 1$ can be chosen independently.*

(3) *If $h_C \colon A^{(m_C)} \to A$ is a member function of an $\mathcal{M}$-family $(h_C : C \in \mathcal{C})$ on $A$ such that $m_C > 1$, then*

   (i) *$h_C$ is a disjoint union*

$$h_C = \bigcup \big( h_C \restriction D^{(m_C)} : D \subseteq A,\ |D| = m_C \big)$$

   *of its restrictions $h_C \restriction D^{(m_C)} \colon D^{(m_C)} \to A$ to the subsets $D^{(m_C)}$ of $A^{(m_C)}$ where $|D| = m_C$;*

   (ii) *these restrictions $h_C \restriction D^{(m_C)}$ can be chosen independently; and*

   (iii) *each such restriction $h_C \restriction D^{(m_C)}$ is constant on the orbits of the symmetry group $G_C = G_{t_C}$ of $t_C$ (as $G_C$ acts on $D^{(m_C)}$ by permuting coordinates), and is otherwise arbitrary.*

*Proof.* We start with the proof of statement (1). In our discussion that led up to the statement of Theorem 3.5 we proved that (3.7) is a one-to-one mapping that assigns an $\mathcal{M}$-family on $A$ to each model of $\mathcal{M}$ with universe $A$. It remains to show that this mapping is onto.

So, let $(h_C : C \in \mathcal{C})$ be an $\mathcal{M}$-family on $A$, and for each $f \in \mathcal{L}$ with arity $d$ define an operation $f^{\mathbf{A}}$ on $A$ as described in (†). Then $f^{\mathbf{A}}$ is defined on the whole set $A^d$, because for every pattern $\mu$ on $[d]$, the required objects $C$, $f(z_1, \dots, z_d)$, $\sigma$, and $t_C(z_{\sigma(1)}, \dots, z_{\sigma(m_C)})$ exist. To see that $f^{\mathbf{A}}$ is well-defined, note that $C$ is uniquely determined by $f$ and the pattern $\mu$ on $[d]$, but there might be multiple choices for $f(z_1, \dots, z_d)$. Therefore we need to show that the definition of $f^{\mathbf{A}} \restriction A^{(\mu)}$ does not depend on the choice of $f(z_1, \dots, z_d)$. To this end, the following claim will be useful.

**Claim 3.6.** *Let $f \in \mathcal{L}$ be an operation symbol with arity $d$, let $\mu$ be a pattern on $[d]$, and let $C$ be the unique member of $\mathcal{C}$ such that $f(z_1, \dots, z_d) \in C$ for some tuple $(z_1, \dots, z_d)$ of variables with pattern $\mu$. Furthermore, let $\sigma$ be a function $[m_C] \to [d]$ such that $x_i = z_{\sigma(i)}$ for all $i \in [m_C]$. If $(w_1, \dots, w_d)$ is another tuple of variables with pattern $\mu$ such that $f(w_1, \dots, w_d) \in C$, and $\tau$ is a function $[m_C] \to [d]$ such that $x_i = w_{\tau(i)}$ for all $i \in [m_C]$, then*

1. *$\{z_{\tau(i)} : i \in [m_C]\} = X_C$,*
2. *the map $\pi \colon X_C \to X_C$ defined by $x_i = z_{\sigma(i)} \mapsto z_{\tau(i)}$ for every $i \in [m_C]$ is a permutation of $X_C$, and*
3. *$\pi \in G_C$; or equivalently,*

$$\Sigma \models t_C(x_1, \dots, x_{m_C}) = t_C(z_{\sigma(1)}, \dots, z_{\sigma(m_C)}) \approx t_C(z_{\tau(1)}, \dots, z_{\tau(m_C)}). \tag{3.8}$$

*Proof of Claim 3.6.* Let $f$, $\mu$, $C$, $(z_1, \dots, z_d)$, $(w_1, \dots, w_d)$, $\sigma$, and $\tau$ satisfy the assumptions of the claim. The terms $f(z_1, \dots, z_d)$, $f(w_1, \dots, w_d)$, and $t_C(x_1, \dots, x_{m_C})$ all belong to $C$, therefore

$$\Sigma \models f(z_1, \dots, z_d) \approx t_C(z_{\sigma(1)}, \dots, z_{\sigma(m_C)}) \quad \text{and} \tag{3.9}$$

$$\Sigma \models f(w_1, \dots, w_d) \approx t_C(w_{\tau(1)}, \dots, w_{\tau(m_C)}). \tag{3.10}$$

Since $(z_1, \dots, z_d)$ and $(w_1, \dots, w_d)$ have the same pattern, the map $\{w_1, \dots, w_d\} \to \{z_1, \dots, z_d\}$ defined by $w_j \mapsto z_j$ for all $j \in [d]$ is a bijection. Hence, by changing variables in the identity in (3.10), we get that

$$\Sigma \models f(z_1, \dots, z_d) \approx t_C(z_{\tau(1)}, \dots, z_{\tau(m_C)}). \tag{3.11}$$

Now (3.9) and (3.11) imply that (3.8) holds, where the equality follows from the fact that $x_i = z_{\sigma(i)}$ for all $i \in [m_C]$. In particular, (3.8) yields that $t_C(z_{\tau(1)}, \dots, z_{\tau(m_C)}) \in C$. Moreover, since $X_C = \{x_1, \dots, x_{m_C}\}$ is the set of essential variables of every term in $C$, we also get that $\{z_{\tau(1)}, \dots, z_{\tau(m_C)}\} = X_C$. Consequently, the map $x_i = z_{\sigma(i)} \mapsto z_{\tau(i)}$ ($i \in [m_C]$) is a permutation of $X_C$. These considerations prove statements (1) and (2) of the claim, and also the displayed line (3.8) in statement (3). The fact that (3.8) is equivalent to $\pi \in G_C$ follows from the last statement in Lemma 2.3. ◇

We return to proving that the operations of $\mathbf{A}$ are well-defined, that is, if $f \in \mathcal{L}$ has arity $d$, $\mu$ is a pattern on $[d]$, and $C$ is the unique member of $\mathcal{C}$ which contains $f(z_1, \dots, z_d)$ for some tuple $(z_1, \dots, z_d)$ of variables with pattern $\mu$, then the definition of $f^{\mathbf{A}}{\restriction}A^{(\mu)}$ by (†) is independent of the choice of the term $f(z_1, \dots, z_d)$ (and the function $\sigma$). So, let $(z_1, \dots, z_d)$ and $(w_1, \dots, w_d)$ be two such tuples of variables, and let $\sigma$ and $\tau$ be the associated functions required in (†). Thus, $f$, $\mu$, $C$, $(z_1, \dots, z_d)$, $(w_1, \dots, w_d)$, $\sigma$, and $\tau$ satisfy the assumptions of Claim 3.6. If we define $f^{\mathbf{A}}{\restriction}A^{(\mu)}$ using the term $f(z_1, \dots, z_d)$, we get that

$$f^{\mathbf{A}}(a_1, \dots, a_d) := h_C(a_{\sigma(1)}, \dots, a_{\sigma(m_C)}) \quad \text{for all } (a_1, \dots, a_d) \in A^{(\mu)}, \tag{3.12}$$

while if we define $f^{\mathbf{A}}{\restriction}A^{(\mu)}$ using the term $f(w_1,\dots,w_d)$, we get that

$$f^{\mathbf{A}}(a_1,\dots,a_d) := h_C(a_{\tau(1)},\dots,a_{\tau(m_C)}) \quad \text{for all } (a_1,\dots,a_d)\in A^{(\mu)}. \tag{3.13}$$

By Claim 3.6, the assignment defined by $x_i = z_{\sigma(i)} \mapsto z_{\tau(i)}$ for all $i\in[m_C]$ defines a permutation $\pi$ of the set $X_C = \{x_1,\dots,x_{m_C}\}$ of variables of $h_C$, and $\pi\in G_C$. Therefore, the tuples $(a_{\sigma(1)},\dots,a_{\sigma(m_C)})$, $(a_{\tau(1)},\dots,a_{\tau(m_C)})\in A^{(m_C)}$ are in the same orbit of $G_C$ (as $G_C$ acts by permuting coordinates). Hence, by condition (2) in the definition of an $\mathcal{M}$-family (Definition 3.4), we get that the right hand sides of the equalities in (3.12) and (3.13) are equal. This finishes the proof that the operations of $\mathbf{A}$ are well-defined.

Next we argue that the $\mathcal{M}$-family (3.5) associated to $\mathbf{A}$ coincides with $(h_C : C\in\mathcal{C})$. Let $C\in\mathcal{C}$. Then $t_C(x_1,\dots,x_{m_C}) = f(x_{\varphi(1)},\dots,x_{\varphi(d)})$ for some $f\in\mathcal{L}$ of arity $d$ and some onto function $\varphi\colon[d]\to[m_C]$. Let $\mu$ denote the kernel of $\varphi$, and let $\sigma\colon[m_C]\to[d]$ be any right inverse of $\varphi$. Hence, $(x_{\varphi(1)},\dots,x_{\varphi(d)})$ is a tuple of variables with pattern $\mu$ such that $f(x_{\varphi(1)},\dots,x_{\varphi(d)})\in C$. Since for every $m_C$-tuple $(a_1,\dots,a_{m_C})\in A^{(m_C)}$ the $d$-tuple $(a_{\varphi(1)},\dots,a_{\varphi(d)})$ also has pattern $\mu$, we get that

$$\begin{aligned} t_C^{\mathbf{A}}(a_1,\dots,a_{m_C}) = f^{\mathbf{A}}(a_{\varphi(1)},\dots,a_{\varphi(d)}) &= h_C(a_{\varphi(\sigma(1))},\dots,a_{\varphi(\sigma(m_C))}) \\ &= h_C(a_1,\dots,a_{m_C}), \end{aligned}$$

where the second equality is a consequence of the definition of $f^{\mathbf{A}}$. This proves the desired equality $t_C^{\mathbf{A}}{\restriction}A^{(m_C)} = h_C$.

It remains to prove that $\mathbf{A}$ is a model of $\mathcal{M}$. We will argue that $\mathbf{A}$ satisfies every linear identity $r\approx s$ (with variables in $X$) such that $\Sigma\models r\approx s$. Let $\overline{\Sigma}$ denote the set of all these identities. Hence, $r\approx s\in\overline{\Sigma}$ iff $(r,s)\in\mathsf{E}$. Let $\overline{\Sigma}_{\mathcal{C}}$ denote the set of all identities $r\approx s\in\overline{\Sigma}$ where $s = t_C(x_1,\dots,x_{m_C})$ for some $C\in\mathcal{C}$. For every positive integer $k\le m\,(=|X|)$, let $\overline{\Sigma}(k)$ denote the set of all identities in $\overline{\Sigma}$ with variables in $\{x_1,\dots,x_k\}$, and let $\overline{\Sigma}_{\mathcal{C}}(k) := \overline{\Sigma}_{\mathcal{C}}\cap\overline{\Sigma}(k)$. Clearly,

$$\begin{aligned} &\overline{\Sigma}(1)\subseteq\overline{\Sigma}(2)\subseteq\cdots\subseteq\overline{\Sigma}(m-1)\subseteq\overline{\Sigma}(m) = \overline{\Sigma} \quad\text{and} \\ &\overline{\Sigma}_{\mathcal{C}}(1)\subseteq\overline{\Sigma}_{\mathcal{C}}(2)\subseteq\cdots\subseteq\overline{\Sigma}_{\mathcal{C}}(m-1)\subseteq\overline{\Sigma}_{\mathcal{C}}(m) = \overline{\Sigma}_{\mathcal{C}}. \end{aligned}$$

**Claim 3.7.** *The following conditions on* $\mathbf{A}$ *are equivalent for every* $k\in[m]$*:*

(a) $\mathbf{A}$ *satisfies all identities in* $\overline{\Sigma}(k)$*;*
(b) $\mathbf{A}$ *satisfies all identities in* $\overline{\Sigma}_{\mathcal{C}}(k)$*.*

*Proof of Claim 3.7.* The implication (a) ⇒ (b) is obvious, since $\overline{\Sigma}_{\mathcal{C}}(k)\subseteq\overline{\Sigma}(k)$.

To prove that (b) ⇒ (a), assume (b) holds, and let $r\approx s\in\overline{\Sigma}(k)$. Then $r$ and $s$ belong to the same $\mathsf{E}$-class, so by renaming variables if necessary (i.e., by replacing $r\approx s$ with $r[\gamma]\approx s[\gamma]$ for some permutation $\gamma\in S_X$) we get an identity $r'\approx s'\in\overline{\Sigma}$ such that $r',s'\in C$ for some $C\in\mathcal{C}$. Clearly, $r\approx s$ holds in $\mathbf{A}$ iff $r'\approx s'$ does. Since $r'$, $s'$, and $t_C = t_C(x_1,\dots,x_{m_C})$ are in the same $\mathsf{E}$-class $C$, the identities $r'\approx t_C$ and

$s' \approx t_C$ both belong to $\overline{\Sigma}_{\mathcal{C}}$. We also have that $x_1, \dots, x_{m_C}$ are essential variables of all terms in $C$, including $r'$ and $s'$, which implies that $m_C \leq k$. Therefore the identities $r' \approx t_C$ and $s' \approx t_C$ both belong to $\overline{\Sigma}_{\mathcal{C}}(k)$, and hence hold in $\mathbf{A}$ by our assumption. It follows that $r' \approx s'$ also holds in $\mathbf{A}$, and therefore so does $r \approx s$. $\diamond$

By Claim 3.7, to show that $\mathbf{A}$ satisfies all identities in $\overline{\Sigma} = \overline{\Sigma}(m)$, it suffices to prove, by induction on $k$, that $\mathbf{A}$ satisfies all identities in $\overline{\Sigma}_{\mathcal{C}}(k)$ for $k = 1, \dots, m$. If $k = 1$ and $r \approx t_C \in \overline{\Sigma}_{\mathcal{C}}(1)$, then $m_C = 1$, $t_C = x_1$, and $r = f(x_1, \dots, x_1)$ for some $f \in \mathcal{L}$ with arity $d$. Hence, for every $a \in A$,

$$t_C^{\mathbf{A}}(a) = a \quad \text{and} \quad r^{\mathbf{A}}(a) = f^{\mathbf{A}}(a, \dots, a) = h_C(a) = a,$$

where the last equality follows from property (3) of $\mathcal{M}$-families (see Definition 3.4). This shows that the identity $r \approx t_C \in \overline{\Sigma}(1)$ holds in $\mathbf{A}$.

Now let $k > 1$, let $r \approx t_C \in \overline{\Sigma}_{\mathcal{C}}(k)$, and assume that $\mathbf{A}$ satisfies every identity in $\overline{\Sigma}_{\mathcal{C}}(k-1)$. Hence, by Claim 3.7, $\mathbf{A}$ satisfies every identity in $\overline{\Sigma}(k-1)$ as well. Our goal is to show that the identity $r \approx t_C$ holds in $\mathbf{A}$. By the induction hypothesis, there is nothing to prove if $r \approx t_C \in \overline{\Sigma}_{\mathcal{C}}(k-1)$, so we will assume that $r \approx t_C \in \overline{\Sigma}_{\mathcal{C}}(k) \setminus \overline{\Sigma}(k-1)$. Then the variables occurring in $r$ are exactly $x_1, \dots, x_k$, and the identity $r \approx t_C$ has the form $r(x_1, \dots, x_k) \approx t_C(x_1, \dots, x_{m_C})$ with $m_C \leq k$. We need to show that for all $(a_1, \dots, a_k) \in A^k$,

$$r^{\mathbf{A}}(a_1, \dots, a_k) = t_C^{\mathbf{A}}(a_1, \dots, a_{m_C}). \tag{3.14}$$

If $(a_1, \dots, a_k) \notin A^{(k)}$, that is, $a_1, \dots, a_k$ are not all distinct, then there exists a function $\psi\colon [k] \to [k]$ such that $\psi$ is not onto and $(a_1, \dots, a_k) = (a_{\psi(1)}, \dots, a_{\psi(k)})$; hence also $(a_1, \dots, a_{m_C}) = (a_{\psi(1)}, \dots, a_{\psi(m_C)})$. The identity

$$r(x_{\psi(1)}, \dots, x_{\psi(k)}) \approx t_C(x_{\psi(1)}, \dots, x_{\psi(m_C)}) \tag{3.15}$$

is obtained from $r \approx t_C \in \overline{\Sigma}$ by variable substitution, so is also lies in $\overline{\Sigma}$. Furthermore, (3.15) contains at most $|\psi([k])| \leq k-1$ variables, therefore it differs from an identity in $\overline{\Sigma}(k-1)$ by renaming variables only. Hence the induction hypothesis forces (3.15) to hold in $\mathbf{A}$. Using this fact in the second equality below we conclude that

$$r^{\mathbf{A}}(a_1, \dots, a_k) = r^{\mathbf{A}}(a_{\psi(1)}, \dots, a_{\psi(k)}) = t_C^{\mathbf{A}}(a_{\psi(1)}, \dots, a_{\psi(m_C)}) = t_C^{\mathbf{A}}(a_1, \dots, a_{m_C}).$$

This proves (3.14) in the case $(a_1, \dots, a_k) \notin A^{(k)}$.

Now let $(a_1, \dots, a_k) \in A^{(k)}$. The term $r = r(x_1, \dots, x_k)$ has the form $r = f(x_{\varphi(1)}, \dots, x_{\varphi(d)})$ for some $f \in \mathcal{L}$ with arity $d$ and some onto function $\varphi\colon [d] \to [k]$. Recall that since $r \approx t_C \in \overline{\Sigma}$, we have that $f(x_{\varphi(1)}, \dots, x_{\varphi(d)}) = r \in C$. Let $\mu$ denote the kernel of $\varphi$, and let $\sigma\colon [k] \to [d]$ be any right inverse of $\varphi$. Hence, $(x_{\varphi(1)}, \dots, x_{\varphi(d)})$ is a tuple of variables with pattern $\mu$ such that $f(x_{\varphi(1)}, \dots, x_{\varphi(d)}) \in C$. Since for the $k$-tuple $(a_1, \dots, a_k) \in A^{(k)}$ the $d$-tuple $(a_{\varphi(1)}, \dots, a_{\varphi(d)})$ also has pattern $\mu$, we get

that

$$r^{\mathbf{A}}(a_1,\dots,a_k) = f^{\mathbf{A}}(a_{\varphi(1)},\dots,a_{\varphi(d)}) = h_C(a_{\varphi(\sigma(1))},\dots,a_{\varphi(\sigma(m_C))}) \\ = h_C(a_1,\dots,a_{m_C}),$$

where the second equality is a consequence of the definition of $f^{\mathbf{A}}$. We also have

$$t_C^{\mathbf{A}}(a_1,\dots,a_{m_C}) = h_C(a_1,\dots,a_{m_C}),$$

because we established earlier in this proof that $h_C = t_C^{\mathbf{A}}{\restriction}A^{(m_C)}$. Thus, (3.14) holds for tuples $(a_1,\dots,a_k) \in A^{(k)}$ as well, which finishes the proof that $r \approx t_C \in \overline{\Sigma}(k)$ holds in $\mathbf{A}$. The proof of statement (1) is now complete.

Statements (2)–(3) follow immediately from the definition of an $\mathcal{M}$-family (see Definition 3.4) and from the fact that for each $C \in \mathcal{C}$ the subsets $D^{(m_C)}$ of $A^{(m_C)}$ for different $m_C$-element subsets $D$ of $A$ are disjoint. □

**Corollary 3.8.** *$\mathcal{M}$ has models with universe $A$ for every nonempty set $A$.*

*Proof.* This follows from statement (1) in Theorem 3.5, because $\mathcal{M}$-families exist on every nonempty set. □

## 4. Subalgebras of Random Models

As in the preceding sections, we will assume that $\mathcal{M} = (\mathcal{L}, \Sigma)$ satisfies our Global Assumption 3.2. Our aim is to prove that, with probability 1, a random finite model of $\mathcal{M}$ has only 'small' proper subalgebras, where the meaning of 'small' depends on some parameters of $\mathcal{M}$. To define these parameters we will use a maximal family of essentially different linear terms for $\mathcal{M}$ where every term has essential variables only — just as we did in the preceding section. However, we will adopt a different notation, which will be more convenient for our purposes here.

**Definition 4.1.** Let $x_1,\dots,x_m$ be distinct variables such that $X = \{x_1,\dots,x_m\}$ is large enough for $\mathcal{M}$, and let $\{t_i : 0 \le i \le r\} \subseteq \mathsf{LT}_X^{\mathcal{L}}$ be a maximal family of essentially different linear terms for $\mathcal{M}$; that is, for $\mathsf{E} = \mathsf{E}_X^{\mathcal{M}}$, the equivalence classes $\mathsf{E}[t_i]$ $(0 \le i \le r)$ of the terms form a transversal for the orbits of $S_X$ on the set of all equivalence classes of $\mathsf{E}$. Furthermore, assume that $t_0 = x_1$, and for $i \in [r]$, we have $t_i = t_i(x_1,\dots,x_{d_i})$ where all variables $x_1,\dots,x_{d_i}$ are essential, and

$$d_{\mathcal{M}} := d_1 = d_2 = \cdots = d_\ell < d_{l+1} \le \cdots \le d_r \ (\ell \in [r]).$$

For arbitrary integer $k \ge d_{\mathcal{M}}$ let

$$p_{\mathcal{M}}(k) := \sum_{i=1}^{r} q_i \binom{k}{d_i},$$

where $q_i$ $(i \in [r])$ is the index of the symmetry group $G_{t_i}$ of $t_i$ in the symmetric group $S_{\{x_1,\dots,x_{d_i}\}}$, and $\binom{k}{d_i} = 0$ if $k < d_i$.

It is easy to see that in Definition 4.1 we have $d_{\mathcal{M}} \geq 2$, and $d_{\mathcal{M}}$ is the minimum of the arities of minimal terms for $\mathcal{M}$. Moreover, it follows from the choice of the terms $t_1, t_2, \ldots, t_r$ that the sequence $d_1 \leq d_2 \leq \cdots \leq d_r$ of their arities, the set of all pairs $(d_i, q_i)$ $(i \in [r])$, and hence the parameters $p_{\mathcal{M}}(k)$ $(k \geq d_{\mathcal{M}})$ depend on $\mathcal{M}$ only, they are independent of the choice of the terms $t_1, t_2, \ldots, t_r$.

Recall from Theorem 3.5 that to every model $\mathbf{A}$ of $\mathcal{M}$ there is an *associated $\mathcal{M}$-family* $(h_i : 0 \leq i \leq r)$ which consists of the functions $h_i = t_i^{\mathbf{A}} \restriction A^{(d_i)}$ $(0 \leq i \leq r)$. The models $\mathbf{A}$ of $\mathcal{M}$ on a fixed set $A$ can be reconstructed from the associated $\mathcal{M}$-families $(h_i : 0 \leq i \leq r)$; moreover, $h_0$ is the identity function $A \to A$ and the functions $h_1, \ldots, h_r$ can be chosen independently so that the following conditions hold for each $i \in [r]$:

(4.1) ◇ $h_i$ is a disjoint union of its restrictions $h_i \restriction D^{(d_i)} \colon D^{(d_i)} \to A$ with $|D| = d_i$,
◇ these restrictions can be chosen independently, and
◇ each such restriction $h_i \restriction D^{(d_i)}$ is constant on the $q_i$ orbits of the symmetry group $G_{t_i}$ of $t_i$ (as $G_{t_i}$ acts on $D^{(d_i)}$ by permuting coordinates), but is otherwise arbitrary.

The significance of the parameters $p_{\mathcal{M}}(k)$ $(k \geq d_{\mathcal{M}})$ is explained by the following lemma.

**Lemma 4.2.** *Let $A$ be a set, and $B$ a $k$-element subset of $A$ such that $k \geq d_{\mathcal{M}}$.*

(1) *The following conditions are equivalent:*
   (a) *$B$ is (the universe of) a subalgebra of $\mathbf{A}$;*
   (b) *the $\mathcal{M}$-family $(h_i : 0 \leq i \leq r)$ associated to $\mathbf{A}$ has the property that*

$$h_i(B^{(d_i)}) \subseteq B \text{ for every } i \in [r]. \tag{4.2}$$

(2) *If $|A| = n$, then in the probability space of random models $\mathbf{A}$ of $\mathcal{M}$ on $A$,*

$$\Pr_A\big(B \text{ is a subalgebra of } \mathbf{A}\big) = \left(\frac{k}{n}\right)^{p_{\mathcal{M}}(k)}.$$

*Proof.* We will use the notation of Definition 4.1. Let $\mathbf{A} = \langle A; \mathcal{L} \rangle$ be a random model of $\mathcal{M}$, and let $(h_i : 0 \leq i \leq r)$ be the associated $\mathcal{M}$-family. We will use Theorem 3.5 in the form as it is restated in (4.1) and the paragraph preceding it. This theorem, combined with the description in (3.6) of how the operations of $\mathbf{A}$ are constructed from the associated $\mathcal{M}$-family, immediately imply that $B$ is a subalgebra of $\mathbf{A}$ if and only if the requirement in condition (4.2) holds for all $i$, $0 \leq i \leq r$. Since $h_0$ is the identity function $A \to A$, it automatically satisfies this requirement, so there is no need for including the case $i = 0$ in (4.2). This proves statement (1).

To prove statement (2), we work in the probability space of all models of $\mathcal{M}$ on $A$ where $|A| = n$. Combining statement (1) above with the fact that the functions $h_i$

$(i \in [r])$ are independent, we get that

$$\Pr_A(B \text{ is a subalgebra}) = \Pr_A\big(h_i(B^{(d_i)}) \subseteq B \text{ for all } i \in [r]\big) = \prod_{i=1}^{r} \Pr_A\big(h_i(B^{(d_i)}) \subseteq B\big).$$

Now, let us fix $i \in [r]$. By (4.1), the restrictions $h_i{\restriction}D^{(d_i)}$ of $h_i$ to the different $d_i$-element subsets $D$ of $A$ are independent. Since $B^{(d_i)}$ is the union of all sets $D^{(d_i)}$ with $D \subseteq B$, $|D| = d_i$, the condition $h_i(B^{(d_i)}) \subseteq B$ holds for $h_i$ if and only if $h_i(D^{(d_i)}) \subseteq B$ for all $D \subseteq B$ with $|D| = d_i$. Thus,

$$\Pr_A\big(h_i(B^{(d_i)}) \subseteq B\big) = \prod_{\substack{D \subseteq B \\ |D| = d_i}} \Pr_A\big(h_i(D^{(d_i)}) \subseteq B\big).$$

Let $D \subseteq B$ with $|D| = d_i$. Again by (4.1), the restriction $h_i{\restriction}D^{(d_i)}$ of $h_i$ to $D$ is constant on the $q_i$ orbits of the action of $G_{t_i}$ on the set $D^{(d_i)}$, and is otherwise arbitrary. Consequently, $h_i{\restriction}D^{(d_i)}$ is determined by $q_i$ free and independent choices of function values — one for each orbit of $G_{t_i}$ on $D^{(d_i)}$. Thus,

$$\Pr_A\big(h_i(D^{(d_i)}) \subseteq B\big) = \left(\frac{k}{n}\right)^{q_i}.$$

By combining the results in the last three displayed lines we obtain that

$$\Pr_A(B \text{ is a subalgebra}) = \prod_{i=1}^{r} \prod_{\substack{D \subseteq B \\ |D| = d_i}} \Pr_A\big(h_i(D^{(d_i)}) \subseteq B\big) = \prod_{i=1}^{r} \left(\frac{k}{n}\right)^{q_i \binom{k}{d_i}} = \left(\frac{k}{n}\right)^{p_{\mathcal{M}}(k)}$$

as claimed. □

The following easy consequences of Lemma 4.2(2) will be useful.

**Corollary 4.3.** *Let $A$ be an $n$-element set with $n > d_{\mathcal{M}}$. The following hold in the probability space of all models $\mathbf{A}$ of $\mathcal{M}$ on $A$.*

(1) *For every integer $k$ such that $d_{\mathcal{M}} \leq k < n$,*

$$\Pr_A\big(\mathbf{A} \text{ has a } k\text{-element subalgebra}\big) \leq \binom{n}{k} \left(\frac{k}{n}\right)^{p_{\mathcal{M}}(k)}. \tag{4.3}$$

(2) *For every integer $u \geq d_{\mathcal{M}}$,*

$$\Pr_A\big(\mathbf{A} \text{ has a proper subalgebra of size} \geq u\big) \leq \sum_{k=u}^{n-1} \binom{n}{k} \left(\frac{k}{n}\right)^{p_{\mathcal{M}}(k)}. \tag{4.4}$$

Our next lemma is an analog of a result Murskiĭ used in [19, pp. 50–51] (see [3, Lemma 6.22]). We postpone the proof to the Appendix.

**Lemma 4.4.**

$$\lim_{n\to\infty} \sum_{k=4}^{n-1} \binom{n}{k} \left(\frac{k}{n}\right)^{\binom{k}{2}} = 0. \tag{4.5}$$

Now we are ready to state and prove the main theorem of this section on the sizes of proper subalgebras of random finite models of $\mathcal{M}$.

**Theorem 4.5.** *Let* $\mathbf{A}$ *be a random finite model of* $\mathcal{M}$*.*

(1) *Every subset of* $A$ *of size less than* $d_{\mathcal{M}}$ *is (the universe of) a subalgebra of* $\mathbf{A}$*.*
(2) *The probability that* $\mathbf{A}$ *has a proper subalgebra of size* $d = d_{\mathcal{M}}$ *is*

$$\begin{cases} 1 & \text{if } p_{\mathcal{M}}(d) < d, \\ 1 - e^{-d^d/d!} & \text{if } p_{\mathcal{M}}(d) = d, \text{ and} \\ 0 & \text{if } p_{\mathcal{M}}(d) > d. \end{cases}$$

(3) *The probability that* $\mathbf{A}$ *has a* $(d_{\mathcal{M}}+1)$*-element proper subalgebra is* 0 *if* $p_{\mathcal{M}}(d_{\mathcal{M}}+1) > d_{\mathcal{M}}+1$*, i.e., if one of the following conditions holds:*
   - $p_{\mathcal{M}}(d_{\mathcal{M}}) > 1$*, or*
   - *there exists a linear term for* $\mathcal{M}$ *with exactly* $d_{\mathcal{M}}+1$ *essential variables.*

(4) *The probability that* $\mathbf{A}$ *has a proper subalgebra of size* $\geq d_{\mathcal{M}}+2$ *is* 0*.*

Table 2 summarizes most results of this theorem. The four rows correspond to parts (1)–(4) of the theorem, and show the probability for a random finite model of $\mathcal{M}$ to have a proper subalgebra of a specific size $k = 2, \ldots, d_{\mathcal{M}} - 1$, or $k = d_{\mathcal{M}}$, or $k = d_{\mathcal{M}} + 1$, or of any size $k > d_{\mathcal{M}} + 1$, respectively, as a function of the parameter $p_{\mathcal{M}}(d_{\mathcal{M}})$ of $\mathcal{M}$. (In the table $1^*$ indicates that an event is certain.)

As indicated by the "?" in Table 2, the analysis in Theorem 4.5 is incomplete: we have been unable to establish a useful bound on the probability that a random finite model of $\mathcal{M}$ has a $(d_{\mathcal{M}}+1)$-element subalgebra, provided the following two conditions hold for $\mathcal{M}$:

(a) $p_{\mathcal{M}}(d_{\mathcal{M}}) = 1$.
   Equivalently: there exists a unique $d_{\mathcal{M}}$-ary minimal term $t$ for $\mathcal{M}$ and $t$ is totally symmetric (i.e., $t$ is invariant, modulo $\mathcal{M}$, under all permutations of its $d_{\mathcal{M}}$ variables), and hence by Theorem 2.9, $d_{\mathcal{M}} \in \{2, 3\}$ and $t$ is an essentially binary term or a minority term or a majority term for $\mathcal{M}$.
(b) There is no linear term for $\mathcal{M}$ with exactly $d_{\mathcal{M}}+1$ essential variables.

We leave this unsettled case as an open problem.

**Problem 4.6.** Let $\mathcal{M}$ satisfy our Global Assumption 3.2. If conditions (a)–(b) in the preceding paragraph hold for $\mathcal{M}$, what is the probability that a random finite model of $\mathcal{M}$ has a proper subalgebra of size $d_{\mathcal{M}}+1$?

| $p_{\mathcal{M}}(d_{\mathcal{M}})$<br>subalg size | $=1$ | $=2,\dots,d_{\mathcal{M}}-1$ | $=d_{\mathcal{M}}$ | $=d_{\mathcal{M}}+1, d_{\mathcal{M}}+2,\dots$ |
|---|---|---|---|---|
| $=2,\dots,d_{\mathcal{M}}-1$ | $1^*$ | $1^*$ | $1^*$ | $1^*$ |
| $=d_{\mathcal{M}}=d$ | 1 | 1 | $1-e^{-d^d/d!}$ | 0 |
| $=d_{\mathcal{M}}+1$ | ? | 0 | 0 | 0 |
| $>d_{\mathcal{M}}+1$ | 0 | 0 | 0 | 0 |

TABLE 2. Probability of the existence of subalgebras of various sizes, as a function of $p_{\mathcal{M}}(d_{\mathcal{M}})$

The zeros in the lower half of Table 2 witness that with probability 1, random finite models of $\mathcal{M}$ have only 'small' proper subalgebras. We restate some of the results of Theorem 4.5 to emphasize this conclusion.

**Corollary 4.7.** *If* $\mathbf{A}$ *is a random finite model of* $\mathcal{M}$*, then with probability* 1*,*

- $\mathbf{A}$ *has no proper subalgebras of any size* $\geq d_{\mathcal{M}}+2$*;*
- $\mathbf{A}$ *has no proper subalgebras of any size* $\geq d_{\mathcal{M}}+1$ *if either* $p_{\mathcal{M}}(d_{\mathcal{M}})>1$ *or there exists a linear term for* $\mathcal{M}$ *with exactly* $d_{\mathcal{M}}+1$ *essential variables; and*
- $\mathbf{A}$ *has no proper subalgebras of any size* $\geq d_{\mathcal{M}}$ *if* $p_{\mathcal{M}}(d_{\mathcal{M}})>d_{\mathcal{M}}$*.*

Now we prove Theorem 4.5.

*Proof of Theorem 4.5.* We will use the notation of Definition 4.1, but for simplicity, we will write $d$ for $d_{\mathcal{M}}$ and $p(k)$ for $p_{\mathcal{M}}(k)$ throughout the proof. Let $\mathbf{A}$ be a random finite model of $\mathcal{M}$, and let $(h_i : 0 \leq i \leq r)$ be the associated $\mathcal{M}$-family. Statement (1) of the theorem is clearly true, because every linear term for $\mathcal{M}$ with less that $d$ variables is trivial (i.e., $\Sigma$-equivalent to a variable). For statements (2)–(4) we will assume without loss of generality that $|A| = n > d+2$.

To prove statement (2), we first work in the probability space of all models $\mathbf{A}$ of $\mathcal{M}$ on a fixed set $A$. Let $B$ be a $d$-element subset of $A$. We see from Lemma 4.2(2) that the probability that $B$ is *not* a subalgebra of $\mathbf{A}$ is $1-(\frac{d}{n})^{p(d)}$. Since for different $d$-element subsets $B$ and $C$ of $A$ the sets $B^{(d_i)}$ and $C^{(d_i)}$ are disjoint for all $i \in [r]$ (moreover, $B^{(d_i)} = C^{(d_i)} = \emptyset$ whenever $d_i > d$), we see that condition (4.2) and its version with $C$ replacing $B$ are independent for any two different $d$-element subsets $B$ and $C$ of $A$. Hence, it follows from Lemma 4.2(1) that the events "$B$ is a subalgebra of $\mathbf{A}$" and "$C$ is a subalgebra of $\mathbf{A}$" are also independent for any two different $d$-element subsets $B$ and $C$ of $A$. Consequently,

$$\Pr_A\big(\text{no } d\text{-element subset of } A \text{ is a subalgebra of } \mathbf{A}\big) = \left(1-\left(\frac{d}{n}\right)^{p(d)}\right)^{\binom{n}{d}}.$$

This implies that for a random finite model $\mathbf{A}$ of $\mathcal{M}$, the probability that no $d$-element subset of $A$ is a subalgebra of $\mathbf{A}$ is

$$\lim_{n\to\infty}\left(1-\left(\frac{d}{n}\right)^{p(d)}\right)^{\binom{n}{d}} = \lim_{n\to\infty}\left((1-x_n)^{x_n^{-1}}\right)^{y_n}$$

where $x_n := \left(\frac{d}{n}\right)^{p(d)}$ and $y_n := \left(\frac{d}{n}\right)^{p(d)}\binom{n}{d}$. Since

$$\lim_{n\to\infty} x_n = 0, \quad \lim_{n\to\infty}(1-x_n)^{x_n^{-1}} = e^{-1}, \quad \text{and} \quad \lim_{n\to\infty} y_n = \begin{cases} \infty & \text{if } p(d) < d, \\ d^d/d! & \text{if } p(d) = d, \\ 0 & \text{if } p(d) > d, \end{cases}$$

we obtain that the probability that $\mathbf{A}$ has *no* $d$-element subalgebra is 0, $e^{-d^d/d!}$, or 1, according to whether $p(d) < d$, $p(d) = d$, or $p(d) > d$. Hence the probability that $\mathbf{A}$ *has* a $d$-element subalgebra is as claimed in (2).

In statement (3),

$$\begin{aligned} p(d+1) &= \sum_{i=1}^{\ell} q_i \binom{d+1}{d} + \sum_{i=\ell+1}^{r} q_i \binom{d+1}{d_i} \\ &= \left(\sum_{i=1}^{\ell} q_i\right)(d+1) + \sum_{\substack{i \text{ with} \\ d_i = d+1}} q_i = p_{\mathcal{M}}(d)(d+1) + \sum_{\substack{i \text{ with} \\ d_i = d+1}} q_i. \end{aligned}$$

Since $p(d) \geq 1$, we have $p(d+1) \geq d+1$; moreover, $p(d+1) > d+1$ holds if and only if $p(d) > 1$ or $d_i = d+1$ for some $i \in [r]$. This proves the correctness of the characterization of the condition $p(d+1) > d+1$.

To verify the main statement of (3) on the probability of the existence of $(d+1)$-element subalgebras, recall from Corollary 4.3(1) that for models $\mathbf{A}$ of $\mathcal{M}$ on a fixed $n$-element set with $n > d+2$, the probability that $\mathbf{A}$ has a $(d+1)$-element proper subalgebra is bounded above by the quantity on the right hand side of (4.3) for $k = d+1$. Therefore statement (3) will follow if we prove the following claim.

**Claim 4.8.** *If $p(k) > k$, then $\lim_{n\to\infty}\binom{n}{k}\left(\frac{k}{n}\right)^{p(k)} = 0$.*

*Proof of Claim 4.8.*

$$\binom{n}{k}\left(\frac{k}{n}\right)^{p(k)} \leq \binom{n}{k}\left(\frac{k}{n}\right)^{k+1} = \frac{k^{k+1}}{k!}\cdot\frac{n(n-1)\dots(n-k+1)}{n^k}\cdot\frac{1}{n} \leq \frac{k^{k+1}}{k!}\cdot\frac{1}{n},$$

and for a fixed $k$, $\frac{k^{k+1}}{k!}\cdot\frac{1}{n} \to 0$ as $n \to \infty$. ◇

Finally, for the proof of statement (4), let $u = d+2$. By Corollary 4.3(2), for models $\mathbf{A}$ of $\mathcal{M}$ on a fixed $n$-element set with $n > d+2$, the probability that $\mathbf{A}$ has a subalgebra of size at least $u$ is bounded above by the sum on the right hand side

of (4.4). Therefore it suffices to show that this sum tends to 0 as $n \to \infty$, as stated in the following claim.

**Claim 4.9.** *For $u = d + 2$ we have that $\lim_{n\to\infty} \sum_{k=u}^{n-1} \binom{n}{k} \left(\frac{k}{n}\right)^{p(k)} = 0$.*

*Proof of Claim 4.9.* Notice that $u \geq 4$, because $d \geq 2$. Furthermore, for all $k \geq u = d + 2$ we have that

$$p(k) \geq q_1 \binom{k}{d_1} \geq \binom{k}{d_1} = \binom{k}{d} \geq \binom{k}{2},$$

because $d \geq 2$ and $k - d \geq u - d = 2$. Therefore,

$$\sum_{k=u}^{n-1} \binom{n}{k} \left(\frac{k}{n}\right)^{p(k)} \leq \sum_{k=u}^{n-1} \binom{n}{k} \left(\frac{k}{n}\right)^{\binom{k}{2}},$$

where the right hand side tends to 0 as $n \to \infty$, by Lemma 4.4. ◇

The proof of Theorem 4.5 is complete. □

## 5. Criterion for Random Models to be Almost Surely Idemprimal

As before, we will assume that $\mathcal{M}$ satisfies our Global Assumption 3.2. Our aim in this section is to show that under fairly mild additional assumptions on $\mathcal{M}$, random models of $\mathcal{M}$ are, with probability 1, idemprimal. Recall that an algebra $\mathbf{A}$ is called *idemprimal* if every idempotent operation on its universe is a term operation of $\mathbf{A}$. In particular, if $\mathbf{A} = (A; \mathcal{L})$ is a model of $\mathcal{M}$, and hence is idempotent, it will be idemprimal if and only if the term operations of $\mathbf{A}$ are exactly the idempotent operations on $A$.

Our main result is the following theorem.

**Theorem 5.1.** *The following conditions on $\mathcal{M} = (\mathcal{L}, \Sigma)$ are equivalent:*

(a) *With probability 1, a random finite model of $\mathcal{M}$ is idemprimal.*
(b) *The minimum arity $d_{\mathcal{M}}$ of a minimal term for $\mathcal{M}$ is 2 and $p_{\mathcal{M}}(2) > 2$.*
(c) *There exist either*
- *three essentially different nontrivial binary terms for $\mathcal{M}$, or*
- *two essentially different nontrivial binary terms, $s$ and $t$, for $\mathcal{M}$ such that $\Sigma \not\models s(x, y) \approx s(y, x)$.*

We will use a criterion for idemprimality, which follows from [25, Cor. 1.4], and characterizes idemprimal algebras — among finite idempotent algebras — by forbidden compatible relations. Recall that a $k$-ary relation $R \subseteq A^k$ on the universe $A$ of an algebra $\mathbf{A}$ is called a *compatible relation of* $\mathbf{A}$ if $R$ is the universe of a subalgebra of $\mathbf{A}^k$.

**Theorem 5.2.** [25] *If $\mathbf{A}$ is a finite idempotent algebra with universe $A$ of size $> 2$, then $\mathbf{A}$ is idemprimal if and only if it satisfies the following three conditions:*

- $\mathbf{A}$ *has no proper subalgebras of size* $> 1$,
- $\mathbf{A}$ *has no nontrivial automorphisms (i.e.,* $\mathbf{A}$ *has no automorphisms other than the identity map), and*
- *no symmetric binary cross* $\mathsf{X}_a := (\{a\} \times A) \cup (A \times \{a\})$ $(a \in A)$ *is a compatible relation of* $\mathbf{A}$.

Subalgebras of random models of $\mathcal{M}$ were studied in Section 4. In the forthcoming lemmas we will discuss the probability that a random model of $\mathcal{M}$ has nontrivial automorphisms or compatible crosses. We start with a lemma which outlines a general method for proving that these probabilities are 0. We will use the following notation:

(5.1) $t = t(x_1, \dots, x_d)$ is a minimal term of arity $d$ for $\mathcal{M}$, and
$q$ is the index of $G_t$ in $S_{\{x_1,\dots,x_d\}}$;

for example, with the notation of Definition 4.1, we may choose $t$ to be $t_1$, whence $d = d_1$ and $q = q_1$. Furthermore, for every finite set $A$,

(5.2) $H_A$ denotes the set of all functions $t^{\mathbf{A}} \restriction A^{(d)}$
as $\mathbf{A}$ runs over all models $\mathbf{A} = \langle A; \mathcal{L} \rangle$ of $\mathcal{M}$.

By (4.1), we have that

(5.3) $H_A$ is the set of all functions $h \colon A^{(d)} \to A$ such that
- $\diamond$ $h$ is the union of its restrictions $h \restriction D^{(d)}$ with $D \subseteq A$, $|D| = d$,
- $\diamond$ these restrictions are independent, and
- $\diamond$ each function $h \restriction D^{(d)}$ is constant on the $q$ orbits of the action of $G_t$ on $D^{(d)}$, and is otherwise arbitrary.

For a $k$-ary relation $\rho$ on $A$ and $h \in H_A$, we will say that $\rho$ *is compatible with* $h$ if for all $r_1, \dots, r_d \in \rho$ such that the $d$-tuple $(r_{1i}, \dots, r_{di})$ of $i$th coordinates of $r_1, \dots, r_d$ lies in $A^{(d)}$ for each $i$ $(1 \leq i \leq k)$, we have that by applying $h$ coordinatewise to $r_1, \dots, r_d$, we get a tuple $h(r_1, \dots, r_d)$ in $\rho$. Clearly, if $h = t^{\mathbf{A}} \restriction A^{(d)}$ for an algebra $\mathbf{A}$ such that $\rho$ is a compatible relation of $\mathbf{A}$, then $\rho$ will be compatible with $h$. We will use the following notation:

(5.4) $$H_{A,\rho} = \{h \in H_A : \rho \text{ is compatible with } h\}.$$

Now let $\mathcal{R}$ be a function which assigns to every finite set $A$ a family $\mathcal{R}_A$ of (finitary) relations on $A$. We will say that $(\mathcal{R}_A : |A| < \omega)$ is a *homogeneous family of relations on finite sets* if for every bijection $\tau \colon A \to B$ between finite sets $A, B$ we have that $\mathcal{R}_B = \{\tau(\rho) : \rho \in \mathcal{R}_A\}$; that is, the system is invariant under renaming elements of the base set. In particular, each family $\mathcal{R}_A$ is invariant under permuting elements of the base set $A$. Examples of homogeneous families of relations on finite sets include the following:

(i) $\mathcal{R}_A$ is the set of all equivalence relations on $A$;

(ii) $\mathcal{R}_A$ is the set of all (graphs of) permutations on $A$;
(iii) $\mathcal{R}_A$ is the set of all partial orders on $A$;
(iv) $\mathcal{R}_A$ is the set of all crosses $\mathsf{X}_a$ ($a \in A$) on $A$.

It is easy to see that $(\mathcal{R}_A : |A| < \omega)$ is a homogeneous family of relations on finite sets if and only if

- $\mathcal{R}_{[n]}$ is a family of finitary relations on $[n]$ such that $\mathcal{R}_{[n]}$ is invariant under all permutations of $[n]$, and
- $\mathcal{R}_A = \{\tau(\rho) : \rho \in \mathcal{R}_{[n]}\}$ whenever $|A| = n$ and $\tau\colon [n] \to A$ is a bijection.

Our interest in homogeneous families of relations stems from the following obvious fact: if $(\mathcal{R}_A : |A| < \omega)$ is a homogeneous family of relations on finite sets, then the property "$\mathbf{A}$ has a compatible relation in $\mathcal{R}_A$" is an abstract property for finite algebras $\mathbf{A}$; therefore, for such families, it makes sense to ask what the probability of this property is for finite models $\mathbf{A}$ of $\mathcal{M}$ (cf. Definition 3.1).

**Lemma 5.3.** *Suppose we are given a homogeneous family $(\mathcal{R}_A : |A| < \omega)$ of finitary relations on finite sets such that each $\mathcal{R}_A$ is finite, and let $t$, $q$, $H_A$, and $H_{A,\rho}$ ($\rho \in \mathcal{R}_A$) be as in* (5.1)–(5.4). *If*

$$\lim_{n\to 0} \sum_{\rho\in\mathcal{R}_{[n]}} \frac{|H_{[n],\rho}|}{|H_{[n]}|} = 0, \tag{5.5}$$

*then the probability that a random finite model $\mathbf{A}$ of $\mathcal{M}$ has a compatible relation in $\mathcal{R}_A$ is* 0.

*Proof.* First we will find an upper bound for the probabilities of the events "$\rho$ is a compatible relation of $\mathbf{A}$" ($\rho \in \mathcal{R}_A$) in the probability space of all finite models of $\mathcal{M}$ on a fixed $n$-element set $A$ with $n > d$.

By our discussion preceding the definition of $H_{A,\rho}$ in (5.4), if $\mathbf{A}$ is a random model of $\mathcal{M}$ on $A$ such that $\rho$ is a compatible relation of $\mathbf{A}$, and $h = t^{\mathbf{A}} \restriction A^{(d)}$, then $h \in H_{A,\rho}$. By the choice of $t$, this function $h$ is a member of the $\mathcal{M}$-family associated to $\mathbf{A}$. For this $\mathcal{M}$-family we will use Theorem 3.5 in the form as it is restated in (4.1) and the paragraph preceding it. Since the members (of arity $> 1$) of this $\mathcal{M}$-family are independent, and $h$ is one of them, we get that

$$\Pr_A(\rho \text{ is a compatible relation of } \mathbf{A}) \leq \Pr_A\big(h \in H_{A,\rho}\big) = \frac{|H_{A,\rho}|}{|H_A|}. \tag{5.6}$$

Thus,

$$\begin{aligned} &\Pr_A(\mathbf{A} \text{ has a compatible relation in } \mathcal{R}_A) \\ &\qquad \leq \sum_{\rho\in\mathcal{R}_A} \Pr_A(\rho \text{ is a compatible relation of } \mathbf{A}) \leq \sum_{\rho\in\mathcal{R}_A} \frac{|H_{A,\rho}|}{|H_A|}. \end{aligned} \tag{5.7}$$

The probability that a finite model $\mathbf{A} = \langle A; \mathcal{L}\rangle$ of $\mathcal{M}$ has a compatible relation in $\mathcal{R}_A$ is the limit, as $n \to \infty$, of the probability estimated in (5.7) for $A = [n]$. As a consequence of assumption (5.5), this limit is 0, which completes the proof of Lemma 5.3. □

**Lemma 5.4.** *If* $\mathbf{A}$ *is a random finite model of* $\mathcal{M}$*, then the probability that* $\mathbf{A}$ *has a nontrivial automorphism is* 0*.*

*Proof.* For every finite set $A$ let $\mathcal{R}_A$ denote the set of all binary relations on $A$ which are graphs of nonidentity permutations of $A$. It is easy to see that $\rho \in \mathcal{R}_A$ is a compatible relation of an algebra $\mathbf{A}$ on $A$ if and only if $\rho$ (considered as a function $A \to A$) is an automorphism of $\mathbf{A}$. Clearly, $(\mathcal{R}_A : |A| < \omega)$ is a homogeneous family of relations on finite sets. Therefore, our statement will follow from Lemma 5.3 if we prove that (5.5) holds for this choice of $\mathcal{R}_A$.

Let $\mathbf{A}$ be a random model of $\mathcal{M}$ on an $n$-element set $A$, let $\rho \in \mathcal{R}_A$, and select $a, b \in A$ such that $\rho(a) = b \neq a$. It is easy to see that for any function $h \in H_A$, $\rho$ is compatible with $h$ — i.e., $h \in H_{A,\rho}$ — if and only if

$$h\big(\rho(a_1), \dots, \rho(a_d)\big) = \rho\big(h(a_1, \dots, a_d)\big) \quad \text{for all } \ (a_1, \dots, a_d) \in A^{(d)}. \tag{5.8}$$

Now let $\Gamma_\rho$ denote the family of all $d$-element subsets $C$ of $A$ such that $a \in C$ and $b \notin C$, and let $\Delta_\rho := \{\rho(C) : C \in \Gamma_\rho\}$. Then the assumption $\rho(a) = b \neq a$ implies that the sets in $\Delta_\rho$ contain $b$, while the sets in $\Gamma_\rho$ don't. Hence, $\Gamma_\rho \cap \Delta_\rho = \emptyset$, and therefore

$$C^{(d)} \text{ is disjoint from } \textstyle\bigcup_{D \in \Delta_\rho} D^{(d)} \text{ for all } C \in \Gamma_\rho. \tag{5.9}$$

Furthermore, if $h \in H_{A,\rho}$, that is, if (5.8) holds for $h$, then

$$h{\restriction}C^{(d)} \text{ with } C \in \Gamma_\rho \text{ determines } h{\restriction}D^{(d)} \text{ with } D = \rho(C) \in \Delta_\rho \text{ via (5.8)}. \tag{5.10}$$

We claim that these facts imply the following inequalities:

$$\frac{|H_{A,\rho}|}{|H_A|} \leq \frac{1}{n^{q|\Delta_\rho|}} \leq \frac{1}{n^{n-2}}. \tag{5.11}$$

For the proof we will use the description in (5.3) for the functions $h \in H_A$. If $h \in H_{A,\rho}$, then by (5.10), for each one of the $|\Delta_\rho|$ choices of $D \in \Delta_\rho$, the constant values of $h$ on the $q$ orbits of $G_t$ on $D^{(d)}$ are determined by the function $h{\restriction}C^{(d)}$ for some $C \in \Gamma_\rho$ satisfying (5.9). Hence, there is no choice for at least $q|\Delta_\rho|$ of the function values of $h$ that for an arbitrary member of $H_A$ could be chosen independently. Therefore $|H_{A,\rho}| \leq |H_A|/n^{q|\Delta_\rho|}$, so the first inequality in (5.11) follows. The second inequality in (5.11) is a consequence of $q \geq 1$ and $|\Delta_\rho| = |\Gamma_\rho| = \binom{n-2}{d-1} \geq n-2$ (as $d \geq 2$).

To prove (5.5) notice that $|\mathcal{R}_{[n]}| \leq n!$. Hence, we get from (5.11) (for $n > d$) that

$$(0 \leq) \sum_{\rho \in \mathcal{R}_{[n]}} \frac{|H_{[n],\rho}|}{|H_A|} \leq \frac{n!}{n^{n-2}} = n \left( \prod_{i=1}^{n-1} \sqrt{i(n-i)} \right) \frac{1}{n^{n-2}} \leq n \Big(\frac{n}{2}\Big)^{n-1} \frac{1}{n^{n-2}} = \frac{n^2}{2^{n-1}},$$

which implies that (5.5) holds. This completes the proof of the lemma. □

We now turn to discussing the probability of the presence of compatible crosses in random finite models of $\mathcal{M}$. It is easy to see that if $\mathcal{M}$ is the set of identities for a single majority operation, then in every model $\mathbf{A}$ of $\mathcal{M}$, all crosses $\mathsf{X}_a$ ($a \in A$) are compatible relations of $\mathbf{A}$. Therefore the analog of Lemma 5.4 will not be true for compatible crosses. In this paper we will restrict to the case when $\mathcal{M}$ has a minimal binary term, which will be sufficient for the proof of Theorem 5.1.

**Lemma 5.5.** *Assume $\mathcal{M}$ has a minimal binary term. If $\mathbf{A}$ is a random finite model of $\mathcal{M}$, then the probability that $\mathbf{A}$ has a compatible symmetric cross $\mathsf{X}_a$ ($a \in A$) is 0.*

*Proof.* Let $\mathbf{A}$ be a random finite model of $\mathcal{M}$ of size $> 2$, and let $t$ be a minimal binary term for $\mathcal{M}$. As before, we will use the notation (5.1)–(5.4) with $d = 2$, and will apply Lemma 5.3 to prove our claim. Let $\mathcal{R}_A := \{\mathsf{X}_a : a \in A\}$ for every finite set $A$. As we mentioned earlier, $(\mathcal{R}_A : |A| < \omega)$ is a homogeneous family of relations on finite sets. Therefore the statement of Lemma 5.5 will follow if we prove that (5.5) holds for this choice of $\mathcal{R}_A$.

Let $A$ be an $n$-element set ($n > 2$), choose $a \in A$, and let $\rho = \mathsf{X}_a$. Further, let $\Delta_\rho$ denote the family of all 2-element subsets $D$ of $A$ with $a \in D$. We claim that for any $h \in H_A$, if $\rho$ is compatible with $h$ — i.e., $h \in H_{A,\rho}$ — then

$$\begin{aligned} &\text{either } \ h(a,b) = a \text{ for all } D = \{a,b\} \in \Delta_\rho, \\ &\qquad\qquad \text{or} \quad h(b,a) = a \text{ for all } D = \{a,b\} \in \Delta_\rho. \end{aligned} \tag{5.12}$$

Indeed, otherwise there would exist $b, c \in A \setminus \{a\}$ such that $h(a,b) \neq a$ and $h(c,a) \neq a$. This would imply $(a,c),(b,a) \in \rho$, $(a,b),(c,a) \in A^{(2)}$, and $h\big((a,c),(b,a)\big) = \big(h(a,b),h(c,a)\big) \notin \rho$, contradicting our assumption that $\rho$ is compatible with $h$.

Next we want to show that

$$\frac{|H_{A,\rho}|}{|H_A|} \leq \frac{q}{n^{|\Delta_\rho|}} \leq \frac{1}{n^{n-2}}. \tag{5.13}$$

As in the proof of Lemma 5.4, we will use the description in (5.3) for the members of $H_A$ (with $d = 2$). To estimate $|H_{A,\rho}|$, let $H'_{A,\rho}$, $H''_{A,\rho}$ denote the sets of all $h \in H_{A,\rho}$ which satisfy the first option or the second option in (5.12), respectively. Clearly, $H_{A,\rho} = H'_{A,\rho} \cup H''_{A,\rho}$. If $q = 1$ (i.e., $|G_t| = 2$), then the functions $h = h(x,y)$ and $h(y,x)$ coincide, and $H'_{A,\rho} = H_{A,\rho} = H''_{A,\rho}$. If $q = 2$ (i.e., $|G_t| = 1$), then $h = h(x,y) \mapsto h(y,x)$ yields a bijection $H'_{A,\rho} \to H''_{A,\rho}$. Therefore in both cases we have that

$$|H_{A,\rho}| \leq q|H'_{A,\rho}|. \tag{5.14}$$

If $h \in H'_{A,\rho}$, then for each one of the $|\Delta_\rho|$ choices of $D = \{a,b\} \in \Delta_\rho$, the constant value of $h$ on the $G_t$-orbit of $(a,b) \in D^{(2)}$ is uniquely determined (namely, it is $a$). Hence, there is no choice for at least $|\Delta_\rho|$ of the function values of $h$ that for an

arbitrary member of $H_A$ could be chosen independently. This implies that $|H'_{A,\rho}| \leq |H_A|/n^{|\Delta_\rho|}$. Combining this inequality with (5.14) we get the first inequality in (5.13). The second inequality in (5.13) follows from $q \leq n$ and $|\Delta_\rho| = n-1$.

Now (5.5) is easy to prove. Since $|\mathcal{R}_{[n]}| = n$, we get from (5.13) (for $n > 2$) that

$$(0 \leq) \sum_{\rho \in \mathcal{R}_{[n]}} \frac{|H_{[n],\rho}|}{|H_A|} \leq \frac{n}{n^{n-2}},$$

which implies that (5.5) holds. This completes the proof of the lemma. □

We can now prove Theorem 5.1 by combining the results of this section with the results of the preceding section.

*Proof of Theorem 5.1.* The equivalence of conditions (b) and (c) is an immediate consequence of the definitions of minimal terms and the parameter $p_{\mathcal{M}}(2)$ for $\mathcal{M}$.

To prove the equivalence of conditions (a) and (b), let $\mathbf{A}$ be a random finite model of $\mathcal{M}$. First we show that (b) ⇒ (a). Assume $\mathcal{M}$ satisfies condition (b). Then $p_{\mathcal{M}}(2) > 2$, therefore we get from Theorem 4.5(2)–(4) (or the last item of Corollary 4.7) that, with probability 1, $\mathbf{A}$ has no proper subalgebras of size greater than 1. By Lemma 5.4, we have that, with probability 1, $\mathbf{A}$ has no nontrivial automorphisms. Finally, by assumption (b), Lemma 5.5 applies, and yields that, with probability 1, no symmetric cross $\mathsf{X}_a$ ($a \in A$) is a compatible relation of $\mathbf{A}$. Thus, $\mathbf{A}$ satisfies the idemprimality criterion in Theorem 5.2 with probability 1. Hence (a) follows.

Conversely, to prove (a) ⇒ (b), assume that (b) fails, that is, either $\mathcal{M}$ has no binary minimal term, or $1 \leq p_{\mathcal{M}}(2) \leq 2$. In the former case every 2-element subset of $A$ is (the universe of) a subalgebra of $\mathbf{A}$ by Theorem 4.5(1), while in the latter case $\mathbf{A}$ has a 2-element subalgebra with positive probability by Theorem 4.5(2). Thus, (a) fails in all these cases. □

## 6. Application to Some Familiar Maltsev Conditions

We conclude the paper by considering our results in the context of a few well-known strong idempotent linear Maltsev conditions.

6.1. **Hagemann–Mitschke terms for congruence $k$-permutable varieties.** The language $\mathcal{L}$ for Hagemann–Mitschke terms [8] consists of $k-1$ ternary operation symbols, $q_1, q_2, \ldots, q_{k-1}$ ($k \geq 2$), and the set $\Sigma$ of identities consists of

$$\begin{aligned} x &\approx q_1(x,y,y), \\ q_i(x,x,y) &\approx q_{i+1}(x,y,y), \quad \text{for } i = 1,2,\ldots,k-2, \\ q_{k-1}(x,x,y) &\approx y. \end{aligned}$$

The Maltsev condition "there exist Hagemann–Mitschke terms $q_1, q_2, \ldots, q_{k-1}$" characterizes those varieties with $k$-permuting congruences. The system $\mathcal{M} = (\mathcal{L}, \Sigma)$ has $2k-3$ essentially different minimal terms, all binary:

$$q_1(x,y,x),\ q_2(x,y,x),\ \ldots,\ q_{k-1}(x,y,x),\ q_1(x,x,y),\ q_2(x,x,y),\ \ldots,\ q_{k-2}(x,x,y).$$

Therefore, if $k \geq 3$ then there are at least 3 such terms, so by Theorem 5.1, random finite models of $\mathcal{M}$ are almost surely idemprimal.

If $k = 2$, then this conclusion fails. In the case $k = 2$ there is only one Hagemann–Mitschke term, $q_1$, which is a Maltsev term. We will discuss this case in the next subsection.

6.2. **Maltsev term for congruence (2-)permutable varieties.** The language $\mathcal{L}$ for a Maltsev term [17] consists of a single ternary operation symbols, $f$, and the set $\Sigma$ of identities consists of

$$x \approx f(x,y,y) \qquad \text{and} \qquad f(x,x,y) \approx y.$$

Then $\mathcal{M} = (\mathcal{L}, \Sigma)$ has a single minimal term, namely $f(x,y,x)$. Since $\Sigma \not\models f(x,y,x) \approx f(y,x,y)$, we obtain $p_{\mathcal{M}}(2) = 2$. From Lemmas 5.4 and 5.5, we learn that random finite models of $\mathcal{M}$ have, almost surely, no nontrivial automorphisms or compatible crosses. However, according to Theorem 4.5(2), a random finite model of $\mathcal{M}$ will have a 2-element subalgebra with probability $1 - e^{-2}$. Thus by Theorem 5.2, a random finite model of $\mathcal{M}$ will be idemprimal with probability $e^{-2} \approx 0.14$.

6.3. **Ternary minority term.** A ternary minority term is a special kind of Maltsev term. The existence of a ternary minority term is perhaps not of interest as a Maltsev condition, but it does provide an interesting case study for random models. The language describing a minority term is $\mathcal{L} = \{f\}$, and the set of identities is

$$\Sigma_1 = \{f(x,y,y) \approx x,\ f(y,y,x) \approx x,\ f(y,x,y) \approx x\}.$$

Clearly, $\mathcal{M}_1 = (\mathcal{L}, \Sigma_1)$ has no binary minimal terms, so $d_{\mathcal{M}_1} = 3$ and the only minimal term for $\mathcal{M}_1$ is $f(x,y,z)$ (up to renaming and permuting variables; cf. Theorem 2.9(2)). The symmetry group of $f(x,y,z)$ is trivial, so $p_{\mathcal{M}_1}(3) = 6 > d_{\mathcal{M}_1}$. Theorem 4.5(1)–(4) tells us that every 2-element subset of every model of $\mathcal{M}_1$ will be a subalgebra, but a random finite model of $\mathcal{M}_1$ will, almost surely, have no proper subalgebras of size 3 or larger. In particular, we see that no finite model of $\mathcal{M}_1$ will be idemprimal.

Now set

$$\Sigma_2 = \Sigma_1 \cup \{f(x,y,z) \approx f(y,z,x)\}.$$

In $\mathcal{M}_2 = (\mathcal{L}, \Sigma_2)$, the symmetry group of $f(x,y,z)$ has order 3, thus $p_{\mathcal{M}_2}(3) = 2$. Then Theorem 4.5(2)–(4) implies that a random finite model of $\mathcal{M}_2$ almost surely has a 3-element subalgebra, but no larger proper subalgebra.

Finally, with

$$\Sigma_3 = \Sigma_2 \cup \{f(x,y,z) \approx f(y,x,z)\},$$

the symmetry group of $f(x,y,z)$ is the full permutation group $S_{\{x,y,z\}}$. At that point we find ourselves in the territory of Problem 4.6, because $p_{\mathcal{M}_3}(3) = 1$ and there is no linear term for $\mathcal{M}_3$ with exactly 4 essential variables. We know from Theorem 4.5(2) and (4) that a random finite model of $\mathcal{M}_3$ almost surely has a 3-element subalgebra and no proper subalgebra of size 5 or larger, but the probability that it has a 4-element subalgebra is unclear.

6.4. **Near unanimity term.** Let $k \geq 3$, and let $\mathcal{L} = \{g\}$ where $g$ is a $k$-ary operation symbol. The set of *$k$-ary near unanimity identities* is

$$\Sigma_k = \left\{ g(x, x, \ldots, \overset{i^{\text{th}}}{y}, x, \ldots, x) \approx x : i = 1, \ldots, k \right\}$$

where the lone $y$ appears in the $i^{\text{th}}$ position. When $k = 3$, $g$ is called a *majority term*. In this case $g$ is the only minimal term for the system $\mathcal{M}_3 = (\mathcal{L}, \Sigma_3)$, so by Theorem 4.5(1), every 2-element subset of every model of $\mathcal{M}_3$ will be a subalgebra. It follows that no finite model of $\mathcal{M}_3$ will be idemprimal.

However, for $k > 3$ there are $2^k - 2k - 2$ essentially different binary terms. Thus by Theorem 5.1, a random finite model of $\mathcal{M}_k = (\mathcal{L}, \Sigma_k)$ will almost surely be idemprimal.

6.5. **Further examples.** In Tables 3–4 we list the answers to the question "Is a random finite model of $\mathcal{M}$ almost surely idemprimal?" for many other systems $\mathcal{M}$ which describe familiar strong idempotent linear Maltsev conditions. Since for some of the Maltsev conditions in Tables 3–4 the literature uses several slightly different descriptions $\mathcal{M}$, we followed the original papers, as indicated.

This introduces a minor inconsistency which has no effect on the random models, as we now explain, using Hagemann–Mitschke terms as an example. Instead of the system $\mathcal{M}$ displayed in subsection 6.1, Hagemann–Mitschke terms are often described by the system $\mathcal{M}' = (\mathcal{L}', \Sigma')$ where $\mathcal{L}'$ consists of the symbols $q_0, \ldots, q_n$ and $\Sigma'$ consists of the identities

$$\begin{aligned} x &\approx q_0(x,y,z), \\ q_i(x,x,y) &\approx q_{i+1}(x,y,y), \quad \text{for } i = 0, 1, 2, \ldots, k-1, \\ q_k(x,y,z) &\approx z. \end{aligned}$$

The only difference between $\mathcal{M}$ and $\mathcal{M}'$ is that the second one has two new symbols, $q_0$ and $q_k$, which are inessential, because they are $\Sigma'$-equivalent to the variables $x$ and $z$, respectively, and upon eliminating $q_0$ and $q_k$ by replacing them with those variables, $\Sigma'$ becomes the same set of identities as $\Sigma$. This implies that $\mathcal{M}$ and $\mathcal{M}'$ define equivalent varieties; in fact, there is a one-to-one correspondence $\mathbf{A} \mapsto \mathbf{A}'$ between the models $\mathbf{A}$ of $\mathcal{M}$ and the models $\mathbf{A}'$ of $\mathcal{M}'$ such that the $\mathcal{M}$-family of

| System $\mathcal{M}$ for the Maltsev condition | Is a random finite model of $\mathcal{M}$ almost surely idemprimal? | |
|---|---|---|
| | YES, if | NO, if |
| Hagemann–Mitschke terms $q_1, \ldots, q_{k-1}$ [8] for congruence $k$-permutability | $k \geq 3$ | $k = 2$ [Maltsev term] |
| Jónsson terms $t_0, \ldots, t_k$ [11] for congruence distributivity | $k \geq 4$ | $k = 2, 3$ [$k = 2$: $\sim$majority term] |
| Day terms $m_0, \ldots, m_k$ [5] for congruence modularity | $k \geq 2$ | — |
| Gumm terms $d_0, \ldots, d_k, p$ [7] for congruence modularity | $k \geq 1$ | $k = 0$ [$\sim$Maltsev term] |
| Terms $d_0, \ldots, d_k$ [9, 12] for congruence join-semidistributivity | $k \geq 4$ | $k = 2, 3$ [$k = 2$: $\sim \frac{2}{3}$-minority term] |
| $k$-ary near unanimity term [10, 1] | $k \geq 4$ | $k = 3$ [majority term] |
| $k$-cube term (arity: $2^k - 1$) [4] | $k \geq 3$ | $k = 2$ [$\sim$Maltsev term] |
| $k$-edge term (arity: $k + 1$) [4] | $k \geq 3$ | $k = 2$ [$\sim$Maltsev term] |
| $(m, n)$-parallelogram term (arity: $m + n + 3$)[15] | $m, n \geq 1$ | — |
| $k$-ary weak near unanimity term [18] | $k \geq 4$ | $k = 3$ |
| $k$-ary cyclic term [2] | $k \geq 4$ | $k = 2, 3$ |

TABLE 3. Idemprimality for random finite models of some familiar strong idempotent linear Maltsev conditions (with parameters)

$\mathbf{A}$ coincides with the $\mathcal{M}'$-family of $\mathbf{A}'$. Therefore, the probability of every abstract property is the same for the finite models of $\mathcal{M}$ as for the finite models of $\mathcal{M}'$.

In Table 3 the papers cited for Jónsson terms, Day terms, Gumm terms, and join semidistributivity terms use the approach of including inessential symbols in the language, namely $t_0, t_k$; $m_0, m_k$; $d_0$; and $d_0, d_k$. Therefore, the claim that the system for Jónsson terms for $k = 2$ reduces to the system for a majority term $t_1$ is true only after eliminating the inessential symbols $t_0, t_2$. This is indicated by the symbol

| System $\mathcal{M}$ for the Maltsev condition | Is a random finite model of $\mathcal{M}$ almost surely idemprimal? |
|---|---|
| 2/3 minority term [22] for characterizing arithmetical varieties | NO |
| Maltsev term and majority term [21] for characterizing arithmetical varieties | NO |
| 6-ary Siggers term [23] | YES |
| 4-ary Siggers term [14] | YES |
| Olšák's 6-ary weak 3-cube term [20] | YES |

TABLE 4. Idemprimality for random finite models of some familiar strong idempotent linear Maltsev conditions

$\sim$ in the last column of the table. The situation is similar for Gumm terms and join semidistributivity terms. For $k$-cube and $k$-edge terms, the case $k = 2$ yields a Maltsev term up to a possible permutation of variables only. This is what $\sim$ indicates in the last column for those cases.

More interestingly, Table 3 also shows that it can happen that two different systems $\mathcal{M} = (\mathcal{L}, \Sigma)$ and $\mathcal{M}' = (\mathcal{L}', \Sigma')$ satisfying our Global Assumption 3.2 determine equivalent Maltsev conditions, but the question "Are the random finite models almost surely idemprimal?" for $\mathcal{M}$ and $\mathcal{M}'$ have different answers. For example, for any fixed integer $k \geq 2$, let $\mathcal{M}_k$ be the system of identities for a $k$-cube term and let $\mathcal{M}'_k$ be the system of identities for a $(1, k-1)$-parallelogram term. It was proved in [15] that a variety has a $k$-cube term if and only if it has a $(1, k-1)$-parallelogram term, so $\mathcal{M}_k$ and $\mathcal{M}'_k$ describe equivalent Maltsev conditions. However, as Table 3 and the conclusion of subsection 6.2 above indicate, in the case $k = 2$ we have that a random finite model of $\mathcal{M}'_2$ is almost surely idemprimal, while a random finite model of $\mathcal{M}_2$ is idemprimal only with probability $e^{-2}$.

Now let us consider a pair of examples from Table 4: let $\mathcal{M}$ be the system of identities for a 2/3-minority term, and let $\mathcal{M}'$ be the system of identities in the language $\{f, d\}$ saying that $f$ is a Maltsev term and $d$ is a majority term. The corresponding Maltsev conditions are equivalent; both of them characterize arithmetical varieties, by [21, 22]. The answers to the question "Are the random finite models almost surely idemprimal?" are also the same for $\mathcal{M}$ and $\mathcal{M}'$. However, there are essential differences between the random finite models of $\mathcal{M}$ and $\mathcal{M}'$. By Theorem 4.5(1)–(2), for the finite models of $\mathcal{M}$ we have that all 2-element subsets are subalgebras, while for the finite models of $\mathcal{M}'$, there is a positive probability, namely $e^{-2}$, that a random finite model has no 2-element subalgebras. The latter fact follows from our result in

subsection 6.2, because the majority term $d$ makes no contribution to the family of binary minimal terms for $\mathcal{M}'$.

6.6. **Answers to our questions in the Introduction.** In the first two paragraphs of the Introduction we mentioned several questions involving specific Maltsev conditions, which have the following form (in the interpretation discussed later on in the Introduction): "For two given finite systems $\mathcal{M}_1$ and $\mathcal{M}_2$ of idempotent linear identities (in a finite language), what is the probability that a random finite model of $\mathcal{M}_1$ satisfies the Maltsev condition $\mathcal{C}_{\mathcal{M}_2}$ described by $\mathcal{M}_2$?"

Our first question was this: What is the probability that a random finite model of the Hagemann–Mitschke identities for congruence 3-permutability (see subsection 6.1) has a Maltsev term? We discussed in subsection 6.1 that a random finite model of the Hagemann–Mitschke identities for $k = 3$ is almost surely idemprimal, and therefore, by Corollary 3.8, almost surely satisfies every strong idempotent linear Maltsev condition. In particular, it follows that a random finite model of the Hagemann–Mitschke identities for $k = 3$ almost surely has a Maltsev term.

We also asked: Will a random finite algebra lying in a congruence semidistributive variety almost surely generate one that is congruence distributive? Since a variety is congruence semidistributive (i.e., both congruence meet- and join-semidistributive) if and only if it is congruence join-semidistributive, our interpretation of this question is the following: Will a random finite model of the system $\mathcal{SD}_k(\vee)$ of identities for join-semidistributivity terms for some $k \geq 2$ almost surely have Jónsson terms for some $\ell \geq 2$? (For the explicit identities, see the papers cited in Table 3.) According to Table 3, if $k \geq 4$, then a random finite model of $\mathcal{SD}_k(\vee)$ is almost surely idemprimal, and therefore by the same argument as in the preceding paragraph, it almost surely has Jónsson terms for all $\ell \geq 2$. If $k = 3$, then $\mathcal{SD}_3(\vee)$ and the system of identities for Jónsson terms for $\ell = 3$ differ only by notation; namely, one can be translated into the other by the definition $t_i(x, y, z) := d_{3-i}(z, y, x)$ $(0 \leq i \leq 3)$. Finally, if $k = 2$, then $\mathcal{SD}_k(\vee)$ implies that $d_1(x, y, z)$ is a $\frac{2}{3}$-minority term. Hence, $d_1(x, d_1(x, y, z), z)$ is a majority term, and therefore Jónsson terms for $\ell = 2$ exist. In summary, we see that for every $k \geq 2$, a random finite model of $\mathcal{SD}_k(\vee)$ will almost surely have Jónsson terms.

Another question was the following: If a random finite algebra has a Maltsev term, will it have (with probability 1) a majority term? Letting $\mathcal{M}$ denote the system of identities for a Maltsev term (see subsection 6.2), our precise interpretation of the question is the following: Will a random finite model of $\mathcal{M}$ have a majority term with probability 1? We saw that a random finite model $\mathbf{A}$ of $\mathcal{M}$ has a 2-element subalgebra with probability $1 - e^{-2}$, and is idemprimal with probability $e^{-2}$. For $\mathbf{A}$ to have a majority term, every 2-element subalgebra of $\mathbf{A}$ must have a majority term. For this it is necessary that for every 2-element subset $B$ of $A$, $B$ is not a minority subalgebra of $\mathbf{A}$, i.e., $B$ is not a subalgebra where $f^{\mathbf{B}}$ is the minority operation on $B$.

It is easy to check that for an $n$-element random model of $\mathcal{M}$ and for fixed 2-element subset $B$ of $A$,

$$\Pr_A\big(B \text{ is the universe of a minority subalgebra of } \mathbf{A}\big) = 1/n^2.$$

Therefore the same argument as in the proof of Theorem 4.5(2) yields that

$$\Pr_A\big(\mathbf{A} \text{ has no 2-element minority subalgebra}\big) = \left(1 - \frac{1}{n^2}\right)^{\binom{n}{2}},$$

so the probability that a random finite model of $\mathcal{M}$ has no 2-element minority subalgebra is $e^{-1/2}$. Hence, the probability that a random finite model of $\mathcal{M}$ has a 2-element minority subalgebra is $1 - e^{-1/2}$. This implies that a random finite model of $\mathcal{M}$ will fail to have a majority term with probability at least $1 - e^{-1/2} \approx .39$.

## Appendix A. Proof of Lemma 4.4

Let $\zeta_n(k)$ denote the $k$-th summand on the left hand side in (4.5), that is,

$$\zeta_n(k) := \binom{n}{k}\left(\frac{k}{n}\right)^{\binom{k}{2}}.$$

Or goal is to prove that

$$\lim_{n\to\infty} \sum_{k=4}^{n-1} \zeta_n(k) = 0. \tag{A.1}$$

**Claim A.1.** *For arbitrary constants $0 < u < v < 1$ we have $\lim\limits_{n\to\infty} \sum\limits_{un\le k\le vn} \zeta_n(k) = 0$.*

*Proof of Claim A.1.* For $un \le k \le vn$,

$$\zeta_n(k) = \binom{n}{k}\left(\frac{k}{n}\right)^{\binom{k}{2}} \le 2^n v^{un(un-1)/2} = \Big(2(\sqrt{v})^{u(un-1)}\Big)^n.$$

Since $(\sqrt{v})^{u(un-1)} < \frac{1}{3}$ for large enough $n$, we get that

$$\sum_{un\le k\le vn} \zeta_n(k) \le n\Big(\frac{2}{3}\Big)^n \to 0 \qquad \text{as } n \to \infty.$$

◇

To establish (A.1), it remains to find $u, v$ with $0 < u < v < 1$ such that

$$\sum_{4\le k<un} \zeta_n(k) \to 0 \quad \text{and} \quad \sum_{vn<k<n} \zeta_n(k) \to 0 \quad \text{as } n \to \infty.$$

This will be accomplished in Claims A.2 and A.3 below.

**Claim A.2.** *For $u = \frac{1}{2}$ we have that $\lim\limits_{n\to\infty} \sum\limits_{4\le k<un} \zeta_n(k) = 0$.*

*Proof of Claim A.2.* The following estimates show that the sequence $\zeta_n(k)$ ($k = 4, 5, \dots$) is decreasing for $4 \le k \le \frac{1}{2}n$:

$$\begin{aligned}\frac{\zeta_n(k+1)}{\zeta_n(k)} &= \frac{n-k}{k+1} \cdot \left(\frac{k+1}{n}\right)^k \cdot \left(\frac{k+1}{k}\right)^{\binom{k}{2}} \\ &= \frac{n-k}{n} \cdot \left(\frac{k+1}{n}\right)^{k-1} \cdot \left(\left(1+\frac{1}{k}\right)^k\right)^{\frac{k-1}{2}} \le \left(\frac{k+1}{n}\right)^{k-1} \cdot e^{\frac{k-1}{2}} \\ &< \left(\frac{k+1}{n}\right)^{k-1} \cdot 2^{k-1} \le 1 \qquad \text{if} \quad k+1 \le \frac{n}{2}.\end{aligned}$$

The first term of the sequence is

$$\zeta_n(4) = \binom{n}{4}\left(\frac{4}{n}\right)^6 \le \frac{4^6}{4!} \cdot \frac{1}{n^2},$$

hence

$$\sum_{4 \le k \le un} \zeta_n(k) \le un \cdot \frac{4^6}{4!} \cdot \frac{1}{n^2} \to 0 \qquad \text{as } n \to \infty.$$

◇

**Claim A.3.** *There exists a constant $v$ with $\frac{1}{2} < v < 1$ such that*

$$\lim_{n\to\infty} \sum_{vn<k<n} \zeta_n(k) = 0.$$

*Proof of Claim A.3.* As in the proof of [3, Lemma 6.22C], letting $\ell := \lfloor vn \rfloor$ we have that

$$\binom{n}{\ell} < \sqrt{n}\left(\left(v-\frac{1}{n}\right)^v \left(1-v\right)^{1-v}\left(1-v\right)^{\frac{1}{n}}\right)^{-n}.$$

Now let $k$ be such that $(\frac{n}{2} <) \, vn < k < n$. We may assume without loss of generality that $n > 8$, so $k \ge 4$, and hence $\binom{k}{2} \ge \frac{k^2}{3}$. Thus,

$$\left(\frac{k}{n}\right)^{\binom{k}{2}} \le \left(\frac{n-1}{n}\right)^{\binom{k}{2}} \le \left(\frac{n-1}{n}\right)^{\frac{k^2}{3}} \le \left(\frac{n-1}{n}\right)^{\frac{v^2n^2}{3}} = \left(\left(1-\frac{1}{n}\right)^n\right)^{\frac{v^2n}{3}} < \left(\frac{1}{e}\right)^{\frac{v^2n}{3}}.$$

Since $k \geq vn \geq \ell$ and $vn > \frac{n}{2}$, it follows that $\binom{n}{k} \leq \binom{n}{\ell}$. Therefore, by combining the previous estimates we obtain that

$$\begin{aligned}
\zeta_n(k) = \binom{n}{k}\left(\frac{k}{n}\right)^{\binom{k}{2}} &\leq \sqrt{n}\left(\left(v-\frac{1}{n}\right)^{v}\left(1-v\right)^{1-v}\left(1-v\right)^{\frac{1}{n}}\right)^{-n}\left(\frac{1}{e}\right)^{\frac{v^2 n}{3}} \\
&= \sqrt{n}\left(\frac{1}{\left(v-\frac{1}{n}\right)^{v}\left(1-v\right)^{1-v}e^{\frac{v^2}{3}}}\right)^{n}(1-v)^{-1} \\
&\leq \sqrt{n}\left(\frac{1}{\left(v-\frac{1}{16}\right)^{v}\left(1-v\right)^{1-v}e^{\frac{v^2}{3}}}\right)^{n}(1-v)^{-1} \\
&\qquad\qquad \text{if } n \geq 16.
\end{aligned}$$

Let $w := \left(v-\frac{1}{16}\right)^{v}\left(1-v\right)^{1-v}e^{\frac{v^2}{3}}$. It can be checked that there exists $v$ with $\frac{1}{2} < v < 1$ such that $w > 1$; for example, $v = .95$ works. Thus,

$$\sum_{vn<k<n} \zeta_n(k) \leq \sum_{vn<k<n} \frac{\sqrt{n}}{1-v}\left(\frac{1}{w}\right)^{n} \to 0 \qquad \text{as } n \to \infty.$$

◇

This completes the proof of Lemma 4.4.

## References


[1] Baker, Kirby A.; Pixley, Alden F., *Polynomial interpolation and the Chinese remainder theorem for algebraic systems.* Math. Z. **143** (1975), no. 2, 165–174.

[2] Barto, Libor; Kozik, Marcin; Maróti, Miklós; McKenzie, Ralph; Niven, Todd, *Congruence modularity implies cyclic terms for finite algebras.* Algebra Universalis **61** (2009), no. 3–4, 365–380.

[3] Bergman, Clifford *Universal Algebra. Fundamentals and Selected Topics,* Pure and Applied Mathematics (Boca Raton), vol. 301, CRC Press, Boca Raton, FL, 2012.

[4] Berman, Joel; Idziak, Paweł; Marković, Petar; McKenzie, Ralph; Valeriote, Matthew; Willard, Ross, *Varieties with few subalgebras of powers.* Trans. Amer. Math. Soc. 362 (2010), no. 3, 1445–1473.

[5] Day, Alan, *A characterization of modularity for congruence lattices of algebras.* Canad. Math. Bull. **12** (1969), 167–173.

[6] Freese, Ralph, *On the two kinds of probability in algebra.* Algebra Universalis **27** (1990), no. 1, 70–79.

[7] Gumm, H.-Peter, *Congruence modularity is permutability composed with distributivity.* Arch. Math. (Basel) **36** (1981), no. 6, 569–576.

[8] Hagemann, Joachim; Mitschke, A., *On n-permutable congruences.* Algebra Universalis **3** (1973), no. 1, 8–12.

[9] Hobby, David; McKenzie, Ralph, *The structure of finite algebras.* Contemporary Mathematics, 76. American Mathematical Society, Providence, RI, 1988.

[10] Huhn, A. P., *Weakly distributive lattices.* preprint, 1972.
[11] Jónsson, Bjarni, *Algebras whose congruence lattices are distributive.* Math. Scand. **21** (1967), 110–121 (1968).
[12] Kearnes, Keith A.; Kiss, Emil W., *The shape of congruence lattices.* Mem. Amer. Math. Soc. **222** (2013), no. 1046, viii+169 pp.
[13] Kearnes, Keith, Kiss, Emil, Szendrei, Ágnes, *Growth rates of finite algebras, I: pointed cube terms.* J. Austral. Math. Soc. **101** (2016), 56–94.
`https://arXiv.org/abs/1311.2352`
[14] Kearnes, Keith; Marković, Petar; McKenzie, Ralph, *Optimal strong Mal'cev conditions for omitting type 1 in locally finite varieties.* Algebra Universalis **72** (2014), no. 1, 91–100.
[15] Kearnes, Keith A.; Szendrei, Ágnes, *Clones of algebras with parallelogram terms.* Internat. J. Algebra Comput. **22** (2012), no. 1, 1250005, 30 pp.
[16] Kelly, David, *Basic equations: word problems and Mal'cev conditions.* Abstract 701-08-04, AMS Notices **20** (1972) A-54.
[17] Mal'cev, A. I., *On the general theory of algebraic systems.* (Russian) Mat. Sb. N.S. **35**(77), (1954), 3–20.
[18] Maróti, Miklós; McKenzie, Ralph, *Existence theorems for weakly symmetric operations.* Algebra Universalis **59** (2008), no. 3–4, 463–489.
[19] Murskiĭ, V. L., *The existence of a finite basis of identities, and other properties of almost all finite algebras* Problemy Kibernet. (1975), no. 30, 43–56.
[20] Olšák, Miroslav, *The weakest nontrivial idempotent equations.* Bull. Lond. Math. Soc. **49** (2017), no. 6, 102–1047.
[21] Pixley, A. F., *Distributivity and permutability of congruence relations in equational classes of algebras.* Proc. Amer. Math. Soc. **14** (1963), 105–109.
[22] Pixley, Alden F., *The ternary discriminator function in universal algebra.* Math. Ann. **191** (1971), 167–180.
[23] Siggers, Mark H., *A strong Mal'cev condition for locally finite varieties omitting the unary type.* Algebra Universalis **64** (2010), no. 1–2, 15–20.
[24] Świerczkowski, S., *Algebras which are independently generated by every n elements.* Fund. Math. **49** (1960–61), 93–104.
[25] Szendrei, Ágnes, *Idempotent algebras with restrictions on subalgebras.* Acta. Sci. Math. (Szeged) **51** (1987), 251–268.

(Clifford Bergman) Department of Mathematics, Iowa State University, Ames, Iowa 50011, USA
*E-mail address*: `cbergman@iastate.edu`

(Ágnes Szendrei) Department of Mathematics, University of Colorado, Boulder, CO 80309-0395, USA
*E-mail address*: `Szendrei@Colorado.EDU`