JOHANNES KEPLER
UNIVERSITY LINZ

Submitted by
Florian Aichinger

Submitted at
Institute of Algebra

Supervisor
Assoz. Univ.-Prof. Dipl.-Ing. Dr. Erhard Aichinger

June 2020

Probability in Universal Algebra

Master Thesis
to obtain the academic degree of
Diplom-Ingenieur
in the Master's Program
Industrial Mathematics

**JOHANNES KEPLER
UNIVERSITY LINZ**
Altenbergerstraße 69
4040 Linz, Österreich
www.jku.at
DVR 0093696

Abstract

In this thesis we investigate what is the probability that a randomly chosen finite algebra has a certain property. To this end we use concepts from universal algebra as well as combinatorics and probability theory. We give an overview about what was already done in this research area and present some new results.

Zusammenfassung

In dieser Arbeit beschäftigen wir uns mit der Frage wie wahrscheinlich es ist, dass eine zufällig ausgewählte endliche Algebra eine gewisse Eigenschaft besitzt. Dafür verwenden wir sowohl Konzepte aus der universellen Algebra als auch Kombinatorik und Wahrscheinlichkeitstheorie. Wir geben einen Überblick über dieses Forschungsgebiet und präsentieren neue Resultate.

Acknowledgements

First of all, I would like to express my gratitude to my supervisor Assoz. Univ.-Prof. Dipl.-Ing. Dr. Erhard Aichinger for his time and for many useful comments and discussions. I very much appreciated the opportunity to write this thesis as a member of his research project.

I am also very grateful to all my colleages at the Institute of Algebra for their support in mathematical as well as in administrative matters.

Finally I want to thank my parents Gerhard and Monika for enabling me to follow my studies and my family and friends, especially my uncle Norbert, for constantly motivating me.

Probability in universal algebra

June 17, 2020

Contents

Chapter 1

Preliminaries

Throughout this thesis we will report on well known results concerning probability in universal algebra, presenting and commenting the proofs given in the literature. In this context, verbatim quotes will be identified as such by indentation and using a smaller font. Often own comments and further explanations are inserted in between.

1.1 Relational structures vs. universal algebras

1.1.1 Relational structures

Definition 1.1.1. A *relational structure* is an ordered pair $\langle A, R\rangle$, where A is a nonempty set and R is a family of finitary relations on A indexed by a set $\mathcal{R}$ of relation symbols.

In this setting, the following zero-one law was established by R. Fagin. For a finite set of (nonlogical) predicate symbols $\mathscr{S}$, we call a relational structure appropriate for $\mathscr{S}$ a $\mathscr{S}$-structure. The set of $\mathscr{S}$-structures with universe $\{1, \ldots, n\}$ is denoted by $\mathscr{A}_n$. In [Fag76], R. Fagin showed that for any first order $\mathscr{S}$-sentence σ the fraction $\mu_n(\sigma)$ of members of $\mathscr{A}_n$ for which σ is true tends to either 0 or 1 and that the convergence is geometrically fast.

1.1.2 Universal algebras

Definition 1.1.2 ([BS81, Def. II.1.1])**.** For a nonempty set A and a nonnegative integer n we define $A^0 = \{\emptyset\}$ and for $n > 0$, A^n is the set of n-tuples of elements from A. An *n-ary operation* (or *function*) on A is a function f from $A^n \to A$; n

is the *arity* (or *rank*) of f. The image of $\langle a_1, \dots, a_n \rangle$ under an n-ary function f is denoted by $f(a_1, \dots, a_n)$. An operation f on A is called a *nullary* operation (or *constant*) if its arity is zero; it is completely determined by the image $f(\emptyset)$ in A of the only element $\emptyset$ in A^0, and as such it is convenient to identify it with the element $f(\emptyset)$. Thus a nullary operation is thought of as an element of A. An operation f on A is *unary*, *binary*, or *ternary* if its arity is $1, 2$, or 3 respectively.

Definition 1.1.3 ([BS81, Def. II.1.2]). A *language* (or *type*) of algebras is a set $\mathcal{F}$ of *function symbols* such that a nonnegative integer is assigned to each member of $\mathcal{F}$. This integer is called the *arity* (or *rank*) of f, and f is said to be an *n-ary function symbol.*

Definition 1.1.4 ([BS81, Def. II.1.3]). If $\mathcal{F}$ is a language of algebras then an *algebra* $\boldsymbol{A}$ of *type* $\mathcal{F}$ is an ordered pair $\langle A, F \rangle$ where A is a nonempty set and F is a family of finitary operations on A indexed by the language $\mathcal{F}$ such that corresponding to each n-ary function symbol f in $\mathcal{F}$ there is an n-ary operation $f^{\boldsymbol{A}}$ on A. The set A is called the *universe* of $\boldsymbol{A} = \langle A, F \rangle$, and the $f^{\boldsymbol{A}}$'s are called the *fundamental operations* of $\boldsymbol{A}$ (in paratice we often just write f for $f^{\boldsymbol{A}}$). If F is finite, say $\mathcal{F} = \{A, f_1, \dots, f_k\}$, we often write $\langle A, f_1, \dots, f_k \rangle$ for $\langle A, F \rangle$, usually adopting the convention:

$$\text{arity } f_1 \geq \text{arity } f_2 \geq \cdots \geq \text{arity } f_k.$$

$\boldsymbol{A}$ is a *groupoid* if it has just one binary operation, usually denoted $\cdot$ or $+$. An algebra $\boldsymbol{A}$ is *finite* if $|A|$ is finite, and *trivial* if $|A| = 1$.

1.2 Important properties of algebras and how they are related

In this section, we introduce some properties of great interest in universal algebra, which we are going to study in the next chapters. We presume knowledge of the elementary concepts from universal algebra (terms, congruences, varieties, etc.) given in [BS81].

Definition 1.2.1. A finite algebra $\mathbf{A}$ is called

- *primal* if and only if its clone contains all finitary operations on A.
- *idemprimal* if and only if its clone contains all idempotent operations on A.

- *quasiprimal* if the ternary discriminator function $t(x, y, z)$ defined as

$$t(x,y,z) := \begin{cases} z & \text{if } x = y, \\ x & \text{if } x \neq y. \end{cases}$$

is a term function of $\boldsymbol{A}$.

- *subalgebra-primal* if and only if $\mathrm{Clo}(\boldsymbol{A}) = \mathcal{F}(\mathrm{Sub}(\boldsymbol{A}))$, where $\mathcal{F}(\mathrm{Sub}(\boldsymbol{A}))$ denotes the set of operations preserving every subuniverse of $\boldsymbol{A}$.
- *simple* if and and only if it has no nontrivial congruence relations.
- *rigid* if and only if its automorphism group is trivial.

Theorem 1.2.2 ([Ber12, Thm. 6.10])**.** *Let $\boldsymbol{A}$ be a finite algebra. The following are equivalent.*

1. *$\boldsymbol{A}$ is quasiprimal;*
2. *every subalgebra of $\boldsymbol{A}$ is simple or trivial, and $\boldsymbol{V}(\boldsymbol{A})$ is arithmetical;*
3. $\mathrm{Clo}(\boldsymbol{A}) = \mathcal{F}(\mathrm{Iso}(\boldsymbol{A}))$*, where* $\mathcal{F}(\mathrm{Iso}(\boldsymbol{A}))$ *is the set of operations preserving all internal isomorphisms*[1] *of $\boldsymbol{A}$.*

Corollary 1.2.3 ([Ber12, Cor. 6.12])**.** *Let $\boldsymbol{A}$ be a finite algebra. Then $\boldsymbol{A}$ is subalgebra-primal if and only if $\boldsymbol{A}$ is quasiprimal, distinct proper subalgebras of $\boldsymbol{A}$ are nonisomorphic, and no subalgebra of $\boldsymbol{A}$ has a nontrivial automorphism.*

Theorem 1.2.4. *Let $\boldsymbol{A}$ be a finite algebra. Then the following are equivalent.*

1. *$\boldsymbol{A}$ is idemprimal;*
2. *$\boldsymbol{A}$ is simple, rigid, has no proper, nontrivial subalgebras, and generates an arithmetical variety;*
3. $\mathrm{Clo}(\boldsymbol{A}) = \mathcal{F}(\mathrm{Sub}_1(\boldsymbol{A}))$.

Proof: (1)⇒(2): Let $\boldsymbol{A}$ be idemprimal. Since $\mathrm{Clo}(\boldsymbol{A})$ contains every idempotent operation on A, it also has a Pixley term (i.e. a term that satisfies $p(x, y, x) \approx p(x, y, y) \approx p(y, y, x) \approx x$) and hence $\boldsymbol{V}(\boldsymbol{A})$ is arithmetical.
Let θ be a congruence on A such that $\theta \neq \Delta_A$. Hence we find $a \neq b$ such that $a\theta b$. Clearly, since $\boldsymbol{A}$ is idemprimal it is also quasiprimal. But then for an arbitrary $c \in A$, we have $a = t^A(a, b, c)\theta t^A(a, a, c) = c$ and hence θ is the universal congruence ∇_A.

[1] see [Ber12], S.173

Let $\boldsymbol{B}$ be a proper, nontrivial subalgebra of $\boldsymbol{A}$. Then we can find distinct $a, b, c \in A$ such that $b, c \in B$ and $a \notin B$. Consider the operation $f : A^2 \to A$;

$$f(x, y) := \begin{cases} x & \text{if } x = y, \\ a & \text{if } x \neq y. \end{cases}$$

Since f is idempotent, $f \in \mathrm{Clo}(\boldsymbol{A})$. But f does not preserve B, since $f(b, c) = a$. Assume there is a nontrivial automorphism ϕ of $\boldsymbol{A}$. Then we can find $a, b, c, d \in A$ with $a \neq b$, $a \neq c$, $c \neq d$, $d \neq b$ such that $\phi(a) = b$ and $\phi(c) = d$. Let $g : A^2 \to A$;

$$g(x, y) := \begin{cases} x & \text{if } x = y, \\ a & \text{if } x = a, x \neq y, \\ d & \text{if } y = d, x \neq y, x \neq a, \\ y & \text{otherwise}. \end{cases}$$

Again $g \in \mathrm{Clo}(\boldsymbol{A})$ but $\phi(g(a, c)) = \phi(a) = b \neq d = g(b, d) = g(\phi(a), \phi(c))$.
(2)⇒(3): Since $\boldsymbol{A}$ is simple, has no proper, nontrivial subalgebras, and generates an arithmetical variety, condition (2) from Theorem 1.2.2 is fulfilled. Thus $\boldsymbol{A}$ is quasiprimal. Since $\boldsymbol{A}$ is also rigid, Corollary 1.2.3 yields that $\boldsymbol{A}$ is subalgebra-primal. Thus $\mathrm{Clo}(\boldsymbol{A}) = \mathcal{F}(\mathrm{Sub}(\boldsymbol{A})) = \mathcal{F}(\mathrm{Sub}_1(\boldsymbol{A}))$, since $\boldsymbol{A}$ has only trivial subalgebras.
(3)⇒(1): Let f be an idempotent function. Then f preserves every trivial subalgebra of $\boldsymbol{A}$ and hence is contained in $\mathrm{Clo}(\boldsymbol{A})$. □

1.3 The probability measure

In this section, we construct a finitely additive probability measure on the set of properties of finite algebras.

Definition 1.3.1. Let Ω be a set. A nonempty subset Σ of $\mathcal{P}(\Omega)$ is called an *algebra of sets* if the following conditions hold:

1. $A, B \in \Sigma \Rightarrow A \cup B \in \Sigma$.

2. $A \in \Sigma \Rightarrow A^c \in \Sigma$.

Definition 1.3.2. A *finitely additive probability measure* μ on a set Ω with an algebra Σ is a function from Σ to $[0, 1]$ satisfying:

1. $\mu(\Omega) = 1$,

2. For all finite collections of pairwise disjoint sets $\{A_i\}_{i=1}^n$ from Σ, $\mu(\bigcup_{i=1}^n A_i) = \sum_{i=1}^n \mu(A_i)$.

For a given finite type ρ (i.e., a type ρ consisting of finitely many operation symbols) and $n \in \mathbb{N}$, we let $\mathrm{Alg}_{\rho,n}$ be the set of algebras of type ρ with universe $\{1, \ldots, n\}$ and define $\mathrm{Alg}_\rho = \bigcup_{n\in\mathbb{N}} \mathrm{Alg}_{\rho,n}$. A property Π of finite algebras of type ρ can be simply seen as a subset of Alg_ρ (i.e. a set of operation tables). Now let $\Omega = \mathrm{Alg}_\rho$ and $\Sigma = \mathcal{P}(\mathrm{Alg}_\rho)$. Clearly (Ω, Σ) is an algebra of sets. Define a function $Pr : \Sigma \to [0, 1]$ by

$$Pr(\Pi; \mathrm{Alg}_\rho) = \lim_{n\to\infty} Pr(\Pi; \mathrm{Alg}_{\rho,n}), \text{ where}$$
$$Pr(\Pi, \mathrm{Alg}_{\rho,n}) := \tfrac{|\{\boldsymbol{A}\in\mathrm{Alg}_{\rho,n} : \boldsymbol{A}\models\Pi\}|}{|\mathrm{Alg}_{\rho,n}|} = \tfrac{|\Pi\cap\mathrm{Alg}_{\rho,n}|}{|\mathrm{Alg}_{\rho,n}|}$$

if this limit exists; $Pr(\Pi; \mathrm{Alg}_\rho)$ is undefined otherwise.
We show that Pr is a finitely additive probability measure. Let Ω be the universal property, i.e. $\Omega = \mathrm{Alg}_\rho$. Then

$$Pr(\Omega, \mathrm{Alg}_{\rho,n}) = \lim_{n\to\infty} \tfrac{|\mathrm{Alg}_{\rho,n}|}{|\mathrm{Alg}_{\rho,n}|} = \lim_{n\to\infty} 1 = 1.$$

Now let Π_1 and Π_2 be two disjoint properties (i.e. disjoint subsets of Alg_ρ) such that the above limit exists for both Π_1 and Π_2. Then

$$Pr(\Pi_1 \cup \Pi_2, \mathrm{Alg}_{\rho,n}) = \lim_{n\to\infty} \tfrac{|(\Pi_1\cup\Pi_2)\cap\mathrm{Alg}_{\rho,n}|}{|\mathrm{Alg}_{\rho,n}|} = \lim_{n\to\infty} \tfrac{|(\Pi_1\cap\mathrm{Alg}_{\rho,n})\cup(\Pi_2\cap\mathrm{Alg}_{\rho,n})|}{|\mathrm{Alg}_{\rho,n}|} =$$
$$\lim_{n\to\infty} \tfrac{|\Pi_1\cap\mathrm{Alg}_{\rho,n}|}{|\mathrm{Alg}_{\rho,n}|} + \tfrac{|\Pi_2\cap\mathrm{Alg}_{\rho,n}|}{|\mathrm{Alg}_{\rho,n}|} =$$
$$\lim_{n\to\infty} \tfrac{|\Pi_1\cap\mathrm{Alg}_{\rho,n}|}{|\mathrm{Alg}_{\rho,n}|} + \lim_{n\to\infty} \tfrac{|\Pi_2\cap\mathrm{Alg}_{\rho,n}|}{|\mathrm{Alg}_{\rho,n}|} = Pr(\Pi_1, \mathrm{Alg}_{\rho,n}) + Pr(\Pi_2, \mathrm{Alg}_{\rho,n}).$$

Thus we will denote the probability that a randomly chosen finite algebra of type ρ has property Π by $Pr(\Pi; \mathrm{Alg}_\rho)$ or simply $Pr_\rho(\Pi)$.

Chapter 2

How rare are primal algebras?

The property of primality defined in the previous section is quite strong and so one might suppose that primal algebras are rather rare. However, by a result of V.L. Murskii from 1975 we know that primal algebras are not unusual at all. In [Mur75] he proved that with a mild assumption on the similarity type ρ, almost every algebra of type ρ is primal. In 1979, R.O. Davies showed that the probability that a finite groupoid is primal is $1/e$ when he investigated so called Sheffer functions. In this section we will mainly present the proofs of the above facts given in [Ber12], only adding some details and further explanations. Verbatim quotes from the literature will be identified as such by indentation and using a smaller font. The theorem we are going to prove states the following.

Theorem 2.0.1 ([Ber12, Thm. 6.17])**.** *Let ρ be a similarity type containing a single k-ary operation symbol with $k > 1$. Let I be the property of being an idemprimal algebra and P be the property of being a primal algebra. Then*

1. *$Pr_\rho(P) = 1/e$;*
2. *$Pr_\rho(I) = 1$.*

If ρ contains at least two operation symbols, at least one of which is nonunary, then $Pr_\rho(P) = 1$

Theorem 2.0.1 (1) is due to R.O. Davies [Dav79]. The remainder of the theorem is due to V.L. Murskii [Mur75]. The proofs in [Ber12] follow unpublished treatments by R. Quackenbush and R. McKenzie.

The proof of the theorem is based on the fact that an algebra is primal if and only if it is idemprimal and has no proper subalgebras (Theorem 1.2.4). Therefore, we will start our analysis investigating the latter two properties. As we will see, the entire theorem follows easily once we have proved part (2) in the case $k = 2$.

2.1 The fraction of algebras without trivial subalgebras

Theorem 2.1.1 ([Ber12, Thm. 6.16])**.** *Let E be the property that an algebra has no trivial subalgebras*

1. *Let ρ be a similarity type containing a single k-ary operation symbol with $k > 1$. Then $Pr_\rho[E] = 1/e \approx 0.368$.*
2. *If ρ contains at least two operation symbols, at least one of which is at least binary, then $Pr_\rho[E] = 1$.*

Proof: Let $\rho = \langle k \rangle$ and f be the k-ary operation. The operation is uniquely specified by its Cayley table. Since there are n^k spaces in the table, and there are n choices for each space, we see that $|\operatorname{Alg}_{\rho,n}| = n^{n^k}$. Now, in order for the algebra to have no trivial subalgebras, we must have $f(i, \dots, i) \neq i$ for all $i \in A$. This means that each diagonal entry of the Cayley table has only $n-1$ choices instead of n. Since there are n diagonal entries, we obtain $\operatorname{Alg}_{\rho,n}[E] = n^{n^k-n}(n-1)^n$. Therefore

$$Pr(E) = \lim_{n\to\infty} \tfrac{n^{n^k-n}(n-1)^n}{n^{n^k}} = \lim_{n\to\infty} (\tfrac{n-1}{n})^n = \tfrac{1}{e}.$$

For the second statement of the theorem, let us assume that $\rho = \langle 2, 1 \rangle$. A more general similarity type follows the same argument but the notation is more difficult. Call the unary operation symbol f. Its operation table is a sequence of length n. Arguing as above, the total number of spaces in the two tables is n^2+n, so $|\operatorname{Alg}_{\rho,n}| = n^{n^2+n}$. Now, in order to have no 1-element subalgebras, we must have either $j \cdot j \neq j$ or $f(j) \neq j$ for every $j \in A$. There are n pairs $(j \cdot j, f(j))$, $j = 1, 2, \dots, n$ and for each pair, there are $n^2 - 1$ ways of filling it in. Thus $|\operatorname{Alg}_{\rho,n}[E]| = (n^2-1)^n \cdot n^{n^2-n}$. Consequently

$$Pr_\rho(E) = \lim_{n\to\infty} \tfrac{(n^2-1)^n \cdot n^{n^2-n}}{n^{n^2+n}} = \lim_{n\to\infty} (\tfrac{n-1}{n} \cdot \tfrac{n+1}{n})^n = \tfrac{1}{e} \cdot e = 1. \text{ [Ber12, p. 179]} \quad \square$$

2.2 An equivalent characterization of idemprimal algebras

Definition 2.2.1 ([Ber12])**.** Let A be a finite set, $m > 1$ and denote by $q_1, \dots, q_m$ the projection maps from A^m to A. Let us define a subset B of A^m to be *reduced* if

1. $\forall i \leq m : |\vec{q}_i(B)| > 1$ and

2. $\forall i \neq j : q_i \restriction_B \neq q_j \restriction_B$.

Note that Bergman writes $\vec{q_i}(B)$ for the image of a subset B of A^m under the ith projection map.

Lemma 2.2.2 ([Ber12, Lem. 6.18]). *Let $\boldsymbol{A}$ be a finite algebra. $\boldsymbol{A}$ is idemprimal if and only if for every $m \geq 1$, $\boldsymbol{A}^m$ has no proper, reduced subalgebra.*

Proof:

> Suppose that $\boldsymbol{A}$ is idemprimal and $\boldsymbol{B}$ is a reduced subalgebra of $\boldsymbol{A}^m$. We want to show $B = A^m$. Let q_i be the i^{th} projection map and $\eta_i = \ker(q_i)$, for $i \leq m$. For every i, $\vec{q_i}(B)$ is a subalgebra of $\boldsymbol{A}$, and nontrivial since B is reduced. [Ber12, p. 180]

Since $\boldsymbol{A}$ is idemprimal, Theorem 1.2.4 yields that $\boldsymbol{A}$ is simple and has no proper, nontrivial subalgebras, implying $\vec{q_i}(B) = A$.

> Since $\boldsymbol{B}/\eta_i \cong \vec{q_i}(B)$ it follows that η_i is a maximal proper congruence of $\boldsymbol{B}$. [Ber12, p. 180]

This follows from [BS81, Thm. 8.9], which states that for an algebra $\boldsymbol{A}$ and $\theta \in \operatorname{Con} \boldsymbol{A}$, $\boldsymbol{A}/\theta$ is a simple algebra if and only if θ is a maximal congruence on $\boldsymbol{A}$ or $\theta = \nabla$. If in our case $\eta_i = \ker(q_i) = \nabla$, then $|\vec{q_i}(B)| = 1$ in contradiction to the assumption that $\boldsymbol{B}$ is reduced.

> Suppose that for some $i \neq j$ we have $\eta_i = \eta_j$. Then there is an isomorphism $f : \boldsymbol{A} \to \boldsymbol{A}$ such that $f \circ q_i = q_j$. [Ber12, p. 181]

To see this, define $f : \vec{q_i}(B) \to \vec{q_j}(B)$; $f(q_i(b)) = q_j(b)$. Since $\eta_i = \eta_j$, we have

$$q_i(b_1) = q_i(b_2) \Leftrightarrow (b_1, b_2) \in \ker(q_i) \Leftrightarrow (b_1, b_2) \in \ker(q_j) \Leftrightarrow q_j(b_1) = q_j(b_2)$$

implying that f is well defined and injectiv. Since $\vec{q_j}(B) = A = \vec{q_j}(B)$, f is a surjective mapping from A to A. Since q_i and q_j are homomorphisms from $\boldsymbol{B}$ to $\boldsymbol{A}$ we have

$$f(g(q_i(b))) = f(q_i(g(b))) = q_j(g(b)) = g(q_j(b)) = g(f(q_i(b))).$$

Thus $f : \boldsymbol{A} \to \boldsymbol{A}$ is an isomorphism with $f \circ q_i = q_j$. But since $\boldsymbol{A}$ is rigid by Theorem 1.2.4, f must be the identity map.

> Consequently $q_i = q_j$ which contradicts the fact that $\boldsymbol{B}$ is reduced. Thus the η_i's are pairwise distinct, and since they are maximal, $\eta_i \vee \eta_j = 1_B$ whenever $i \neq j$. [Ber12, p. 181]

Theorem 1.2.4 yields that $\boldsymbol{A}$ generates an arithmetical variety. Thus

$$\eta_i \circ \bigcap_{j\neq i} \eta_j = \eta_i \vee \bigcap_{j\neq i} \eta_j = \bigcap_{j\neq i} (\eta_i \vee \eta_j) = 1$$

> and $\bigcap_{i=1}^{m} \eta_i = 0_B$. Therefore $\boldsymbol{B} \cong \boldsymbol{A}^m$. [Ber12, p. 181]

The last implication is an immediate consequence of [BS81, Thm. 7.5].

Now, for the converse suppose that $\boldsymbol{A}$ is not idemprimal. Then by Theorem 1.2.4 there is an operation f with $f \in \mathcal{F}(\mathrm{Sub}_1(\boldsymbol{A})) - \mathrm{Clo}(\boldsymbol{A})$.

> Let $n = \operatorname{rank} f$. Recall that $\mathrm{Clo}_n(\boldsymbol{A})$ is a subalgebra of $\boldsymbol{A}^{(A^n)}$ ([Ber12, Thm. 4.9]). Because it omits f, it is a proper subalgebra. Unfortunately it is not quite reduced, so we have to throw away several coordinates. Let us define
>
> $$I = A^n - \{(u, u, \dots, u) : \{u\} \in \mathrm{Sub}_1(\boldsymbol{A})\}$$
> $$B = \{g \restriction_I : g \in \mathrm{Clo}_n(\boldsymbol{A})\}.$$
>
> Then $\boldsymbol{B} \leq \boldsymbol{A}^{\boldsymbol{I}}$. We claim that $f \restriction_I \notin B$. To see this, observe that if $f \restriction_I = g \restriction_I$ for some $g \in \mathrm{Clo}_n(\boldsymbol{A})$, then, since $g(u, u, \dots, u) = u$ for each $\{u\} \in \mathrm{Sub}_1(\boldsymbol{A})$, $f = g \in \mathrm{Clo}(\boldsymbol{A})$ which is false. Thus $\boldsymbol{B}$ is a proper subalgebra of $\boldsymbol{A}^{\boldsymbol{I}}$. We show it is reduced. Keep in mind that the "coordinates" of a member of B are the elements of I, which are n-tuples from A. For the second condition, suppose that $\boldsymbol{x}$ and $\boldsymbol{y}$ are distinct elements of I. Then for some $j \leq n$, $x_j \neq y_j$. Let $p_j^n \in \mathrm{Clo}_n(\boldsymbol{A})$ be the projection operation. Thus $q_{\boldsymbol{x}}(p_j^n) = p_j^n(\boldsymbol{x}) = x_j \neq y_j = q_{\boldsymbol{y}}(p_j^n)$. So condition (2) holds. Finally suppose that for some $\boldsymbol{x} \in I$, $q_{\boldsymbol{x}}(B) = \{u\}$. Since for every $j \leq n$, $x_j = q_{\boldsymbol{x}}(p_j^n)$, we must have that $\boldsymbol{x} = \{u, u, \dots, u\}$. Since $\boldsymbol{B}$ is an algebra, u must be an idempotent of $\boldsymbol{A}$, contradicting the fact that $\boldsymbol{x} \in I$. [Ber12, p. 181] □

2.3 The fraction of idemprimal binars

In order to prove theorem, we divide the set of nonidemprimal binars into 10 subsets and prove that the probability that each each one occurs is 0. In the next lemma, X and Y range over arbitrary subsets of A, a, b, c over elements of A and α, β over permutations of A.

Lemma 2.3.1 ([Ber12, Lem. 6.19])**.** *Let $\boldsymbol{A} = \langle A, \cdot \rangle$ be a binar of cardinality n. If $\boldsymbol{A}$ is not idemprimal, then (at least) one of the following conditions must hold.*

1. $\exists X(2 \leq |X| \leq n-1 \,\&\, X \cdot X \subseteq X)$;
2. $\exists X(3 \leq |X| \leq n-1 \,\&\, |X \cdot X| \leq |X|)$;
3. $\exists X(|X| = 2 \,\&\, |X \cdot X| = 1)$;
4. $\exists X, Y(|X| = |Y| = 2 \,\&\, X \cdot X = Y \,\&\, |Y \cdot Y| = 2)$

5. $A \cdot A \neq A$*;*

6. $\exists a, b(a \neq b \,\&\, a \cdot a = a \cdot b = b \cdot a = a)$*;*

7. $\exists X(1 \leq |X \cdot A| \leq |X| \leq n-1)$*;*

8. $\exists X(1 \leq |A \cdot X| \leq |X| \leq n-1)$*;*

9. $\exists a, b(a \neq b \,\&\, (\forall c)(a \cdot c = b \cdot c))$*;*

10. $\exists \alpha, \beta(\alpha \neq \beta \,\&\, (\forall a, b)(\alpha(a) \cdot \alpha(b) = \beta(a \cdot b)))$*.*

Proof:

Assume that $\langle A, \cdot \rangle$ is not idemprimal. Then by Lemma 2.2.2, for some $m > 0$, $\boldsymbol{A}^m$ has a proper reduced subalgebra $\boldsymbol{B}$. Choose $\boldsymbol{B}$ so as to minimize m. Since the projection of B onto any $m-1$ coordinates will still be reduced, by the minimality of m, these projections must all be isomorphic to $\boldsymbol{A}^{m-1}$. Suppose $m = 1$. Then $\boldsymbol{B}$ is a proper nontrivial subalgebra of $\boldsymbol{A}$, so (1) holds. So from now on assume that $m > 1$. For every $\boldsymbol{a} = \langle a_1, a_2, \ldots, a_{m-1} \rangle$ in A^{m-1} let

$$B(\boldsymbol{a}) = \{b \in A : \langle a_1, a_2, \ldots, a_{m-1}, b \rangle \in B\}.$$

Note that

$$B(\boldsymbol{a}) \cdot B(\boldsymbol{a}') \subseteq B(\boldsymbol{a} \cdot \boldsymbol{a}'). \tag{2.3.1}$$

Also, for every $\boldsymbol{a} \in A^{m-1}$, $B(\boldsymbol{a}) \neq \emptyset$ since B projects onto A^{m-1}. Finally, let $k = \max\{|B(\boldsymbol{a})| : \boldsymbol{a} \in A^{m-1}\}$. Let $\boldsymbol{a}$ give rise to the maximum value of k. The argument breaks into cases depending on the value of k.

Case 1. $3 \leq k \leq n-1$. Then $X = B(\boldsymbol{a})$ satisfies (2) since $B(\boldsymbol{a}) \cdot B(\boldsymbol{a}) \subseteq B(\boldsymbol{a} \cdot \boldsymbol{a})$ by (2.3.1).

Case 2. $k = 2$. Let $X = B(\boldsymbol{a})$ and let $Y = X \cdot X$. Note that $|Y| \leq |X| = 2$. If $|Y| = 1$ or $|Y \cdot Y| = 1$ then (3) holds. Otherwise, $|Y \cdot Y| = 2$, so (4) holds.

Case 3. $k = n$. Let $C = \{\boldsymbol{c} \in A^{m-1} : B(\boldsymbol{c}) = A\}$. By assumption, C is nonempty. If $C = A^{m-1}$ then $B = A^m$ which is false. So C is a proper nonempty subset of A^{m-1}. If $A \cdot A \neq A$ then (5) holds. So assume $A \cdot A = A$. It follows that C is a subuniverse of $\boldsymbol{A}^{m-1}$. For suppose that $\boldsymbol{c}$, $\boldsymbol{c}' \in C$. For any $x \in A$ there are b, $b' \in A$ such that $x = b \cdot b'$ (since $A \cdot A = A$). Thus

$$\begin{gathered}\langle c_1 \cdot c_1', c_2 \cdot c_2', \ldots, c_{m-1} \ldots c_{m-1}' \rangle = \\ \langle c_1, c_2, \ldots, c_{m-1}, b \rangle \cdot \langle c_1', c_2', \ldots, c_{m-1}', b' \rangle \in B \cdot B = B\end{gathered}$$

From the previous two paragraphs we conclude that $\boldsymbol{C}$ is a proper subalgebra of $\boldsymbol{A}^{m-1}$. By the minimality of m, $\boldsymbol{C}$ is not reduced. One of the two conditions in the definition of reduced must fail. Suppose first that condition (1) fails, i.e., for some $i \leq m-1$ we have $\vec{q}_i(C) = \{a\}$. Note that since C is a subuniverse, a must be an idempotent element. Choose $\boldsymbol{b} \in A^{m-1}$ with $b_i \neq a$ and $B(\boldsymbol{b})$ as large as possible. If $a \cdot b_i = b_i \cdot a = a$ then (6) holds. On the other hand, if $b_i \cdot a \neq a$ then (7) holds and if $a \cdot b_i \neq a$ then (8) holds. To see this, assume that $b_i \cdot a \neq a$ and let $X = B(\boldsymbol{b})$. Since $b_i \neq a$, $\boldsymbol{b} \notin C$, so $B(\boldsymbol{b}) \neq A$, and therefore $|X| < n$. Also, $X \cdot A = B(\boldsymbol{b}) \cdot B(\boldsymbol{a}) \subseteq B(\boldsymbol{b} \cdot \boldsymbol{a})$. By assumption, $b_i \cdot a \neq a$, so $\boldsymbol{b} \cdot \boldsymbol{a} \notin C$. Therefore, by the maximality of $\boldsymbol{b}$, $|X \cdot A| \leq |B(\boldsymbol{b} \cdot \boldsymbol{a})| \leq |B(\boldsymbol{b})| = |X|$. This is (7). The argument for (8) is dual. Now assume that $\boldsymbol{C}$ satisfies condition (1) but fails to be reduced because of condition (2). Thus, there are $i \neq j$ such that for all $\boldsymbol{c} \in C$, $c_i = c_j$. Since C satisfies condition (1), $|\vec{q}_i(C)| > 1$. If $|\vec{q}_i(C)| < n$ then (1) holds (C is a subuniverse of $\boldsymbol{A}^{m-1}$ so $X = \vec{q}_i(C)$ is a subuniverse of $\boldsymbol{A}$). So we assume that $\vec{q}_i(C) = \vec{q}_j(C) = A$. Pick $\boldsymbol{u} \in A^{m-1}$ with $u_i \neq u_j$ and $|B(\boldsymbol{u})|$ as large as possible. Let $a = u_i$ and $b = u_j$. If (9) fails, there is $c \in A$ with $a \cdot c \neq b \cdot c$. Pick $\boldsymbol{x} \in C$ with $x_i = c$. Then $x_j = c$ as well. Now $\boldsymbol{v} = \boldsymbol{u} \cdot \boldsymbol{x}$ has $v_i = a \cdot c \neq b \cdot c = v_j$. And therefore

$$1 \leq |B(\boldsymbol{u}) \cdot B(\boldsymbol{x})| \leq |B(\boldsymbol{u} \cdot \boldsymbol{x})| = |B(\boldsymbol{v})| \leq |B(\boldsymbol{u})|,$$

the last inequality following from the maximality of $\boldsymbol{u}$. Therefore (7) holds with $X = B(\boldsymbol{u})$ and $A = B(\boldsymbol{x})$.

Case 4. $k = 1$. Let B' be the result of transposing the last two coordinates of each element of B. If any of cases 1-3 apply to B', we are done. So we may assume that for all $\boldsymbol{a} \in A^{m-1}$, $|B'(\boldsymbol{a})| = |B(\boldsymbol{a})| = 1$. Put more explicitly

$$(\forall a_1, a_2, \ldots, a_{m-1})(\exists! b)\langle a_1, a_2, \ldots, a_{m-1}, b\rangle \in B \tag{2.3.2}$$

and for this b we have

$$\langle a_1, a_2, \ldots, a_{m-2}, b, a_{m-1}\rangle \in B' \tag{2.3.3}$$

Fix $\boldsymbol{c} = \langle c_1, c_2, \ldots, c_{m-2}\rangle \in A^{m-2}$. Because of (2.3.2), there is a map $f_{\boldsymbol{c}} : A \to A$ such that for every x, $\langle c_1, \ldots, c_{m-2}, x, f_{\boldsymbol{c}}(x)\rangle \in B$. (2.3.3) says that $f_{\boldsymbol{c}}$ is injective. Therefore by the finiteness of A, $f_{\boldsymbol{c}}$ is a permutation. Recall that B is reduced. Thus $q_{m-1} \restriction_B \neq q_m \restriction_B$. Therefore there is $\langle u_1, u_2, \ldots, u_m\rangle \in B$ with $u_{m-1} \neq u_m$. Let $\boldsymbol{u} = \langle u_1, \ldots, u_{m-2}\rangle$. Then $f_{\boldsymbol{u}}$ is not the identity. Let $\boldsymbol{y} = \boldsymbol{u} \cdot \boldsymbol{u}$, $\alpha = f_{\boldsymbol{u}}$, and $\beta = f_{\boldsymbol{y}}$. Then for every $a, b \in A$, $\langle \boldsymbol{u}, a, \alpha(a)\rangle \in B$ and $\langle \boldsymbol{u}, b, \alpha(b)\rangle \in B$, so (since B is a subuniverse) $\langle \boldsymbol{y}, a \cdot b, \alpha(a) \cdot \alpha(b)\rangle \in B$. From this last relationship we obtain $\beta(a \cdot b) = \alpha(a) \cdot \alpha(b)$, so (10) holds. [Ber12, pp. 182, 183] □

Lemma 2.3.2 ([Ber12, Lem. 6.20]). *For $c = 1, \ldots, 10$, the probability that a random binar satisfies condition (c) and not condition (2) of Lemma 2.3.1 is 0.*

Proof:

Suppose that $\boldsymbol{A}$ satisfies (1) but not (2). Then for some subset X

$$(2 \leq |X| \leq n-1 \,\&\, X \cdot X \subseteq X) \text{ but not}$$
$$(3 \leq |X| \leq n-1 \,\&\, |X \cdot X| \leq |X|).$$

Thus X must be a two-element subuniverse of $\boldsymbol{A}$. There are 16 possible Cayley tables for each X. We compute

$$\frac{|\operatorname{Alg}_n[\text{cond. (1) not (2)}]|}{|\operatorname{Alg}_n|} \leq \frac{\binom{n}{2} \cdot 16 \cdot n^{n^2-4}}{n^{n^2}} = \frac{8n(n-1)}{n^4} \to 0.$$

[Ber12, pp. 184, 185]

Clearly the probability that $\boldsymbol{A}$ satisfies condition (2) but not condition (2) is 0.

Suppose that $\boldsymbol{A}$ satisfies condition (3). There are $\binom{n}{2}$ ways to choose X but all 4 entries $x \cdot y$ where $x, y \in X$ in the Cayley table have to be equal. Therefore

$$\frac{|\operatorname{Alg}_n[\text{cond. (3)}]|}{|\operatorname{Alg}_n|} \leq \frac{\binom{n}{2} \cdot n \cdot n^{n^2-4}}{n^{n^2}} = \frac{n^2(n-1)}{2n^4} \to 0.$$

Suppose that $\boldsymbol{A}$ satisfies condition (4). We consider the case that X and Y are distinct. In case that X and Y are not distinct, the reasoning follows similar arguments. There are $\binom{n}{2}$ choices for the sets X, Y and $Y \cdot Y$ whereas $X \cdot X$ is determined by Y. Therefore

$$\frac{|\operatorname{Alg}_n[\text{cond. (4)}]|}{|\operatorname{Alg}_n|} \leq \frac{\binom{n}{2} \cdot \binom{n}{2} \cdot \binom{n}{2} \cdot 2^4 \cdot 2^4 \cdot n^{n^2-8}}{n^{n^2}} \leq \frac{32n^6}{n^8} = \frac{32}{n^2} \to 0.$$

If $\boldsymbol{A}$ satisfies (5) but not (2) then $n \leq 3$, since otherwise we may choose $a \in A - A \cdot A$ and take $X = A - \{a\}$ in condition (2). [Ber12, pp. 184, 185]

Suppose that $\boldsymbol{A}$ satisfies condition (6). There are $\binom{n}{2}$ ways to choose a and b but the entries of $a \cdot a$, $a \cdot b$ and $b \cdot a$ in the Cayley table are determined by a. Thus

$$\frac{|\operatorname{Alg}_n[\text{cond. (6)}]|}{|\operatorname{Alg}_n|} \leq \frac{\binom{n}{2} \cdot n^{n^2-3}}{n^{n^2}} = \frac{n(n-1)}{2n^3} \to 0.$$

Suppose $\boldsymbol{A}$ satisfies condition (7) but not condition (2). Then

$$(\exists X)(1 \leq |X \cdot A| \leq |X| \leq n-1) \text{ but not}$$
$$(\exists X)(3 \leq |X| \leq n-1 \,\&\, |X \cdot X| \leq |X|).$$

So the X that satisfies the first condition must have cardinality at most 2, and so must $X \cdot A$. Thus there are $\binom{n}{2} < n^2$ choices for each of those two sets. If $a \in X$ then the a-row of the Cayley table contains only two distinct values. There are 2^n choices for such a row. Therefore

$$\frac{|\operatorname{Alg}_n[\text{cond. (7) not (2)}]|}{|\operatorname{Alg}_n|} \leq \frac{n^2 \cdot n^2 \cdot 2^n \cdot 2^n \cdot n^{n^2-2n}}{n^{n^2}} = \frac{4^n}{n^{2n-4}} = \left(\frac{4}{n}\right)^n \cdot \frac{1}{n^{n-4}} \to 0.$$

Of course (8) is dual to (7).

Now assume that $\boldsymbol{A}$ satisfies (9). Thus there are $a, b \in A$ such that for all $c \in A, a \cdot c = b \cdot c$. This means the a-row and the b-row are equal. Then

$$\frac{|\operatorname{Alg}_n[\text{cond. (9)}]|}{|\operatorname{Alg}_n|} = \frac{\binom{n}{2} \cdot n^{n^2-n}}{n^{n^2}} \leq \frac{n^2}{2n^n} \to 0.$$

Finally suppose that $\boldsymbol{A}$ satisfies condition (10) of Lemma 2.3.1. Since α is not the identity, there are $a, b \in A$ with $\alpha(b) = a$ and $a \neq b$. Then for all $x \in A$

$$a \cdot x = \alpha(b) \cdot \alpha(y) = \beta(b \cdot y)$$
$$x \cdot a = \alpha(y) \cdot \alpha(b) = \beta(y \cdot b)$$

with $y = \alpha^{-1}(x)$. This means that in the Caley table, the row for a is completely determined by the row for b, and similarly for the column of a. Actually, there is one possible exception. If $\alpha(a) = b$ then $b \cdot a = \beta(a \cdot b)$. In this case one of the entries in the a-column is not determined by the b-column. There are $n!$ choices for each of α and β. Note that $n! = 2 \cdot (3 \cdot 4 \ldots n) \leq 2 \cdot n^{n-2}$. There are at most $(n-1)^2+1$ free (i.e. undetermined) squares in the Caley table. Thus we compute

$$\frac{|\operatorname{Alg}_n[\text{cond. } (10)]|}{|\operatorname{Alg}_n|} \leq \frac{(n!)^2 \cdot n^{(n-1)^2+1}}{n^{n^2}} \leq \frac{4 \cdot n^{2n-4} \cdot n^{n^2-2n+2}}{n^{n^2}} = \frac{4}{n^2} \to 0.$$

[Ber12, pp. 184, 185]

□

Lemma 2.3.3 ([Ber12, Lem. 6.21, 6.22]). *The probability that a random finite binar satisfies condition* (2) *from Lemma 2.3.1 is* 0.

Proof: Condition (2) is equivalent to the assertion

$$(\exists X, Y \subseteq A)(3 \leq |X| = |Y| \leq n-1 \,\&\, X \cdot X \subseteq Y).$$

Let $|A| = n$, $X, Y \subseteq A$, $|X| = |Y| = k$ with $3 \leq k \leq n-1$. What is the probability that $X \cdot X \subseteq Y$? There are k^2 positions in the Cayley table for the products that make up $X \cdot X$ and the probability that each falls into Y is k/n. Thus the desired probability is $(k/n)^{k^2}$. [Ber12, p. 185]

Since there are $\binom{n}{k}$ choices for each of X and Y, the probability that a random binar of cardinality n satisfies condition (2) is at most $\sum_{k=3}^{n-1} \binom{n}{k}^2 \cdot (\frac{k}{n})^{k^2}$. This expression now can be shown to converge to 0 as $n \to \infty$ using Stirling's formula (cf. [Ber12, Lem. 6.22]). □

Combining the previous Lemmata, we obtain

Theorem 2.3.4 ([Ber12, Thm. 6.23]). *The probability that a random finite binar is idemprimal is* 1.

2.4 The fraction of idemprimal and primal algebras

Proof of Theorem 2.0.1: It follows from Theorem 1.2.4 that a finite algebra is primal iff it is idemprimal and has no trivial subalgebras.

If we view the properties P, E and I as subsets of Alg_ρ, this means $P = E \cap I$.
Let $\bar{I}$ denote the complement of the set I.
Now let $\rho = \langle k \rangle$ with $k > 2$ and let $\boldsymbol{A} = \langle A, f \rangle$ be a finite algebra of type ρ. Define $x \cdot y = f(x, y, y, \ldots, y)$ and $\boldsymbol{A}_0 = \langle A, \cdot \rangle$. Then $\operatorname{Clo}(\boldsymbol{A}_0) \subseteq \operatorname{Clo}(\boldsymbol{A})$. Since

with probability 1, a randomly chosen $\boldsymbol{A}_0$ is idemprimal (i.e. $\mathrm{Clo}(\boldsymbol{A}_0)$ contains every idempotent operation on A), the same is true for a random $\boldsymbol{A}$. This proves 2.0.1(2).

Since by Theorem 2.1.1(1) $Pr_\rho(E) = 1/e$ and $E = (E \cap I)\dot{\cup}(E \cap \bar{I}) = P\dot{\cup}(E \cap \bar{I})$, we obtain

$$1/e = Pr(P) + Pr(E \cap \bar{I}) = Pr(P)$$

since $E \cap \bar{I} \subseteq \bar{I}$, which occurs with probability 0 by the previous paragraph.

Finally, if the similarity type contains at least one more operation symbol, then $1/e$ can be replaced with 1 according to Theorem 2.1.1(2). [Ber12, p. 188] □

Chapter 3

On the fraction of simple algebras

In this section we investigate the rate of convergence of the fraction of simple algebras. Clearly, since every idemprimal algebra is simple, the fraction of simple algebras is bounded from below by the fraction of idemprimal algebras. We will consider the convergence rate of the limit given in section 1.3. Denote by S the property of being simple. For a type containing at least one operation symbol of arity > 1, if we extract a bound from Murskii's proof, we obtain $f(n)$ with $P(S, \mathrm{Alg}_{\rho,n}) \geq f(n)$, where $\lim_{n\to\infty} = 1$ but $f(n) \leq 1 - 4/n^2$ for all $n \in \mathbb{N}$ [Ber12, Theorem 6.17]. In the case where there is at least one operation symbol of arity ≥ 3, we provide a lower bound with faster convergence to 1.

Theorem 3.0.1. *Let $k \geq 3$, and let ρ be a finite type that contains at least one operation symbol of arity k. Then*

$$P(S, \mathrm{Alg}_{\rho,n}) \geq 1 - \exp(-n^{k-1} + 2n^{k-2} + n\ln(n)).$$

We note that this implies that for $k \geq 3$, we have $P(S, \mathrm{Alg}_\rho) = 1$.

3.1 Preliminariy inequalities

In this section we provide the inequalities that we will need in the proof of Theorem 2.0.1.

Lemma 3.1.1. *Let $n \in \mathbb{N}$, $n > 1$ and define*

$$f_n := (1 + \tfrac{1}{n})^n, g_n := (1 + \tfrac{1}{n})^{n+1}, h_n := (1 - \tfrac{1}{n})^n, i_n := (1 - \tfrac{1}{n})^{n-2}.$$

Then $(f_n)_{n\in\mathbb{N}}$ is an increasing sequence converging to e, $(g_n)_{n\in\mathbb{N}}$ is a decreasing sequence converging to e, $(h_n)_{n\in\mathbb{N}}$ is an increasing sequence converging to $1/e$ and $(i_n)_{n\in\mathbb{N}}$ is a decreasing sequence converging to $1/e$.

Proof: It is a well known fact that the $(f_n)_{n\in\mathbb{N}}$ and $(g_n)_{n\in\mathbb{N}}$ are converging to e while $(h_n)_{n\in\mathbb{N}}$ and $(i_n)_{n\in\mathbb{N}}$ are converging to $1/e$.

We show that $(f_n)_{n\in\mathbb{N}}$ is increasing using Bernoulli's inequality:

$$\frac{f_{n+1}}{f_n} = \frac{(1+\frac{1}{n+1})^{n+1}}{(1+\frac{1}{n})^n} = \frac{n+2}{n+1}(\frac{n(n+2)}{(n+1)^2})^n = \frac{n+2}{n+1}(1-\frac{1}{(n+1)^2})^n \geq \frac{n+2}{n+1}(1-\frac{n}{(n+1)^2}) = \frac{(n+2)(n^2+n+1)}{(n+1)^3} = \frac{n^3+3n^2+3n+2}{n^3+3n^2+3n+1} > 1$$

We show that $(g_n)_{n\in\mathbb{N}}$ is decreasing:

$$\frac{g_n}{g_{n+1}} = \frac{(1+\frac{1}{n})^{n+1}}{(1+\frac{1}{n+1})^{n+2}} = (\frac{(n+1)^2}{n(n+2)})^{n+1}\frac{1}{1+\frac{1}{n+1}} = (1+\frac{1}{n^2+2n})^{n+1}\frac{1}{1+\frac{1}{n+1}} > 1$$

The above inequality holds since, using Bernoulli's inequality, we have

$$(1+\frac{1}{n^2+2n})^{n+1} \geq 1+\frac{n+1}{n^2+2n} > 1+\frac{n+1}{(n+1)^2} = 1+\frac{1}{n+1}.$$

We show that $(h_n)_{n\in\mathbb{N}}$ is increasing:

$$\frac{h_{n+1}}{h_n} = \frac{(1-\frac{1}{n+1})^{n+1}}{(1-\frac{1}{n})^n} = \frac{(\frac{n}{n+1})^{n+1}}{(\frac{n-1}{n})^n} = \frac{\frac{n(1-\frac{1}{n})+1}{n+1}}{((1-\frac{1}{n})^n\cdot 1)^{\frac{1}{n+1}}} > 1$$

Here we have used the inequality of arithmetic and geometric means.

It remains to show that $(i_n)_{n\in\mathbb{N}}$ is decreasing:

$$\frac{i_n}{i_{n+1}} = \frac{(1-\frac{1}{n})^{n-2}}{(1-\frac{1}{n+1})^{n-1}} = \frac{(\frac{n-1}{n})^{n-2}}{(\frac{n}{n+1})^{n-1}} = \frac{n+1}{n}(\frac{n^2-1}{n^2})^{n-2} = \frac{n+1}{n}(1-\frac{1}{n^2})^{n-2} \geq \frac{n+1}{n}(1-\frac{n-2}{n^2}) = \frac{n+1}{n}\frac{n^2-n+2}{n^2} = \frac{n^3+n+2}{n^3} > 1$$

Here we have again used Bernoulli's inequality. □

Lemma 3.1.2. *For $n \in \mathbb{N}$, let $f_n := (\frac{n}{e}+1)^{\frac{n}{e}} n^{n-\frac{n}{e}-1}(n-1)^{2-n}$. Then $(f_n)_{n\geq 7}$ is decreasing.*

Proof: We want to show that for $n \geq 7$, $f_n \geq f_{n+1}$, i.e.:

$$(\frac{n}{e}+1)^{\frac{n}{e}} n^{n-\frac{n}{e}-1}(n-1)^{2-n} \geq (\frac{n+1}{e}+1)^{\frac{n+1}{e}}(n+1)^{n-\frac{n+1}{e}} n^{1-n}$$

or equivalently

$$\frac{(\frac{n}{e}+1)^{\frac{n}{e}}}{(\frac{n+1}{e}+1)^{\frac{n+1}{e}}} \cdot \frac{n^{n-\frac{n}{e}-1}}{(n+1)^{n-\frac{n+1}{e}}} \cdot \frac{(n-1)^{2-n}}{n^{1-n}} \geq 1.$$

We can find a lower bound for the first factor, since

$$\frac{(\frac{n}{e}+1)^{\frac{n}{e}}}{(\frac{n+1}{e}+1)^{\frac{n+1}{e}}} = \frac{(\frac{n}{e}+1)^{\frac{n}{e}}}{(\frac{n+1}{e}+1)^{\frac{n}{e}}(\frac{n+1}{e}+1)^{\frac{1}{e}}} = (\frac{n+1}{e}+1)^{-\frac{1}{e}}(\frac{\frac{n}{e}+1+\frac{1}{e}}{\frac{n}{e}+1})^{-\frac{n}{e}} =$$
$$(\frac{n+1}{e}+1)^{-\frac{1}{e}}(1+\frac{1}{e(\frac{n}{e}+1)})^{-\frac{n}{e}} \geq (\frac{n+1}{e}+1)^{-\frac{1}{e}}(1+\frac{1}{n})^{-\frac{n}{e}}.$$

For the second factor we have

$$\frac{n^{n-\frac{n}{e}-1}}{(n+1)^{n-\frac{n+1}{e}}} = \frac{n^{-1}n^{n-\frac{n}{e}}}{(n+1)^{-\frac{1}{e}}(n+1)^{n-\frac{n}{e}}} = n^{-1}(n+1)^{\frac{1}{e}}(\frac{n}{n+1})^{n-\frac{n}{e}} =$$
$$n^{-1}(n+1)^{\frac{1}{e}}(1+\frac{1}{n})^{-n}(1+\frac{1}{n})^{\frac{n}{e}} \geq n^{-1}(n+1)^{\frac{1}{e}}\frac{1}{e}(1+\frac{1}{n})^{\frac{n}{e}}\ .$$

And for the third factor we get

$$\frac{(n-1)^{2-n}}{n^{1-n}} = n(\frac{n-1}{n})^{2-n} = n\frac{1}{(1-\frac{1}{n})^{n-2}} \geq n\frac{1}{(1-\frac{1}{7})^{5}} = (\frac{7}{6})^5 n,$$

since $(1-\frac{1}{n})^{n-2}$ is decreasing and $n \geq 7$.

Thus for the product we have

$$\frac{(\frac{n}{e}+1)^{\frac{n}{e}}}{(\frac{n+1}{e}+1)^{\frac{n+1}{e}}} \cdot \frac{n^{n-\frac{n}{e}-1}}{(n+1)^{n-\frac{n+1}{e}}} \cdot \frac{(n-1)^{2-n}}{n^{1-n}} \geq$$
$$(\frac{n+1}{e}+1)^{-\frac{1}{e}}(1+\frac{1}{n})^{-\frac{n}{e}} \cdot n^{-1}(n+1)^{\frac{1}{e}}\frac{1}{e}(1+\frac{1}{n})^{\frac{n}{e}} \cdot (\frac{7}{6})^5 n = (\frac{7}{6})^5\frac{1}{e}(n+1)^{\frac{1}{e}}(\frac{n+1}{e}+1)^{-\frac{1}{e}} =$$
$$(\frac{7}{6})^5\frac{1}{e}(\frac{n+1}{\frac{n+1}{e}+1})^{\frac{1}{e}} = (\frac{7}{6})^5\frac{1}{e}(\frac{e(n+1)}{(n+1)+e})^{\frac{1}{e}} = (\frac{7}{6})^5\frac{1}{e}e^{1/e}(\frac{n+1}{n+1+e})^{1/e}.$$

Clearly $\frac{n+1}{n+1+e}$ is converging to 1 increasingly as $n \to \infty$ and so is $(\frac{n+1}{n+1+e})^{1/e}$, and thus $(\frac{n+1}{n+1+e})^{1/e} \geq (\frac{8}{8+e})^{\frac{1}{e}}$ for $n \geq 7$. Hence

$$(\frac{7}{6})^5 e^{-1}e^{1/e}(\frac{n+1}{n+1+e})^{1/e} \geq (\frac{7}{6})^5 e^{-1}e^{1/e}(\frac{8}{8+e})^{\frac{1}{e}} \geq 1.03 > 1.$$

□

Lemma 3.1.3. *Let $n \in \mathbb{N}$ with $n \geq 3$, and for $m \in \{2, \dots, n-1\}$, let $a_m := m^{m-1}n^{n-m+1}$. Then for all $m \in \{2, \dots, n-1\}$, we have $a_m \leq a_{n-1} = n^2(n-1)^{n-2}$.*

Proof: We proof the statement distinguishing between three cases:

Case: $m \leq n/e$: Then $n/m \geq e$. Since $(1+\frac{1}{m})^m$ is an increasing sequence converging to e, we have $\frac{n}{m} \geq (\frac{m+1}{m})^m$. Thus $nm^{m-1} \geq (m+1)^m$ and hence $nm^{m-1}n^{n-m} \geq (m+1)^m n^{n-m}$. But then $a_m = m^{m-1}n^{n-m+1} \geq (m+1)^{(m+1)-1}n^{n-(m+1)+1} = a_{m+1}$. Thus (a_m) is decreasing for $2 \leq m \leq n/e$, i.e. $a_2 = 2n^{n-1} \geq a_m$ in this interval. We now show that for $n \geq 3$, $a_2 \leq a_{n-1}$, i.e.: $2n^{n-1} \leq n^2(n-1)^{n-2}$ or equivalently $2 \leq n(\frac{n-1}{n})^{n-2}$. For $3 \leq n \leq 5$ it can be seen easily that the inequality holds. Therefore, let $n \geq 6$. Since $(\frac{n-1}{n})^{n-2}$ converges to $1/e$ monotonically decreasing, $n(\frac{n-1}{n})^{n-2} \geq \frac{n}{e} \geq 6/e > 2$.

Case: $m \geq n/e+1$: Then $n/m \leq e(\frac{m-1}{m})$. Since $(\frac{m+1}{m})^{m+1}$ is a decreasing sequence converging to e, we can write

$$\tfrac{n}{m} \leq e(\tfrac{m-1}{m}) \leq (\tfrac{m+1}{m})^{m+1}(\tfrac{m-1}{m}) = (\tfrac{m+1}{m})^{m}(\tfrac{m^2-1}{m^2}) \leq (\tfrac{m+1}{m})^{m}.$$

Therefore, proceeding as in the previous case, we obtain $a_m = m^{m-1}n^{n-m+1} \leq (m+1)^{(m+1)-1}n^{n-(m+1)+1} = a_{m+1}$. Thus (a_m) is increasing in this interval and hence $\leq a_{n-1}$.

Case: $n/e < m < n/e+1$: For $3 \leq n \leq 11$ it can be checked easily that $a_m \leq a_n$. Therefore, let $n \geq 12$. Since $n/e < m < n/e+1$,

$$a_m = m^{m-1}n^{n-m+1} \leq (\tfrac{n}{e}+1)^{(\frac{n}{e}+1)-1}n^{n-\frac{n}{e}+1} = (\tfrac{n}{e}+1)^{\frac{n}{e}}n^{n-\frac{n}{e}+1}.$$

We want to show that $(\frac{n}{e}+1)^{\frac{n}{e}}n^{n-\frac{n}{e}+1} \leq n^2(n-1)^{n-2} = a_{n-1}$ or equivalently $(\frac{n}{e}+1)^{\frac{n}{e}}n^{n-\frac{n}{e}-1}(n-1)^{2-n} =: f_n \leq 1$.

By Lemma 3.1.2, we know that $(f_n)_{n\geq 7}$ is decreasing. Thus, since $f_{12} < 1$, $f_n < 1$ for $n \geq 12$. □

For our purposes, the following rough estimation of the Bell number will be sufficient.

Lemma 3.1.4. *There are at most $n!$ possible partitions of an n-element set.*

Proof: Consider the mapping $\mu : S_n \to P_n$ from the symmetric group of an n-element set to the set of partitions of an n-element set, where a cycle decomposition is mapped to the corresponding set of subsets

$$(\sigma_1), \ldots, (\sigma_k) \mapsto \{\{\sigma_1\}, \ldots, \{\sigma_k\}\}.$$

Since μ is obviously surjective, $|P_n| \leq |S_n| = n!$. □

3.2 The fraction of simple algebras

Proof of Theorem 2.0.1: Obviously every one or two-element algebra is simple and thus we we can restrict ourselves to the case $n \geq 3$. Let $k \in \mathbb{N}$ and let ρ be a finite type containing at least one operation symbol of arity k. Thus for $m \in \mathbb{N}$ and finitary operation symbols $f_1, \ldots, f_m$, we can write $\rho = \{f_1, \ldots, f_m\}$ and we assume that $\text{arity}(f_1) = k$.
In order to prove the statement of the theorem, we will show that $P(\neg S, \text{Alg}_{\rho,n}) \leq \exp(-n^{k-1} + 2n^{k-2} + n\ln(n))$. To this end, we call an algebra $\boldsymbol{A} \in \text{Alg}_{\rho,n}$ ρ-admissible if and only if its operations preserve a nontrivial equivalence relation.

We denote the number of ρ-admissible algebras by $N(\rho) = N(f_1, \ldots, f_m)$. Clearly, if $\boldsymbol{A}$ is ρ-admissible, then for every $f_i \in \rho$, $\langle A, f_i \rangle$ is $\{f_i\}$-admissible. Thus

$$N(f_1, \ldots, f_m) \leq N(f_1) \cdot \cdots \cdot N(f_m) \leq N(f_1) \prod_{i=2}^{m} n^{n^{\mathrm{ar}(f_i)}}.$$

Hence for the fraction of such tables we get

$$\frac{N(f_1, \ldots, f_m)}{|\mathrm{Alg}_{\rho,n}|} = \frac{N(f_1, \ldots, f_m)}{\prod_{i=1}^{m} n^{n^{\mathrm{ar}(f_i)}}} \leq \frac{N(f_1) \prod_{i=2}^{m} n^{n^{\mathrm{ar}(f_i)}}}{\prod_{i=1}^{m} n^{n^{\mathrm{ar}(f_i)}}} = \frac{N(f_1)}{n^{n^k}}.$$

Therefore we may restrict ourselves to the case that ρ contains only one single k-ary operation symbol f.

Fix a nontrivial equivalence relation θ on A. How many algebras in $\mathrm{Alg}_{\rho,n}$ preserve θ? Since A/θ is a partition of A, there are $l \in \mathbb{N}$ with $1 \leq l \leq n$ and some disjoint $A_i \in \mathcal{P}(A)$ with $\bigcup_{i=1}^{l} A_i = A$ such that we can write $A/\theta = \{A_1, \ldots, A_l\}$. Fix $1 \leq i \leq l$ and $(\alpha_1, \ldots, \alpha_{k-1}) \in \{1, \ldots, n\}^{k-1}$ and let $a, b \in A_i$ (i.e. $a\theta b$). If f preserves θ, we have $f(a, \alpha_1, \ldots, \alpha_{k-1})\theta f(b, \alpha_1, \ldots, \alpha_{k-1})$ and hence for some $1 \leq j \leq l$, $f(a, \alpha_1, \ldots, \alpha_{k-1}), f(b, \alpha_1, \ldots, \alpha_{k-1}) \in A_j$. Thus there are

$$\sum_{j=1}^{l} |A_j|^{|A_i|}$$

ways to choose all values of $f(a_, \alpha_1, \ldots, \alpha_{k-1})$ where $a \in A_i$. Since this can be done for every $1 \leq i \leq l$, there are

$$\prod_{i=1}^{l} \sum_{j=1}^{l} |A_j|^{|A_i|}$$

ways to choose the values of $f(a, \alpha_1, \ldots, \alpha_{k-1})$ with $a \in A$. Hence there are at most

$$\prod_{\alpha \in \{1,\ldots,n\}^{k-1}} \prod_{i=1}^{l} \sum_{j=1}^{l} |A_j|^{|A_i|} = (\prod_{i=1}^{l} \sum_{j=1}^{l} |A_j|^{|A_i|})^{n^{k-1}} \tag{3.2.1}$$

algebras in $\mathrm{Alg}_{\rho,n}$ preserving θ. We will now find an upper bound for (3.2.1). Let $m := \max\{|A_i| : A_i \in A/\theta\}$. Then

$$\sum_{j=1}^{l} |A_j|^{|A_i|} \leq \sum_{j=1}^{l} |A_j| m^{|A_i|-1} = m^{|A_i|-1} \sum_{j=1}^{l} |A_j| = nm^{|A_i|-1}.$$

Thus

$$\prod_{i=1}^{l} \sum_{j=1}^{l} |A_j|^{|A_i|} \leq \prod_{i=1}^{l} nm^{|A_i|-1} = n^l m^{\sum\limits_{i=1}^{l} |A_i| - l} = n^l m^{n-l}.$$

Since l is the number of equivalence classes and m the size of the equivalence class of maximal cardinality in A/θ, clearly $1 \leq l \leq n - m + 1$ and hence $n^l m^{n-l} \leq n^{n-m+1} m^{m-1}$. Since θ is neither Δ_A nor ∇_A, we have $2 \leq m \leq n - 1$. Thus Lemma 3.1.3 yields $n^{n-m+1} m^{m-1} \leq n^2(n-1)^{n-2}$, and hence the number of algebras in $\mathrm{Alg}_{\rho,n}$ preserving θ is bounded from above by $(n^2(n-1)^{n-2})^{n^{k-1}}$.

Since every equivalence relation can be identified with its corresponding partition, by Lemma 3.1.4 there are at most $n! \leq n^n$ choices for θ. For every such θ we have at most $(n^2(n-1)^{n-2})^{n^{k-1}}$ algebras preserving it and hence in total there are at most $n^n(n^2(n-1)^{n-2})^{n^{k-1}}$ algebras in $\mathrm{Alg}_{\rho,n}$ admitting a nontrivial congruence relation. Since the number of all possible algebras is n^{n^k}, we are interested in the fraction

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

which is an upper bound for $P(\neg S, \mathrm{Alg}_{\rho,n})$, the fraction of n-element non-simple algebras of type ρ. Using the fact that $(1 - \frac{1}{n})^n$ converges to $1/e$ monotonically increasing, we get

$$P(\neg S, \mathrm{Alg}_{\rho,n}) \leq \frac{n^n(n^2(n-1)^{n-2})^{n^{k-1}}}{n^{n^k}} = n^n \frac{(n-1)^{(n-2)n^{k-1}}}{n^{(n-2)n^{k-1}}} = n^n(\tfrac{n-1}{n})^{(n-2)n^{k-1}} =$$
$$n^n((1 - \tfrac{1}{n})^n)^{(n-2)n^{k-2}} \leq n^n e^{(2-n)n^{k-2}} = e^{-n^{k-1}+2n^{k-2}+n\ln(n)}.$$

Thus $P(S, \mathrm{Alg}_{\rho,n}) \geq 1 - \exp(-n^{k-1} + 2n^{k-2} + n\ln(n))$, and hence for $k > 2$ converges to 1 as $n \to \infty$. □

Chapter 4

About the two kinds of probability in algebra

The probability measure we have defined in section 1.3 counts every single algebra of a specific type having a certain property. Now one could propose a different kind of probability measure counting algebras only up to isomorphism instead. In [Fre90], R. Freese investigated these two concepts of probability, showing that they are closely related to each other. Verbatim quotes from the literature will be identified as such by indentation and using a smaller font.

4.1 Labeled and unlabeled probability

Let $\mathcal{K}_n$ be a finite, nonempty set of algebras with universe $\{0, \dots, n-1\}$ and define $\mathcal{K} = \bigcup_{n \in \mathbb{N}} \mathcal{K}_n$. Freese defined the probability of a property P in $\mathcal{K}$ as

$$\begin{gathered} Pr(P; \mathcal{K}) = \lim_{n \to \infty} Pr(P; \mathcal{K}_n), \text{ where} \\ Pr(P, \mathcal{K}_n) = \tfrac{|\{\boldsymbol{A} \in \mathcal{K}_n : A \models P\}|}{|\mathcal{K}_n|} \end{gathered}$$

if this limit exists.

For a finite similarity type τ, denote by $\mathcal{T}(\tau)$ the set of all finite algebras of type τ and by $\mathcal{A}(\tau)$ the set of all isomorphism classes of finite algebras of type τ. Then $Pr(P, \mathcal{T}(\tau))$ is called the *labeled* and $Pr(P, \mathcal{A}(\tau))$ the *unlabeled* probability of a property P.

In his proofs, Freese uses some basic and well known concepts from probability theory. For a random variable X on a class $\mathcal{K}$ of algebras (i.e. a function $\mathcal{K} \to \mathbb{R}$), he defined the expected value of X as

$$E(X;\mathcal{K}) = \lim_{n\to\infty} \frac{\sum_{\boldsymbol{A}\in\mathcal{K}_n} X(\boldsymbol{A})}{|\mathcal{K}_n|}.$$

4.2 Relations between the two kinds of probability

Theorem 4.2.1 ([Fre90, Thm. 1]). *Let τ be a similarity type and let $X(\boldsymbol{T}) = |\operatorname{Aut}(\boldsymbol{T})|$ for $\boldsymbol{T} \in \mathcal{T}(\tau)$. Let P be an algebraic property. If $E(X; T(\tau)) = 1$ then if either $Pr(P;\mathcal{T}(\tau))$ or $Pr(P;\mathcal{A}(\tau))$ exists then both exist and are equal.*

Proof:

> Let $\boldsymbol{T} \in \mathcal{T}_n$ and let $\sigma \in \boldsymbol{S}_n$, the full symmetric group on $\{0, 1, \ldots, n-1\}$. For each fundamental operation f of $\boldsymbol{T}$, we define an operation f^σ on the same set by
>
> $$f^\sigma(x_0,\ldots,x_{n-1}) = \sigma^{-1}(f(\sigma(x_0),\ldots,\sigma(x_{n-1}))))$$
>
> Let $\boldsymbol{T}^\sigma$ be the algebra with these operations. Then σ is an isomorphism from $\boldsymbol{T}$ onto $\boldsymbol{T}^\sigma$. Notice that $\boldsymbol{T}^\sigma = \boldsymbol{T}$ if and only if $\sigma \in \operatorname{Aut}\boldsymbol{T}$. [Fre90, p. 3]

The following equality holds if and only if $\exists\alpha \in \operatorname{Aut}\boldsymbol{T}$ such that $\sigma_2 = \alpha\circ\sigma_1$, i.e. $\sigma_1 \backsim_{\operatorname{Aut}\boldsymbol{T}} \sigma_2$ or equivalently $\operatorname{Aut}\boldsymbol{T}\circ\sigma_1 = \operatorname{Aut}\boldsymbol{T}\circ\sigma_2$.

$$\begin{gathered} f^{\sigma_2}(x_0,\ldots,x_{n-1}) = f^{\alpha\circ\sigma_1}(x_0,\ldots,x_{n-1}) = \\ (\alpha\circ\sigma_1)^{-1} f((\alpha\circ\sigma_1)(x_0),\ldots,(\alpha\circ\sigma_1)(x_{n-1})) = \\ \sigma_1^{-1}\circ\alpha^{-1} f(\alpha(\sigma_1(x_0)),\ldots,\alpha(\sigma_1(x_{n-1}))) = \sigma_1^{-1} f^\alpha(\sigma_1(x_0),\ldots,\sigma_1(x_{n-1})) = \\ \sigma_1^{-1} f(\sigma_1(x_0),\ldots,\sigma_1(x_{n-1})) = f^{\sigma_1}(x_0,\ldots,x_{n-1}). \end{gathered}$$

Thus the number of distinct $\boldsymbol{T}' \in \mathcal{T}_n$ isomorphic to $\boldsymbol{T}$ is exactly the index (i.e. the number of cosets) of **Aut T** in $\boldsymbol{S}_n$. Applying Lagrange's theorem, we get

$$|\{\boldsymbol{T}' \in \mathcal{T}_n : \boldsymbol{T}' \cong \boldsymbol{T}| = [\boldsymbol{S}_n : \mathbf{Aut\ T}] = \frac{n!}{|\operatorname{Aut}\boldsymbol{T}|}. \qquad (4.2.1)$$

> Now using this we can calculate $\sum_{\boldsymbol{T}\in\mathcal{T}_n} |\operatorname{Aut}\boldsymbol{T}|$ by summing $|\operatorname{Aut}\boldsymbol{A}|$ over $\boldsymbol{A} \in \mathcal{A}_n$ multiplied by the number of tables corresponding to $\boldsymbol{A}$ and obtain the following usefull formula.
>
> $$\sum_{\boldsymbol{T}\in\mathcal{T}_n} |\operatorname{Aut}\boldsymbol{T}| = |\mathcal{A}_n| n! \qquad (4.2.2)$$
>
> For a class of algebras $\mathcal{K}$, let $\mathcal{K}[P] = \{\boldsymbol{A} \in \mathcal{K} : \boldsymbol{A} \vDash P\}$. The isomorphism relation divides $\mathcal{T}_n$ into classes and each of this classes contains at most $n!$ elements. Hence $n!|\mathcal{A}_n[P]| \geq |\mathcal{T}_n[P]|$. Using this and (4.2.2) we see

$$\frac{|\mathcal{A}_n[P]|}{|\mathcal{A}_n|} \geq \frac{|\mathcal{T}_n[P]|/n!}{|\mathcal{A}_n|} = \frac{\mathcal{T}_n[P]|/n!}{(|\mathcal{T}_n|/n!)(1/|\mathcal{T}_n|)\sum|\mathrm{Aut}\,\boldsymbol{T}|} = \frac{|\mathcal{T}_n[P]|}{|\mathcal{T}_n|}\frac{1}{E(X;\mathcal{T}_n)} \tag{4.2.3}$$

Thus

$$Pr(P;\mathcal{A}_n) \geq \frac{1}{E(X;\mathcal{T}_n)}Pr(P;\mathcal{T}_n) \tag{4.2.4}$$

This same inequality applies to $Q = \neg P$, the logical negation of P. Using this and the fact that $Pr(Q) = 1 - Pr(P)$, we obtain the following formulae, where $E_n = E(X;\mathcal{T}_n)$.

$$\frac{1}{E_n}Pr(P;\mathcal{T}_n) \leq Pr(P,\mathcal{A}_n) \leq \frac{1}{E_n}(Pr(P,\mathcal{T}_n) + E_n - 1) \tag{4.2.5}$$

$$E_nPr(P;\mathcal{A}_n) - (E_n - 1) \leq Pr(P;\mathcal{T}_n) \leq E_nPr(P;\mathcal{A}_n) \tag{4.2.6}$$

Now the theorem follows easily from this inequalities. [Fre90, p. 3]

□

The above theorem basically states that the two kinds of probability coincide if the expected value of the number of automorphisms of finite algebras of type τ is 1 (i.e. only the trivial automorphism).

In the next theorem, Freese also provides a very useful condition when this is the case.

Theorem 4.2.2 ([Fre90, Thm. 2])**.** *If the similarity type τ contains an operation symbol of rank at least 2, or if it has at least three unary operation symbols, then*

$$E(X;T(\tau)) = 1$$

where $X(\boldsymbol{T}) = |\,\mathrm{Aut}(\boldsymbol{T})|$.

Proof:

For $\sigma \in \boldsymbol{S}_n$ let X_σ be the indicator random variable defined by

$$X_\sigma(\boldsymbol{T}) := \begin{cases} 1 & \text{if } \sigma \in \mathrm{Aut}\,\boldsymbol{T} \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$X = \sum_{\sigma \in \boldsymbol{S}_n} X_\sigma.$$

First assume that the similarity type τ contains an operation symbol f of arity k where k is at least 2. In the proof we will now give we assume that τ has only the operation symbol f. The proof in the general case is the same except that the size of all sets in question gets multiplied by a constant. Of course quotients of such sizes will be the same. If $\sigma \in \boldsymbol{S}_n$, let $c_i(\sigma)$ be the number of cycles of length i in the decomposition of σ into disjoint cycles and let $c(\sigma)$ be the total number of cycles in this decomposition, counting 1-cycles, i.e., $c(\sigma) = \sum_{i=1}^{n} c_i(\sigma)$. Notice that if $c(\sigma) = n$ then σ is the identity permutation and that if $c(\sigma) = n-1$ then σ is a transposition, i.e., it interchanges two numbers and fixes the others.

Now suppose that $\sigma \in \operatorname{Aut} \boldsymbol{T}$ for $\boldsymbol{T} \in \mathcal{T}_n(\tau)$ and that i and j are in the same orbit of σ. Then the values of $f(i, x_2, \ldots, x_k)$, where $0 \leq x_i < n$ for $i = 2, \ldots, k$ determine the values $f(j, y_2, \ldots, y_k)$. From this we see that

$$|\{\boldsymbol{T} \in \mathcal{T}_n : \sigma \in \operatorname{Aut} \boldsymbol{T}\}| \leq n^{c(\sigma)n^{k-1}} \tag{4.2.7}$$

We can write $\mathcal{T}_n = \mathcal{T}_n' \cup \mathcal{T}_n'' \cup \mathcal{T}_n'''$ where $\mathcal{T}_n'$ is the set of those members of $\mathcal{T}_n$ with trivial automorphism group, $\mathcal{T}_n''$ are those whose automorphism group contains only a transposition and the identity, and $\mathcal{T}_n'''$ are those whose automorphism group contains a nonidentity element which is not a transposition. Now using (4.2.7) and this decomposition, we have

$$1 \leq \frac{1}{|\mathcal{T}_n|} \sum_{\boldsymbol{T} \in \mathcal{T}_n} |\operatorname{Aut} \boldsymbol{T}| \leq \frac{|\mathcal{T}_n'|}{n^{n^k}} + \frac{2\binom{n}{2} n^{(n-1)n^{k-1}}}{n^{n^k}} + \frac{n! n! n^{(n-2)n^{k-1}}}{n^{n^k}}. \tag{4.2.8}$$

The second term corresponds to $\mathcal{T}_n''$ and $\binom{n}{2}$ is the number of transpositions in $\boldsymbol{S}_n$. In the last term we have used $|\operatorname{Aut} \boldsymbol{T}| \leq n!$. Now the first term is at most 1 and it is easy to see that the second and third terms tend to 0 as $n \to \infty$. Hence $E(X; \mathcal{T}(\tau)) = 1$, as desired. Thus we may assume that τ has only unary operation symbols.

Assume that the similarity type contains r unary operations, $r \geq 3$ and no other operation symbols. Suppose that $\sigma \in \operatorname{Aut} \boldsymbol{T}$ and that f is a basic unary operation of $\boldsymbol{T}$. Let $x \in T = \{0, 1, \ldots, n-1\}$ lie in a cycle of lenght k in the unique cycle decomposition of σ into disjoint cycles. Then $f(x)$ must lie in a cycle of length i, for some $i | k$. The values of f on the elements of the cycle containing x are determined by $f(x)$. Moreover, the values of f on distinct cycles are independent. It follows from this that if $c_i(\sigma)$ is the number of cycles of σ of length i, then

$$E(X_\sigma; \mathcal{T}_n(\tau)) = \tfrac{1}{n^{rn}} \prod_{k=1}^{n} (\sum_{i|k} i c_i(\sigma))^{r c_k(\sigma)}.$$

The cycle structure of σ is determined by the vector of the cycle lengths,

$$\langle c_1(\sigma), c_2(\sigma), \ldots, c_n(\sigma) \rangle.$$

The entries of this vector are nonnegative integers and satisfy $\sum i c_i(\sigma) = n$. If $\bar{j} = \langle j_1, j_2, \ldots, j_n \rangle$ is a vector of nonnegative integers satisfying $\sum i j_i = n$, then the number of elements of S_n with this cycle structure is

$$\frac{n!}{j_1! j_2! \ldots j_n! 1^{j_1} 2^{j_2} \ldots n^{j_n}}.$$

Hence

$$E(X; \mathcal{T}_n(\tau)) = \frac{1}{n^{rn}} \sum_{\bar{j}} \frac{n!}{j_1! j_2! \ldots j_n! 1^{j_1} 2^{j_2} \ldots n^{j_n}} \prod_{k=1}^{n} (\sum_{i|k} i j_i)^{r j_k}. \tag{4.2.9}$$

The term in the sum corresponding to $\bar{j} = \langle n, 0, \ldots, 0\rangle$ is 1, reflecting the fact that the identity permutation is an automorphism of every algebra. The term corresponding to $\bar{j} = \langle n-2, 1, 0, \ldots, 0\rangle$, i.e., to a permutation which is a single transposition, is

$$\tfrac{1}{n^{rn}} \tfrac{n!}{(n-2)!2}(n-2)^{r(n-2)} n^r \leq \tfrac{1}{n^{rn}} \tfrac{n^2}{2} n^{r(n-2)} n^r = \tfrac{1}{2n^{r-2}}.$$

Since $r \geq 3$, this term goes to 0, as $n \to \infty$.
In each of the remaining terms j_1 has the form $j_1 = n - t$, for $t = 3, \ldots, n$. The number of $\sigma \in \boldsymbol{S}_n$ with $c_1(\sigma) = n - t$ is at most $\binom{n}{n-t} t!$. Moreover, $\sum_{i|k} ij_i \leq n$ and $\sum_{i=2}^n j_i \leq t/2$. From this it follows that the sum of the remaining terms is bounded above by

$$\frac{1}{n^{rn}} \sum_{t=3}^{n} \binom{n}{n-t} t! (n-t)^{r(n-t)} n^{rt/2}. \tag{4.2.10}$$

Now the t^{th} term of this sum is

$$\tfrac{1}{n^{rn}} \tfrac{n!}{(n-t)!} (n-t)^{r(n-t)} n^{rt/2} \leq \tfrac{1}{n^{rn}} n^t n^{r(n-t)} n^{rt/2} = \tfrac{1}{n^{t(r/2-1)}} \leq \tfrac{1}{n^{3/2}},$$

since $t \geq 3$ and $r \geq 3$. Thus (4.2.10) is at most $n(1/n^{3/2}) = 1/n^{1/2} \to 0$ as $n \to \infty$. Thus $E(X; \mathcal{T}(\tau)) = 1$, as desired. [Fre90, pp. 4,5] □

The requirements on the similarity type in Theorem 4.2.2 can not be loosened.

Theorem 4.2.3 ([Fre90, Thm. 3])**.** *If the similarity type τ consists of of two unary operation symbols and nothing else, then*

$$E(X; \mathcal{T}(\tau)) = e^{1/(2e^4)} = 1.009\ldots$$

where $X(\boldsymbol{T}) = |\operatorname{Aut}(\boldsymbol{T})|$.

Proof:

As in the last theorem,

$$E(X; \mathcal{T}_n(\tau)) = \frac{1}{n^{2n}} \sum_{\bar{j}} \frac{n!}{j_1! j_2! \ldots j_n! 1^{j_1} 2^{j_2} \ldots n^{j_n}} \prod_{k=1}^{n} (\sum_{i|k} ij_i)^{2j_k}. \tag{4.2.11}$$

summed over all $\bar{j} = \langle j_1, \ldots, j_n\rangle$ with $\sum_{i=1}^n ij_i = n$.
Consider the contribution to the sum of terms of the form $j_1 = n-t, j_2 = t/2, j_i = 0$, for $i > 2$, where $0 \leq t < n$ and t is even. These correspond to permutations of order 2 consisting of exactly $t/2$ transpositions. (It is easy to see that the term for $t = n$ gives a contribution which goes to 0 as $n \to \infty$.) These terms give

$$\sum_{t=0,\, t\,\text{even}}^{n-1} \tfrac{1}{n^{2n}} \tfrac{n!}{(n-t)!} \tfrac{1}{(t/2)! 2^{t/2}} (n-t)^{2(n-t)} n^t =$$
$$\sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \tfrac{1}{n^{2n}} \tfrac{n!}{(n-2k)!} \tfrac{1}{k! 2^k} (n-2k)^{2(n-2k)} n^{2k}$$

$$= \sum_{k=0}^{\lfloor\frac{n-1}{2}\rfloor} \frac{1}{k!2^k} \left[\Big(\frac{n-2k}{n}\Big)^{2n} \frac{n^{2k}}{(n-2k)^{2k}} \frac{n(n-1)\dots(n-2k+1)}{(n-2k)^{2k}} \right] \tag{4.2.12}$$

Let $a_k(n)$ be the term in the square brackets in (4.2.12) provided that $k \le (n-1)/2$ and let $a_k(n) = 0$ otherwise. Thus we wish to evaluate

$$\lim_{n\to\infty} \sum_{k=0}^{\infty} \frac{1}{k!2^k} a_k(n) \tag{4.2.13}$$

Notice that $a_k(n) \le 1$, for all n and k. Thus the above sum is bounded by $e^{1/2}$. Hence we can interchange the limit and the sum. Now clearly, for k fixed,

$$\lim_{n\to\infty} \tfrac{n^{2k}}{(n-2k)^{2k}} \tfrac{n(n-1)\dots(n-2k+1)}{(n-2k)^{2k}} = 1$$

Thus $\lim_{n\to\infty} a_k(n) = (1/e^4)^k$. From this it follows that (4.2.13) evaluates to $e^{1/(2e^4)}$. Thus to complete the proof we need to show that the contribution of the other terms goes to 0 as $n \to \infty$.

Consider $\bar{j}$ with $j_1 = n-t, j_2 = \frac{t-3}{2}, j_3 = 1$, and $j_i = 0$ for $i > 3$, where $t \ge 3$ and odd. The contribution of these terms to (11) is

$$\sum_{t=3,\,t\,\mathrm{odd}}^{n} \tfrac{1}{n^{2n}} \tfrac{n!}{(n-t)!(\frac{t-3}{2})!2^{\frac{t-3}{2}}3} (n-t)^{2n-2t}(n-3)^{(t-3)}(n-t+3)^2 \le$$
$$\sum_{t=3,\,t\,\mathrm{odd}}^{n} \tfrac{1}{(\frac{t-3}{2})!2^{\frac{t-3}{2}}3} \tfrac{n^t}{n^t} \tfrac{(n-t)^{2n-2t}}{n^{2n-2t}} \tfrac{(n-3)^{t-3}}{n^t} (n-t+3)^2 \le \tfrac{1}{3n} \sum_{t=3,\,t\,\mathrm{odd}}^{n} \tfrac{1}{(\frac{t-3}{2})!2^{\frac{t-3}{2}}} \le$$
$$\tfrac{1}{3n} \sum_{k=0}^{\infty} \tfrac{1}{k!2^k} = \tfrac{1}{3n} e^{1/2}.$$

Thus the contribution of these terms tends to 0 as $n \to \infty$.

Now let $\bar{j}$ be arbitrary with $j_1 = n-t$. As noted above, there are at most $n!/(n-t)!$ such $\bar{j}$. Since $\sum_{i=1}^{n} ij_i = n$ and $\sum_{i=2}^{n} ij_i = t$, the contribution of all such terms to the sum (11) is bounded by

$$\frac{1}{n^{2n}} \frac{n!}{(n-t)!} (n-t)^{2(n-t)} n^{(2\sum_{i=2}^{n} j_i)}. \tag{4.2.14}$$

Clearly, for $\bar{j}$ satisfying $t = \sum_{t=2}^{n} ij_i$, the maximum value of $\sum_{i=2}^{n} j_i$ is $t/2$, and this can only be obtained when $j_2 = t/2$ and $j_i = 0$ for $i > 2$. Since we have already considered this case, we may assume that

$$\sum_{i=2}^{n} j_i \le \frac{t-1}{2}. \tag{4.2.15}$$

If equality obtains in (4.2.15), then from the fact that $t = \sum_{i=2}^{n} j_i$ we have that $\sum_{i=2}^{n} (i-2)j_i = 1$. It follows from this, that equality in (4.2.15) obtains only if $j_2 = \frac{t-3}{2}$, $j_3 = 1$, and $j_i = 0$, for $i > 3$. Since we have already shown that the contribution from these terms tends to 0, we may assume that $\sum_{i=2}^{n} j_i \le \frac{t-2}{2}$. In this case (4.2.14) is bounded above by

$$\tfrac{1}{n^{2n}} \tfrac{n!}{(n-t)!} (n-t)^{2n-2t} n^{t-2} \le \tfrac{n^t}{n^t} \tfrac{(n-t)^{2n-2t}}{n^{2n-2t}} \tfrac{n^{t-2}}{n^t} \le \tfrac{1}{n^2}.$$

Since there are at most n such terms, there total contribution is at most $n(1/n^2) = 1/n$. Thus as $n \to \infty$ the contribution of these terms goes to 0. [Fre90, pp. 6,7] □

This last result, together with (4.2.5) and (4.2.6), give the following corollary:

Corollary 4.2.4 ([Fre90, Cor. 4])**.** *For* 2 *unary algebras, the labeled and the unlabeled probabilities can differ by at most* 0.01 *when they both exist.* □

Chapter 5

Probability in group theory

Among the great number of publications in the field of probability in group theory, we present a few results on this topic just to give a short insight into this vast field of research.

5.1 On the probability of generating a minimal d-generated group

Definition 5.1.1 ([DVLM01])**.** We denote by $\mathcal{L}$ the set of finite groups L with the following properties: L has a unique minimal normal subgroup, say M, and if M is abelian then M has a complement in L.
Let $L_0 = L/M$ and for any positive integer t define $L_t = \{(l_1, \ldots, l_t) \in L^t | l_1 \equiv \cdots \equiv l_t \bmod M\}$.

Definition 5.1.2 ([DVLM01])**.** Denote by $d(G)$ the minimal number of generators of a finite group G. A group G is a *minimal d-generated group* if $d(G) = d$ but $d(G/N) < d$ whenever N is a nontrivial normal subgroup of G.

> In [DVL98] it is proved that for any nontrivial finite group G there exists $L \in \mathcal{L}$ and a positive integer t such that L_t is an epimorphic image of G and $d(G) = d(L_t) > d(L_{t_1})$. In particular, if G is a minimal d-generated group, then $G \cong L_t$ for a suitable choice of $L \in \mathcal{L}$ and $t \in \mathbb{N}$. [DVLM01, p. 3]

Definition 5.1.3 ([DVLM01])**.** For any finite group G, let $\phi_G(s)$ denote the number of s-bases, that is, ordered s-tuples $(g_1, \ldots, g_s)$ of elements of G that generate G. The number $P_G(s) = \phi_G(s)/|G|^s$ gives the probability that s randomly chosen elements of G generate G. If G is a finite group and N is a normal subgroup of G, let $P_{G,N}(s) = P_G(s)/P_{G/N}(s)$ denote the probability that an s-tuple generates G, given that it generates G modulo N.

Theorem 5.1.4 ([DVLM01] Thm.1)**.** *Given a real number α with $0 < \alpha < 1$ there exist two absolute constants β_1 and β_2 such that for any $L \in \mathcal{L}$ and any $t \in \mathbb{N}$*

- *if* $\operatorname{soc} L$ *is abelian and $s \geq \beta_1 + d(L_t)$, then $P_{L_t,\operatorname{soc} L_t} \geq \alpha$;*
- *if* $\operatorname{soc} L$ *is non-abelian and $s \geq \beta_2 \log(t+1)$, then $P_{L_t,\operatorname{soc} L_t}(s) \geq \alpha$*

Theorem 5.1.5 ([DVLM01] Thm. 2)**.** *Let $\mathcal{L}_{ab}$ be the set of finite groups $L \in \mathcal{L}$ satisfying the property that soc L is abelian. For any $L \in \mathcal{L}_{ab}$ and any $t, u \in \mathbb{N}$*

$$P_{L_t,\operatorname{soc} L_t}(d(L_t) + u) \geq 1 - 2^{-u}$$

Theorem 5.1.6 ([DVLM01] Thm. 3)**.** *Let $\mathcal{L}_{nonab} = \mathcal{L} \backslash \mathcal{L}_{ab}$. There exist two positive real numbers η_1 and η_2 such that for any $L \in \mathcal{L}_{nonab}$ and any $t, u \in \mathbb{N}$, if $P_{L_0}(u) > 0$ then*

$$P_{L_t,\operatorname{soc} L_t}(u) \geq 1 - \tfrac{\eta_1 t^2}{2^{\eta_2 u}}$$

Now suppose $X, Y \in \mathcal{L}$ with $\operatorname{soc} X = \operatorname{soc} Y$ and let $t \in \mathbb{N}$. What can be said about $d(Y_t)$ if we know $d(X_t)$?

Theorem 5.1.7 ([DVLM01] Thm. 4)**.** *There exists a positive integer r with the following property: for any pair of groups $X, Y \in \mathcal{L}_{nonab}$ with* $\operatorname{soc} X = \operatorname{soc} Y$ *and any non negative integer t, $d(Y_t) \leq \max(d(Y_0), d(X_t) + r)$*

Theorem 5.1.8 ([DVLM01] Thm. 5)**.** *There exists a positive real number ζ with the following property: for any pair of groups $X, Y \in \mathcal{L}_{nonab}$ with* $\operatorname{soc} X = \operatorname{soc} Y$ *and any nonnegative integer t, if $|\operatorname{soc} X| \geq \zeta$, then $d(Y_t) \leq \max(d(Y_0), d(X_t)+1)$.*

5.2 Completeness for concrete near-rings

Definition 5.2.1 ([AMPW04])**.** Given a group $\langle \Gamma, +, -, 0 \rangle$, a subset N of the set Γ^Γ of maps from Γ to Γ is said to be a concrete near-ring over Γ if N is closed with respect to composition (of functions), and pointwise addition and negation. A set $F \subseteq \Gamma^\Gamma$ of maps is said to be near-ring complete if the near-ring generated by F is equal to $M(\Gamma)$, the full concrete near-ring over Γ whose carrier is Γ^Γ .

The following lemma yields a characterization of those operations, which are near-ring complete.

Lemma 5.2.2 ([AMPW04, Thm. B])**.** *Let F be a set of unary operations on Γ where $\langle \Gamma, +, -, 0 \rangle$ is a finite group with at least three elements. Then F is near-ring complete if and only if the following conditions are satisfied:*

- *F separates points, that is, for all $a, b \in \Gamma$ such that $a \neq b$ there is an $f \in F$ with $f(a) \neq f(b)$;*

- *for every subgroup $H \neq \Gamma$ of Γ there exist an $f \in F$ and $h \in H$ such that $f(h) \notin H$;*

- *for every proper normal subgroup $0 \neq N \neq \Gamma$ of Γ there exist an $f \in F$ and $x, y \in \Gamma$ such that $x - y \in N$ and $f(x) - f(y) \in N$;*

- *in case $\langle \Gamma, +, -, 0 \rangle$ is an elementary abelian p-group, there exists an $f \in F$ and $x, y \in \Gamma$ such that $f(x + y) \neq f(x) + f(y) - f(0)$.*

Based on this lemma we obtain a lower bound for the fraction of near-ring complete bijections from $\Gamma \to \Gamma$.

Theorem 5.2.3 ([AMPW04, Thm. C])**.** *Write p_Γ for the probability that a randomly chosen bijection from Γ to Γ generates $M(\Gamma)$ and let $n := |\Gamma|$. Then $p_\Gamma > (n - 6)/n$ for $n \geq 6$, and thus p_Γ tends to 1 as $n \to \infty$.*

Chapter 6

Applications of better quasi-order theory

In [AA18] we investigated an ordering of tupels of natural numbers and two different word orderings showing that they (and even their upward closed subsets ordered by set inclusion) are well quasi-ordered. In the present note our aim is to prove that all these orderings are even better-quasi ordered, resorting to the theory of bad arrays introduced by Crispin St. J. A. Nash-Williams in [NW65].

6.1 Barriers, bad arrays and better quasi-orders

In the following, we will use the notation given in [AH07]. We denote sets ranging over $[\mathbb{N}]^{\omega}$, the set of infinite subsets of $\mathbb{N}$, with capital letters. Sets ranging over $[\mathbb{N}]^{<\omega}$, the set of finite subsets of $\mathbb{N}$, are denoted by small letters. We assume that all our sets are written in increasing order of their elements. We denote by $l(s)$ the cardinality of s. For every $1 \leq i \leq l(s)$ we write s_i for the i-th element of s; therefore, we can write $s = \{s_1, \dots, s_{l(s)}\}$, with $s_1 < \cdots < s_{l(s)}$. We write $s \preccurlyeq t$ if s is an initial segment of t, that is $l(s) \leq l(t)$ and $s_i = t_i$ for all $1 \leq i \leq l(s)$. We put $s \prec t$ if s is a proper initial segment of t, i.e., $s \preccurlyeq t$ and $s \neq t$. Clearly $s \preccurlyeq t$ implies $s \subseteq t$.

If s, t are finite subsets of $\mathbb{N}$, we write $s \lhd t$ to mean that there are $i_1 < \cdots < i_k$ and j $(1 \leq j < k)$ such that $s = \{i_1, \dots, i_j\}$ and $t = \{i_2, \dots, i_k\}$.

Definition 6.1.1. Let X be an infinite subset of $\mathbb{N}$. We say that $\mathcal{B} \subseteq [X]^{<\omega}$ is a barrier on X if:

- for every infinite $Y \subseteq X$ there is an initial segment of Y in $\mathcal{B}$,

- $\mathcal{B}$ is an antichain with respect to $\subseteq$.

Definition 6.1.2 ([AH07])**.** Let $\mathcal{B}$ be a barrier on X. Write $\mathcal{B}_2 = \{s \cup t : s, t \in \mathcal{B},\ s \lhd t\}$.

Lemma 6.1.3 ([AH07, Lem. 1.5])**.** *Let $\mathcal{B}$ be a barrier on a set X. Then for every $Y \in [X]^\omega$ and $s \in \mathcal{B}$ with $s \prec Y$ there exists $t \in \mathcal{B}$ such that $s \lhd t$ and $s \cup t \prec Y$.*

Proof: Let $s \in \mathcal{B}$, $s \prec Y$. Write $s = \{y_1, \dots, y_l\}$. $Y \setminus \{y_1\} \in [X]^\omega$ has an initial segment t in $\mathcal{B}$, i.e. $t = \{y_2, \dots, y_k\}$. If $k \leq l$, $t \subset s$ contradicting the fact that $\mathcal{B}$ is an antichain. Hence $l < k$ and thus $s \lhd t$. Obviously $s \cup t \prec Y$. □

Theorem 6.1.4 ([AH07, Prop. 1.4])**.** *$\mathcal{B}_2$ is a barrier on X.*

Proof: The first item of the definition follows directly from Lemma 6.1.3.

For the second item, we show that if $s, t, s', t' \in \mathcal{B}, s \lhd t, s' \lhd t'$, and $s \cup t \subseteq s' \cup t'$, then $s = s'$ and $t = t'$. For let $s \cup t = \{i_1, \dots, i_k\}$ and $s' \cup t' = \{j_1, \dots, j_m\}$ in increasing order. Then $t = \{i_2, \dots, i_k\}$ and $t' = \{j_2, \dots, j_m\}$. Assume $t \not\subseteq t'$.
Case: $i_r \notin t'$ for $2 < r \leq k$: Since clearly $t \subseteq s' \cup t'$, $i_r = j_1$. But then $i_{r-1} < j_1$ and hence $i_{r-1} \notin s' \cup t'$, a contradiction.
Case: $i_2 \notin t'$. Then $i_2 = j_1$: But then $i_1 < j_1$ in contradiction to $s \cup t \subseteq s' \cup t'$.
Hence $t \subseteq t'$, and since $\mathcal{B}$ is a barrier we have $t = t'$. It follows that $s \cup t = s' \cup t'$ and $s = s'$. □

Theorem 6.1.5 (Nash-Williams barrier theorem)**.** *Let $\mathcal{B}$ be a barrier on $X \in [\mathbb{N}]^\omega$. Suppose that $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$. Then there is an infinite subset Y of X such that one of $\mathcal{B}_i \cap [Y]^{<\omega} (i = 1, 2)$ is a barrier on Y.*

In the context of bqo-theory, the concept of bad sequences has been generalized to *bad arrays*:

Definition 6.1.6 ([AH07])**.**

- Given a barrier $\mathcal{B}$ and a pre-ordered set Q, we call a map $f : \mathcal{B} \to Q$ a Q-array.
- We say that a Q-array is bad if there are no $s, t \in \mathcal{B}$ with $s \lhd t$ such that $f(s) \leq f(t)$ and good otherwise.

Definition 6.1.7. [AH07] We say that a pre-ordered set $(Q, \leq)$ is *better quasi-ordered* if there is no bad Q-array.

A detailed overview on how the concept of well quasi-orderings has been generalized to the concept of better-quasi-orderings is given in [Peq17]. However, it can be seen easily that a better quasi-ordered set is also well quasi-ordered:

Theorem 6.1.8. *If Q is better quasi-ordered, then Q is also well quasi-ordered.*

Proof: Suppose that Q is not wqo. Then there is a bad sequence $s := (s_i)_{i \in \mathbb{N}}$ from Q. Let $\mathcal{B}$ be a barrier on $\mathbb{N}$ and define $f : \mathcal{B} \to Q$; $f(b) := s_{\min(b)}$. Since $b \lhd c$ implies $\min(b) < \min(c)$ and s is bad, we get that $b \lhd c$ implies $f(b) = s_{\min(b)} \nleq s_{\min(c)} = f(c)$. Hence $f : \mathcal{B} \to Q$ is a bad array and thus Q is not bqo. □

The following theorem shows that better quasi-orderedness is a particularly strong property with far reaching consequences.

Definition 6.1.9. [AA18] A subset U of A is called *upward closed* if $u \in U$, $a \in A$, and $u \leq a$ imply $a \in U$. For a subset B of A, we define the *upward closed set generated by B* by $\uparrow B := \{a \in A \mid \exists b \in B : b \leq a\}$. By $U(A, \leq)$ or simply $U(A)$ we denote the set of upward closed subsets of A. This set can be ordered by set inclusion $\subseteq$. Dually, $D \subseteq A$ is called *downward closed* if $A \setminus D$ is upward closed.

Theorem 6.1.10 ([AH07, Prop. 5.5])**.** *Suppose that the ordered set A is bqo. Then the ordered sets $(U(A), \supseteq)$ and $(D(A), \subseteq)$ are bqo.*

Proof:

> Let $f : \mathcal{B} \to D(A)$ be a bad $D(A)$-array. The set $\mathcal{B}_2$ is a barrier. We construct a bad A-array $g : \mathcal{B}_2 \to A$ as follows: For every $s \cup t \in \mathcal{B}_2$, we have $f(s) \nsubseteq f(t)$; so we can choose $g(s \cup t) \in f(s) \setminus f(t)$. Now suppose $s' \cup t' \in \mathcal{B}_2$ with $s \cup t \lhd s' \cup t'$. Then $s' = t$, hence $g(s \cup t) \nleq g(s' \cup t')$. Therefore, g is bad. This shows, that $D(A)$ is bqo.
>
> Suppose $h : \mathcal{C} \to U(A)$ is an $U(A)$-array. We then consider the $D(A)$-array $h' : \mathcal{C} \to D(A)$ defined by $h'(c) = S \setminus h(c)$ for all $c \in \mathcal{C}$. Since $D(A)$ is bqo, we find $c_1 \lhd c_2$ in $\mathcal{C}$ with $h'(c_1) \subseteq h'(c_2)$, and hence $h(c_1) \supseteq h(c_2)$. Thus h is good, and $U(A)$ is bqo. [AH07, p. 14] □

For well-quasi orders there does not exist a similar property.

6.2 Minimal bad maps

Definition 6.2.1 ([Lav78])**.** Suppose Q is quasi-ordered by $\leq$. A *partial ranking* on Q is a well-founded partial order $<'$ on Q such that if $q, r \in Q$ and $q <' r$ then $q < r$.[1]

[1] Since all the sets we are considering carry a well founded partial ordering, we may simply take $<$ for $<'$.

- For barriers $\mathcal{B}, \mathcal{C}$ on X, Y, we write $\mathcal{B} \sqsubseteq \mathcal{C}$ if $Y \subseteq X$ and every element of $\mathcal{C}$ has an initial segment in $\mathcal{B}$. We write $\mathcal{B} \sqsubset \mathcal{C}$ if $\mathcal{B} \sqsubseteq \mathcal{C}$ and some element of $\mathcal{C}$ has a proper initial segment in $\mathcal{B}$.

- Given $f : \mathcal{B} \to Q$ and $g : \mathcal{C} \to Q$, we say f *foreruns* g, written $f \sqsubseteq g$ if

  1. $\mathcal{B} \sqsubseteq \mathcal{C}$,
  2. $f(s) = g(s)$ for all $s \in \mathcal{B} \cap \mathcal{C}$,
  3. for all $b \in \mathcal{B}$, $c \in \mathcal{C}$ with $b \prec c$, we have $g(c) <' f(b)$.

  We say f *strictly foreruns* g and write $f \sqsubset g$ if $f \sqsubseteq g$ and $\mathcal{B} \sqsubset \mathcal{C}$.[2]

- We say that a bad map $f : \mathcal{B} \to Q$ is *minimal* if there is no bad g with $f \sqsubset g$.

Theorem 6.2.2 (Minimal bad array lemma, [Lav78, Thm. 1.9])**.** *Let $(Q, \leq)$ be quasi-ordered, $<'$ a partial ranking on Q. Then for every barrier $\mathcal{B}$ and bad map $f : \mathcal{B} \to Q$, there are a barrier $\mathcal{C} \sqsupseteq \mathcal{B}$ and a minimal bad $g : \mathcal{C} \to Q$ with $f \sqsubseteq g$.*

6.3 Higman's ordering

Let A be a finite alphabet and define the set of words over A as $A^* = \bigcup_{n \in \mathbb{N}_0} A^n$. A word $u \in A^*$ *embeds into* $v \in A^*$ if u can be obtained from v by cancelling some letters, writing $u \leq_e v$. For example $u = aexzzl$ embeds into $v = \underline{a}b\underline{e}\underline{x}a\underline{z}\underline{z}k\underline{l}c$.
A formal definition when $x \leq_e y$ holds is based on recursion on the length of x. The empty word ϵ can be embedded in every $y \in A^*$. Now let $x = au$ for some $a \in A$ and $u \in A^*$. Then $x \leq_e y$ if there are words $v, w \in A^*$ such that $y = vaw$ and $u \leq_e w$.
A result of G. Higman from 1952 states that there do not exist infinite antichains for this ordering of words [Hig52]. In [AA18] we provided a proof for the fact that also $(U(A^*, \leq_e), \subseteq)$ has no infinite antichains, using the concept of *minimal bad sequences* introduced in [NW63]. It turns out that an even stronger result can be obtained using the theory of bad arrays.

Theorem 6.3.1. *$(A^*, \leq_e)$ is better quasi-ordered.*

Proof: Assume that there is a barrier $\mathcal{B}$ and a bad map $f : \mathcal{B} \to A^*$. Since $(A^*, \leq_e)$ is well founded, by theorem 6.2.2 there exists a barrier $\mathcal{C} \sqsupseteq \mathcal{B}$ on a set X and a minimal bad map $g : \mathcal{C} \to A^*$ with $f \sqsubseteq g$. Define $\mathcal{C}_2 := \{s \cup t : s, t \in \mathcal{C},\ s \lhd t\}$. By

[2] In [Lav78], $\sqsubseteq$ is used in the context of barriers as well as for comparing arrays/maps. However, notice that in each context $\sqsubseteq$ has a different meaning.

theorem 6.1.4, $\mathcal{C}_2$ is a barrier on X. Define $\mathcal{C}_2^\epsilon := \{s \cup t \in \mathcal{C}_2 : g(s) = \epsilon\}$. Assume there exists $s \cup t$ in $\mathcal{C}_2^\epsilon$. Then $g(s) = \epsilon \leq_e g(t)$. Since $s \cup t \in \mathcal{C}_2$, $s \lhd t$ and hence g is good contradicting the assumptions. Thus $\mathcal{C}_2^\epsilon = \varnothing$.
Let $\mathcal{C}_2^a := \{s \cup t \in \mathcal{C}_2 : g(s) = aw \,\text{for some}\, a \in A \,\text{and}\, w \in A^*\}$. Clearly $\mathcal{C}_2 = \bigcup_{a \in A} \mathcal{C}_2^a$. Since A is a finite alphabet, by the Nash-Williams barrier theorem we can find $a \in A$ and an infinite subset Y of X such that $\mathcal{C}_2^a \cap [Y]^{<\omega} =: \mathcal{D}$ is a barrier on Y.
For a word $w = av$, where $a \in A$ and $v \in A^*$, we define $a^{-1}w := v$. Let $h : \mathcal{D} \to A^*$; $h(s \cup t) := a^{-1}g(s)$. We show that $g \sqsubset h$:

1. We prove that $\mathcal{C} \sqsubset \mathcal{D}$. To this end, let $s \cup t \in \mathcal{D}$. By definition, $s \cup t \in \mathcal{C}_2$ and thus $s \lhd t$, i.e.: $s = \{i_1, \ldots, i_l\}$, $t = \{i_2, \ldots, i_k\}$, $l < k$. Thus $s \prec s \cup t$ and hence every element of $\mathcal{D}$ has a proper initial segment in $\mathcal{C}$.

2. We have to show that $g(s) = h(s)$ for all $s \in \mathcal{C} \cap \mathcal{D}$. Assume $s \in \mathcal{C} \cap \mathcal{D}$. Since $s \in \mathcal{C}_2$, $s = u \cup v$ for some $u \lhd v \in C$. Again $u \prec u \cup v$, i.e. $u \prec s$ in $\mathcal{C}$ (obviously implying $u \subseteq s$), contradicting the fact that $\mathcal{C}$ is an antichain (with respect to $\subseteq$). Thus $\mathcal{C} \cap \mathcal{D} = \varnothing$.

3. It remains to prove that for all $s \cup t \in \mathcal{D}$ and $c \in \mathcal{C}$ with $c \prec s \cup t$, we have $h(s \cup t) <_e g(c)$. Obviously for $s \cup t \in \mathcal{D}$, s is the only element in $\mathcal{C}$ such that $s \prec s \cup t$, since otherwise $\mathcal{C}$ would not be an antichain. But then $h(s \cup t) = a^{-1}g(s) <_e g(s)$.

Now, since g is a minimal bad map and $g \sqsubset h$, h has to be good. Thus there exist $s \cup t \lhd s' \cup t' \in \mathcal{D}$ such that $h(s \cup t) \leq_e h(s' \cup t')$, i.e. $a^{-1}g(s) \leq_e a^{-1}g(s')$. But then also $g(s) \leq_e g(s')$. Since $s \cup t \lhd s' \cup t'$, for $m < n$ we can write $s \cup t = \{i_1, \ldots, i_m\}$, $s' \cup t' = \{i_2, \ldots, i_n\}$. Since $s \cup t \in \mathcal{C}_2$, $s \lhd t$ in $\mathcal{C}$ and thus for $l < m < n$, $s = \{i_1, \ldots, i_l\}$, $t = \{i_2, \ldots, i_m\}$. Obviously $t \prec s' \cup t'$, but also $s' \prec s' \cup t'$. Since t and s' are both in $\mathcal{C}$ and $\mathcal{C}$ is an antichain, it must be $t = s'$ and hence $s \lhd s'$. That means we have found $s \lhd s'$ in $\mathcal{C}$ such that $g(s) \leq_e g(s')$. But in this case the map g is good, contradicting the minimal badness of g. Hence there cannot exist bad A^*-arrays and therefore A^* is bqo. □

6.4 Dickson's ordering

The set $\mathbb{N}_0^m$ of vectors of natural numbers of some fixed length m is ordered by $(a_1, \ldots, a_m) \leq (b_1, \ldots, b_m)$ if $a_i \leq b_i$ for all $i \in \{1, \ldots, m\}$. In 1913, L.E. Dickson proved that $(\mathbb{N}_0^m, \leq)$ has no infinite antichains [Dic13]. From Theorem 6.3.1 it can be derived easily that also $(\mathbb{N}_0^m, \leq)$ is bqo, using quasi-embeddings.

Definition 6.4.1. [AH07] Let $\mathbb{A} = (A, \leq_A)$ and $\mathbb{B} = (B, \leq_B)$ be partially ordered sets. A mapping $f : A \to B$ is a *quasi-embedding* from $\mathbb{A}$ into $\mathbb{B}$ if for all $a_1, a_2 \in A : f(a_1) \leq_B f(a_2) \Rightarrow a_1 \leq_A a_2$.

Lemma 6.4.2 ([AH07, Lem. 5.3])**.** *Let $(S, \leq_S)$ and $(T, \leq_T)$ be ordered sets. If there exists a quasi-embedding $S \to T$ and T is bqo, then S is bqo.*

Proof:

> Let $\phi : S \to T$ be a quasi-embedding and let $g : \mathcal{B} \to S$ be an S-array (i.e. a function from a barrier to the set S). Then $\phi \circ g : \mathcal{B} \to T$ is a T-array. Since T is Nash-Williams, there exist $b_1, b_2 \in \mathcal{B}$ with $b_1 \lhd b_2$ and $\phi(g(b_1)) \leq_T \phi(g(b_2))$. But since ϕ is a quasi-embedding, also $g(b_1) \leq_S g(b_2)$ holds. [AH07, p. 14] □

Lemma 6.4.3 ([AA18])**.** *There exists a quasi-embedding from $(\mathbb{N}_0^m, \leq)$ to $(A^*, \leq_e)$.*

Proof:

> We construct a quasi-embedding f from $(\mathbb{N}_0^m, \leq)$ into $(\{1, \ldots, m\}^*, \leq_e)$ by
>
> $$f(x_1, \ldots, x_m) := \underbrace{11\ldots1}_{x_1}\underbrace{22\ldots2}_{x_2}\ldots\underbrace{mm\ldots m}_{x_m} = 1^{x_1}2^{x_2}\ldots m^{x_m}$$
>
> for all $(x_1, \ldots, x_m) \in \mathbb{N}_0^m$.
> Now if $1^{x_1}2^{x_2}\ldots m^{x_m} \leq_e 1^{y_1}2^{y_2}\ldots m^{y_m}$, then $(x_1, \ldots, x_m) \leq (y_1, \ldots, y_m)$. Thus f is a quasi-embedding. [AA18, p. 10]

Corollary 6.4.4. $(\mathbb{N}_0^m, \leq)$ *is better quasi-ordered.*

Proof: By Theorem 6.3.1, Lemma 6.4.2 and Lemma 6.4.3. □

6.5 Another word ordering

We consider the following word ordering given in [AMM11]. Let A be a finite set, and let $B := (A \times \{0\}) \cup (A \times \{1\})$. We define a mapping $\varphi : A^* \to B^*$ by $\varphi(a_1, \ldots, a_n) := (b_1, \ldots, b_n)$ with $b_i := (a_i, 0)$ if $a_i \notin \{a_1, \ldots, a_{i-1}\}$ and $b_i := (a_i, 1)$ if $a_i \in \{a_1, \ldots, a_{i-1}\}$. For $u = (a_1, \ldots, a_n)$, we use $S(u)$ to denote the set of letters that occur in u, formally $S(u) := \{a_i \mid i \in \{1, \ldots, n\}\}$. For $u, v \in A^*$, we say that $u \leq_E v$ if $\varphi(u) \leq_e \varphi(v)$ and $S(u) = S(v)$.

Theorem 6.5.1. $(A^*, \leq_E)$ *is better quasi-ordered.*

Proof: We define a mapping $f : A^* \to B^* \times \mathcal{P}(A)$ by $f(u) := (\varphi(u), S(u))$. We order the set $B^* \times \mathcal{P}(A)$ by $(u, S) \leq (v, T)$ if $u \leq_e v$ and $S = T$. Then f is a quasi-embedding from $(A^*, \leq_E)$ into $B^* \times \mathcal{P}(A)$.

Assume $B^* \times \mathcal{P}(A)$ is not better quasi-ordered. Then there exists a barrier $\mathcal{B}$ on a set X and a bad map $g : \mathcal{B} \to B^* \times \mathcal{P}(A)$, i.e. $\nexists s \lhd t \in \mathcal{B}$ such that $g(s) \leq g(t)$. Let $g(b) = (v_b, T_b) \in B^* \times \mathcal{P}(A)$. Define $\mathcal{B}_P := \{b \in \mathcal{B} : T_b = P \in \mathcal{P}(A)\}$. Clearly $\mathcal{B} = \bigcup_{P \in \mathcal{P}(A)} \mathcal{B}_P$. Since $\mathcal{P}(A)$ is finite, we can apply the NW barrier theorem and thus find $\bar{P} \in \mathcal{P}(A)$ and an infinite subset Y of X such that $\mathcal{B}_{\bar{P}} \cap [Y]^{<\omega} =: \mathcal{B}^Y_{\bar{P}}$ is a barrier on Y.

Now for $s \lhd t \in \mathcal{B}^Y_{\bar{P}}$, we have $g(s) \nleq g(t)$ by the badness of g. By definition, $T_s = T_t = \bar{P}$ and thus it must be $v_s \nleq_e v_t$ in $(B^*, \leq_e)$. But then $\hat{g} : \mathcal{B}^Y_{\bar{P}} \to B^*$, $\hat{g}(b) = v_b$ is a bad map from the barrier $\mathcal{B}^Y_{\bar{P}}$ into $(B^*, \leq_e)$, in contradiction to theorem 6.3.1. Thus $B^* \times \mathcal{P}(A)$ is bqo and so is $(A^*, \leq_E)$ by Lemma 6.4.2. $\square$

Chapter 7

Bibliography

[AA18] Erhard Aichinger and Florian Aichinger. Dickson's lemma, higman's theorem and beyond: a survey of some basic results in order theory. 12 2018.

[AH07] Matthias Aschenbrenner and Raymond Hemmecke. Finiteness theorems in stochastic integer programming. *Found. Comput. Math.*, 7(2):183–227, 2007.

[AMM11] Erhard Aichinger, Peter Mayr, and Ralph McKenzie. On the number of finite algebraic structures. *arXiv preprint arXiv:1103.2265*, 2011.

[AMPW04] E. Aichinger, D. Mašulović, R. Pöschel, and J. S. Wilson. Completeness for concrete near-rings. *J. Algebra*, 279(1):61–78, 2004.

[Ber12] Clifford Bergman. *Universal algebra*, volume 301 of *Pure and Applied Mathematics (Boca Raton).* CRC Press, Boca Raton, FL, 2012. Fundamentals and selected topics.

[BS81] Stanley Burris and H. P. Sankappanavar. *A course in universal algebra*, volume 78 of *Graduate Texts in Mathematics.* Springer-Verlag, New York-Berlin, 1981.

[Dav79] Roy O. Davies. On n-valued Sheffer functions. *Z. Math. Logik Grundlagen Math.*, 25(4):293–298, 1979.

[Dic13] Leonard Eugene Dickson. Finiteness of the Odd Perfect and Primitive Abundant Numbers with n Distinct Prime Factors. *Amer. J. Math.*, 35(4):413–422, 1913.

[DVL98] Francesca Dalla Volta and Andrea Lucchini. Finite groups that need more generators than any proper quotient. *J. Austral. Math. Soc. Ser. A*, 64(1):82–91, 1998.

[DVLM01] F. Dalla Volta, A. Lucchini, and F. Morini. On the probability of generating a minimal d-generated group. volume 71, pages 177–185. 2001. Special issue on group theory.

[Fag76] Ronald Fagin. Probabilities on finite models. *J. Symbolic Logic*, 41(1):50–58, 1976.

[Fre90] Ralph Freese. On the two kinds of probability in algebra. *Algebra Universalis*, 27(1):70–79, 1990.

[Hig52] Graham Higman. Ordering by divisibility in abstract algebras. *Proc. London Math. Soc. (3)*, 2:326–336, 1952.

[Lav78] Richard Laver. Better-quasi-orderings and a class of trees. In *Studies in foundations and combinatorics*, volume 1 of *Adv. in Math. Suppl. Stud.*, pages 31–48. Academic Press, New York-London, 1978.

[Mur75] V. L. Murskiĭ. The existence of a finite basis of identities, and other properties of "almost all" finite algebras. *Problemy Kibernet.*, (30):43–56, 1975.

[NW63] C. St. J. A. Nash-Williams. On well-quasi-ordering finite trees. *Proc. Cambridge Philos. Soc.*, 59:833–835, 1963.

[NW65] C. St. J. A. Nash-Williams. On well-quasi-ordering infinite trees. *Proc. Cambridge Philos. Soc.*, 61:697–720, 1965.

[Peq17] Yann Pequignot. Towards better: a motivated introduction to better-quasi-orders. *EMS Surv. Math. Sci.*, 4(2):185–218, 2017.

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Masterarbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw. die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe. Die vorliegende Masterarbeit ist mit dem elektronisch übermittelten Textdokument identisch.

Gallneukirchen 18.06.2020
Ort, Datum

Aichinger
Unterschrift