RESEARCH STATEMENT

PAUL SHAFER
APRIL 2016

I study computability theory, a branch of mathematical logic concerned with classifying mathematical objects (typically coded as subsets of $\mathbb{N}$) by how much extra information is needed to describe them by computer programs. Much of my research is connected by the basic theme of using computability to study the complexities of mathematical problems, both locally and globally. By "locally," I mean comparing the complexities of individual, concrete problems, as is typically done in reverse mathematics. By "globally," I mean analyzing the complexities of structures that model complexity or hardness relations, as is typically done in the Turing degrees. This statement presents an overview of my work in a variety of areas in computability—reverse mathematics, the Weihrauch degrees, the Medvedev and Muchnik degrees, and algorithmic randomness—and it raises a few questions that I am currently pursuing or plan to pursue in the future.

1. Reverse mathematics

Reverse mathematics, introduced by Friedman [21], is an analysis of the logical strength of the theorems of ordinary mathematics in the context of second-order arithmetic. The idea is that a mathematical problem is a statement in second-order arithmetic, and one problem is more complex than another if the more-complex problem requires stronger axioms to prove than the less-complex problem. Five main axiomatic systems are used as benchmarks for logical strength. The "Big Five" are named RCA_0, WKL_0, ACA_0, ATR_0, and Π^1_1-CA_0, in order of increasing strength. These axiom systems posit the existence of certain subsets of $\mathbb{N}$, where stronger systems provide more complicated sets than weaker systems. The complexity of a set is measured by the complexity of the formula that defines it and is closely related to the computability-theoretic complexity (i.e., Turing degree) of that set. The Big Five axiom systems can be described roughly as follows.

- RCA_0 (for *recursive comprehension axiom*): If X is Δ^0_1 (i.e., if X is computable or can be computed from an existing set), then X exists.
- WKL_0 (for *weak König's lemma*): RCA_0 plus the axiom "if T is an infinite binary branching tree, then T has an infinite path."
- ACA_0 (for *arithmetical comprehension axiom*): If X can be defined by a formula that has number quantifiers but not set quantifiers, then X exists.
- ATR_0 (for *arithmetical transfinite recursion*): Arithmetical comprehension can be iterated along any well-order.
- Π^1_1-CA_0 (for Π^1_1 *comprehension axiom*): If X can be defined by a formula of the form $\forall Y \varphi(n, Y)$, where φ has number quantifiers but not set quantifiers, then X exists.

(The subscript "0" in the names of the Big Five indicates that the systems only assume induction for Σ^0_1 formulas. However, ACA_0 and the stronger systems prove induction schemes for wider classes of formulas.)

A typical result in reverse mathematics has the form "theorem T is equivalent to $\mathsf{StrongSystem}$ over $\mathsf{WeakSystem}$," where T is some theorem from ordinary mathematics. This means that T is provable in $\mathsf{StrongSystem}$ and that all the axioms of $\mathsf{StrongSystem}$ are provable from $\mathsf{WeakSystem}+\mathsf{T}$. The proof of $\mathsf{StrongSystem}$ from $\mathsf{WeakSystem} + \mathsf{T}$ is called a *reversal*. Usually $\mathsf{WeakSystem}$ is taken to be RCA_0.

Much of the appeal of reverse mathematics is due to its ability to distinguish between a theorem and a special case of that theorem or between two theorems that appear “equivalent” (in a non-rigorous sense) in ordinary mathematics. For example, König’s lemma, the statement “if T is an infinite finitely branching tree, then T has an infinite path,” is equivalent to ACA_0 over RCA_0 (see [65] Theorem III.7.2). Thus weak König’s lemma (the special case restricted to binary branching trees) is indeed weaker than König’s lemma. Another example is compactness in $\mathbb{R}$. The Heine/Borel compactness of the interval $[0, 1]$ is equivalent to WKL_0 over RCA_0, but the sequential compactness of $[0, 1]$ is equivalent to ACA_0 over RCA_0 (see [65] Theorem IV.1.2 and Theorem III.2.2).

Second-order arithmetic is rich enough to formalize theorems throughout mathematics, and any statement of second-order arithmetic can be analyzed in the style of reverse mathematics. My work to date studies theorems from logic, combinatorics, algebra, analysis, and topology.

1.1. Reverse mathematics and logic.

A function $f\colon \mathbb{N} \to \mathbb{N}$ is DNR (for *diagonally non-recursive*) if $\forall e(f(e) \neq \Phi_e(e))$, where $(\Phi_e)_{e\in\mathbb{N}}$ is a fixed effective list of all Turing functionals. For $k \geq 2$, a function $f\colon \mathbb{N} \to \mathbb{N}$ is DNR(k) if it is DNR and $\mathrm{ran}(f) \subseteq \{0, 1, \dots, k-1\}$. These notions can also be relativized to any set X. For example, f is DNR relative to X if $\forall e(f(e) \neq \Phi_e^X(e))$. Let DNR be the statement “for every X there is a function that is DNR relative to X,” and let $\mathsf{DNR}(k)$ be the statement “for every X there is a function that is DNR(k) relative to X.” It is well-known that DNR is strictly between RCA_0 and WKL_0.

By a classic result of Jockusch [33], every $\mathsf{DNR}(k)$ function for every $k \geq 2$ computes a $\mathsf{DNR}(2)$ function. Combining Jockusch’s theorem with the classic work of Jockusch and Soare [34] on Π^0_1 classes yields the following well-known equivalence: for every *fixed* $k \geq 2$, $\mathsf{DNR}(k)$ is equivalent to WKL_0. Simpson [63] asked if $(\exists k \geq 2)\mathsf{DNR}(k)$ is also equivalent to WKL_0. Dorais, Hirst, and I [19] prove that it is not. Jockusch’s argument can be implemented with the Σ^0_2-induction scheme but not with the weaker Σ^0_2-bounding scheme, whereas RCA_0 only provides the weaker-still Σ^0_1-induction scheme. A consequence is that Jockusch’s result may fail in models where Σ^0_2 induction fails.

Theorem 1.1 ([19]).

- $(\exists k \geq 2)\mathsf{DNR}(k)$ *is equivalent to* WKL_0 *over* $\mathsf{RCA}_0 + \mathsf{I}\Sigma^0_2$.
- $(\exists k \geq 2)\mathsf{DNR}(k)$ *is strictly weaker than* WKL_0 *over* $\mathsf{RCA}_0 + \mathsf{B}\Sigma^0_2$ *(and hence also over* RCA_0*).*

The system WWKL (for *weak weak König’s lemma*) is the restriction of WKL_0 to trees of positive measure. It is strictly between DNR and WKL_0 [5], and it is an important principle for studying measure theory and randomness. In light of the previous theorem, it is natural to ask about the relationship between $\mathsf{DNR}(k)$ functions and paths through trees of positive measure. WWKL cannot imply $(\exists k \geq 2)\mathsf{DNR}(k)$ (because every ω-model of $(\exists k \geq 2)\mathsf{DNR}(k)$ is a model of WKL_0, and there are ω-models of WWKL that are not models of WKL_0), but the converse remains open.

Question 1.2. Does $(\exists k \geq 2)\mathsf{DNR}(k)$ imply WWKL over RCA_0?

1.2. Reverse mathematics and combinatorics.

1.2.1. *Menger’s theorem.* The case of Menger’s theorem and König’s duality theorem is another example of trying to detect a difference between a theorem and one of its special cases. Menger’s theorem states that if G is a graph and A and B are sets of vertices of G, then there is a collection M of disjoint A-B paths and a selection C of one vertex from each path in M such that every A-B path in G contains a vertex in C. König’s duality theorem is the restriction to bipartite graphs G with sides A and B. These problems have long histories. The forgoing formulation of Menger’s theorem for infinite graphs was posed as a problem by Erdős. König’s duality theorem was first proved for countable graphs by Podewski and Steffens [52] and then proved for arbitrary graphs by Aharoni [1]. Menger’s theorem was then proved for countable graphs by Aharoni [2] and proved for arbitrary graphs by Aharoni and Berger [3].

König's duality theorem is equivalent to ATR_0 by work of Aharoni, Magidor, and Shore [4] and of Simpson [61], so *a priori* Menger's theorem implies ATR_0. I prove Menger's theorem in Π^1_1-CA_0. The proof uses meta-mathematical techniques similar to Simpson's proof of König's duality theorem in ATR_0 [61].

Theorem 1.3 ([56]). *Menger's theorem is provable in* Π^1_1-CA_0.

However, by general considerations Menger's theorem cannot imply Π^1_1-CA_0. So Menger's theorem is either equivalent to ATR_0 or strictly between ATR_0 and Π^1_1-CA_0.

Question 1.4. Is Menger's theorem provable in ATR_0?

Towsner introduces the system TLPP_0, whose strength is strictly between ATR_0 and Π^1_1-CA_0 [69], and he shows that TLPP_0 encapsulates enough of the consequences of Π^1_1-CA_0 to implement my proof of Menger's theorem. Hence Menger's theorem is provable in TLPP_0. TLPP_0 is an interesting target for a reversal for Menger's theorem. If Menger's theorem is not provable in ATR_0, it would be a rare example of a theorem from ordinary mathematics whose logical strength is strictly between ATR_0 and Π^1_1-CA_0.

1.2.2. *Ramsey-type weak König's lemma.* Flood [20] introduces Ramsey-type weak König's lemma (RWKL), a simultaneous weakening of WKL_0 and RT^2_2 (Ramsey's theorem for pairs and two colors), in which, given an infinite binary branching tree, one asks not for an infinite path through T but for an infinite set *consistent with being a path through* T. Before Flood's work, DNR was the most natural of a very few principles simultaneously below WKL_0 and RT^2_2, so it would not have been unreasonable to guess that RWKL is equivalent to DNR. Among several results, Flood proves that RWKL implies DNR, but he leaves as a question whether or not the reverse implication holds.

My recent work with Bienvenu and Patey [7] answers Flood's question. Part of our motivation is to identify other combinatorial problems whose Ramsey-type version (in which one asks for an infinite set consistent with being a solution instead of a full solution) is equivalent to RWKL. Our most interesting examples are the *Ramsey-type graph coloring principles.* Let $k \geq 2$. Recall that a graph is *locally k-colorable* if every finite subgraph is k-colorable. For every fixed $k \geq 2$, the statement "every locally k-colorable graph is k-colorable" is well-known to be equivalent to WKL_0. Let $\mathsf{RCOLOR}(k)$ be the statement "for every infinite locally k-colorable graph there is an infinite set of vertices H such that every finite subgraph can be colored by a k coloring that always colors the vertices in H the same color." The set H can be thought of as an infinite partial solution to the problem of k-coloring the graph. The following theorem summarizes our main results.

Theorem 1.5 ([7]).

(i) *For every $k \geq 3$,* $\mathsf{RCOLOR}(k)$ *and* RWKL *are equivalent.*
(ii) WWKL *does not imply* $\mathsf{RCOLOR}(2)$.
(iii) RWWKL *and* DNR *are equivalent (where* RWWKL *is* RWKL *restricted to trees of positive measure).*

Item (ii) answers Flood's question. WWKL implies DNR and RWKL implies $\mathsf{RCOLOR}(2)$, so by item (ii) DNR does not imply RWKL. However, item (iii) states that equivalence with DNR is obtained by restricting RWKL to trees of positive measure. This reflects results of Kjos-Hanssen [35] and Greenberg and Miller [28]. $\mathsf{RCOLOR}(2)$ appears to be weaker than RWKL, and we have not yet been able to determine its strength.

Question 1.6. Does $\mathsf{RCOLOR}(2)$ imply RWKL? Does $\mathsf{RCOLOR}(2)$ imply DNR?

1.3. **Reverse mathematics and algebra.** The foundational work on the reverse mathematics of algebra is that of Friedman, Simpson, and Smith [22]. My work with Dorais and Hirst [18] extends that of Friedman, Simpson, and Smith by analyzing the strengths of various theorems relating to algebraic field extensions. The following theorem summarizes a few of our results.

Theorem 1.7 ([18]). *The following are equivalent:*

(i) WKL_0.

(ii) *If F is a field, K is an algebraic extension of F, and $\varphi\colon K \to K$ is an automorphism of K that fixes F, then φ extends to an automorphism of the algebraic closure of K that fixes F.*

(iii) *If F is a field that is not algebraically closed, then there is an automorphism of the algebraic closure of F that fixes F but is not the identity.*

(iv) *If F is a field, J and K are algebraic extensions of F each having the property that every irreducible polynomial over F that has a root in the extension splits into linear factors over the extension, and $F(k)$ embeds into J for every $k \in K$, then K embeds into J.*

The J and K in item (iv) are required to be *normal* extensions of F. Several characterizations of normality appear in various algebra texts, and we show that proving these equivalences requires WKL_0 in general. Item (iv) is still true if the normality requirement is removed, but we show that the more general statement is equivalent to ACA_0 instead of WKL_0.

1.4. **Reverse mathematics and analysis.**

1.4.1. *Dichotomy and trichotomy for sequences of reals.* A real number is a countable object in general, and therefore, when working in second-order arithmetic, a real number must somehow be coded as a set or a function. Typically this is done by implementing a straightforward coding of $\mathbb{Q}$ in $\mathbb{N}$ and by defining a real number to be a rapidly converging sequence of rationals $(q_n)_{n\in\mathbb{N}}$, where rapidly converging means $\forall k \forall i(|q_k - q_{k+i}| \leq 2^{-k})$. The field operations on real numbers are definable in RCA_0, but not all seemingly innocent properties of the reals are trivial. My work with Dorais and Hirst [17] shows that dichotomy and trichotomy for sequences of reals requires some axiomatic strength.

Theorem 1.8.

- WKL_0 *is equivalent to the statement "if $(\alpha_i)_{i\in\mathbb{N}}$ is a sequence of reals, then there is a set $I \subseteq \mathbb{N}$ such that, for all i, $i \in I$ implies $\alpha_i \leq 0$ and $i \notin I$ implies $\alpha_i \geq 0$."*
- ACA_0 *is equivalent to the statement "if $(\alpha_i)_{i\in\mathbb{N}}$ is a sequence of reals, then there is a partition $L \cup E \cup G = \mathbb{N}$ such that, for all i, $i \in L$ implies $\alpha_i < 0$, $i \in E$ implies $\alpha_i = 0$, and $i \in I$ implies $\alpha_i > 0$."*

By the work of Hirst and Mummert [30], this theorem implies that dichotomy and trichotomy for pairs of real numbers (not just sequences of real numbers) is not provable in various weak systems of constructive analysis.

1.4.2. *The Tietze extension theorem.* In its most basic form, the Tietze extension theorem is stated in second-order arithmetic by formalizing "if X is a complete, separable metric space, $C \subseteq X$ is closed, and $f\colon C \to \mathbb{R}$ is continuous and bounded, then there is a continuous $F\colon X \to \mathbb{R}$ extending f. This version of the theorem is provable in RCA_0 (see [65]). Giusto and Simpson [25], however, consider what they call the *strong Tietze extension theorem*, in which the space X is assumed to be compact, the function f is assumed to be uniformly continuous, and the extension F is also required to be uniformly continuous. They prove the strong Tietze extension theorem in RCA_0 under the extra assumption that C is *located*, which means that the function mapping every $x \in X$ to its distance to C exists and is continuous. Giusto and Simpson also prove that the strong Tietze extension theorem without this extra locatedness assumption is provable WKL_0 but not in RCA_0, and they conjecture that it is equivalent to WKL_0 over RCA_0. In recent work, I prove that the strong Tietze extension theorem does indeed imply WKL_0 over RCA_0, thus confirming the conjecture.

Theorem 1.9 ([58]). *The following are equivalent:*

(i) WKL_0.

(ii) *Let X be a compact complete separable metric space, let C be a closed subset of X, and let $f\colon C \to \mathbb{R}$ be a continuous function with a modulus of uniform continuity. Then there is a continuous function $F\colon X \to \mathbb{R}$ with a modulus of uniform continuity that extends f.*

(iii) *Special case of* (ii) *with $X = [0,1]$.*

1.5. **Reverse mathematics and topology.** A topological space is *Noetherian* if every open set is compact. The work of Goubault-Larrecq [26, 27] develops the theory of Noetherian spaces and applies it to verification problems. Given a quasi-order Q, one defines two quasi-orders, $\mathcal{P}^\flat_f(Q)$ and $\mathcal{P}^\sharp_f(Q)$, on the finite subsets of Q by

$$A \leq^\flat B \Leftrightarrow (\forall a \in A)(\exists b \in B)(a \leq b)$$
$$A \leq^\sharp B \Leftrightarrow (\forall b \in B)(\exists a \in A)(a \leq b).$$

If Q is a well-quasi order, then $\mathcal{P}^\flat_f(Q)$ and $\mathcal{P}^\sharp_f(Q)$ are not necessarily well-quasi orders. However, Goubault-Larrecq proves that if Q is a well-quasi order, then the upper topologies associated with $\mathcal{P}^\flat_f(Q)$ and $\mathcal{P}^\sharp_f(Q)$ are Noetherian. (The basic closed sets of a quasi order's upper topology are generated by the downward closures of finite sets; it is the coarsest topology from which the quasi order can be recovered.) My work with Frittaion, Hendtlass, Marcone, and Van der Meeren [23] uses Dorais's [15] framework for compact countable second-countable spaces in second-order arithmetic to study Goubault-Larrecq's theorems. We prove that for both $* = \flat$ and $* = \sharp$ the statement "if Q is a well-quasi order, then the upper topology of $\mathcal{P}^*_f(Q)$ is Noetherian" is equivalent to ACA_0. We also show that it is possible to phrase Goubault-Larrecq's theorems for $\mathcal{P}^\flat(Q)$ and $\mathcal{P}^\sharp(Q)$ in second-order arithmetic, even though this leaves the framework of countable second-countable spaces, and that these theorems are equivalent to ACA_0. As Noetherian spaces can be thought of as topological analogs of well-quasi orders, this project can also be seen a contribution to the reverse mathematics of well-quasi orders, a subject that has enjoyed attention from Marcone [43] and Cholak, Marcone, and Soloman [14], to give two examples.

2. Weihrauch degrees

In reverse mathematics, a typical question is, given theorems T and Q, whether or not T implies Q over RCA_0. In principle, a proof of Q in $\mathsf{RCA}_0 + \mathsf{T}$ can use multiple applications of T, and these applications can be made non-uniformly. In practice, a proof of Q in $\mathsf{RCA}_0 + \mathsf{T}$ often exhibits a direct computable encoding of Q into T. The notion of *Weihrauch reducibility* [70, 71] from computable analysis provides the right formalization for this kind of encoding.

For multi-valued partial functions $f, g\colon \subseteq \mathbb{N}^\mathbb{N} \rightrightarrows \mathbb{N}^\mathbb{N}$, f *Weihrauch reduces to* g ($f \leq_\mathrm{W} g$) if there are Turing functionals Φ and Ψ such that $\Psi(X, g(\Phi(X))) \subseteq f(X)$ whenever X is in the domain of f. The intuition is that, given an input X to f, Φ translates X into an input to g, and Ψ translates X and the possible outputs of $g(\Phi(X))$ back into possible outputs of $f(X)$. Similarly, f *strong Weihrauch reduces to* g ($f \leq_\mathrm{sW} g$) if there are Turing functionals Φ and Ψ such that $\Psi(g(\Phi(X))) \subseteq f(X)$ whenever X is in the domain of f. The difference is that in strong Weihrauch reducibility, Ψ does not have access to the original f-input X. Two functions are *(strong) Weihrauch equivalent* if they reduce to each other, and the *(strong) Weihrauch degrees* are the partial order of (strong) Weihrauch equivalence classes.

Every Π^1_2 statement $\forall X \exists Y \varphi(X, Y)$ corresponds to a multi-valued partial function f whose inputs are the (appropriately coded) X's and whose outputs are the corresponding (and appropriately coded) Y's. For example, weak König's lemma corresponds to the function that maps each infinite binary branching tree to its set of infinite paths. Using this correspondence, we may consider Weihrauch reducibility among Π^1_2 statements of arithmetic. This line of research has been pursued in depth by Brattka and his colleagues [8–12, 24, 51].

Roughly speaking, $\mathsf{Q} \leq_{\mathrm{W}} \mathsf{T}$ is a stronger statement than $\mathsf{RCA}_0 + \mathsf{T} \vdash \mathsf{Q}$, so Weihrauch and strong Weihrauch reducibility can reveal differences among theorems that are equivalent over RCA_0. My work with Dorais, Dzhafarov, Hirst, and Mileti [16] considers Weihrauch and strong Weihrauch reducibility among many statements derived from Ramsey's theorem and from weak König's lemma. One of our main results is that, although Ramsey's theorem for fewer colors can prove Ramsey's theorem for more colors by using multiple applications of Ramsey's theorem for fewer colors, there is no uniformly computable way to solve an instance of Ramsey's theorem for more colors using only one application of Ramsey's theorem for fewer colors.

Theorem 2.1 ([16])**.** *For all $n \geq 1$ and all $j, k \geq 2$ with $j < k$, we have that $\mathsf{RT}^n_k \nleq_{\mathrm{sW}} \mathsf{RT}^n_j$.*

Thus one could describe the implication $\mathsf{RT}^2_2 \to \mathsf{RT}^2_3$ as being *computably true* (as it is provable in RCA_0) but not *uniformly computably true* (as there is no strong Weihrauch reduction).

My recent work with Hölzl [31] builds on Brattka, Hölzl, and Gherardi's study of probability and randomness using the Weihrauch degrees [12]. We study the Weihrauch degree of the function LAY, whose domain is the set of Martin-Löf random sequences and whose outputs for a given Martin-Löf random X are the upper bounds for X's randomness deficiency (i.e., the upper bounds for the least n such that $X \notin \mathcal{U}_n$, where $(\mathcal{U}_n)_{n\in\mathbb{N}}$ is a fixed universal Martin-Löf test). Both Weihrauch reducibility to LAY and layerwise computability (defined by Hoyrup and Rojas [32]) formalize the idea of a function being uniformly computable on Martin-Löf random sequences when also given the input sequence's randomness deficiency. We compare these two notions, finding that Weihrauch reducibility to LAY comprises a wider class of functions than layerwise computability and that LAY does not depend on the universal Martin-Löf test used to define it while layerwise computability does. We also study the algebraic properties of LAY in the Weihrauch degrees and show that it is idempotent in various ways.

3. Medvedev and Muchnik degrees

A *mass problem* is simply a set of functions $\mathcal{A} \subseteq \mathbb{N}^{\mathbb{N}}$. The name comes from the idea that a mass problem $\mathcal{A}$ represents a mathematical problem in the abstract, namely the problem of finding a member of $\mathcal{A}$. This is similar to the previous section's idea that a function $f\colon \subseteq \mathbb{N}^{\mathbb{N}} \rightrightarrows \mathbb{N}^{\mathbb{N}}$ represents the problem whose instances are the members of $\mathrm{dom}(f)$ and an instance X's solutions are the members of $f(X)$. The sets $f(X)$ are mass problems—the set of solutions to the problem coded by X. Unlike with reverse mathematics and the Weihrauch degrees, with mass problems each instance of weak König's lemma, for example, is treated as a separate problem: the problem of finding an infinite path in this particular infinite binary branching tree.

Mass problem $\mathcal{A}$ *Medvedev reduces* (or *strongly reduces*) to mass problem $\mathcal{B}$ ($\mathcal{A} \leq_{\mathrm{s}} \mathcal{B}$) if there is a Turing functional Φ such that $(\Phi(\mathcal{B}) \subseteq \mathcal{A})$. Mass problem $\mathcal{A}$ *Muchnik reduces* (or *weakly reduces*) to mass problem $\mathcal{B}$ ($\mathcal{A} \leq_{\mathrm{w}} \mathcal{B}$) if $(\forall f \in \mathcal{B})(\exists g \in \mathcal{A})(g \leq_{\mathrm{T}} f)$. Two mass problems are *Medvedev (Muchnik) equivalent* if they reduce to each other, and the *Medvedev degrees (Muchnik degrees)* are the partial order of Medvedev (Muchnik) equivalence classes.

Medvedev introduced his degrees in [44] to formalize Kolmogorov's ideas of a "calculus of problems" and a "logic of problem solving." Under the interpretation of mass problems as mathematical problems, $\mathcal{A} \leq_{\mathrm{s}} \mathcal{B}$ means that problem $\mathcal{B}$ is at least as hard as problem $\mathcal{A}$ in a strongly intuitionistic sense: solutions to $\mathcal{B}$ can be translated to solutions to $\mathcal{A}$ by a uniform effective procedure. Muchnik introduced his non-uniform variant in [49].

The Medvedev and Muchnik degrees are intermediate between the Turing degrees and the Weihrauch degrees (the Turing degrees embed into the Medvedev and Muchnik degrees, and the Medvedev degrees embed into the Weihrauch degrees), they enjoy a richer algebraic structure than the Turing degrees and the Weihrauch degrees (the Medvedev and Muchnik degrees are distributive lattices), and they have naturally occurring substructures (obtained by restricting to closed and effectively closed mass problems, for example). I study complexity in the Medvedev and Muchnik degrees, and I study the algebraic properties of these structures.

3.1. Complexity in the degrees of mass problems.

A classic question in computability theory is, given a degree structure such as the Turing, Medvedev, or Muchnik degrees, what is the complexity of its first-order theory? The benchmarks are theories of arithmetic, and the results typically express that these theories are as complicated as possible. Three main classical results are that the first-order theory of the Turing degrees is computably isomorphic to the second-order theory of arithmetic [60], that the first-order theory of the Turing degrees below $\mathbf{0}'$ is computably isomorphic to the first-order theory of arithmetic [59], and that the first-order theory of the Turing degrees of r.e. sets is computably isomorphic to the first-order theory of arithmetic (see [50]). I have an array of analogous results for $\mathcal{D}_{\mathrm{s}}$, $\mathcal{D}_{\mathrm{w}}$, and several of their substructures. The most important substructures are the *effectively closed* Medvedev and Muchnik degrees, which are those obtained by restricting to Π^0_1 subsets of $2^{\mathbb{N}}$. The Π^0_1 subsets of $2^{\mathbb{N}}$ are persistent objects of study throughout computability theory owning to analogies with the r.e. sets and to applications to computable mathematics and reverse mathematics. The effectively closed Medvedev and Muchnik degrees enjoy considerable attention from many authors, beginning with Simpson's suggestion to the Foundations of Mathematics discussion group in August 1999 that the effectively closed Muchnik degrees are analogous to the Turing degrees of r.e. sets but with more natural examples [62].

Theorem 3.1 ([54, 55])**.**

- *The first-order theories of the Medvedev and Muchnik degrees are computably isomorphic to the third-order theory of arithmetic. (This result was obtained independently by Lewis, Nies, and Sorbi* [40]*.)*
- *The first-order theories of the closed Medvedev and Muchnik degrees are computably isomorphic to the second-order theory of arithmetic.*
- *The first-order theory of the effectively closed Medvedev degrees is computably isomorphic to the first-order theory of arithmetic.*

The perhaps most interesting case, that of the first-order theory of the effectively closed Muchnik degrees, is open.

Question 3.2. What is the complexity of the first-order theory of the effectively closed Muchnik degrees?

I show that the first-order theory of the effectively closed Muchnik degrees is undecidable [55], but I do not yet have first-order arithmetic as a lower bound for its complexity.

The effectively closed Medvedev and Muchnik degrees are countable lattices, so one may study the complexity of these structures by asking how complicated it is to present them. I show that presenting the effectively closed Medvedev degrees is equivalent to computing $\mathbf{0}'''$.

Theorem 3.3 ([55])**.** *A Turing degree* $\mathbf{d}$ *computes a presentation of the effectively closed Medvedev degrees if and only if* $\mathbf{d} \geq_{\mathrm{T}} \mathbf{0}'''$*.*

No analogous result for the effectively closed Muchnik degrees is known.

Question 3.4. What is the complexity of presenting the effectively closed Muchnik degrees?

3.2. Algebra and logic in the Medvedev and Muchnik degrees.

In [53], I contribute to the study of the algebraic structure of the Medvedev and Muchnik degrees by answering a question of Sorbi and Terwijn [68] with the following theorem.

Theorem 3.5 ([53])**.** *A Medvedev degree is join-irreducible if and only if it is the degree of a mass problem that is the complement of a Turing ideal. (A mass problem is a Turing ideal if it is closed downward under Turing reducibility and closed under Turing joins.)*

The Medvedev and Muchnik degrees have more structure than that of a distributive lattice. They are *Brouwer algebras*, which means they are distributive lattices with a top element, a bottom element, and the property that for every a and b there is a least c such that $a \vee c \geq b$. This Brouwer algebra structure is a major part of Kolmogorov and Medvedev's original vision because it means that the Medvedev and Muchnik degrees and their subalgebras provide semantics for propositional logic. This aspect of the Medvedev and Muchnik degrees is studied by many authors, the main results being that both structures give semantics for the logic obtained by adding the scheme of *weak excluded middle* ($\neg p \vee \neg\neg p$) to intuitionistic logic [45,67] and that both structures have initial segments that give semantics for intuitionistic logic [38,39,66,68]. My work in [53] also contributes to this study. Unfortunately, the closed and effectively closed Medvedev and Muchnik degrees are not Brouwer algebras [29,41,64] and so do not provide semantics for propositional logics.

Question 3.6. What are the "simplest" natural sublattices of the Medvedev and Muchnik degrees that are Brouwer algebras? Are the Borel, analytic, or co-analytic Medvedev or Muchnik degrees Brouwer algebras?

4. Algorithmic randomness

Algorithmic randomness is a prominent part of computability theory and is concerned with the computational properties of algorithmically unpredictable sequences. The central notion is *Martin-Löf randomness.* A *Martin-Löf test* is a uniformly r.e. sequence $(\mathcal{U}_n)_{n\in\mathbb{N}}$ of open subsets of $2^{\mathbb{N}}$ such that $\forall n(\mu(\mathcal{U}_n) \leq 2^{-n})$, where μ is Lebesgue measure on $2^{\mathbb{N}}$. An $X \in 2^{\mathbb{N}}$ is *Martin-Löf random* if $X \notin \bigcap_{n\in\mathbb{N}} \mathcal{U}_n$ for every Martin-Löf test $(\mathcal{U}_n)_{n\in\mathbb{N}}$. The idea here is that the intersection of a Martin-Löf test is an algorithmically recognizable unusual (i.e., measure 0) collection of sequences and that a sequence is random if it is not unusual. The characterization in terms of unpredictability can be made precise with effective notions of betting strategies.

Algorithmic randomness considerations appear in several places in my work. The reverse mathematics of weak weak König's lemma (the statement that every binary branching tree of *positive measure* has an infinite path) is closely connected to Martin-Löf randomness, and weak weak König's lemma plays a role in my work with Bienvenu and Patey [7] (explained in Section 1.2.2). My work with Hölzl [31] (explained in Section 2) explores the differences between universal Martin-Löf tests and optimal Martin-Löf tests (*à la* Miyabe [48]), particularly with regard to layerwise computability and the Weihrauch degrees.

My work with Bienvenu, Hölzl, and Porter [6] studies algorithmic randomness more directly. In it, we begin to develop a theory of randomness for the so-called *left-r.e. semi-measures*, which are measure-like objects that are naturally induced by Turing functionals. Our results indicate that *weak 2-randomness* (in which the measure condition on a Martin-Löf test is relaxed to $\lim_{n\to\infty} \mu(\mathcal{U}_n) = 0$) may be the best analog of Martin-Löf randomness in this generalized setting.

Furthermore, I am interested in the following question concerning algorithmic randomness and the Medvedev and Muchnik degrees. The problem of randomness extraction, that is, informally, the problem of producing a "more random" sequence from a "less random" sequence, has been studied by many authors. Miller [47] proves a compelling result expressing the difficulty of randomness extraction. For an infinite binary sequence A, the *effective dimension* of A is $\dim(A) = \liminf K(A \restriction n)/n$, where $A \restriction n$ is the finite sequence consisting of the first n bits of A and K is prefix-free Kolmogorov complexity. If $\dim(A) > \dim(B)$, then A is considered to be more random than B. Miller's result is that there is a sequence of effective dimension $1/2$ that does not compute any sequence of effective dimension greater than $1/2$. Thus the sequence in Miller's result is an example of a "less random" sequence that cannot, by itself, produce a "more random" sequence.

The Medvedev and Muchnik degrees provide a convenient language for discussing Miller's result. Recall (from Section 3) that these structures are Brouwer algebras, which means that for every a and b there is a least c such that $a \vee c \geq b$. This least c is denoted $a \to b$. For an $\alpha \in [0,1]$, let

$\mathcal{D}_\alpha = \{X \in 2^{\mathbb{N}} : \dim(X) = \alpha\}$ and let $\mathcal{D}_{>\alpha} = \{X \in 2^{\mathbb{N}} : \dim(X) > \alpha\}$. Then Miller's result can be rephrased either as $\mathcal{D}_{>1/2} \not\leq_{\mathrm{w}} \mathcal{D}_{1/2}$ or as $\mathcal{D}_{1/2} \to \mathcal{D}_{>1/2} >_{\mathrm{w}} 0$. This last phrasing begs the following question.

Question 4.1. What are the Medvedev and Muchnik degrees of $\mathcal{D}_{1/2} \to \mathcal{D}_{>1/2}$?

Answering this question would exactly characterize the difficulty of randomness extraction (at least for sequences of effective dimension 1/2). For example, Miller's result says that randomness extraction is non-trivial. A result of the form $\mathcal{D}_{1/2} \to \mathcal{D}_{>1/2} \equiv_{\mathrm{s}} \mathcal{D}_{>1/2}$ or $\mathcal{D}_{1/2} \to \mathcal{D}_{>1/2} \equiv_{\mathrm{w}} \mathcal{D}_{>1/2}$ would say that randomness extraction is as hard as possible.

5. Honest elementary degrees

Subrecursive degree theory brought degree-theoretic analyses to the class of computable functions in response to difficulties that researchers faced in attempts to classify the computable functions into hierarchies and in attempts to solve difficult problems in computational complexity theory. Machtey [42] and Meyer and Ritchie [46] develop the notion of *honest elementary degree* considered here. Like the Turing degrees, the elementary degrees formalize the hardness relation among functions $f\colon \mathbb{N} \to \mathbb{N}$. Unlike the Turing degrees, the honest elementary degrees are non-trivial when restricted to the computable functions. Thus the honest elementary degrees provide a setting for analyzing complexity among the computable functions. There is also a compelling correspondence between an extension called the *honest ϵ_0-elementary degrees* and provability in Peano arithmetic that is due to Kristiansen, Schlage-Puchta, and Weiermann [37].

A function g is *elementary* in a function f if g can be generated from f, the projection functions, the constant functions, addition, and subtraction by the operations of function composition, bounded sum, and bounded product. A function is *elementary* if it is elementary in the 0 function. A function f has *elementary graph* if the characteristic function of the relation "$f(x) = y$" is elementary, and a function is *honest* if it is monotone, dominates 2^x, and has elementary graph. Two honest functions have the same *honest elementary degree* if they are elementary in each other.

Although the honest elementary degrees are similar in spirit to the Turing degrees, the techniques used to study the honest elementary degrees are quite different than the classical computability-theoretic techniques used to study the Turing degrees. For example, Kristiansen's Growth Theorem [36], which states that, for honest f and g, g is elementary in f if and only if g is bounded by an iterate of f, allows asymptotic analyses in the honest elementary degrees that have no analog in the Turing degrees.

My work in the honest elementary degrees has been mostly concerned with its algebraic structure thus far. An element a of a lattice *cups* to an element $b > a$ if there is a $c < b$ such that $a \vee c = b$, and we say that an element a has the *cupping property* if it cups to every $b > a$. Kristiansen, Schlage-Puchta, and Weiermann [37] show that every sufficiently large honest elementary degree has the cupping property. This prompts them to ask if in fact every non-zero honest elementary degree has the cupping property. I prove that this is not the case by showing that for every sufficiently large (in the same sense as Kristiansen, Schlage-Puchta, and Weiermann) honest elementary degree $\mathbf{b}$, there is a non-zero $\mathbf{a} <_{\mathrm{E}} \mathbf{b}$ that does not cup to $\mathbf{b}$.

Theorem 5.1 ([57]). *Let $f\colon \mathbb{N} \to \mathbb{N}$ be an honest function that eventually dominates every iterate of the exponential function, and let $\mathbf{b} = \deg_{\mathrm{E}}(f)$ denote the honest elementary degree of f. Then there is a non-zero honest elementary degree $\mathbf{a} <_{\mathrm{E}} \mathbf{b}$ that does not cup to $\mathbf{b}$.*

This result of course begs the question of whether or not it can be improved to all $\mathbf{b} >_{\mathrm{E}} \mathbf{0}$. Building on work of Cai [13], I also study cupping in versions of the *degrees of relative provability*, which are closely related to the honest elementary degrees.

Furthermore, I am interested in complexity questions concerning the honest elementary degrees because it would be interesting if the complexity phenomena that are hallmarks of the Turing degrees and related structures are already present in this computable setting.

Question 5.2.

- What is the complexity of the first-order theory of the honest elementary degrees?
- What is the complexity of presenting the honest elementary degrees?

References

[1] Ron Aharoni, *König's duality theorem for infinite bipartite graphs*, Journal of the London Mathematical Society **29** (1984), no. 2, 1–12.

[2] ______, *Menger's theorem for countable graphs*, Journal of Combinatorial Theory, Series B **43** (1987), no. 3, 303–313.

[3] Ron Aharoni and Eli Berger, *Menger's theorem for infinite graphs*, Inventiones Mathematicae **176** (2009), no. 1, 1–62.

[4] Ron Aharoni, Menachem Magidor, and Richard A. Shore, *On the strength of König's duality theorem for infinite bipartite graphs*, Journal of Combinatorial Theory, Series B **54** (1992), no. 2, 257–290.

[5] Klaus Ambos-Spies, Bjørn Kjos-Hanssen, Steffen Lempp, and Theodore A. Slaman, *Comparing DNR and WWKL*, Journal of Symbolic Logic **69** (2004), no. 4, 1089–1104.

[6] Laurent Bienvenu, Rupert Hölzl, Christopher P. Porter, and Paul Shafer, *Randomness and semi-measures*, 2014. to appear in Notre Dame Journal of Formal Logic.

[7] Laurent Bienvenu, Ludovic Patey, and Paul Shafer, *On the logical strengths of partial solutions to mathematical problems*, 2014. preprint.

[8] Vasco Brattka, Matthew de Brecht, and Arno Pauly, *Closed choice and a uniform low basis theorem*, Annals of Pure and Applied Logic **163** (2012), no. 8, 986–1008.

[9] Vasco Brattka and Guido Gherardi, *Effective choice and boundedness principles in computable analysis*, Bulletin of Symbolic Logic **17** (2011), no. 1, 73–117.

[10] ______, *Weihrauch degrees, omniscience principles and weak computability*, Journal of Symbolic Logic **76** (2011), no. 1, 143–176.

[11] Vasco Brattka, Guido Gherardi, and Alberto Marcone, *The Bolzano-Weierstrass theorem is the jump of weak König's lemma*, Annals of Pure and Applied Logic **163** (2012), no. 6, 623–655.

[12] Vasco Brattka, Rupert Hölzl, and Guido Gherardi, *Probabilistic computability and choice*, Information and Computation **242** (2015), 249–286.

[13] Mingzhong Cai, *Higher unprovability*, 2015. preprint.

[14] Peter Cholak, Alberto Marcone, and Reed Solomon, *Reverse mathematics and the equivalence of definitions for well and better quasi-orders*, Journal of Symbolic Logic **69** (2004), no. 3, 683–712.

[15] François G. Dorais, *Reverse mathematics of compact countable second-countable spaces*, 2011. preprint.

[16] François G. Dorais, Damir D. Dzhafarov, Jeffry L. Hirst, Joseph R. Mileti, and Paul Shafer, *On uniform relationships between combinatorial problems*, Transactions of the American Mathematical Society **368** (2016), 1321–1359.

[17] François G. Dorais, Jeffry L. Hirst, and Paul Shafer, *Reverse mathematics, trichotomy and dichotomy*, Journal of Logic and Analysis **4** (2012), 1–14.

[18] ______, *Reverse mathematics and algebraic field extensions*, Computability **2** (2013), no. 2, 75–92.

[19] ______, *Comparing the strength of diagonally non-recursive functions in the absence of Σ^0_2 induction*, Journal of Symbolic Logic **80** (2015), no. 4, 1211–1235.

[20] Stephen Flood, *Reverse mathematics and a Ramsey-type König's Lemma*, Journal of Symbolic Logic **77** (2012), no. 4, 1272–1280.

[21] Harvey M. Friedman, *Some systems of second order arithmetic and their use*, Proceedings of the International Congress of Mathematicians, 1975, pp. 235–242.

[22] Harvey M. Friedman, Stephen G. Simpson, and Rick L. Smith, *Countable algebra and set existence axioms*, Annals of Pure and Applied Logic **25** (1983), no. 2, 141–181.

[23] Emanuele Frittaion, Matthew Hendtlass, Alberto Marcone, Paul Shafer, and Jeroen Van der Meeren, *Reverse mathematics, well-quasi-orders, and Noetherian spaces*, Archive for Mathematical Logic (2016), 1–29.

[24] Guido Gherardi and Alberto Marcone, *How incomputable is the separable Hahn-Banach theorem?*, Notre Dame Journal of Formal Logic **50** (2009), no. 4, 393–425.

[25] Mariagnese Giusto and Stephen G. Simpson, *Located sets and reverse mathematics*, Journal of Symbolic Logic **65** (2000), no. 3, 1451–1480.

[26] Jean Goubault-Larrecq, *On Noetherian spaces*, Proceedings of the 22nd Annual IEEE Symposium on Logic in Computer Science (LICS'07), July 2007, pp. 453–462.

[27] ———, *Noetherian spaces in verification*, Proceedings of the 37th International Colloquium on Automata, Languages and Programming (ICALP'10) – Part II, July 2010, pp. 2–21.

[28] Noam Greenberg and Joseph Miller, *Lowness for Kurtz randomness*, Journal of Symbolic Logic **74** (2009), no. 2, 665–678.

[29] Kojiro Higuchi, *Effectively closed mass problems and intuitionism*, Annals of Pure and Applied Logic **163** (2012), no. 6, 693–697.

[30] Jeffry L. Hirst and Carl Mummert, *Reverse mathematics and uniformity in proofs without excluded middle*, Notre Dame Journal of Formal Logic **52** (2011), no. 2, 149–162.

[31] Rupert Hölzl and Paul Shafer, *Universality, optimality, and randomness deficiency*, Annals of Pure and Applied Logic **166** (2015), no. 10, 1049–1069.

[32] Mathieu Hoyrup and Cristóbal Rojas, *An application of Martin-Löf randomness to effective probability theory*, Mathematical Theory and Computational Practice, 2009, pp. 260–269.

[33] Carl G. Jockusch Jr., *Degrees of functions with no fixed points*, Logic, Methodology and Philosophy of Science VIII (1989), 191–201.

[34] Carl G. Jockusch Jr. and Robert I. Soare, *Π^0_1 classes and degrees of theories*, Transactions of the American Mathematical Society **173** (1972), 33–56.

[35] Bjørn Kjos-Hanssen, *Infinite subsets of random sets of integers*, Mathematics Research Letters **16** (2009), 103–110.

[36] Lars Kristiansen, *Information content and computational complexity of recursive sets*, Gödel '96 (Brno, 1996), 1996, pp. 235–246.

[37] Lars Kristiansen, Jan-Christoph Schlage-Puchta, and Andreas Weiermann, *Streamlined subrecursive degree theory*, Annals of Pure and Applied Logic **163** (2012), no. 6, 698–716.

[38] Rutger Kuyper, *Natural factors of the Muchnik lattice capturing IPC*, Annals of Pure and Applied Logic **164** (2013), no. 10, 1025–1036.

[39] ———, *Natural factors of the Medvedev lattice capturing IPC*, Archive for Mathematical Logic (2014), 1–15.

[40] Andrew E.M. Lewis, André Nies, and Andrea Sorbi, *The first order theories of the Medvedev and Muchnik lattices*, CiE, 2009, pp. 324–331.

[41] Andrew E.M. Lewis, Richard A. Shore, and Andrea Sorbi, *Topological aspects of the Medvedev lattice*, Archive for Mathematical Logic **50** (2011), no. 3–4, 319–340.

[42] Michael Machtey, *Augmented loop languages and classes of computable functions*, Journal of Computer and System Sciences **6** (1972), 603–624.

[43] Alberto Marcone, *Wqo and bqo theory in subsystems of second order arithmetic*, Reverse mathematics 2001, 2005, pp. 303–330.

[44] Yuri T. Medvedev, *Degrees of difficulty of the mass problems*, Doklady Akademii Nauk SSSR (NS), 1955, pp. 501–504.

[45] ———, *Finite problems*, Doklady Akademii Nauk SSSR (NS), 1962, pp. 1015–1018.

[46] Albert R. Meyer and Dennis M. Ritchie, *A classification of the recursive functions*, Zeitschrift für Mathematische Logik und Grundlagen der Mathematik **18** (1972), 71–82.

[47] Joseph S. Miller, *Extracting information is hard: a Turing degree of non-integral effective Hausdorff dimension*, Advances in Mathematics **226** (2011), no. 1, 373–384.

[48] Kenshi Miyabe, *The difference between optimality and universality*, Logic Journal of the Interest Group in Pure and Applied Logics **20** (2012), no. 1, 222–234.

[49] Albert A. Muchnik, *On strong and weak reducibilities of algorithmic problems*, Sibirskii Matematicheskii Zhurnal **4** (1963), 1328–1341.

[50] André Nies, Richard A. Shore, and Theodore A. Slaman, *Interpretability and definability in the recursively enumerable degrees*, Proceedings of the London Mathematical Society **77** (1998), no. 3, 241–291.

[51] Arno Pauly, *On the (semi)lattices induced by continuous reducibilities*, Mathematical Logic Quarterly **56** (2010), no. 5, 488–502.

[52] Klaus-Peter Podewski and Karsten Steffens, *Injective choice functions for countable families*, Journal of Combinatorial Theory, Series B **21** (1976), no. 1, 40–46.

[53] Paul Shafer, *Characterizing the join-irreducible Medvedev degrees*, Notre Dame Journal of Formal Logic **52** (2011), no. 1, 21–38.

[54] ———, *Coding true arithmetic in the Medvedev and Muchnik degrees*, Journal of Symbolic Logic **76** (2011), no. 1, 267–288.

[55] ———, *Coding true arithmetic in the Medvedev degrees of Π^0_1 classes*, Annals of Pure and Applied Logic **163** (2012), no. 3, 321–337.

[56] ———, *Menger's theorem in Π^1_1-CA_0*, Archive for Mathematical Logic **51** (2012), no. 3-4, 407–423.

[57] ———, *Honest elementary degrees and degrees of relative provability without the cupping property*, 2016. preprint.

[58] ———, *The reverse mathematics of the Tietze extension theorem*, 2016. to appear in Proceedings of the American Mathematical Society.

[59] Richard A. Shore, *The theory of the degrees below* $\mathbf{0}'$, Journal of the London Mathematical Society **24** (1981), 1–14.

[60] Stephen G. Simpson, *First-order theory of the degrees of recursive unsolvability*, Annals of Mathematics **105** (1977), no. 1, 121–139.

[61] ———, *On the strength of König's duality theorem for countable bipartite graphs*, Journal of Symbolic Logic **59** (1994), no. 1, 113–123.

[62] ———, *FOM: natural r.e. degrees; Pi01 classes*, 1999.

[63] ———, *Why the recursion theorists ought to thank me (talk given at the Annual Meeting of the American Philosophical Association)*, 2001.

[64] ———, *Mass problems and intuitionism*, Notre Dame Journal of Formal Logic **49** (2008), no. 2, 127–136.

[65] ———, *Subsystems of Second Order Arithmetic*, Cambridge University Press, 2009.

[66] Elena Z. Skvortsova, *A faithful interpretation of the intuitionistic propositional calculus by means of an initial segment of the Medvedev lattice*, Sibirskii Matematicheskii Zhurnal **29** (1988), no. 1, 171–178.

[67] Andrea Sorbi, *Embedding Brouwer algebras in the Medvedev lattice*, Notre Dame Journal of Formal Logic **32** (1991), no. 2, 266–275.

[68] Andrea Sorbi and Sebastiaan A. Terwijn, *Intermediate logics and factors of the Medvedev lattice*, Annals of Pure and Applied Logic **155** (2008), no. 2, 69–85.

[69] Henry Towsner, *Partial impredicativity in reverse mathematics*, Journal of Symbolic Logic **78** (2013), no. 2, 459–488.

[70] Klaus Weihrauch, *The degrees of discontinuity of some translators between representations of the real numbers*, Informatik-Berichte, International Computer Science Institute, Berkeley, 1992.

[71] ———, *The TTE interpretation of three hierarchies of omniscience principles*, Informatik-Berichte, FernUniversität Hagen, Hagen, 1992.

Department of Mathematics, Ghent University, Krijgslaan 281, S22, 9000 Ghent, Belgium
E-mail address: `paul.shafer@ugent.be`
URL: `http://cage.ugent.be/~pshafer/`