THE MEDVEDEV LATTICE OF COMPUTABLY CLOSED SETS

Sebastiaan A. Terwijn*

Abstract

Simpson introduced the lattice $\mathfrak{P}$ of Π^0_1 classes under Medvedev reducibility. Questions regarding completeness in $\mathfrak{P}$ are related to questions about measure and randomness. We present a solution to a question of Simpson about Medvedev degrees of Π^0_1 classes of positive measure that was independently solved by Simpson and Slaman. We then proceed to discuss connections to constructive logic. In particular we show that the dual of $\mathfrak{P}$ does not allow an implication operator (i.e. that $\mathfrak{P}$ is not a Heyting algebra). We also discuss properties of the class of PA-complete sets that are relevant in this context.

Keywords: Π^0_1 classes – Medvedev reducibility – intuitionistic propositional logic.
Mathematics Subject Classification: 03D30, 03B55, 03G10.

1 Introduction

The Medvedev lattice $\mathfrak{M}$ was introduced in [11] as an implementation of Kolmogorov's idea of a "calculus of problems". Let us briefly recall the definition of $\mathfrak{M}$. Let ω denote the naturals and let ω^ω be the set of all functions from ω to ω (Baire space). A *mass problem* is a subset of ω^ω. We think of such subsets as a "problem", namely the problem of producing an element of it, and so we can think of the elements of the mass problem as its set of solutions. We say that a mass problem $\mathcal{A}$ *Medvedev reduces* to mass problem $\mathcal{B}$ if there is an effective procedure of transforming solutions to $\mathcal{B}$ into solutions to $\mathcal{A}$. Formally: $\mathcal{A} \leq_M \mathcal{B}$ if there is a recursive functional $\Psi : \omega^\omega \to \omega^\omega$ such that for all $f \in \mathcal{B}$, $\Psi(f) \in \mathcal{A}$. The relation $\leq_M$ induces an equivalence relation on mass problems: $\mathcal{A} \equiv_M \mathcal{B}$ if $\mathcal{A} \leq_M \mathcal{B}$ and $\mathcal{B} \leq_M \mathcal{A}$.

*Institute of Discrete Mathematics and Geometry, Technical University of Vienna, Wiedner Hauptstrasse 8–10/E104, A-1040 Vienna, Austria, terwijn@logic.at. Supported by the Austrian Research Fund (Lise Meitner grant M699-N05).

The equivalence class of $\mathcal{A}$ is denoted by $[\mathcal{A}]$ and is called the *Medvedev degree*, or the *degree of difficulty* of $\mathcal{A}$. We usually denote Medvedev degrees by boldface symbols. There is a smallest Medvedev degree, denoted by $\mathbf{0}$, namely the degree of any mass problem containing a computable function. There is also a largest degree $\mathbf{1}$, the degree of the empty mass problem, of which it is impossible to produce an element by whatever means. Finally, it is possible to define a meet operator $\times$ and a join operator $+$ on mass problems: For functions f and g, as usual define the function $f \oplus g$ by $f \oplus g(2x) = f(x)$ and $f \oplus g(2x+1) = g(x)$. Let $n\frown\mathcal{A} = \{n\frown f : f \in \mathcal{A}\}$, where $\frown$ denotes concatenation. Define

$$\mathcal{A} + \mathcal{B} = \big\{ f \oplus g : f \in \mathcal{A} \wedge g \in B \big\}$$

and

$$\mathcal{A} \times \mathcal{B} = 0\frown\mathcal{A} \cup 1\frown\mathcal{B}.$$

It is not hard to show that $\times$ and $+$ indeed define a greatest lower bound and a least upper bound operator on the Medvedev degrees:[1] The structure $\mathfrak{M}$ of all Medvedev degrees, ordered by $\leq_M$ and together with $+$ and $\times$ is a distributive lattice [11]. But $\mathfrak{M}$ carries more structure as the following theorem shows.

A distributive lattice $\mathfrak{L}$ with 0, 1 is called a *Brouwer algebra* if for any elements a and b one can show that the element $a \to b$ defined by

$$a \to b := \text{least}\big\{ c \in \mathfrak{L} : b \leq a + c \big\}$$

always exists. (Here $+$ denotes the join operator of $\mathfrak{L}$.)

Theorem 1.1 (Medvedev [11]) *$\mathfrak{M}$ is a Brouwer algebra.*

Proof. Define $\mathcal{A} \to \mathcal{B} = \big\{ n\frown f : (\forall g \in \mathcal{A})[\Phi_n(g \oplus f) \in \mathcal{B}] \big\}$, where Φ_n is the n-th partial recursive functional. □

[1] There is an annoying notational conflict between the various papers in this area. Sorbi [24] maintains the usual lattice theoretic notation with $\wedge$ for meet and $\vee$ for join, but e.g. Rogers [16] and Skvortsova [20] use $\wedge$ and $\vee$ exactly the other way round! The advantage of the latter choice will become clear below, namely that $\wedge$ and $\vee$ then nicely correspond with "and" and "or" in the propositional logic corresponding to the lattice. To avoid confusion we introduced in [27] separate notation for the lattices ($+$ for join and $\times$ for meet) and the logic (the usual $\wedge$ for "and" and $\vee$ for "or"). This is in line with notation that is used in some textbooks on lattice theory, cf. [1]. It has as an additional advantage that the join operator $+$ in $\mathfrak{M}$ corresponds to the usual notation $\oplus$ for the join operator in the Turing degrees.

$\mathfrak{L}$ is called a *Heyting algebra* if its dual is a Brouwer algebra. Sorbi [21] has shown that $\mathfrak{M}$ is not a Heyting algebra. Some more discussion and facts about $\mathfrak{M}$ can be found in Rogers [16]. A good survey of what is known about $\mathfrak{M}$ is Sorbi [24], where also a more complete list of references can be found.

Simpson (see e.g. [17, 18]) introduced the structure $\mathfrak{P}$ of Medvedev degrees of nonempty Π^0_1 subsets of 2^ω. This is a lattice under Medvedev reducibility in the same way as $\mathfrak{M}$, with meet $\times$ and join $+$ defined as before. $\mathfrak{P}$ has smallest element $\mathbf{0}$, the degree of 2^ω, and largest degree $\mathbf{1}$, the degree of the class of all PA-complete sets. For information about Π^0_1 classes in general we refer to the survey by Cenzer [4]. The following is a sample of results showing what is possible for Π^0_1 classes under Medvedev reducibility. The list is of course not exhaustive.

- (Binns and Simpson [3]) Every finite distributive lattice is embeddable into $\mathfrak{P}$.
- (Cenzer and Hinman [5]) $\mathfrak{P}$ is dense.
- (Binns [2]) Every degree in $\mathfrak{P}$ splits in two lesser ones.

In section 2 we will discuss the Medvedev degrees of Π^0_1 classes of positive measure. The Medvedev lattice has some very interesting connections to constructive logics such as intuitionistic propositional logic. In section 4 we briefly review these connections and extend the discussion to $\mathfrak{P}$. In particular we discuss some relevant properties of the class of PA-complete sets. In section 3 we prove that $\mathfrak{P}$ is not a Heyting algebra.

We conclude this section with some definitions that we will use later. Note that $\mathcal{A} \leq_M \mathcal{B}$ means that there is a *uniform* way to transform solutions for the one problem into solutions to the other. There is also an interesting *nonuniform* variant of this definition [13]: We say that $\mathcal{A}$ *Muchnik reduces* to $\mathcal{B}$, denoted $\mathcal{A} \leq_w \mathcal{B}$, if $(\forall f \in \mathcal{B})(\exists g \in \mathcal{A})[f \leq_T g]$, where $\leq_T$ denotes Turing reducibility. The corresponding degrees are called *Muchnik degrees*. They form a distributive lattice in the same way as the Medvedev degrees.

A Π^0_1 class is called *special* when it is nonempty and it does not have any computable elements. Our notation is fairly standard. Unexplained notation from computability theory can be found e.g. in Odifreddi [14]. We use the following notation for finite strings. 2^ω is the Cantor space of infinite binary strings, and $2^{<\omega}$ is the tree of finite binary strings. μ is the uniform Lebesgue measure on 2^ω. $\sigma \sqsupseteq \tau$ denotes that the finite or infinite string σ extends the finite string τ. $[\sigma]$ denotes the set $\{X \in 2^\omega : X \sqsupset \sigma\}$. If no confusion can be caused by it we will sometimes denote by 2^n the set of binary strings of length n.

2 Medvedev reducibility and sets of positive measure

As pointed out by Simpson [17, 18], the structure $\mathfrak{P}$ possesses many natural elements that are strictly between $\mathbf{0}$ and $\mathbf{1}$. In particular he showed that completeness in $\mathfrak{P}$ is related to measure theory.

Theorem 2.1 (Simpson [17]) *Let P be any special Π^0_1 class of positive measure. Then the Medvedev degree of P is strictly between $\mathbf{0}$ and $\mathbf{1}$.*

The proof of Theorem 2.1 uses considerations about 1-random sets, such as Theorem 2.2 below. For the definition, discussion, and references about 1-random sets see e.g. [26].

Define the *left shift* $T : 2^\omega \to 2^\omega$ by $T(X)(n) = X(n+1)$. Let T^k denote the k-iteration of T.

Theorem 2.2 (Kučera [10]) *For any Π^0_1 class $\mathcal{P}$ of positive measure we have the following: For every 1-random X there exists $k \in \omega$ such that $T^k(X) \in \mathcal{P}$.*

It follows from Theorem 2.2 that in particular

$$(\forall X \text{ 1-random })(\exists Y \in \mathcal{P})[X \equiv_T Y]. \tag{1}$$

Next we show that Theorem 2.2 and its corollary (1) do not hold *uniformly*:

Proposition 2.3 *Let $\mathcal{P}$ be any special Π^0_1 class of positive measure. Then $\mathcal{P} \not\leq_M \mathcal{R}$, where $\mathcal{R}$ is the class of 1-random sets.*

Proof. Suppose that $\mathcal{P} \leq_M \mathcal{R}$ via the partial recursive functional Φ. Then $\mathrm{dom}(\Phi)$ contains a computable set: Since $\mathcal{R}$ is dense in 2^ω we can recursively find for any $\sigma \in 2^{<\omega}$ an extension $\tau \sqsupset \sigma$ such that $\Phi(\tau)\downarrow$. Let $X \in \mathrm{dom}(\Phi)$ be computable. Then $\Phi(X)$ is also computable, hence since $\mathcal{P}$ is special there is n such that $\Phi(X{\upharpoonright}n) \in \mathcal{U}$, where $\mathcal{U}$ is the open complement of $\mathcal{P}$. Now let Z be a 1-random set extending $X{\upharpoonright}n$. Then $\Phi(Z) \in \mathcal{U}$, but also $\Phi(Z) \in \mathcal{P}$ by assumption on Φ, which is a contradiction. $\square$

Simpson [17], using Theorem 2.2, proved that the *Muchnik* degrees of positive measure have a largest element. The next theorem shows that this does not hold for the Medvedev degrees, answering a question posed by

Simpson. This result was obtained independently and earlier by Simpson and Slaman [19] (personal communication Simpson, March 2004). These authors also proved that every nonzero Muchnik degree of a Π^0_1 subset of 2^ω contains Π^0_1 subsets of infinitely many distinct Medvedev degrees.

Our proof makes use of the following elementary combinatorial lemma:

Lemma 2.4 *Let the real interval $[0,H]$ be partitioned in N pieces σ, ordered by length from left to right in decreasing order. Let $J < H$. Then the number of pieces σ contained in $[0,J]$ is bounded by $\lfloor \frac{J}{H} N \rfloor$, i.e. the optimum is reached when all σ have length equal to the average $\frac{H}{N}$.*

Proof. This can be proved by induction on N. □

Theorem 2.5 *The set of elements of $\mathfrak{P}$ of positive measure does not have a maximal element.*

Proof. Suppose that $\mathcal{P} \in \mathfrak{P}$ of positive measure is given as the complement of the Σ^0_1 class $\mathcal{U}$. We construct a Π^0_1 class $\mathcal{Q}$ of positive measure such that $\mathcal{Q} \not\leq_M \mathcal{P}$. We will make $\mathcal{Q} \subseteq \mathcal{P}$ so that $\mathcal{P} \leq_M \mathcal{Q}$ and hence $\mathcal{Q}$ is strictly bigger than $\mathcal{P}$. Without loss of generality $\mu(\mathcal{U}) < 1/4$ and $\mathcal{U}$ is given as a computable prefix-free set of strings U. We construct the Π^0_1 class $\mathcal{Q}$ as the complement of an effectively open set V such that for all e

$$R_e: \qquad \mathcal{P} \subseteq \mathrm{dom}(\Phi_e) \Longrightarrow (\exists X \in \mathcal{P})[\,\Phi_e(X) \notin \mathcal{Q}\,].$$

$$M: \qquad \mu(V) < 1.$$

Clearly, the requirement M will make $\mathcal{Q}$ a set of positive measure, and the requirement R_e guarantees that Φ_e does not reduce $\mathcal{Q}$ to $\mathcal{P}$. For notational convenience we start counting at 3, so we only have to consider R_e with $e \geq 3$. The construction is in fact not difficult since there is no conflict between the requirements R_e. We only have to satisfy them in such a way that M is satisfied. We will have $U \subseteq V$, and we let R_e add at most an additional amount of $2^{-e} + \mu(U)$ in measure to V, where the "$\mu(U)$-part" is shared with all other R_e-requirements, so that if a part of this is added to V by R_e then another $R_{e'}$ does not have to add it anymore. This will ensure that $\mu(V) < 1$.

Note that if $\mathcal{Q} \leq_M \mathcal{P}$ via Φ_e then by compactness of 2^ω there exist a level $n \geq e$ and a stage s in the enumeration of U such that for all $\tau \in 2^n$, either $[\tau] \subseteq \mathcal{U}_s$ or the string $\Phi_{e,s}(\tau)$ is defined and has length $\geq e$. Now the idea to satisfy R_e is the following. We wait until we see n and s as above. Then if we delete the string $\sigma = \Phi_{e,s}(\tau)\restriction e$ from $\mathcal{Q}$ by putting it into V we have a potential candidate for an $X \in \mathcal{P}$ such that $\Phi_e(X) \notin \mathcal{Q}$. We need that σ is not too short in order not to add too much measure to V. However, it may happen that later all the τ with $\Phi_{e,s}(\tau) \sqsupseteq \sigma$ turn out to be in U. Then we have to pick a new σ and repeat the procedure. Every time we add a σ to V we add the amount 2^{-e} in measure to $\mu(V)$. In order to prevent $\mu(V)$ from growing too big we have to bound the number of times we have to pick a new σ. We do this by picking first those σ's that have the largest *weight*, i.e. those that get mapped the largest number of τ's to them. Since in order to disqualify σ all these τ's have to enter U, and $\mu(U)$ is bounded, not too many σ's will be disqualified. We now describe the construction in more technical detail.

Construction At stage $s = 0$ of the construction we let $V_0 = U_0$. At stage $s+1$, add all strings from $U_{s+1} - U_s$ to V_{s+1}. We say that requirement R_e with $e \leq s$ requires attention at $s+1$ if there is $n \leq s$ such that for all $\tau \in 2^n$ either we have $\tau \in U_s$ or $\Phi_s(\tau)\downarrow$ and has length $\geq e$. Given such n, let the *weight* of $\sigma \in 2^e$ at stage $s+1$ be

$$\sum \left\{2^{-n} : \tau \in 2^n \wedge \tau \notin U_s \wedge \Phi_{e,s}(\tau)\downarrow\sqsupseteq \sigma\right\}.$$

Now for every R_e that requires attention at $s+1$ and that does not have a current witness σ, let n as above be minimal, select $\sigma \in 2^e$ such that σ has maximal weight and put σ into V. We say that σ is the current witness of R_e. If at a later stage it happens that all $\tau \in 2^n$ with $\Phi_{e,s}(\tau)\downarrow\sqsupseteq \sigma$ have entered U then we say that σ is disqualified and that R_e has no current witness. This completes the construction.

We verify that every R_e is eventually satisfied. For this it suffices to show that after a certain stage of the construction R_e never requires attention or its witness is never disqualified. We do this by giving an explicit bound on the number of times this can happen.

Suppose that at some stage s the string σ is put into V for the sake of R_e, and n is the level as in the construction. If at the end of the construction there is a $\tau \in 2^n$ such that $[\tau] \nsubseteq \mathcal{U}$ then there is an $X \in \mathcal{P}$ extending τ such that $\Phi_e(X) \sqsupset \sigma \notin \mathcal{Q}$, hence R_e is satisfied. But the action for R_e may be destroyed when during the construction $[\tau] \subseteq \mathcal{U}$ (either because τ enters U or because a (by compactness finite) number of strings covering $[\tau]$ enter U). If this happens for all τ with $\Phi_e(\tau)\downarrow\sqsupseteq \sigma$ we have to pick a new σ and repeat. Now the weights of all the $\sigma \in 2^e$ give a partition on $[0, 1 - \mu(\mathcal{U}_s)]$, so by the combinatorial Lemma 2.4 (with $H = 1 - \mu(\mathcal{U}_s)$, $J = \mu(\mathcal{U}) - \mu(\mathcal{U}_s)$, and $N = 2^e$) this can happen at most

$$\left\lfloor \frac{\mu(\mathcal{U}) - \mu(\mathcal{U}_s)}{1 - \mu(\mathcal{U}_s)} 2^e \right\rfloor \leq \mu(\mathcal{U}) 2^e$$

times. Every time 2^{-e} in measure is added to $\mu(V)$, so in total at most $\mu(U) + 2^{-e}$ (the number of disqualifications $+1$) is added to $\mu(V)$ by R_e. Moreover, measure added by R_e on the basis of a "false" σ that is later discarded is not added by any other $R_{e'}$. Thus the total extra amount added to V is less than $\sum_{e \geq 3} 2^{-e} + \mu(U) < 1/2$, so that $\mu(V) < \mu(U) + 1/2 < 1$. Hence the measure requirement M is also satisfied. This concludes the proof of the theorem. □

3 $\mathfrak{P}$ is not a Heyting algebra

In this section we prove that the dual of $\mathfrak{P}$ is not an implicative lattice. The motivation for this comes from the connection with constructive logic discussed in section 4. We first prove a lemma. Note that for mass problems $\mathcal{A}$ and $\mathcal{B}$, $\mathcal{A} \times \mathcal{B}$ is basically a disjoint union of $\mathcal{A}$ and $\mathcal{B}$. We can of course take the disjoint union of more sets at a time: For mass problems $\mathcal{A}_n$, $n \in \omega$, define

$$\textstyle\prod_{n \in \omega} \mathcal{A}_n = \left\{ n\widehat{\ } f \in \omega^\omega : f \in \mathcal{A}_n \right\}.$$

Lemma 3.1 *There exist $\mathcal{A} \in \mathfrak{P}$ and a uniform sequence $\mathcal{B}_n \in \mathfrak{P}$, $n \in \omega$, such that*

(i) *For every m, $\prod_{n \neq m} \mathcal{B}_n \not\leq_M \mathcal{B}_m$,*

(ii) *For every n, $\mathcal{A} \leq_M \mathcal{B}_n$,*

(iii) *For every n, $(\forall X \in \mathcal{B}_n)[\, \Phi_n(X) \notin A \,]$.*

Proof. $\mathcal{A}$ and the $\mathcal{B}_n$ can be constructed using methods similar to the ones used in Binns and Simpson [3], which in turn uses ideas from Jockusch and Soare [8, 9].

By [3, Theorem 2.1], let $\{\mathcal{C}_n\}_{n \in \omega}$ be a uniform sequence of Π^0_1 classes satisfying the strong independence property

(iv) $(\forall m)(\forall e)(\forall X \in \mathcal{C}_m)[\, \Phi_e(X) \notin \prod_{n \neq m} \mathcal{C}_n \,]$.

Clearly property (iv) implies (i).

Now we build $\mathcal{A}$ and the $\mathcal{B}_n$, where the latter are only a slight modification of the $\mathcal{C}_n$. To build $\mathcal{A}$ satisfying (ii) and (iii) it is actually not needed to know exactly how the $\mathcal{C}_n$ have been constructed. We define $\mathcal{A} = \prod_m \mathcal{A}_m$, where the $\mathcal{A}_m$ are a permutation of the $\mathcal{B}_n$ together with a number of copies of the empty Π^0_1 class. The idea is that we assign the classes $\mathcal{C}_n$ to locations $m \in \omega$ (where we think of m as the m-th location in the product $\prod_m \mathcal{A}_m$). If $\mathcal{C}_n$ is assigned to location m we let $\mathcal{A}_m = \mathcal{B}_n = \mathcal{C}_n$, until, if ever, we see that Φ_n tries to map something to location m. In that case we redefine $\mathcal{B}_n$ in such a way to make sure that Φ_n maps all of $\mathcal{B}_n$ to location m, we make $\mathcal{A}_m = \emptyset$, and we relocate $\mathcal{C}_n$ to another location. This will ensure property (iii).

Simultaneous construction of $\mathcal{A}$ and the $\mathcal{B}_n$. At stage $s = 0$ all $\mathcal{A}_m$ are empty. At the start of the construction no $\mathcal{C}_n$ is assigned a location yet. The $\mathcal{B}_n$ start out by copying the $\mathcal{C}_n$.

At stage $s+1$ we have started the construction of finitely many $\mathcal{A}_m$, and the first s $\mathcal{C}_n$ have been assigned a location.

For every $n \leq s$ see if there is a string σ, $|\sigma| \leq s$, such that $\Phi_{n,s}(\sigma)(0)\downarrow= m$ for some m. This means that Φ_n maps something to location m. If $\mathcal{C}_n$ happens to be assigned to location m, we *relocate* it to a fresh location, namely to the smallest location m' that is not yet in use. In this case we also change the definition of $\mathcal{B}_n$, and for the rest of the construction $\mathcal{B}_n$ will copy the Π^0_1 class $\sigma\widehat{\ }\mathcal{C}_n$, i.e. we start the copying of $\mathcal{C}_n$ anew, but now we move it above σ.

Next pick the first location m that is not yet in use, and assign $\mathcal{C}_{s+1}$ to m.

Finally we define the $\mathcal{A}_m$ as follows. First note that every location m gets assigned some $\mathcal{C}_n$ during the construction. If m gets assigned $\mathcal{C}_n$, then define $\mathcal{A}_m = \mathcal{B}_n$, until, if ever, $\mathcal{C}_n$ is relocated, in which case we redefine $\mathcal{A}_m = \emptyset$. Clearly $\mathcal{A}_m$ is Π^0_1. This completes the construction of $\mathcal{A}$ and the $\mathcal{B}_n$.

To verify that $\mathcal{A}$ and the $\mathcal{B}_n$ satisfy (i)–(iii), first note that the $\mathcal{B}_n$ still satisfy (iv) (because the $\mathcal{C}_n$ satisfy (iv)), and hence satisfy (i). Further note that every $\mathcal{C}_n$ is assigned a location (namely at stage $n+1$) and that it is relocated at most once (namely if Φ_n tries to map some σ to the location of $\mathcal{C}_n$). If $\mathcal{C}_n$ is initially assigned to location m and is never relocated, then $\mathcal{A}_m = \mathcal{B}_n = \mathcal{C}_n$. If $\mathcal{C}_n$ is later relocated to m' then $\mathcal{A}_m = \emptyset$ and $\mathcal{B}_n$ is of the form $\sigma\widehat{\ }\mathcal{C}_n$, $\mathcal{A}_{m'} = \mathcal{B}_n$, and $(\forall X \in \mathcal{B}_n)[\,\Phi_n(X)(0) = m\,]$. From this it is clear that $\mathcal{A} \leq_M \mathcal{B}_n$, hence item (ii) is also satisfied. Finally, to see that (iii) is satisfied, note that if $X \in \mathcal{B}_n$ and $\Phi_n(X)(0)\downarrow= m$, then either some $\mathcal{C}_k$ with $k \neq n$ is assigned to location m, in which case $\Phi_n(X) \notin \mathcal{A}_m$ by property (iv), or $\mathcal{C}_n$ is assigned to location m, in which case it is relocated and $\mathcal{A}_m = \emptyset$, hence again $\Phi_n(X) \notin \mathcal{A}_m$. This concludes the proof of the lemma. $\square$

Theorem 3.2 $\mathfrak{P}$ *is not a Heyting algebra.*

Proof. The proof builds on a scheme also used by Sorbi in his proof that $\mathfrak{M}$ is not a Heyting algebra [21, Theorem 5.4] (the situation here being more complicated because single sets are replaced by Π^0_1 classes).

Let $\mathcal{A}$ and $\mathcal{B}_n$ be as in Lemma 3.1, and let $\mathcal{B} = \prod_{n\in\omega} \mathcal{B}_n$. We claim that the set

$$\big\{\mathcal{C} \in \mathfrak{P} : \mathcal{A} \times \mathcal{C} \leq_M \mathcal{B}\big\}$$

does not have a largest (in fact, not even a maximal) element. Suppose that $\mathcal{A} \times \mathcal{C} \leq_M \mathcal{B}$ via Ψ. Define

$$\mathcal{B}' = \big\{X \in \mathcal{B} : \Psi(X)(0) = 1\big\},$$

i.e. $\mathcal{B}'$ consists of everything in $\mathcal{B}$ that is mapped to the $\mathcal{C}$-side. Clearly $\mathcal{B}' \in \mathfrak{P}$, and it is easily checked that $\mathcal{B} \leq_M \mathcal{B}'$ (via the identity) and $\mathcal{C} \leq_M \mathcal{B}'$. Also, we have $\mathcal{A} \times \mathcal{B}' \leq_M \mathcal{B}$. By item (iii) in Lemma 3.1, there exists n such that $\mathcal{B}_n \subseteq \mathcal{B}'$ (namely, if $\Psi = \Phi_n$ then Ψ has to send all $X \in \mathcal{B}_n$ to $\mathcal{C}$). Now consider $\mathcal{B}' - \mathcal{B}_n$. Normally the difference of two Π^0_1 classes need not be Π^0_1, but in this case it is because all the $\mathcal{B}_n$ are neatly separated in $\mathcal{B}$. Since $\mathcal{A} \leq_M \mathcal{B}_n$ by item (ii) in Lemma 3.1, we also have $\mathcal{A} \times (\mathcal{B}' - \mathcal{B}_n) \leq_M \mathcal{B}$ because the elements that got sent to $\mathcal{B}_n$ can be sent on to $\mathcal{A}$. On the other hand, $\mathcal{B}' - \mathcal{B}_n \not\leq_M \mathcal{B}'$ because of $\mathcal{B}_n \subseteq \mathcal{B}'$ and item (i) in Lemma 3.1. So $\mathcal{B}' - \mathcal{B}_n$ is strictly bigger than $\mathcal{B}'$, hence strictly bigger than $\mathcal{C}$, and as we have seen it still caps with $\mathcal{A}$ below $\mathcal{B}$. Hence $\mathcal{C}$ was not a maximal element with this property. $\square$

4 Logic, Π^0_1 classes, and PA-complete sets

The original motivation for studying the Medvedev lattice was to give a computational semantics for the intuitionistic propositional calculus IPC. We first make precise what is meant by this. In section 1 we have already defined the operations $\times$, $+$, and $\rightarrow$ on $\mathfrak{M}$. We can also define a negation operator $\neg$ by defining $\neg\mathbf{A} = \mathbf{A} \rightarrow \mathbf{1}$ for any Medvedev degree $\mathbf{A}$. More generally, given any Brouwer algebra $\mathfrak{L}$ (such as $\mathfrak{M}$) with join denoted by $+$ and meet by $\times$, we can evaluate propositional formulas as follows. An $\mathfrak{L}$-*valuation* is a function v : Form $\rightarrow \mathfrak{L}$ from formulas to $\mathfrak{L}$ such that for all formulas α and β, $v(\alpha \vee \beta) = v(\alpha) \times v(\beta)$, $v(\alpha \wedge \beta) = v(\alpha) + v(\beta)$,

$v(\alpha \to \beta) = v(\alpha) \to v(\beta)$, $v(\neg\alpha) = v(\alpha) \to 1$.[2] Write $\mathfrak{L} \models \alpha$ if $v(\alpha) = 0$ for any $\mathfrak{L}$-valuation v. Finally, define

$$\mathrm{Th}(\mathfrak{L}) = \big\{\alpha : \mathfrak{L} \models \alpha\big\}.$$

Now since the operations on the Medvedev lattice were supposed to give an interpretation for the intuitionistic propositional connectives, one would of course hope that $\mathrm{Th}(\mathfrak{M})$ would equal intuitionistic propositional logic IPC. Indeed it is easy to verify that IPC $\subseteq \mathrm{Th}(\mathfrak{M})$. However Medvedev himself already observed that for every $\mathbf{A} \in \mathfrak{M}$ we have that either $\neg\mathbf{A} = \mathbf{0}$ or $\neg\mathbf{A} = \mathbf{1}$, hence that always $\neg\mathbf{A} \times \neg\neg\mathbf{A} = \mathbf{0}$. That is, $\mathfrak{M}$ satisfies the *weak law of the excluded middle* $\neg\alpha \vee \neg\neg\alpha$, and hence is strictly larger than IPC. In fact, we have the following result:

Theorem 4.1 (Medvedev [12], Jankov [6], Sorbi [22])[3] $\mathrm{Th}(\mathfrak{M})$ *is the deductive closure of* IPC *and the weak law of the excluded middle (also known as De Morgan, or Jankov logic).*

Although Theorem 4.1 shows that the Kolmogorov/Medvedev approach does not work directly, the ideas can still be used to interpret IPC. A very natural idea, from an algebraic point of view, is to look at *factors* of $\mathfrak{M}$, i.e. to study $\mathfrak{M}$ modulo a filter or an ideal. Given a Brouwer algebra $\mathfrak{L}$ and an ideal I in $\mathfrak{L}$, $\mathfrak{L}/I$ is still a Brouwer algebra. If G is a filter in $\mathfrak{L}$ then $\mathfrak{L}/G$ is not necessarily a Brouwer algebra, but if G is principal then $\mathfrak{L}/G$ is again a Brouwer algebra. In such a factorized lattice G plays the role of 1. E.g. if G is the principal filter in $\mathfrak{M}$ generated by the degree $\mathbf{D}$ then negation in $\mathfrak{M}/G$ can be defined by $\neg\mathbf{A} = \mathbf{A} \to \mathbf{D}$.

Now it is quite easy to find a factor $\mathfrak{M}/G$ of $\mathfrak{M}$ such that $\mathrm{Th}(\mathfrak{M}/G)$ is classical propositional logic. (Take G the principal filter generated by $\mathbf{0}'$, the degree containing the set of all nonrecursive functions. This is the unique nonzero minimal degree of $\mathfrak{M}$. Note that $\mathbf{0}' = \mathbf{1}$ in $\mathfrak{M}/G$, so that $\mathfrak{M}/G$ has exactly the elements $\mathbf{0}$ and $\mathbf{1}$, corresponding to the classical truth values 1 and 0, respectively.) In general, the theory of $\mathrm{Th}(\mathfrak{M}/G)$ is determined by the algebraic properties of the element that generates the principal filter G. For

[2]Note the upside-down reading of $\wedge$ and $\vee$ when compared to the usual lattice theoretic interpretation, see also footnote 1.

[3]Medvedev [12] actually proved that the *positive* fragments of $\mathrm{Th}(\mathfrak{M})$ and IPC coincide. Jankov proved that IPC$+\neg\alpha\vee\neg\neg\alpha$ is the largest propositional calculus that is conservative over IPC with respect to positive formulas. The theorem follows from these results, since the weak law of the excluded middle holds in $\mathfrak{M}$. The result also follows directly from the embedding result in Sorbi [24].

example, whether the weak law of the excluded middle holds in $\mathrm{Th}(\mathfrak{M}/G)$ is related to whether the element that generates G is join-reducible in $\mathfrak{M}$. (For more information see [24, 27].) Of course, what we *really* would like is a factor of $\mathfrak{M}$ that captures IPC. That such a factor indeed exists is the content of the following beautiful theorem.

Theorem 4.2 (Skvortsova [20]) *There exists a principal filter G such that* $\mathrm{Th}(\mathfrak{M}/G)$ *equals* IPC.

Now what about the logic of $\mathfrak{P}$? First note that the definitions of $\times$ and $+$ are unproblematic, since they are computable operators, so when restricted to Π^0_1 classes they yield again Π^0_1 classes. But this is not the case for the implication operator $\rightarrow$. On the face of it the definition of $\mathcal{A} \rightarrow \mathcal{B}$ in $\mathfrak{M}$ is Π^1_1 in $\mathcal{A}$ and $\mathcal{B}$. Although it is currently open whether $\mathfrak{P}$ is indeed not a Brouwer algebra it seems unlikely that this is the case. Hence we make the following

Conjecture 4.3 $\mathfrak{P}$ *is not a Brouwer algebra.*

That $\mathfrak{P}$ is not a Heyting algebra was proved in section 3. Sorbi [21] proved that $\mathfrak{M}$ is not a Heyting algebra. He also proved in [21] that the Muchnik lattice $\mathfrak{M}_w$ is both a Brouwer and a Heyting algebra, and that $\mathrm{Th}(\mathfrak{M}_w)$ is the De Morgan logic $\mathrm{IPC} + \neg\alpha \vee \neg\neg\alpha$, just as for $\mathfrak{M}$. In [23] he proved that the theory of the dual of $\mathfrak{M}_w$ is also De Morgan logic.

If $\mathfrak{P}$ does not admit an $\rightarrow$ operator, it does not make sense to ask what its propositional theory is. But we can go to a larger structure, like $\mathfrak{M}$, where $\rightarrow$ does exist. Note however that in $\mathfrak{M}$ we work with subsets of ω^ω and in $\mathfrak{P}$ with 2^ω. First we note that as far as the logic of these structures is concerned this does not make a difference. Denote by $\mathfrak{M}_{0,1}$ the lattice of Medvedev degrees of subsets of 2^ω. (This is a Brouwer algebra in much the same way as $\mathfrak{M}$. Theorem 1.1 is proved in the same way, except that for the functions $n\hat{\ }f$ have to be replaced by $1^n\hat{\ }0\hat{\ }f$, for example.)

Fact 4.4

- $\mathrm{Th}(\mathfrak{M}_{0,1}) = \mathrm{IPC} + \neg\alpha \vee \neg\neg\alpha$.
- *There exists a principal filter* $G \subseteq \mathfrak{M}_{0,1}$ *such that* $\mathrm{Th}(\mathfrak{M}_{0,1}/G) = \mathrm{IPC}$.

Proof. The first item follows by inspection of Sorbi's proofs in [23]. The second item follows by inspection of Skvortsova's proof [20]. Both authors, like Medvedev, work in ω^ω. The big difference with 2^ω is of course that the latter is compact, but for these proofs this difference is immaterial. □

Let PA be the class of PA-complete sets. Simpson [18] showed that the Medvedev degree of PA is the top element of $\mathfrak{P}$. For brevity let us write $\mathrm{Th}(\mathfrak{M}/\mathrm{PA})$ for $\mathrm{Th}(\mathfrak{M}/G)$, where G is the principal filter generated by PA. Now we can ask the following

Question 4.5 *What is* $\mathrm{Th}(\mathfrak{M}_{0,1}/\mathrm{PA})$ *? In particular, is it equal to* IPC *?*

We close by making a number of remarks regarding this question.

1. If indeed $\mathrm{Th}(\mathfrak{M}_{0,1}/\mathrm{PA}) = \mathrm{IPC}$ this would give a *natural* example of a filter satisfying Theorem 4.2. It would be very interesting to find such natural examples.

2. Note that $\mathrm{Th}(\mathfrak{M}_{0,1}/\mathrm{PA})$ contains IPC and that it is included in IPC + $\neg\alpha \vee \neg\neg\alpha$ since PA is a closed set [25]. It follows that $\mathrm{Th}(\mathfrak{M}_{0,1}/\mathrm{PA})$ is strictly less than IPC + $\neg\alpha \vee \neg\neg\alpha$ since the top element of $\mathfrak{M}_{0,1}/\mathrm{PA}$ splits by Binns result [2], so that the weak law of the excluded middle does not hold in it, cf. [23, Theorem 4.3].

3. Skvortsova [20, Remark 2] proved that for every Muchnik degree $\mathbf{A} \in \mathfrak{M}$, $\mathrm{Th}(\mathfrak{M}/\mathbf{A})$ contains the Kreisel-Putnam formula
$$(\neg p \to q \vee r) \to (\neg p \to q) \vee (\neg p \to r), \tag{2}$$
which shows that these theories are strictly larger than IPC. Now it is not immediately clear whether [PA] is a Muchnik degree: Although it is known by a result of Solovay (cf. [14, p511]) that the *Turing degrees* of PA sets are upwards closed, PA is itself not upwards closed. But of course [PA] might contain some other upwards closed set. Proposition 4.6 below shows that this is not the case.

4. By Proposition 4.7 below PA is effectively homogeneous. It follows from this and Lemma 6 in Skvortsova [20] that the degree of PA itself satisfies
$$(p \to q \vee r) \to (p \to q) \vee (p \to r), \tag{3}$$
where p is interpreted by the degree of PA and q and r by arbitrary Medvedev degrees.

Proposition 4.6 [PA] *is not a Muchnik degree.*

Proof. N.B. this result holds both for $\mathfrak{M}$ and for $\mathfrak{M}_{0,1}$. We have to show that [PA] does not contain a set that is upwards closed. So let $\mathcal{A}$ be upwards closed under Turing reducibility. We show that $\mathrm{PA} \not\leq_M \mathcal{A}$. Fix any computable functional Φ, and suppose that PA $\leq_M \mathcal{A}$ via Φ. Since $\mathcal{A}$ is upwards closed it is in particular dense in the usual topology on 2^ω. From this it follows that for every $X \in 2^\omega$,

$$\Phi(X) \text{ total } \Longrightarrow \Phi(X) \in \text{PA}.$$

Because $\mathcal{A}$ is dense and a subset of the domain of Φ, we can construct a computable X such that $\Phi(X)$ is total by looking for larger and larger segments on which Φ is defined. But then $\Phi(X)$ is a computable element of PA, contradiction. □

For any finite string σ and any mass problem $\mathcal{A}$ let $\mathcal{A}_\sigma$ denote $\{f \in \mathcal{A} : f \sqsupset \sigma\}$. $\mathcal{A}$ is called *effectively homogeneous* [20] if $\mathcal{A}_\sigma \leq_M \mathcal{A}$ in a uniform way, i.e. if there is a partial recursive function φ that is defined for all σ such that $\mathcal{A}_\sigma \neq \emptyset$ and such that in this case $\varphi(\sigma)$ is a code of a computable functional mapping $\mathcal{A}$ into $\mathcal{A}_\sigma$.

Proposition 4.7 PA *is effectively homogeneous.*

Proof. We think of theories such as PA as coded by binary strings. Let $X \lhd Y$ denote that theory Y faithfully interprets X, meaning that there is a computable function f such that $X \vdash \varphi \Leftrightarrow Y \vdash f(\varphi)$. First we note that for any finite string (theory) σ that is consistent with PA it holds that $\text{PA} + \sigma \lhd PA$. This holds in fact effectively and uniformly in σ: There is a computable function f such that for every PA-consistent string σ and every first-order formula φ,

$$\text{PA} + \sigma \vdash \varphi \Longleftrightarrow \text{PA} \vdash f(\sigma, \varphi).$$

Given an initial segment σ of a set in PA, and given $A \in \text{PA}$, define $A' \sqsupset \sigma$ by putting φ into A' if and only if $f(\sigma, \varphi) \in A$. Then $A' \in \text{PA}$ and $A' \sqsupset \sigma$. This works uniformly for all $A \in \text{PA}$, so $\text{PA}_\sigma \leq_M \text{PA}$. □

Acknowledgment. We are grateful to Andrea Sorbi for providing us with several pointers to the literature about the Medvedev lattice. We also thank Rosalie Iemhoff for helpful remarks concerning intuitionistic logic.

References

[1] R. Balbes and P. Dwinger, *Distributive lattices*, University of Missouri Press, 1974.

[2] Stephen Binns, *A splitting theorem for the Medvedev and Muchnik lattices*, Mathematical Logic Quarterly 49 (2003) 327–335.

[3] Stephen Binns and Stephen G. Simpson, *Embeddings into the Medvedev and Muchnik lattices of* Π^0_1 *classes*, Archive for Mathematical Logic 43 (2004) 399–414.

[4] Douglas Cenzer, Π^0_1 *classes in computability theory*, Handbook of computability theory, 37–85, Studies in Logic and the Foundations of Mathematics **140**, North-Holland, Amsterdam, 1999.

[5] Douglas Cenzer and Peter Hinman, *Density of the Medvedev lattice of* Π^0_1 *classes*, Archive for Mathematical Logic **42**(6) (2003) 583–600.

[6] A. V. Jankov, *Calculus of the weak law of the excluded middle*, Izv. Akad. Nauk SSSR Ser. Mat. 32 (1968) 1044–1051. (In Russian.)

[7] Carl G. Jockusch, Jr. and Thomas G. McLaughlin, *Countable retracing functions and* Π^0_2 *predicates*, Pacific Journal of Mathematics **30** (1969) 67–93.

[8] Carl G. Jockusch, Jr. and Robert I. Soare, *Degrees of members of* Π^0_1 *classes*, Pacific Journal of Mathematics **40**(3) (1972) 605–616.

[9] Carl G. Jockusch, Jr. and Robert I. Soare, Π^0_1 *classes and degrees of theories*, Transactions of the American Mathematical Society **173** (1972) 35–56.

[10] Antonín Kučera, Measure, Π^0_1*-classes and complete extensions of PA*, in: H.-D. Ebbinghaus, G. H. Müller, and G. E. Sacks (eds), Recursion theory week, Lect. Notes in Math. **1141**, 245–259, Springer-Verlag, 1985.

[11] Yu. T. Medvedev, *Degrees of difficulty of the mass problems*, Dokl. Akad. Nauk. SSSR **104**(4) (1955) 501–504.

[12] Yu. T. Medvedev, *Finite problems*, Dokl. Akad. Nauk. SSSR (NS) **142**(5) (1962) 1015–1018.

[13] Albert A. Muchnik, *On strong and weak reducibility of algorithmic problems*, Sibirsk. Math. Zh. **4** (1963) 1328–1341. (In Russian.)

[14] Piergiorgio G. Odifreddi, *Classical recursion theory*, Vol. I, Studies in logic and the foundations of mathematics **125**, North-Holland, 1989.

[15] Piergiorgio G. Odifreddi, *Classical Recursion Theory* Vol. II, Studies in logic and the foundations of mathematics **143**, North-Holland, 1999.

[16] Hartley Rogers Jr., *Theory of recursive functions and effective computability*, McGraw-Hill, 1967.

[17] Stephen G. Simpson, slides for a talk posted on www.math.psu.edu/simpson/talks/umn0105, 2003.

[18] Stephen G. Simpson, Π^0_1 *sets and models of* WKL_0, to appear in: Reverse Mathematics 2001, Lecture Notes in Logic, ASL.

[19] Stephen G. Simpson and Theodore A. Slaman, *Medvedev degrees of* Π^0_1 *subsets of* 2^ω, unpublished manuscript.

[20] Elena Z. Skvortsova, *A faithful interpretation of the intuitionistic propositional calculus by means of an initial segment of the Medvedev lattice*, Sibirsk. Math. Zh. **29**(1) (1988) 171–178. (In Russian.)

[21] Andrea Sorbi, *Some remarks on the algebraic structure of the Medvedev lattice*, Journal of Symbolic Logic **55**(2) (1990) 831–853.

[22] Andrea Sorbi, *Embedding Brouwer algebras in the Medvedev lattice*, Notre Dame Journal of Formal Logic **32**(2) (1991) 266–275.

[23] Andrea Sorbi, *Some quotient lattices of the Medvedev lattice*, Zeitschrift für mathematische Logik und Grundlagen der Mathematik **37** (1991) 167–182.

[24] Andrea Sorbi, *The Medvedev lattice of degrees of difficulty*, In: S. B. Cooper, T. A. Slaman, and S. S. Wainer (eds.), Computability, Enumerability, Unsolvability: Directions in Recursion Theory, London Mathematical Society Lecture Notes **224**, Cambridge University Press, 1996, 289–312.

[25] Andrea Sorbi, personal communication, Siena, July 2004.

[26] Sebastiaan A. Terwijn, *Complexity and Randomness*, Rendiconti del Seminario Matematico di Torino **62**(1) (2004) 1–38.

[27] Sebastiaan A. Terwijn, *Constructive logic and the Medvedev lattice*, submitted.