INTUITIONISTIC LOGIC AND COMPUTATION

Sebastiaan A. Terwijn*

On the occasion of the 65th birthday of Dick de Jongh

1 Introduction

My first encounter with the theory of computation was the basic course on this subject by Dick de Jongh in the spring of 1991. For years to follow, Dick would be one of my teachers in mathematical logic. Close colleagues of Dick will know that this did not actually involve a lot of teaching, but rather the presence of a steering force, sometimes working in mysterious ways. For example, I cannot boast to actually having proved a theorem together with Dick, but indirectly he has been responsible for me proving a number of theorems, for example in learning theory.

Although recursion theory never was the focus of Dick's own research, he has always had a serious interest in it, and encouraged me to study this field from the beginning. Intuitionistic logic and constructivism being his major scientific interests he had good reasons to be interested in it too, since there are of course many relations between these topics.

In this paper we illustrate one way in which constructive logic and computability theory are related, namely through the structure of the Medvedev degrees. This is a very rich structure from computability theory (e.g. it contains the Turing degrees, as an upper semilattice) that can be used as a semantics for propositional logic. Thus, the study of the Medvedev degrees, involving the full range of techniques from computability theory, connects various constructions and results from this area to other parts of mathematical logic, in this case proof theory. In section 2, we review the basic definitions of the Medvedev lattice. In section 3 we then discuss the connection with logic and recall a beautiful theorem about the intuitionistic propositional calculus. In section 4 we take some steps in exploring the algebraic structure of the Medvedev degrees. In particular we discuss join-irreducible elements, that are related to the weak law of the excluded middle. In section 5 we make some remarks on the Medvedev degrees of Π^0_1 classes and their connection to constructive logic. In particular, we discuss the Π^0_1 class of complete extensions of Peano Arithmetic. Finally, in section 6 we discuss autoreducible degrees.

*Institute for 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).

2 The Medvedev lattice

First we briefly recall the definition of the Medvedev lattice $\mathfrak{M}$, originally introduced in Medvedev [9]. 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: $\mathcal{A} \leq \mathcal{B}$ if there is a recursive functional $\Psi : \omega^\omega \to \omega^\omega$ such that for all $f \in \mathcal{B}$, $\Psi(f) \in \mathcal{A}$. This can be seen as an implementation of Kolmogorov's idea of a calculus of problems. The relation $\leq$ induces an equivalence relation on the mass problems: $\mathcal{A} \equiv \mathcal{B}$ if $\mathcal{A} \leq \mathcal{B}$ and $\mathcal{B} \leq \mathcal{A}$. 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. Note that there is a smallest Medvedev degree, denoted by $\mathbf{0}$, namely the degree of any mass problem containing a recursive 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]

Theorem 2.1 (Medvedev [9]) *The structure $\mathfrak{M}$ of all Medvedev degrees, ordered by $\leq$ and together with $\times$ and $+$ is a distributive lattice.*

Let $\mathcal{F} = \big\{ f : f \text{ nonrecursive} \big\}$. We note the following important fact, namely that for all mass problems $\mathcal{A}$, if $[\mathcal{A}] \not\leq \mathbf{0}$ (i.e. $\mathcal{A}$ does not contain any recursive function) then $\mathcal{F} \leq \mathcal{A}$ via the identity. That is, the Medvedev degree of $\mathcal{F}$, which is denoted by $\mathbf{0}'$, is the unique nonzero minimal degree of $\mathfrak{M}$.

[1] There is an annoying notational conflict between the various papers in this area. Sorbi [20] maintains the usual lattice theoretic notation with $\wedge$ for meet and $\vee$ for join, but e.g. Rogers [13] and Skvortsova [16] 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 (see section 3). To avoid headaches we have introduced separate notation for the lattices ($+$ for join and $\times$ for meet) and the logic (the usual $\wedge$ for "and" and $\vee$ for "or") here. 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.

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

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

always exists. We even have:

Theorem 2.2 (Medvedev [9]) *$\mathfrak{M}$ is a Brouwer algebra.*

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

$\mathfrak{L}$ is called a *Heyting algebra* if its dual is a Brouwer algebra. Sorbi [17] has shown that $\mathfrak{M}$ is not a Heyting algebra. Some more discussion and facts about $\mathfrak{M}$ can be found in Rogers [13]. A good survey of what is known about $\mathfrak{M}$ is Sorbi [20], where also a more complete list of references can be found.

We conclude this section with one more definition that we will use later. Note that $\mathcal{A} \le \mathcal{B}$ 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 [11]: We say that $\mathcal{A}$ *Muchnik reduces* to $\mathcal{B}$, denoted $\mathcal{A} \le_w \mathcal{B}$, if $(\forall f \in \mathcal{B})(\exists g \in \mathcal{A})[f \le_T g]$, where $\le_T$ denotes Turing reducibility. The corresponding degrees are called *Muchnik degrees.* They form a distributive lattice in the same way as the Medvedev degrees.

Define $C(\mathcal{A}) = \big\{f : (\exists e)[\Phi_e(f) \in \mathcal{A}]\big\}$, where Φ_e is the e-th partial recursive functional. The Muchnik degrees can be seen as a sublattice of the Medvedev degrees by the embedding $[\mathcal{A}] \mapsto [C(\mathcal{A})]$. The Muchnik degrees are then precisely the Medvedev degrees that contain a mass problem $\mathcal{A}$ such that $C(\mathcal{A}) = \mathcal{A}$. This is equivalent to saying that $\mathcal{A}$ is upward closed under Turing reducibility.

3 Logic and computation

Ever since Heyting wrote down the axioms of intuitionistic logic (in 1930), people have tried to give a semantics for this logic that *explains* their constructive content. Many people felt that such an explanation should have something to do with the theory of computation, but most approaches based on this idea (such as Kleene's realizability) failed to capture intuitionistic provability. As we have seen, the Medvedev lattice implemented an idea of Kolmogorov that was also supposed to give a computational meaning to the logical connectives. Below we make precise what is meant by this, and point out that unfortunately also this approach does not succeed to capture intuitionistic logic, at least not directly. However, a slight extension of the idea *does* work, and gives us, in an algebraically very natural way, a computational semantics for intuitionistic propositional logic IPC.

In section 2 we have already defined the operations $\times$, $+$, and $\to$ on $\mathfrak{M}$. We can also define a negation operator $\neg$ by defining $\neg\mathbf{A} = \mathbf{A} \to \mathbf{1}$ for any Medvedev degree $\mathbf{A}$.

Given any Brouwer algebra $\mathfrak{L}$ (such as $\mathfrak{M}$) with join denoted by $+$ and meet by $\times$, we can evaluate formula's as follows. An $\mathfrak{L}$-*valuation* is a function $v : \text{Form} \to \mathfrak{L}$ from formulas to $\mathfrak{L}$ such that for all formula's α and β, $v(\alpha \times \beta) = v(\alpha) \vee v(\beta)$, $v(\alpha + \beta) = v(\alpha) \wedge v(\beta)$, $v(\alpha \to \beta) = v(\alpha) \to v(\beta)$, $v(\neg\alpha) = v(\alpha) \to 1$.[2] Write $\mathfrak{L} \models \alpha$ if $v(\alpha) = 0$ for any $\mathfrak{L}$-valuation v. Finally, define

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

On page 289 of Rogers [13] it is stated that Medvedev has shown that the identities of $\mathfrak{M}$ (i.e. $\text{Th}(\mathfrak{M})$) are the theorems of IPC, the intuitionistic propositional calculus. This however seems to be a misquotation. It is certainly *not* true that $\text{Th}(\mathfrak{M}) = \text{IPC}$. (That would have been a great result!) Indeed, it is easy to see 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* $\neg\alpha \vee \neg\neg\alpha$. In fact, we have the following result:

Theorem 3.1 (Medvedev [10][3], Sorbi [18]) $\text{Th}(\mathfrak{M})$ *is the deductive closure of* IPC *and the weak law of the excluded middle (Jankov logic).*

This is already very interesting, but in the light of our quest for a computational semantics for IPC it may be a disappointment. Since $\mathfrak{M}$ does not do the trick, we need to look at other Brouwer algebras. 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 $\text{Th}(\mathfrak{M}/G)$ is classical propositional logic. (Take G the principal filter generated by $\mathbf{0}'$, the degree containing the set of all nonrecursive functions, see page 2. 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.) 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 3.2 (Skvortsova [16]) *There exists a principal filter G such that the theory* $\text{Th}(\mathfrak{M}/G)$ *equals* IPC*.*

The proof of Theorem 3.2 consists of a number of clever algebraic coding techniques, combined with some computability theory. Through a series of lattice embedding results (including one by Lachlan for the Turing degrees) it is shown that the magic interval can be found. The main problem is the control of the infima, which is taken care of by making use of so-called *canonical* subsets on

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

[3] Medvedev [10] actually proved that the *positive* fragments of $\text{Th}(\mathfrak{M})$ and IPC coincide.

which the infima are well-behaved. As a canonical subset of $\mathfrak{M}$ those degrees are used that contain a mass problem that is upward closed under Turing reducibility. Note that these are precisely the Muchnik degrees defined at the end of section 2. So, interestingly, both the Turing degrees and the Muchnik degrees play a role in the proof of Theorem 3.2.

4 Irreducible elements

In the previous section we saw how the algebraic structure of $\mathfrak{M}$ and its factors $\mathfrak{M}/G$ relates to the theories $\mathrm{Th}(\mathfrak{M}/G)$. In this section we discuss one special aspect of the algebraic structure of $\mathfrak{M}$, namely its join-irreducible elements. Recall that an element a of a lattice $\mathfrak{L}$ is join-reducible if there are $b, c \in \mathfrak{L}$ such that $a = b + c$ and $a \not\leq b$, $a \not\leq c$. In this case we say that a *splits* into b and c. In this section we discuss the join-irreducible elements of $\mathfrak{M}$. For a discussion of the dual notion of meet-reducibility see e.g. [20]. Join- and meet-irreducible elements also play a crucial role in various results about embeddings of degree structures that are needed in the proof of Theorem 3.2.

In Theorem 3.1 we saw that $\mathfrak{M}$ satisfies the weak law of the excluded middle $\neg\alpha \vee \neg\neg\alpha$. This is due to the fact that $\mathbf{1}$ is join-irreducible, as the following proposition shows.

Proposition 4.1 *Let G be the principle filter generated by Medvedev degree $\mathbf{D}$. Then the weak law of the excluded middle holds in $\mathfrak{M}/G$ if and only if $\mathbf{D}$ is join-irreducible.*

Proof. Suppose that $\mathbf{D}$ is join-reducible, say $\mathbf{A}$ and $\mathbf{B}$ are incomparable such that $\mathbf{A} + \mathbf{B} = \mathbf{D}$. First note that $\neg\mathbf{A} \neq \mathbf{1}$ in $\mathfrak{M}/G$ (where $\mathbf{1}$ is now the top element $\mathbf{D}$ of $\mathfrak{M}/G$) because $\neg\mathbf{A} \leq \mathbf{B} \notin G$. Hence $\neg\neg\mathbf{A} \neq \mathbf{0}$, for otherwise it would hold that $\mathbf{D} \leq \neg\mathbf{A}$. Also, $\neg\mathbf{A} \neq \mathbf{0}$ since $\mathbf{A} \not\geq \mathbf{D}$. Now from $\neg\mathbf{A} \neq \mathbf{0}$ and $\neg\neg\mathbf{A} \neq \mathbf{0}$ it follows that $\neg\mathbf{A} \times \neg\neg\mathbf{A} \neq \mathbf{0}$, since $\mathfrak{M}$ does not have any minimal pairs (because there is exactly one nonzero minimal degree $\mathbf{0}'$ in $\mathfrak{M}$, see page 2). So the weak law of the excluded middle does not hold in $\mathfrak{M}/G$.

Conversely, if $\mathbf{D}$ is join-irreducible it is easy to see that for $\mathbf{A} \neq \mathbf{1}$ we have that $\neg\mathbf{A} = \mathbf{1}$. Since $\neg\mathbf{1} = \mathbf{0}$ we then have that $\neg\mathbf{A} \times \neg\neg\mathbf{A} = \mathbf{0}$ for every $\mathbf{A}$. □

In fact, Sorbi proved the following theorem about the connection between irreducible elements and the theories $\mathrm{Th}(\mathfrak{M}/G)$:

Theorem 4.2 (Sorbi [19, Theorem 4.3]) *For every principal filter G generated by a join-irreducible element greater than $\mathbf{0}'$ it holds that* $\mathrm{Th}(\mathfrak{M}/G) = \mathrm{IPC} + \neg\alpha \vee \neg\neg\alpha$.

The Medvedev degrees $\mathbf{0}$ and $\mathbf{1}$ are trivial examples of join-irreducible elements. More interesting examples of irreducible elements are the degrees $[\mathcal{B}_f]$, for any nonrecursive f, where $\mathcal{B}_f$ is defined as $\mathcal{B}_f = \{g : g \not\leq_T f\}$, cf. Sorbi [18]. (To see that $[\mathcal{B}_f]$ is join-irreducible suppose that $\mathcal{B}_f \equiv \mathcal{A} + \mathcal{C}$ and that $\mathcal{B}_f \not\leq \mathcal{A}$. Then it cannot be that $\mathcal{A} \subseteq \mathcal{B}_f$ (for otherwise the identity would be a reduction) so there is $h \in \mathcal{A}$ with $h \leq_T f$. Now $\mathcal{B}_f \leq \{h \oplus g : g \in \mathcal{C}\}$, via Ψ say. But then $\Psi(h \oplus g) \leq_T h \oplus g \not\leq_T f$, hence all $g \in \mathcal{C}$ satisfy $g \not\leq_T f$. So $\mathcal{B}_f \leq \mathcal{C}$ via the identity.) Notice that $[\mathcal{B}_f]$ together with $[\{f\}]$ forms a maximal antichain of size two in $\mathfrak{M}$.

Splittings in the Turing degrees give many examples of join-reducible elements of $\mathfrak{M}$, as the next lemma shows.

Lemma 4.3 (Sorbi [20]) *Suppose $\mathcal{A}$ is a mass problem such that the following condition holds:*

$$\text{There exist functions } g, h \notin C(\mathcal{A}) \text{ such that } g|_T h \text{ and } g \oplus h \in C(\mathcal{A}). \tag{1}$$

Then the Medvedev degree $[\mathcal{A}]$ is join-reducible.

Proof. If condition (1) holds then it is easy to see that

$$[\mathcal{A}] = [\mathcal{A} \times \{g\}] + [\mathcal{A} \times \{h\}].$$

On the other hand, by incomparability of g and h and the fact that they cannot compute anything in $\mathcal{A}$, it follows that the degrees $[\mathcal{A} \times \{g\}]$ and $[\mathcal{A} \times \{h\}]$ are incomparable. □

Problem 5.4 in Sorbi [20] asks for a characterization of the join-irreducible elements of $\mathfrak{M}$. Below we show that condition (1) of Lemma 4.3 characterizes the join-reducible *Muchnik degrees*, and that it does *not* characterize the join-reducible elements of $\mathfrak{M}$. We then point out how an easy generalization of the condition characterizes the join-irreducible elements of $\mathfrak{M}$.

Recall from section 2 that the Muchnik degrees are precisely the Medvedev degrees containing a mass problem $\mathcal{A}$ such that $\mathcal{A} \equiv C(\mathcal{A})$.

Proposition 4.4 *Condition (1) characterizes the join-reducible Muchnik degrees.*

Proof. Suppose that $[\mathcal{A}]$ is a Muchnik degree. Lemma 4.3 holds for the Muchnik degrees just as well as for the Medvedev degrees, so we only have to show that if condition (1) does not hold for $\mathcal{A}$ then $\mathcal{A}$ is join-irreducible. So suppose (1) does not hold, and suppose that $\mathcal{A} \equiv \mathcal{B} + \mathcal{C}$ and $\mathcal{A} \not\leq \mathcal{B}$. We show that $\mathcal{A} \leq \mathcal{C}$. Since $\mathcal{A} \equiv C(\mathcal{A})$, $\mathcal{A} \not\leq \mathcal{B}$ implies that there is $g \in \mathcal{B} \setminus C(\mathcal{A})$. Now $\mathcal{A} \leq \{g \oplus h : h \in \mathcal{C}\}$, via Ψ say. But then, since $\Psi(g \oplus h) \leq_T g \oplus h$, all $h \in \mathcal{C}$ must be in $C(\mathcal{A})$. Hence $\mathcal{A} \equiv C(\mathcal{A}) \leq \mathcal{C}$ via the identity. □

In Dyment[4] [4] it was shown that *every* Muchnik degree is meet-reducible.

Proposition 4.4 points out a way in which a Medvedev degree $[\mathcal{A}]$ can be join-reducible without satisfying condition (1): It may happen that $\mathcal{B} \subseteq C(\mathcal{A})$ but that nevertheless $\mathcal{A} \not\leq \mathcal{B}$ because there is no *uniform* procedure that reduces $\mathcal{A}$ to $\mathcal{B}$.

[4] It may be informative to note that E. Z. Dyment and E. Z. Skvortsova are in fact the same person.

Theorem 4.5 *Condition (1) does not characterize the join-reducible elements of $\mathfrak{M}$: There is a join-reducible Medvedev degree $[\mathcal{A}]$ such that (1) does not hold.*

Proof. We prove this by constructing such an $\mathcal{A}$ by brute force. Let B_e, C_e, $e \in \omega$, be subsets of ω such that their Turing degrees form a strongly independent set. That is, for any e, B_e does not Turing reduce to any finite join of B_j's, $j \neq e$, and C_j's. Moreover, we need that B_e does not bound a minimal Turing degree, and that there are sets $B'_e <_T B_e$ such that B'_e is not below any finite join of B'_j's, $j \neq e$, and C_j's. That all this is possible follows from standard results about lattice embeddings into the Turing degrees.[5]

Now define $\mathcal{C}' = \big\{C_e : e \in \omega\big\}$,

$$\mathcal{B}' = \big\{B_e : \Phi_e(B_e) \neq B_e\big\} \cup \big\{B'_e : \Phi_e(B_e) = B_e\big\},$$

(where Φ_e is the e-th partial recursive functional) and

$$\begin{aligned}\mathcal{A} \quad = \quad & \big\{f : f \not\leq_T X \text{ for any } X \text{ that is the join of} \\ & \text{finitely many elements from } \mathcal{C}'\big\} \setminus \\ & \big(\big\{\Phi_e(B_e) : \Phi_e(B_e) \text{ total}\big\} \cup \big\{\Phi_e(B'_e) : \Phi_e(B'_e) \text{ total}\big\}\big).\end{aligned}$$

Finally, define $\mathcal{B} = \mathcal{A} \times \mathcal{B}'$, $\mathcal{C} = \mathcal{A} \times \mathcal{C}'$. Then $\mathcal{B}$, $\mathcal{C} \leq \mathcal{A}$ so $\mathcal{B} + \mathcal{C} \leq \mathcal{A}$. We further prove that $\mathcal{A} \leq \mathcal{B} + \mathcal{C}$, $\mathcal{A} \not\leq \mathcal{C}'$, $\mathcal{A} \not\leq \mathcal{B}'$, and that $\mathcal{A}$ satisfies the negation of condition (1).

$\mathcal{A} \leq \mathcal{B} + \mathcal{C}$: It is enough to show that $\mathcal{A} \leq \mathcal{B}' + \mathcal{C}'$. For this it is in turn enough to see that for all $g \in \mathcal{B}'$ and $h \in \mathcal{C}'$, $g \oplus h \in \mathcal{A}$. That $g \oplus h$ is not below a finite join of elements from $\mathcal{C}'$ follows from the strong independence assumptions on the B_j, B'_j, and C_j's. That $g \oplus h$ is not equal to any $\Phi_e(B_e)$ or $\Phi_e(B'_e)$ also follows from these independence properties, since $\Phi_e(B_e) \leq_T B_e$.

$\mathcal{A} \not\leq \mathcal{C}'$: This is clear since $\mathcal{C}'$ is contained in the complement of $C(\mathcal{A})$.

$\mathcal{A} \not\leq \mathcal{B}'$: This is by construction of $\mathcal{A}$; When $\Phi_e(B_e) \neq B_e$ then $B_e \in \mathcal{B}'$ and $\Phi_e(B_e) \notin \mathcal{A}$ (either because $\Phi_e(B_e)$ is not total or by definition of $\mathcal{A}$). When $\Phi_e(B_e) = B_e$ then $B'_e \in \mathcal{B}'$ and $\Phi_e(B'_e) \notin \mathcal{A}$. So Φ_e cannot be a reduction from $\mathcal{A}$ to $\mathcal{B}'$ for any e.

$\mathcal{A}$ satisfies $\neg(1)$: Let $\mathcal{J}$ be the set of all functions whose Turing degree is bounded by a finite join of elements from $\mathcal{C}'$. Note that the elements of $\mathcal{J}$ satisfy $\neg(1)$ (i.e. no two functions from $\mathcal{J}$ together compute an element from $\mathcal{A}$) by definition of $\mathcal{A}$. Now suppose that $g \notin C(\mathcal{A})$. Then $g \notin \mathcal{A}$, so either $g \in \mathcal{J}$ or $g = \Phi_e(B_e)$ or $g = \Phi_e(B'_e)$. In the latter two cases $g \leq_T B_e$, and hence g is not minimal since by assumption B_e bounds no minimal degrees. Hence in both cases $g \in C(\mathcal{A})$ because we can always find an element below g unequal to $\Phi_e(B_e)$ and $\Phi_e(B'_e)$. So the only $g \notin C(\mathcal{A})$ are the ones in $\mathcal{J}$, and these satisfy $\neg(1)$. □

[5] One can use here the result of Lachlan and Lebeuf [7] that every countable upper semilattice with a least element is isomorphic to an initial segment of the Turing degrees. See e.g. Lerman [8].

Lemma 4.3 gives a special example of a situation where $[\mathcal{A}]$ is join-reducible, namely when an $f \in \mathcal{A}$ can be split into g and h both not in $C(\mathcal{A})$. We conclude with the observation that if we generalize g and h to *sets* of functions we more or less get the definition back: $[\mathcal{A}]$ is join-reducible if and only if there is a set of g's that do not uniformly compute elements in $\mathcal{A}$ (generalizing that $g \notin C(\mathcal{A})$) and a set of h's that also does not uniformly compute elements in $\mathcal{A}$ (generalizing that $h \notin C(\mathcal{A})$), such that the pairs $g \oplus h$ uniformly compute elements of $\mathcal{A}$ (generalizing that $g \oplus h \in C(\mathcal{A})$).

5 Π^0_1 classes and PA-complete sets

Simpson (see e.g. [15, 14]) 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. (A set is PA-complete if it computes a complete and consistent extension of Peano Arithmetic.)

The following is a sample of results showing what is possible for Π^0_1 classes under Medvedev reducibility. The list is far from exhaustive.

- (Jockusch and Soare [6]) There is a minimal pair of Π^0_1 classes.
- (Cenzer and Hinman [3]) $\mathfrak{P}$ is dense.
- (Binns [2]) Every degree in $\mathfrak{P}$ splits in two lesser ones.

Part of Simpsons motivation to study $\mathfrak{P}$ are the interesting connections with the area of reverse mathematics. There are many other interesting connections, e.g. with the theory of randomness, see Simpson [15] and Terwijn [21].

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. We do however have:

Theorem 5.1 (Terwijn [21]) *$\mathfrak{P}$ is not a Heyting algebra.*

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 logics 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.

Fact 5.2

- $\mathrm{Th}(\mathfrak{M}_{0,1}) = \mathrm{IPC} + \neg\alpha \vee \neg\neg\alpha$.
- *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 [18, 19]. The second item follows by inspection of Skvortsova's proof [16]. 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. 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 5.3 *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 3.2. 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 strictly less than $\mathrm{IPC} + \neg\alpha \vee \neg\neg\alpha$ 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. Proposition 4.1.

3. Skvortsova [16] proved that for every Muchnik degree $\mathbf{A} \in \mathfrak{M}$ the theory $\mathrm{Th}(\mathfrak{M}/\mathbf{A})$ satisfies 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. [12, 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 5.4 below shows that this is not the case.

4. By Proposition 5.5 below PA is effectively homogeneous. It follows from this and the analysis in Skvortsova [16] 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 5.4 [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 $\mathcal{A} \not\leq \mathrm{PA}$. Fix any computable functional Φ, and suppose that $\mathcal{A} \leq \mathrm{PA}$ 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. $\square$

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* [16] if $\mathcal{A}_\sigma \leq \mathcal{A}$ 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 5.5 *The class of* PA*-complete sets 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. 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 $\text{PA}_\sigma \leq \text{PA}$. $\square$

6 Variation on a theme: Autoreducibility

In computability theory, a set A is called autoreducible if A can compute the answers to membership questions of the form "$x \in A$?" without using the bit $A(x)$, that is, if there is a code e such that for all x, $\{e\}^{A - \{x\}}(x) = A(x)$. E.g. for every set A one can easily see that $A \oplus A$ is autoreducible, since all information of the form $x \in A$ is doubly stored. This shows that every m-degree contains an autoreducible set (Trakhtenbrot). A noncomputable degree is completely autoreducible if it contains *only* autoreducible sets. That there is a completely autoreducible Turing degree was shown by Jockusch and Paterson [5], using the same method with which one can build a minimal Turing degree. Now let us define in an analogous way autoreducibility for Medvedev degrees:

Definition 6.1 A mass problem $\mathcal{A}$ is *autoreducible* if for every $f \in \mathcal{A}$, $\mathcal{A} - \{f\} \leq \mathcal{A}$. A Medvedev degree is autoreducible if it contains an autoreducible mass problem, and *completely autoreducible* if it contains only autoreducible mass problems.

First we note that every Medvedev degree is autoreducible: Given any mass problem $\mathcal{A}$, $\mathcal{A}+\mathcal{A} \equiv \mathcal{A}$ and $\mathcal{A}+\mathcal{A}$ is autoreducible. (Note the similarity to Trakhtenbrots argument for sets quoted above.) Next we turn to completely autoreducible degrees.

Proposition 6.2 *There exists a completely autoreducible Medvedev degree.*

Proof. Let $\mathcal{A} = \{X_n : n \in \omega\}$ be a uniform sequence of sets of descending Turing degree: $X_{n+1} <_T X_n$ for every n and there exists a computable functional Φ such that $\Phi(X_n) = X_{n+1}$ for every n. Such a sequence can be constructed by standard methods (even in the c.e. degrees), cf. [12]. Now suppose that $\mathcal{B} \equiv \mathcal{A}$. Then $\mathcal{B}$ is also autoreducible: Suppose that $\mathcal{A} \leq \mathcal{B}$ via Ψ_0 and $\mathcal{B} \leq \mathcal{A}$ via Ψ_1. Suppose $Y \in \mathcal{B}$. Suppose that $\Psi_0(Y) = X_n$. Let $\Phi^{(n)}$ denote the n-th iterate of Φ. Then for every $X \in \mathcal{B}$, $\Psi_1 \circ \Phi^{(n)} \circ \Psi_0(X) \in \mathcal{B}$, and moreover

$$\begin{aligned} \Psi_1 \circ \Phi^{(n+1)} \circ \Psi_0(X) &\leq_T \Phi^{(n+1)} \circ \Psi_0(X) \\ &\leq_T \Phi^{(n+1)}(X_0) \\ &<_T X_n \\ &\leq_T Y \end{aligned}$$

for every $X \in \mathcal{B}$. In particular $\mathcal{B} - \{Y\} \leq \mathcal{B}$ via $\Psi_1 \circ \Phi^{(n+1)} \circ \Psi_0$. □

We could also have defined a mass problem $\mathcal{A}$ to be autoreducible if $\{f\} \leq \mathcal{A} - \{f\}$ for every $f \in \mathcal{A}$. (The reader may be of the opinion that this definition more closely resembles the one from computability theory.) Under this alternative definition the autoreducible Medvedev degrees are precisely the degrees of solvability, i.e. the ones containing a mass problem of the form $\{f\}$:

Proposition 6.3 *Under the new definition, $\mathcal{A}$ is autoreducible if and only if $\mathcal{A} \equiv \{f\}$ for some f.*

Proof. Every degree of solvability is autoreducible because $\{f\} + \{f\}$ is autoreducible. Conversely, if $\mathcal{A}$ is autoreducible then we claim that $\{f\} \equiv \mathcal{A}$ for some $f \in \mathcal{A}$: If $\mathcal{A}$ contains an isolated branch f (in the usual tree topology on ω^ω) then this is easy to see: Suppose $\sigma \in \omega^{<\omega}$ is a finite string such that f is the only element of $\mathcal{A}$ extending σ. Then $\{f\} \leq \mathcal{A}$ by using the functional for $\{f\} \leq \mathcal{A} - \{f\}$ for elements that do not extend σ, and by using the identity otherwise.

Now suppose that $\mathcal{A}$ has no isolated branches. Then in particular $\mathcal{A}$ is uncountable. By autoreducibility for every $f \in \mathcal{A}$ there is a computable functional Φ_f such that $\{f\} \leq \mathcal{A} - \{f\}$ via Φ_f. Since $\mathcal{A}$ is uncountable, and since there are only countably many computable functionals, there must be $f, g \in \mathcal{A}$, $f \neq g$, such that $\Phi_f = \Phi_g$. We then have that $\{f\} \leq \mathcal{A} - \{f\}$ via Φ_g and $\{g\} \leq \mathcal{A} - \{g\}$ via Φ_g. Let Ψ be such that $\{f\} \leq \{f, g\}$ via Ψ. (Ψ exists since by autoreducibility $f \equiv_T g$.) Then for all $h \in \mathcal{A}$, $\Psi \circ \Phi_g(h) = f$, hence $\{f\} \leq \mathcal{A}$ via $\Psi \circ \Phi_g$. □

Since for noncomputable f clearly $\{f\}$ is not autoreducible, we see that under this definition noncomputable completely autoreducible degrees do not exist.

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] S. Binns, *A splitting theorem for the Medvedev and Muchnik lattices*, to appear in Mathematical Logic Quarterly.

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

[4] E. Z. Dyment, *Certain properties of the Medvedev lattice*, Mathematics of the USSR Sbornik 30 (1976) 321–340. (English translation.)

[5] C. G. Jockusch, jr. and M. Paterson, *Completely autoreducible degrees*, Zeit. Math. Log. Grund. Math. 22 (1976) 571–575.

[6] C. G. Jockusch, jr. and R. I. Soare, *A minimal pair of* Π^0_1 *classes*, Journal of Symbolic Logic 36(1) (1971) 66–78.

[7] A. H. Lachlan and R. Lebeuf, *Countable initial segments of the degrees of unsolvability*, Journal of Symbolic Logic 41 (1976) 289–300.

[8] M. Lerman, *Degrees of unsolvability*, Springer, 1983.

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

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

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

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

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

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

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

[16] E. 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.)

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

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

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

[20] A. 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.

[21] S. A. Terwijn, *The Medvedev lattice of computably closed sets*, in preparation, March 2004.