A note on universal measures for weak implicit computational complexity

Arnold Beckmann*

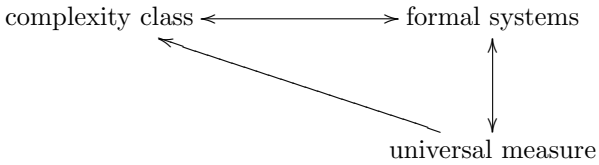
Institute of Algebra and Computational Mathematics
Vienna University of Technology
Wiedner Hauptstr. 8-10/118, A-1040 Vienna, Austria
Arnold.Beckmann@logic.at

Abstract. This note is a case study for finding universal measures for weak implicit computational complexity. We will instantiate "universal measures" by "dynamic ordinals", and "weak implicit computational complexity" by "bounded arithmetic". Concretely, we will describe the connection between dynamic ordinals and witness oracle TURING machines for bounded arithmetic theories.

Keywords: Bounded arithmetic; Dynamic ordinals; Witness oracle TURING machines; Weak implicit computational complexity.

1 Introduction

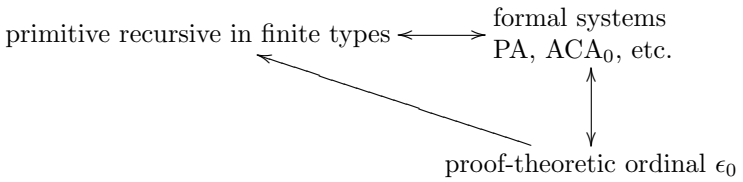
Implicit computational complexity denotes the collection of approaches to computational complexity which define and classify the complexity of computations without direct reference to an underlying machine model. These approaches are formal systems which cover a wide range, including applicative functional programming languages, linear logic, bounded arithmetic and finite model theory (c.f. [13]). In this note we contribute to the idea of characterizing the computational complexity of such formal systems by universal measures, such that the formal systems describe exactly the same complexity class if and only if they agree in their universal measure. In general, we aim at connections which can be represented as follows:



Many formal systems admit such kind of universal measures. For example, in case of "strong" implicit computational complexity, e.g. for number-theoretic functions which are computable by primitive recursive functionals in finite types,

* Supported by a Marie Curie Individual Fellowship #HPMF-CT-2000-00803 from the European Commission.

so-called proof-theoretic ordinals have proven useful as universal measures of proof and computation (and also consistency) strength (cf. [15]). With respect to our general picture this situation can be represented as follows:



In this note we will focus on "weak" complexity classes. By this we mean complexity classes strictly below EXPTIME. We will approach the general idea of finding universal measures by doing a case study for a particular framework of weak implicit computational complexity called bounded arithmetic. Bounded arithmetic theories are logical theories of arithmetic given as restrictions of PEANO arithmetic. Quantification and induction are restricted ("bounded") in such a manner that complexity-theoretic classes can be closely tied to provability in these theories. A hierarchy of bounded formulas, Σ^b_i, and of theories $\mathrm{S}^1_2 \subseteq \mathrm{T}^1_2 \subseteq \mathrm{S}^2_2 \subseteq \mathrm{T}^2_2 \subseteq \mathrm{S}^3_2 \ldots$ has been defined (cf. [5]). The class of predicates definable by Σ^b_i (or Π^b_i) formulas is precisely the class of predicates in the ith level Σ^p_i (resp. Π^p_i) of the polynomial hierarchy. The Σ^b_i-definable functions of S^i_2 are precisely the $\Box^p_i$-functions, which are the functions which are polynomial time computable with an oracle from Σ^p_{i-1} (cf. [5]). KRAJÍČEK [10] characterizes the Σ^b_{i+1}-definable multivalued functions of S^i_2 as $\mathrm{FP}^{\Sigma^b_i}(\mathrm{wit}, O(\log n))$. $\mathrm{FP}^{\Sigma^b_i}(\mathrm{wit}, O(\log n))$ is the class of multivalued functions computable by a polytime Σ^b_i-witness oracle TURING machine with the number of queries bounded by $O(\log n)$, that is, a TURING machine running in polynomial time which on inputs of length n uses fewer than $O(\log n)$ witness queries to a Σ^b_i-oracle. A witness query to a Σ^b_i-oracle is one which in case of a positive answer also supplies a poly-size witness string, i.e. one whose binary length is polynomially bounded in the binary length of the query. These kind of results are extended and generalized by POLLETT [16].

It is an open problem of bounded arithmetic whether the hierarchy of theories collapses. This problem is connected with the open problem in complexity theory whether the polynomial hierarchy PH collapses – the P=?NP problem is a subproblem of this. The bounded arithmetic hierarchy collapses if and only if PH collapses provably in bounded arithmetic (cf. [12, 6, 19]). The case of relativized complexity classes and theories behave completely differently. The existence of an oracle A is proven in [2, 18, 8], such that the polynomial hierarchy in this oracle PH^A does not collapse, hence in particular $\mathrm{P}^A \neq \mathrm{NP}^A$ holds. Building on this one can show $\mathrm{T}^i_2(X) \neq \mathrm{S}^{i+1}_2(X)$ [12]. Here, the relativized theories $\mathrm{S}^i_2(X)$ and $\mathrm{T}^i_2(X)$ result from S^i_2 and T^i_2, resp., by adding a free set variable X and the relation symbol $\in$. Similarly also, $\mathrm{S}^i_2(X) \neq \mathrm{T}^i_2(X)$ is proven in [10], and separation results for further relativized theories (dubbed $\Sigma^b_n(X)$-$\mathrm{L}^m\mathrm{IND}$) are proven in [16]. Independently of these, and with completely different methods (see below), we have shown separation results for theories of relativized bounded

arithmetic in [3, 4]. Despite all answers in the relativized case, all separation questions continue to be open for theories without set parameters.

Recently, there has been a new approach to the study of relativized theories of bounded arithmetic called dynamic ordinal analysis [3, 4]. Inspired from proof-theoretic ordinals which have their origin in GENTZEN's consistency proof for PA, the proof theoretic strength of fragments of bounded arithmetic is characterized by so called dynamic ordinals. The dynamic ordinal $\mathrm{DO}(T(X))$ of a relativized theory of bounded arithmetic $T(X)$ is a set of unary number-theoretic functions which characterizes the amount of $\Pi^b_1(X)$-order-induction which $T(X)$ can prove. For example, the dynamic ordinals of $\mathrm{T}^1_2(X)$, $\mathrm{S}^1_2(X)$ and $\mathrm{sR}^2_2(X)$ are computed to be

$$\begin{aligned}
\mathrm{DO}(\mathrm{T}^1_2(X)) &= \{\lambda n.2^{|n|^c} \,:\, c \text{ a number}\} \\
\mathrm{DO}(\mathrm{S}^1_2(X)) &= \{\lambda n.|n|^c \,:\, c \text{ a number}\} \\
\mathrm{DO}(\mathrm{sR}^2_2(X)) &= \{\lambda n.2^{||n||^c} \,:\, c \text{ a number}\} \ .
\end{aligned}$$

In this way, separation results can be obtained between those relativized theories which have been assigned different dynamic ordinals.

In this note we will connect the dynamic ordinal of some relativized theories of bounded arithmetic with the Σ^b_2-definable multivalued functions of their unrelativized companions. This shows that dynamic ordinals do in fact also characterize the *computational complexity* of theories of bounded arithmetic. For T from the following infinite list

> T^1_2, S^2_2, S^1_2, sR^2_2, sR^1_2, and Σ^b_m-$\mathrm{L}^{m+1}\mathrm{IND}$ and Σ^b_m-$\mathrm{L}^m\mathrm{IND}$ for all $m > 0$,

we obtain

> T and the theory which has induction for Σ^b_1-formulas for all functions in $\mathrm{DO}(T(X))$ prove the same Σ^b_2-formulas.

and, therefore,

> A multivalued function f is Σ^b_2-definable in T if and only if f is computable by some polytime Σ^b_1-witness oracle TURING machine with the number of queries bounded by $\log(\mathrm{DO}(T(X)))$.

The paper is organized as follows. In the following section we will review the definition of bounded arithmetic theories. The third section summarizes definition and results on dynamic ordinals. In section 4 we define witness oracle TURING machines and review results characterizing definable multivalued functions of bounded arithmetic theories by witness oracle TURING machines. In section 5 we apply the results from the previous sections to obtain the connection of dynamic ordinals and witness oracle TURING machines. The last section discusses open questions and possible extensions of these connections.

2 Bounded arithmetic

Bounded arithmetic, in the way we consider it, can be formulated as the fragment $I\Delta_0+\Omega_1$ of PEANO arithmetic in which induction is restricted to bounded formulas and Ω_1 expresses a growth rate strictly smaller than exponentiation, namely that $2^{|x|^2}$ exists for all x, with $|x|$ being the length of the binary representation of x, i.e. an integer valued logarithm of x. The same fragment is obtained by extending the language, and we will follow this approach (cf. [5, 11]). Let us recall some definitions.

The language of bounded arithmetic $\mathcal{L}_{\mathrm{BA}}$ consists of function symbols 0 (zero), S (successor), + (addition), $\cdot$ (multiplication), $|x|$ (binary length), $\lfloor \frac{1}{2}x \rfloor$ (binary shift right), $x \# y$ (smash, $n\#m := 2^{|n|\cdot|m|}$), $x \dot{-} y$ (arithmetical subtraction), $\mathrm{MSP}(x,i)$ (Most Significant Part) and $\mathrm{LSP}(x,i)$ (Less Significant Part), and relation symbols $=$ (equality) and $\leq$ (less than or equal). The meaning of MSP and LSP is given by

$$x = \mathrm{MSP}(x,i) \cdot 2^i + \mathrm{LSP}(x,i) \qquad \text{and} \qquad \mathrm{LSP}(x,i) < 2^i$$

for all x and i. Restricted exponentiation $2^{\min(x,|y|)}$ can be defined by

$$2^{\min(x,|y|)} \quad = \quad \mathrm{MSP}(y \# 1, |y| \dot{-} x) \ ,$$

hence we can assume that restricted exponentiation is also part of our language $\mathcal{L}_{\mathrm{BA}}$. We often write 2^t and mean $2^{\min(t,|x|)}$ if $t \leq |x|$ is clear from the context.

Relativized bounded arithmetic is formulated in the language $\mathcal{L}_{\mathrm{BA}}(X)$ which is $\mathcal{L}_{\mathrm{BA}}$ extended by one set variable X and the element relation symbol $\in$.

BASIC is a finite set of open axioms (cf. [5, 17, 9]) which axiomatizes the non-logical symbols. When dealing with $\mathcal{L}_{\mathrm{BA}}(X)$ we assume that BASIC also contains the equality axioms for X.

Bounded quantifiers play an important rôle in bounded arithmetic. We abbreviate

$$\begin{array}{ll} (\forall x \leq t)A \ := \ (\forall x)(x \leq t \to A) & (\exists x \leq t)A \ := \ (\exists x)(x \leq t \wedge A) \\ (\forall x < t)A \ := \ (\forall x \leq t)(t \not\leq x \to A) & (\exists x < t)A \ := \ (\exists x \leq t)(t \not\leq x \wedge A) \end{array}$$

The quantifiers $(Q\, x \leq t)$, $(Q\, x < t)$, $Q \in \{\forall, \exists\}$, are called *bounded quantifiers*. A bounded quantifier of the form $(Q\, x \leq |t|)$, $Q \in \{\forall, \exists\}$, is called a *sharply bounded quantifier*. A formula in which all quantifiers are (sharply) bounded is called a *(sharply) bounded formula*. Bounded formulas are stratified into levels:

1. $\Delta_0^b = \Sigma_0^b = \Pi_0^b$ is the set of all sharply bounded formulas.
2. Σ_n^b-formulas are those which have a block of n alternating bounded quantifiers, starting with an existential one, in front of a sharply bounded kernel.
3. Π_n^b is defined dually, i.e. the block of alternating quantifiers starts with an universal one.

In the relativized case $\Delta_0^b(X)$, $\Sigma_n^b(X)$, $\Pi_n^b(X)$ are defined analogously.
Attention: In our definition, the class Σ_n^b consists only of *prenex*, also called

strict, formulas. In other places like [5, 11], the definition of Σ^b_n is more liberal, and the class defined here is then denoted $s\Sigma^b_n$, where the "s" indicates "strict".

Induction is also stratified. Let $|x|_0 := x$ and $|x|_{m+1} := |(|x|_m)|$.

For Ψ is a set of formulas and m is a natural number, let Ψ-L^{m}IND denote the schema

$$\varphi(0) \wedge (\forall x < |t|_m)(\varphi(x) \to \varphi(\mathrm{S}\, x)) \to \varphi(|t|_m)$$

for all $\varphi \in \Psi$ and terms t.

For $m = 0$ this is the usual successor induction schema and will be denoted by Ψ-IND. In case $m = 1$ we usually write Ψ-LIND.

The theories of bounded arithmetic under consideration are given by

$$\mathrm{BASIC} + \Sigma^b_n\text{-L}^m\mathrm{IND}\ .$$

Usually we do not mention BASIC and simply call this theory Σ^b_n-L^{m}IND. Some of the theories have special names:

$$\begin{aligned} \mathrm{T}^i_2 &:= \Sigma^b_i\text{-IND}\ , \\ \mathrm{S}^i_2 &:= \Sigma^b_i\text{-LIND}\ , \\ \mathrm{sR}^i_2 &:= \Sigma^b_i\text{-L}^2\mathrm{IND}\ . \end{aligned}$$

For theories S, T let $S \subseteq T$ denote that all axioms in S are consequences of T. From the definition of the theories it immediately follows

$$\begin{aligned} \Sigma^b_n\text{-L}^{m+1}\mathrm{IND} &\subseteq \Sigma^b_n\text{-L}^m\mathrm{IND}\ , \\ \Sigma^b_n\text{-L}^m\mathrm{IND} &\subseteq \Sigma^b_{n+1}\text{-L}^m\mathrm{IND}\ . \end{aligned}$$

A little bit more insight is needed to obtain

$$\Sigma^b_n\text{-L}^m\mathrm{IND} \subseteq \Sigma^b_{n+1}\text{-L}^{m+1}\mathrm{IND}\ ,$$

see [5, 3] for a proof. Figure 1 reflects the just obtained relations – going from left to right in the diagram means that the theory on the lefthand side of an edge is included in the theory on the righthand side. Similar definitions and results can be stated for relativized theories of bounded arithmetic.

3 Dynamic ordinals

In this section we summarize results on dynamic ordinals. Full proofs can be found in [4]. In this section the underlying language will always be the language $\mathcal{L}_{\mathrm{BA}}(X)$ of relativized bounded arithmetic.

Theories of bounded arithmetic are axiomatized by using successor induction, where dynamic ordinals are based on order induction. In the following we will compare these two kinds of induction. Let us first fix some useful abbreviations.

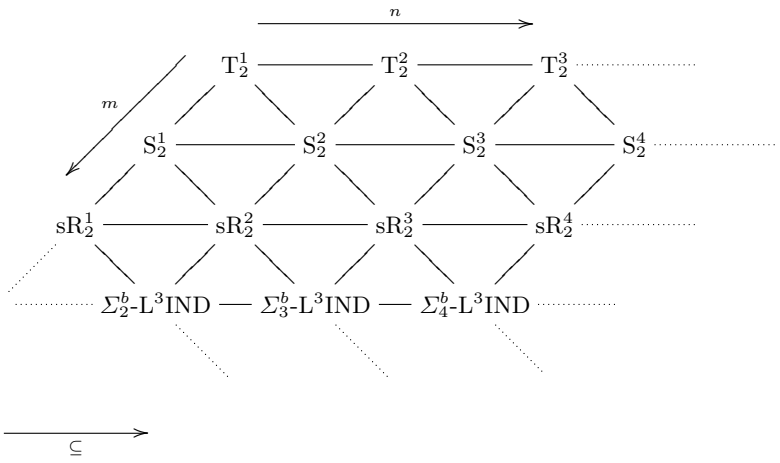


Fig. 1. The theories Σ_n^b-L^{m}IND

We adopt from set theory the convention of identifying numbers with the set of their predecessors, i.e. y is identified with $\{z : z < y\}$. E.g., we write $y \subseteq X$ instead of $(\forall z < y)(z \in X)$.

$$\begin{aligned}
\mathcal{S}\mathrm{Prog}(x, X) &:= 0 \in X \wedge (\forall y < x)(y \in X \to \mathrm{S}\, y \in X) \\
\mathcal{S}\mathrm{Ind}(x, X) &:= \mathcal{S}\mathrm{Prog}(x, X) \to x \in X \\
\mathcal{O}\mathrm{Prog}(x, X) &:= (\forall y \leq x)(y \subseteq X \to y \in X) \\
\mathcal{O}\mathrm{Ind}(x, X) &:= \mathcal{O}\mathrm{Prog}(x, X) \to \mathrm{S}\, x \subseteq X
\end{aligned}$$

Order induction, here denoted $\mathcal{O}$Ind, is logically equivalent to minimization:

$$(\exists y \leq x)A(y) \to (\exists y \leq x)(A(y) \wedge (\forall z < y)\neg A(z)).$$

It is well-known (cf. [5, 11]) that over the base theory BASIC the schema Σ_i^b-IND is equivalent to minimization for Σ_i^b-formulas which is equivalent (by coding one existential quantifier) to minimization for Π_{i-1}^b-formulas.

We first examine direct relations between $\mathcal{S}$Ind and $\mathcal{O}$Ind. We will often consider sets $\{y : A(y)\}$ for a formula $A(a)$, and we usually will abbreviate this set by A if the variable a is clear or unimportant. For Φ is a set of formulas, let $\mathcal{O}\mathrm{Ind}(t, \Phi)$ denote the schema of all instances $\mathcal{O}\mathrm{Ind}(t, A)$ for $A \in \Phi$, where $\mathcal{O}\mathrm{Ind}(t, A)$ is the result of replacing X in $\mathcal{O}\mathrm{Ind}(t, X)$ by the formula A. Similarly for $\mathcal{S}$Ind. When saying "let T be a theory" we always mean that T contains some weak base theory, say $\mathrm{S}_2^0 \subseteq T$.

Lemma 1. *1.* BASIC $\vdash \mathcal{O}\mathrm{Ind}(t, A) \to \mathcal{S}\mathrm{Ind}(t, A)$ *for arbitrary formulas* A.

2. Let Φ *be a set of formulas, which is closed under bounded universal quantification,* T *be a theory, and* t *be a term. Then* $T \vdash \mathcal{S}\mathrm{Ind}(t, \Phi)$ *implies* $T \vdash \mathcal{O}\mathrm{Ind}(t, \Phi)$.

Proof. 1. is obvious. For 2. we argue in T. Assuming $T \vdash \mathcal{S}\mathrm{Ind}(t, \Phi)$, $A \in \Phi$ and $\mathcal{O}\mathrm{Prog}(t, A)$ we can show $t + 1 \subseteq A$ by induction for y up to $t + 1$ in $y \subseteq A$. □

Now we define the dynamic ordinal of an $\mathcal{L}_{\mathrm{BA}}(X)$-theory based on $\mathcal{O}\mathrm{Ind}$. Afterwards, we will characterize dynamic ordinals in terms of $\mathcal{S}\mathrm{Ind}$ using Lemma 1.

Definition 2. *The dynamic ordinal of an $\mathcal{L}_{\mathrm{BA}}(X)$-theory T is defined by*

$$\mathrm{DO}(T) \quad := \quad \{\lambda x.t \,:\, T \vdash (\forall x)\ \mathcal{O}\mathrm{Ind}(t, \Pi^b_1(X))\} \ .$$

Of course, t always denotes a term in which at most x occurs as a variable in the last definition and in the next theorem.

Theorem 3. $\mathrm{DO}(T) \quad = \quad \{\lambda x.t \,:\, T \vdash (\forall x)\ \mathcal{S}\mathrm{Ind}(t, \Pi^b_1(X))\}$.

Proof. Lemma 1.1 shows "$\subseteq$", and part 2. of Lemma 1 shows "$\supseteq$". □

Dynamic ordinals are sets of number theoretic functions, i.e. subsets of ${}^{\mathbb{N}}\mathbb{N}$. We arrange subsets of ${}^{\mathbb{N}}\mathbb{N}$ by eventual majorizability:

$$f \trianglelefteq g \quad :\Leftrightarrow \quad g \text{ eventually majorizes } f \quad \Leftrightarrow \quad (\exists m)(\forall n \geq m) f(n) \leq g(n) \ .$$

For subsets of number theoretic functions $D, E \subseteq {}^{\mathbb{N}}\mathbb{N}$ we define

$$D \trianglelefteq E \quad :\Leftrightarrow \quad (\forall f \in D)(\exists g \in E) f \trianglelefteq g$$

and from this

$$\begin{aligned} D \equiv E \quad &:\Leftrightarrow \quad D \trianglelefteq E \ \ \& \ \ E \trianglelefteq D \\ D \lhd E \quad &:\Leftrightarrow \quad D \trianglelefteq E \ \ \& \ \ E \not\trianglelefteq D \end{aligned}$$

$\trianglelefteq$ is a partial, transitive, reflexive ordering, $\lhd$ is a partial, transitive, irreflexive, not well-founded ordering, and $\equiv$ is an equivalence relation.

Lemma 4. *Let S, T be two theories in the language of bounded arithmetic and assume* $\mathrm{DO}(S) \neq \mathrm{DO}(T)$. *Then S is separated from T.*

Proof. Assume $f \in \mathrm{DO}(T) \setminus \mathrm{DO}(S)$. By the definition of dynamic ordinals there is a term $t(x)$ and a $\Pi^b_1(X)$-formula A such that $f(n) = t(n)$ and $T \vdash (\forall x)\, \mathcal{O}\mathrm{Ind}(t(x), A)$. But $f \notin \mathrm{DO}(S)$ implies $S \nvdash (\forall x)\, \mathcal{O}\mathrm{Ind}(t(x), A)$. □

Using the well-known big-O notation we will denote sets

$$f(O(g(\mathrm{id}))) \quad := \quad \{\lambda n. f(c \cdot g(n)) \,:\, c \in \mathbb{N}\}$$

for unary number-theoretic functions f and g, where id denotes the identity function, i.e. $\mathrm{id}(n) = n$. We have the following crude upper bound on dynamic ordinals which is simply given by the growth rates of the functions representable by terms in the language $\mathcal{L}_{\mathrm{BA}}$:

$$\mathrm{DO}(T) \quad \trianglelefteq \quad 2_2(O(|\,\mathrm{id}\,|_2)) \ .$$

The language $\mathcal{L}_{\mathrm{BA}}$ includes the successor function, $+$ and $\cdot$, which enables us to speed-up induction polynomially.

Lemma 5. *Let T be a theory and Φ a set of formulas closed under substitution. Suppose $T \vdash \mathcal{S}\mathrm{Ind}(t, \Phi)$. Then $T \vdash \mathcal{S}\mathrm{Ind}(p(t), \Phi)$ for all polynomials p.*

Proof. We suppose that the assumptions of the lemma hold. We prove the assertion by induction on the complexity of the polynomial p. The interesting case is that $p(x)$ is of the form $q(x) \cdot x$. Let $A \in \Phi$, $C(z) :\equiv A(z \cdot t)$ and $D(u) :\equiv A(c \cdot t + u)$, then by assumption $C, D \in \Phi$, hence by induction hypothesis $\mathcal{S}\mathrm{Ind}(q, C)$ and by assumption $\mathcal{S}\mathrm{Ind}(t, D)$. These are used to conclude $\mathcal{S}\mathrm{Ind}(p(t), A)$ in T. □

Lemma 6. *Let T be a theory and Φ a set of formulas closed under bounded universal quantification and substitution. Suppose $T \vdash \mathcal{O}\mathrm{Ind}(t, \Phi)$. Then $T \vdash \mathcal{O}\mathrm{Ind}(p(t), \Phi)$ for all polynomials p.*

Proof. Suppose $T \vdash \mathcal{O}\mathrm{Ind}(t, \Phi)$. Then Lemma 1.1. shows $T \vdash \mathcal{S}\mathrm{Ind}(t, \Phi)$. Hence $T \vdash \mathcal{S}\mathrm{Ind}(p(t), \Phi)$ by Lemma 5. Hence $T \vdash \mathcal{O}\mathrm{Ind}(p(t), \Phi)$ using Lemma 1.2. □

The last Lemma together with Lemma 1 yields

Theorem 7. *Σ^b_n-$\mathrm{L}^m\mathrm{IND} \vdash \mathcal{O}\mathrm{Ind}(p(|x|_m), \Pi^b_n)$ for polynomials p, if $m > 0$ or $n > 0$.*

Proof. Let T be Σ^b_n-$\mathrm{L}^m\mathrm{IND}$, then T proves the schema $\mathcal{S}\mathrm{Ind}(|x|_m, \Pi^b_n)$. In case $n > 0$, Lemma 1.2. shows $T \vdash \mathcal{O}\mathrm{Ind}(|x|_m, \Pi^b_n)$. In case $n = 0$ we have $m > 0$ by assumption. An inspection of the proof of Lemma 1.2. shows that the induction is on a sharply bounded formula for sharply bounded A. Thus, we always have $T \vdash \mathcal{O}\mathrm{Ind}(|x|_m, \Pi^b_n)$, hence the assertion follows from Lemma 6. □

For special theories these results can be rewritten as

$$\mathrm{T}^{i+1}_2 \vdash \mathcal{O}\mathrm{Ind}(2^{|t|^c}, \Pi^b_{i+1})$$
$$\mathrm{S}^{i+1}_2 \vdash \mathcal{O}\mathrm{Ind}(|t|^c, \Pi^b_{i+1})$$
$$\mathrm{sR}^{i+1}_2 \vdash \mathcal{O}\mathrm{Ind}(||t||^c, \Pi^b_{i+1})$$

for any positive integer c.

Order induction for higher formula complexity is connected to larger order induction by speed-up techniques. The main ingredient which formalizes this is the following jump set $\mathrm{Jp}(t, x, X)$:

$$\left\{ y \leq t \,:\, t \leq |x| \wedge (\forall z \leq 2^t)[z \subseteq X \wedge z + 2^y \leq 2^t + 1 \rightarrow z + 2^y \subseteq X] \right\} .$$

Iterations of Jp are defined by

$$\begin{aligned} \mathrm{Jp}_0(t, x, X) &= X \ , \\ \mathrm{Jp}_{i+1}(t, x, X) &= \mathrm{Jp}(t, |x|_i, \mathrm{Jp}_i(t, x, X)) \ , \end{aligned}$$

where $|\cdot|_i$ is the i-fold iteration of $|\cdot|$. Also, 2_m denotes the m-fold iteration of exponentiation. Using the iterated jump set we obtain the following connections:

Theorem 8.

$$\mathrm{BASIC} \vdash t \leq |x|_m \rightarrow [\mathcal{O}\mathrm{Ind}(2_m(t), A) \leftrightarrow \mathcal{O}\mathrm{Ind}(t, \mathrm{Jp}_m(t, x, A))] \ .$$

Proof. The direction from left to right follows directly. For the other direction we would have to prove the following lemma

$$\mathrm{BASIC} \vdash t \leq |x| \wedge \mathcal{O}\mathrm{Prog}(2^t, A) \rightarrow \mathcal{O}\mathrm{Prog}(t, \mathrm{Jp}(t, x, A)) \ . \qquad \square$$

Concerning the complexity of the iterated jump we observe that

$$\mathrm{Jp}_i(t, x, \Pi^b_1) \subset \Pi^b_{i+1}$$

hence Theorem 7 and Theorem 8 together show

Corollary 9. *Let $0 \leq n < m$ or $n = m = 1$, and let c be some natural number, then Σ^b_{n+1}-$\mathrm{L}^m\mathrm{IND} \vdash \mathcal{O}\mathrm{Ind}(2_n(|x|^c_m), \Pi^b_1)$, hence Σ^b_{n+1}-$\mathrm{L}^m\mathrm{IND} \vdash \mathcal{O}\mathrm{Ind}(2_{n+1}(c \cdot |x|_{m+1}), \Pi^b_1)$.* $\square$

This establishes already tight lower bounds on dynamic ordinals. Tight upper bounds on dynamic ordinals are obtained by dynamic ordinal analysis (see [3] or [4]) for theories $\Sigma^b_m(X)$-$\mathrm{L}^m\mathrm{IND}$ for $m > 0$. Results from Arai [1], section 2.4, yield tight upper bounds on dynamic ordinals for theories $\Sigma^b_m(X)$-$\mathrm{L}^{m+1}\mathrm{IND}$ for $m > 0$ (see [4]). Altogether we obtain the following results:

$$\begin{aligned}
\mathrm{DO}(\mathrm{T}^1_2(X)) &\equiv 2_2(O(|\,\mathrm{id}\,|_2)) \equiv \mathrm{DO}(\mathrm{S}^2_2(X)) \\
\mathrm{DO}(\mathrm{S}^1_2(X)) &\equiv 2_1(O(|\,\mathrm{id}\,|_2)) \\
\mathrm{DO}(\mathrm{sR}^2_2(X)) &\equiv 2_2(O(|\,\mathrm{id}\,|_3)) \\
\mathrm{DO}(\mathrm{sR}^1_2(X)) &\equiv 2_1(O(|\,\mathrm{id}\,|_3)) \ ,
\end{aligned}$$

and more generally for $m > 0$

$$\begin{aligned}
\mathrm{DO}(\Sigma^b_m(X)\text{-}\mathrm{L}^{m+1}\mathrm{Ind}) &\equiv 2_m(O(|\,\mathrm{id}\,|_{m+2})) \\
\mathrm{DO}(\Sigma^b_m(X)\text{-}\mathrm{L}^m\mathrm{Ind}) &\equiv 2_m(O(|\,\mathrm{id}\,|_{m+1})) \ .
\end{aligned}$$

Thus by the previous Lemma and remarks these dynamic ordinals lead to relationships of bounded arithmetic theories which we display in Fig. 2. Here we mean with $S < T$ that the theories S and T are separated and S is included in the consequences of T; with $S \equiv T$ that S and T have the same dynamic ordinals (this does not imply that S and T prove the same consequences); and with $S \nsubseteq T$ that S is not included in the consequences of T.

4 Witness oracle query complexity

In this section we define witness oracle Turing machines and summarize how definable multivalued functions in bounded arithmetic theories are connected to witness oracle Turing machines.

A Turing machine with a witness oracle $Q(x) = (\exists y)R(x, y)$ is a Turing machine with a query tape for queries to Q that answers a query a as follows:

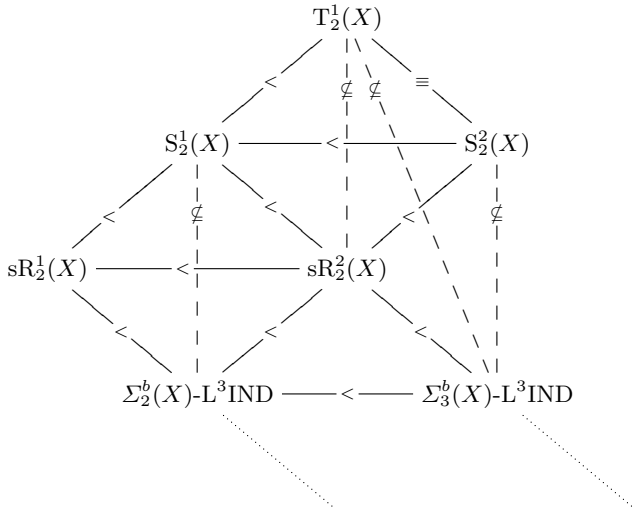


Fig. 2. Separations by dynamic ordinal analysis

1. if $Q(a)$ holds, then it returns YES and some b such that $R(a, b)$;
2. if $\neg Q(a)$ holds, then it returns NO.

In general this type of Turing machine, called witness oracle Turing machine (WOTM), computes only *multivalued* functions rather than functions, as there may be multiple witnesses to affirmative oracle answers. A multivalued function is a relation $f \subseteq \mathbb{N} \times \mathbb{N}$ such that for all $x \in \mathbb{N}$ there exists some $y \in \mathbb{N}$ with $(x, y) \in f$. We express $(x, y) \in f$ as $f(x) = y$. A natural stratification of WOTMs, called bounded WOTMs, is obtained by bounding the number of oracle queries.

Pollett in [16] has given characterization of definable multivalued functions of theories of bounded arithmetic analogous to Krajíček's characterization of the Σ_{i+1}^b-multivalued functions of S_2^i as $\mathrm{FP}^{\Sigma_i^b}(\mathrm{wit}, O(\log n))$ (cf. [10]). $\mathrm{FP}^{\Sigma_i^b}(\mathrm{wit}, O(\log n))$ is the class of multivalued functions computable by a polynomial time WOTM which on inputs of length n uses fewer than $O(\log n)$ witness queries to a Σ_i^b-oracle. For Φ is a set of formulas, a multivalued function f is called Φ-definable in some theory T if there is a formula $\varphi(x, y)$ in Φ such that φ describes the graph of f and T proves the totality of f via φ:

$$T \vdash (\forall x)(\exists y)\varphi(x, y)$$
$$\mathbb{N} \vDash (\forall x)(\forall y)[f(x) = y \leftrightarrow \varphi(x, y)]$$

Pollett generalizes polynomial time WOTM classes and bounded arithmetic theories in the following form to obtain a very general relationship of definable multivalued functions and bounded polynomial time WOTM classes.

Definition 10. *Let τ be a set of unary functions represented by terms in $\mathcal{L}_{\mathrm{BA}}$.*

1. $\mathrm{FP}^{\Sigma_i^b}(\mathrm{wit}, \tau)$ *is the class of multivalued functions computable by a polynomial time WOTM which on input* x *uses fewer than* $l(t(x))$ *witness queries to a* Σ_i^b*-oracle for some* $l \in \tau$ *and* $\mathcal{L}_{\mathrm{BA}}$*-term* t*.*
2. *Let* $\hat{\mathrm{T}}_2^{i,\tau}$ *be the theory* $\mathrm{BASIC} + \Sigma_i^b\text{-IND}^\tau$*, where* $\Sigma_i^b\text{-IND}^\tau$ *is the schema*

$$\varphi(0) \wedge (\forall x)(\varphi(x) \to \varphi(x+1)) \to (\forall x)\varphi(l(x))$$

with $\varphi \in \Sigma_i^b$ *and* $l \in \tau$*.*

As said before, id denotes identity $\mathrm{id}(n) = n$. The class $\mathrm{FP}^{\Sigma_i^b}(\mathrm{wit}, O(\log n))$ considered by Krajíček can be expressed as $\mathrm{FP}^{\Sigma_i^b}(\mathrm{wit}, O(|\,\mathrm{id}\,|_2))$ by the previous definition. Also the bounded arithmetic theories defined in previous sections can be expressed in terms of the last Definition.

$$\begin{aligned} \mathrm{T}_2^i &= \hat{\mathrm{T}}_2^{i,\mathrm{id}} & \mathrm{S}_2^i &= \hat{\mathrm{T}}_2^{i,|\,\mathrm{id}\,|} \\ \mathrm{sR}_2^i &= \hat{\mathrm{T}}_2^{i,||\,\mathrm{id}\,||} & \Sigma_i^b\text{-L}^m\mathrm{IND} &= \hat{\mathrm{T}}_2^{i,|\,\mathrm{id}\,|_m} \quad . \end{aligned}$$

Pollett obtains the following general characterization of definable multivalued functions by bounded polynomial time WOTMs.

Theorem 11 (Pollett [16])**.**

1. *A multivalued function* f *is* Σ_{i+1}^b*-definable in* $\hat{\mathrm{T}}_2^{i,\tau}$ *iff* $f \in \mathrm{FP}^{\Sigma_i^b}(\mathrm{wit}, O(|\tau|))$ *for* $i \geq 1$*.*
2. *A multivalued function* f *is* Σ_{i+k}^b*-definable in* $\hat{\mathrm{T}}_2^{i,\tau}$ *iff* $f \in \mathrm{FP}^{\Sigma_{i+k-1}^b}(\mathrm{wit}, O(1))$ *for* $k \geq 2$ *and* $i \geq 0$*.* □

Furthermore, Pollett obtains conservation results, which we do not state here in its general form, but in a form suitable for later use. Let τ be the set

$$\tau \quad := \quad 2_k(O(|\,\mathrm{id}\,|_l))$$

for some fixed k, l satisfying $k + 2 \leq l$; in particular, this implies $\tau \trianglelefteq \{|\,\mathrm{id}\,|\}$.

Theorem 12 (Pollett [16])**.** *For* τ *as defined above, the theories* $\hat{\mathrm{T}}_2^{i+1,\tau}$ *and* $\hat{\mathrm{T}}_2^{i,2^\tau}$ *prove the same* Σ_{i+1}^b*-formulas. I.e.,* $\hat{\mathrm{T}}_2^{i+1,\tau}$ *is* Σ_{i+1}^b*-conservative over* $\hat{\mathrm{T}}_2^{i,2^\tau}$*, in symbols* $\hat{\mathrm{T}}_2^{i,2^\tau} \preceq_{\Sigma_{i+1}^b} \hat{\mathrm{T}}_2^{i+1,\tau}$*.* □

5 Connecting dynamic ordinals and witness oracle query complexity

In this section we use the results from the previous two sections to compare dynamic ordinals and definable multivalued functions. We want to compute the Σ_2^b-definable multivalued functions of Σ_i^b-L^{m}IND for $0 < i \leq m$. To this end we first conclude that Σ_i^b-L^{m}IND is Σ_2^b-conservative over $\hat{\mathrm{T}}_2^{1,2_i(O(|\,\mathrm{id}\,|_{m+1}))}$ by applying Theorem 12, hence both theories have the same Σ_2^b-definable multivalued

functions. For the second equality in the following computation, we use the fact that induction can always be speeded up polynomially, cf. Lemma 5.

$$\begin{array}{lllll} \Sigma_i^b\text{-L}^m\text{IND} & = & \hat{\mathrm{T}}_2^{i,|\,\mathrm{id}\,|_m} & = & \hat{\mathrm{T}}_2^{i,|\,\mathrm{id}\,|_m^{O(1)}} \quad = \quad \hat{\mathrm{T}}_2^{i,2_1(O(|\,\mathrm{id}\,|_{m+1}))} \\ & \succeq_{\Sigma_i^b} & \hat{\mathrm{T}}_2^{i-1,2_2(O(|\,\mathrm{id}\,|_{m+1}))} & & \\ & \vdots & & & \\ & \succeq_{\Sigma_2^b} & \hat{\mathrm{T}}_2^{1,2_i(O(|\,\mathrm{id}\,|_{m+1}))} \ . & & \end{array}$$

This can be used to argue that Σ_i^b-L^{m}IND and $\hat{\mathrm{T}}_2^{1,2_i(O(|\,\mathrm{id}\,|_{m+1}))}$ have the same Σ_2^b-definable multivalued functions. The argument is the following: Let T be one of Σ_i^b-L^{m}IND or $\hat{\mathrm{T}}_2^{1,2_i(O(|\,\mathrm{id}\,|_{m+1}))}$, and let $\varphi(x,y)$ be in Σ_2^b such that $T \vdash (\forall x)(\exists y)\varphi(x,y)$. By Parikh's Theorem ([14], or see [5, p.83, Theorem 11]), there is a term $t(x)$ in $\mathcal{L}_{\mathrm{BA}}$ such that $T \vdash (\exists y \leq t(x))\varphi(x,y)$. Furthermore, $(\exists y \leq t(x))\varphi(x,y)$ is in Σ_2^b.

Now we can compute the Σ_2^b-definable multivalued functions of Σ_i^b-L^{m}IND. As argued above, they are the same as the Σ_2^b-definable multivalued functions of $\hat{\mathrm{T}}_2^{1,2_i(O(|\,\mathrm{id}\,|_{m+1}))}$. By Theorem 11, these are $\mathrm{FP}^{\Sigma_1^b}(\mathrm{wit}, 2_{i-1}(O(|\,\mathrm{id}\,|_{m+1})))$.

Corollary 13 (Pollett **[16]**). *The multivalued function f is Σ_2^b-definable in Σ_i^b-L^{m}IND iff $f \in \mathrm{FP}^{\Sigma_1^b}(\mathrm{wit}, 2_{i-1}(O(|\,\mathrm{id}\,|_{m+1})))$.* □

Now we can compare the Σ_2^b-definable multivalued functions of certain unrelativized theories with the dynamic ordinals of their relativized companions. At the end of section 3 we have computed the dynamic ordinal of some theories of bounded arithmetic:

$$\begin{array}{lll} \mathrm{DO}(\mathrm{T}_2^1(X)) & \equiv & 2_2(O(|\,\mathrm{id}\,|_2)) \quad \equiv \quad \mathrm{DO}(\mathrm{S}_2^2(X)) \\ \mathrm{DO}(\mathrm{S}_2^1(X)) & \equiv & 2_1(O(|\,\mathrm{id}\,|_2)) \\ \mathrm{DO}(\mathrm{sR}_2^2(X)) & \equiv & 2_2(O(|\,\mathrm{id}\,|_3)) \\ \mathrm{DO}(\mathrm{sR}_2^1(X)) & \equiv & 2_1(O(|\,\mathrm{id}\,|_3)) \\ \mathrm{DO}(\Sigma_m^b(X)\text{-L}^m\mathrm{Ind}) & \equiv & 2_m(O(|\,\mathrm{id}\,|_{m+1})) \\ \mathrm{DO}(\Sigma_m^b(X)\text{-L}^{m+1}\mathrm{Ind}) & \equiv & 2_m(O(|\,\mathrm{id}\,|_{m+2})) \ . \end{array}$$

for $m > 0$. For example, in case of sR_2^2 we obtain:

$$\begin{array}{rcl} \mathrm{DO}(\mathrm{sR}_2^2(X)) & \equiv & 2_2(O(|\,\mathrm{id}\,|_3)) \\ \mathrm{sR}_2^2 & \succeq_{\Sigma_2^b} & \hat{\mathrm{T}}_2^{1,2_2(O(|\,\mathrm{id}\,|_3))} \\ \Sigma_2^b\text{-definable multivalued functions of } \mathrm{sR}_2^2 & = & \mathrm{FP}^{\Sigma_1^b}(\mathrm{wit}, 2_1(O(|\,\mathrm{id}\,|_3))) \ . \end{array}$$

Hence we can state the following connection between the Σ_2^b-definable multivalued functions of those unrelativized theories with the dynamic ordinals of their relativized companion.

Theorem 14. *For any theory T from the infinite list*

$$\mathrm{T}_2^1,\ \mathrm{S}_2^2,\ \mathrm{S}_2^1,\ \mathrm{sR}_2^2,\ \mathrm{sR}_2^1,\quad \Sigma_m^b\text{-}\mathrm{L}^{m+1}\mathrm{IND},\ \Sigma_m^b\text{-}\mathrm{L}^m\mathrm{IND}\ \text{ for arbitrary } m>0,$$

we have

1. *T is Σ_2^b-conservative over $\hat{\mathrm{T}}_2^{1,\mathrm{DO}(T(X))}$.*
2. *A multivalued function f is Σ_2^b-definable in T if and only if $f \in \mathrm{FP}^{\Sigma_1^b}(\mathrm{wit}, \log(\mathrm{DO}(T(X))))$.* □

6 Final remarks and possible extensions

• As we have seen the Σ_2^b-definable multivalued functions of certain unrelativized theories T of bounded arithmetic are strongly connected to the dynamic ordinals of their relativized companion $T(X)$. Up to now the computations of the definable multivalued functions and the dynamic ordinals are based on completely different methods. In a next step these different paths of computation should be brought together.

• It should be possible to extend the connection to other bounded arithmetic theories. In the same way as before Pollett's results show that Σ_{k+i-1}^b-$\mathrm{L}^m\mathrm{IND}$ is Σ_{k+1}^b-conservative over $\hat{\mathrm{T}}_2^{k,2_i(O(|\,\mathrm{id}\,|_{m+1}))}$ for $0 < i \le m$ and $k \ge 1$:

$$\begin{aligned}
\Sigma_{k+i-1}^b\text{-}\mathrm{L}^m\mathrm{IND} &= \hat{\mathrm{T}}_2^{k+i-1,|\,\mathrm{id}\,|_m} = \hat{\mathrm{T}}_2^{k+i-1,|\,\mathrm{id}\,|_m^{O(1)}} \\
&= \hat{\mathrm{T}}_2^{k+i-1,2_1(O(|\,\mathrm{id}\,|_{m+1}))} \\
&\succeq_{\Sigma_{k+i-1}^b} \hat{\mathrm{T}}_2^{k+i-2,2_2(O(|\,\mathrm{id}\,|_{m+1}))} \\
&\ \ \vdots \\
&\succeq_{\Sigma_{k+1}^b} \hat{\mathrm{T}}_2^{k,2_i(O(|\,\mathrm{id}\,|_{m+1}))}\ .
\end{aligned}$$

For $k \ge 2$, the Σ_2^b-definable multivalued functions of $\hat{\mathrm{T}}_2^{k,2_m(O(|\,\mathrm{id}\,|_{m+1}))}$ cannot be expressed adequately in terms of bounded witness oracle Turing machines with Σ_1^b witness oracles, because $|\,\mathrm{id}\,| \lhd 2_m(O(|\,\mathrm{id}\,|_{m+1}))$, $\mathrm{T}_2^{k-1} \subseteq \mathrm{S}_2^k = \hat{\mathrm{T}}_2^{k,|\,\mathrm{id}\,|}$, and already for T_2^1 we have the maximal possible number of oracle accesses, namely polynomially many. This class of definable function has to be expressed in terms of a different type of computation like polynomial local search. E.g., by a result of Buss and Krajíček 1994 [7] the Σ_1^b-definable multivalued functions of T_2^1 can be expressed in terms of polynomial local search problems.

But if we look at Σ_{k+1}^b-definable multivalued functions we again obtain reasonable classes of bounded witness oracle Turing machines: In the following

table let $0 < i \leq m$, $j < k$ and $k \geq 1$. The values listed in the next table have the following properties for a given theory T:

$$T \succeq_{\Sigma^b_{k+1}} \hat{\mathrm{T}}^{k,\nu_T}_2$$

$$\Sigma^b_{k+1}\text{-definable multivalued functions of } T = \mathrm{FP}^{\Sigma^b_k}(\mathrm{wit}, \sigma_T) \ .$$

We obtain:

T	ν_T	σ_T
T^k_2	$2_2(O(\lvert \mathrm{id} \rvert_2))$	$2_1(O(\lvert \mathrm{id} \rvert_2))$
S^{k+1}_2	$2_2(O(\lvert \mathrm{id} \rvert_2))$	$2_1(O(\lvert \mathrm{id} \rvert_2))$
S^k_2	$2_1(O(\lvert \mathrm{id} \rvert_2))$	$O(\lvert \mathrm{id} \rvert_2)$
sR^{k+1}_2	$2_2(O(\lvert \mathrm{id} \rvert_3))$	$2_1(O(\lvert \mathrm{id} \rvert_3))$
sR^k_2	$2_1(O(\lvert \mathrm{id} \rvert_3))$	$O(\lvert \mathrm{id} \rvert_3)$
Σ^b_{k-1+i}-$\mathrm{L}^m\mathrm{IND}$	$2_i(O(\lvert \mathrm{id} \rvert_{m+1}))$	$2_{i-1}(O(\lvert \mathrm{id} \rvert_{m+1}))$
Σ^b_j-$\mathrm{L}^m\mathrm{IND}$		$O(1)$

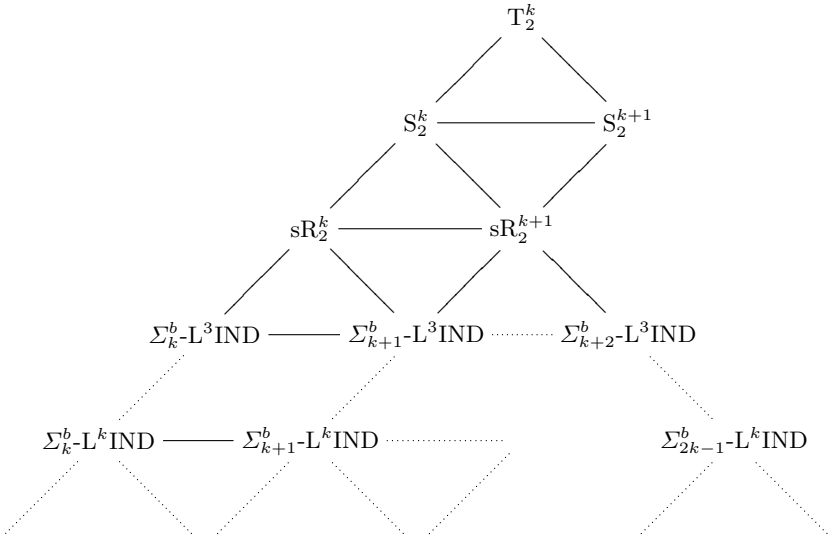


Fig. 3. Theories which have their Σ^b_{k+1}-definable multivalued functions characterized by bounded witness oracle TURING machines. ($k \geq 1$)

Hence, all theories displayed in Fig. 3 have their Σ^b_{k+1}-definable multivalued functions reasonably characterized by bounded witness oracle TURING machines. From this Figure we can conjecture that an adequate definition of a dynamic ordinal of these theories is likely to exist such that they are connected to Σ^b_{k+1}-definable multivalued functions in the same way as before. An obvious candidate

would be

$$\mathrm{DO}_k(T) \quad = \quad \{\lambda x.t \,:\, T \vdash (\forall x)\, \mathcal{O}\mathrm{Ind}(t, \Pi^b_k(X))\} \ .$$

Another observation drawn from Fig. 3 is that it should be possible for example to compute directly $\mathrm{DO}(\Sigma^b_1\text{-L}^3\text{IND})$ by proof theoretic means similar to dynamic ordinal analysis.

References

1. Toshiyasu Arai. Some results on cut-elimination, provable well-orderings, induction and reflection. *Ann. Pure Appl. Logic*, 95:93–184, 1998.
2. Theodore Baker, John Gill, and Robert Solovay. Relativizations of the $\mathcal{P} =? \mathcal{NP}$ question. *SIAM J. Comput.*, 4:431–442, 1975.
3. Arnold Beckmann. *Seperating fragments of bounded predicative arithmetic.* PhD thesis, Westf. Wilhelms-Univ., Münster, 1996.
4. Arnold Beckmann. Dynamic ordinal analysis. *Arch. Math. Logic*, 2001. accepted for publication.
5. Samuel R. Buss. *Bounded arithmetic*, volume 3 of *Stud. Proof Theory, Lect. Notes.* Bibliopolis, Naples, 1986.
6. Samuel R. Buss. Relating the bounded arithmetic and the polynomial time hierarchies. *Ann. Pure Appl. Logic*, 75:67–77, 1995.
7. Samuel R. Buss and Jan Krajíček. An application of boolean complexity to separation problems in bounded arithmetic. *Proc. London Math. Soc.*, 69:1–21, 1994.
8. Johan Håstad. *Computational Limitations of Small Depth Circuits.* MIT Press, Cambridge, MA, 1987.
9. Jan Johannsen. A note on sharply bounded arithmetic. *Arch. Math. Logik Grundlag.*, 33:159–165, 1994.
10. Jan Krajíček. Fragments of bounded arithmetic and bounded query classes. *Trans. Amer. Math. Soc.*, 338:587–98, 1993.
11. Jan Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory.* Cambridge University Press, Heidelberg/New York, 1995.
12. Jan Krajíček, Pavel Pudlák, and Gaisi Takeuti. Bounded arithmetic and the polynomial hierarchy. *Ann. Pure Appl. Logic*, 52:143–153, 1991.
13. Daniel Leivant. Substructural termination proofs and feasibility certification. In *Proceedings of the 3rd Workshop on Implicit Computational Complexity (Aarhus)*, pages 75–91, 2001.
14. Rohit J. Parikh. Existence and feasibility in arithmetic. *J. Symbolic Logic*, 36:494–508, 1971.
15. Wolfram Pohlers. *Proof Theory. An Introduction.* Number 1407 in Lect. Notes Math. Springer, Berlin/Heidelberg/New York, 1989.
16. Chris Pollett. Structure and definability in general bounded arithmetic theories. *Ann. Pure Appl. Logic*, 100:189–245, 1999.
17. Gaisi Takeuti. RSUV isomorphism. In Peter Clote and Jan Krajíček, editors, *Arithmetic, proof theory, and computational complexity*, Oxford Logic Guides, pages 364–86. Oxford University Press, New York, 1993.
18. Andrew C. Yao. Separating the polynomial-time hierarchy by oracles. *Proc. 26th Ann. IEEE Symp. on Foundations of Computer Science*, pages 1–10, 1985.
19. Domenico Zambella. Notes on polynomially bounded arithmetic. *J. Symbolic Logic*, 61:942–966, 1996.