INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI

A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor MI 48106-1346 USA
313/761-4700 800/521-0600

UNIVERSITY OF CALIFORNIA, SAN DIEGO

Arithmetic Theories with Prenex Normal Form Induction

A dissertation submitted in partial satisfaction of the
requirements for the degree Doctor of Philosophy
in Mathematics

by

Christopher J. Pollett

Committee in charge:

Professor Samuel R. Buss, Chair
Professor Jeff Remmel
Professor Peter Doyle
Professor Russell Impagliazzo
Professor Ramamohan Paturi

1997

The dissertation of Christopher J. Pollett is approved. and it is acceptable in quality and form for publication on microfilm:

Chair

University of California, San Diego

1997

To Ronghui Xu and my parents and little James

TABLE OF CONTENTS

List of Symbols

ACKNOWLEDGEMENTS

First and foremost I would like to thank my advisor, Sam Buss, for introducing me to the area of bounded arithmetic. I have greatly appreciated his advice both academic and nonacademic, his attention to rigour, and his insights into logic and complexity.

Besides my advisor I have learned a good deal from discussions and classes I have taken with Jeffrey Remmel and Russell Impagliazzo. I have also benefitted from e-mail exchanges with Stephen Bloch, Jan Johannsen, and Arnold Beckmann. During the last three years of my stay here at UCSD, I have had a GAANN fellowship. I would like to thank Jim Lin for helping me to get this fellowship.

VITA

August 19, 1970	Born, Halifax, Canada
1992	B.S., California Institute of Technology, U.S.A.
1993–1996	Teaching Assistant, Department of Mathematics University of California, San Diego
1995	M.A., University of California, San Diego
1995	Candidate of Philosophy University of California, San Diego
1997	Doctor of Philosophy University of California, San Diego

FIELDS OF STUDY

Major Field: Mathematical Logic

Studies in Proof theory and Computational Complexity.
Professor Sam Buss

ABSTRACT OF THE DISSERTATION

Arithmetic Theories with Prenex Normal Form Induction

by

Christopher J. Pollett
Doctor of Philosophy in Mathematics
University of California, San Diego, 1997
Professor Sam Buss, Chair

This thesis investigates bounded arithmetic theories whose inductions axioms use prenex formulas. The standard bounded arithmetic theories are R_2^i, S_2^i, and T_2^i. Their prenex versions are $\hat{R}_2^i$, $\hat{S}_2^i$, and $\hat{T}_2^i$. We show $\hat{S}_2^i = S_2^i$ and $\hat{T}_2^i = T_2^i$. It is unclear whether $\hat{R}_2^i$ equals R_2^i. Nevertheless, we show $S_2^{i-1} \subseteq \hat{R}_2^i$, and R_2^i is $B(\hat{\Sigma}_i^b)$-conservative over $\hat{R}_2^i$ if $i > 1$. We extend $BASIC$, the base theory of R_2^i, S_2^i and T_2^i, by three open axioms for pairing to get a theory $EBASIC$, contained in $\hat{R}_2^0$, which we use as a base theory for our results. We define $\hat{T}_2^{i,\tau} := EBASIC + \hat{\Sigma}_i^b\text{-}IND^\tau$ where $\hat{\Sigma}_i^b\text{-}IND^\tau$ is $\hat{\Sigma}_i^b$-induction up to 1-ary terms in a set τ. In particular, the theory $\hat{T}_2^{i,\{id\}}$ is T_2^i. For an operation $\circ$, a set τ is $\circ$-closed if whenever $t(a)$ and $s(a)$ are in τ, there is a $t \circ s$ in τ and a term r such that $(t \circ s)(r(a)) = t(a) \circ s(a)$. We write $\dot{\tau}$, $\tau^\#$ for the $\cdot$-closure and $\#$-closure of τ. We prove $\hat{T}_2^{i,\tau} = \hat{T}_2^{i,\dot{\tau}}$; however, it is unknown if $\hat{T}_2^{i,\tau} = \hat{T}_2^{i,\tau^\#}$. The set $|\tau|$ are the terms $|t|$ where $t \in \tau$. We define an algebra $B_{i,2}^{|\tau|}$ for the $\hat{\Sigma}_i^b$-definable multifunctions of $\hat{T}_2^{i,|\tau|}$. We show the $\hat{\Sigma}_i^b$-definable multifunctions of $\hat{T}_2^{i,\tau}$ are the local search class $\pi LS_i^{B_{i,2}}$ and the $\hat{\Sigma}_{i+1}^b$-definable multifunctions of $\hat{T}_2^{i,\tau}$ are the class $FP^{\Sigma_i^p}(wit, |\tau|)$. For $\hat{\Sigma}_{i+k+2}^b$-definability we get $FP^{\Sigma_{i+k+1}^p}(wit, 1)$. We prove $\hat{T}_2^{i+1,|\tau|} = \hat{T}_2^{i+1,|\tau^\#|}$ is $B(\hat{\Sigma}_{i+1}^b)$-conservative over $\hat{T}_2^{i,\tau^\#}$. We show $\hat{T}_2^{i,|\tau|}$ proves $\hat{\Delta}_{i+1}^b\text{-}IND^{|\tau|}$. This gives a proof theoretic proof that S_2^i proves $\Delta_{i+1}^b\text{-}LIND$ and $\hat{R}_2^i$ proves $\hat{\Delta}_{i+1}^b\text{-}LLIND$. We consider $\hat{C}_2^{i,|\tau|}$ consisting of $EBASIC$, $open\text{-}IND^{|\tau|}$, and the replacement schema $\hat{\Pi}_i^b\text{-}REPL^{|\tau|}$. We show $\hat{C}_2^{i,|\tau|}$

is $B(\hat{\Sigma}^b_{i+1})$-conservative over $\hat{T}^{i,|\tau|}_2$. We characterize the τ-bounded $\hat{\Sigma}^b_{i-1}$-and $\hat{\Sigma}^b_i$-definable functions of $\hat{T}^{i,\tau}_2$ and $\hat{C}^{i,|\tau|}_2$ using parallel function classes. We show the $\hat{\Sigma}^b_i$-definable functions of R^i_2 are the class $FNC^{\Sigma^p_i}$. We weaken $\hat{C}^{0,|\tau|}_2$ to a theory $\bar{C}^{0,|\tau|}_2$ by $|\tau|$-bounding $\hat{\Pi}^b_0$-formulas in replacement axioms. We show the $\hat{\Sigma}^b_{1,|\tau|}$-definable functions of $\bar{C}^{0,|\tau|}_2$ are FTC^0_τ. The class $FTC^0_{\{id\}}$ equals the standard FTC^0. We show $FTC^0_{|\tau|} \subsetneq FTC^0_{\{id\}}$ and $\bar{C}^{0,|\tau|}_2 \subsetneq \hat{C}^{0,\{id\}}_2$. We show if $T^i_2 = \hat{T}^{i-1,\tau'}_2$ or if $T^i_2 = \hat{C}^{i+1,|\tau'|}_2$ or if $\hat{C}^{i,|\tau|}_2 = \hat{T}^{i+1,\tau'}_2$ where τ contains an unbounded term then $\Sigma^p_{i-3} = \Pi^p_{i+3}$. We separate $P^{\Sigma^p_i(A)}(\{||\ell||\})$ from $P^{\Sigma^p_i(A)}(\{|\ell|\})$ for reasonably behaved ℓ and deduce oracle separations for our theories.

Chapter I

Introduction

Three important families of bounded arithmetic theories, R^i_2 , S^i_2, and T^i_2, were developed in Buss [13], Allen [2],Clote-Takeuti [19], and Takeuti [49]. These theories have been intensively studied because of their close connection to computational complexity. In this chapter, we introduce the background necessary to properly define these theories and to briefly discuss this connection. Given this introduction, we then motivate the use of prenex versions of these theories and describe the format of the rest of this thesis. This thesis assumes the knowledge of an introductory course in mathematical logic at the level of Enderton [22] or van Dalen [50]. Two important logic results we state and use without proof are Parikh's Theorem and Gentzen's Cut Elimination Theorem. Proofs of these results can be found in Buss [13] and Takeuti [48]. Although we try to be self-contained, we also assume some knowledge of computational complexity. A good introduction to the computational complexity topics which we will sometimes casually introduce can be found in Balcazár, Diaz, and Gabarró [3, 4] and can also be found in Papadimitriou [37]. We state and use without proof the correspondence between the polynomial-time hierarchy and the bounded arithmetic hierarchy. This can be found in Buss [13]. We also state and use without proof the results of Chang and Kadin [17] and Kadin [30] that if the Boolean hierarchy collaspes over Σ^p_i then the polynomial hierarchy collapses to the $i+3$rd level.

I.A The Polynomial Hierarchy

In the 1930's many different formalisms were introduced by such luminaries as Church, Gödel, Post, and Turing to try to capture the idea of what it means for a function to be effectively computable. All of these notions turned out to be equivalent and Church's Thesis states that these equivalent formulations do in fact characterize the meaning of effective computable function. We call the class of effectively computable functions the *recursive functions*.

Our model of a recursive set of natural numbers is a set of natural numbers, membership in which can be determined by a Turing machine in a finite number steps on a given input of a natural number. Closely associated to the notion of computable function is that of a computably listable set of numbers. A set of natural numbers is recursively enumerable (r.e.) if there is a recursive procedure which will eventually list out all of its members. If x is in an r.e. set then one will see it listed out by the recursive procedure in a finite amount of time, but in general if x is not in the set one has to wait until forever to find out. The set K of programs (coded as natural numbers) which eventually halt when fed themselves as input is an example of a set which is recursively enumerable but not recursive. Recursively enumerable sets are sometimes called Σ_1-sets. If one attaches a Σ_1-set to a Turing Machine as an oracle so that in one time step the machine can ask a question and get an answer about whether some number belongs to the Σ_1-set, one can get a much more powerful machine. The Σ_2-sets are those sets which are recursively enumerable by machines with oracles for Σ_1-sets. Iterating this procedure one gets an infinite hierarchy called the arithmetic hierarchy of sets $\cup_n \Sigma_n$ and one can show $\Sigma_n \subsetneq \Sigma_{n+1}$. Complements of Σ_n-sets are called Π_n-sets. Sets which are both Σ_n and Π_n are called Δ_n. It turns outs the recursive sets are the Δ_1-sets. Two good books on recursion theory where these issues are discussed are Soare [46] and Odifreddi [36].

The arithmetic hierarchy get its name from the fact that if one takes

formulas over the language of arithmetic $0, S, +, \cdot, \leq$ then Σ_n-sets correspond to relations determined by formulas with at most n-alternations of quantifiers (not counting bounded quantifiers) the outermost being an existential quantifier. Similarly, Π_n-sets correspond to relations determined by formulas with at most n-alternations of quantifiers the outermost being a universal quantifier. The set of relations computable by bounded formula is called Σ_0. One of the most studied theories in logic is Peano Arithmetic (PA). It consists of a finite set of open axioms Q for $0, S, +, \cdot, \leq$ as well as induction for any formula in the arithmetic hierarchy. Well studied fragments of PA are the theories $I\Sigma_n$ which consists of Q and induction for Σ_n-formulas. Good book on Peano Arithmetic and its fragments are Hájek and Pudlák [24] and Kaye [31].

The notion of recursive function suffered from the fact that although a recursive function is guaranteed to halt it might take a very long time as a function of the length of the input to do so. In the 1960's and early 1970's the notion of a *feasible* computation was developed. Generally, it was believed that membership in a feasible predicate should take at most polynomial time in the input length to determine. However, there were problems like the satisfiability of a boolean formula (SAT) which could be solved in polynomial time provided one allowed nondeterminism. In the case of SAT if one first "guesses" a truth assignment for the boolean formula in question one can verify in polynomial time whether or not the truth assignment satisfies the formula. Relations computable in deterministic polynomial time were called P and those in nondeterministic polynomial time NP. It is unknown whether these two classes are equal, yet the intuition is that some NP problems should take exponential time. The study of NP began essentially with Cook [21] who showed that SAT was in a sense the hardest problem in NP in that every problem in NP could be reduced in deterministic polynomial time to the SAT problem. Problems in NP with this property are called NP-complete. It turned out that many interesting problems were NP-complete [23] and so the study of the P vs. NP began in earnest. Stockmeyer [47] in analogy with the situation

The polynomial hierarchy

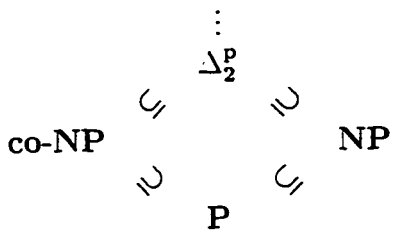

Figure I.A.1

with recursive and r.e. sets defined a presumably infinite hierarchy called the polynomial time hierarchy based on the class NP. The polynomial time hierarchy is defined as follows: at the bottom of the polynomial time hierarchy we have the class $P = \Delta_1^p$ of deterministic polynomial time computable predicates. At the next level up, we have the classes $\Sigma_1^p = NP$ and $\Pi_1^p = co\text{-}NP$. Here $co\text{-}NP$ sets are complements of NP sets. Using oracles, we then extend these classes of predicates to a presumably infinite hierarchy of predicates. We write P^Ψ to denote predicates which can be computed in P with an oracle set in Ψ. We define NP^Ψ, and $(co\text{-}NP)^\Psi$ similarly. We define $\Delta_i^p := P^{\Sigma_{i-1}^p}$, $\Sigma_i^p := NP^{\Sigma_{i-1}^p}$, and $\Pi_i^p := co\text{-}\Sigma_i^p$. Whether or not this hierarchy is proper is one of the fundamental open problems in theoretical computer science. An answer to this question would not only have applications to the study of algorithms but also to the field of cryptography. An illustration of the inclusions in the polynomial time hierarchy is given in Figure I.A.1.

I.B Bounded arithmetic

Given the connection between Σ_n-sets and formulas of arithmetic, it was natural to try to find similar correspondences between the polynomial hierarchy and arithmetic. These correspondences do in fact exist as we will see below where we introduce the three classical theories of bounded arithmetic and discuss their

properties.

The three classical bounded arithmetic theories R^i_2, S^i_2, and T^i_2 are formulated over the language L_2 which contains the non-logical symbols: 0, S, $+$, $\cdot$, $\leq$, $\dot{-}$, $\lfloor \frac{1}{2}x \rfloor$, $|x|$, $MSP(x,i)$ and $\#$. (Usually MSP and $\dot{-}$ are not included in the language of S^i_2 and T^i_2, since when $i \geq 1$ they can be defined in these theories given the axioms for the other symbols and using the induction axioms available in these theories.) The symbols 0, $S(x) = x+1$, $+$, $\cdot$, and $\leq$ have the usual meaning. The intended meaning of $x \dot{-} y$ is x minus y if this number is greater than zero and zero otherwise, the meaning of $\lfloor \frac{1}{2}x \rfloor$ is x divided by 2 rounded down, and the meaning of $|x|$ is $\lceil \log_2(x) + 1 \rceil$, that is, the length of x in binary notation. The symbol $MSP(x,i)$ stands 'for most significant part' is intended to mean $\lfloor x/2^i \rfloor$. In other words, the number obtained by cutting off the i last bits of x. Finally, $x\#y$ reads 'x smash y' and is intended to mean $2^{|x||y|}$.

The operation $\#$ is also written $\#_2$. In general, $x\#_k y = 2^{|x|\#_{k-1}|y|}$. The 2 in S^i_2 denotes the presence of $\#_2$ in the language: a 3 would indicate the presence of $\#_2$ and $\#_3$, etc. The language L_k is the language including $\#_j$ for $2 \leq j \leq k$. The reason for the new symbols in L_2 versus the language of Q is that because of their more restricted nature it is harder to bootstrap bounded arithmetic theories. In general the exponential function is not provably total in bounded arithmetic and so we need the function $\#$ as a minimum to be able to do sequence coding.

To define R^i_2, S^i_2, and T^i_2 we first need to define the theory $BASIC = BASIC_2$. This is the bounded arithmetic theory which consists of a finite set of quantifier free axioms for the non-logical symbols of L_2. We list these axioms, which are from Buss [13] and Takeuti [49], below:

1. $y \leq x \supset y \leq Sx$
2. $\neg(x = Sx)$
3. $0 \leq x$
4. $(x \leq y \wedge \neg x = y) \equiv Sx \leq y$

5. $\neg(x = 0) \supset \neg(2 \cdot x = 0)$

6. $y \leq x \vee x \leq y$

7. $(x \leq y \wedge y \leq x) \supset x = y$

8. $(x \leq y \wedge y \leq z) \supset x \leq z$

9. $|0| = 0$

10. $\neg(x = 0) \supset |2 \cdot x| = S(|x|) \wedge |S(2 \cdot x)| = S(|x|)$

11. $|1| = 1$

12. $x \leq y \supset |x| \leq |y|$

13. $|x\#y| = S(|x| \cdot |y|)$

14. $0\#y = 1$

15. $\neg(x = 0) \supset 1\#(2 \cdot x) = 2(1\#x) \wedge 1\#(S(2 \cdot x)) = 2(1\#x)$

16. $x\#y = y\#x$

17. $|x| = |y| \supset x\#z = y\#z$

18. $|x| = |u| + |v| \supset x\#y = (u\#y) \cdot (v\#y)$

19. $x \leq x + y$

20. $x + 0 = x$

21. $x + Sy = S(x + y)$

22. $(x + y) + z = x + (y + z)$

23. $x + y \leq x + z \equiv y \leq z$

24. $x \cdot 0 = 0$

25. $x \cdot (Sy) = x \cdot y + z$

26. $x \cdot y = y \cdot x$

27. $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$

28. $x \geq 1 \supset (x \cdot y \leq x \cdot z \equiv y \leq z)$

29. $\neg(x = 0) \supset |x| = S(|\lfloor \frac{1}{2}x \rfloor|)$

30. $x = \lfloor \frac{1}{2}x \rfloor \equiv (2 \cdot x = y \vee S(2 \cdot x) = y)$

31. $MSP(a, 0) = a$

32. $MSP(a, i + 1) = \lfloor \frac{1}{2}MSP(a, i) \rfloor$

33. $x \dot{-} y = z \equiv (y + z = x \vee (z = 0 \wedge x \leq y))$

We sometimes write Sx for $S(x)$. The 1 and 2 which appear in the above axioms are abbreviations for $S0$ and $S(S(0))$ respectively. We will frequently make use of such abbreviations for numerals. For $k \geq 2$, the theory $BASIC_k$ is $BASIC$ plus a finite set of additional axioms of the form $|x\#_j y| = |x|\#_{j-1}|y|$ where $2 < j \leq k$.

In R_2^i, S_2^i and T_2^i the syntax of first order logic is enlarged to include bounded quantifiers. These are quantifiers of the form $(\forall x \leq t)$ or $(\exists x \leq t)$ where t is a term not containing x. The intended meaning of $(\forall x \leq t)$ is $(\forall x)(x \leq t \supset \cdots$ and the intended meaning of $(\exists x \leq t)$ is $(\exists x)(x \leq t \wedge \cdots$. A formula is *bounded* if all its quantifiers are bounded. If a quantifier is of the form $(\forall x \leq |t|)$ or is of the form $(\exists x \leq |t|)$ then it is called sharply bounded. A formula is *sharply bounded* if all its quantifiers are sharply bounded. As usual, a formula is *open* if it contains no quantifiers.

Given these definitions we can define a hierarchy of bounded arithmetic formulas. $\Sigma_0^b = \Pi_0^b$ is the class of all sharply bounded formulas. Σ_i^b is the smallest class containing Π_{i-1}^b and closed under conjunction, disjunction, sharply bounded universal quantifiers, and bounded existential quantifiers. Π_i^b is the smallest class containing Σ_{i-1}^b and closed under conjunction, disjunction, sharply bounded existential quantifiers, and bounded universal quantifiers. This hierarchy corresponds

in a natural way to the polynomial time hierarchy. In the standard model Σ_i^b-formulas describe exactly predicates in Σ_i^p. Similarly, Π_i^b formulas correspond to Π_i^p-predicates. A proof of this correspondence can be found in Buss [13]. Thus, as with the r.e. sets case, we end up with a connection between arithmetic formulas and computation classes.

Another possible hierarchy of bounded arithmetic formulas is the prenex bounded arithmetic hierarchy. We define $\hat{\Sigma}_0^b$ to be the set of formulas of the form $(\exists x \leq |s|)\phi$ and $\hat{\Pi}_0^b$ to be the set of formulas of the form $(\forall x \leq |s|)\phi$ where ϕ is an open formula. The set $\hat{\Sigma}_i^b$ is the set of formulas of the form $(\exists x \leq t)\phi$ where ϕ is a $\hat{\Pi}_{i-1}^b$-formula. The set $\hat{\Pi}_i^b$ is the set of formulas of the form $(\forall x \leq t)\phi$ where ϕ is $\hat{\Sigma}_{i-1}^b$-formula. For $i \geq 1$, it is not hard to show that the sets described by $\hat{\Sigma}_i^b$-formulas and Σ_i^b-formulas are equivalent. In Chapter II, we will actually show various bounded arithmetic theories can prove this equivalence. Similarly, sets described by $\hat{\Pi}_i^b$-formulas and Π_i^b-formulas are equivalent. We call any formula which is in $\bigcup_i \hat{\Sigma}_i^b \cup \hat{\Pi}_i^b$ a *prenex formula.*

We define the classes of formulas $\Sigma_{i,k}^b$, $\Pi_{i,k}^b$, $\hat{\Sigma}_{i,k}^b$, and $\hat{\Pi}_{i,k}^b$ in the same way as above except formulated over the language of L_k. For $k > 2$, these classes of formulas correspond to computational complexity classes of predicates involving quasi-polynomial time computations.

Let $|x|_m$ denote m applications of the length of operator to x, i.e., $|x|_0$ is x, $|x|_1$ is $|x|$, and $|x|_{i+1}$ is $|(|x|_i)|$. Let Ψ be a set of formulas. We now give the different types of induction axioms which are used in defining the most common bounded arithmetic theories. The Ψ-PL^mIND axioms are the axioms PL^mIND_α for $\alpha \in \Psi$ and where the formula PL^mIND_α is

$$\alpha(0) \wedge (\forall x)(\alpha(\lfloor \frac{1}{2} x \rfloor) \supset \alpha(x)) \supset (\forall x)\alpha(|x|_m).$$

The Ψ-L^mIND axioms are the axioms L^mIND_α for $\alpha \in \Psi$ and where the formula L^mIND_α is

$$\alpha(0) \wedge (\forall x)(\alpha(x) \supset \alpha(S(x))) \supset (\forall x)\alpha(|x|_m).$$

We usually write Ψ-IND rather than Ψ-L^0IND. Similarly, we write Ψ-$LIND$ rather than Ψ-L^1IND, write Ψ-$PIND$ rather than Ψ-PL^0IND, write Ψ-$PLIND$ rather than Ψ-PL^1IND, and write Ψ-$LLIND$ rather than Ψ-L^2IND.

Originally, the theory T_2^i was defined as the theory with axioms $BASIC$ + Σ_i^b-IND, S_2^i was defined as the theory with axioms $BASIC$ + Σ_i^b-$PIND$, and the theory R_2^i was defined as the theory with axioms $BASIC$ + Σ_i^b-$PLIND$. Since we have MSP in our language (in the usual formulation of S_2^i and T_2^i we have to show it can be defined), one can use the methods of Buss [13] to show S_2^i can be axiomatized as $BASIC$ + Σ_i^b-$LIND$ and R_2^i can be axiomatized as $BASIC$ + Σ_i^b-$LLIND$. (With the more careful bootstrapping of Buss Ignjatović [11] one can show this for S_2^i without having MSP in the language.) This is how we will define these theories. Since the conclusions of the induction hypotheses become progressively weaker going from T_2^i to S_2^i to R_2^i, it follows that $R_2^i \subseteq S_2^i \subseteq T_2^i$.

Another useful scheme of axioms are replacement axioms. These axioms are useful for converting formulas into prenex formulas. We need the following definition before we can define these axioms. Given a term t in our language we define a monotonic term t^* called the *dominator for* t by induction on the complexity of t. If t is 0 then t^* is 0. If t is $S(f)$ then t^* is $S(f^*)$. If t is $f \circ g$ for $\circ$ a binary operation other than $\dot{-}$ or MSP then t^* is $f^* \circ g^*$. Lastly, if t is $f \dot{-} g$ or $MSP(f,g)$ then t^* is f^*. It is easy to see $BASIC$ proves $t \leq t^*$. The Ψ-$REPL^m$ axioms are the axioms

$$(\forall x \leq |s|_m)(\exists y \leq t)\alpha(x,y) \Leftrightarrow$$
$$(\exists w \leq 2 \cdot (t^* \# s))(\forall x \leq |s|_m)\alpha(x, \dot{\beta}(x, |t^*|, t, w)))$$

where α is a formula in Ψ. Here $\dot{\beta}(x, |t^*|, t, w)$ is a term in our language which returns the value $\hat{\beta}(x, |t^*|, w)$ if this is less than t and returns the value t otherwise. The function $\hat{\beta}(x, |t^*|, w)$ is $MSP(LSP(w, Sx \cdot |t^*|), x \cdot |t^*|)$ where the function $LSP(w,x)$ is $w \dot{-} MSP(w,x) \cdot 2^{\min(|w|,x)}$. (We will argue that LSP, min, etc. can be defined in our theories later.) We will usually write Ψ-$REPL$ for Ψ-$REPL^1$.

Let Ψ be a set of formulas. A theory T can Ψ-define a function $f(x)$, if there is a Ψ-formula $A_f(x,y)$ such that $T \vdash \forall x \exists! y A_f(x,y)$ and $\mathbb{N} \models A_f(x, f(x))$. We will mainly be interested in the Σ^b_i-definable functions of a theory or the $\hat{\Sigma}^b_i$-definable functions of a theory. A predicate is said to Δ^b_i with respect to a theory T if it is provably equivalent in T to both a Σ^b_i-formula and a Π^b_i-formula. We say a predicate is $\hat{\Delta}^b_i$ with respect to a theory T if it is provably equivalent to both a $\hat{\Sigma}^b_i$-formula and a $\hat{\Pi}^b_i$-formula. (By adding a trivial universal quantifier to the outside of a $\hat{\Sigma}^b_i$-formula one can show that a given $\hat{\Sigma}^b_i$-formula is logically equivalent to a $\hat{\Pi}^b_{i+1}$-formula, and by a trivial sharply bounded formula in front of the matrix of a $\hat{\Sigma}^b_i$-formula one show the same $\hat{\Sigma}^b_i$-formula is equivalent to a $\hat{\Sigma}^b_{i+1}$-formula. Hence, any $\hat{\Sigma}^b_i$-formula is $\hat{\Delta}^b_{i+1}$ with respect to any theory. Similarly, any $\hat{\Pi}^b_i$-formula is $\hat{\Delta}^b_{i+1}$ with respect to any theory.)

We now discuss what is known about the definable functions of various bounded arithmetic theories. This and the discussion below will hopefully give some indication of why it might be useful to study bounded arithmetic theories to better understand various computational complexity classes. Buss [13] showed that for $i \geq 1$ the Σ^b_i-definable functions of S^i_2 are precisely the $\square^p_i$-functions where $\square^p_1$ is the set of the functions computable in deterministic polynomial time and for i greater than one, $\square^p_i$ is the set of the functions computable in deterministic polynomial time using a Σ^p_{i-1}-oracle. In [14] he showed the Σ^b_{i-1}-definable functions of T^i_2 are the $\square^p_{i+1}$-functions. Allen [2] and Clote and Takeuti [19] show that the Σ^b_1-definable functions of R^1_2 are the functions in logspace-uniform FNC. FNC is the set of functions which are computable by a polylogarithmic depth and polynomial size families of Boolean circuits. Logspace-uniform FNC means the circuit computing a particular FNC function for inputs of length n can be computed in logspace. A multifunction is a total relation. Krajíček [33] shows that the Σ^b_{i-1}-definable multifunctions of S^i_2 are the multifunctions computable by machines in $FP^{\Sigma^p_i}(wit, \log)$. That is, those multifunctions which can be computed by Turing machine which run in polynomial time with only logarithmically many queries to a

Σ_i^p-oracle such that if the oracle answers 'Yes' to a query it also supplies a poly-size witness string.

Remark I.B.1 We can generalize the notion of the class $FP^{\Sigma_i^p}(wit.\log)$ to the notion $FP^{\Sigma_i^p}(wit.s)$ where we restrict the number of queries on inputs of length n to be bounded by $O(s(n))$ for some fixed function s. Classes of this form turn out to be useful in generalizing Krajíček's result to other theories as we will show later.

Given the above characterization of the Σ_i^b-definable functions of bounded arithmetic it was hoped that various techniques that had been useful in answering questions about Peano arithmetic would be useful in answering questions about bounded arithmetic and in turn questions about the polynomial time hierarchy. In particular, Gödel's Incompleteness Theorem had been used to separate $I\Sigma_n$ from $I\Sigma_{n+1}$ and it was hoped that it could be used to separate S_2^i from S_2^{i+1}. Buss [13] showed S_2^1 could sufficiently arithmetize syntax to prove a version of Gödel's result. However, he was unable to use his result to separate S_2^i from S_2^{i+1}. Since Buss [13] there has been a good deal of research on what consistency notions are provable in what theories of bounded arithmetic, but so far without success in showing S_2^i is different from S_2^{i+1}. Some of these consistency notions have been formulated in terms of the consistency of various propositional proof systems. This and the connection between propositional proof systems and the NP=$co-NP$? question has led to a burgeoning field of research into trying to prove lower bound results for stronger and stronger propositional proof systems.

Another area of active research is in showing independence results of the P=NP problem from some significant fragment of arithmetic. A first step in this direction was given by Razborov and Rudich [43] which showed that assuming the existence of pseudo-random number generators there is no "natural" proof of $P \neq NP$. A "natural proof" was a combinatorial property satisfying certain weak conditions. They argued in their paper that all currently known methods of proving

lower bounds were "natural". They then showed if there was a "natural" property then a pseudo-random number generator could be converted into a pseudo-random function generator which the "natural" property could distinguish as not pseudo-random. Razborov [42] used this result to show the theory $S_2^2(\alpha)$ cannot prove $P \neq NP$ assuming there are pseudo-random number generators. Here α is a 1-ary predicate symbol with no defining equations. His original technique used the characterization of the Σ_1^b-definable multifunctions of T_2^1 in terms of projections of PLS problems. He suggested his argument in his paper could be made using interpolations and later simplifications use this method.

There are several reasons why a refined analysis of what is definable in a bounded arithmetic theory is important. Buss [14] showed that the theory S_2^{i+1} is Σ_{i+1}^b-conservative over T_2^i. Also Krajíček, Pudlak, and Takeuti [35] have shown if $T_2^i = S_2^{i+1}$ then the polynomial hierarchy collapses. Thus, it is important as far as computational complexity is concerned to know the precise relationship between these two theories. Another benefit of a refined analysis of definability in bounded arithmetic is that it would potentially help in strengthening the $S_2^2(\alpha)$ independence result to stronger fragments of arithmetic or would help show independence results for separations of other complexity classes. It is this author's personal conjecture that the above independence results cannot be extended to the theories $T_2^2(\alpha)$ since the construction used to make a pseudo-random function generator from a pseudo-random number generator can essentially be carried out in $T_2^2(\alpha)$ [40].

It is especially interesting to carry out an analysis of definability for very weak systems of arithmetic. This is because understanding why things break down or why they continue to work in weak theories can often shed light on the stronger theories such as S_2^i and T_2^i. To refine the current analyses of definability, in this thesis we consider the $\hat{\Sigma}_i^b$-definable functions of bounded arithmetic theories. It is not hard to see that if a theory can prove Σ_i^b-$REPL$ and has some kind of pairing function, that the notion of $\hat{\Sigma}_i^b$-definability and Σ_i^b-definability coincide. Similarly,

in such a theory the notions of $\hat{\Delta}_i^b$ and Δ_i^b will be equivalent. It is known, for instance, that T_2^i, S_2^i, and R_2^i can prove Σ_i^b-$REPL$, so their $\hat{\Sigma}_i^b$ and Σ_i^b-definable functions will be the same. On the other hand, it is not known if any of these theories proves Σ_{i+1}^b-$REPL$, so in this case the notions of $\hat{\Sigma}_{i+1}^b$-definability and Σ_{i+1}^b-definability are potentially different.

Another issue we consider is what happens when we axiomatize the theories R_2^i, S_2^i, and T_2^i with induction only for $\hat{\Sigma}_i^b$-formulas rather than induction for Σ_i^b-formulas. We call these theories with $\hat{\Sigma}_i^b$-induction $\hat{R}_2^i$, $\hat{S}_2^i$ and $\hat{T}_2^i$. In general, we call these kind of theories *prenex theories*. The advantage of prenex theories is the following. Suppose one has a sequent calculus proof of a prenex formula in one of the theories $\hat{R}_2^i$, $\hat{S}_2^i$ or $\hat{T}_2^i$ (where rather than using induction axioms one uses induction rules of inference). Then by cut-elimination we can get a free-cut free proof of these formulas in which all of the formulas in the proof are prenex formulas. If we applied cut-elimination to a proof of the same formula in Σ_i^b-L^mIND based theories we could not guarantee that every formula in the resulting proof would be a prenex formula. In carrying out the witnessing argument of Buss [13], both the argument itself and the witness predicates become simpler in prenex theories because of this restriction on the formulas in the proof. Standard results known about R_2^i, S_2^i, and T_2^i also seem to generalize in the prenex setting to much weaker theories of arithmetic; whereas, they do not seem to generalize in the non-prenex setting. In fact, because of the prenex restriction we are even able to strengthen many of the standard results.

I.C Outline of thesis and results

We now briefly outline the format of the rest of this thesis. It turns out that the theories $\hat{S}_2^i$ and $\hat{T}_2^i$ are equivalent to S_2^i and T_2^i respectively, yet we conjecture $\hat{R}_2^i$ is not equivalent to R_2^i. In Chapter II, we formally introduce our prenex theories and prove these facts. To do this we consider a very weak theory

LIOpen which consists of *BASIC+Open-LIND*. We isolate several key theorems needed to prove the existence of pairing functions and replacement axioms in $\hat{R}^i_2$, $\hat{S}^i_2$, and $\hat{T}^i_2$. Adding this finite list of theorems which can be written as open formulas to $BASIC_k$ we define a new theory $EBASIC_k$. We call the $k = 2$ case *EBASIC*. We then define the theories $\hat{T}^{i,m}_k$ as $EBASIC_k$+$\hat{\Sigma}^b_i$-$L^m IND$ and briefly consider their properties. We define various classes of terms $Term^{m,j}_k$. Let $id(a) = a$. The class $Term^{m,0}_k$ consists of 1-ary terms of the form $|id|_m$. The class $Term^{m,j}_k$ consists of 1-ary terms of the form $2^{\min(p(s),|t|)}$ where p is a polynomial, s is in $Term^{m,j-1}_k$, and t is an L_k-term. We finally define the theories $\hat{T}^{i,m,j}_k$ to consist of $EBASIC_k$ plus $\hat{\Sigma}^b_{i-j}$ induction up to any term in $Term^{m,j}_k$. These theories turn out to be useful in characterizing the $\hat{\Sigma}^b_{i-j}$-definable consequences of the theories $\hat{T}^{i,m}_k$. However, the number of indices in these theories is very unwieldy. We, therefore, consider more abstract theories $\hat{T}^{i,\tau}_k$. Here τ is a collection of 1-ary terms. The theory $\hat{T}^{i,\tau}_k$ consists of $EBASIC_k$ together with $\hat{\Sigma}^b_i$-induction up to terms in τ. To finish the chapter, we briefly discuss the properties of the theories $\hat{T}^{i,\tau}_k$.

In Chapter III, we define multifunction algebras $B_{i,k}$ and $B^{|\tau|}_{i,k}$. We show *EBASIC* can $\hat{\Sigma}^b_i$-define the multifunctions in $B_{i,2}$ and $\hat{T}^{i,|\tau|}_2$ can $\hat{\Sigma}^b_i$-define the multifunctions in $B^{|\tau|}_{i,2}$. We also define the classes LS^{Ψ}_{τ} of multifunctions computed as optima of (Ψ, τ)-local search problems. We show $\hat{T}^{i,\tau}_2$ can prove any (Ψ, τ)-local search problem in $\hat{T}^{i,\tau}_2$ has a local optima. Thus, $\hat{T}^{i,\tau}_2$ can define these multifunctions.

In Chapter IV we discuss the sequent calculus and give $\hat{T}^{i,\tau}_2$ and $\hat{C}^{i,|\tau|}_2$ sequent calculus formulations. We then discuss the cut-elimination theorem and Parikh's theorem. Both of these results are used in Chapter V to prove converses to out definability results of Chapter III

In Chapter V we prove our algebras and local search classes precisely characterize the $\hat{\Sigma}^b_i$-definable multifunctions of *EBASIC*. $\hat{T}^{i,|\tau|}_2$ and $\hat{T}^{i,\tau}_2$. To do this we use a witnessing argument in the style of Buss [13]. We conclude this chapter with a discussion on theories based on prefix type inductions.

In Chapter VI. we show for $i \geq 1$ that the $\hat{\Sigma}^b_{i-1}$-definable multifunctions of $\hat{T}^{i,\tau}_2$ are precisely the functions in $FP^{\Sigma^p_i}(wit.|\tau|)$. We show that $\hat{T}^{i,\tau^\#}_2 \preceq_{\hat{\Sigma}^b_{i-1}} \hat{T}^{i+1,|\tau^\#|}_2$. We then give applications of these results to the theories $EBASIC$. $\hat{R}^i_2$. $\hat{T}^{i,m}_2$. and $\hat{T}^{i,m,j}_2$. Our conservation result will allow us to show $\hat{T}^{i,m}_2$ is $\hat{\Sigma}^b_{i-j-1}$-conservative over $\hat{T}^{i,m,j}_2$ and so we can use our characterization of the $\hat{\Sigma}^b_{i-j-1}$-definable multifunctions of the latter theory to characterize those of the former theory. In this chapter we also show $\hat{\Sigma}^b_{i+1}$-definable multifunctions of $EBASIC$ is the class $FP^{\Sigma^p_i}(wit.1)$. The results of Chapter III, Chapter V. and Chapter VI generalize easily to the theories $\hat{T}^{i,\tau}_k$; however, we concentrate on the $\hat{T}^{i,\tau}_2$ case as it is the most significant from the computational complexity standpoint.

In Chapter VII we discuss various applications of the witnessing argument. We characterize the $\hat{\Sigma}^b_{i+k}$-definable multifunctions of $\hat{T}^{i,\tau}_2$ for $k \geq 1$ as the class $FP^{\Sigma^p_{i+k-1}}(wit.1)$. We show $\hat{T}^{i+1,|\tau^\#|}_k$ is conservative over $\hat{T}^{i,\tau^\#}_k$ with respect to Boolean combinations of $\hat{\Sigma}^b_{i+1}$-formulas. In symbols. this is

$$\hat{T}^{i,\tau^\#}_k \preceq_{B(\hat{\Sigma}^b_{i+1})} \hat{T}^{i+1,|\tau^\#|}_k.$$

This implies $T^i_2 \preceq_{B(\hat{\Sigma}^b_{i+1})} S^{i+1}_2$. In general. this result implies

$$\hat{T}^{i,m}_{m+2} \preceq_{B(\hat{\Sigma}^b_{i+1})} \hat{T}^{i+1,m+1}_{m+2}$$

We also show in Chapter VII that $\hat{T}^{i,|\tau|}_2$ can prove $\hat{\Delta}^b_{i-1}$-$IND^{|\tau|}$ axioms and $\hat{T}^{i,\tau^\#}_2$ can prove $\hat{\Delta}^b_{i+1}$-$IND^{\tau^\#}$ axioms.

In Chapter VIII develop the properties of prenex theories $\hat{C}^{i,|\tau|}_2$ defined as

$$EBASIC\text{+}Open\text{-}IND^{|\tau|}\text{+}\hat{\Sigma}^b_i\text{-}REPL^{|\tau|}.$$

We show these theories are $B(\hat{\Sigma}^b_{i+1})$-conservative over $\hat{T}^{i,|\tau|}_2$. In this chapter we also show for $i \geq 1$ that R^{i+1}_2 is $B(\hat{\Sigma}^b_{i+1})$-conservative over $\hat{R}^{i+1}_2$. In general. we show for $i \geq 1$ that $\hat{T}^{i+1,||\tau||}_2\text{+}\hat{\Pi}^b_i$-$REPL^{|\tau|}$ is $B(\hat{\Sigma}^b_{i+1})$-conservative over $\hat{T}^{i+1,||\tau||}_2$.

In Chapter IX we investigate the functions (as opposed to multifunctions) definable in the theories $\hat{T}^{i,|\tau|}_2$ and $\hat{T}^{i,\tau}_2$. We show $\hat{T}^{i,|\tau|}_2$ and $\hat{T}^{i,\tau}_2$ proves multifunctions defined using $\hat{\Delta}^b_{i+1}$-$COMP^{|\tau|}$ axioms are single-valued. We also show as a

converse that for $j \leq i+1$ every τ-bounded $\hat{\Sigma}^b_{i+1}$-definable function in $\hat{T}^{i,\tau}_2$ and $\hat{T}^{i,|\tau|}_2$ can be defined using a $\hat{\Delta}^b_j$-$COMP^{|\tau|}$ axiom. This enables us to give a characterization for $j \leq i+1$ the $\hat{\Sigma}^b_j$-definable τ-bounded functions of $\hat{T}^{i,|\tau|}_2$ and $\hat{T}^{i,\tau}_2$ in terms of parallel computations of $\hat{\Delta}^b_j$-predicates. We suggest some characterizations of these classes. In particular, we show the $\hat{\Sigma}^b_i$-definable functions of $\hat{R}^i_2$ are precisely the function in $FNC^{\Sigma^p_i}$. Our results are mainly for the case where $i > 0$. In the last section, however, we show some results about the $\hat{\Sigma}^b_{1,|\tau|}$-definable functions of $\bar{C}^{0,|\tau|}_2$, a subtheory of $\hat{C}^{0,|\tau|}_2$. Here $\hat{\Sigma}^b_{1,|\tau|}$ is the subset of $\hat{\Sigma}^b_1$ where the innermost universal quantifier is bounded by $|\tau|$-terms. In the $\tau = \{id\}$ case, it turn out one gets the class FTC^0 of functions computable by constant depth threshold circuits. In general, one gets the class FTC^0_τ which we define. The predicate class in FTC^0, TC^0 is of interest to computer science both because of its connection with neural nets and the fact that it is one of the weakest classes not known to be different from NP. We give a nonconditional separation results between $FTC^0_{|\tau|}$ and $FTC^0_{\{id\}}$ and also between $\bar{C}^{0,|\tau|}_2$ and $\hat{C}^{0,\{id\}}_2$.

Chapter X shows some collapse and oracle separation results for the theories $\hat{T}^{i,|\tau|}_2$ and $\hat{C}^{i,|\tau|}_2$. We first show if $T^i_2 = \hat{T}^{i+1,|\tau|}_2$ or if $T^i_2 = \hat{C}^{i+1,|\tau|}_2$ or if $\hat{C}^{i,|\tau|}_2 = \hat{T}^{i+1,|\tau'|}_2$ where τ contains at least one unbounded iterm then $\Sigma^p_{i+3} = \Pi^p_{i+3}$. The last equality implying a collapse is interesting since it gives some evidence that TC^0 is not equal to NC or P. Then in the rest of the chapter we construct an oracle X which separates $P^{\Sigma^p_i}(\{||\dot{\ell}||\})$ from $P^{\Sigma^p_i}(\{|\ell|\})$ where ℓ is a nondecreasing, unbounded iterm. This oracle is then used to show $\hat{T}^{i,\{||\dot{\ell}||\}}_2(\alpha) \subsetneq \hat{T}^{i,\{\ell\}}_2(\alpha)$. By $\hat{T}^{i,\{\ell\}}_2(\alpha)$ we mean the theory obtained by expanding the language of $\hat{T}^{i,\{\ell\}}_2$ by a new unary predicate symbol α with no defining relations. Many other separations are also derived from this result.

Finally, we include some diagrams and tables of the principal results of this paper in an appendix at the end.

Bounded arithmetic theories with generalized induction schemes have been considered before in Razborov [41]. He considers second order theories with

various bounds on induction and discusses their connection to the formalizability of various arguments of circuit complexity. His results on generalized inductions in Bounded Arithmetic are thus somewhat different from ours.

Chapter II

Prenex theories

In this chapter we introduce a variety of prenex theories and develop some of their properties. We begin by defining the prenex versions of the theories T_2^i, S_2^i, and R_2^i. We also define a weak theory $LIOpen$ which we show is contained in these theories. We will show $LIOpen$ can do a simple form of pairing and can prove some facts about sequence coding. Isolating these facts will allow us to define a strengthened version of $BASIC$ we call $EBASIC$ and to define the prenex theories $\hat{T}_2^{i,m}$. For $m = 0, 1, 2$ the theories $\hat{T}_2^{i,m}$ correspond to prenex versions of T_2^i, S_2^i, and R_2^i. We also consider theories $\hat{T}_2^{i,\tau}$ where τ is a collection of 1-ary terms. The theories $\hat{T}_2^{i,\tau}$ consist of $EBASIC$ and $\hat{\Sigma}_i^b$-induction up to terms in τ.

II.A Preliminaries

We begin with the following definition.

Definition II.A.1 ($i \geq 0$)

1. $\hat{T}_2^i$ *is the theory* $BASIC + \hat{\Sigma}_i^b$-IND.
2. $\hat{S}_2^i$ *is the theory* $BASIC + \hat{\Sigma}_i^b$-$LIND$.
3. $\hat{R}_2^i$ *is the theory* $BASIC + \hat{\Sigma}_i^b$-$LLIND$

We define L^mIOpen to be the theory

$$BASIC + Open\text{-}L^mIND.$$

That is, L^mIND_ϕ for ϕ an open formula. We write $IOpen$ for L^0IOpen and we write $LIOpen$ for L^1IOpen.

Remark II.A.2 The theory $IOpen$ is usually formulated over the language consisting of only '0', 'S', '+', and '$\cdot$'. Our version, since it has #, MSP, $\dot{-}$, and $\lfloor x \rfloor$, is a fair bit stronger. We are mainly going to use the theory $LIOpen$ in this thesis so little conflict should arise between these two definitions of $IOpen$.

Theorem II.A.3 $(i \geq 0)$ $\hat{R}^i_2 \subseteq \hat{S}^i_2 \subseteq \hat{T}^i_2$.

Proof: Let $A(x)$ be a $\hat{\Sigma}^b_i$-formula. Then IND_A implies $LIND_A$ and $LIND_A$ implies $LLIND_A$, since $(\forall x)A(x)$ implies $(\forall x)A(\lfloor x \rfloor)$ implies $(\forall x)A(\lfloor \lfloor x \rfloor \rfloor)$. □

Our immediate goal is to determine the classes of formulas provably equivalent to $\hat{\Sigma}^b_i$-formulas in the theories $\hat{R}^i_2$, $\hat{S}^i_2$, and $\hat{T}^i_2$. This is important to determine since our prenex theories will be able to prove induction for these types of formulas. To do this we first show our prenex theories can *open*-define some simple functions.

II.B Some frequently used L_2-terms

From the axioms of $BASIC$ one can *open*-define the following functions, their definitions are similar to those in [19], but have been modified so that they

are all L_2-terms:

$$
\begin{aligned}
2^{|y|} = 2^{|y|^1} &:= 1\#y \\
2^{|y|^n} = 2^{1\cdot|y|^n} &:= 2^{|y|^{n-1}}\#y \\
2^{k\cdot|y|^n} &:= 2^{|y|^n} \cdot 2^{(k-1)\cdot|y|^n} \\
\mathrm{mod2}(a) &:= a \dot{-} 2\cdot\lfloor\frac{1}{2}a\rfloor \\
cond(x,y,z) &:= (1\dot{-}x)\cdot y + (1\dot{-}(1\dot{-}x))\cdot z \\
K_{=}(x,y) &:= 1\dot{-}((y\dot{-}x)+(x\dot{-}y)) \\
K_{\leq}(x,y) &:= 1\dot{-}(y\dot{-}x) \\
K_{\wedge}(x,y) &:= x\cdot y \\
K_{\neg}(x) &:= 1\dot{-}x. \\
\max(x,y) &:= cond(K_{\leq}(x,y),y,x) \\
\min(x,y) &:= cond(K_{\leq}(x,y),x,y) \\
2^{\min(|y|,x)} &:= MSP(2^{|y|},|y|\dot{-}x) \\
LSP(x,i) &:= x\dot{-}MSP(x,i)\cdot 2^{\min(|x|,i)} \\
\hat{\beta}(x,|t|,w) &:= MSP(LSP(w,Sx\cdot|t|),x\cdot|t|) \\
Bit(i,x) &:= \hat{\beta}(i,1,x) \\
\dot{\beta}(x,|t|,s,w) &:= cond(K_{\leq}(\hat{\beta}(x,|t|,w),s),\hat{\beta}(x,|t|,w),s).
\end{aligned}
$$

The k and the n which appear in $2^{k\cdot|y|^n}$ are fixed integers. Taking products of terms of the form $2^{k\cdot|s|^n}$ we can construct terms representing $2^{p(|s|)}$ where p is any polynomial. We will often use the predicate $x < y$ as an abbreviation for $Sx \leq y$. Since the above definitions are all L_2-terms we can use them freely in an L_2-formulas without increasing its quantifier complexity. It is a theorem of Buss [13] that once we can Σ^b_1-define a function f in a bounded arithmetic theory we can add the function symbol to the theory without changing the Σ^b_i or Π^b_i -consequences of the theory $i \geq 1$. A similar result also holds for adding

Δ_1^b-predicate symbols [13]. We will not need this more general result, however.

Remark II.B.1 For the purposes of this thesis, we view $A \supset B$ as an abbreviation for $\neg A \vee B$. In transforming formulas into prenex ones we also will make use of the fact that $\neg\forall x\neg$ and $\exists x$ are logically equivalent. This will allow us to push negations inward into a formula.

II.C Pairing in *LIOpen*

The next step in establishing what formulas our prenex theories can prove are equivalent to $\hat{\Sigma}_i^b$-formulas is to show that theories as weak as *LIOpen* have a pairing function. For this to be useful for all of the theories $\hat{R}_2^i$ we first show that $\hat{R}_2^0 \supseteq LIOpen$. This fact follows from the next two theorems.

Theorem II.C.1 *Let Ψ be a class of formulas over our language closed under term substitution. Let $\neg\Psi$ denote those formulas which are negations of formulas in Ψ.*

Then $BASIC$+Ψ-L^mIND is equivalent to $BASIC$+$\neg\Psi$-L^mIND.

Proof: Both directions of this proof are the same so we only prove the forward implication. Let $A \in \neg\Psi$. We want to show $BASIC + \Psi\text{-}L^mIND$ can prove

$$A(0) \wedge (\forall x)(A(x) \supset A(Sx)) \supset (\forall x)A(|x|_m). \tag{II.1}$$

Let $B(x, y)$ be the formula $\neg A(y \dot{-} x)$. This formula is logically equivalent to a formula in Ψ, hence, $BASIC + \Psi\text{-}L^mIND$ proves

$$B(0, |y|_m) \wedge (\forall x)(B(x, |y|_m) \supset B(Sx, |y|_m)) \supset B(|y|_m, |y|_m).$$

So $BASIC + \Psi\text{-}L^mIND$ proves

$$\neg A(|y|_m) \wedge (\forall x)(\neg A(|y|_m \dot{-} x) \supset \neg A(|y|_m \dot{-} Sx)) \supset \neg A(0)$$

from which (II.1) follows. □

Theorem II.C.2 *LIOpen* $\subseteq \hat{R}^0_2$

Proof: Let $A(x)$ be an open formula. Consider the following formula $B(b)$

$$(\forall x \leq |c|)(A(x) \supset A(\min(x + 2^b, |c|))).$$

To keep the notation simple we are writing 2^b rather than $2^{\min(||c||,b)}$. This formula is a $\hat{\Pi}^b_0$-formula, i.e., logically equivalent to a $\neg\hat{\Sigma}^b_0$-formula, so by Theorem II.C.1 the theory $\hat{R}^0_2$ can prove $LLIND_B$. The theory $\hat{R}^0_2$ can also prove $(\forall x)(A(x) \supset A(Sx))$ implies $B(0)$. Further, $\hat{R}^0_2$ proves $B(b) \supset B(Sb)$ and $B(||c||) \supset (A(0) \supset A(|c|))$. So $\hat{R}^0_2$ proves

$$(\forall x)(A(x) \supset A(Sx)) \supset (A(0) \supset A(|c|)).$$

which is equivalent to $LIND_A$. □

We now proceed to show *LIOpen* has a pairing operation.

Lemma II.C.3 *The theory LIOpen proves*

$$b < 2^{|d|} \supset MSP(a \cdot 2^{|d|} + b, |d|) = a.$$

Proof: Recall the axioms for MSP in $BASIC$ are

$$\begin{aligned} MSP(a, 0) &= a \quad \text{and} \\ MSP(a, i+1) &= \lfloor \tfrac{1}{2} MSP(a, i) \rfloor. \end{aligned}$$

To prove the lemma it suffices to prove the following three statements are provable in *LIOpen*.

$$a \leq b \supset MSP(a, |d|) \leq MSP(b, |d|). \tag{II.2}$$

$$MSP(a \cdot 2^{|d|} + 2^{|d|} \dot{-} 1, |d|) = a \tag{II.3}$$

$$MSP(a \cdot 2^{|d|}, |d|) = a. \tag{II.4}$$

To prove (II.2) we first consider the formula

$$a \leq b \supset MSP(a, j) \leq MSP(b, j).$$

Call this formula $A(j)$. The first axiom for MSP implies $A(0)$. The implication $A(j) \supset A(j+1)$ follows from the second axiom. Thus, $LIOpen$ proves $A(|d|)$ which in turn implies

$$a \leq b \supset MSP(a, |d|) \leq MSP(b, |d|). \tag{II.5}$$

For (II.3), let $B(j)$ be the formula

$$MSP(a \cdot 2^{|d|} + 2^{|d|} \dot{-} 1, j) = a \cdot 2^{|d| \dot{-} j} + 2^{|d| \dot{-} j} \dot{-} 1.$$

The formula $B(0)$ follows from the first axiom for MSP. The implication $B(j) \supset B(Sj)$ follows from the second axiom for MSP as well as the axiom for $\lfloor \frac{1}{2} x \rfloor$. Hence, by $LIND_B$, the theory $LIOpen$ proves $B(|d|)$ which implies

$$MSP(a \cdot 2^{|d|} + 2^{|d|} \dot{-} 1, |d|) = a \tag{II.6}$$

Finally for (II.4), let $C(j)$ be the formula

$$MSP(a \cdot 2^{|d|}, j) = a \cdot 2^{|d| \dot{-} j}.$$

Arguing in the same way as with $B(j)$, the theory $LIOpen$ proves $C(|d|)$ which in turn implies

$$MSP(a \cdot 2^{|d|}, |d|) = a. \tag{II.7}$$

Combining the facts (II.2), (II.3), (II.4) proves the Lemma, since

$$a \cdot 2^{|d|} \leq a \cdot 2^{|d|} + b$$

and since

$$a \cdot 2^{|d|} + b \leq a \cdot 2^{|d|} + 2^{|d|} \dot{-} 1$$

provided $b < 2^{|d|}$. □

One can generalize the above argument to show:

Corollary II.C.4 *The theory LIOpen proves*

$$b < 2^{\min(k\cdot|d|,|d|^2)} \supset MSP(a \cdot 2^{\min(k\cdot|d|,|d|^2)} + b, \min(k \cdot |d|, |d|^2)) = a.$$

Lemma II.C.3 allows us to prove the next theorem which shows *LIOpen* does indeed have some form of pairing.

Theorem II.C.5 *The theory LIOpen proves*

$$(b < 2^{|d|} \wedge a < 2^{|d|}) \supset (\hat{\beta}(0, |d|, a \cdot 2^{|d|} + b) = b \wedge \hat{\beta}(1, |d|, a \cdot 2^{|d|} + b) = a).$$

Proof: Recall $\hat{\beta}(x, |d|, w)$ is the function $MSP(LSP(w, Sx\cdot|d|), x\cdot|d|)$. If $a = 0$ the theorem is not hard to show, so assume $a > 0$. From the axioms for MSP one can see that *LIOpen* proves $\hat{\beta}(0, |d|, a \cdot 2^{|d|} + b)$ is

$$LSP(a \cdot 2^{|d|} + b, |d|).$$

The definition of LSP gives us that $LSP(a \cdot 2^{|d|} + b, |d|)$ is

$$a \cdot 2^{|d|} + b \dot{-} MSP(a \cdot 2^{|d|} + b, |d|) \cdot 2^{\min(|a\cdot 2^{|d|}+b|,|d|)}$$

As $a > 0$, the theory *LIOpen* proves this is just

$$a \cdot 2^{|d|} + b \dot{-} MSP(a \cdot 2^{|d|} + b, |d|) \cdot 2^{|d|}.$$

By Lemma II.C.3 if $b < 2^{|d|}$ then *LIOpen* proves this is just b. Now consider $\hat{\beta}(1, |d|, a \cdot 2^{|d|} + b)$ by definition this function is

$$MSP(LSP(a \cdot 2^{|d|} + b, 2 \cdot |d|), |d|). \tag{II.8}$$

The function $LSP(a \cdot 2^{|d|} + b, 2 \cdot |d|)$ is equal to

$$a \cdot 2^{|d|} + b \dot{-} MSP(a \cdot 2^{|d|} + b, 2 \cdot |d|) \cdot 2^{2\cdot|d|}. \tag{II.9}$$

Since $a < 2^{|d|}$ and $b < 2^{|d|}$, we have

$$a \cdot 2^{|d|} + b \leq (2^{|d|} \dot{-} 1)2^{|d|} + 2^{|d|} \dot{-} 1 \leq 2^{2\cdot|d|} \dot{-} 1.$$

By a simple induction as in Lemma II.C.3, one can show $LIOpen$ proves

$$MSP(2^{2\cdot|d|} \dot{-} 1, 2 \cdot |d|) = 0.$$

Hence, $LIOpen$ proves

$$MSP(a \cdot 2^{|d|} + b, 2 \cdot |d|) = 0$$

Thus, equation (II.9) is equal to $a \cdot 2^{|d|} + b$. So $\dot{\beta}(1, |d|, a \cdot 2^{|d|} + b)$ which by definition is equation (II.8) is equal to a by Lemma II.C.3. □

It is not known to the author whether any of the theories $L^m IOpen$ where $m \geq 2$ can prove Theorem II.C.5 or whether any of these weaker theories has some other form of pairing. One could always add Theorem II.C.5 to these weaker theories to obtain a pairing function. In any case, the next lemma gives us our first method for converting formulas into prenex ones.

Lemma II.C.6 *Let $A(x)$ and $B(y)$ be formulas in our language such that the variable x does not appear in B and the variable y does not appear in A. Let $m = \max(s(a), t(a, s))$ where $s(a)$ and $t(a, b)$ are terms in our language. Then $LIOpen$ can prove:*

$$(\exists w \leq 2^{2\cdot|m|})A(\dot{\beta}(0, |m|, s, w), \dot{\beta}(1, |m|, t, w)) \qquad \text{(II.10)}$$
$$\Leftrightarrow (\exists x \leq s)(\exists y \leq t)A(x, y)$$

$$(\forall w \leq 2^{2\cdot|m|})A(\dot{\beta}(0, |m|, s, w), \dot{\beta}(1, |m|, t, w)) \qquad \text{(II.11)}$$
$$\Leftrightarrow (\forall x \leq s)(\forall y \leq t)A(x, y).$$

Proof: Each of these statements is proved in essentially the same way so we only prove the first one. We use equality axioms and logical rules to prove

$$\dot{\beta}(0,|m|,s,b\cdot 2^{|m|}+a)=a\wedge\dot{\beta}(1,|m|,t,b\cdot 2^{|m|}+a)=b)\supset$$
$$(A(\dot{\beta}(0,|m|,s,b\cdot 2^{|m|}+a),\dot{\beta}(1,|m|,t,b\cdot 2^{|m|}+a))\Leftrightarrow A(a,b)).$$

Using Theorem II.C.5, the theory *LIOpen* can prove

$$(a\leq s\wedge b\leq t\wedge A(a,b))\supset b\cdot 2^{|m|}+a\leq 2^{2\cdot|m|}\wedge$$
$$A(\dot{\beta}(0,|m|,s,b\cdot 2^{2\cdot|m|}+a),\dot{\beta}(1,|m|,t,b\cdot 2^{|m|}+a)).$$

Existentially quantifying first over the term $b\cdot 2^{2\cdot|m|}+a$ then over the variables a, and b, the theory *LIOpen* can derive

$$(\exists x\leq s)(\exists y\leq t)A(x,y)\supset$$
$$(\exists w\leq 2^{2\cdot|m|})A(\dot{\beta}(0,|m|,s,w),\dot{\beta}(1,|m|,t,w)).$$

For the other direction *LIOpen* can derive

$$c\leq 2^{2\cdot|m|}\wedge A(\dot{\beta}(0,|m|,s,c),\dot{\beta}(1,|m|,t,c))\supset$$
$$\dot{\beta}(0,|m|,s,c)\leq s\wedge\dot{\beta}(1,|m|,t,c)\leq t\wedge A(\dot{\beta}(0,|m|,s,c),\dot{\beta}(1,|m|,t,c)).$$

Existentially quantifying first over the terms $\dot{\beta}(1,|m|,t,c)$ and $\dot{\beta}(0,|m|,s,c)$ then over the variables c, we thus get

$$(\exists w\leq 2^{2\cdot|m|})A(\dot{\beta}(0,|m|,s,w),\dot{\beta}(1,|m|,t,w))$$
$$\supset(\exists x\leq s)(\exists y\leq t)A(x,y).$$

So *LIOpen* can prove formula (II.10). Similar methods shows (II.11). □

Remark II.C.7 Let A and B be formulas in our language. We recall some useful tautologies

$$(\forall y\leq t)(A(a)\wedge B(y))\Leftrightarrow A(a)\wedge(\forall y\leq t)B(y) \qquad \text{(II.12)}$$

$$(\exists y \leq t)(A(a) \wedge B(y)) \Leftrightarrow A(a) \wedge (\exists y \leq t)B(y) \tag{II.13}$$

$$(\forall y \leq t)(A(a) \vee B(y)) \Leftrightarrow A(a) \vee (\forall y \leq t)B(y) \tag{II.14}$$

$$(\exists y \leq t)(A(a) \vee B(y)) \Leftrightarrow A(a) \vee (\exists y \leq t)B(y). \tag{II.15}$$

We therefore have induction in $\hat{R}^i_2$, $\hat{S}^i_2$ and $\hat{T}^i_2$ for any formula we can prove equivalent to a $\hat{\Sigma}^b_i$-formula using Lemma II.C.6 and Remark II.C.7.

II.D Replacement axioms available in prenex theories

In this section we show the class of provably $\hat{\Sigma}^b_i$-formulas in these theories is closed under a form of sharply bounded quantification. To do this we first need the following technical lemma.

Lemma II.D.1 *The theory LIOpen proves*

$$Si \cdot |a| \leq k \supset \hat{\beta}(i, |a|, w) = \hat{\beta}(i, |a|, LSP(w, k))$$

Proof: This proof is somewhat painful so we omit most of the details. Assume $Si \cdot |a| \leq k$ and argue informally in *LIOpen*. We want to show

$$\hat{\beta}(i, |a|, w) = \hat{\beta}(i, |a|, LSP(w, k)).$$

By definition this is

$$MSP(LSP(w, Si \cdot |a|), i \cdot |a|) = MSP(LSP(LSP(w, k), Si \cdot |a|), i \cdot |a|).$$

So it suffices to show $LSP(w, Si \cdot |a|) = LSP(LSP(w, k), Si \cdot |a|)$. Using the definition of LSP it is not hard to show

$$LSP(LSP(w, Si \cdot |a|), Si \cdot |a|) \leq LSP(LSP(w, k), Si \cdot |a|) \leq LSP(w, Si \cdot |a|).$$

Then one argues $LSP(LSP(w, Si \cdot |a|), Si \cdot |a|) = LSP(w, Si \cdot |a|)$ since

$$LSP(LSP(w, Si \cdot |a|), Si \cdot |a|) =$$
$$LSP(w, Si \cdot |a|) \dot{-} MSP(LSP(w, Si \cdot |a|), Si \cdot |a|)$$

and one can show $MSP(LSP(w, Si \cdot |a|), Si \cdot |a|) = 0$. □

Theorem II.D.2 *($i \geq 1$) $\hat{S}^i_2$ proves $\hat{\Pi}^b_{i-1}$-$REPL$ and $\hat{R}^i_2$ proves $\hat{\Pi}^b_{i-1}$-$REPL^2$.*

Proof: Let A be a $\hat{\Pi}^b_{i-1}$-formula. Let X and Y be the formulas

$$X = (\forall x \leq |t|)(\exists y \leq s)A(x, y)$$
$$Y(u) = (\exists w \leq 2 \cdot (t \# s^*))(\forall x \leq |t|)(x \leq u \supset A(x, \dot{\beta}(x, |s^*|, s, w))).$$

We want to show $\hat{S}^i_2 \vdash X \Leftrightarrow Y(|t|)$. That $\hat{S}^i_2 \vdash Y(|t|) \supset X$ is obvious. We also have that

$$\hat{S}^i_2 \vdash X \supset Y(0)$$

and if $Su \leq t$ then $X \supset A(Su, y)$ for some $y \leq s$. If $Y(u)$ holds then there is some $w \leq 2 \cdot (t \# s^*)$ such that

$$(\forall x \leq |t|)(x \leq u \supset A(x, \dot{\beta}(x, |s^*|, s, w))).$$

Let $w' := y \cdot 2^{\min(Si \cdot |s^*|, |t| \cdot |s^*|)} + LSP(w, Si \cdot |s^*|)$. By Lemma II.C.4 and Lemma II.D.1 we have

$$(\forall x \leq |t|)(x \leq Su \supset A(x, \dot{\beta}(x, |s^*|, s, w'))).$$

Hence,

$$X \supset (u < |t| \wedge Y(u) \supset Y(Su)).$$

Since Y is a $\hat{\Sigma}^b_i$-formula, we have by Lemma II.C.6 $LIND_Y$:

$$Y(0) \wedge (\forall u < |t|)(Y(u) \supset Y(Su)) \supset (\forall u \leq |t|)Y(|t|).$$

Thus, it follows $\hat{S}^i_2 \vdash X \supset Y(|t|)$.

A similar proof shows $\hat{R}_2^i$ proves $\hat{\Pi}_{i-1}^b$-$REPL^2$. □

Remark II.D.3 It should be noted that having replacement for $\hat{\Pi}_{i-1}^b$-formulas implies replacement for both $\hat{\Pi}_{i-2}^b$ and $\hat{\Sigma}_{i-2}^b$-formulas, since we can do the same adding of dummy quantifiers that we did when we argued in Chapter I that every $\hat{\Sigma}_i^b$ and $\hat{\Pi}_i^b$-formula will be $\hat{\Delta}_{i+1}^b$ with respect to any theory. This kind of padding with quantifiers can also be used to show if a theory $\hat{\Sigma}_i^b$-defines a functions it also $\hat{\Sigma}_{i+k}^b$-defines that function.

The idea for Theorem II.D.2 was used in [13] to show the theory S_2^i has Σ_i^b-$REPL$. In the prenex case, it relied on us being able to prove Corollary II.C.4 and Lemma II.D.1.

Definition II.D.4 *The theory $EBASIC = EBASIC_2$ is the theory obtained by adding Corollary II.C.4, Theorem II.C.5 and Lemma II.D.1 as axioms to $BASIC$.*

Similarly, the theory $EBASIC_k$ is the theory obtained by adding Corollary II.C.4, Theorem II.C.5, and Lemma II.D.1 as axioms to $BASIC_k$.

Let $\hat{T}_k^{i,m}$ be the theory

$$EBASIC_k + \hat{\Sigma}_{i,k}^b\text{-}L^m IND.$$

Notice $\hat{T}_2^{i,0} = \hat{T}_2^i$, $\hat{T}_2^{i,1} = \hat{S}_2^i$, and $\hat{T}_2^{i,2} = \hat{R}_2^i$. It should be clear that $\hat{T}_2^{i,m+1} \subseteq \hat{T}_2^{i,m}$ and, in general, $\hat{T}_k^{i,m+1} \subseteq \hat{T}_k^{i,m}$. The theory $EBASIC$ can prove Theorem II.C.5 and Lemma II.C.6. Thus, using the argument in Theorem II.D.2 which makes use of Corollary II.C.4 and Lemma II.D.1, we can prove the following generalization:

Corollary II.D.5 $(i \geq 1, m \geq 1)$ *The theory $\hat{T}_2^{i,m}$ proves $\hat{\Pi}_{i-1}^b$-$REPL^m$ and the theory $EBASIC$ proves*

$$\bigwedge_{j=0}^{n} (\exists y \leq t) A(j, y) \Leftrightarrow$$

$$(\exists w \leq 2 \cdot (t^* \# 2^{|S^n(0)|}) \wedge \bigwedge_{j=0}^{n} A(j, \beta(x, |t^*|, t, w)))$$

where A is a $\hat{\Pi}^b_{i-1}$-formula and t is a term.

One can improve Theorem II.D.2 for $\hat{R}^i_2$ in the following way.

Theorem II.D.6 *($i \geq 1$) $\hat{R}^i_2$ proves*

$$(\forall x \leq p(||t||))(\exists y \leq s)A(x,y) \Leftrightarrow$$
$$(\exists w \leq 2 \cdot (s^* \# 2^{p(||t||)}))(\forall x \leq p(||t||))A(x, \dot{\beta}(x, |s^*|, s, w)))$$

where A is a $\hat{\Pi}^b_{i-1}$-formula, t and $s \in L_2$, and p is a polynomial.

Before we give the proof we note that the above result is stronger than $\hat{\Pi}^b_{i-1}$-$REPL^2$. To see this consider $||x||^n$ where n is a fixed integer. None of the functions in L_2 grow fast enough to bound this by a term of the form $||r(x)||$ where r is an L_2-term.

Proof: Although there is a term s such that an L_2-term of the form $n||t||$ is bounded by $||s||$ we want to be able to generalize our result to the theories $\hat{T}^{i,m}_2$, so we first note that we can prove directly that

$$(\forall x \leq n||t||)(\exists y \leq s)A(x,y) \Leftrightarrow \tag{II.16}$$
$$(\exists w \leq 2 \cdot (s^* \# 2^{n \cdot ||t||}))(\forall x \leq n||t||))A(x, \dot{\beta}(x, |s^*|, s, w)))$$

where A is a $\hat{\Pi}^b_{i-1}$-formula and n is a fixed integer. To do this, we do essentially the same proof as in Theorem II.D.2, except that for each induction step we add n elements to w to make the new w. Since n is finite this works out. We now argue that we can prove

$$(\forall x \leq n||t||^2)(\exists y \leq s)A(x,y) \Leftrightarrow$$
$$(\exists w \leq 2 \cdot (s^* \# 2^{n \cdot ||t||^2}))(\forall x \leq n||t||^2))A(x, \dot{\beta}(x, |s^*|, s, w)))$$

First, let

$$X = (\forall x \leq n \cdot ||t||^2)(\exists y \leq s)A(x,y)$$
$$Y(u) = (\exists w \leq 2 \cdot (s^* \# 2^{n \cdot ||t||^2}))(\forall x \leq n \cdot u \cdot ||t||)A(x, \dot{\beta}(x, |s^*|, s, w))$$

We want to show $\hat{R}_2^i \vdash X \Leftrightarrow Y(||t||)$. That $\hat{R}_2^i \vdash Y(||t||) \supset X$ is obvious. The formula $Y(u)$ is equivalent to a $\hat{\Sigma}_i^b$-formula. Hence, $\hat{R}_2^i$ proves $LLIND_Y$. We also have $\hat{R}_2^i \vdash X \supset Y(0)$, and by (II.16), we have $\hat{R}_2^i \vdash X \supset Y(1)$. We can also use (II.16) to show

$$X \supset (u < |t| \wedge Y(u) \supset Y(Su)).$$

Thus, $\hat{R}_2^i$ prove $X \supset Y(||t||)$. Repeating this speed-up several time allows us to define replacement for any term of the form $n \cdot ||t||^j$. It is not hard to prove replacement for a polynomial p of terms of this form from replacement for the individual terms. □

Corollary II.D.7 ($i \geq 1, m \geq 1$) $\hat{T}_2^{i,m}$ *proves*

$$(\forall x \leq p(|s|_m))(\exists y \leq t)A(x,y) \Leftrightarrow$$
$$(\exists w \leq 2 \cdot (t^* \# 2^{p(|s|_m)}))(\forall x \leq p(|s|_m))A(x, \dot{\beta}(x, |t^*|, t, w)))$$

where A *is a* $\hat{\Pi}_{i-1}^b$*-formula,* t *and* $s \in L_2$*, and* p *is a polynomial.*

The proof of the corollary is essentially the same as Theorem II.D.6.

II.E Equivalence results

Another application of Theorem II.D.2 is the following important theorem.

Theorem II.E.1 ($i \geq 1$)

1. S_2^i *and* $\hat{S}_2^i$ *are equivalent theories.*

2. T_2^i *and* $\hat{T}_2^i$ *are equivalent theories.*

3. R_2^i *and* $\hat{R}_2^i + \hat{\Pi}_{i-1}^b$*-REPL are equivalent theories*

Proof: It is not hard to see that we can convert any Σ_i^b-formula to a $\dot{\Sigma}_i^b$-formula using Theorem II.C.5, Remark II.B.1, Remark II.C.7, Remark II.D.3, and $\hat{\Pi}_{i-1}^b$-$REPL$. Hence, the above prenex theories can prove their induction schemes for any Σ_i^b-formula. □

It is conjectured that $\hat{R}_2^i$ and R_2^i are not equivalent since it seems difficult to show $\hat{R}_2^i$ proves $\hat{\Pi}_{i-1}^b$-$REPL$. However, the next result shows $\hat{R}_2^i$ can prove $\hat{\Pi}_{i-2}^b$-$REPL$.

Theorem II.E.2 *($i \geq 2$) $\hat{R}_2^i$ proves $\hat{\Pi}_{i-2}^b$-$REPL$.*

Proof: The idea for this proof was originally used by Allen [2] to show R_2^i could prove Σ_i^b-replacement. Let A be a $\hat{\Pi}_{i-2}^b$-formula. Let X and Y be the formulas

$$X \;=\; (\forall x \leq |t|)(\exists y \leq s)A(x,y)$$

$$Y \;=\; (\exists w \leq 2 \cdot (t\#s^*))(\forall x \leq |t|)(A(x, \dot{\beta}(x, |s^*|, s, w))).$$

We want to show $\hat{R}_2^i \vdash Y \Leftrightarrow X$. That $\hat{R}_2^i \vdash Y \supset X$ is obvious. Let $Z(j)$ be the following formula.

$$(\forall u \leq |t|)(\exists w \leq 2t\#s^*)(\forall x \leq |t|)$$
$$[(x \leq 2^{\min(j,||t||)} \dot{-} 1 \wedge u + x \leq |t|) \supset A(u+x, \dot{\beta}(x, |s^*|, s, w))].$$

It is easy to see that $\hat{R}_2^i$ can prove this formula equivalent to a $\hat{\Pi}_i^b$-formula. (Note we are counting sharply bounded quantifiers in the number of quantifier alternations.) So by Lemma II.C.1 we have $LLIND_Z$ for this formula. It is trivial that $\hat{R}_2^i$ proves $X \supset Z(0)$. It is also not hard to see that $\hat{R}_2^i$ proves $X \wedge Z(j) \supset Z(Sj)$. Together with $LLIND_Z$ this implies $X \supset Z(||t||)$. As $Z(||t||) \supset Y$ can trivially be proven in $\hat{R}_2^i$ this completes the proof. □

One can of course generalize this theorem to show:

Theorem II.E.3 *($i \geq 2, m \geq 2$) $\hat{T}_2^{i,m}$ proves $\hat{\Pi}_{i-2}^b$-$REPL^{m-1}$.*

Definition II.E.4 ($i \geq 0$) *The class* $\Sigma^b_{i+1} \cap_m \Pi^b_{i+1}$ *is the smallest class containing* Σ^b_i *and closed under Boolean operations and* $(\exists y \leq p(|r(x)|_m))$ *where* $r(x)$ *is a term in our language and where* p *is a polynomial. Similarly, the class* $\hat{\Sigma}^b_{i+1} \cap_m \hat{\Pi}^b_{i+1}$ *is the smallest class containing* $\hat{\Sigma}^b_i$ *and closed under Boolean operations and quantifications* $(\exists y \leq p(|r(x)|_m))$ *where* $r(x)$ *is an* L_2*-term and* p *is a polynomial.*

In the $m = 1$ case of the above definition we simply close under sharply bounded quantification since $p(|r(x)|)$ can be rewritten in the form $|s(x)|$ where s is an L_2-term. We will usually write $\hat{\Sigma}^b_{i+1} \cap \hat{\Pi}^b_{i+1}$ rather than $\hat{\Sigma}^b_{i+1} \cap_1 \hat{\Pi}^b_{i+1}$.

Theorem II.E.5 ($i \geq 1$) *Any formula* ϕ *in the class of formulas containing* $\hat{\Sigma}^b_i \cap \hat{\Pi}^b_i$ *and closed under conjunction, disjunction, and quantifications of the form* $(\exists x \leq t)$ *and* $(Qx \leq p(||t||))$ *is provably equivalent to a* $\hat{\Sigma}^b_i$*-formula in* $\hat{R}^i_2$*. Hence,* $\hat{R}^i_2$ *can prove* $LLIND_\phi$ *for such formulas. Further for* $i \geq 2$*, we can replace* $\hat{\Sigma}^b_i \cap \hat{\Pi}^b_i$ *in the above with* $\Sigma^b_i \cap \Pi^b_i$.

Proof: We can use Theorem II.E.2 and the method of proof in Theorem II.E.1 to show for $i \geq 2$ that $\hat{R}^i_2$ proves every Σ^b_{i-1}-formula is equivalent to a $\hat{\Sigma}^b_{i-1}$-formula. (The theory $\hat{R}^1_2$ by this method proves every formula which is made up of conjunctions and disjunctions of $\hat{\Sigma}^b_0$-formulas is equivalent to a formula of the form $(\exists x \leq |t|)\phi$ where ϕ is an open formula.) Using Remark II.B.1, this also shows that $\hat{R}^i_2$ proves every Π^b_{i-1}-formula is equivalent to a $\hat{\Pi}^b_{i-1}$-formula. The theorem then follows from Lemma II.C.6 and Theorem II.D.6. □

Corollary II.E.6 ($i \geq 1$) *Any formula* ϕ *logically equivalent to a formula in the negation of the class mentioned in Theorem II.E.5 is provably equivalent to a* $\hat{\Pi}^b_i$*-formula in* $\hat{R}^i_2$.

Proof: Let A be such a formula. Then $\neg A$ is logically equivalent to a formula in class mentioned in Theorem II.E.5. So $\neg A$ is provably equivalent to a $\hat{\Sigma}^b_i$-formula B in $\hat{R}^i_2$. Thus, $\hat{R}^i_2$ can prove A equivalent to $\neg B$. By pushing the negation in to the matrix, the theory $\hat{R}^i_2$ proves A is equivalent to a $\hat{\Pi}^b_i$-formula. □

In the same vein as the above theorem and corollary, we have the following result for $\hat{T}_2^{i,m}$.

Theorem II.E.7 ($i \geq 1, m \geq 1$) *Any formula ϕ in the class of formulas containing $\hat{\Sigma}_i^b \cap_{m-1} \hat{\Pi}_i^b$ and closed under conjunction, disjunction, and quantifications of the forms $(\exists x \leq t)$ and $(Qx \leq p(|t|_m))$ where p is a polynomial is provably equivalent to a $\hat{\Sigma}_i^b$-formula in $\hat{T}_2^{i,m}$. Hence, $\hat{T}_2^{i,m}$ can prove $L^m IND_\phi$ for such formulas. Further $\hat{T}_2^{i,m}$ can prove any formula logically equivalent to a formula in the negation of this class is equivalent to a $\hat{\Pi}_i^b$-formula.*

The above result allows us to prove the next theorem, which in turns allows to us show how some of these prenex theories are related.

Theorem II.E.8 ($i \geq 1, m \geq 1$) *$\hat{R}_2^i$ proves the $\hat{\Delta}_i^b$-$LIND$ axioms. In general, $\hat{T}_2^{i,m}$ proves the $\hat{\Delta}_i^b$-$L^{m-1}IND$ axioms.*

Proof: Let $A(x)$ be $\hat{\Delta}_i^b$ with respect to $\hat{T}_2^{i,m}$. Let $A_\Sigma(x)$ be the $\hat{\Sigma}_i^b$-formula to which $A(x)$ is equivalent and let $A_\Pi(x)$ be the $\hat{\Pi}_i^b$-formula to which $A(x)$ is equivalent. The theory $\hat{T}_2^{i,m}$ can prove

$$(\forall x \leq |c|_{m-1})(A_\Sigma(x) \supset A_\Pi(\min(x + 2^b, |c|_{m-1}))) \tag{II.17}$$

is equivalent to a $\hat{\Pi}_i^b$-formula. Call this formula $B(b)$. We can now perform the same proof as in Theorem II.C.2. □

Corollary II.E.9 ($i \geq 1, m \geq 1$) *$\hat{S}_2^{i-1} \subseteq \hat{R}_2^i$. Hence, for $i \geq 2$ we have $S_2^{i-1} \subset \hat{R}_2^i$. In general, we have $\hat{T}_2^{i-1,m-1} \subseteq \hat{T}_2^{i,m}$.*

Proof: The corollary follows from Theorem II.E.1 and Theorem II.E.8. □

II.F The theories $\hat{T}_2^{i,m,j}$

One can actually improve Theorem II.E.8 provided $m > 1$. Let p be a fixed polynomial. If one starts with the formula $B(y)$ defined as

$$(\forall x \leq 2^{p(|c|_m)})(A_\Sigma(x) \supset A_\Pi(\min(x + 2^y, 2^{p(|c|_m)}))) \tag{II.18}$$

rather than equation (II.17), than by $\hat{\Pi}_i^b$-$L^m IND$ one can prove using the speed-up trick of Theorem II.D.6 one can derive.

$$A(0) \wedge (\forall x)(A(x) \supset A(Sx)) \supset (\forall x)A(2^{p(|x|_m)}).$$

Provided $m > 1$ and p is of degree greater than 1, the term $2^{p(|x|_m)}$ will majorize $|x|_{m-1}$. As a specific example, in the $\hat{R}_2^i$ case we can prove the following induction scheme for A a $\hat{\Delta}_i^b$-predicate

$$A(0) \wedge (\forall x)(A(x) \supset A(Sx)) \supset (\forall x)A(2^{p(||x||)})$$

where p is any fixed polynomial. Even $2^{||x||^2}$ will majorize $|x|$ so this scheme is potentially stronger than $LIND_A$. This suggests that it might be interesting to consider theories of arithmetic defined with this kind of induction up to terms of the form $2^{p(|x|_m)}$. First, a definition.

Definition II.F.1 *We define $Term_k^{m,0}$ to be the set containing the 1-ary L_k-term $|x|_m$. For $j > 0$, $Term_k^{m,j}$ is the class of 1-ary L_k terms of the form $2^{\min(p(s),|t|)}$ where t is an L_k-term, s in in $Term_k^{m,j-1}$ and p is a polynomial.*

Recall from the beginning of this chapter, $2^{\min(s,|t|)}$ can actually be defined with an L_k-term so the above classes of terms will in fact all be classes of L_k-terms.

Example II.F.2 *We give some examples of terms in $Term_2^{3,j}$. The term $|||x|||$ will be in $Term_2^{3,0}$, the term $2^{|||x|||^5}$ will be in $Term_2^{3,1}$, and the term $2^{(2^{|||x|||^3})^2}$ will be in $Term_2^{3,2}$. The term $2^{\min(2^{|x|^k},|x\#x|)} = 2^{|x|^2}$ is in $Term_2^{3,3}$. In general, a term in $Term_2^{m,j}$ for $0 < j < m$ looks like*

$$2^{p_1(2^{p_2(2^{p_3(\ldots^{p_j(|x|_m)})})})}.$$

The min *operation will kick in for* $Term_2^{m,m}$ *so this class will contain terms of the form* $2^{|x|^n}$ *for* n *fixed and all terms in this class will be bounded by terms of the form* $2^{|x|^n}$.

We are now ready to define some new induction schemes.

Definition II.F.3 *Let* Ψ *be a class of formulas in* L_k. *The* Ψ-$L^{m,j}IND$ *axioms are axioms of the form*

$$A(0) \wedge (\forall x)(A(x) \supset A(Sx)) \supset (\forall x)A(\ell(x)).$$

where A *is a formulas in* Ψ *and* ℓ *is in* $Term_k^{m,j}$.

For $i \geq m \geq j \geq 0$ *we define* $\hat{T}_k^{i,m,j}$ *to be the theory*

$$EBASIC_k + \hat{\Sigma}^b_{i-j}\text{-}L^{m,j}IND.$$

The next theorem shows that $\hat{T}_k^{i,m,j} \vdash \hat{T}_k^{i,m,j+1}$.

Theorem II.F.4 ($i \geq 1$, $i \geq m \geq j \geq 0$) *The theory* $\hat{T}_k^{i,m,j}$ *proves the* $\hat{\Delta}^b_{i-j}$-$L^{m,j+1}IND$ *axioms. In particular, this implies* $\hat{T}_k^{i,m,j} \vdash \hat{T}_k^{i,m,j+1}$ *so we have*

$$\hat{T}_k^{i,m} = \hat{T}_k^{i,m,0} \supseteq \hat{T}_k^{i,m,1} \supseteq \cdots \supseteq \hat{T}_k^{i,m,m-1} \supseteq \hat{T}_k^{i,m,m} = \hat{T}_k^{i-m}.$$

Proof: The lefthand equality follows by definition. The inclusions follow since we defined the class $Term_k^{m,j}$ specifically so that the proof method of Theorem II.E.8 would go through. The equality between $\hat{T}_k^{i,m,m} = \hat{T}_k^{i-m}$ requires a little bit of work. That $\hat{T}_k^{i-m}$ contains $\hat{T}_k^{i,m,m}$ follows since both of these theories are axiomatized with induction for $\Sigma^b_{i-m,k}$-formulas and the conclusion of the inductions for $\hat{T}_k^{i-m}$ is $(\forall x)A(x)$ which is stronger than $(\forall x)A(\ell(x))$ where $\ell \in Term_k^{m,m}$. On the other hard as we said in Example II.F.2, $Term_k^{m,m}$ contains terms of the form $2^{|x|^k}$ for any fixed k. Using Theorem II.C.1 we could have axiomatized these theories with $\Pi^b_{i-m,k}$-formulas in their induction schmeas instead of $\Sigma^b_{i-m,k}$-formulas.

Then in $\hat{T}_k^{i,m,m}$ we can do induction on $(\forall y \leq 2^{|x|})A(y)$ where $A(x)$ is a $\Pi^b_{i-m,k}$-formula to derive the $IND_A^{\{id\}}$ axiom of $\hat{T}_k^{i-m}$. □

By Definition II.F.3. $T_2^i = \hat{T}_2^{i,0,0}$. We write $\hat{R}_2^{i,1}$ for the theories $\hat{T}_2^{i,2,1}$. The term $|x|$ is less than $2^{||x||}$ which is in $Term_2^{2,1}$. We will show at the end of this chapter that this implies for $i \geq 1$ we have $S_2^{i-1} \subseteq \hat{R}_2^{i,1}$. It is unknown whether these two theories are equal. We will show in Chapter VIII that $\hat{R}_2^{i,1} \preceq_{\hat{\Sigma}_i^b} \hat{R}_2^i$. By [16], we know $S_3^{i-1} \preceq_{\Sigma_i^b} R_3^i$ and this can be viewed as a consequence of the fact that terms in $Term_3^{2,1}$ can be bounded by terms of the form $|t|$ where t is a term in L_3. Thus, $S_3^{i-1} = \hat{R}_3^{i,1}$. The general result we will show in Chapter VI is that for $i \geq m > j > 0$ or for $i > m = j = 1$ we have

$$\hat{T}_k^{i,m,j} \preceq_{\hat{\Sigma}^b_{i-j+1}} \hat{T}_k^{i,m}.$$

Notice the terms in $Term_2^{1,1}$ can grow as large as any term L_2. We will see at the end of this chapter this implies $\hat{T}_2^{i,1,1}$ will equal T_2^{i-1}. So by the above result, we have

$$T_2^{i-1} = \hat{T}_2^{i,1,1} \preceq_{\hat{\Sigma}_i^b} \hat{T}_2^{i,1} = S_2^i$$

which is a result already known from Buss [14].

II.G Theories with term bounded induction or replacement

The theories we are considering have at this point become overloaded with too many indices. In order to simplify our proofs in later chapters, we define slightly more abstract theories which involve fewer indices, but which subsume all the theories considered thus far. We begin by defining some general schemes of induction and replacement.

Definition II.G.1 *A set τ of* 1*-ary terms in L_k is called a set of* k-iterms *(k-induction terms). We call* 2-iterms *just* iterms. *Let τ be a set of iterms. The*

Ψ-IND^τ axioms are the axioms IND^ℓ_α:

$$\alpha(0) \wedge (\forall x)(\alpha(x) \supset \alpha(Sx)) \supset (\forall x)\alpha(\ell(x))$$

where α is a formula in Ψ and ℓ is a term in τ. We write IND^τ_α for the set of axioms IND^ℓ_α for each $\ell \in \tau$.

The Ψ-$REPL^{|\tau|}$ are the axioms $REPL^{|\ell|}_{\alpha,s,t}$:

$$(\forall x \leq |\ell(s)|)(\exists y \leq t)\alpha(x,y) \Leftrightarrow$$
$$(\exists w \leq 2 \cdot (t^* \# \ell(s)))(\forall x \leq |\ell(s)|)\alpha(x, \dot{\beta}(x, |t^*|, t, w)))$$

where α is a formula in Ψ, ℓ is in τ, and s and t are in L_k. We write $REPL^\tau_\alpha$ for the set of axioms $REPL^{|\ell|}_{\alpha,s,t}$ for each $\ell \in \tau$.

As an example of the above definitions, let $id(a) = a$. Then the set $\{id\}$ is a set of iterms. $\hat{\Sigma}^b_i$-$IND^{\{id\}}$ is just $\hat{\Sigma}^b_i$-IND and $\hat{\Pi}^b_i$-$REPL^{\{|id|\}}$ is just $\hat{\Pi}^b_i$-$REPL^1$. Notice in the above definition we write $|\tau|$ to denote the class of terms of the form $|\ell|$ for ℓ in τ. We will frequently use this nomenclature. Let cl_k denote the set of closed iterms in L_k. We will write cl for cl_2. It is not hard to see that the $\hat{\Sigma}^b_i$-IND^{cl} axioms are provable in $BASIC$. As another example of choices of τ consider τ defined as the set containing the term $1\#(MSP(x, \lfloor \frac{1}{2}|x| \rfloor)$. This term has growth rate approximately $2^{|\sqrt{x}|}$ which is a potentially interesting growth rate between that of id and $|id|$. Notice iterms need not be monotonic we will see below that this will not have any pathological consequences. We now define some useful properties for iterms to have:

Definition II.G.2 *A set τ of k-iterms is called* product closed *if whenever $s(x)$ and $t(x)$ are terms in τ there is a iterm $(s \cdot t)$ in τ and a term r in L_k such that $(s \cdot t)(r(x)) = s(x) \cdot t(x)$.*

A class τ of k-iterms is called smash closed *if in addition whenever $s(x)$ and $t(x)$ are iterms in τ there is a term $(s\#t)$ in τ and a term r in L_k such that $(s\#t)(r(x)) = s(x)\#t(x)$.*

The obvious example of a product closed and smash closed set of terms is just $\{id\}$ since $id(x \cdot x) = id(x) \cdot id(x)$ and $id(x\#x) = id(x)\#id(x)$. The class $\{|id|\}$ is product closed but not smashed closed. The class $Term_2^{2,1}$, however, is also smash closed and product closed. To see this consider ℓ_1 and ℓ_2 in $Term_2^{2,1}$. By definition of $Term_2^{2,1}$ these terms can be written in the form $2^{p_{\ell_1}(||x||)}$ and $2^{p_{\ell_2}(||x||)}$ where p_{ℓ_1} and p_{ℓ_2} are polynomials and

$$2^{p_{\ell_1}(||x||)}\#2^{p_{\ell_2}(||x||)} = 2^{p_{\ell_1}(||x||)\cdot p_{\ell_2}(||x||)}$$

and the right hand side is also a term in $Term_2^{2,1}$. A similar argument works for product closure. The product closure of $\{||x||\}$ consists of all iterms of the form $p(||x||)$ where x is a polynomial.

One point of closing under smash and product is given by the next lemma. We will also see in a Chapter VI that smash closure plays an important role in conservation results between bounded arithmetic theories.

Lemma II.G.3 *Let Ψ be a class of formulas and let τ be smash closed. Then $T := EBASIC{+}\Psi\text{-}IND^\tau$ can prove $IND_A^{\ell_1(x)\#\ell_2(x)}$ for any A in Ψ and $\ell_1, \ell_2 \in \tau$.*

Similarly, if τ is product closed T can prove $IND_A^{\ell(x)\cdot\ell(x)}$.

Proof: Let τ be smash closed and consider an axiom of the form $IND_A^{\ell_1(x)\#\ell_2(x)}$ where A is in Ψ and ℓ_1, ℓ_2 are in τ. Since τ is smash closed there is a term ℓ in τ such that $\ell(r(x)) = \ell_1(x)\#\ell_2(x)$ where r is an L_2-term. Since the conclusion of the induction hypothesis is weaker it follows that IND_A^{ℓ} implies $IND_A^{\ell(r)} = IND_A^{\ell_1(x)\#\ell_2(x)}$. This establishes the lemma. The product closure statement is proven in the same way. □

There are many possible ways one could close a set under product or smash. The *naive smash closure* of τ is defined inductively by letting $\sigma_0 = \tau$, then letting

$$\sigma_{i+1} = \sigma_i \cup \{\ell_1(x)\#\ell_2(x)\ , \ell_1(x)\cdot\ell_2(x)\ \mid \ell_1, \ell_2 \in \sigma_i\},$$

and finally letting the smash closure be $\cup_i \sigma_i$. It is easy to verify this set of terms will be smash closed. One can define the *naive product closure* similarly by deleting the smash term from the definition of σ_{i+1}. The problem with these definitions of smash and product closure is that a smash (resp. product) closed set is not necessarily equal to its closure. Consider for example the case of the set $\{id\}$. This set is both smash and product closed but its closure under the above definition has infinitely many members. To remedy this situation we inductively define the *smash closure* of τ by letting $\sigma_0 = \tau$. then letting

$$\begin{aligned}\sigma_{i+1} = \sigma_i \ \cup \ & \{\ell_1(x)\#\ell_2(x) \mid \ell_1, \ell_2 \in \sigma_i \text{ and } (\forall r \in L_2)(\forall \ell \in \sigma_i)(\neg \ell(r) = \ell_1 \# \ell_2)\} \\ \cup \ & \{\ell_1(x) \cdot \ell_2(x) \mid \ell_1, \ell_2 \in \sigma_i \text{ and } (\forall r \in L_2)(\forall \ell \in \sigma_i)(\neg \ell(r) = \ell_1 \cdot \ell_2)\}\end{aligned}$$

and finally letting the smash closure be $\cup_i \sigma_i$. It is easy to verify this set of terms will be smash closed. One can define the *product closure* similarly by deleting the smash operation from the definition of σ_{i+1}. Using these definitions of smash and product closure a smash (resp. product) closed set is equal to its closure. The next lemma shows that having induction up to terms in the naive smash closure of a set is no stronger than having induction up to terms in the smash closure of a set and similarly for naive product closure and product closure.

Lemma II.G.4 *Let τ' be the naive smash closure of τ and let τ'' be the smash closure of τ. Let $T' := EBASIC{+}\Psi\text{-}IND^{\tau'}$ and let $T'' := EBASIC{+}\Psi\text{-}IND^{\tau''}$. Then $T' = T''$.*

A similar statement holds with regard to product closure.

Proof: This is proven by an induction on the construction of the naive smash closure. Since τ'' contains τ certainly T'' proves the $\Psi\text{-}IND^{\tau} = \Psi\text{-}IND^{\sigma_0}$ axioms. Let A be in Ψ and suppose ℓ_1 and ℓ_2 are two terms in σ_i, the set of terms at the ith stage in the construction of the naive smash closure of τ. Our induction hypothesis is that there are terms ℓ_1' and ℓ_2' in τ'' such that $\ell_i'(r_i(x)) = \ell_i(x)$ where r_i is an L_2-term. Since τ'' is smash closed there is a term ℓ in τ'' such that $\ell(r(x)) =$

$\ell'_1(x)\#\ell'_2(x)$. Thus, T'' will prove $IND_A^{\ell_1(x)\#\ell_2(x)}$ since IND_A^{ℓ} implies $IND_A^{\ell'_1\#\ell'_2}$ implies $IND_A^{\ell_1(x)\#\ell_2(x)}$ since the conclusion of these axioms become progressively weaker. The product case of the construction is handled similarly. This completes the induction step and the proof. The product closure statement is proven in the same way. □

Definition II.G.5 *We write $\dot{\tau}$ to denote the product closure of τ. We write $(|\dot{\tau}|)$ to denote the product closure of $|\tau|$.*

We write $\tau^{\#}$ to denote the smash closure of τ. We write $(|\tau|)^{\#}$ to denote the smash closure of $|\tau|$.

The abstract theories we will consider in later chapters are the following:

Definition II.G.6 *Let τ be a set of k-iterms.*

For $i \geq 0$ we define $\hat{T}_k^{i,\tau}$ to be the theory

$$EBASIC_k + \hat{\Sigma}_i^b\text{-}IND^{\tau}$$

and we define $\hat{C}_k^{i,|\tau|}$ to be the theory

$$EBASIC_k + open\text{-}IND^{\tau} + \hat{\Pi}_i^b\text{-}REPL^{|\tau|}$$

The C in $\hat{C}_k^{i,\tau}$ stands for collection axiom which is often what the replacement axioms are called in bounded arithmetic. The theories $\hat{C}_2^{i,|\tau|}$ will appear again in Chapter IV and will be discussed in detail in Chapter VIII. To see the theories $\hat{T}_2^{i,\tau}$ and $\hat{C}_2^{i,|\tau|}$ are more general than the theories considered thus far notice

$$\begin{aligned} \hat{T}_k^{i,m,j} &= \hat{T}_k^{i-j,Term_k^{m,j}}, \\ \hat{T}_k^{i,m} &= \hat{T}_k^{i,\{|id|_m\}}, \\ EBASIC_k &= \hat{T}_k^{i,cl} = \hat{T}_k^{i,|cl|_m} \end{aligned}$$

One can show using the iteration of induction arguments of Theorem II.D.6 the following important theorem about abstract theories:

Theorem II.G.7 ($i \geq 0$) *Let τ be a set of k-iterms.*

1. $\hat{T}_k^{i,\tau} = \hat{T}_k^{i,\dot{\tau}}$
2. $\hat{T}_k^{i,|\tau|} = \hat{T}_k^{i,(|\dot{\tau}|)} = \hat{T}_k^{i,|\tau^{\#}|}$
3. $EBASIC_k$+$\hat{\Pi}^b_{i,k}$-$REPL^{|\tau|}$= $EBASIC_k$+$\hat{\Pi}^b_{i,k}$-$REPL^{(|\dot{\tau}|)}$
4. $\hat{C}_k^{i,|\tau|} = \hat{C}_k^{i,(|\dot{\tau}|)} = \hat{C}_k^{i,|\tau^{\#}|}$

Using the argument at the beginning of Section II.F one can show:

Theorem II.G.8 ($i \geq 0$) *Let τ be a set of k-iterms. The theory $\hat{T}_k^{i-1,|\tau|}$ proves the $\hat{\Delta}^b_{i+1}$-$IND^{\tau^{\#}}$ axioms. Therefore,*

$$\hat{T}_k^{i,\tau^{\#}} \subseteq \hat{T}_k^{i+1,|\tau|}.$$

The other theorems of this chapter also generalize using essentially the same proofs to the theories $\hat{T}_2^{i,\tau}$. We first give a definition and state the results we will need in later chapters. We often assume τ is a set of iterms without explicitly mentioning it.

Definition II.G.9 ($i \geq 0$) *The class $\hat{\Sigma}^b_{i+1} \cap_{|\tau|} \hat{\Pi}^b_{i+1}$ is the smallest class containing $\hat{\Sigma}^b_i$ and closed under Boolean operations and $(\exists y \leq p(|\ell(x)|))$ where $\ell(x)$ is a iterm in τ and where p is a polynomial.*

Theorem II.G.10 *Let Ψ be a class of formulas over our language closed under term substitution. Let $\neg\Psi$ denote those formulas which are negations of formulas in Ψ. Then $BASIC$+Ψ-IND^{τ} is equivalent to $BASIC$+$\neg\Psi$-IND^{τ}.*

Theorem II.G.11 ($i \geq 1$) *The theories $\hat{T}_2^{i,\tau}$, $\hat{T}_2^{i,|\tau|}$, and $\hat{T}_2^{i+1,||\tau||}$ each prove $\hat{\Pi}^b_{i-1}$-$REPL^{(|\dot{\tau}|)}$.*

Theorem II.G.12 ($i \geq 1$) *Any formula ϕ in the class of formulas containing $\hat{\Sigma}_i^b \cap_{|\tau|} \hat{\Pi}_i^b$ and closed under conjunction, disjunction, and quantifications of the forms $(\exists x \leq t)$ and $(Qx \leq p(|\ell(t)|))$ where p is a polynomial is provably equivalent to a $\hat{\Sigma}_i^b$-formula in $\hat{T}_2^{i,|\tau|}$. Hence, $\hat{T}_2^{i,|\tau|}$ can prove $IND_\phi^{|\tau|}$ for such formulas. Further $\hat{T}_2^{i,|\tau|}$ can prove any formula logically equivalent to a formula in the negation of this class is equivalent to a $\hat{\Pi}_i^b$-formula.*

Note the Theorem II.G.12 has content even for $EBASIC$ since $EBASIC$ is equal to $\hat{T}_2^{i,|\epsilon|}$. We finish this chapter with an important theorem which allows to determine the relative strength of induction up to an arbitrary iterm.

Theorem II.G.13 *Let Ψ be a class of formulas closed under quantifications of the form $(\forall x \leq t)$. Then if ℓ_1 and ℓ_2 are two iterms and*

$$EBASIC_k \vdash (\forall x)(\exists y)(\ell_1(x) < \ell_2(y)) \tag{II.19}$$

then

$$EBASIC_k{+}\Psi\text{-}IND^{\{\ell_1\}} \subseteq EBASIC_k{+}\Psi\text{-}IND^{\{\ell_2\}}$$

If $EBASIC$ proves (II.19) we say ℓ_2 *surpasses* ℓ_1.

Proof: Suppose $A(a)$ is a formula in Ψ. Then $B(b) := (\forall x \leq b)A(x)$ is also in Ψ. It is not hard to see that $A(0)$ implies $B(0)$ and $(\forall x)(A(x) \supset A(Sx))$ implies $(\forall x)(B(x) \supset B(Sx))$. Finally, (II.19) together with $(\forall x)B(\ell_2(x))$ imply $(\forall x)A(\ell_1(x))$. Thus, $EBASIC{+}IND_B^{\{\ell_2\}}$ implies $IND_A^{\{\ell_1\}}$, which suffices to establish the theorem. □

Corollary II.G.14 ($i \geq 0$) *Let τ and τ' be two collections of k-iterms such that $EBASIC$ can prove every k-iterm in τ is surpassed by a k-iterm in τ' then $\hat{T}_k^{i,\tau} \subseteq \hat{T}_k^{i,\tau'}$. In particular, $S_2^i \subseteq \hat{R}_2^{i+1,1}$.*

Proof: The class of formulas provably equivalent to $\hat{\Pi}^b_{i,k}$-formulas in $\hat{T}^{i,\tau'}_k$ satisfies the conditions of Theorem II.G.13. Therefore, as every term in τ is surpassed by some term in τ', the theory $\hat{T}^{i,\tau'}_k$ proves the $\hat{\Pi}^b_{i,k}$-IND^τ axioms and, thus, by Theorem II.G.10 it also proves the $\hat{\Sigma}^b_{i,k}$-IND^τ axioms. □

Corollary II.G.14 gives us some indication of the power of a theory of the form $\hat{T}^{i,\{\ell\}}_2$ where ℓ might not be monotonic since it shows this theory is contained in any $\hat{T}^{i,\tau}_2$ which has terms which surpass it (for instance, T^i_2) and it contains any theory $\hat{T}^{i,\{\ell'\}}_2$ involving a monotonic ℓ' which ℓ surpasses.

Chapter III

Multifunction algebras and local search problems

In this chapter, we define multifunction algebras $B_{i,2}^{|\tau|}$, and $B_{i,2}$. We show $\hat{T}_2^{i,|\tau|}$ can $\hat{\Sigma}_i^b$-define the multifunctions in $B_{i,2}^{|\tau|}$ and $EBASIC$ can $\hat{\Sigma}_i^b$-define the multifunctions in $B_{i,2}$. We also define the classes LS_τ^Ψ of multifunctions computed as optima of (Ψ, τ)-local search problems. We show $\hat{T}_2^{i,\tau}$ can prove any (Ψ, τ)-local search problem in $\hat{T}_2^{i,\tau}$ has a local optima. Thus, $\hat{T}_2^{i,\tau}$ can define these multifunctions. In Chapter V we will show that any $\hat{\Sigma}_i^b$-definable multifunction of $\hat{T}_2^{i,|\tau|}$ is computable by a multifunction in $B_{i,2}^{|\tau|}$. We will also show the corresponding results for $EBASIC$. Hence, we will have precise characterization of the $\hat{\Sigma}_i^b$-definable multifunctions of these classes. For complexity theorists it may seem more interesting if we had given a characterization of the $\hat{\Sigma}_i^b$-definable multifunctions of $\hat{T}_2^{i,|\tau|}$ in terms of polynomial-time computations with limited access to an oracle set. We give such a characterization in Chapter VI. We begin with our algebra characterizations because we feel it helps shed light on what kind of reasoning is available in our proof systems and it helps shed light on what it means for a theory to define a multifunction which queries an oracle.

Throughout this chapter and the rest of this thesis when we refer to a set of terms τ, we will mean a set of iterms.

III.A The algebras $B^{\tau}_{i,2}$ and $B_{i,2}$

Before we introduce our algebras it is important to make precise what we mean by multifunction and what we mean by various relations between multifunctions.

Definition III.A.1 *A* multifunction *is a set $f \subseteq \mathbf{N} \times \mathbf{N}$ such that for all $x \in \mathbf{N}$ there exists $\langle x, y\rangle \in f$. We usually express $\langle x, y\rangle \in f$ as $f(x) = y$. We write $f \circ g$ for the composition of the two multifunctions f, g and define $(f \circ g)(x) = z$ if there is some $y \in \mathbf{N}$ such that $f(x) = y$ and $g(y) = z$. If f is a multifunction and r is a function, we write $f(x) > r(x)$ if there exists $y > r(x)$ such that $f(x) = y$. We define $f(x) < r(x)$ if there exists $y < r(x)$ such $f(x) = y$.*

We now give some definitions of some operations on multifunctions necessary to define our algebras.

Definition III.A.2

1. *Let C be a multifunction. The function $(\mu x \leq z)[C(x, \vec{y}, z) = 0]$ returns the least value $x \leq z$ such that $C(x, \vec{y}, z) = 0$ holds and returns $z + 1$ if no such value exists. This operation is called the μ-operator.*

2. *Let C be a multifunction. The multifunction $(Wx \leq z)[C(x, \vec{y}, z) = 0]$ returns an $x \leq z$ such that $C(x, \vec{y}, z) = 0$ holds if one exists and returns $z + 1$ if no such value exists. This operation is called the W-operator.*

3. *A multifunction f is defined using τ-bounded primitive recursion (BPR^{τ}_{k}) from (multi)functions g, h, t, and r if*

$$\begin{aligned} F(0, \vec{x}) &= g(\vec{x}) \\ F(n+1, \vec{x}) &= \min(h(n, \vec{x}, F(n, \vec{x})), r(n, \vec{x})) \\ f(n, \vec{x}) &= F(\ell(t(n, \vec{x})), \vec{x}) \end{aligned}$$

for some r in L_k and for some L_k-term t and some τ-term ℓ. We write BPR^{τ} for BPR^{τ}_{2}.

If g, h, t, and r are multifunctions then f obtained by BPR^τ is the multifunction which results by viewing each step in the above iteration as a composition of multifunctions. The min step is well-defined as a composition of the multifunctions with the term min from Chapter II. The output of the min step will be a multifunction whose values are bounded by r.

Definition III.A.3

1. $(k \geq 2)$ *The function algebra* $B^\tau_{0,k} = B_{0,k}$ *is the algebra containing* $zero(x) = 0$, $S(x)$, $\lfloor \frac{1}{2}x \rfloor$, MSP, $+$, $\cdot$, $\dot{-}$, $\#_2, \ldots, \#_k$, *and* $|a|$ *and closed under composition.*

2. $(k \geq 2)$ *The multifunction algebra* $B_{1,k}$ *is the smallest class containing* $B_{0,k}$, *containing* $(\forall x \leq |z|)[C(x, \vec{y}) = 0]$ *for any* C *in* $B_{0,k}$, *and closed under composition.*

3. $(k \geq 2)$ *The multifunction algebra* $B^\tau_{1,k}$ *is the smallest class containing* $B^\tau_{0,k}$, *containing* $(\forall x \leq |z|)[C(x, \vec{y}) = 0]$ *for any* C *in* $B_{0,k}$, *closed under composition, and closed under the recursion scheme* BPR^τ_k.

4. $(i > 1, k \geq 2)$ *The multifunction algebra* $B_{i,k}$ *is the smallest class containing* $B_{i-1,k}$, *containing* $(\forall x \leq z)[D(x, \vec{y}) = 0]$ *for any* D *in* $B_{i-1,k}$ *and closed under composition.*

5. $(i > 1, k \geq 2)$ *The multifunction algebra* $B^\tau_{i,k}$ *is the smallest class containing* $B_{i-1,k}$, *containing* $(\forall x \leq z)[D(x, \vec{y}) = 0]$ *for any predicate* D *in* $B_{i-1,k}$, *closed under composition, and closed under the recursion scheme* BPR^τ_k.

Lemma III.A.4 $(i \geq 1)$ *The algebra* $B^\tau_{i,k}$ *is closed under the following type of recursion:*

$$\begin{aligned} F(0, \vec{x}) &= g(\vec{x}) \\ F(n+1, \vec{x}) &= \min(h(n, \vec{x}, F(n, \vec{x})), r(n, \vec{x})) \\ f(n, \vec{x}) &= F(\min(n, \ell(t(n, \vec{x}))), \vec{x}) \end{aligned}$$

where g and h are in $B^{\tau}_{i,k}$. r and t are in L_k and ℓ is in τ.

Proof: To define f we first define the multifunction f' as

$$\begin{aligned} F'(0,\vec{x}) &= g(\vec{x}) \\ F'(n+1,\vec{x}) &= \min(F'(n,\vec{x}) + \\ &\quad \min(h(n,\vec{x},\hat{\beta}(n,|r^*|,F'(n,\vec{x}))),r)\cdot(i\cdot 2^{|r^*|}),(\ell(t)+1)\cdot 2^{|r^*|}) \\ f'(n,\vec{x}) &= F'(\ell(t(n,\vec{x})),\vec{x}) \end{aligned}$$

From f' we can define f as $\hat{\beta}(\min(n,\ell(t)),|r^*|,f'(n,\vec{x}))$. □

We will for the rest of the chapter mainly consider the case when $k=2$: however, our results readily generalize.

Definition III.A.5 *Let $\mathcal{C}$ be a collection of multifunctions. We write $\mathcal{C}=0$ to denote the set of relations of the form $f=0$ where f is a multifunction in $\mathcal{C}$. We define $\mathcal{C}>0$ similarly.*

The next lemma will help us show that $\hat{T}^{i,|\tau|}_2$ can $\hat{\Sigma}^b_i$-define the functions in $B^{|\tau|}_{i,2}$.

Lemma III.A.6

1. *The relations in $B_{0,2}=0$ can express precisely the open formulas of L_2.*
2. *($i\geq 1$) The relations in $B_{i,2}=0$ can express any predicate which is a Boolean combination of $\hat{\Sigma}^b_{i-1}$-formulas.*
3. *($i\geq 0$) The relations in $B_{i,2}=0$ can be expressed by $\hat{\Sigma}^b_i$-formula.*

Proof:

(1) The functions in $B_{0,2}$ are precisely the terms in L_2 as $B^{\tau}_{0,2}=B_{0,2}$ is just the closure of the initial functions of L_2 under composition. In particular, $B^{\tau}_{0,2}=B_{0,2}$ can define the terms $K_{=}$, $K_{\leq}$, $K_{\wedge}$, and K_{-} which we defined at the

beginning of Chapter II. From these terms one can express any open formula. Now suppose t is a function in $B^1_{0,2} = B_{0,2}$, then since t is an L_2-term, $t = 0$ is an open formula.

(2) The proof of the second statement is by induction on i. When $i = 1$ by (1) it suffices to show $B_{1,2}$ can express a sharply bounded quantifier. Consider the formula $A := (\exists x \leq |t|)B$ where B is an open formula equivalent to $f_B = 0$ in $B_{0,2} = 0$. Then A can be expressed as

$$[K_\neg(K_=((Wx \leq |t|)[f_B = 0], |t| + 1))] = 0.$$

For all $j < i$ assume $B_{j,2}$ can express Boolean combinations of $\hat{\Sigma}^b_{j-1}$-predicates. Consider the $\hat{\Sigma}^b_{i-1}$-formula $A := (\exists x \leq t)B$ where B is a $\hat{\Pi}^b_{i-2}$-predicate which by assumption can be expressed in $B_{i-2,2} = 0$ as $f_B = 0$. Then A can be expressed as

$$[K_\neg(K_=((Wx \leq t)[f_B = 0], t + 1))] = 0.$$

(3) We show the graph of any multifunction $f(\vec{x})$ in $B_{i,2}$ can be expressed in the form $A_f(\vec{x}, y)$ where A_f is a $\hat{\Sigma}^b_i$-formula and y is bounded in A_f by a term t. From this one can see that $f(\vec{x}) = 0$ is expressible as a $\hat{\Sigma}^b_i$-formula since $A_f(\vec{x}, 0)$ is a $\hat{\Sigma}^b_i$-formula.

In the $i = 1$ case, by Remark II.D.3 we can express the base functions of $B_{0,2}$ with $\hat{\Sigma}^b_1$-formulas. So it remains to show $\hat{\Sigma}^b_1$-formulas can express the graphs of functions defined by sharply bounded W-operator on open formulas (by (1)).

Suppose $f(x) = y$ is a function in $B_{0,2}$. Hence, f is an L_2-term. So we can define the graph of $((Wx \leq |t|)[f(x) = 0]) = y$ with the following formula which is equivalent in $EBASIC$ to a $\hat{\Sigma}^b_1$-formula

$$[(\exists x \leq |t|)(f(x) = 0 \wedge y = x) \vee (\forall x \leq |t|)(f(x) > 0 \wedge y = |t| + 1)].$$

Now suppose $f = h(g_1(\vec{x}_1), \ldots, g_n(\vec{x}_n))$ and we can $\hat{\Sigma}^b_1$-define the functions $h(z_1, \ldots z_n)$ and $g_j(\vec{x}_j)$ with graphs H, G_j. Then we can define f with the

following formula which is provably equivalent to a $\hat{\Sigma}^b_1$-formula in $EBASIC$:

$$y \leq t \wedge (\exists y_1 \leq t_1) \cdots (\exists y_n \leq t_n)[G_1(\vec{x}_1, y_1) \\ \wedge \cdots \wedge G_n(\vec{x}_1, y_1) \wedge H(y_1, \ldots, y_n, y)].$$

For $i \geq 1$ we can use essentially the same argument to argue the graphs of $\hat{\Sigma}^b_i$-formulas are closed composition. What is left to show is that one can express with $\hat{\Sigma}^b_i$-formulas the graphs of multifunctions defined by W-operator on multifunctions in $B_{i-1,2}$. Suppose $f_C(x)$ is a multifunction in $B_{i-1,2}$. Our induction hypothesis is that the graph of $f_C(x) = y$ can be defined with some $\hat{\Sigma}^b_{i-1}$-formula, $C(x, y)$. We can define $(\mathrm{W}y \leq t)[f_C(x) = 0] = z$ with the following formula which $EBASIC$ can prove equivalent to a $\hat{\Sigma}^b_i$-formula

$$[(C(x, 0) \wedge x = z) \vee (\forall x \leq t)(\neg(C(x, 0) \wedge z = t + 1)].$$

□

III.B Defining algebras in prenex theories

We now show that $\hat{T}^{i,|\tau|}_2$ can $\hat{\Sigma}^b_i$-define the multifunctions in $B^{|\tau|}_{i,2}$ and $EBASIC$ can $\hat{\Sigma}^b_i$-define the multifunctions in $B_{i,2}$.

Theorem III.B.1 ($i \geq 0$) *The theory $\hat{T}^{i,|\tau|}_2$ can $\hat{\Sigma}^b_i$-define the multifunctions in the algebra $B^{|\tau|}_{i,2}$.*

Proof: Since functions in $B^{|\tau|}_{0,2} = B_{0,2}$ are all L_2-terms, the theory

$$EBASIC \subseteq \hat{T}^{i,|\tau|}_2$$

can $\hat{\Sigma}^b_0$-define them. For $i \geq 1$, it suffices by Remark II.D.3 to show that $\hat{T}^{i,|\tau|}_2$ proves the class $B^{|\tau|}_{i,2}$ contains the appropriate W-operators, and is closed under composition and $BPR^{|\tau|}_2$.

(W-operator) We first show $EBASIC$ can $\hat{\Sigma}^b_1$-define $(Wx \leq |t|)[f(x,\vec{z}) = 0]$ for $f(x,\vec{z})$ a function in $B_{0,2} = B^{\vec{\tau}}_{0,2}$. i.e., f is just an L_2-terms. To do this one just needs to notice that

$$(\exists y \leq |t|+1)[(\exists x \leq |t|)(f(x,\vec{z}) = 0 \wedge y = x) \vee (\forall x \leq |t|)(f(x,\vec{z}) > 0 \wedge y = |t|+1)].$$

is provable in $EBASIC$. Further the formula inside the scope of $(\exists y \leq |t|+1)$ is equivalent to a $\hat{\Sigma}^b_1$-formula by Remark II.C.7. Next we show $EBASIC$ can $\hat{\Sigma}^b_i$-define $(Wx \leq t)[f_C(x,\vec{z}) = 0]$ for $f_C(x,\vec{z})$ a multifunction in $B_{i-1,2}$. By Lemma III.A.6, the relation $f_C = 0$ is expressible by a $\hat{\Sigma}^b_{i-1}$-formula $C(x,\vec{z})$. So $(Wx \leq t)[f_C(x,\vec{z}) = 0]$ will be $\hat{\Sigma}^b_i$-definable since

$$(\exists y \leq t+1)[(\exists x \leq t)(C(x,\vec{z}) \wedge y = x) \vee (\forall x \leq t)(\neg C(x,\vec{z}) \wedge y = t+1)].$$

is provable in $EBASIC$ and the formula inside the scope of $(\exists y \leq t+1)$ is equivalent to a $\hat{\Sigma}^b_i$-formula by Remark II.C.7. Since $\hat{T}^{i,|\tau|}_2$ contains $EBASIC$, this shows $\hat{T}^{i,|\tau|}_2$ is also closed under the appropriate W-operators.

(Composition) Suppose $f = h(g_1(\vec{x}_1), \ldots g_n(\vec{x}_n))$ and that $\hat{T}^{i,|\tau|}_2$ can $\hat{\Sigma}^b_i$-define the multifunctions $h(z_1, \ldots z_n)$ and $g_j(\vec{x}_j)$ where $1 \leq j \leq n$ and where $h, g_j \in B^{\vec{\tau}}_{i,2}$. Then there are $\hat{\Sigma}^b_i$-formulas $H, G_1, \ldots, G_n$ such that

$$\hat{T}^{i,|\tau|}_2 \vdash (\forall \vec{z})(\exists y \leq t) H(\vec{z}, y)$$

and

$$\hat{T}^{i,|\tau|}_2 \vdash (\forall \vec{x}_j)(\exists y \leq t_j) G_j(\vec{x}_j, y), \quad \text{for } 1 \leq j \leq n.$$

So

$$\hat{T}^{i,|\tau|}_2 \vdash (\forall \vec{x}_1) \cdots (\forall \vec{x}_n)(\exists y \leq t)(\exists y_1 \leq t_1) \cdots (\exists y_n \leq t_n)(G_1(\vec{x}_1, y_1) \wedge \cdots \wedge G_n(\vec{x}_1, y_1) \wedge H(y_1, \ldots y_n, y)).$$

The formula inside the scope of the $(\exists y \leq t)$ is equivalent to a $\hat{\Sigma}^b_i$-formula provably in $EBASIC$ and the above formula defines f.

$(BPR_2^{|\tau|})$ Suppose f is obtained by $BPR_2^{|\tau|}$ from g and h which are $\hat{\Sigma}^b_i$-definable in $\hat{T}_2^{i,|\tau|}$, r and t which are L_2-terms, and ℓ in τ. Let G and H be the $\hat{\Sigma}^b_i$-graphs of g and h such that

$$\begin{aligned} \hat{T}_2^{i,|\tau|} &\vdash (\forall \vec{x})(\exists y \leq t_1) G(\vec{x}, y) \\ \hat{T}_2^{i,|\tau|} &\vdash (\forall n, \vec{x}, u)(\exists v \leq t_2) H(n, \vec{x}, u, v). \end{aligned}$$

We can assume $r(0, \vec{x}) \leq t_1(\vec{x})$. So let $A(n, \vec{x}, w, y)$ be the formula

$$\begin{aligned} & G(\vec{x}, \dot{\beta}(0, |r^*(|\ell(t)|, \vec{x})|, r(0, \vec{x}), w))) \wedge \\ & \quad \dot{\beta}(n, |r^*(|\ell(t)|, \vec{x})|, r(|\ell(t)|), \vec{x}), w) = y \wedge \\ & \quad (\forall j < |\ell(t)|)((H(j, \vec{x}, \dot{\beta}(j, |r^*(|\ell(t)|, \vec{x})|, w), \dot{\beta}(Sj, |r^*(|\ell(t)|, \vec{x})|, w)) \\ & \quad \wedge \dot{\beta}(Sj, |r^*(|\ell(t)|, \vec{x})|, w) < r(n, \vec{x})) \vee \dot{\beta}(Sj, |r^*(|\ell(t)|, \vec{x})|, w) = r(n, \vec{x})) \end{aligned}$$

and let $B(n, \vec{x})$ be the formula

$$(\exists y \leq r)(\exists w \leq 2^{|\ell(t)| \cdot (|r^*|+1)}) A(n, \vec{x}, z, w, y)$$

Let $F(n, \vec{x}, y)$ denote the formula within the scope of the $(\exists y \leq r)$. This formula is equivalent to a $\hat{\Sigma}^b_i$-formula provably in $\hat{T}_2^{i,|\tau|}$ and we can define f if we can show

$$(\forall \vec{x}, n)(\exists y \leq r) F(|\ell(t(n, \vec{x})|), \vec{x}, y).$$

So it suffices to show $(\forall \vec{x}, n) B(|\ell(t)|, \vec{x})$. The formula B is also equivalent to a $\hat{\Sigma}^b_i$-formula, so $\hat{T}_2^{i,|\tau|}$ can use $IND_B^{|\tau|}$ axioms. Since $\hat{T}_2^{i,|\tau|}$ proves $(\forall \vec{x})(\exists y \leq t_1) G$, it can also prove $B(0, \vec{x})$. Now suppose $\hat{T}_2^{i,|\tau|}$ proves $B(m, \vec{x})$ where $m \leq |\ell(t)|$. So there are v, w, y satisfying $A(m, \vec{x}, w, y)$. If we set $y' = h(m, \vec{x}, y)$, and

$$w' = y' \cdot 2^{\min((m+1) \cdot |r^*|, |\ell(c)| \cdot |r^*|)} + LSP(w, (m+1) \cdot |r^*|)$$

then using Lemma II.C.4 and Lemma II.D.1 which are axioms of $EBASIC$ we can show that $\hat{T}_2^{i,|\tau|}$ proves $A(m+1, \vec{x}, z, w', y')$. Hence, $\hat{T}_2^{i,|\tau|}$ proves $B(m+1, \vec{x})$. By the $IND_B^{|\tau|}$ axioms, the theory $\hat{T}_2^{i,|\tau|}$ proves $(\forall \vec{x}, n) B(|\ell(t)|, \vec{x})$. $\square$

The $\tau = cl$ version of the above theorem shows the $EBASIC = \hat{T}_2^{i,cl}$ can $\hat{\Sigma}_i^b$-define the multifunctions in $B_{i,2}^{|cl|}$. It is not hard to see that $B_{i,2}^{|cl|} = B_{i,2}$ since defining a multifunction using $BPR_2^{|cl|}$ uses only a constant number of iterations, so the same effect can be achieved using a finite number of compositions of multifunctions.

III.C Local search problems

The reason why $\hat{T}_2^{i,\tau}$ cannot necessarily $\hat{\Sigma}_i^b$-define the multifunctions in $B_{i,2}^{\tau}$ is that in general it could take an exponentially long string w to define a function by BPR_2^{τ} using the method of Theorem III.B.1. For example, this would be the case if $\tau = \{id\}$. We know from Buss and Krajíček [12] that the $\hat{\Sigma}_1^b$-consequences of T_2^1 can be characterized by projections of polynomial local search (PLS) problems. The PLS problems were first studied in Papadimitriou and Yannakakis [38]. We modify their definitions to get local search problems which can be used to characterize the $\hat{\Sigma}_i^b$-definable multifunctions of $\hat{T}_2^{i,\tau}$. We use $\tau(L_k)$ to denote terms obtained by substituting L_k-terms into τ terms.

Definition III.C.1 *Let Ψ be a class of multifunctions in L_k and τ a class of terms in L_k. The multifunctions $F_P(a,x)$, and $N_P(a,x) = b$ in Ψ, the single-valued $c_P(a,x)$ in Ψ, $t_P(x)$ in L_k, and $M_P(x)$ in $\tau(L_k)$ define a (Ψ,τ)-local search problem P with input x if*

1. *For all x, $F_P(0,x) > 0$.*
2. *For all x and a, $F_P(N_P(a,x),x) > 0$.*
3. *For all x and a, $F_P(a,x) > 0 \supset a \leq t_P(x)$.*
4. *For all x and a, $\neg(N_P(a,x) = a) \supset c_P(a,x) < c_P(N_P(a,x),x)$.*
5. *For all x and a, $c_P(a,x) < M_P(x)$.*
6. *For all x and a and b, $N_P(a,x) = a \wedge N_P(a,x) = b \supset a = b$.*

A solution $Opt_P(x) = y$ *to the above local search problem is a value* y *such that* $N_P(y, x) = y$. *If a theory* $T \supseteq EBASIC$ *can prove the above conditions hold (including* c_P *being single-valued) then* P *is a* (Ψ, τ)*-local search problem in* T.

The point of the last condition is to insure that N_P is single-valued when $Opt_P(x) = y$. The idea of the above definition is that F is supposed to be a set of feasible answers to the problem P, c is supposed to be a cost function, and N is supposed to return a neighbour to a given feasible answer, and our goal is to find the feasible answer which maximizes the cost. For instance, one can imagine a ticket scalper with one ticket to sell for the Stanley Cup going around outside a hockey rink trying to find the person he can charge the most. He searches around locally outside to find who is willing to pay the most for the ticket and then sells it. There might be other people who would have been willing to pay more for the ticket but not in his nearby vicinity.

One can also define local search classes in terms of minimization and the classes will be equivalent to the ones defined above using the standard trick of Theorem II.C.1 and Theorem II.G.10; however, it is more convenient for us to use maximization principles. The class PLS we mentioned earlier is the class of multi-functions computed by optima of $(\Box_1^p, \{id\})$-local search problems. An interesting problem in PLS is given a weighted graph G, find a travelling salesperson tour T of G that cannot be improved by swapping the successors of two nodes [29]. This problem is based on a popular heuristic for the travelling salesperson problem.

Lemma III.C.2 *If* $(B_{i,2}, \tau)$*-local search problem in* $T \supseteq EBASIC$ *then the above six conditions which are provable in* T *are all* $\forall\hat{\Sigma}_i^b$*-formulas. That is as an universal quantifier followed by a* $\hat{\Sigma}_i^b$*-formula.*

Proof: Using essentially the same proof as Lemma III.A.6, one can show the predicates in $B_{i,2} > 0$ are all expressible by $\hat{\Sigma}_i^b$-formulas. Conditions (1), (2), and (5) are then seen to be equivalent to a $\forall\hat{\Sigma}_i^b$-formula in T since $T \supseteq EBASIC$.

Condition (3) and (6) are equivalent to $\forall\hat{\Pi}^b_i$-formulas and hence, $\forall\hat{\Sigma}^b_{i-1}$-formulas. Lastly, condition (4) consists of a universal quantification of a $\hat{\Pi}^b_i$-formula implying a $\hat{\Sigma}^b_i$-formula and so is equivalent to a $\forall\hat{\Sigma}^b_i$-formula. □

Definition III.C.3 *We define LS^Ψ_τ to be the class of multifunctions which can be computed as optima of (Ψ, τ)-local search problems.*

We define $LS^\Psi_{\tau,T}$ to be the class of multifunctions which can be computed as optima of (Ψ, τ)-local search problems in T.

When the theory is clear we will abuse notation and write LS^Ψ_τ for $LS^\Psi_{\tau,T}$. The next lemma will allow us to show $\hat{T}^{i,\tau}_2$ can define every multifunction in $LS^{B,a}_\tau$.

Lemma III.C.4 $(i \geq 1)$

(a) The theory $\hat{T}^{i,\tau}_2$ and $EBASIC$+$\hat{\Sigma}^b_i$-MIN^τ are the same where the $\hat{\Sigma}^b_i$-MIN^τ axioms are:

$$A(\ell(a)) \supset (\exists x \leq \ell(a))[A(x) \wedge (\forall y < x)(\neg A(y))]$$

for $A \in \hat{\Sigma}^b_i$ and $\ell \in \tau$.

(b) The theory $\hat{T}^{i,\tau}_2$ and $EBASIC$+$\hat{\Sigma}^b_i$-MAX^τ are the same where the $\hat{\Sigma}^b_i$-MAX^τ axioms are:

$$A(0) \supset (\exists x \leq \ell(a))[A(x) \wedge (\forall y \leq \ell(a))(y > x \supset \neg A(y))]$$

for $A \in \hat{\Sigma}^b_i$ and $\ell \in \tau$.

(c) The theory $\hat{T}^{i,\tau}_2$ and $EBASIC$+$\hat{\Pi}^b_{i-1}$-MIN^τ are the same.

(d) The theory $\hat{T}^{i,\tau}_2$ and $EBASIC$+$\hat{\Pi}^b_{i-1}$-MAX^τ are the same.

Proof: (a) The proof of this is essentially from Buss [13]. Let A be a $\hat{\Sigma}^b_i$-formula and let $B(a)$ be the formula $(\forall y \leq a)(\neg A(y))$ where ℓ is in τ. This formula is provably equivalent to a $\hat{\Pi}^b_i$-formula in $EBASIC$, so by $\hat{\Pi}^b_i$-IND^τ we have

$$\neg B(\ell(a)) \supset \neg B(0) \vee (\exists x < \ell(a))(B(x) \wedge \neg B(Sx))$$

and since $A(\ell(a)) \supset \neg B(\ell(a))$ and $A(0) \supset \neg B(0)$, we have

$$A(\ell(a)) \supset A(0) \vee (\exists x < \ell(a))[(\forall z \leq x)(\neg A(z)) \wedge (\exists y \leq Sx)A(y)].$$

From this $EBASIC$ can prove

$$A(\ell(a)) \supset A(0) \vee (\exists y \leq \ell(a))(\forall z < y)(\neg A(z) \wedge A(y))$$

which implies the desired $\hat{\Sigma}^b_i$-MIN^τ axiom.

For the other direction, we show $EBASIC$+$\hat{\Sigma}^b_i$-MIN^τ proves $\hat{\Pi}^b_i$-IND^τ axioms and so contains $\hat{T}^{i,\tau}_2$ by Theorem II.G.10. Let A be a $\hat{\Pi}^b_i$-formula. Then by $\hat{\Sigma}^b_i$-MIN^τ:

$$\neg A(\ell(a)) \supset \neg A(0) \vee (\exists x \leq \ell(a))[\neg A(x) \wedge (\forall y < x)A(y)]$$

and so

$$\neg A(\ell(a)) \wedge A(0) \supset (\exists x)(A(x) \wedge \neg A(Sx))$$

which implies IND^ℓ_A.

(b) To prove the $\hat{\Sigma}^b_i$-MAX^τ axioms for the formula A and the term τ, one only needs to use $\hat{\Sigma}^b_i$-MIN^τ with respect to y on the formula $A(\ell(x) \dot{-} y)$. Similarly, to show $\hat{\Sigma}^b_i$-MIN^τ axioms for the formulas $A(x)$ and the term τ, one only needs to use $\hat{\Sigma}^b_i$-MAX^τ with respect to y one the formula $A(\ell(x) \dot{-} y)$. Thus, $EBASIC$+$\hat{\Sigma}^b_i$-MAX^τ is also equivalent to $\hat{T}^{i,\tau}_2$.

(c) and (d) We show only (c) as (d) is similar. It suffices to show $\hat{\Pi}^b_{i-1}$-MIN^τ implies $\hat{\Sigma}^b_i$-MIN^τ as the other direction is trivial. Suppose $A(x) := (\exists y \leq t)B(x, y)$ is in $\hat{\Sigma}^b_i$ and we want to prove the MIN^ℓ_A for ℓ in τ. Consider the $\hat{\Pi}^b_{i-1}$-formula

$$B^*(w) := B(MSP(w, 2^{|t^*|}), \dot{\beta}(0, |t^*|, t, w)).$$

By using Corollary II.C.4 and Theorem II.C.5 which are axioms of $EBASIC$, $EBASIC$ can prove $(\exists x)A(x) \supset (\exists w)B^*(w)$ by setting w equal to $x \cdot 2^{|t^*|}y$. So given $(\exists x)A(x)$ and using MIN^ℓ_B axioms we get a minimal value w such that $B^*(w)$ holds. Finally, $EBASIC$ can show $x := MSP(w, 2^{|t^*|})$ must be a minimal value

such that $A(x)$. This is because if $A(x')$ for any $x' \leq x$ then there must be some y such that $B(x', y)$ and then $B^*(w')$ for $w' = x' \cdot 2^{|t^*|}y$ and $w' < w$. □

Theorem III.C.5 *($i \geq 1$) Let P be a $(B_{i,2}, \dot{\tau})$-problem in $\hat{T}_2^{i,\tau}$. Then $\hat{T}_2^{i,\tau}$ proves $(\forall x)(\exists y)(Opt_P(x) = y)$. Since $Opt_P(x) = y$ is provably equivalent to a $\hat{\Sigma}_i^b$-formula we get $\hat{T}_2^{i,\tau}$ can $\hat{\Sigma}_i^b$-define the multifunctions in $LS_\tau^{B_{i,2}}$.*

Proof: Let P be a $(B_{i,2}, \dot{\tau})$-problem. Consider the formula

$$A(c) := (\exists a \leq t_P(x))(F_P(a, x) > 0 \wedge c_P(a, x) \geq c)$$

which is provably equivalent to a $\hat{\Sigma}_i^b$-formula in $\hat{T}_2^{i,\tau}$ since $F_P(a, x) > 0$ is provable equivalent $\hat{\Sigma}_i^b$-formula and similarly $c_P(a, x) \geq c$ is equivalent to a $\hat{\Sigma}_i^b$-formula. Using $\hat{\Sigma}_i^b$-MAX^τ, the theory $\hat{T}_2^{i,\tau}$ can prove

$$A(0) \supset$$
$$(\exists c \leq M_P(x))[A(c) \wedge (\forall c' < M_P(x))(c' > c \supset \neg A(c'))].$$

Now $\hat{T}_2^{i,\tau}$ can prove $A(0)$ since 0 is always a solution to a local search problem and all solutions have cost ≥ 0. So this implies $\hat{T}_2^{i,\tau}$ can prove there is a feasible answer c which maximizes the cost. Given the definition of N_P such a value c must satisfy the relation $Opt_P(x) = c$. □

III.D Another pairing function

Our next major goal is to show the converses of Theorem III.B.1 and Theorem III.C.5. We will not reach this goal until Chapter V. Nevertheless, as a first step in this direction we show that $B_{0,2}^\tau = B_{0,2}$ can define a slightly better form of pairing than we have been using up to the present.

Let $B = 2^{|\max(x,y)|+1}$. So B will be longer than either x or y. Hence, we can code pairs as

$$\langle x, y \rangle \quad := \quad (2^{|\max(x,y)|} + y) \cdot B + (2^{|\max(x,y)|} + x).$$

To project out the coordinates from an ordered pair we need the following function which has the effect of deleting the most significant bit of a number.

$$DMSB(x) \;:=\; x \dot{-} \lfloor \tfrac{1}{2} 2^{|x|} \rfloor.$$

Then

$$\beta(1, w) \;:=\; DMSB(LSP(w, \lfloor \tfrac{1}{2}|w| \rfloor)).$$

and

$$\beta(2, w) \;:=\; DMSB(MSP(w, \lfloor \tfrac{1}{2}|w| \rfloor))$$

will return the left and right coordinate respectively of the ordered pair w. (The real Gödel beta function can project out $\beta(i, w)$, the ith element of a sequence w. However, as we never use this function in this thesis we will allow the suggestive notation.) To check if something is an ordered pair one can use the predicate $ispair(w)$ which is true if and only if

$$Bit(w, \lfloor \tfrac{1}{2}|w| \rfloor \dot{-} 1) = 1 \wedge 2 \cdot |\max(\beta(1, w), \beta(2, w))| + 2 = |w|.$$

The above form of pairing can also be done in $EBASIC$. For integers x and y one can show there is a unique pair $w = \langle x, y \rangle$ satisfying $ispair(w)$ and such that $\beta(1, w) = x$ and $\beta(2, w) = y$.

Chapter IV

The sequent calculus and cut-elimination

Until this point we have not been specific about the deduction systems in which we have been carrying out proofs for $\hat{T}_2^{i,\tau}$ and $\hat{C}_2^{i,|\tau|}$. To show the converses of Theorem III.B.1 and Theorem III.C.5; however, we will need to work with proofs in the sequent calculus. We shall use the same formulation of the sequent calculus as in Buss [13] where a basic system called LKB was defined and then augmented with the $BASIC$ axioms and various induction rules. A good reference for material on the sequent calculus is Takeuti [48].

IV.A The sequent calculus

Proofs in the sequent calculus are made up of *sequents*. A sequent is an ordered pair of two finite sequences of formulas represented pictorially as:

$$A_1, \ldots, A_n \to B_1, \ldots, B_m. \tag{IV.1}$$

In the above sequent, the sequence of formulas $A_1, \ldots, A_n$ is called the *antecedent* and the sequence of formulas $B_1, \ldots, B_m$ is called the *succedent*. In general, a sequence of formulas occurring in a sequent is called a *cedent*. We will use capital Greek letters such as Γ and Δ for cedents. The symbol $\to$ is called the *sequent*

arrow. The intended meaning of the sequent (IV.1) is

$$\bigwedge_i A_i \supset \bigvee_j B_j.$$

A sequent calculus proof is usually viewed as a tree of sequents with the result of the proof, the root of the tree called the *endsequent*, appearing at the bottom of the proof, and the leaves of the tree, called *initial sequents*, appearing at the top. The internal nodes of a sequent calculus proof are supposed to follow from their children by means of a deduction called an inference. The types of inferences allowed depend on the version of the sequent calculus being formulated. We will work with the sequent calculus system LKB_k which allows the following rules of inference for sequents of formulas in the language L_k:

Structural Inferences

(contract:right) $\dfrac{\Gamma \to A, A, \Delta}{\Gamma \to A, \Delta}$ (contract:left) $\dfrac{A, A, \Gamma \to \Delta}{A, \Gamma \to \Delta}$

(weaken:left) $\dfrac{\Gamma \to \Delta}{A, \Gamma \to \Delta}$ (weaken:right) $\dfrac{\Gamma \to \Delta}{\Gamma \to A, \Delta}$

(exchange:right) $\dfrac{\Gamma \to \Delta, A, B, \Delta'}{\Gamma \to \Delta, B, A, \Delta'}$ (exchange:left) $\dfrac{\Gamma, A, B, \Gamma' \to \Delta}{\Gamma, B, A, \Gamma' \to \Delta}$

Propositional Inferences

($\neg$:left) $\dfrac{\Gamma \to A, \Delta}{\neg A, \Gamma \to \Delta}$ ($\neg$:right) $\dfrac{A, \Gamma \to \Delta}{\Gamma \to \neg A, \Delta}$

($\wedge$:left1) $\dfrac{A, \Gamma \to \Delta}{A \wedge B, \Gamma \to \Delta}$ ($\wedge$:left2) $\dfrac{A, \Gamma \to \Delta}{B \wedge A, \Gamma \to \Delta}$

($\wedge$:right) $\dfrac{\Gamma \to B, \Delta \qquad \Gamma \to B, \Delta}{\Gamma \to A \wedge B, \Delta}$

(∨:left) $$\frac{A, \Gamma \to \Delta \qquad B, \Gamma \to \Delta}{A \vee B, \Gamma \to \Delta}$$

(∨:right1) $$\frac{\Gamma \to A, \Delta}{\Gamma \to A \vee B, \Delta}$$ (∨:right2) $$\frac{\Gamma \to A, \Delta}{\Gamma \to B \vee A, \Delta}$$

(⊃:left) $$\frac{\Gamma \to A, \Delta \qquad B, \Gamma \to \Delta}{A \supset B, \Gamma \to \Delta}$$

(⊃:right) $$\frac{A, \Gamma \to B, \Delta}{\Gamma \to A \supset B, \Delta}$$

Quantifier Inferences

(∀:left) $$\frac{A(t), \Gamma \to \Delta}{(\forall x)A(x), \Gamma \to \Delta}$$ (∀:right) $$\frac{\Gamma \to A(a), \Delta}{\Gamma \to (\forall x)A(x), \Delta}$$

(∀ ≤:left) $$\frac{A(t), \Gamma \to \Delta}{t \leq s, (\forall x \leq s)A(x), \Gamma \to \Delta}$$

(∀ ≤:right) $$\frac{a \leq s, \Gamma \to A(a), \Delta}{\Gamma \to (\forall x \leq s)A(x), \Delta}$$

(∃:left) $$\frac{A(a), \Gamma \to \Delta}{(\exists x)A(x), \Gamma \to \Delta}$$ (∃:right) $$\frac{\Gamma \to A(t), \Delta}{\Gamma \to (\exists x)A(x), \Delta}$$

(∃ ≤:left) $$\frac{a \leq s, A(a), \Gamma \to \Delta}{(\exists x \leq s)A(x), \Gamma \to \Delta}$$

(∃ ≤:right) $$\frac{\Gamma \to A(t), \Delta}{t \leq s, \Gamma \to (\exists x \leq s)A(x), \Delta}$$

Cut Inference

(Cut) $$\frac{\Gamma \to A, \Delta \qquad A, \Gamma \to \Delta}{\Gamma \to \Delta}$$

The symbols Γ, Δ,Ω, and Λ above are supposed to represent finite sequences of formulas. The t and s which appear in the quantifier inferences must be terms in L_k. The variable a which appears in the quantifier inferences is called an *eigenvariable* and must not occur in the lower sequent. We call the sequents on the top line of an inference *upper sequents* and we call the sequent on the bottom line of an inference the *lower sequent.* The lower sequent of a propositional or quantifier inference contains a newly formed formula which we call the *principal formula* of the inference. The formulas in the upper sequents of a propositional or quantifier inference from which a principal formula is constructed are called *auxiliary formulas.* All other formulas in an inference other than principal and auxiliary formulas are called *side formulas.*

We now describe the two types of initial sequents of in LKB_k proof: logical axioms and equality axioms. A *logical axiom* is a sequent of the form $A \to A$ where A is an atomic formula in L_k. An *equality axiom* is a sequent of the form $\to t_1 = t_1$,

$$t_1 = s_1, \ldots, t_n = s_n \to f(t_1, \ldots, t_n) = f(s_1, \ldots s_n).$$

or

$$t_1 = s_1, \ldots, t_n = s_n, A(t_1, \ldots, t_n) \to A(s_1, \ldots s_n).$$

Here t_i and s_i are L_k-terms, f is a function symbol in L_k, and A is an atomic formula in L_k.

Definition IV.A.1 *An LKB_k-proof is a sequent calculus proof containing L_k-formulas using the above rules of inference and using logical axioms and equality axioms as initial sequents.*

The theory LKB_k is the collection of all sequents viewed as formulas derivable by LKB_k-proofs.

Proposition IV.A.2 *The system LKB_k is consistent, sound, and complete.*

Proof: We refer the reader to Buss [13] and Takeuti [49] for the details. □

Definition IV.A.3 *A* substitution instance *of a formula* $A(a_1, \ldots, a_n)$ *with free variables as indicated is a formula* B *such that* $B = A(t_1, \ldots t_k)$ *where* t_i *are terms.*

Definition IV.A.4 *The sequent calculus formulation of a theory* T *with a set of* L_k*-formulas as axioms is the system* LKB_k *expanded to allow initial sequents of the form* $\rightarrow B$ *where* B *is a substitution instance of an axiom.*

We use the above definition to give a sequent calculus formulation of $EBASIC_k$. To formulate $\hat{T}_2^{i,\tau}$ and $\hat{C}_2^{i,|\tau|}$ we will use the following definitions.

Definition IV.A.5

A Ψ*-*IND^τ *inference is an inference of the form:*

$$\frac{A(b), \Gamma \rightarrow A(Sb), \Delta}{A(0), \Gamma \rightarrow A(\ell(t(x))), \Delta}$$

where b *in the above is an eigenvariable and must not appear in the lower sequent.* t *is in* L_k*.* ℓ *is in* τ*, and* A *is a* Ψ*-formula.*

A Ψ*-*$REPL^{|\tau|}$ *inference is an inference of the form:*

$$\frac{\Gamma \rightarrow (\forall x \leq |\ell(s)|)(\exists y \leq t) A(x, y), \Delta}{\Gamma \rightarrow (\exists w \leq 2 \cdot (t^* \# \ell(s)))(\forall x \leq |\ell(s)|) A(x, \dot{\beta}(x, |t^*|, t, w))), \Delta}$$

where A *is a* Ψ*-formula,* $\ell \in |\tau|$*, and* $s, t \in L_k$*.*

Theorem IV.A.6

The theory of the system LKB_k *expanded to allow* Ψ*-*IND^τ *inferences is the same theory as the system* LKB_k *expanded by* Ψ*-*IND^τ *axioms.*

The theory of the system LKB_k *expanded to allow* Ψ*-*$REPL^{|\tau|}$ *inferences is the same theory as the system* LKB_k *expanded by* Ψ*-*$REPL^{|\tau|}$ *axioms.*

Proof: We show only the first statement as both proofs are not hard and somewhat tedious. Nevertheless, we thought we would provide an illustration of what sequent calculus proofs look like. Let $\ell \in \tau$. We derive the IND_A^ℓ axiom from the rule.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A(a)\rightarrow A(a) \qquad A(Sa)\rightarrow A(Sa)}{A(a)\supset A(Sa), A(a)\rightarrow A(Sa)}}{(\forall x)(A(x)\supset A(Sx)), A(a)\rightarrow A(Sa)}}{(\forall x)(A(x)\supset A(Sx)), A(0)\rightarrow A(\ell(b))}}{(\forall x)(A(x)\supset A(Sx)), A(0)\rightarrow (\forall x)A(\ell(x))}}{A(0)\wedge(\forall x)(A(x)\supset A(Sx)), A(0)\rightarrow(\forall x)A(\ell(x))}}{A(0), A(0)\wedge(\forall x)(A(x)\supset A(Sx))\rightarrow(\forall x)A(\ell(x))}}{A(0)\wedge(\forall x)(A(x)\supset A(Sx)), A(0)\wedge(\forall x)(A(x)\supset A(Sx)\rightarrow(\forall x)A(\ell(x))}}{A(0)\wedge(\forall x)(A(x)\supset A(Sx)\rightarrow(\forall x)A(\ell(x))}}{\rightarrow A(0)\wedge(\forall x)(A(x)\supset A(Sx))\supset(\forall x)A(\ell(x))}$$

For the other direction we first derive

$$A(0)\wedge(\forall x)(A(x)\supset A(Sx))\rightarrow A(\ell(t)) \tag{IV.2}$$

with the proof

$$\dfrac{\dfrac{A(\ell(t))\rightarrow A(\ell(t))}{(\forall x)A(\ell(x))\rightarrow A(\ell(t))} \qquad A(0)\wedge(\forall x)(A(x)\supset A(Sx))\rightarrow A(0)\wedge(\forall x)(A(x)\supset A(Sx))}{A(0)\wedge(\forall x)(A(x)\supset A(Sx))\supset(\forall x)A(\ell(x)), A(0)\wedge(\forall x)(A(x)\supset A(Sx))\rightarrow A(\ell(t))}$$

followed by a cut against IND^{ℓ}_{A}. Then we derive

$$(\forall x)(A(x)\supset A(Sx)), A(0)\rightarrow A(0)\wedge(\forall x)(A(x)\supset A(Sx))$$

with the proof

$$\dfrac{\dfrac{A(0)\rightarrow A(0)}{(\forall x)(A(x)\supset A(Sx)), A(0)\rightarrow A(0)} \qquad \dfrac{\dfrac{(\forall x)(A(x)\supset A(Sx))\rightarrow(\forall x)(A(x)\supset A(Sx))}{A(0), (\forall x)(A(x)\supset A(Sx))\rightarrow(\forall x)(A(x)\supset A(Sx))}}{(\forall x)(A(x)\supset A(Sx)), A(0)\rightarrow(\forall x)(A(x)\supset A(Sx))}}{(\forall x)(A(x)\supset A(Sx)), A(0)\rightarrow A(0)\wedge(\forall x)(A(x)\supset A(Sx))}$$

Cutting against (IV.2) gives us

$$(\forall x)(A(x)\supset A(Sx)), A(0)\rightarrow A(\ell(t)) \tag{IV.3}$$

Given a proof of the upper sequent $A(a), \Gamma\rightarrow\Delta, A(Sa)$ of the induction rule we derive

$$\dfrac{\Gamma\rightarrow\Delta, A(a)\supset A(Sa)}{\Gamma\rightarrow\Delta, (\forall x)(A(x)\supset A(Sx))}$$

Cutting against the (IV.3) yields the lower sequent of the induction rule. □

Given Theorem IV.A.6 we are justified in the next definition:

Definition IV.A.7

$\hat{T}_k^{i,\tau}$ is the sequent calculus theory of the system LKB_k expanded with $EBASIC_k$ axioms and $\hat{\Sigma}_i^b$-IND^τ inferences.

$\hat{C}_k^{i,|\tau|}$ is the sequent calculus theory of the system LKB_k expanded with $EBASIC_k$ axioms, open-IND^τ inferences, and $\hat{\Pi}_i^b$-$REPL^{|\tau|}$ inferences.

IV.B Cut-elimination and Parikh's Theorem

The reason we formulate proofs over the sequent calculus is that they have a particularly nice normal form which we will discuss after the following definitions:

Definition IV.B.1 *Let C be a formula in a sequent calculus proof P in the language L_k. The* successor *of C is a formula in the sequent directly below C defined according to the following cases:*

1. *If C is in the endsequent of P or C is a cut-formula, then C has no successor.*
2. *If C is the auxiliary formula of an LKB_k inference or of a $REPL^{|\tau|}$ inference, then the principal formula of the inference is the successor of C.*
3. *If C is one of the formulas A or B in an exchange inference, the successor of C is the formula denoted by the same letter in the lower sequent.*
4. *If C is a side formula in the upper sequent of an inference, then the corresponding side formula in the lower sequent, is its successor.*
5. *If C is the left (resp. right) auxiliary formula of an induction inference, then the successor of C is the left (resp. right) principal formula of the inference.*

A formula C is an *ancestor* of D in a sequent calculus proof P if there is a sequence of formulas $C = C_1, \ldots, C_n = D$ such that for each i the formula C_{i-1} is a successor in P of the formula C_i.

We call C a *direct ancestor* of D in a sequent calculus proof if C is an ancestor of D, and the formulas C and D are different occurences of the same formula.

If C is an ancestor of D then we call D a *descendant* of C. Similarly, D is called a *direct descendant* of C if C is a direct ancestor of D.

Definition IV.B.2 *A formula A in a sequent calculus proof is* free *if and only if it is not directly descended from a principal formula of a non-LKB_k inference and also not directly descended from an initial sequent.*

A cut inference is free *if and only if both of the cut formulas in the upper sequent are free.*

A sequent calculus proof is free-cut free *if it has no free cuts.*

The normal form for sequent calculus proofs is given by the following cut-elimination theorem.

Theorem IV.B.3 ($i \geq 0, k \geq 1$) *Suppose $\Gamma \rightarrow \Delta$ is provable in the sequent calculus formulation of $EBASIC_k$, $\hat{T}_k^{i,\tau}$, or $\hat{C}_k^{i,\tau}$. Then there is a free-cut free proof of $\Gamma \rightarrow \Delta$ in the same theory.*

Proof: The proof is essentially the same as in Takeuti [48], pp22-29,111-112 and in Buss [13]. □

Given a set Ψ of prenex formulas let $L\Psi$ be the class of formulas which can be made into formulas in the set Ψ by padding the left hand side with zero or more dummy quantifiers. The next corollary is the primary reason why we will use the sequent calculus and in particular why we formulate $\hat{T}_2^{i,\tau}$ aand $\hat{C}_2^{i,|\tau|}$ with rules of inference rather just axioms. The proof is from Buss [13] modified slightly to the prenex setting. We write $|A|_{|\tau|}$ to mean a quantifier of the form $(\forall x \leq |\ell(t)|)$ where ℓ is in $|\tau|$ and t is in L_2.

Corollary IV.B.4 ($i \geq 0, k \geq 1$)

Let $\Psi \supseteq L\hat{\Sigma}^b_{i,k}$ be a set of L_k-formulas such that any subformula of a Ψ-formula is a Ψ-formula. Let $\Gamma \to \Delta$ be a sequent of Ψ-formulas provable in $EBASIC_k$, $\hat{T}^{i,\tau}_k$. Then $\Gamma \to \Delta$ is provable in the same theory by a proof in which only Ψ-formulas occur.

Let Ψ containing

$$L|A|_{|\tau|}\hat{\Sigma}^b_{i+1} \cup LE|A|_{|\tau|}\hat{\Pi}^b_i.$$

be a set of L_k-formulas such that any subformula of a Ψ-formula is a Ψ-formula and such that Ψ is closed under L_k-term substitution. Let $\Gamma \to \Delta$ be a sequent of Ψ-formulas provable in $\hat{C}^{i,\tau}_k$. Then $\Gamma \to \Delta$ is provable in the same theory by a proof in which only Ψ-formulas occur.

Proof: Both statements are proven in essentially the same way so we only prove the first one. Let P be a free cut-free proof of $\Gamma \to \Delta$, a sequent of Ψ-formulas. Suppose C is a formula in P and $C \notin \Psi$. As $\Psi \supset L\hat{\Sigma}^b_{i,k}$, C cannot be a direct descendant of the principal formula of an induction inference or the direct descendent of an initial sequent. Hence, C is free and all of its descendants must be free. Since P is free-cut free, some descendant C' of C must appear in the endsequent. As $C \notin \Psi$ is a subformula of C', we have also that $C' \notin \Psi$. This contradicts the fact that $\Gamma \to \Delta$ is a sequent of Ψ-formulas. □

In particular, Corollary IV.B.4 says a sequent of $L\hat{\Sigma}^b_i$-formulas provable in $\hat{T}^{i,\tau}_2$ has a $\hat{T}^{i,\tau}_2$-proof in which only $L\hat{\Sigma}^b_i$-formulas occur.

Another important theorem provable from the cut-elimination theorem is the following variant of Parikh's Theorem [39].

Theorem IV.B.5 *($i \geq 0, k \geq 1$) Suppose $(\forall x)(\exists y)A(x,y)$ is provable in one of the theories $EBASIC_k$, $\hat{T}^{i,\tau}_k$, or $\hat{C}^{i,\tau}_k$ where A is a bounded formula, then there is a term t in L_k such that in fact $(\forall x)(\exists y < t)A(x,y)$ is provable in the theory.*

This theorem holds in a more general theories than we give above. We ask the reader to consult either Hájek and Pudlák [24] or Buss [13] for a proof.

IV.C $\hat{\Sigma}_i^b$ versus $\hat{\Pi}_{i-1}^b$-definability

In this section, we give a simple application of Parikh's Theorem.

Definition IV.C.1 *The function $f(x) = \beta(1, g(x))$ is called a* projection *of $g(x)$.*

We define $\pi\Psi$ to be class of multifunctions which are projections of multifunctions in Ψ.

The reason why we are interested in projections is that we will show the $\hat{\Sigma}_i^b$-definable multifunctions of $\hat{T}_2^{i,\tau}$ are precisely the class $\pi LS_{\dot{\tau}}^{B_{i,2}}$. It is unknown if the $LS_{\dot{\tau}}^{B_{i,2}}$ is closed under composition. This is also open for PLS. This suggests that $LS_{\dot{\tau}}^{B_{i,2}}$ might more naturally correspond to some weaker notion of definability. We show below two weaker notions of definability which are not necessarily closed under composition but whose projections are equivalent to $\hat{\Sigma}_i^b$-definability. We make no claim about a connection between these notions of definability and local search. However, we will discuss this problem a bit more after our results in the next chapter.

Theorem IV.C.2 *Let $T \supseteq EBASIC$ be a theory in which Parikh's Theorem holds. A multifunction is $\hat{\Sigma}_i^b$-definable in T if and only it is a projection of a $\hat{\Pi}_{i-1}^b$-definable multifunction in T.*

Proof: Suppose f is $\hat{\Sigma}_i^b$-definable in T with by the formula

$$B_f(x, y) := (\exists z \leq s) A_f(x, y, z)$$

where A_f is $\hat{\Pi}_{i-1}^b$. By Parikh's Theorem T proves $(\exists y \leq t) B_f(x, y)$. So f can be defined as a projection of a $\hat{\Pi}_{i-1}^b$-definable function by proving

$$(\exists z)(\exists w \leq 2^{2 \cdot |\max(s,t)|})(A_f(x, \beta(1, w), \beta(2, w)) \wedge z = \beta(1, w)).$$

On the other hand, consider a projection of a $\hat{\Pi}_{i-1}^b$-definable multifunction f. Let f be defined by the formula $A_f(x, y)$. By Parikh's Theorem, T proves $(\exists y \leq$

$t)A_f(x,y)$. This last formula is provably equivalent to a $\hat{\Sigma}_i^b$-formula. The theory T can thus $\hat{\Sigma}_i^b$-define its projection by proving

$$(\exists z)(\exists y \leq t)[A_f(x,y) \wedge \beta(1,y) = z].$$

□

Corollary IV.C.3 *Let $T \supseteq EBASIC$ be a theory in which Parikh's Theorem holds. A multifunction is $\hat{\Sigma}_i^b$-definable in T if and only it is a projection of a $\hat{\Delta}_i^b$-definable multifunction in T.*

Proof: The proof is essentially the same as Theorem IV.C.2. If f is $\hat{\Sigma}_i^b$-definable it is projection of $\hat{\Pi}_{i-1}^b$-definable multifunction and hence, it is a projection of a $\hat{\Delta}_i^b$-definable multifunction. On the other hand, consider a projection of a $\hat{\Delta}_i^b$-definable multifunction f. Let f be defined by the formula $A_f(x,y)$. By Parikh's Theorem, T proves $(\exists y \leq t)A_f(x,y)$. Since A_f is $\hat{\Delta}_i^b$ with respect to T, this last formula is provably equivalent to a $\hat{\Sigma}_i^b$-formula. The theory T can thus $\hat{\Sigma}_i^b$-define its projection by proving

$$(\exists z)(\exists y \leq t)[A_f(x,y) \wedge \beta(1,y) = z].$$

□

Chapter V

Definability and the witnessing argument

In this chapter we show the converses of Theorem III.B.1 and Theorem III.C.5. So we show the $\hat{\Sigma}^b_i$-definable multifunctions of $\hat{T}^{i,|\tau|}_2$ are precisely the $B^{|\tau|}_{i,2}$ multifunctions. As corollaries to this characterization we get characterizations of the $\hat{\Sigma}^b_i$-definable multifunctions of S^i_2, $\hat{R}^i_2$, and $\hat{T}^{i,m}_2$. We also get a characterization of the $\hat{\Sigma}^b_{i-j}$-consequences of $\hat{T}^{i,m,j}_2$. In Chapter VI we will show for $i \geq 1$ the algebra $B^{|\tau|}_{i+1,2}$ equals the class $FP^{\Sigma^p_i}(wit, |\tau^{\#}|)$.

We conclude this chapter with some remarks about theories defined with prefix induction schemes.

V.A The witness predicate

Let T be one of the theories $EBASIC_2$, $\hat{T}^{i,\tau}_2$, or $\hat{C}^{i,\tau}_2$. In view of Theorem IV.B.5, T can $\hat{\Sigma}^b_i$-define a function f if and only if there is a $\hat{\Sigma}^b_i$-formula $A_f(x,y)$ such that T proves $(\forall x)(\exists! y \leq t)A_f(x,y)$. To define a multifunction one does not have to show uniqueness. A formula is an $E\hat{\Sigma}^b_i$-formula if it is of the form $(\exists y \leq t)A$ where A is a $\hat{\Sigma}^b_i$-formula. Because of the cut-elimination theorem all the formulas in a free cut-free $\hat{T}^{i,\tau}_2$-proof of a sequent of $LE\hat{\Sigma}^b_i$-formulas will be in $LE\hat{\Sigma}^b_i$. We define a witness predicate in the following manner.

If $A(\vec{a}) \in L\hat{\Pi}^b_{i-1}$ then

$$Wit^i_A(w, \vec{a}) \;:=\; A(\vec{a})$$

If $A(\vec{a})$ is of the form $(\exists x \leq t(\vec{a}))B$ where $A \in \hat{\Sigma}^b_i$ then

$$Wit^i_A(w, \vec{a}) \;:=\; w \leq t(\vec{a}) \wedge B(w, \vec{a})$$

If $A(\vec{a})$ is of the form $(\exists x_1 \leq t_1)(\exists x_2 \leq t_2)B$ where $A \in E\hat{\Sigma}^b_i$ then

$$\begin{aligned} Wit^i_A(w, \vec{a}) \;:=\; & ispair(w) \wedge \beta(1, w) \leq t_1 \wedge \beta(2, w) \leq t_2 \wedge \\ & B(\beta(1, 2), \beta(2, w), \vec{a}). \end{aligned}$$

Thus, if A is in $LE\hat{\Sigma}^b_i$ then Wit^i_A will be provably equivalent in $EBASIC$ to a $\hat{\Pi}^b_{i-1}$-formula. The witness predicate as defined above is a simplified version of the witness predicate defined in Buss [13]. The simplification arises because we are working in the prenex setting. It is easy to prove from the definition of witness the following useful properties.

Lemma V.A.1 ($i \geq 1$) *Let A be any $LE\hat{\Sigma}^b_i$-formula with free variables $\vec{a}$. Then:*

$$EBASIC \vdash Wit^i_A(w, \vec{a}) \supset A(\vec{a}). \tag{V.1}$$

There is a term t_A such that

$$EBASIC \vdash A(\vec{a}) \Leftrightarrow (\exists w \leq t_A(\vec{a}))Wit^i_A(w, \vec{a}). \tag{V.2}$$

For this term t_A we also have

$$EBASIC \vdash Wit^i_A(w, \vec{a}) \supset w \leq t_A. \tag{V.3}$$

Proof:

(V.1) This statement is immediate from the definition of Wit^i_A.

(V.2) If A is in $\hat{\Sigma}^b_i$ then t_A is just the bounds on the outermost existential quantifier. Otherwise, if the outermost two existential quantifiers are bounded by t_1 and t_2, their pair will be bounded by $2^{2\cdot(\max(t_1,t_2)+1)}$.

(V.3) Follows from (V.2) and the definition of Wit^i_A. In particular, the definition of *ispair* forces any pair for a witness to be unique □

For a cedent of formulas $\Gamma = \{A_1, \ldots, A_n\}$ we use $\vee\Gamma$ (resp. $\wedge\Gamma$) to denote the disjunction (resp. conjunction) of its formulas. We write $w = \langle\langle w_1, \cdots, w_n\rangle\rangle$ to denote pairings of the form $\langle w_1, \langle w_2, \cdots, \langle w_{n-1}, w_n\rangle \cdots\rangle\rangle$. We will use this convention for defining witnesses for $Wit^i_{\wedge\Gamma}$ and $Wit^i_{\vee\Gamma}$.

We define $Wit^i_{\wedge\Gamma}(w, \vec{a})$ by induction. If Γ is empty define $Wit^i_{\wedge\Gamma}(w, \vec{a})$ to be $0 = 0$. If Γ consists of a single formula A then $Wit^i_{\wedge\Gamma}(w, \vec{a})$ is $Wit^i_A(w, \vec{a})$. Otherwise, if Γ is a cedent of formulas $\Gamma = \{A_1, \ldots, A_n\}$, let Γ' be $\{A_2, \ldots, A_n\}$ and define $Wit^i_{\wedge\Gamma}(w, \vec{a})$ to be

$$Wit^i_{A_1}(\beta(1, w), \vec{a}) \wedge Wit_{\Gamma'}(\beta(2, w), \vec{a}).$$

Now we inductively define $Wit^i_{\vee\Gamma}(w, \vec{a})$. If Γ is empty define $Wit^i_{\vee\Gamma}(w, \vec{a})$ to be $\neg(0 = 0)$. If Γ consists of a single formula A then $Wit^i_{\vee\Gamma}(w, \vec{a})$ is $Wit^i_A(w, \vec{a})$. Otherwise, if Γ is a cedent of formulas $\Gamma = \{A_1, \ldots, A_n\}$, let Γ' be $\{A_2, \ldots, A_n\}$ and define $Wit^i_{\vee\Gamma}(w, \vec{a})$ to be

$$(Wit^i_{A_1}(\beta(1, w), \vec{a}) \wedge w_1 \leq t_{A_1}) \vee Wit^i_{\Gamma'}(\beta(2, w), \vec{a})$$

where t_{A_1} is the term from Lemma V.A.1.

From the above definitions it follows that both $Wit^i_{\wedge\Gamma}$ and $Wit^i_{\vee\Gamma}$ are provably equivalent to $\hat{\Pi}^b_{i-1}$-formulas in $EBASIC$. From the definition of witness for a cedent it is also easy to prove the following lemma.

Lemma V.A.2 ($i \geq 1$) *Let Γ be a cedent of $LE\hat{\Sigma}^b_i$-formula with free variables $\vec{a}$. There is a term t_Γ such that*

$$EBASIC \vdash Wit^i_{\wedge\Gamma}(w, \vec{a}) \supset w \leq t_\Gamma$$

and

$$EBASIC \vdash Wit^i_{\vee\Gamma}(w, \vec{a}) \supset w \leq t_\Gamma.$$

We also have

$$EBASIC \vdash (\exists w \leq t_\Gamma) Wit^i_{\wedge\Gamma}(w, \vec{a}) \rightarrow (\exists w \leq t_\Delta) Wit^i_{\vee\Delta}(w, \vec{a})$$

if and only if

$$EBASIC \vdash \Gamma \rightarrow \Delta.$$

Proof: This follows from the definition of witness for a cedent, the fact that witnesses for a cedent are made up of pairings, and by the bounds for witnesses for formulas given by Lemma V.A.1. □

V.B Witnessing arguments

The next theorem implies the $\hat{\Sigma}^b_i$-definable multifunctions of $\hat{T}^{i,|\tau|}_2$ are contained in $B^{|\tau|}_{i,2}$. With Theorem III.B.1 we have the $\hat{\Sigma}^b_i$-definable functions of $\hat{T}^{i,|\tau|}_2$ are precisely the functions in $B^{|\tau|}_{i,2}$.

Theorem V.B.1 ($i \geq 1$) *Suppose $\hat{T}^{i,|\tau|}_2 \vdash \Gamma \rightarrow \Delta$ where Γ and Δ are cedents of $LE\hat{\Sigma}^b_i$-formulas. Let $\vec{a}$ be the free variables in this sequent. Then there is a $B^{|\tau|}_{i,2}$ multifunction f which is $\hat{\Sigma}^b_i$-defined in $\hat{T}^{i,|\tau|}_2$ such that:*

$$\hat{T}^{i,|\tau|}_2 \vdash Wit^i_{\wedge\Gamma}(w, \vec{a}) \supset Wit^i_{\vee\Delta}(f(w, \vec{a}), \vec{a}).$$

Similarly, suppose $EBASIC \vdash \Gamma \rightarrow \Delta$ where Γ and Δ are cedents of $LE\hat{\Sigma}^b_i$-formulas. Let $\vec{a}$ be the free variables in this sequent. Then there is a $B_{i,2}$-multifunction f which is $\hat{\Sigma}^b_i$-defined in $EBASIC$ such that:

$$EBASIC \vdash Wit^i_{\wedge\Gamma}(w, \vec{a}) \supset Wit^i_{\vee\Delta}(f(w, \vec{a}), \vec{a}).$$

Proof: This is proved by induction on the number of sequents in an $\hat{T}_2^{i,\tau}$-proof (resp. $EBASIC$-proof) of $\Gamma \rightarrow \Delta$. By cut elimination, we can assume all the sequents in the proof are in $L\hat{\Sigma}_i^b$. In the base case, the proof consists of a logical axiom, an equality axiom, or an $EBASIC$ axiom. In each of these cases the witness predicate is the original formula. So we can choose f to be the identity function. To define f for logical inferences or for the structural inferences is reasonably easy. For instance, consider the ($\wedge$: right case).

($\wedge$:right case) Suppose we have the inference:

$$\frac{\Gamma \rightarrow A, \Delta \qquad \Gamma \rightarrow B, \Delta}{\Gamma \rightarrow A \wedge B, \Delta}$$

By the induction hypothesis there are $g, h \in B_{i,2}^{|\tau|}$ such that

$$\begin{aligned} \hat{T}_2^{i,|\tau|} &\vdash Wit^i_{\wedge\Gamma}(w,\vec{a}) \supset Wit^i_{A\vee\Delta}(g(w,\vec{a}),\vec{a}) \\ \hat{R}_2^i &\vdash Wit^i_{\wedge\Gamma}(w,\vec{a}) \supset Wit^i_{B\vee\Delta}(h(w,\vec{a}),\vec{a}). \end{aligned}$$

As $Wit^i_{\vee\Delta}$ is provably equivalent to a $\hat{\Pi}^b_{i-1}$-formula in $EBASIC$, by Lemma III.A.6, there is a relation $f_W = 0$ in $B_{i,2} = 0$, which expresses $Wit^i_{\vee\Delta}$. We define the function k as

$$k(v,w,\vec{a}) = cond(f_W(v,\vec{a}), v, w)$$

So k will be a predicate in $B_{i,2} \subset B_{i,2}^{|\tau|}$. Now define f by

$$f(w,\vec{a}) \;=\; \langle 0, k(\beta(2, g(w,\vec{a}), \beta(2, h(w,\vec{a})), \vec{a}\rangle.$$

The formula $A \wedge B$ must be open as it is an $L\hat{\Sigma}_i^b$-formula. So $Wit^i_{A\wedge B} = A \wedge B$ and we do not need a witness for this formula. The function f is obviously in $B_{i,2}^{|\tau|}$ and it provides a witness, if needed, to the remaining formulas in the succedent. So

$$\hat{T}_2^{i,|\tau|} \vdash Wit^i_{\wedge\Gamma}(w,\vec{a}) \supset Wit^i_{A\wedge B\vee\Delta}(f(w,\vec{a}),\vec{a}).$$

The $EBASIC$ version of this case is handled in the same way.

We now prove the remaining cases.

(Cut rule case) Suppose we have the inference:

$$\frac{\Gamma \to A, \Delta \qquad A, \Gamma \to \Delta}{\Gamma \to \Delta}$$

By the induction hypothesis there are $g, h \in B_{i,2}^{|\tau|}$ such that

$$\begin{aligned} \hat{T}_2^{i,|\tau|} &\vdash Wit^i_{\wedge\Gamma}(w, \vec{a}) \supset Wit^i_{A \vee \Delta}(g(w, \vec{a}), \vec{a}) \\ \hat{T}_2^{i,|\tau|} &\vdash Wit^i_{A \wedge \Gamma}(w, \vec{a}) \supset Wit^i_{\vee\Delta}(h(w, \vec{a}), \vec{a}). \end{aligned}$$

We define the function k as

$$k(v, w, \vec{a}) = cond(f_W(v, \vec{a}), v, w)$$

Here f_W is as in the $\wedge$:right case. We define the function f to be

$$f(w, \vec{a}) = k(\beta(2, g(w, \vec{a})), h(\langle \beta(1, g(w, \vec{a})), w \rangle, \vec{a}).$$

Clearly, f is in $B_{i,2} \subset B_{i,2}^{|\tau|}$ and it is easy to see that

$$\hat{T}_2^{i,|\tau|} \vdash Wit^i_{\wedge\Gamma}(w, \vec{a}) \supset Wit^i_{\vee\Delta}(f(w, \vec{a}), \vec{a}).$$

Again, the $EBASIC$ version of this case is handled in the way.

($\exists$:left case) Suppose we have the inference:

$$\frac{b \leq t, A(b), \Gamma \to \Delta}{\exists x \leq t A(x), \Gamma \to \Delta}$$

By the induction hypothesis there is a $g \in B_{i,2}^{|\tau|}$ such that

$$\hat{T}_2^{i,|\tau|} \vdash Wit^i_{b \leq t \wedge A \wedge \Gamma}(w, \vec{a}, b) \supset Wit^i_{\vee\Delta}(g(w, \vec{a}, b), \vec{a}, b).$$

There are three subcases to consider. In each case, we need some way to determine a value for the free variable b and then run g using that value. First, suppose $(\exists x \leq t) A(x)$ is an $E\hat{\Sigma}_i^b$-formula. If w is a witness for $(\exists x \leq t) A(x) \wedge \Gamma$, then $\beta(1, (\beta(1, w))$ is a value for b such that $A(b)$ holds and $\beta(2, \beta(1, w))$ is a witness for $A(b)$. So let our new witness function be

$$f(w, \vec{a}) = g(\langle\langle 0, \beta(2, \beta(1, w)), \beta(2, w)\rangle\rangle, \vec{a}, \beta(1, \beta(1, w))).$$

It is easy to see that

$$\hat{T}_2^{i,|\tau|} \vdash Wit^i_{(\exists x \le t)A \wedge \Gamma}(w, \vec{a}) \supset Wit^i_{\vee \Delta}(f(w, \vec{a}), \vec{a}).$$

In the second case suppose $(\exists x \le t)A(x)$ is an $\hat{\Sigma}^b_i$-formula. If w is a witness for $(\exists x \le t)A(x) \wedge \Gamma$, then $\beta(1, w)$ is a value for b such that $A(b)$ holds. Let our new witness function be

$$f(w, \vec{a}) = g(\langle\langle 0, 0, \beta(2, w)\rangle\rangle, \vec{a}, \beta(1, w)).$$

It is easy to see that

$$\hat{T}_2^{i,|\tau|} \vdash Wit^i_{(\exists x \le t)A \wedge \Gamma}(w, \vec{a}) \supset Wit^i_{\vee \Delta}(f(w, \vec{a}), \vec{a}).$$

The last case is when $(\exists x \le t)A(x) \in L\hat{\Sigma}^b_{i-2}$. (Notice by the definitions of $\hat{\Sigma}^b_i$ and $\hat{\Pi}^b_i$ if $(\exists x \le t)A(x) \in L\hat{\Pi}^b_{i-1}$ then $(\exists x \le t)A(x) \in L\hat{\Sigma}^b_{i-2}$. So $(\exists x \le t)A(x) \in L\hat{\Sigma}^b_{i-2}$ is the only remaining case.) In this case, let f_A be the multifunction in $B_{i-1,2}$ which by Lemma III.A.6 has the property that $f_A(x) = 0$ iff $A(x)$. We define f to be the same as in the above case except rather than use $\beta(1, \beta(1, w))$ to give a value b we instead use the $B_{i,2} \subset B^{|\tau|}_{i,2}$ multifunction $(Wx \le t)[f_A(x) = 0]$ to give a value for b. Note if $(\exists x \le t)A(x) \in \hat{\Sigma}^b_0$ then t is sharply bounded and A is open so this function is definable in $B_{1,2}$.

As usual we can do the $EBASIC$ version of this case in the same way.

($\exists$:right case) Suppose we have the inference:

$$\frac{\Gamma \rightarrow A(t), \Delta}{t \le s, \Gamma \rightarrow (\exists x \le s)A(x), \Delta}$$

By the induction hypothesis there is a $g \in B^{|\tau|}_{i,2}$ such that

$$\hat{T}_2^{i,|\tau|} \vdash Wit^i_{\wedge \Gamma}(w, \vec{a}) \supset Wit^i_{A(t) \vee \Delta}(g(w, \vec{a}), \vec{a}).$$

The definition of Wit^i implies

$$\hat{T}_2^{i,|\tau|} \vdash Wit^i_{t \le s \wedge \Gamma}(w, \vec{a}) \supset t \le s \wedge Wit^i_{\wedge \Gamma}(\beta(2, w), \vec{a}).$$

So if A is a $\hat{\Sigma}^b_i$-formula we define f to be

$$f(w,\vec{a}) \;:=\; \langle\langle t(\vec{a}), \beta(1, g(\beta(2,w),\vec{a})\rangle, \beta(2, g(\beta(2,w),\vec{a}))\rangle$$

If A is a $\hat{\Pi}^b_{i-1}$-formula we define f to be

$$f(w,\vec{a}) \;:=\; \langle t(\vec{a}), \beta(2, g(\beta(2,w),\vec{a}))\rangle$$

For all other A we define f to be

$$f(w,\vec{a}) \;:=\; g(\beta(2,w),\vec{a}))$$

These functions are all $B^{|\tau|}_{i,2}$ and it is not hard to see that

$$\hat{T}^{i,|\tau|}_2 \vdash Wit^i_{t\le s\wedge\Gamma}(w,\vec{a}) \supset Wit^i_{(\exists x\le s)A(x)\vee\Delta}(f(w,\vec{a}),\vec{a}).$$

This same method handles the $EBASIC$ version of this case.

(∀:left case) Suppose we have the inference:

$$\frac{A(t),\Gamma\rightarrow\Delta}{t\le s,(\forall x\le s)A(x),\Gamma\rightarrow\Delta}$$

By the induction hypothesis there is a $g\in B^{|\tau|}_{i,2}$ such that

$$\hat{T}^{i,|\tau|}_2 \vdash Wit^i_{A(t)\wedge\Gamma}(w,\vec{a}) \supset Wit^i_{\vee\Delta}(g(w,\vec{a}),\vec{a}).$$

The definition of Wit^i implies

$$\hat{T}^{i,|\tau|}_2 \vdash Wit^i_{t\le s\wedge(\forall x\le s)A(x)\wedge\Gamma}(w,\vec{a}) \supset t\le s\wedge Wit^i_{(\forall x\le s)A(x)\wedge\Gamma}(\beta(2,w),\vec{a}).$$

By cut-elimination every sequent in the proof is in $LE\hat{\Sigma}^b_i$, so $(\forall x\le s)A(x)$ is in $L\hat{\Pi}^b_{i-1}$. We define f to be

$$f(w,\vec{a}) \;:=\; g(\beta(2,w),\vec{a})$$

This function is in $B^{|\tau|}_{i,2}$ and it is not hard to see that

$$\hat{T}^{i,|\tau|}_2 \vdash Wit^i_{t\le s\wedge(\forall x\le s)A(x)\wedge\Gamma}(w,\vec{a}) \supset Wit^i_{\vee\Delta}(f(w,\vec{a}),\vec{a}).$$

This same method handles the $EBASIC$ version of this case.

(∀:right case) Suppose we have the inference:

$$\frac{b \leq t, \Gamma \rightarrow A(b), \Delta}{\Gamma \rightarrow (\forall x \leq t) A(x), \Delta}$$

By the induction hypothesis there is a $g \in B^{|\tau|}_{i,2}$ such that

$$\hat{T}^{i,|\tau|}_2 \vdash Wit^i_{b \leq t \wedge \Gamma}(w, \vec{a}, b) \supset Wit^i_{A \vee \Delta}(g(w, \vec{a}, b), \vec{a}, b).$$

By cut-elimination, $(\forall x \leq t) A(x) \in L\hat{\Pi}^b_{i-1}$. Since A is in $L\hat{\Sigma}^b_{i-2}$ by Lemma III.A.6 there is a multifunction $f_{\neg A}$ in $B_{i-1,2}$ with the property that $f_{\neg A}(x) = 0$ iff $\neg A(x)$. Let $h(w, \vec{a})$ be the $(Wx \leq t)[f_{\neg A(x)} = 0]$ and define f to be $g(\langle 0, w \rangle, \vec{a}, h(w, \vec{a}))$. It is not hard to see that f the desired properties. Note if $(\forall x \leq t) A(x) \in \hat{\Pi}^b_0$ then t is sharply bounded and A is open so we can define this function in $B^{|\tau|}_{1,2}$.

This same method handles the $EBASIC$ version of this case.

($\hat{\Sigma}^b_i$-$IND^{|\tau|}$ case) Suppose we have the inference:

$$\frac{A(b), \Gamma \rightarrow A(Sb), \Delta}{A(0), \Gamma \rightarrow A(|\ell(t)|), \Delta}$$

where ℓ is in $|\tau|$. By the induction hypothesis there is a $g \in B^{|\tau|}_{i,2}$ such that

$$\hat{T}^{i,|\tau|}_2 \vdash Wit^i_{A(b) \wedge \Gamma}(w, \vec{a}) \supset Wit^i_{A(Sb) \vee \Delta}(g(w, \vec{a}), \vec{a}).$$

Let $h(m, w, \vec{a}, b)$ be the function defined by

$$cond(Wit^i_{A(Sb) \vee \Delta}(m, \vec{a}, b), m, g(\langle m, \beta(2, w) \rangle, \vec{a}, b))$$

Define the function f by $BPR^{|\tau|}_2$ in the following way

$$\begin{aligned} F(0, w, \vec{a}) &= \langle \beta(1, w), 0 \rangle \\ F(b+1, w, \vec{a}) &= \min(h(F(b, w, \vec{a}), w, \vec{a}, b), t_{\vee \Delta \vee A(Sb)}) \end{aligned}$$

Define $f(u, w, \vec{a}) := h(\min(u, |\ell(t)|), w, \vec{a})$. Recall $t_{\vee \Delta \vee A(Sb)}$ is the term guaranteed to bound a witness for $A(Sb) \vee \Delta$ by Lemma V.A.2. It is easy to see

$$\hat{T}^{i,|\tau|}_2 \vdash Wit^i_{A(0) \wedge \Gamma}(w, \vec{a}) \supset Wit^i_{A(0) \vee \Delta}(f(0, w, \vec{a}), \vec{a})$$

From this one can then show that

$$\hat{T}_2^{i,|\tau|} \vdash Wit^i_{A(0)\wedge\Gamma}(w,\vec{a}) \wedge Wit^i_{A(b)\vee\Delta}(f(b,w,\vec{a}),b,\vec{a}) \supset Wit^i_{A(Sb)\vee\Delta}(f(Sb,w,\vec{a}),Sb,\vec{a}).$$

Since t is in $|\tau|$, it then follows by $\hat{\Sigma}^b_i$-$IND^{|\tau|}$ that

$$\hat{T}_2^{i,|\tau|} \vdash Wit^i_{A(0)\wedge\Gamma}(w,\vec{a}) \supset Wit^i_{A(|\ell(t)|)\vee\Delta}(f(|\ell(t)|,w,\vec{a}),\vec{a}).$$

This case does not come up for $EBASIC$.

This completes all possible cases and the proof. □

We get a similar result to the above theorem for the theories $\hat{T}_2^{i,\tau}$ and the class $LS_{\dot{\tau}}^{B_{i,2}}$. We will discuss relationships between our results and the results of Buss and Krajíček [12] after Corollary V.B.3.

Theorem V.B.2 ($i \geq 1$) *Suppose* $\hat{T}_2^{i,\tau} \vdash \Gamma \to \Delta$ *where* Γ *and* Δ *are cedents of* $LE\hat{\Sigma}^b_i$*-formulas. Let* $\vec{a}$ *be the free variables in this sequent. Then there is a* $(B_{i,2},\dot{\tau})$*-problem* P *in* $\hat{T}_2^{i,\tau}$ *such that:*

$$\hat{T}_2^{i,\tau} \vdash Wit^i_{\wedge\Gamma}(w,\vec{a}) \supset Wit^i_{\vee\Delta}(Opt_P(w,\vec{a}),\vec{a}).$$

Proof: This is proved by induction on the number of sequents in an $\hat{T}_2^{i,\tau}$-proof of $\Gamma \to \Delta$. By cut elimination, we can assume all the sequents in the proof consist of $LE\hat{\Sigma}^b_i$-formulas. The base case and all cases except the $\hat{\Sigma}^b_i$-IND^τ case are reasonably easy. We handle this last case and then show the ($\forall$: *right*) case to illustrate why we need to define our local search problems using multifunctions N_P in $B_{i,2}$.

($\hat{\Sigma}^b_i$-IND^τ **case**) Suppose we have the inference:

$$\frac{A(b),\Gamma\to A(Sb),\Delta}{A(0),\Gamma\to A(|\ell(t)|),\Delta}$$

Here ℓ is a term in τ. By the induction hypothesis there is a $(B_{i,2}, \dot{\tau})$-problem P such that

$$\hat{T}_2^{i,\tau} \vdash Wit^i_{A(b)\wedge\Gamma}(w, b, \vec{a}) \supset Wit^i_{A(Sb)\vee\Delta}(Opt_P(w, b, \vec{a}), b, \vec{a}).$$

By assumption, the problem P is defined using $c_P(w', \langle w, b, \vec{a}\rangle)$, $N_P(w', \langle w, b, \vec{a}\rangle)$, and $F_P(w', \langle w, b, \vec{a}\rangle)$ in $B_{i,2}$. The tuple $\langle w, b, \vec{a}\rangle$ is the fixed arity tuple which consists of a witness for $A(b)\wedge\Gamma$ and consists of the free variables which appear in the upper sequent of the inference. The input w' in c_P, N_P, and F_P is a candidate witness for $A(Sb)\vee\Delta$. The neighbour function on input $w', \langle w, b, \vec{a}, \rangle$ outputs a new candidate witness w''. By the definition of P, there must be a least one candidate witness since we must have $F_P(0, \langle w, b, \vec{a}\rangle) > 0$.

We now describe a $(B_{i,2}, \dot{\tau})$-problem P' based on P which witnesses the lower sequent of the above inference. The new feasible answers predicate F'_P will be given by

$$F_{P'}(w', \langle w, \vec{a}\rangle) =$$
$$cond((w' = 0 \vee F_P(\beta(2, w'), \langle w, \beta(1, w'), \vec{a}\rangle) > 0 \vee Wit^i_{A(t)\vee\Delta}(w', \vec{a})), 1, 0).$$

Using Lemma III.A.6, one can show $F_{P'}$ will be a multifunction in $B_{i,2}$. Notice 0 is a feasible answer. Other feasible answers are ordered pairs, the first coordinate of which is supposed to code a value for b and the second coordinate codes a feasible answer for the problem P. The last type of feasible answer are witnesses for the lower antecedent. Given the L_2-term t_P which in the definition of $(B_{i,2}, \dot{\tau})$-problem bounds all feasible answers and the term $t_{A(\ell(t))\vee\Delta}$ which by Lemma V.A.2 bounds the size of witnesses for the antecedent, it is not hard to construct a term $t_{P'}$ which bounds the size of feasible answers of P'.

We now define a new cost function $c_{P'}(w', \langle w, \vec{a}\rangle)$. If $w' = 0$ this function outputs 0. Otherwise, we define it as

$$c_{P'}(w', \langle w, \vec{a}\rangle) \;=\; (\beta(1, w') + 1) \cdot M(\langle w, \vec{a}\rangle) + c_P(\beta(2, w'), \langle w, \beta(1, w'), \vec{a}\rangle)$$

Here M is a term in $\dot{\tau}(L_2)$ which majorizes $c_P(w', \langle w, b, \vec{x}\rangle)$ for all values of b less than $\ell(t)$. By $\ell(t)$ we mean the L_2-term which appears in the lower sequent of the induction hypothesis. Notice M does not depend on b so M is not just M_P. However, such an M exists since by the definition of P we have $c_P(w', \langle w, b, \vec{x}\rangle) \leq M_P(w, b, \vec{x})$ and if we substitute $\ell(t)$ for b, we get a $\dot{\tau}(L_2)$-term involving only w and $\vec{a}$ which provably majorizes c_P. We can define $M_{P'}$ to be some function greater than $(\ell(t)+1)\cdot M + M$ in $\dot{\tau}(L_2)$. This will exist since M and $\ell(t)$ are in $\dot{\tau}(L_2)$. It is easy to see $c_{P'}$ will be single-valued provided c_P is. The last function we need to define is the neighbourhood function $N_{P'}(w', \langle w, \vec{a}\rangle)$. This definition breaks up into several cases.

If $w' = 0$ we define $N_{P'}(w', \langle w, \vec{a}\rangle)$ to be $\langle 0, 0\rangle$.

If w' satisfies $Wit^i_{A(t)\vee\Delta}(w', \vec{a})$ then $N_{P'}(w', \langle w, \vec{a}\rangle)$ just outputs w'.

If $N_P(\beta(2, w'), \langle w, \beta(1, w'), \vec{a}\rangle) \neq \beta(2, w')$ then we define

$$N_{P'}(w', \langle w, \vec{a}\rangle) \;=\; \langle \beta(1, w'), N_P(\beta(2, w'), \langle w, \beta(1, w'), \vec{a}\rangle)\rangle.$$

If $N_P(\beta(2, w'), \langle w, \beta(1, w'), \vec{a}\rangle) = \beta(2, w')$ there are two subcases either $\beta(2, w')$ satisfies $Wit^i_{A(t)\vee\Delta}(\beta(2, w'), \vec{a})$ in which case we set

$$N_{P'}(w', \langle w, \vec{a}\rangle) \;=\; \beta(2, w')$$

or it does not, in which case, we set

$$N_{P'}(w', \langle w, \vec{a}\rangle) \;=\; \langle 0, \langle w, \beta(1, w') + 1, \vec{a}\rangle.$$

It should be reasonably clear that the functions $F_{P'}$, $c_{P'}$, and $N_{P'}$ are in $B_{i,2}$ given their definitions and since F_P, c_P and N_P are in $B_{i,2}$. So the above does define a $(B_{i,2}, \tau)$-problem P' and $\hat{T}^{i,\tau}_2$ can prove this. Using $\hat{\Sigma}^b_i$-IND^τ one can show

$$\hat{T}^{i,\tau}_2 \vdash Wit^i_{A(0)\wedge\Gamma}(w, \vec{a}) \supset Wit^i_{A(\ell(t))\vee\Delta}(Opt_{P'}(w, \vec{a}), \vec{a}).$$

($\forall$:right case) Suppose we have the inference:

$$\frac{b \leq t, \Gamma \rightarrow A(b), \Delta}{\Gamma \rightarrow (\forall x \leq t) A(x), \Delta}$$

By the induction hypothesis there is a $(B_{i,2}, \tau)$-problem P such that

$$\hat{T}_2^{i,\tau} \vdash Wit^i_{b \leq t \wedge \Gamma}(w, b, \vec{a}) \supset Wit^i_{A \vee \Delta}(Opt_P(w, b, \vec{a}), b, \vec{a}).$$

By assumption, the problem P is defined using $c_P(w', \langle w, b, \vec{a} \rangle)$, $N_P(w', \langle w, b, \vec{a} \rangle)$, and $F_P(w', \langle w, b, \vec{a} \rangle)$ in $B_{i,2}$. Cut-elimination implies $(\forall x \leq t) A(x) \in L\hat{\Pi}^b_{i-1}$ and since A is in $L\hat{\Sigma}^b_{i-2}$ by Lemma III.A.6 there is a multifunction $f_{\neg A}$ in $B_{i,2}$ with the property that $f_{\neg A}(x) = 0$ iff $\neg A(x)$. Let $h(w, \vec{a})$ be the $B_{i,2}$ multifunction $(\forall x \leq t)[f_{\neg A(x)} = 0]$. We are now ready to define a $(B_{i,2}, \tau)$-problem for the lower sequent. The new feasible answers predicate $F_{P'}$ will be given by

$$F_{P'}(w', \langle w, \vec{a} \rangle) =$$
$$cond((w' = 0 \vee F_P(\beta(2, w'), \langle w, \beta(1, w'), \vec{a} \rangle) > 0 \vee Wit^i_{(\forall x \leq t) A \vee \Delta}(w', \vec{a})), 1, 0).$$

Using Lemma III.A.6, one can show $F_{P'}$ will be a multifunction in $B_{i,2}$. Notice 0 is a feasible answer. Other feasible answers are ordered pairs, the first coordinate of which is supposed to code a value for b and the second coordinate codes a feasible answer for the problem P. The last type of feasible answer are witnesses for the lower antecedent. Given the L_2-term t_P which in the definition of $(B_{i,2}, \tau)$-problem bounds all feasible answers and the term $t_{(\forall x \leq t) A \vee \Delta}$ which by Lemma V.A.2 bounds the size of witnesses for the antecedent, it is not hard to construct a term $t_{P'}$ which bounds the size of feasible answers of P'.

We now define a new cost function $c_{P'}(w', \langle w, \vec{a} \rangle)$. If $w' = 0$ this function outputs 0. If $F_P(\beta(2, w'), \langle w, \beta(1, w'), \vec{a} \rangle) > 0$ we define this function to be

$$c_P(\beta(2, w'), \langle \langle 0, w \rangle, \beta(1, w'), \vec{a} \rangle).$$

Lastly, if w' is a witness to the lower antecedent, we define $c_{P'}$ as

$$M_P(\langle \langle 0, w \rangle, \beta(1, w'), \vec{a} \rangle) + 1.$$

We can define $M_{P'}(\langle w, \vec{a} \rangle)$ as

$$M_P(\langle \langle 0, w \rangle, \beta(1, w'), \vec{a} \rangle) + 1.$$

Notice c'_P will be provably single-valued in $\hat{T}_2^{i,\tau}$ if c_P was since the query $F_{P'} > 0$ is either true or false and does not introduce nondeterminism. The last multifunction we need to define is the neighbourhood multifunction $N_{P'}(w', \langle w, \vec{a}\rangle)$. This definition breaks into several cases.

If $w' = 0$ we define $N_{P'}(w', \langle w, \vec{a}\rangle)$ to be $\langle h(w, \vec{a}), 0\rangle$.

If w' satisfies $Wit^i_{(\forall x \le t)A(x)\vee\Delta}(w', \vec{a})$ then $N_{P'}(w', \langle w, \vec{a}\rangle)$ just outputs w'.

If $N_P(\beta(2, w'), \langle w, \beta(1, w'), \vec{a}\rangle) \neq \beta(2, w')\rangle$ then we define

$$N_{P'}(w', \langle w, \vec{a}\rangle) \;=\; \langle \beta(1, w'), N_P(\beta(2, w'), \langle w, \beta(1, w'), \vec{a}\rangle)\rangle.$$

If $N_P(\beta(2, w'), \langle w, \beta(1, w'), \vec{a}\rangle) = \beta(2, w')$ then we define

$$N_{P'}(w', \langle w, \vec{a}\rangle) \;=\; \beta(2, w').$$

It should be reasonably clear that the functions $F_{P'}$, $c_{P'}$, and $N_{P'}$ are in $B_{i,2}$ given their definitions and since F_P, c_P and N_P are in $B_{i,2}$. So the above does define a $(B_{i,2}, \tau)$-problem P' and $\hat{T}_2^{i,\tau}$ can prove this. It is also not hard to see that

$$\hat{T}_2^{i,\tau} \vdash Wit^i_\Gamma(w, \vec{a}) \supset Wit^i_{(\forall x \le t)A(x)\vee\Delta}(Opt_{P'}(w, \vec{a}), \vec{a}).$$

This completes the proof. □

Corollary V.B.3 $(i \geq 1, m \geq 1)$

1. *A multifunction f is a $\hat{\Sigma}_i^b$-definable in $\hat{T}_2^{i,|\tau|}$ if and only if f is in $B_{i,2}^{|\tau|}$.*
2. *A multifunction f is a $\hat{\Sigma}_i^b$-definable in $\hat{R}_2^i$ if and only if f is in $B_{i,2}^{\{||id||\}}$.*
3. *A multifunction f is a $\hat{\Sigma}_i^b$-definable in $EBASIC$ if and only if f is in $B_{i,2}^{cl} = B_{i,2}$.*
4. *A multifunction f is a $\hat{\Sigma}_i^b$-definable in $\hat{T}_2^{i,m}$ if and only if f is in $B_{i,2}^{\{|id|_m\}}$.*

$(i \geq 1, i \geq m \geq j \geq 0)$

5. *A multifunction f is $\hat{\Sigma}_i^b$-definable in $\hat{T}_2^{i,\tau}$ if and only if f is in $\pi LS_\tau^{B_{i,2}}$.*
6. *A multifunction f is $\hat{\Sigma}_{i-j}^b$-definable in $\hat{T}_2^{i,m,j}$ if and only if it is in $\pi LS_{Term_2^{m,j}}^{B_{i-j}}$*

Proof: (1) For the 'if' direction we use Theorem III.B.1. For the other direction consider Theorem V.B.1 when we take Γ empty and Δ to be a $E\hat{\Sigma}_i^b$ formula $(\exists y \leq t(x))A(x,y)$ provable in $\hat{T}_2^{i,|\tau|}$. Then we get that there is a $B_{i,2}^{|\tau|}$ function f such that

$$\hat{T}_2^{i,\tau} \vdash \rightarrow Wit_A^i(x, f(x)).$$

Given the definition of witness we thus have

$$\hat{T}_2^{i,\tau} \vdash \rightarrow A(x, \beta(1, f(x)).$$

(2), (3), and (4) These parts follow similarly from Theorem III.B.1 and Theorem V.B.1 and the definition of these theories as $\hat{T}_2^{i,\tau}$ theories.

(5) and (6) These follow from Theorem III.C.5 and Theorem V.B.2. For instance, suppose $(\exists y \leq t(x))A(x,y)$ is provable in $\hat{T}_2^{i,\tau}$. Then we get by Theorem III.C.5 that there is a $(B_{i,2}, \tau)$-problem P such that

$$\hat{T}_2^{i,\tau} \vdash \rightarrow Wit_A^i(x, Opt_P(x)).$$

Given the definition of witness we thus have

$$\hat{T}_2^{i,\tau} \vdash \rightarrow A(x, \beta(1, Opt_P(x)).$$

□

By Corollary V.B.3, the $\hat{\Sigma}_i^b$-definable multifunctions of T_2^i are $\pi LS_{\{id\}}^{B_{i,2}}$. In the T_2^1 case, Buss Krajíček [12] get $\pi LS_{\{id\}}^{FP}$. Our result shows the cost, neighbourhood, and feasibility predicates only have to be in $B_{1,2}$ which is presumably a fair bit weaker than the class FP. In fact, one can single-value any function in $B_{1,2}$ in FTC^0. That is, the class of functions computable by uniform constant depth threshold circuits. This is because FTC^0 is closed under sharply bounded minimization for any $g \in FTC^0$. In [28], it was shown that the Σ_1^b-definable functions of $\bar{R}_2^0 \supset R_2^0 \supset EBASIC$ are precisely the class FTC^0. We will show in Chapter IX that the $\hat{\Sigma}_1^b$-definable functions of $\hat{C}_2^{0,\{|id|\}}$ are also the class FTC^0.

Remark V.B.4 We mentioned in Chapter IV that it is difficult to show local search classes are closed under composition. This was why we introduced projections of these classes. We also suggested that local search classes without projection might correspond to some weaker notion of definability than $\hat{\Sigma}_i^b$-definability. One approach to this problem in the T_2^1 case is the following. First, expand the language of T_2^1 to include function symbols for all the polynomial-time functions by the method of Buss [13] where he creates the theory $S_2^1(PV)$. Since $S_2^1 \subseteq T_2^1$, the latter can Σ_1^b-define these functions. Now look at E_1-definability and open-definability in the expanded theory. Here an E_1-formula is one of the form $(\exists x \leq t)open$. One should get by the same proof as above the E_1-definable multifunctions of T_2^1 are πPLS and the *open*-definable multifunctions are PLS.

Remark V.B.5 A class of terms of the form $|\tau|$ can be product closed. (Consider $\{|id|\}$.) In these cases our characterization above coincide, showing $\pi LS_{(|\tau|)}^{B_{i,2}} = B_{i,2}^{\tau}$.

Theorem V.B.6 *Fix $i \geq 1$ and let $\Gamma \rightarrow \Delta$ be a sequent of $L\hat{\Pi}^b_{i-1}$-formulas consistent with $\hat{T}_2^{i,|\tau|}$. Then the $\hat{\Sigma}^b_i$-definable multifunctions of $\hat{T}_2^{i,|\tau|} + \{\Gamma \rightarrow \Delta\}$ are precisely the class $B_{i,2}^{|\tau|}$.*

Similarly, if $\Gamma \rightarrow \Delta$ is consistent with $\hat{T}_2^{i,\tau}$. Then the $\hat{\Sigma}^b_i$-definable multifunctions of $\hat{T}_2^{i,\tau} + \{\Gamma \rightarrow \Delta\}$ are precisely the class $\pi LS_{\dot{\tau}}^{B_{i,2}}$.

It should be pointed out that there are potentially more $(B_{i,2}, \dot{\tau})$-problems in $\hat{T}_2^{i,\tau} + \{\Gamma \rightarrow \Delta\}$ than in $\hat{T}_2^{i,\tau}$.

Proof: Certainly, $\hat{T}_2^{i,|\tau|} + \{\Gamma \rightarrow \Delta\}$ can $\hat{\Sigma}^b_i$-define the multifunction in $B_{i,2}^{|\tau|}$, since $\hat{T}_2^{i,|\tau|}$ can. On the other hand, if we consider $\hat{T}_2^{i,|\tau|} + \{\Gamma \rightarrow \Delta\}$ as the extension of the sequent calculus proof system $\hat{T}_2^{i,|\tau|}$ where we also allow $\Gamma \rightarrow \Delta$ as an axiom. We can carry out essentially the same witnessing argument as in Theorem V.B.1 to show that if $\hat{T}_2^{i,|\tau|}$ proves $\Gamma' \rightarrow \Delta'$ where Γ' and Δ' are cedents of $LE\hat{\Sigma}^b_i$-formulas then there is a $B_{i,2}^{|\tau|}$ multifunction f which is $\hat{\Sigma}^b_i$-defined in $\hat{T}_2^{i,|\tau|} + \{\Gamma \rightarrow \Delta\}$ such that:

$$\hat{T}_2^{i,|\tau|} + \{\Gamma \rightarrow \Delta\} \vdash Wit^i_{\wedge\Gamma'}(w, \vec{a}) \supset Wit^i_{\vee\Delta'}(f(w, \vec{a}), \vec{a}).$$

We can use the identity function to give witness to initial sequents of the form $\Gamma \rightarrow \Delta$. The witnessing argument is otherwise the same.

The $\hat{T}_2^{i,\tau} + \{\Gamma \rightarrow \Delta\}$ statement is proved in a similar manner. □

Remark V.B.7 All of our results for this section generalize in a straightforward manner to the theories $\hat{T}_k^{i,\tau}$. That is, the $\hat{\Sigma}^b_{i,k}$-definable multifunction of $\hat{T}_k^{i,|\tau|}$ are precisely the class $B_{i,k}^{\tau}$. The $\hat{\Sigma}^b_{i,k}$-definable multifunctions of $\hat{T}_k^{i,\tau}$ are precisely the class $\pi LS_{\dot{\tau}}^{B_{i,k}}$. Essentially, the same proofs as we gave above go through. We concentrated on the $k = 2$ case in that it is related to the most computationally interesting classes of functions.

V.C Prefix induction

We conclude this chapter with some remarks about prefix induction. In Chapter I we briefly mentioned the induction scheme Ψ-$PIND$ of the form

$$\alpha(0) \wedge (\forall x)(\alpha(\lfloor \frac{1}{2}x \rfloor) \supset \alpha(x)) \supset (\forall x)\alpha(x).$$

where α is in Ψ. In general, one could consider the induction scheme Ψ-$P^{\tau}IND$ of the form

$$\bigwedge_{i=0}^{n} \alpha(n) \wedge (\forall x)(\alpha(\ell(x)) \supset \alpha(x)) \supset (\forall x)\alpha(x).$$

where α is in Ψ, n is a constant, and $\ell(x)$ is in τ. Here τ is a nondecreasing set of iterms with the property that $x > n$ implies $\ell'(x) < x$ for ℓ' in τ. Intuitively, this kind of induction scheme allows one to automate the following steps in the proof a property $A(x)$ in Ψ: from $A(i)$ for some $i \leq n$, deduce ..., $A(\ell(\ell(x)))$, $A(\ell(x))$, $A(x)$. For example, to prove $A(100)$ with the Ψ-$PIND$ scheme deduces $A(0)$, $A(1)$, $A(3)$, $A(6)$, $A(12)$, $A(25)$, $A(50)$, $A(100)$. The number of steps automated in a deduction of $A(x)$ from a Ψ-$P^{\{\ell\}}IND$ scheme will be the number of applications, m, of ℓ to x such that $\ell^m(x) \leq n$. For instance, for Ψ-$PIND$ the number of steps automated will be $|x|$ since $\lfloor x/2^{|x|} \rfloor = 0$. Thus, it should come as little surprise that for instance S_2^i can be axiomatized with either Σ_i^b-$PIND$ or Σ_i^b-$LIND$ axioms [13, 11], since both induction scheme automate essentially the same number of steps. Another prefix scheme which has appeared in the literature [6] is the Ψ-$PPIND$ scheme

$$\alpha(0) \wedge \alpha(1) \wedge (\forall x)(\alpha(MSP(x, \lfloor \frac{1}{2}|x| \rfloor)) \supset \alpha(x)) \supset (\forall x)\alpha(x).$$

where α in Ψ. Let ℓ be $MSP(id, \lfloor \frac{1}{2}|id| \rfloor)$. It is not hard to see that $\ell^{||x||}(x) = 0$ or 1 so this scheme automates $||x||$ steps. As one would expect one can axiomatize R_2^i using Σ_i^b-$PPIND$ (see [7]).

If the number of steps automated by a Ψ-$P^{\{\ell\}}IND$ can be represented by some L_2-term ℓ' then using this scheme rather than Ψ-$IND^{\ell'}$ probably does

not buy one much. However, consider the following prefix scheme

$$\alpha(1) \wedge (\forall x)(\alpha(|x|) \supset \alpha(x)) \supset (\forall x)\alpha(x).$$

where α in Ψ. The number of steps this scheme automates is the number of iterations of $|id|$ neccessary to produce 1. We will call this number $|id|^*$. This number grows at roughly the rate of the computer science function $\log^*$ (the number of iterations of $\log_2$ need at get a number < 1. Thus, it may be interesting to study inductions which are of this power. On the other hand, it seems unlikely $|id|^*$ can be defined with an L_2-term. So in this case there is an advantage to prefix induction scheme since to get a Ψ-IND^τ equivalent we would probably have to expand the language.

For the rest of this discussion we will assume the iterms in τ are of the correct form. Let $P\hat{T}_k^{i,\tau}$ be the theory $EBASIC$+$\hat{\Sigma}_i^b$-$P^\tau IND$. We now indicate how to construct multifunction algebras for the theories $P\hat{T}_k^{i,\tau}$. First, some definitions:

Definition V.C.1 *A (multi)function f is defined using τ-prefix bounded primitive recursion ($PB^\tau PR_k$) from (multi)functions g_i for $i = 0, \ldots n$, h, t, and r if*

$$\begin{aligned} F(i, \vec{x}) &= g_i(\vec{x}) \text{for } i = 1, \ldots, n \\ F(m, \vec{x}) &= \min(h(m, \vec{x}, F(\ell(m), \vec{x})), r(\vec{x})) \\ f(m, \vec{x}) &= F(t(m, \vec{x}), \vec{x}) \end{aligned}$$

for some L_k-term r, for some L_k-term t, and some τ-term ℓ. We write $PB^\tau PR$ for $PB^\tau PR_2$.

From this we define the multifunction algebra $PB_{i,k}^\tau$ to be the smallest class containing $B_{i-1,k}$, containing $(Wx \leq z)[D(x, \vec{y}) = 0]$ for any predicate D in $B_{i-1,k}$, closed under composition, and closed under the recursion scheme $PBPR_k^\tau$.

It is not hard to see that by arguments essentially the same as Theorem III.B.1 the theory $P\hat{T}_2^{i,\tau}$ can define the multifunctions in $PB_{i,2}^\tau$. The converse also follows from essentially the same witnessing argument as in Theorem V.B.1

where we formulate the sequent calculus version of $PB^{\tau}_{i,2}$ with the following rule of inference

$$\frac{A(\ell(b)), \Gamma \rightarrow A(b), \Delta}{A(0), \ldots, A(n), \Gamma \rightarrow A(t), \Delta}$$

where A is a $\hat{\Sigma}^b_i$-formula and ℓ is in τ and n is a fixed number. i.e.. a closed term of the form $S^n(0)$.

Chapter VI

Machine classes and definability in prenex theories

We now give machine characterizations of the $\hat{\Sigma}^b_{i+1}$-definable multifunctions of the theories $\hat{T}^{i,\tau}_2$. Our characterization will be analogous to that of the Krajíček paper [33] where the Σ^b_{i+1}-multifunctions of S^i_2 were shown to be the class $FP^{\Sigma^p_i}(wit.\log)$. We also show

$$\hat{T}^{i,\tau^\#}_2 \preceq_{\hat{\Sigma}^b_{i+1}} \hat{T}^{i+1,|\tau^\#|}_2 = \hat{T}^{i+1,|\tau|}_2.$$

We give specific applications of our results to the theories $\hat{R}^i_2$. $\hat{T}^{i,m}_2$ and $\hat{T}^{i,m,j}_2$. In particular, we show the $\hat{\Sigma}^b_{i+1}$-definable multifunctions of $\hat{R}^i_2$ are precisely the class $FP^{\Sigma^p_i}(wit.\log\log)$. Lastly, we give a syntactic characterization of the $\hat{\Delta}^b_i$-predicates of $\hat{T}^{i,\tau}_2$. In this chapter, we will often use the fact that $|\tau^\#|$ is a product closure of $|\tau|$ and the fact from Theorem II.G.7 that $\hat{T}^{i,|\tau|}_2 = \hat{T}^{i,|\tau^\#|}_2$.

VI.A Technical tools

To begin we define some rather restricted classes of machines which will serve as a technical tool in our results. The idea is that for $i \geq 1$ the multifunctions computed by these machines will turn out to be the class $FP^{\Sigma^p_i}(wit.\tau)$. We will then show our theories $\hat{T}^{i,\tau}_2$ can $\hat{\Sigma}^b_{i+1}$-define the multifunctions computed

by this restricted class of machines and, hence, can define the multifunctions in $FP^{\Sigma_i^p}(wit, \tau)$. The reason we do not show $\hat{T}_2^{i,\tau}$ can directly define $FP^{\Sigma_i^p}(wit, \tau)$ computations is that this would involve showing $\hat{T}_2^{i,\tau}$ can manipulate polynomial length sequences coding polynomial time computations. For a general set of items τ this seems unlikely.

Definition VI.A.1 ($i \geq 1$) $F[|\tau|]_2^{\Sigma_i^p}(wit)$ *is the class of multifunctions f for which there is a machine M which operates in the following way:*

1. *M on input x runs in time $|\ell'_M(h(x))|$ for some fixed term ℓ'_M in $\dot{\tau}$ and L_2-term h. i.e., It runs in time $c \cdot |\ell_M(h(x))|$ for some fixed term ℓ_M in τ and L_2-term h. M has access to a Σ_i^p witness oracle, but except for the non-determinism inherent from the witness oracle, M is an otherwise deterministic machine. M can only write in binary.*

2. *M has three tapes: an oracle query tape, a work tape, and an oracle response tape. At the start of a computation, the input x is written in binary on M's query tape followed by the number 2. The query tape head begins on the square to the right of the 2. The oracle response tape is blank at the start of a computation of M.*

3. *During a single step of a computation, M is allowed to perform one of the following actions: (1) read the first square of the oracle response tape, (2) step the query tape right, (3) write a 0 or 1 to the current square of the query tape, or (4) perform one of the usual single step actions of a Turing machine on a work tape. A query state is entered whenever there is a write to the query tape. When a query state is entered, the oracle returns an answer in one time step. A query to the oracle is defined to be the contents of the query tape at the time that the query state is entered. The oracle read head is always fixed at the first square of the response and the first location of an oracle response is always 1 or 0 depending on whether the oracle responded 'Yes' or 'No'. If the answer is 'Yes' the remaining contents of the oracle tape*

will be a witness of the correctness of the answer of size at most $|s(x)|^n$ *where* s *is an* L_2*-term and* n *is constant. Although this witness must be correct,* M *is cannot read from this witness as the oracle read head is fixed.*

4. *The oracle tape after the first location is partitioned into blocks of size* $|t|^m$ *where* $|t(x)|^m \leq |s(x)|^n$ *and* t *is an* L_2*-term. The output of* M *is defined to be the contents of the first block of the oracle tape after the last query has been written.*

One thing to notice about the above definition is that depending on ℓ and h it is possible that two different inputs of the same length to an $F[|\tau|]_2^{\Sigma_i^p}(wit)$ machine have different run-time bounds. The reason we put $|\cdot|$ outside the $\ell(h(x))$ is that it will keep our notation and some of our arguments simpler. The squeamish can always pretend that the class we are dealing with is the subclass of $F[|\tau|]_2^{\Sigma_i^p}(wit)$ of machines with h's of the form $g(2^{|x|})$.

Definition VI.A.2 *Let* τ *be a set of iterm. We define* $FP^{\Sigma_i^p}(wit, |\tau|)$ *to be the class of multifunctions computable in polynomial time with fewer than* $O(|\ell(h)|)$ *witness queries to a* Σ_i^p*-oracle where* ℓ *is a fixed term in* τ *and* h *is an* L_2*-term that depend on the multifunction being computed.*

The way in which this definition differs from that of Remark I.B.1 is that here $|\tau|$ is a set of terms and the bound on the number of queries might be different for two inputs of the same length; whereas, in the remark there was a single bound of the number queries which was a function of the length of the input. we write $FP^{\Sigma_i^p}(wit, \{|\ell|\})$ rather than $FP^{\Sigma_i^p}(wit, |\ell|)$ to make this distinction clear. In the case where $|\tau|$ consists of only one term $|\ell|$ we write $FP^{\Sigma_i^p}(wit, \{|\ell|\})$ rather than $FP^{\Sigma_i^p}(wit, |\ell|)$ to make this distinction clear. Given the restricted nature of the class $F[|\tau|]_2^{\Sigma_i^p}(wit)$, the next result, which is based on a result in [16], is somewhat surprising.

Theorem VI.A.3 $(i \geq 1)$ *The following equality holds:*

$$F[|\tau|]_2^{\Sigma_i^p}(wit) = FP^{\Sigma_i^p}(wit, |\tau|)$$

Proof: Given any machine M in $F[|\tau|]_2^{\Sigma_i^p}(wit)$ it is not hard to construct a machine N in $FP^{\Sigma_i^p}(wit, |\tau|)$ which accepts the same language. First, on input x the machine computes $c \cdot |\ell(h(x))|$, where ℓ is a term in τ and h is in L_2, and then begins simulating M. After M halts, it writes as its output the contents of the first block of M's oracle tape.

On the other hand suppose M is in $FP^{\Sigma_i^p}(wit, |\tau|)$ with number of queries bounded by $c \cdot |\ell(h)|$ for $\ell \in \tau$ and $h \in L_2$. We may assume without loss of generality that M is a two tape machine and when M terminates the output of M is all that remains on M's worktape. Consider the following procedure on an $F[|\tau|]_2^{\Sigma_i^p}(wit)$ machine N.

Input $x2$ /* on query tape.*/
For $j = 1, \ldots (c \cdot |\ell(h(x))|) - 1$
  /* $c \cdot |\ell(x)|$ = max. # of queries in M. This counter is
  implemented on the work tape. The stepping and writing below are for
  the query tape.*/
  If $j \neq 1$ **then Step** Right.
  Write 1.
  /* N's Σ_i^p oracle answers the question:
  "Is there a valid computation of M on the input x with
  the first j queries answered by the string to the right of the 2?"
  Remember: There is a query whenever there is a write to the query
  tape.*/
  If oracle head = 0 **Write** 0
End For

We choose our oracle such that the encoding it uses for each step of M's computation has length $2|\ell(h(x))|^r$ where the first $|\ell(h(x))|^r$ blocks are used to

encode the contents of M's work tape; the second $|\ell(h(x))|^r$ squares are used to encode the state of M's oracle tape. We also require that the encoding of steps of M is from right to left so that the last step of M's computation appears to the right of the first square of the oracle response tape. We then use $|\ell(h(x))|^r$ as our block size for N's oracle tape. The output of the above $F[|\tau|]_2^{\Sigma_i^p}(wit)$ machine N will thus be the final contents of the work tape of a valid computation of M on input x. i.e., the output of the machine M. □

VI.B Defining machine classes in prenex theories

We now use Theorem VI.A.3 to show $\hat{T}_2^{i,\tau}$ can $\hat{\Sigma}_{i-1}^b$-define the functions in $FP^{\Sigma_i^p}(wit.|\tau|)$. Notice this will show $EBASIC$ can $\hat{\Sigma}_{i+1}^b$-define the multifunctions in $FP^{\Sigma_i^p}(wit.1)$ since $\hat{T}_2^{i,cl} = EBASIC$.

Theorem VI.B.1 ($i \geq 1$) *The theory $\hat{T}_2^{i,\tau}$ can $\hat{\Sigma}_{i+1}^b$-define the multifunctions in the class*

$$FP^{\Sigma_i^p}(wit.|\tau|).$$

Proof: By Theorem VI.A.3, it suffices to show $\hat{T}_2^{i,\tau}$ can $\hat{\Sigma}_{i+1}^b$-define any machine in $F[|\tau|]_2^{\Sigma_i^p}(wit)$. Let $M(x)$ be a machine in the class $F[|\tau|]_2^{\Sigma_i^p}(wit)$ that uses a oracle $\Omega(q)$ and runs in time $c \cdot |\ell(h)|$ for ℓ in τ. Without loss of generality, we can write this Σ_i^p-oracle as $(\exists z \leq t(q))B(z,q)$ where $B \in \hat{\Pi}_{i-1}^b$ and $t \in L_2$.

An instantaneous description (ID) of a configuration of M is a 7-tuple (the notion of 7-tuple can be easily defined using composition of ordered pairs) of the form:

$$\langle u, x, o, w, t_L^q, t_L^W, t_R^W \rangle.$$

Here u represents the state of M, x represents the input, o represents the first square of the oracle response tape, w represents any witness returned by the oracle, t_L^q is a number which after deleting the most significant bit represents the contents

of the oracle query tape to the left of the 2. t_L^W is a number which after deleting the most significant bit represents the visited squares to the left of work tape head. and t_R^W is a number which after deleting the most significant bit represents the visited squares to the right of the work tape head.

Following [16] we define a *precomputation* of M to be a sequence of configurations of M's execution with respect to an unspecified oracle. We can put an upper bound on the size of an ID based on M's runtime and use this upper bound as a block size in our encoding of this sequence. We access this sequences elements with the $\dot{\beta}$ function. A precomputation specifies that the first ID of M must be of the form:

$$\langle 1, x, 0, 0, 1, 1, 1 \rangle.$$

It also specifies that each ID must follow from the previous according to M: however, when M enters a query state by performing a write, the next ID can have either 0 or 1 as the oracle response and if 1 is the response it can have anything for the witness. Since M's runtime is less than $c \cdot |\ell(h(x))|$ for some τ-term ℓ. and L_2-term h. we can write a formula checking if a number codes a precomputation with a single quantifier of the form $(\forall j \leq c \cdot |\ell(h(x))|)$.

A *Q-computation* is a precomputation in which the 1 answers are correct for the oracle Ω but the 0 answers are not required to be correct. We define $QComp_M^{\dagger}(w, x, v)$ to be the following formula:

$$\begin{aligned} QComp_M^{\dagger}(w, x, v) := {} & w \text{ is a precomputation of } M(x) \text{ and} \\ & (\forall j \leq c \cdot |\ell(h(x))|)(YAns(w, j) \Leftrightarrow Bit(c \cdot |\ell(h(x))| \dot{-} j, v) = 1) \\ & \text{and } (\forall j \leq c \cdot |\ell(h(x))|)(Bit(c \cdot |\ell(h(x))| \dot{-} j, v) = 1 \supset \\ & CorrectYes(w, j)) \end{aligned}$$

Here $YAns(w, j)$ says the first oracle square of the jth ID in precomputation w was 1. It can be defined with an open formula using $\dot{\beta}$ and using projections of the pairing function. $CorrectYes(w, j)$ is just the predicate $B(z, q)$. where q is the contents of worktape 1 at time j and z is the minimum of $t(q)$ and the

witness on the oracle tape at time j. Both z and q can be defined as L_2-terms so $CorrectYes(w,j)$ is a $\hat{\Pi}^b_{i-1}$-formula. Hence, $QComp^{\dot{\tau}}_M$ is provably equivalent in $\hat{T}^{i,\tau}_2$ to a $\hat{\Pi}^b_{i-1}$-formula. Since the number of distinct IDs in a computation of M on input x is bounded by $c \cdot |\ell(h(x))|$, v in $QComp^{\dot{\tau}}_M$ can be bounded by

$$2^{c\cdot|\ell(h(x))|} \leq (\ell(h(x)))^{c+1} \leq \ell'(h(x))$$

where ℓ' is a $\dot{\tau}$-term. This will also bound the number of potential queries. An M-computation w can be bounded by an L_2-term t dependent on the length of M's IDs. Since these IDs contain oracle witnesses t need not be sharply bounded. As $QComp^{\dot{\tau}}_M$ is provably equivalent to a $\hat{\Pi}^b_{i-1}$-formula, we know

$$\Psi := (\exists w \leq t) QComp^{\dot{\tau}}_M(w,x,v)$$

is provably equivalent to a $\hat{\Sigma}^b_i$-formula. Now $\hat{T}^{1,\tau}_2$ can prove there is a precomputation of x with all the oracle answers 0 using IND^{τ}_{Ψ}, Lemma II.C.4, and Lemma II.D.1. So $\hat{T}^{1,\tau}_2$ proves $(\exists w \leq t) QComp^{\dot{\tau}}_M(w,x,0)$. Let $A(u)$ be the formula

$$(\exists v \leq \ell'(h(x)))(\exists w \leq t)(QComp^{\dot{\tau}}_M(w,x,v) \wedge v \geq u).$$

We thus have $A(0)$. The formula A is provably equivalent to a $\hat{\Sigma}^b_i$-formula, so using $IND^{\dot{\tau}}_A$ axioms which are provable in $\hat{T}^{i,\tau}_2$ by Theorem II.G.7, we either have $A(\ell'(h(x)))$ or

$$(\exists u < \ell'(h(x)))(A(u) \wedge \neg A(u+1)).$$

Hence, we can show there is a maximum value $v \leq \ell'(h(x))$ for which

$$(\exists w \leq t) QComp^{\dot{\tau}}_M(w,x,v)$$

holds. All of the 1 answers in v must be correct since $QComp^{\dot{\tau}}_M$ holds. We argue that $\hat{T}^{i,\tau}_2$ can prove all the 0 answers must also be correct. Suppose the jth 0 was incorrect. We could then change it to a 1 and set the lower order bits to 0, thus, making a number $v' > v$. Now from $\exists w QComp^{\dot{\tau}}_M(w,x,v)$ we can show

$$\hat{T}^{1,\tau}_2 \vdash (\exists w') QComp^{\dot{\tau}}_M(w',x,v')$$

by letting w' be w up to the jth query, then coding a 1 with a valid witness on the response tape for the jth query and then coding M's computation where all the answers to subsequent queries are 0.

Therefore, $\hat{T}_2^{i,\tau}$ proves $M(x)$ has at least one computation with correct oracle responses. Define the function $Output(w)$ which when given a precomputation w outputs the contents of the first block of the witness string using projections of the pairing function and MSP. So for $i \geq 1$ the theory $\hat{T}_2^{i,\tau}$ can prove:

$$\begin{aligned}(\forall x)(\exists y)(\exists v \leq \ell'(h'(x)))[&\\ &(\exists w \leq t)(Output(w) = y \wedge QComp_M^{\dagger}(w, x, v))\\ &\wedge\neg(\exists v' \leq \ell'(h'(x)))(\exists w' \leq t)(v' > v \wedge QComp_M^{\dagger}(w', x, v')]\end{aligned}$$

Further the formula inside the scope of the $(\exists y)$ can be put into the form of a $\hat{\Sigma}_{i+1}^b$-formula using Theorem II.G.12, Remark II.C.7, and Lemma II.C.6. □

VI.C Query definability

To prove the converse of the above theorem we would like to know that $\hat{T}_2^{i,\tau}$ can $\hat{\Sigma}_{i+1}^b$-define the composition of $FP^{\Sigma_i^p}(wit, |\tau|)$ functions and that we can define this composition in a "nice" way. First, let us be a bit more precise in our definition of "nice".

Definition VI.C.1 *We say a multifunction $f(x) = y$ is $Q^{i,\tau}$-definable in a theory T, if there is a formula of the form*

$$\begin{aligned}B(x, y) := (\exists v \leq \ell(s(x)))[&(\exists w \leq t)(Out(w) = y \wedge A(x, w, v))\\ &\wedge\neg(\exists v' \leq \ell(s(x)))(\exists w' \leq t)(v' \geq v \wedge A(x, w', v'))].\end{aligned}$$

where A is a $\hat{\Pi}_{i-1}^b$-formula, $Out(w)$, s are L_2-terms, and ℓ is in τ such that $\mathbf{N} \models B(x, y) \Leftrightarrow f(x) = y$ and T proves $(\forall x)(\exists y \leq t)B$.

A variant of $Q^{i,\tau}$-definition (also called query definition) was first given

in the Buss paper [14]. Since the formula inside the scope of the $(\exists y \leq t)$ is provably equivalent to a $\hat{\Sigma}^b_{i+1}$-formula in $\hat{T}^{i,\tau}_2$ the multifunction $f(x,y)$ will also be $\hat{\Sigma}^b_{i+1}$-defined in $\hat{T}^{i,\tau}_2$. The proof of Theorem VI.B.1 shows the multifunctions in $FP^{\Sigma^p_i}(wit,|\tau|)$ are $Q^{i,\dot{\tau}}$-definable in $\hat{T}^{i,\tau}_2$.

Lemma VI.C.2 $(i \geq 1)$ *The theory $\hat{T}^{i,\tau}_2$ proves its $Q^{i,\dot{\tau}}$-definable multifunctions are closed under composition.*

Proof: Suppose f and g are $Q^{i,\dot{\tau}}$-definable functions in $\hat{T}^{i,\tau}_2$. Let f be defined by proving in $\hat{T}^{i,\tau}_2$ the following formula B_f:

$$\begin{aligned}
&(\forall x)(\exists y \leq t_f)(\exists v_f \leq \ell_f(s_f(x)))[\\
&\quad (\exists w_f \leq t_f)(Out_f(w_f) = y \wedge A_f(x, w_f, v_f))\\
&\quad \wedge\neg(\exists v'_f \leq \ell_f(s_f(x)))(\exists w'_f \leq t_f)(v'_f > v_f \wedge A_f(x, w'_f, v'_f))].
\end{aligned}$$

and let g be defined by proving in $\hat{T}^{i,\tau}_2$ the formula B_g similarly. To define $h = g \circ f$. consider the formula C_h:

$$\begin{aligned}
&(\forall x)(\exists y \leq t_g)(\exists v_f \leq \ell_f(s_f(x)))(\exists v_g \leq \ell_g(s_g(x)))[(\exists w_f \leq t_f)\\
&\quad (\exists w_g \leq t_g)(Out_g(w_g) = y \wedge A_f(x, w_f, v_f) \wedge A_g(Out(w_f), w_g, v_g))\\
&\quad \wedge\neg(\exists v'_f \leq \ell(s_f(x)))(\exists v'_g \leq \ell_g(s_g(x)))(\exists w'_f \leq t_f)(\exists w'_g \leq t_g)(\\
&\quad (v'_f > v_f \vee (v'_f = v_f \wedge v'_g > v_g)) \wedge A_f(x, w'_f, v'_f) \wedge A_g(Out(w'_f), w'_g, v'_g))].
\end{aligned}$$

Since $\hat{T}^{i,\tau}_2$ proves B_g and B_f, it will prove C_h. Now C_h can be converted into the desired B_h using Theorem II.G.12 and pairing. In doing the pairing we bound the size of the pair $\langle v_f, v_g\rangle$ by $(\ell_f(s_f) \cdot \ell_g(s_g))^3$ then use *cond* to guarantee $v_f \leq \ell_f(s_f)$ and $v_g \leq \ell_g(s_g)$. Using product closure this bound can be put in the form $\ell(r)$ where ℓ is in $\dot{\tau}$ and r is in L_2, so the function h is $Q^{i,\dot{\tau}}$-definable in $\hat{T}^{i,\tau}_2$. □

Lemma VI.C.3 $(i \geq 1)$ *The theory $\hat{T}^{i,\tau^\#}_2$ proves its $Q^{i,\tau^\#}$-definable multifunctions are closed under $BPR^{|\tau^\#|}_2$.*

Proof: The recursion scheme $BPR_2^{|\tau^\#|}$ was defined at the beginning of the last section. Recall a function f is defined by $BPR_2^{|\tau^\#|}$ from functions g, h, F, k, and r if

$$\begin{aligned} F(0,\vec{x}) &= g(\vec{x}) \\ F(n+1,\vec{x}) &= \min(h(n,\vec{x},F(n,\vec{x})),r(n,\vec{x})) \\ f(n,\vec{x}) &= F(|\ell(k(n,\vec{x}))|,\vec{x}) \end{aligned}$$

where r and k must be in L_2 and ℓ must be in $\tau^\#$. Let $h'(n,vecx)$ be the multifunction $\min(h(n,\vec{x},y),r(n,\vec{x}))$. This is $Q^{i,\tau^\#}$-definable by Lemma VI.C.2 provided h, and r are. Suppose g is defined by proving

$$\begin{aligned} &(\forall\vec{x})(\exists y \le t_g)(\exists v_g \le \ell_g(s_g(\vec{x})))[\\ &\quad (\exists w_g \le t_g)(Out_g(w_g) = y \wedge A_g(\vec{x},w_g,v_g)) \\ &\quad \wedge\neg(\exists v_g' \le \ell_g(s_g(\vec{x})))(\exists w_g' \le t_g)(v_g' > v_g \wedge A_g(\vec{x},w_g',v_g'))]. \end{aligned}$$

where ℓ_g is in $\tau^\#$ and suppose h' is defined by proving

$$\begin{aligned} &(\forall n,z,\vec{x})(\exists y \le r)(\exists v_{h'} \le \ell_{h'}(s_{h'}(\vec{x})))[\\ &\quad (\exists w_{h'} \le t_{h'})(Out_{h'}(w_{h'}) = y \wedge A_{h'}(n,\vec{x},z,w_{h'},v_{h'})) \wedge \\ &\quad \neg(\exists v_{h'}' \le \ell_{h'}(s_{h'}(\vec{x})))(\exists w_{h'}' \le t_{h'})(v_{h'}' > v_{h'} \wedge A_{h'}(n,z,\vec{x},w_{h'}',v_{h'}'))]. \end{aligned}$$

where $\ell_{h'}$ is in $\tau^\#$. Let $A_f(n,\vec{x},w,v)$ be the formula

$$\begin{aligned} &A_g(\vec{x},\hat{\beta}(0,|r^*|,w),\hat{\beta}(0,|s_{h'}^*|,v)) \wedge (\forall j < |\ell(k(n,\vec{x}))|) \\ &\quad ((A_{h'}(j,Out_{h'}(\hat{\beta}(j,|r^*|,w)),\vec{x},\hat{\beta}(j+1,|r^*|,w),\hat{\beta}(j+1,|s_h^*|,s_{h'},v) \end{aligned}$$

Since A_g and $A_{h'}$ are $\hat{\Pi}_{i-1}^b$-formulas, $\hat{T}_2^{i,\tau^\#}$ can prove A_f is equivalent to a $\hat{\Pi}_{i-1}^b$-formula. Using $\hat{\Sigma}_i^b$-$IND^{\tau^\#}$ induction on the formula $A(u)$ defined as

$$(\exists v_f \le 2\cdot(\ell(s_{h'}^*)\#\ell_{h'}(k))(\exists w_f \le 2\cdot(r^*\#\ell_{h'}(k)))(A_f(x,w_f,v_f) \wedge v_f > u)$$

as we did in Theorem VI.B.1. $\hat{T}_2^{i,\tau^\#}$ can then define f in by proving

$$(\forall n, x)(\exists y \leq r)(\exists v \leq 2 \cdot (\ell(s_h^*)\#\ell(k)))[$$
$$(\exists w_f \leq 2 \cdot (r^*\#\ell(k)))(Out_f(w_f) = y \wedge A_f(x, w_f, v_f)) \wedge$$
$$\neg(\exists v'_f \leq 2 \cdot (\ell_{h'}(s_{h'}^*)\#\ell_{h'}(k)))(\exists w'_f \leq 2 \cdot (r^*\#\ell_{h'}(k))(v'_f > v_f \wedge A_f(x, w'_f, v'_f))].$$

Here $Out_f(w_f)$ is $Out_{h'}(\hat{\beta}(|\ell_{h'}(k(n,x))|, |r^*|, w_{h'}))$. Since k is in $\tau^\#$, it will also be the case that $2 \cdot (\ell(s_{h'}^*)\#\ell_{h'}(k))$ is in $\tau^\#$. □

The next lemma can be proved in the same way as Lemma III.A.4.

Lemma VI.C.4 ($i \geq 1$) *The theory $\hat{T}_2^{i,\tau^\#}$ proves its $Q^{i,\tau^\#}$-definable multifunctions are closed under the following type of recursion:*

$$\begin{aligned} F(0, \vec{x}) &= g(\vec{x}) \\ F(n+1, \vec{x}) &= \min(h(n, \vec{x}, F(n, \vec{x})), r(n, \vec{x})) \\ f(n, \vec{x}) &= F(\min(n, \ell(t(n, \vec{x}))), \vec{x}) \end{aligned}$$

where g and h are in $B_{i,k}^\tau$, r and t are in L_k and ℓ is in τ.

The pairing function and β-functions of the last chapter are computable in $FP^{\Sigma_i^p}(wit, |\tau|)$. So they will be $Q^{i,\dot{\tau}}$-definable in $\hat{T}_2^{i,\tau}$.

VI.D More witnessing arguments

We now carry out a witnessing argument to prove the converse of Theorem VI.B.1. To do this we will use the same form of witness predicate as in the last section, except we will be working with $\hat{\Sigma}_{i+1}^b$-formulas and so we will use predicates of the form Wit_A^{i+1} for A an $E\hat{\Sigma}_{i+1}^b$-formula.

Theorem VI.D.1 ($i \geq 1$) *Suppose $\hat{T}_2^{i,\tau} \vdash \Gamma \rightarrow \Delta$ where Γ and Δ are cedents of $LE\hat{\Sigma}_{i+1}^b \cup L\hat{\Sigma}_i^b$ formulas. Let $\vec{a}$ be the free variables in this sequent. Then there is a $FP^{\Sigma_i^p}(wit, |\tau|)$ multifunction f which is $Q^{i,\dot{\tau}}$-defined in $\hat{T}_2^{i,\tau}$ such that:*

$$\hat{T}_2^{i,\tau} \vdash Wit_{\wedge\Gamma}^{i+1}(w, \vec{a}) \supset Wit_{\vee\Delta}^{i+1}(f(w, \vec{a}), \vec{a}).$$

Proof: This is proved by induction on the number of sequents in an $\hat{T}_2^{i,\tau}$ proof of $\Gamma \rightarrow \Delta$. By cut elimination, we can assume all the sequents in the proof are in $LE\hat{\Sigma}^b_{i+1} \cup L\hat{\Sigma}^b_i$. In the base case, the proof consists of an $EBASIC$ axiom, a logical axiom, or an equality axiom. In each of these cases the witness predicate is the original formula. So we can choose f to be the identity function. To define f for logical inferences, cut inferences, or for the structural inferences is the same as in witnessing argument for the $\hat{\Sigma}^b_i$-definable functions of $\hat{T}_2^{i,\tau}$. The ($\exists$:right) and the ($\forall$:left) case also remain the same as in the witnessing argument in the last section. We prove the remaining cases.

($\exists$:left case) Suppose we have the inference:

$$\frac{b \leq t, A(b), \Gamma \rightarrow \Delta}{(\exists x \leq t)A(x), \Gamma \rightarrow \Delta}$$

By the induction hypothesis there is a $Q^{i,\tau}$-definable g in $FP^{\Sigma^p_i}(wit.|\tau|)$ such that

$$\hat{T}_2^{i,\tau} \vdash Wit^{i+1}_{b \leq t \wedge A \wedge \Gamma}(w, \vec{a}, b) \supset Wit^{i+1}_{\vee \Delta}(g(w, \vec{a}, b), \vec{a}, b).$$

There are three subcases to consider. In each case, we need some way to determine a value for the free variable b and then run g using that value. First, suppose $(\exists x \leq t)A(x)$ is an $E\hat{\Sigma}^b_{i+1}$-formula. In which case, if w is a witness for

$$(\exists x \leq t)A(x) \wedge \Gamma,$$

then $\beta(1, \beta(1, w))$ is a value for b such that $A(b)$ holds and $\beta(2, \beta(1, w))$ is a witness for $A(b)$. So let our new witness function be

$$f(w, \vec{a}) = g(\langle\langle 0, \beta(2, \beta(1, w)), \beta(2, w)\rangle\rangle, \vec{a}, \beta(1, \beta(1, w))).$$

It is easy to see that

$$\hat{T}_2^{i,\tau} \vdash Wit^{i+1}_{(\exists x \leq t) A \wedge \Gamma}(w, \vec{a}) \supset Wit^{i}_{\vee \Delta}(f(w, \vec{a}), \vec{a}).$$

In the second case suppose $(\exists x \leq t)A(x)$ is an $\hat{\Sigma}^b_{i+1}$-formula. If w is a witness for $(\exists x \leq t)A(x) \wedge \Gamma$, then $\beta(1, w)$ is a value for b such that $A(b)$ holds. Let our new witness function be

$$f(w, \vec{a}) = g(\langle\langle 0, 0, \beta(2, w)\rangle\rangle, \vec{a}, \beta(1, w)).$$

It is easy to see that

$$\hat{T}_2^{i,|\tau|} \vdash Wit^{i+1}_{(\exists x \leq t)A \wedge \Gamma}(w, \vec{a}) \supset Wit^{i+1}_{\forall \Delta}(f(w, \vec{a}), \vec{a}).$$

The last subcase is when $(\exists x \leq t)A(x) \in L\hat{\Sigma}^b_i$ or $(\exists x \leq t)A(x) \in L\hat{\Sigma}^b_{i-1}$. In this case we define f to be the same as above except rather than use $\beta(1, \beta(1, w))$ or $\beta(1, w)$ to give a value b we instead use the multivalued function which queries a witness oracle about $(\exists x \leq t)A(x)$. If the latter is satisfiable then the oracle will return a value satisfying it. Notice $\beta(1, \beta(1, w))$ in f would in this case be null.

($\forall$:right case) Suppose we have the inference:

$$\frac{b \leq t, \Gamma \rightarrow A(b), \Delta}{\Gamma \rightarrow (\forall x \leq t)A(x), \Delta}$$

By the induction hypothesis there is a $Q^{i,\dot{\tau}}$-definable g in $FP^{\Sigma^p_i}(wit, |\tau|)$ such that

$$\hat{T}_2^{i,\tau} \vdash Wit^{i+1}_{b \leq t \wedge \Gamma}(w, \vec{a}, b) \supset Wit^{i+1}_{A \vee \Delta}(g(w, \vec{a}, b), \vec{a}, b).$$

By cut-elimination, $(\forall x \leq t)A(x) \in L\hat{\Pi}^b_i$. Thus, $(\exists x \leq t)\neg A(x)$ is a Σ^p_i-predicate. So we ask an oracle for this predicate for a value $b \leq t$ such that $\neg(A(b))$ holds. If such a value exists we set $f(w, \vec{a}) = g(\langle 0, w\rangle, \vec{a}, b)$. If no such value exists we let $f(w, \vec{a}) = \langle 0, 0\rangle$ since $(\forall x \leq t)A(x)$ would in that case be a valid $L\hat{\Pi}^b_i$-formula.

($\hat{\Sigma}^b_i$-IND^τ case) Suppose we have the inference

$$\frac{A(b), \Gamma \rightarrow A(Sb), \Delta}{A(0), \Gamma \rightarrow A(\ell(r(c, \vec{a}))), \Delta}$$

where ℓ is in τ and r is in L_2. By the induction hypothesis there is a $Q^{i,\dot{\tau}}$-definable g in $FP^{\Sigma^p_i}(wit, |\tau|)$ such that

$$\hat{T}_2^{i,\tau} \vdash Wit^{i+1}_{A(b) \wedge \Gamma}(w, b, \vec{a}) \supset Wit^{i+1}_{A(Sb) \vee \Delta}(g(w, b, \vec{a}), b, \vec{a}).$$

Let f be the $FP^{\Sigma_i^p}(wit, |\tau|)$ function which does the following: First, f computes $v = \ell(r(c, \vec{a}))$ and makes the query $[A(v)]$? If the answer is 'Yes' then f outputs a sequence of zeros. If $A(v)$ is valid any value will witness it and hence the succedent will be witnessed. If the answer to the query is 'No', f makes the query $[A(0)?]$. If it receives 'No' as a reply it outputs 0; the antecedent will be false.

If the reply was 'Yes', then f performs a binary search for a value $d \leq v$ such that $A(d)$ holds but $A(Sd)$ does not. This takes $|v|$ many queries to an oracle of the form $(\exists i \leq \ell(r(c, a)))(i > d \wedge A(d))$. Using pairing this predicate is provably equivalent to a $\hat{\Sigma}_i^b$-formula in $\hat{T}_2^{i,\tau}$. The theory $\hat{T}_2^{i,\tau}$ can prove using $\hat{\Sigma}_i^b$-MAX^τ axioms that there is a maximal d satisfying the above formula. So it can prove the d found by this binary search will be such that $A(d)$ holds but $A(Sd)$ does not. Using this value of d, f can run $g(w, \vec{a}, d)$ to get a witness for the succedent. This step involves only a composition of $Q^{i,\dot{\tau}}$-definable functions in $FP^{\Sigma_i^p}(wit, |\tau|)$. Thus,

$$\hat{T}_2^{i,\tau} \vdash Wit^{i+1}_{A(0)\wedge\Gamma}(w, \vec{a}) \supset Wit^{i+1}_{A(\ell(r))\vee\Delta}(f(w, \vec{a}), \vec{a}).$$

This completes the cases remained to be shown and the proof. □

Theorem VI.D.2 ($i \geq 1$) *Suppose* $\hat{T}_2^{i+1,|\tau|} = \hat{T}_2^{i+1,|\tau^\#|} \vdash \Gamma \rightarrow \Delta$ *where* Γ *and* Δ *are cedents of* $LE\hat{\Sigma}_{i+1}^b$*-formulas. Let* $\vec{a}$ *be the free variables in this sequent. Then there is a* $FP^{\Sigma_i^p}(wit, |\tau^\#|)$ *multifunction* f *which is* $Q^{i,\tau^\#}$*-defined in* $\hat{T}_2^{i,\tau^\#}$ *such that:*

$$\hat{T}_2^{i,\tau^\#} \vdash Wit^{i+1}_{\wedge\Gamma}(w, \vec{a}) \supset Wit^{i+1}_{\vee\Delta}(f(w, \vec{a}), \vec{a}).$$

Proof: This is proved by induction on the number of sequents in an $\hat{T}_2^{i+1,|\tau^\#|}$ proof of $\Gamma \rightarrow \Delta$. By cut elimination, we can assume all the sequents in the proof are in $LE\hat{\Sigma}_{i+1}^b$. All of the cases of the witnessing argument except for the ($\hat{\Sigma}_{i+1}^b$-$IND^{|\tau^\#|}$) case can be handled in the same way as Theorem VI.D.1. We now show how to do this last case

($\hat{\Sigma}^b_{i+1}$-$IND^{(|\tau^\#|)}$ case) Suppose we have the inference

$$\frac{A(b), \Gamma \rightarrow A(Sb), \Delta}{A(0), \Gamma \rightarrow A(|\ell(s)|), \Delta}$$

Here ℓ is in $\tau^\#$ and s in L_2. By the induction hypothesis there is a $Q^{i,\tau^\#}$-definable g in $FP^{\Sigma^p_i}(wit, (|\tau^\#|))$ such that

$$\hat{T}^{i,\tau^\#}_2 \vdash Wit^{i+1}_{A(b)\wedge\Gamma}(w, b, \vec{a}) \supset Wit^{i+1}_{A(Sb)\vee\Delta}(g(w, b, \vec{a}), b, \vec{a}).$$

Using Lemma VI.C.4, $Q^{i,\tau^\#}$-define the function f by $BPR^{(|\dot{\tau}|)}_2$ in the following way

$$\begin{aligned} F(0, w, \vec{a}) &= \langle \beta(1, w), 0 \rangle \\ F(b+1, w, \vec{a}) &= min(g(F(b, w, \vec{a}), w, \vec{a}, b), t_{\vee\Delta\vee A}) \end{aligned}$$

Define $f(u, w, \vec{a}) := g(\min(u, |\ell(s)|), w, \vec{a})$. Recall $t_{\vee\Delta\vee A}$ is the term guaranteed to bound a witness for $A(Sb) \vee \Delta$ by Lemma V.A.2. It is easy to see

$$\hat{T}^{i,\tau^\#}_2 \vdash Wit^{i+1}_{A(0)\wedge\Gamma}(w, \vec{a}) \supset Wit^{i+1}_{A(0)\vee\Delta}(f(0, w, \vec{a}), \vec{a}) \tag{VI.1}$$

Also, it is not hard to show

$$\hat{T}^{i,\tau^\#}_2 \vdash Wit^{i+1}_{A(0)\wedge\Gamma}(w, \vec{a}) \wedge Wit^{i+1}_{A(b)\vee\Delta}(f(b, w, \vec{a}), b, \vec{a}) \tag{VI.2}$$

$$\supset Wit^{i+1}_{A(Sb)\vee\Delta}(f(Sb, w, \vec{a}), Sb, \vec{a}) \tag{VI.3}$$

We would now like to show this implies

$$\hat{T}^{i,\tau^\#}_2 \vdash Wit^{i+1}_{A(0)\wedge\Gamma}(w, \vec{a}) \supset Wit^{i+1}_{A(|\ell(s)|)\vee\Delta}(f(|\ell(s)|, w, \vec{a}), \vec{a}).$$

To do this we $Q^{i,\tau^\#}$-define a function h by $BPR^{(|\dot{\tau}|)}_2$ in the following way:

$$\begin{aligned} H(0, w, \vec{a}) &= f(0, w, \vec{a}) \\ H(b+1, w, \vec{a}) &= f(b+1, w, \vec{a}) \cdot 2^{(b+1)\cdot t^*_{\vee\Delta\vee A(Sb)}} + H(b, w, \vec{a}) \\ h(|\ell(s)|, w, \vec{a}) &= H(|\ell(s)|, w, \vec{a}) \end{aligned}$$

We have deleted min's from the above recursion for readability sake. It is not hard to come up with terms to bound the above sum. Now let $B_H(w, \vec{a}, w')$ be the

formula which $Q^{i,\tau^\#}$-defines h. Then from (VI.1) above

$$\hat{T}_2^{i,\tau^\#} \vdash B_H(w,\vec{a},w') \wedge Wit^{i+1}_{A(0)\wedge\Gamma}(w,\vec{a}) \wedge Wit^{i+1}_{A(b)\vee\Delta}(\dot{\beta}(b.|t^*_{\forall\Delta\vee A}|.w').b.\vec{a}) \supset Wit^{i+1}_{A(Sb)\vee\Delta}(\dot{\beta}(Sb.|t^*_{\forall\Delta\vee A}|.w').Sb.\vec{a})$$

By $\hat{\Pi}^b_i$-$IND^{\tau^\#}$ on

$$Wit^{i+1}_{A(b)\vee\Delta}(\dot{\beta}(b.|t^*_{\forall\Delta\vee A}|.w').b.\vec{a})$$

a $\hat{\Pi}^b_i$-formula and (VI.1), this implies

$$\hat{T}_2^{i,\tau^\#} \vdash B_H(w,\vec{a},w') \wedge Wit^{i+1}_{A(0)\wedge\Gamma}(w,\vec{a}) \supset$$
$$Wit^{i+1}_{A(|\ell(s)|)\vee\Delta}(\dot{\beta}(|\ell(s)|.|t^*_{\forall\Delta\vee A}|.w'),|\ell(s)|.\vec{a})$$

Hence, from the definition of h, the theory $\hat{T}_2^{i,\tau^\#}$ proves the desired

$$\hat{T}_2^{i,\tau^\#} \vdash Wit^{i+1}_{A(0)\wedge\Gamma}(w,\vec{a}) \supset Wit^{i+1}_{A(|\ell(s)|)\vee\Delta}(f(|\ell(s)|.w.\vec{a}).\vec{a}).$$

This completes the proof. □

VI.E Implications of the witnessing argument

We end this section with a series of corollaries which we can derive from the above results and those of the last section.

Corollary VI.E.1 $(i \geq 2)$

$$\hat{T}_2^{i-1,\tau^\#} \preceq_{\hat{\Sigma}^b_i} \hat{T}_2^{i,|\tau|} = \hat{T}_2^{i,|\tau^\#|}$$

By choosing τ appropriately, we thus have:
$(i \geq m > j > 0)$ *or* $(i > m = j = 1)$

1. $T_2^{i-1} \preceq_{\hat{\Sigma}^b_i} S_2^i$.
2. $\hat{R}_2^{i,1} \preceq_{\hat{\Sigma}^b_i} \hat{R}_2^i$.
3. $\hat{T}_2^{i,m,j} \preceq_{\hat{\Sigma}^b_{i-j+1}} \hat{T}_2^{i,m,j-1}$.

4. $\hat{T}_2^{i,m,j} \preceq_{\hat{\Sigma}^b_{i-j-1}} \hat{T}_2^{i,m}$.

Proof: Suppose $\hat{T}_2^{i,|\tau|} = \hat{T}_2^{i,|\tau^\#|}$ proves $A(\vec{a})$. Then by Theorem VI.D.2 we have $\hat{T}_2^{i-1,\tau^\#}$ proves $Wit^i_A(f(w,\vec{a}),\vec{a})$ where f is an $FP^{\Sigma^p_{i-1}}(wit.|\tau^\#|)$ multifunction. So by Lemma V.A.1, the theory $\hat{T}_2^{i-1,\tau^\#}$ proves A.

(1) This follows if we choose $\tau = \{id\}$.

(2) This follows if we choose $\tau = Term_2^{2,1}$. Recall $\hat{R}_2^{i,1}$ is

$$EBASIC{+}\hat{\Sigma}^b_{i-1}\text{-}IND^{Term_2^{2,1}}$$

(3) This follows if we choose $\tau = Term_2^{m,j}$. Recall $\hat{T}_2^{i,m,j}$ is

$$EBASIC{+}\hat{\Sigma}^b_{i-1}\text{-}IND^{Term_2^{m,j}}$$

(4) This follows from (3) since

$$\begin{aligned}\hat{T}_2^{i,m,j} &\preceq_{\hat{\Sigma}^b_{i-j+1}} \hat{T}_2^{i,m,j-1} \preceq_{\hat{\Sigma}^b_{i-j+2}} \cdots \\ &\preceq_{\hat{\Sigma}^b_i} \hat{T}_2^{i,m,0} = \hat{T}_2^{i,m}.\end{aligned}$$

□

By $\log x$ we mean $\log_2 x$. We write $\log^{(m)} n$ to denote

$$\overbrace{\log\log\cdots\log n}^{m}$$

and we write $\log^{(0)} n$ to just denote n where n will usually be the length of an input to some function.

Corollary VI.E.2 $(i \geq 1)$

A multifunction f is $\hat{\Sigma}^b_{i+1}$-definable in $\hat{T}_2^{i,\tau}$ iff f is computable by a multifunction in $FP^{\Sigma^p_i}(wit.|\tau|)$. By choosing τ appropriately, we thus have:
$(i \geq 1, m \geq 0)$

(a) A multifunction f is $\hat{\Sigma}^b_{i+1}$-definable in T_2^i iff f is computable by a multifunction in $FP^{\Sigma^p_i}(wit.poly)$.

(b) A multifunction f is $\hat{\Sigma}^b_{i+1}$-definable in S^i_2 iff f is computable by a multifunction in $FP^{\Sigma^p_i}(wit.\log)$.

(c) A multifunction f is $\hat{\Sigma}^b_{i+1}$-definable in $\hat{R}^i_2$ iff f is computable by a multifunction in $FP^{\Sigma^p_i}(wit, \log\log)$.

(d) A multifunction f is $\hat{\Sigma}^b_{i+1}$-definable in $\hat{T}^{i,m}_2$ iff f is computable by a multifunction in $FP^{\Sigma^p_i}(wit, \log^{(m)})$.

(e) A multifunction f is $\hat{\Sigma}^b_{i+1}$-definable in $\hat{T}^{i+1,m}_2$ for $m > 0$ iff f is computable by a multifunction in $FP^{\Sigma^p_i}(wit, (\log^{(m-1)})^{O(1)})$.

(f) A multifunction f is $\hat{\Sigma}^b_{i-j+1}$-definable in $\hat{T}^{i,m,j}_2$ and $\hat{T}^{i,m}_2$ for $i \geq m > j > 0$ iff f is computable by a multifunction in $FP^{\Sigma^p_{i-j}}(wit, |Term^{m,j}_2|)$.

(g) A multifunction f is $\hat{\Sigma}^b_{i+1}$-definable in $EBASIC$ iff f is computable by a multifunction in $FP^{\Sigma^p_i}(wit, 1)$.

Proof: For the 'if' direction we use Theorem VI.B.1. For the other direction consider the Theorem VI.D.1 when we take Γ empty and Δ to be an $E\hat{\Sigma}^b_{i+1}$-formula $(\exists y \leq t(x))A(x,y)$ provable in $\hat{T}^{i,\tau}_2$. Then we get that there is a $Q^{i,\tau}$-defined (and hence, $FP^{\Sigma^p_i}(wit, |\tau|)$) multifunction f such that

$$\hat{T}^{i,\tau}_2 \vdash\rightarrow Wit^{i+1}_A(x, f(x)).$$

Given the definition of witness we thus have

$$\hat{T}^{i,\tau}_2 \vdash\rightarrow A(x, \beta(1, f(x)).$$

The other results follow from the $\hat{T}^{i,\tau}_2$ result, the definition in Remark I.B.1, and Definition VI.A.2. We are making use of the fact that $|x|_m$ is in $\theta(\log^{(m-1)}(|x|))$. □

Statement (a) in the above corollary was essentially known from Buss [14] and statement (b) was known from Krajíček [34].

Corollary VI.E.3 ($i \geq 1$) *The following equality holds:*

$$B^{|\tau|}_{i+1,2} = FP^{\Sigma^p_i}(wit, |\tau^{\#}|)$$

Proof: We know $\hat{T}^{i,|\tau|}_2 = \hat{T}^{i,(|\tau|)}_2 = \hat{T}^{i,|\tau^{\#}|}_2$ by Theorem II.G.7. The $\hat{\Sigma}^b_{i-1}$-definable multifunctions of $\hat{T}^{i+1,|\tau|}_2$ are $B^{|\tau|}_{i+1.2}$ from Corollary V.B.3 and the $\hat{\Sigma}^b_{i-1}$-definable multifunctions of $\hat{T}^{i+1,|\tau^{\#}|}_2$ are the same as those of $\hat{T}^{i,\tau^{\#}}_2$ by Corollary VI.E.1. Together with Corollary VI.E.2 this implies the result. □

Corollary VI.E.4 ($i \geq 2, i \geq m \geq j \geq 0$)

1. *A multifunction f is a $\hat{\Sigma}^b_i$-definable in $\hat{T}^{i,\tau}_2$ iff there is an $(FP^{\Sigma^p_{i-1}}(wit.1).\tau)$-local search problem P in $\hat{T}^{i,\tau}_2$ such that $\beta(1, Opt_P(x)) = y$ if and only if $f(x) = y$.*

2. *A multifunction f is a $\hat{\Sigma}^b_{i-m+1}$-definable in $\hat{T}^{i,m.m-1}_2$ and $\hat{T}^{i,m}_2$ if and only if there is an $(FP^{\Sigma^p_{i-m}}(wit.1), Term^{m,m-1}_2)$-local search problem P in $\hat{T}^{i,m.m-1}_2$ such that $\beta(1, Opt_P(x)) = y$ if and only if $f(x) = y$.*

3. *A multifunction f is a $\hat{\Sigma}^b_i$-definable in T^i_2 and $\hat{T}^{i,1,1}_2$ if and only if there is an $(FP^{\Sigma^p_{i-1}}(wit, 1), \{id\})$-local search problem P in T^i_2 such that $\beta(1.Opt_P(x)) = y$ if and only if $f(x) = y$.*

4. *A multifunction f is a $\hat{\Sigma}^b_i$-definable in $\hat{R}^{i+1}_2$ and $\hat{R}^{i+1,1}_2 = \hat{T}^{i+1.2.1}_2$ if and only if there is an $(FP^{\Sigma^p_{i-1}}(wit, 1), Term^{2,1}_2)$-local search problem P in $\hat{R}^{i+1,1}_2$ such that $\beta(1, Opt_P(x)) = y$ if and only if $f(x) = y$.*

Proof: Recall from Chapter III that $B_{i,2} = B^{|cl|}_{i,2}$. Hence, with Corollary VI.E.3 this implies $B_{i,2} = FP^{\Sigma^p_{i-1}}(wit.1)$ provided $i \geq 2$. The above results then follow from Corollary V.B.3 and the definition of $(B_{i,2}.\tau)$-problem. □

Corollary VI.E.5 ($i \geq 1$) *The $\hat{\Delta}^b_{i+1}$-predicates of $\hat{T}^{i,\tau}_2$ are the class $P^{\Sigma^p_i}(|\tau|)$. By choosing τ appropriately, we thus have:*

$(i \geq 1, m \geq 0)$

(a) The $\hat{\Delta}^b_{i+1}$-predicates of T^i_2, S^i_2, and $\hat{R}^i_2$ are the classes $P^{\Sigma^p_i}$, $P^{\Sigma^p_i}(\log)$, and $P^{\Sigma^p_i}(\log\log)$, respectively.

(b) The $\hat{\Delta}^b_{i+1}$-predicates of $\hat{T}^{i,m}_2$ are the class $P^{\Sigma^p_i}(\log^{(m)})$.

(c) The $\hat{\Delta}^b_i$-predicates of $\hat{T}^{i,m}_2$ where $i > 1, m > 0$ are the class

$$P^{\Sigma^p_{i-1}}((\log^{(m-1)})^{O(1)}).$$

(d) The $\hat{\Delta}^b_{i-j+1}$-predicates of $\hat{T}^{i,m,j}_2$ and $\hat{T}^{i,m}_2$ where $i \geq m > j > 0$, are the class $P^{\Sigma^p_{i-j}}(|Term^{m,j}_2|)$.

(e) The $\hat{\Delta}^b_{i+1}$-predicates of $EBASIC$ are the class $P^{\Sigma^p_i}(1)$ where we allow a machine in $P^{\Sigma^p_i}(1)$ is allowed $O(1)$ many queries to a Σ^p_i-oracle.

Proof: Suppose $f \in P^{\Sigma^p_i}(|\tau|)$. Since

$$P^{\Sigma^p_i}(|\tau|) \subset FP^{\Sigma^p_i}(wit.|\tau|).$$

by Theorem VI.B.1, $\hat{T}^{i,\tau}_2$ can $\hat{\Sigma}^b_{i+1}$-define f. Hence, $\hat{T}^{i,\tau}_2$ proves

$$(\forall x)(\exists y \leq 1)A_f(x,y).$$

where A_f is a $\hat{\Sigma}^b_{i+1}$-formula. The theory $\hat{T}^{i,\tau}_2$ can prove the formula $(\exists y \leq 1)A_f(x,y)$ is equivalent to

$$(A_f(x,1) \supset y = 1) \wedge (A_f(x,0) \supset y = 0)$$

which by Theorem II.G.12 is provably equivalent to a $\hat{\Pi}^b_{i+1}$-formula.

On the other hand suppose A is $\hat{\Delta}^b_{i+1}$ with respect to $\hat{T}^{i,\tau}_2$. Let A_Σ be the $\hat{\Sigma}^b_{i+1}$-formula to which A is equivalent and let A_Π be the $\hat{\Pi}^b_{i+1}$-formula to which A is equivalent. Consider the formula $B(x,y)$,

$$(\neg A_\Pi(x) \wedge y = 0) \vee (A_\Sigma(x) \wedge y = 1).$$

Certainly, the theory $\hat{T}_2^{i,\tau}$ proves $(\forall x)(\exists y \leq 1)B(x,y)$. By Remark II.B.1 and Theorem II.G.12, the theory $\hat{T}_2^{i,\tau}$ proves $(\exists y \leq 1)B(x,y)$ is equivalent to a $E\hat{\Sigma}_{i+1}^b$-formula. So by Theorem VI.D.1 there is a $FP^{\Sigma_i^p}(wit, |\tau|)$ function g such that

$$\hat{T}_2^{i,\tau} \vdash Wit_B^i(x, g(x)).$$

Given our definition of the witness predicate this implies

$$\hat{T}_2^{i,\tau} \vdash B(x, \beta(1, g(x)). \tag{VI.4}$$

Let $f(x) = \beta(1, g(x))$. Since g is $Q^{i,\dot{\tau}}$-definable, the theory $\hat{T}_2^{i,\tau}$ proves f can be defined in the form

$$(\forall x)(\exists y \leq t)(\exists v \leq \ell(s(x)))[(\exists w \leq t)(\beta(1, Out(w)) = y \wedge C(x, w, v)) \\ \wedge \neg(\exists v' \leq \ell(s(x)))(\exists w' \leq t)(v' > v \wedge C(x, w', v'))].$$

where C is a $\hat{\Sigma}_i^b$-formula, Out, s are L_2-terms (Out is supposed to return the output of g) and ℓ is a $\dot{\tau}$-term. From the definition of B, we have $f(x) = 1 \Leftrightarrow B(x,1) \Leftrightarrow A(x)$. We claim $f(x) = 1$, which is just the predicate,

$$(\exists v \leq \ell(s(x)))[(\exists w \leq t)(\beta(1, Out(w)) = 1 \wedge C(x, w, v)) \\ \wedge \neg(\exists v' \leq \ell(s(x)))(\exists w' \leq t)(v' > v \wedge C(x, w', v'))].$$

is computable in $P^{\Sigma_i^p}(|\tau|)$. This follows because the formula inside the scope of $(\exists v \leq \ell(s(x)))$ is the conjunction of a formula provably equivalent to $\hat{\Sigma}_i^b$-formula with a formula provably equivalent to a $\hat{\Pi}_i^b$-formula. Thus, with $O(|\ell(s(x))|)$ queries to a Σ_i^p-oracle one could search for a value that satisfied the first predicate inside the $(\exists v \leq \ell(s(x)))$ but did not satisfy the second. □

The S_2^i and T_2^i statements in the last corollary were known from Buss [14] and Krajíček [34]. An easy observation from the proof of Corollary VI.E.5 is the following:

Corollary VI.E.6 ($i \geq 1$) *The theory $\hat{T}_2^{i,\tau}$ proves its $\hat{\Delta}_{i+1}^b$-predicates can be written in the form*

$$(\exists v \leq \ell(s(x)))[A(x, v) \wedge \neg B(x, v+1)].$$

where A and B are $\hat{\Sigma}^b_i$-formulas and ℓ is a $\dot{\tau}$-term and s is an L_2-term.

(a) The theory S^i_2 proves its $\hat{\Delta}^b_{i+1}$-predicates can be written in the form

$$(\exists v \leq p(|s(x)|))[A(x,v) \wedge \neg B(x,v+1)].$$

where A and B are $\hat{\Sigma}^b_i$-formulas and p is a polynomial and s is a term in L_2.

(b) The theory $\hat{R}^i_2$ proves its $\hat{\Delta}^b_{i+1}$-predicates can be written in the form

$$(\exists v \leq p(||s(x)||))[A(x,v) \wedge \neg B(x,v+1)].$$

where A and B are $\hat{\Sigma}^b_i$-formulas and p is a polynomial and s is a term in L_2.

(c) For $i \geq 1, m \geq 0$, the theory $\hat{T}^{i,m}_2$ proves its $\hat{\Delta}^b_{i+1}$-predicates can be written in the form

$$(\exists v \leq p(|s(x)|_m))[A(x,v) \wedge \neg B(x,v+1)].$$

where A and B are $\hat{\Sigma}^b_i$-formulas and p is a polynomial and s is an L_2-term.

(d) Provided $i > 1, i \geq m > j > 0$, the theory $\hat{T}^{i,m,j}_2$ proves its $\hat{\Delta}^b_{i-j+1}$-predicates can be written in the form

$$(\exists v \leq \ell(s(x)))[A(x,v) \wedge \neg B(x,v+1)].$$

where A and B are $\hat{\Sigma}^b_i$-formulas and ℓ is a $Term^{m,j}_2$-term and s is an L_2-term.

(e) The theory $EBASIC$ proves its $\hat{\Delta}^b_{i+1}$-predicates can be written in the form

$$\vee^n_{v=0}[A(x,v) \wedge \neg B(x,v+1)].$$

where A and B are $\hat{\Sigma}^b_i$-formulas.

Proof: From the proof of Corollary VI.E.5 every $\hat{\Delta}^b_{i+1}$-predicate in $\hat{T}^{i,\tau}_2$ is equivalent to a formula of the form

$$(\exists v \leq \ell(s(x)))[(\exists w \leq t)(\beta(1, Out(w)) = 1 \wedge C(x,w,v))$$
$$\wedge \neg(\exists v' \leq \ell(s(x)))(\exists w' \leq t)(v' > v \wedge C(x,w',v'))].$$

where C is a $\hat{\Sigma}^b_i$-formula. The above formula is in turn provably equiavlent to

$$(\exists v \leq \ell(s(x)))[(\exists w \leq t)(\beta(1, Out(w)) = 1 \wedge C(x, w, v))$$
$$\wedge \neg(\exists v' \leq \ell(s(x)))(\exists w' \leq t)(v' \geq v + 1 \wedge C(x, w', v'))].$$

Set $A(x, v)$ to be a $\hat{\Sigma}^b_i$-formula provably equivalent to

$$(\exists w \leq t)(\beta(1, Out(w)) = 1 \wedge C(x, w, v))$$

and set $B(x, v + 1)$ to be the $\hat{\Sigma}^b_i$-formula provably equivalent to

$$(\exists v' \leq \ell(s(x)))(\exists w' \leq t)(v' \geq v + 1 \wedge C(x, w', v')).$$

This then gives the corollary. □

Corollary VI.E.6 is similar to a result of Buss Hay [10] where they show the predicates in $\Sigma^b_{i+1} \cap \Pi^b_{i+1}$ equal the class $P^{\Sigma^p_i}(\log)$ and can be written in the form $(\exists v \leq |s(x)|)(A(x, v) \wedge \neg B(x, v))$ where A and B are Σ^b_i. The S^i_2 case of our result shows the $\hat{\Delta}^b_{i+1}$-predicates of S^i_2 which are the $P^{\Sigma^p_i}(\log)$ relations can be written provably in this form in S^i_2. This is a somewhat different statement.

Theorem VI.E.7 *Fix $i \geq 1$ and let $\Gamma \rightarrow \Delta$ be a $L\hat{\Pi}^b_{i-1}$-sequent consistent with $\hat{T}^{i,\tau}_2$. The $\hat{\Sigma}^b_{i+1}$-definable multifunctions of $\hat{T}^{i,\tau}_2 + \{\Gamma \rightarrow \Delta\}$ are precisely the class $FP^{\Sigma^p_i}(wit, |\tau|)$.*

Proof: The argument is essentially the same as Theorem V.B.6. □

Remark VI.E.8 The results of this section generalize in a straightforward to the theories $T^{i,\tau}_k$ for $k \geq 2$. Using the same proof as in Theorem VI.B.1, we can $\hat{\Sigma}^b_{i+1,k}$-define $F[|\tau|]^{\hat{\Sigma}^b_{i,k}}_k(wit)$ machines in $\hat{T}^{i,\tau}_k$. An $F[|\tau|]^{\hat{\Sigma}^b_{i,k}}_k(wit)$ on input x runs in time $O(|\ell(s(x))|)$ using an oracle for a $\hat{\Sigma}^b_{i,k}$-set, where s is an L_k-term and ℓ is in τ. In terms of quasi-polynomial computations, using the same proof as in Theorem VI.A.3 one can show

$$F[|\tau|]^{\hat{\Sigma}^b_{i,k}}_k(wit) = FP^{\hat{\Sigma}^b_{i,k}}_k(wit, |\tau|).$$

where an $FP_k^{\hat{\Sigma}^b_{i,k}}(wit, |\tau|)$-computation on input x runs in time $|s(x)|$ for s an L_k-term and can make $O(\ell(|t(x)|))$ queries where t is an L_k-term.

The witnessing argument and its corollaries also go through using the same proofs as above, thus, showing that the $\hat{\Sigma}^b_{i+1,k}$-definable functions of $\hat{T}^{i,\tau}_k$ are precisely the class $FP_k^{\hat{\Sigma}^b_{i,k}}(wit, |\tau|)$.

Remark VI.E.9 Given the above remark, it is not hard to use Corollary VI.E.1 to show for $i \geq 1$ and $k \geq m \geq 0$ that

$$\hat{T}^{i,m}_{k+2} \preceq_{\hat{\Sigma}^b_{i,k+2}} \hat{T}^{i+1,m+1}_{k+2}. \tag{VI.5}$$

This will be true since for such k, $|L_{k+2}|_m$ terms and $Term^{m+1,1}_{k+2}$ terms will have the same growth so

$$\hat{T}^{i,m}_{k+2} = \hat{T}^{i+1,m+1,1}_{k+2}.$$

Yet, the generalization of Corollary VI.E.1 implies

$$\hat{T}^{i+1,m+1,1}_{k+2} \preceq_{\hat{\Sigma}^b_{i,k+2}} \hat{T}^{i+1,m+1}_{k+2}.$$

One other observation: in [16] it was shown that $S^i_3 \preceq_{\Sigma^b_{i+1,3}} R^{i+1}_3$, by (VI.5) above we have $S^i_3 \preceq_{\hat{\Sigma}^b_{i+1,3}} \hat{R}^{i+1}_3$; thus, we also have $\hat{R}^{i+1}_3 \preceq_{\hat{\Sigma}^b_{i+1,3}} R^{i+1}_3$. In Chapter VIII we will show for $k \geq 0$,

$$\hat{R}^{i+1}_{k+2} \preceq_{\hat{\Sigma}^b_{i+1,3}} R^{i+1}_{k+2}.$$

Chapter VII

Applications of the witnessing argument

In this chapter we give some applications of the witnessing argument with respect to prenex theories.

VII.A The $\hat{\Sigma}^b_{i+k}$-definable multifunctions of prenex theories

We begin by briefly discussing the $\hat{\Sigma}^b_{i+k}$-definable multifunctions of the theories $\hat{T}^{i,\tau}_2$ where $k \geq 2$. To make sure the reader is not confused by indices we emphasize we are talking about $\hat{\Sigma}^b_{i+k,2}$-definability not $\hat{\Sigma}^b_{i,k}$-definability.

The first thing to notice about the $\hat{\Sigma}^b_{i+k}$-definable multifunction of $\hat{T}^{i,\tau}_2$ is that since $EBASIC$ is contained in all of these theories, these theories can at least $\hat{\Sigma}^b_{i+k}$-define the multifunctions in the class $FP^{\Sigma^p_{i+k-1}}(wit.1)$. The second thing to notice is that $FP^{\Sigma^p_i}(wit.|\tau|)$ is contained in $FP^{\Sigma^p_{i+k-1}}(wit.1)$ for $k \geq 2$. This is because with a single query to a Σ^p_{i+1} witness oracle one can ask for a witness of the sequence of steps in a computation of an $FP^{\Sigma^p_i}(wit.|\tau|)$ machine M. Then using this witness one can read off the final output of M.

Now consider what happens with the witnessing argument for a proof of a sequent of $LE\hat{\Sigma}^b_{i+k} \cup L\hat{\Sigma}^b_i$-formulas $\Gamma \rightarrow \Delta$ in the theory $\hat{T}^{i,\tau}_2$. All of the cases can be handled as in the $EBASIC = \hat{T}^{i+k,cl}_2$ version of Theorem VI.D.1 except we

now also have a $\hat{\Sigma}^b_i$-IND^τ inference case. Recall how this case was handled in the $\hat{T}^{i,\tau}_2$ version of Theorem VI.D.1. Given the inference

$$\frac{A(b), \Gamma \rightarrow A(Sb), \Delta}{A(0), \Gamma \rightarrow A(\ell(r)), \Delta}$$

where ℓ is in τ and r is in L_2, one uses an $FP^{\Sigma^p_i}(wit, |\tau|)$ machine to binary search for a value $c \leq t(r)$ such that $A(c)$ holds but $A(Sc)$ does not. This machine was then composed with the machine that would provide a witness for the top sequent. Now by induction we can assume the top sequent can be witnessed with a function in $FP^{\Sigma^p_{i+k-1}}(wit.1)$. Since $FP^{\Sigma^p_i}(wit, |\tau|)$ is contained in the class $FP^{\Sigma^p_{i+k-1}}(wit.1)$. this whole case can be handled by a machine in $FP^{\Sigma^p_{i+k-1}}(wit.1)$. Thus, the following witnessing theorem goes through.

Theorem VII.A.1 ($i \geq 1, k \geq 2$) *Suppose* $\hat{T}^{i,\tau}_2 \vdash \Gamma \rightarrow \Delta$ *where* Γ *and* Δ *are cedents of* $LE\hat{\Sigma}^b_{i+k} \cup L\hat{\Sigma}^b_i$*-formulas. Let* $\vec{a}$ *be the free variables in this sequent. Then there is a* $Q^{i,cl}$*-definable in* $\hat{T}^{i,\tau}_2$, $FP^{\Sigma^p_{i+k-1}}(wit, 1)$ *multifunction* f *such that:*

$$\hat{T}^{i,\tau}_2 \vdash Wit^{i+k}_{\wedge\Gamma}(w, \vec{a}) \supset Wit^{i+k}_{\vee\Delta}(f(w, \vec{a}), \vec{a}).$$

When $i = 0$ *there is a* $FP^{\Sigma^p_{k-1}}(wit, 1)$ *multifunction* f *such that*

$$\mathbf{N} \models Wit^{k}_{\wedge\Gamma}(w, \vec{a}) \supset Wit^{k}_{\vee\Delta}(f(w, \vec{a}), \vec{a}).$$

For the $i = 0$ case we can certainly perform the above witnessing with a multifunction from $FP^{\Sigma^p_{k-1}}(wit, 1)$ (the induction case can be handled by a function in FP since these will all be subtheories of S^1_2); however, it seems difficult to prove in $\hat{T}^{0,\tau}_2$. From the above theorem the next theorem and its two corollaries follow by the same type of proofs as in Chapter VI.

Theorem VII.A.2 ($i \geq 0, k \geq 2$) *A multifunction* f *is a* $\hat{\Sigma}^b_{i+k}$*-definable multifunction of* $\hat{T}^{i,\tau}_2$ *if and only if* f *is in the class* $FP^{\Sigma^p_{i+k-1}}(wit, 1)$.

Corollary VII.A.3 ($i \geq 0, k \geq 2$) *The $\hat{\Delta}^b_{i+k}$-predicates of $\hat{T}^{i,\tau}_2$ are precisely the predicates in $P^{\Sigma^p_{i+k-1}}(1)$.*

Corollary VII.A.4 ($i \geq 1, k \geq 2$) *The theory $\hat{T}^{i,\tau}_2$ proves its $\hat{\Delta}^b_{i+k}$-predicates can be written in the form*

$$\vee^n_{v=0}[A(x,v) \wedge \neg B(x,v)].$$

where A and B are $\hat{\Sigma}^b_{i+k-1}$-formulas and p is a polynomial.

It should be stressed that although $EBASIC$, $\hat{T}^{i,|\tau|}_2$, and $\hat{T}^{i,\tau}_2$ all have the same $\hat{\Sigma}^b_{i+k}$-definable multifunctions, it does not seem to be the case that either $EBASIC$ or $\hat{T}^{i,|\tau|}_2$ can carry out the witnessing argument needed to show they have the same $\hat{\Sigma}^b_{i+k}$-definable functions as $\hat{T}^{i,\tau}_2$. This is because neither of these theories seems to be able to simulate the $\hat{\Sigma}^b_i$-IND^τ case of the $\hat{T}^{i,\tau}_2$ witnessing argument which required $\hat{\Sigma}^b_i$-IND^τ to prove.

VII.B A strengthened conservation result

We begin with the following result.

Theorem VII.B.1 ($i \geq 1, k \geq 0$)

(a) The theory $\hat{T}^{i+1,(|\dot{\tau}|)}_{k+2}$ is conservative over $\hat{T}^{i,\tau^\#}_{k+2}$ with respect to Boolean combinations of $\hat{\Sigma}^b_{i+1,k+2}$-formulas. That is,

$$\hat{T}^{i,\tau^\#}_{k+2} \preceq_{B(\hat{\Sigma}^b_{i+1})} \hat{T}^{i+1,(|\dot{\tau}|)}_{k+2}.$$

(b) $T^i_2 \preceq_{B(\hat{\Sigma}^b_{i+1})} S^{i+1}_2$.

(c) $S^i_3 \preceq_{B(\hat{\Sigma}^b_{i+1,3})} \hat{R}^{i+1}_3$.

(d) $\hat{T}^{i,m}_{k+2} \preceq_{B(\hat{\Sigma}^b_{i+1,k+2})} \hat{T}^{i+1,m+1}_{k+2}$.

Proof: (a) Suppose $A(\vec{a})$ is a Boolean combination of $\hat{\Sigma}^b_{i-1,k+2}$-formulas provable in $\hat{T}^{i+1,(|\dot{\tau}|)}_{k+2}$. Then A is tautologically equivalent to a formula of the form $\wedge_n \vee_j A_{nj}$ where each A_{nj} is either a $\hat{\Sigma}^b_{i+1,k+2}$-formula or a $\hat{\Pi}^b_{i+1,k+2}$-formula. So $\hat{T}^{i+1,(|\dot{\tau}|)}_{k+2}$ proves each disjunct $\vee_j A_{nj}$. Consider one such disjunct $\vee_j A_{nj}$. Let Δ_n be the cedent of $\hat{\Sigma}^b_{i+1,k+2}$-formulas in this disjunct. and let Γ_n be the $\hat{\Sigma}^b_{i+1,k+2}$-formulas that are equivalent to the negations of $\hat{\Pi}^b_{i+1,k+2}$-formulas in this disjunct. Hence, $\hat{T}^{i+1,(|\dot{\tau}|)}_{k+2}$ proves $\Gamma_n \rightarrow \Delta_n$. Now this sequent can be proved with a proof such that all formula are $L\hat{\Sigma}^b_{i+1,k+2} \cup L\hat{\Sigma}^b_{i,k+2}$. By Lemma V.A.1

$$\hat{T}^{i,\tau^\#}_{k+2} \vdash \wedge\Gamma_n \supset (\exists w \leq t_{\Gamma_n}) Wit^{i+1}_{\wedge\Gamma_n}(w, \vec{a})$$

and

$$\hat{T}^{i,\tau^\#}_{k+2} \vdash (\exists w \leq t_{\Delta_n}) Wit^{i+1}_{\vee\Delta_n}(w, \vec{a}) \supset \vee\Delta_n.$$

We can then carry out the witnessing argument of Remark VI.E.9 to show

$$\hat{T}^{i,\tau^\#}_{k+2} \vdash (\exists w \leq t_{\Gamma_n}) Wit^{i+1}_{\wedge\Gamma_n}(w, \vec{a}) \supset (\exists w \leq t_{\Delta_n}) Wit^{i+1}_{\vee\Delta_n}(w, \vec{a})$$

Hence,

$$\hat{T}^{i,\tau^\#}_{k+2} \vdash \Gamma_n \rightarrow \Delta_n.$$

Thus, $\hat{T}^{i,\tau^\#}_{k+2}$ proves $\vee_j A_{nj}$. So $\hat{T}^{i,\tau^\#}_{k+2}$ proves $A(\vec{a})$.

The remaining parts of the theorem are special cases of (a). □

The proof of Theorem VII.B.1 was adapted from the proof in Buss [14] that

$$T^i_2 + \Sigma^b_i\text{-}REPL \preceq_{B(\Sigma^b_{i+1})} S^{i+1}_2.$$

One interesting corollary of the above theorem is the following:

Corollary VII.B.2 $(i \geq 1, k \geq m \geq n \geq 0)$

$$\hat{T}^{i+n,n}_{k+2} \preceq_{B(\hat{\Sigma}^b_{i+n+1,k+2})} \hat{T}^{i+m,m}_{k+2}.$$

In particular,

$$\hat{T}^{i}_{k+2} \preceq_{B(\hat{\Sigma}^b_{i+1,k+2})} \hat{T}^{i+m,m}_{k+2}.$$

Proof: This follows from Theorem VII.B.1 since

$$\hat{T}^{i+n.n}_{k+2} \preceq_{B(\hat{\Sigma}^b_{i+n+1.k+2})} \hat{T}^{i+n+1.n+1}_{k+2} \preceq_{B(\hat{\Sigma}^b_{i+n+2.k+2})}$$
$$\cdots \preceq_{B(\hat{\Sigma}^b_{i+m-1.k+2})} \hat{T}^{i+m-1.m-1}_{k+2} \preceq_{B(\hat{\Sigma}^b_{i+m.k+2})} \hat{T}^{i+m.m}_{k+2}.$$

□

VII.C $\hat{\Delta}^b_{i+1}$-$IND^{(|\dot{\tau}|)}$

We now give a new proof that S^i_2 proves Δ^b_{i+1}-$LIND$. This fact was previously shown in Buss, Krajíček, and Takeuti [16] using an unpublished model theoretic argument of Ressayre that S^i_2+Σ^b_{i+1}-$REPL^{\{|id|\}}$ is Σ^b_i-conservative over S^i_2. We use two known results in our proof: (1) the result of Buss [14] that S^i_2 proves $\Sigma^b_{i+1} \cap \Pi^b_{i+1}$-$LIND$ and (2) the result of Krajíček [34] that the Δ^b_i-predicates are the class $P^{\Sigma^b_i}(\log)$. Once we have shown S^i_2 proves Δ^b_{i+1}-$LIND$ we show $\hat{T}^{i.|\tau|}_2$ proves $\hat{\Sigma}^b_{i+1} \cap_{|\tau|} \hat{\Pi}^b_{i+1}$-$IND^{|\dot{\tau}|}$ and use this together with Corollary VI.E.5 and our proof method for S^i_2 to show that $\hat{T}^{i.|\tau|}_2$ proves $\hat{\Delta}^b_{i+1}$-$IND^{(|\dot{\tau}|)}$. As particular cases, this shows S^i_2 proves $\hat{\Delta}^b_{i+1}$-$LIND$ and $\hat{R}^i_2$ proves $\hat{\Delta}^b_{i+1}$-$LLIND$. In Corollary IX.A.3 we show give a proof theoretic proof that S^i_2+$\hat{\Sigma}^b_{i+1}$-$REPL^{\{|id|\}}$ is $B(\hat{\Sigma}^b_{i+1})$-conservative over S^i_2. Together with the $\hat{\Delta}^b_{i+1}$-$LIND$ result this suffices to show S^i_2 proves Δ^b_{i+1}-$LIND$ without relying on results not shown in this thesis. The $\hat{R}^i_2$ result and the general result were previously unknown.

Theorem VII.C.1 *($i \geq 1$) S^i_2 proves the Δ^b_{i+1}-$LIND$ axioms.*

Proof: By Buss [14] the theory S^i_2 can prove $\Sigma^b_{i+1} \cap \Pi^b_{i+1}$-$LIND$, and by Krajíček [34], $P^{\Sigma^p_i}(\log)$ are precisely the Δ^b_{i+1}-definable predicates of S^i_2. Recall how the proof of this latter fact went. Let A be Δ^b_{i+1} with respect to S^i_2. Let A_Π be the Π^b_{i+1}-formula it is equivalent to in S^i_2 and let A_Σ be the Σ^b_{i+1}-formula it is equivalent to in S^i_2. Consider the formula $B(\vec{x}, y)$

$$(\neg A_\Pi(\vec{x}) \wedge y = 0) \vee (A_\Sigma(\vec{x}) \wedge y = 1).$$

Certainly, S_2^i proves $(\forall \vec{x})(\exists y \leq 1)B(\vec{x}, y)$. Thus, by the witnessing theorem in [33] (which is similar to the $\tau = \{|id|\}$ case of Theorem VI.D.1), there is a $FP^{\Sigma_i^p}(wit, \log)$ function g such that $S_2^i \vdash Wit^i_{(\exists y \leq 1)B}(g(\vec{x}), \vec{x})$. So by the definition of the witness predicate,

$$S_2^i \vdash Wit^i_B(\beta(2, g(\vec{x})), \vec{x}, \beta(1, g(\vec{x}))).$$

and also

$$S_2^i \vdash Wit^i_B(w, \vec{x}, y) \supset B(\vec{x}, y)$$

Thus, the theory S_2^i proves $B(\vec{x}, \beta(1, g(\vec{x}))$. Let $f(\vec{x}) = \beta(1, g(\vec{x}))$. Then S_2^1 proves $f(x) = 1 \Leftrightarrow A(x)$. This function f can be defined in S_2^i using almost the same notion of $Q^{i,\{|id|\}}$-definition that we used in Chapter VI. That is, it can be defined with a formula of the form:

$$\begin{aligned}(\forall x)(\exists y \leq 1)(\exists v \leq p(|s(x)|))[&(\exists w \leq t)(Out(w) = y \wedge A(x, w, v)) \\ &\wedge \neg(\exists v' \leq p(|s(x)|))(\exists w' \leq t)(v' > v \wedge A(x, w', v'))].\end{aligned}$$

where A is a Π_i^b-formula and where s and $Out(w)$ are L_2-terms. But this is a $\forall(\Sigma_{i+1}^b \cap \Pi_{i+1}^b)$-formula, so S_2^i proves $LIND_{f(x)=1}$. As S_2^i proves $f(x) = 1 \Leftrightarrow A(x)$, we also have S_2^i proves $LIND_A$. Hence, S_2^i proves Δ_{i+1}^b-$LIND$. □

We will now make appropriate modifications to the above argument to show $\hat{R}_2^i$ proves $\hat{\Delta}_i^b$-$LLIND$ axioms and also that $\hat{T}_2^{i,|\tau|}$ proves the $\hat{\Delta}_{i+1}^b$-$IND^{(\dot{\tau})}$ axioms. We first show $\hat{T}_2^{i,|\tau|}$ can prove $\hat{\Sigma}_{i+1}^b \cap_{|\tau|} \hat{\Pi}_{i+1}^b$-$IND^{|\dot{\tau}|}$ axioms. To do this we need the next two theorems, both of which are modifications of results found in Buss' paper [14]. First, we define a type of comprehension axiom for bounded formulas.

Definition VII.C.2 *The Ψ-$COMP^{|\tau|}$ axioms are the axioms $COMP_\alpha^{|\ell|}$:*

$$(\exists w)(\forall x \leq |\ell(b)|)(\alpha(v, x) \Leftrightarrow Bit(x, w) = 1).$$

where α is a formula in Ψ and ℓ is a term in τ.

Theorem VII.C.3 ($i \geq 1$) *The theory* $\hat{T}_2^{i,|\tau|}$ *proves the* $\hat{\Sigma}_i^b$-$COMP^{|\tau|}$ *axioms.*

Proof: Let $B(n, v)$ be the formula

$$(\exists w < 2^{|\ell(b)|})(\exists w' \leq 2^{|w|^2})[(\forall j \leq |w| \dot{-} 1)(\hat{\beta}(0, |w|, w') = Bit(1, w) \wedge$$
$$\hat{\beta}(j+1, |w|, w') = \hat{\beta}(j, |w|, w') + Bit(j+1, w)) \wedge \hat{\beta}(|w| \dot{-} 1, |w|, w') = n$$
$$\wedge(\forall x \leq |\ell(b)|)(Bit(x, w) = 1 \supset A(v, x))].$$

The first two lines of the above equation are used to say w' is a sequence of blocks of size $|w|$ which count up the number of 'On' bits in w and that n is this number. We note $\hat{T}_2^{i,|\tau|} \vdash B(0, v)$ and $\hat{T}_2^{i,|\tau|} \vdash n > j \wedge B(n, v) \supset B(j, v)$. By Theorem II.E.7, B is equivalent to a $\hat{\Sigma}_i^b$-formula. Further,

$$\hat{T}_2^{i,|\tau|} \vdash \neg B(|\ell(b)|, v),$$

so it follows from IND_B that

$$\hat{T}_2^{i,|\tau|} \vdash (\exists n \leq |\ell(b)|)(B(n, v) \wedge \neg B(n+1, v)).$$

So $\hat{T}_2^{i,|\tau|}$ proves there is a maximum value for n such that $B(n, v)$ holds. Thus, the string w whose existence is asserted for this n will have bit x turned on if and only if $A(v, x)$. □

We can now use the same sort of speed-up argument as we did with $\hat{R}_2^i$ and $\hat{\Pi}_{i-1}^b$-$REPL^2$ to get the following corollary.

Corollary VII.C.4 ($i \geq 1$). *Let* $A(v, x)$ *be a* $\hat{\Sigma}_i^b$*-formula and* $r(v)$ *be a* L_2*-term and* p *a polynomial. Then*

$$\hat{T}_2^{i,|\tau|} \vdash (\exists w)(\forall x \leq p(|\ell(r)|))(A(v, x) \Leftrightarrow Bit(x, w) = 1).$$

Theorem VII.C.5 ($i \geq 1$) $\hat{T}_2^{i,|\tau|}$ *proves* $\hat{\Sigma}_{i+1}^b \cap_{|\tau|} \hat{\Pi}_{i+1}^b$-$IND^{|\tau|}$. *In particular,* $\hat{R}_2^1$ *proves* $\hat{\Sigma}_{i+1}^b \cap_{\{||id||\}} \hat{\Pi}_{i+1}^b$-$LLIND$.

Proof: Using Remark II.C.7, it is not hard to see that any formula $A(b, \vec{v})$ in the class $\hat{\Sigma}^b_{i+1} \cap_{|\tau|} \hat{\Pi}^b_{i+1}$ can be put into the form

$$(Q_1 x_1 \leq p_1(|\ell_1(r_1)|)) \cdots (Q_m x_n \leq p_m(|\ell_n(r_n)|)) B(A_1, \ldots, A_s).$$

where each A_j is a $\hat{\Sigma}^b_i$-formula and $B(A_1, \ldots, A_s)$ denotes a Boolean combination of $A_1, \ldots, A_s$, the ℓ_i's in the above are supposed to be terms in τ, the p_i's polynomial, and the r_i's are L_2-terms. Without loss of generality we can assume that each term r_j contains only $\vec{v}$ as variables.

By an easy modification of Corollary VII.C.4, $\hat{T}^{i,|\tau|}_2$ can prove there exist $w_1, \ldots, w_s$ such that

$$(\forall x_1 \leq p_1(|\ell_1(r_1)|)) \cdots (\forall x_n \leq p_n(|\ell_n(r_n)|))[Bit(\langle \vec{x} \rangle, w_j) \Leftrightarrow A_j(\vec{x}, \vec{v})].$$

Here $\langle \vec{x} \rangle$ denotes ordered n-tuple $\langle x_1, \ldots, x_n \rangle$. Thus, given $w_1, \ldots, w_s$, A is actually equivalent to a $\hat{\Delta}^b_1$-formula. So the theorem follows as $\hat{T}^{i,|\tau|}_2$ will be able to prove $IND^{|\tau|}_A$ axioms. □

The above two theorems allow us to prove that $\hat{R}^i_2$ can prove $\hat{\Delta}^b_{i+1}$-$LLIND$ axioms and $\hat{T}^{i,|\tau|}_2$ can prove $\hat{\Delta}^b_{i+1}$-$IND^{|\tau|}$ axioms.

Corollary VII.C.6 ($i \geq 1$) *The theory $\hat{R}^i_2$ proves $\hat{\Delta}^b_{i+1}$-$LLIND$. The theories $\hat{T}^{i,|\tau|}_2$ can prove $\hat{\Delta}^b_{i+1}$-$IND^{|\tau|}$ axioms.*

Proof: The proof is almost the same as in Theorem VII.C.1. Given a $\hat{\Delta}^b_{i+1}$-predicate B in $\hat{T}^{i,|\tau|}_2$, we will have a $P^{\Sigma^p_i}(|\tau|)$ predicate $f(x) = 1$ of the form

$$(\exists v \leq p(|\ell(s(x))|))[(\exists w \leq t)(Out(w) = 1 \wedge A(x, w, v))$$
$$\wedge \neg(\exists v' \leq p(|\ell(s(x))|))(\exists w' \leq t)(v' > v \wedge A(x, w', v'))].$$

where A is a $\hat{\Pi}^b_{i-1}$-formula which is provably equivalent to B. This is a $\hat{\Sigma}^b_{i+1} \cap_{|\tau|} \hat{\Pi}^b_{i+1}$-formula so by Theorem VII.C.5, $\hat{T}^{i,|\tau|}_2$ can prove $IND^{|\tau|}_{f(x)=1}$. So we have $IND^{|\tau|}_B$. Hence, $\hat{T}^{i,|\tau|}_2$ proves $\hat{\Delta}^b_{i+1}$-$IND^{|\tau|}$. □

Another corollary of the proof of Theorem VII.C.5 is the following:

Corollary VII.C.7 ($i \geq 1$) *The* $\hat{\Sigma}^b_{i+1} \cap_{|\tau|} \hat{\Pi}^b_{i+1}$*-formulas are* $\hat{\Delta}^b_{i+1}$ *with respect to* $\hat{T}^{i,|\tau|}_2$. *The* $\hat{\Sigma}^b_{i+1} \cap_{\{||id||\}} \hat{\Pi}^b_{i+1}$*-formulas are* $\hat{\Delta}^b_{i+1}$ *with respect to* $\hat{R}^i_2$.

Proof: After substituting the w_j for the A_j in the proof of Theorem VII.C.5 the formula is a $\hat{\Delta}^b_1$-formula in $\hat{T}^{i,|\tau|}_2$. So it is equivalent in $\hat{T}^{i,|\tau|}_2$ to a $\hat{\Sigma}^b_1$-formula or a $\hat{\Pi}^b_1$-formula. Resubstituting A_j's means $\hat{T}^{i,|\tau|}_2$ can prove the original formula equivalent to a $\hat{\Sigma}^b_{i+1}$-formula or a $\hat{\Pi}^b_{i+1}$-formula. □

Corollary VII.C.8 ($i \geq 1$) *The theory* $\hat{T}^{i,|\tau|}_2$ *proves the* $\hat{\Sigma}^b_{i+1} \cap_{|\tau|} \hat{\Pi}^b_{i+1}$*-formulas can be written in the form*

$$(\exists v \leq p(|\ell(s(x))|))[A(x,v) \wedge \neg B(x,v+1)].$$

where A *and* B *are* $\hat{\Sigma}^b_i$*-formulas and* ℓ *is in* τ *and* s *is in* L_2 *and* p *is a polynomial.*

Proof: This follows from Theorem VI.E.6 and Corollary VII.C.7. □

It is unknown to the author whether for arbitrary τ, the theory $\hat{T}^{i,\tau}_2$ proves $\hat{\Delta}^b_{i+1}$-IND^τ. However, the next theorem gives another wide range of τ's for which it is provable.

Theorem VII.C.9 ($i \geq 1$) $\hat{T}^{i,\tau^\#}_2 \vdash \hat{\Delta}^b_{i+1}$-$IND^{\tau^\#}$.

Proof: Let A be $\hat{\Delta}^b_{i+1}$ with respect to $\hat{T}^{i,\tau^\#}_2$.. Let A_Σ be a $\hat{\Sigma}^b_{i+1}$-formula provably equivalent to A in $\hat{T}^{i,\tau^\#}_2$ and let A_Π be a $\hat{\Pi}^b_{i+1}$-formula provably equivalent to A in $\hat{T}^{i,\tau^\#}_2$. Let ℓ be an iterm in τ. Then the IND^ℓ_A axiom can be expressed as

$$A_\Pi(0) \wedge (\forall x \leq \ell(b))(A_\Sigma \supset A_\Pi) \supset A_\Sigma(\ell(b))$$

which is a $\hat{\Sigma}^b_{i+1}$-formula. Since $\hat{T}^{i+1,|\tau|}_2$ proves the $\hat{\Delta}^b_{i+1}$-$IND^{\tau^\#}$ axioms by Theorem II.G.8 it is a consequence $\hat{T}^{i+1,|\tau|}_2$. But then by Theorem VII.B.1, it is a consequence of $\hat{T}^{i,\tau^\#}_2$. □

Chapter VIII

Prenex replacement theories

In this chapter we investigate the prenex replacement theories of arithmetic, $\hat{C}_2^{i,|\tau|}$, which we defined in Chapter II. We will show $\hat{C}_2^{i,|\tau|} \vdash \hat{T}_2^{i,|\tau|}$ and that $\hat{C}_2^{i,|\tau|}$ is $B(\hat{\Sigma}_{i+1}^b)$-conservative over $\hat{T}_2^{i,|\tau|}$. This same method can be used to show for $i \geq 1$ that $\hat{T}_2^{i+1,\|\tau\|}+\hat{\Pi}_i^b\text{-}REPL^{|\tau|}$ is $B(\hat{\Sigma}_{i+1}^b)$-conservative over $\hat{T}_2^{i+1,|\tau|}$. In particular, this will show for $i \geq 1$ that R_2^{i+1} is $B(\hat{\Sigma}_{i+1}^b)$-conservative over $\hat{R}_2^{i-1}$. We have delayed this chapter until now because our witness predicate will be slightly different from earlier chapters and we did not want to cause undue confusion by switching between the types of witness predicate.

VIII.A Preliminaries

To begin we prove the following theorem.

Theorem VIII.A.1 $(i \geq 0)$ $\hat{C}_2^{i,|\tau|} \vdash \hat{T}_2^{i,|\tau|}$.

Proof: The proof is by induction on i. Since the base case and the induction step are similar we will prove both cases simultaneously and indicate any differences. Let $A(x) := (\exists y \leq t)B(x,y)$ be a $\hat{\Sigma}_i^b$-formula. We want to show

$$\hat{C}_2^{i,|\tau|} \vdash A(0) \wedge (\forall x)(A(x) \supset A(Sx)) \supset (\forall x)A(|\ell(x)|)$$

for each term ℓ in τ. Let u be a new variable. By Remark II.C.7.

$$\hat{C}_2^{i,|\tau|} \vdash (\forall x)(A(x) \supset A(Sx)) \\ \supset (\forall x < |\ell(u)|)(\exists y \leq t(Sx))(\forall z \leq t(x))(B(x,z) \supset B(Sx,y)).$$

$\hat{C}_2^{i,|\tau|}$ can convert the formula inside the scope of the $(\exists y \leq t(Sx))$ into a $\hat{\Pi}_i^b$-formula using Remark II.C.7 and Lemma II.C.6 since B is a $\hat{\Pi}_{i-1}^b$-formula. So by $\hat{\Pi}_i^b$-$REPL^{|\tau|}$.

$$\hat{C}_2^{i,|\tau|} \vdash (\forall x)(A(x) \supset A(Sx)) \supset \\ (\exists w \leq 2 \cdot (t^* \# \ell(u)))(\forall x < |\ell(u)|) \\ (\forall z \leq t(x))(B(x,z) \supset B(Sx, \dot{\beta}(x, |t^*|, t, w))).$$

Let $f(a,w,b) := cond(a, b, \dot{\beta}(a, |t^*|, t, w))$. Thus,

$$\hat{C}_2^{i,|\tau|} \vdash B(0,b) \wedge (\forall x)(A(x) \supset A(Sx)) \supset \\ (\exists w \leq 2 \cdot (t^* \# \ell(u)))(\forall x < |\ell(u)|) \\ (B(x, f(x,w,b)) \supset B(Sx, \dot{\beta}(x, |t^*|, t, w))).$$

So,

$$\hat{C}_2^{i,|\tau|} \vdash A(0) \wedge (\forall x)(A(x) \supset A(Sx)) \supset \\ (\exists w \leq 2 \cdot (t^* \# \ell(u)))[B(0, \dot{\beta}(0, |t^*|, t, w) \wedge (\forall x < |\ell(u)|)(\exists y \leq t(Sx)) \\ (B(x, \dot{\beta}(x, |t^*|, t, w)) \supset B(Sx, \dot{\beta}(x+1, |t^*|, t, w)))].$$

Since $B \in \hat{\Pi}_{i-1}^b$ (in the $i = 0$ case B is open), we can use $\hat{\Pi}_{i-1}^b$-$IND^{|\tau|}$ (in the base case we use $Open$-$IND^{|\tau|}$), to get

$$\hat{C}_2^{i,|\tau|} \vdash A(0) \wedge (\forall x)(A(x) \supset A(Sx)) \supset \\ (\exists w \leq 2 \cdot t^* \# \ell(u)) B(|\ell(u)|, \dot{\beta}(|u|, |t^*|, t, w)).$$

In the base case we have $Open$-$IND^{|\tau|}$ axioms in our theory so the above goes through. For $i > 0$ we are justified in using $\hat{\Pi}_{i-1}^b$-$IND^{|\tau|}$ by the induction hypothesis and Theorem II.C.1. From this last equation we at last derive

$$\hat{C}_2^{i,|\tau|} \vdash A(0) \wedge (\forall x)(A(x) \supset A(Sx)) \supset (\forall x) A(|\ell(x)|).$$

The above proof was a modification of the proof in Buss [13] that S_2^i is contained in S_2^1+Σ_{i+1}^b-$REPL$. To show $\hat{C}_2^{i,|\tau|}$ is $B(\hat{\Sigma}_{i+1}^b)$-conservative over $\hat{T}_2^{i,|\tau|}$ we first show $\hat{C}_2^{i,|\tau|}$ is $\hat{\Sigma}_{i+1}^b$-conservative over $\hat{T}_2^{i,|\tau|}$. To do this we need to show the class $FP^{\Sigma_i^p}(wit, |\dot{\tau}|)$ is closed under a certain kind of parallel computation. This result is a modification of a result in Buss, Krajíček, and Takeuti [16].

Theorem VIII.A.2 *($i \geq 1$) Suppose $f(j, \vec{x}) \in FP^{\Sigma_i^p}(wit, ||\tau||)$ is bounded by an L_2-term $t^*(\vec{x})$ for each $j \leq p(|\ell|)$ where p is a polynomial and $\ell \in \tau$. Then:*

(a) $f_{p(|\ell|)}(\vec{x}) = \sum_{j=0}^{p(|\ell|)-1} f(j, \vec{x}) \cdot 2^{j \cdot |t^*|}$ *is in* $FP^{\Sigma_i^p}(wit, ||\tau||)$.

(b) $\hat{T}_2^{i,|\tau|}$ *proves* $\hat{\beta}(j, |t^*|, f_{p(|\ell|)}(\vec{x})) = f(j, \vec{x})$.

Proof: For (a) we can assume that f is computed by an $F[||\tau||]_2^{\Sigma_i^p}(wit)$ machine M_f with runtime bounded by $c \cdot ||s(x)||$. Such a machine runs oblivious to the witness strings provided with the 'Yes' answers. So the jth query of a run of M_f will only depend on the inputs and the previous queries. For the moment fix j and $\vec{x}$. For each string of $c \cdot ||s(\vec{x})||$ possible oracle responses to queries posed by $M_f(j, \vec{x})$ there is a different valid precomputation of $M_f(j, \vec{x})$. Thus, there are potentially $2^{c \cdot ||s(\vec{x})||} - 1$ many different queries that could be posed in any valid precomputation of $M_f(i, \vec{x})$. Thus, for all the j's less than $p(|\ell(a)|) - 1$ there are potentially $p(|\ell(a)|) \cdot (2^{c \cdot ||s(\vec{x})||} - 1)$ different queries that could be made. One can put all such potentially different queries into a table indexed by pairs (j, k) where $j < p(|\ell(a)|)$ and $0 < k < 2^{c \cdot ||s(\vec{x})||}$. Let $l = |k| - 1$ and define $q_{j,k}$ to be the $(l+1)$st query in a precomputation of $M_f(j, \vec{x})$ if, for all $r \leq l$, the $(r+1)$st query in the precomputation was answered 'Yes' if and only if $Bit(r, k) = 1$. So $q_{j,k}$ is the next query of $M_f(j, \vec{x})$ will ask, if the previous queries were answered as specified by the bits in the binary representation of k.

We now described an $FP^{\Sigma_i^p}(wit, ||\tau||)$ machine, $M'_{f_{p(|\ell|)}}$, that computes $f_{p(|\ell|)}$. First, $M'_{f_{p(|\ell|)}}$ computes all entries in the above table. Let $\Omega(q)$ be M'_f's

Σ_i^p-oracle. It then binary searches for the number m of 'Yes' answers that $\Omega(q)$ would provide for this table. A witness for the query: "Do there exist m entries of our table answered 'Yes' by $\Omega(q)$?" provides all the 'Yes' answers in the table. The machine $M_{f_{p(|\ell|)}}(a, \vec{x})$ then computes $M_f(j, \vec{x})$ for each $j \leq p(|\ell(a)|)$ using the table rather than the oracle. As M_f runs this computation it makes a list of the final queries of each machine. Since this list of final queries is $(|\dot{\tau}|)$-sharply bounded. M_f can query an appropriate Σ_i^p-modification of $\Omega(q)$ to get witnesses for these queries concatenated together in the form that $f_{p(|\ell|)}$ is supposed to output. The binary search takes

$$O(|(p(|\ell(a)|) \cdot (2^{c \cdot ||s(\vec{x})||} - 1))|)$$

many queries. This is $O(||\ell(a)||) + c \cdot ||s(\vec{x})||)$ many queries so the machine $M'_{f_{p(|\ell|)}}$ in $FP^{\Sigma_i^p}(wit, ||\tau||)$.

For (b), one first represents $M'_{f_{p(|\ell|)}}$ in $\hat{T}_2^{i,|\tau|}$ by the $F[||\tau||]_2^{\Sigma_i^p}(wit)$ machine $M_{f_{p(|\ell|)}}$ from Theorem VI.A.3 which simulates it. One then needs to argue that $\hat{T}_2^{i,|\tau|}$ can prove simple facts about the witnesses returned by the oracle for $M_{f_{p(|\ell|)}}$. The machine $M_{f_{p(|\ell|)}}$ can be defined in $\hat{T}_2^{i,|\tau|}$ with a $\hat{\Sigma}_{i+1}^b \cap_{|\tau|} \hat{\Pi}_{i+1}^b$-formula by Theorem VI.B.1. Using $\hat{\Sigma}_{i+1}^b \cap_{|\tau|} \hat{\Pi}_{i+1}^b$-$IND^{(|\dot{\tau}|)}$, $\hat{T}_2^{i,|\tau|}$ can prove the witness returned by the oracle for $M_{f_{p(|\ell|)}}$ must be a valid computation of $M'_{f_{p(|\ell|)}}$ using oracle $\Omega(q)$ and has the desired properties. □

Essentially the same proof can be used to show:

Theorem VIII.A.3 *($i \geq 1$) Suppose $f(j, \vec{x}) \in FP^{\Sigma_i^p}(wit, ||\tau|^{\#}|)$ is bounded by an L_2-term $t^*(\vec{x})$ for each $j \leq p(|\ell|)$ where p is a polynomial and $\ell \in \tau^{\#}$. Then:*

(a) $f_{p(|\ell|)}(\vec{x}) = \sum_{j=0}^{p(|\ell|)-1} f(j, \vec{x}) \cdot 2^{j \cdot |t^*|}$ *is in* $FP^{\Sigma_i^p}(wit, ||\tau|^{\#}|)$.

(b) $\hat{T}_2^{i,|\tau|^{\#}}$ *can prove* $\hat{\beta}(j, |t^*|, f_{p(|\ell|)}(\vec{x})) = f(j, \vec{x})$.

We also need the $Q^{i,(|\dot{\tau}|)}$-definable multifunctions of $\hat{T}_2^{i,|\tau|}$ are closed under $(|\dot{\tau}|)$-bounded μ-operator.

Theorem VIII.A.4 ($i \geq 1$) *Let f be a $Q^{i,(|\dot{\tau}|)}$-definable multifunctions of $\hat{T}_2^{i,\dot{\tau}}$. Then the function*

$$(\mu j < |\ell(x)|)[f(j,x) = 0]$$

is $Q^{i,(|\dot{\tau}|)}$-definable in $\hat{T}_2^{i,|\tau|}$.

Proof: Consider the multifunction

$$g(j,x) := cond((\forall n < |\ell(x)|)(n < j \wedge f(n,x) > 0), 1.0).$$

Define $(\mu i < |\ell(x)|)[f(i,x) = 0]$ to be

$$\sum_{j=0}^{|\ell(x)=1|} g(j,x) \cdot 2^j.$$

Then $(\mu j < |\ell(x)|)[f(j,x) = 0]$ is $|\ell(x)| \dot{-} h(x)$. □

VIII.B Witnessing arguments for replacement theories

We now use a witnessing argument to show that $\hat{C}_2^{i,|\tau|}$ is $\hat{\Sigma}_{i+1}^b$-conservative over $\hat{T}_2^{i,|\tau|}$.

By Corollary IV.B.4, a free-cut free $\hat{C}_2^{i,|\tau|}$-proof of an $E\hat{\Sigma}_{i+1}^b$-formula can contain formulas in

$$LE\hat{\Sigma}_{i+1}^b \cup L|A|_{|\tau|}\hat{\Sigma}_{i+1}^b \cup LE|A|_{|\tau|}\hat{\Pi}_i^b.$$

where $|A|_{|\tau|}$ means a quantifier of the form $(\forall x \leq |\ell(t)|)$ where ℓ is in $|\tau|$ and t is in L_2. So we have to modify our witness predicate of Chapter III slightly to carry out the witnessing argument. For this section, we define our witness predicate as follows:

If $A(\vec{a}) \in L|A|_{|\tau|}\hat{\Pi}_i^b$ then

$$Wit_A^{i+1}(w,\vec{a}) \quad := \quad A(\vec{a})$$

If $A(\vec{a})$ is of the form $(\exists x \leq t(\vec{a}))B$ where $A \in \hat{\Sigma}^b_{i-1} \cup E|A|_{|\tau|}\hat{\Pi}^b_i$ then

$$Wit^{i+1}_A(w, \vec{a}) \;:=\; b \leq t(\vec{a}) \wedge B(b, \vec{a})$$

If $A(\vec{a})$ is of the form $(\forall x \leq |\ell(s)|)(\exists y \leq t)B$ where $A \in |A|_{|\tau|}\hat{\Sigma}^b_{i+1}$, then we define

$$Wit^{i+1}_A(w, \vec{a}) \;:=\; w \leq 2 \cdot (t^* \# \ell(s)) \wedge (\forall x \leq |\ell(s)|)B(\dot{\beta}(x, |t^*|, t, w), \vec{a})$$

If $A(\vec{a})$ is of the form $(\exists x_1 \leq t_1)(\exists x_2 \leq t_2)B$ where $A \in E\hat{\Sigma}^b_{i+1}$ then

$$Wit^{i+1}_A(w, \vec{a}) \;:=\; ispair(w) \wedge \beta(1, w) \leq t_1 \wedge \beta(2, w) \leq t_2 \wedge B(\beta(1, 2), \beta(2, w), \vec{a}).$$

From the above definitions, it is easy to see we have the following analog of Lemma V.A.1.

Lemma VIII.B.1 ($i \geq 1$) *Let A be any formula in*

$$LE\hat{\Sigma}^b_{i+1} \cup L|A|_{|\tau|}\hat{\Sigma}^b_{i+1} \cup LE|A|_{|\tau|}\hat{\Pi}^b_i$$

with free variables $\vec{a}$. Then:

$$EBASIC \vdash Wit^{i+1}_A(w, \vec{a}) \supset A(\vec{a}). \tag{VIII.1}$$

There is a term t_A such that

$$\hat{C}^{i,|\tau|}_2 \vdash A(\vec{a}) \Leftrightarrow (\exists w \leq t_A(\vec{a}))Wit^i_A(w, \vec{a}). \tag{VIII.2}$$

For this term t_A we also have

$$EBASIC \vdash Wit^{i+1}_A(w, \vec{a}) \supset w \leq t_A. \tag{VIII.3}$$

Remark VIII.B.2 If $A \in LE\hat{\Sigma}^b_{i+1}$ then (VIII.2) requires only $EBASIC$ to prove.

We extend the definition of witness for a formula to a definition for witness for a cedent in the same way as in the section on the $\hat{\Sigma}^b_i$-definable functions of $\hat{R}^i_2$. A lemma similar to the above will also hold for cedents.

Theorem VIII.B.3 ($i \geq 1$) *Suppose* $\hat{C}^{i,|\tau|}_2 \vdash \Gamma \rightarrow \Delta$ *where* Γ *and* Δ *are cedents of formulas in*

$$LE\hat{\Sigma}^b_{i+1} \cup L|A|_{|\tau|}\hat{\Sigma}^b_{i+1} \cup LE|A|_{|\tau|}\hat{\Pi}^b_i.$$

Let $\vec{a}$ *be the free variables in this sequent. Then there is a* $FP^{\Sigma^p_i}(wit, ||\tau||)$ *multi-function* f *which is* $Q^{i,(|\tau|)}$*-defined in* $\hat{T}^{i,|\tau|}_2$ *such that:*

$$\hat{T}^{i,|\tau|}_2 \vdash Wit^{i+1}_{\wedge\Gamma}(w, \vec{a}) \supset Wit^{i+1}_{\vee\Delta}(f(w, \vec{a}), \vec{a}).$$

Proof: This is proved by induction on the number of sequents in an $\hat{C}^{i,|\tau|}_2$ proof of $\Gamma \rightarrow \Delta$. By cut elimination, we can assume all the sequents in the proof are in

$$LE\hat{\Sigma}^b_{i+1} \cup L|A|_{|\tau|}\hat{\Sigma}^b_{i+1} \cup LE|A|_{|\tau|}\hat{\Pi}^b_i.$$

Almost all of the cases can be handled as in the witnessing argument for the $\hat{\Sigma}^b_{i+1}$-definable functions of $\hat{T}^{i,|\tau|}_2$. However, the $\forall$: cases change, and we also have the additional case for $REPL^{|\tau|}$-inferences.

($\forall$:left case) Suppose we have the inference:

$$\frac{A(t), \Gamma \rightarrow \Delta}{t \leq s, (\forall x \leq s)A(x), \Gamma \rightarrow \Delta}$$

By the induction hypothesis there is a $Q^{i,(|\tau|)}$-definable g such that

$$\hat{T}^{i,|\tau|}_2 \vdash Wit^{i+1}_{A(t)\wedge\Gamma}(w, \vec{a}) \supset Wit^{i+1}_{\vee\Delta}(g(w, \vec{a}), \vec{a}).$$

The definition of Wit^{i+1} implies

$$\hat{T}^{i,|\tau|}_2 \vdash Wit^{i+1}_{t\leq s\wedge(\forall x\leq s)A(x)\wedge\Gamma}(w, \vec{a}) \supset t \leq s \wedge Wit^{i+1}_{(\forall x\leq s)A(x)\wedge\Gamma}(\beta(2, w), \vec{a}).$$

By cut-elimination, $(\forall x \leq s)A(x)$ must be in $L|A|_{|\tau|}\hat{\Pi}^b_i$ or in $|A|_{|\tau|}\hat{\Sigma}^b_{i-1}$. In the first case, we define f to be

$$f(w,\vec{a}) \;:=\; g(\langle 0, \beta(2,\beta(2,w))\rangle,\vec{a})$$

This function is $Q^{i,(|\tau|)}$ definable in $\hat{T}^{i,|\tau|}_2$ and it is not hard to see that

$$\hat{T}^{i,|\tau|}_2 \vdash Wit^{i+1}_{t\leq s\wedge(\forall x\leq s)A(x)\wedge\Gamma}(w,\vec{a}) \supset Wit^{i+1}_{\forall\Delta}(f(w,\vec{a}),\vec{a}).$$

In the second case, $(\forall x \leq s)A(x)$ is $|A|_{|\tau|}\hat{\Sigma}^b_{i+1}$. So s is of the form $|\ell(s')|$ where ℓ is in τ. Let

$$h(w,\vec{a}) \;=\; \langle \dot{\beta}(s(\vec{a}),|t^*|,t,\beta(1,\beta(2,w))),\beta(2,\beta(2,w))\rangle.$$

By the definition of witness, we have

$$\hat{T}^{i,|\tau|}_2 \vdash Wit^{i+1}_{t\leq s\wedge(\forall x\leq s)A(x)\wedge\Gamma}(w,\vec{a}) \supset$$
$$Wit^{i+1}_{A(t)\wedge\Gamma}(h(w,\vec{a}),\vec{a})$$

So define $f(w,\vec{a})$ to be $g(h(w,\vec{a}),\vec{a})$. It is easy to see f has the desired properties.

($\forall$:right case) Suppose we have the inference:

$$\frac{b \leq t, \Gamma\rightarrow A(b),\Delta}{\Gamma\rightarrow(\forall x\leq t)A(x),\Delta}$$

By the induction hypothesis there is a $Q^{i,(|\tau|)}$-definable g in $FP^{\Sigma^p_i}(wit,||\tau||)$ such that

$$\hat{T}^{i,|\tau|}_2 \vdash Wit^{i+1}_{b\leq t\wedge\Gamma}(w,\vec{a},b) \supset Wit^{i+1}_{A\vee\Delta}(g(w,\vec{a},b),\vec{a},b).$$

By cut-elimination, $(\forall x \leq t)A(x)$ is either in $L|A|_{|\tau|}\hat{\Pi}^b_i$ or is in $|A|_{|\tau|}\hat{\Sigma}^b_{i-1}$. In the first case, $(\exists x \leq t)\neg A(x)$ is a Σ^p_i-predicate. So we ask an oracle for this predicate for a value $b \leq t$ such that $\neg A(b)$ holds. If such a value exists we set $f(w,\vec{a}) = g(\langle 0,w\rangle,\vec{a},b)$. If no such value exists we let $f(w,\vec{a}) = \langle 0,0\rangle$ since

$(\forall x \leq t)A(x)$ would in that case be a valid $L|A||_{|\tau|}\hat{\Pi}^b_i$-formula. In the second case, $(\forall x \leq t)A(x)$ is really of the form

$$(\forall x \leq |\ell(s)|)(\exists y \leq t')B(x,y)$$

where B is a $\hat{\Pi}^b_i$-formula. Since Wit^{i+1}_A is provably equivalent to $\hat{\Pi}^b_i$-formula in $EBASIC$, its characteristic function $\chi_{Wit^{i+1}_A}$ is $Q^{i,(|\dot{\tau}|)}$-definable in $\hat{T}^{i,|\tau|}_2$. Let k be the multifunction

$$k(w,\vec{a}) = (\mu j < |\ell(s)|)[\neg\chi_{Wit^{i+1}_A}(\beta(1,g(w,\vec{a},j)),\vec{a},j) = 0]$$

Clearly, k can be $Q^{i,(|\dot{\tau}|)}$-defined as a composition of $FP^{\Sigma^p_i}(wit,||\tau||)$ multifunctions. Now define $f(w,\vec{a})$ from k as follows:

$$f(w,\vec{a}) = \\ cond(K_{=}(k,|\ell(s)|), \sum_{j=0}^{|\ell(s)-1|} \beta(1,g(w,\vec{a},j)\cdot 2^{j\cdot|(t')^*|},\beta(2,g(w,\vec{a},k))$$

It is not hard to see using Theorem VIII.A.2 that

$$\hat{T}^{i,|\tau|}_2 \vdash Wit^{i+1}_\Gamma(w,\vec{a}) \supset Wit^{i+1}_{(\forall x\leq|\ell(s)|)A\vee\Delta}(f(w,\vec{a}),\vec{a}).$$

($\hat{\Pi}^b_i - REPL^{|\tau|}$**:case**) Suppose we have the inference:

$$\frac{\Gamma\rightarrow(\forall x \leq |\ell(s)|)(\exists y \leq t)A(x,y),\Delta}{\Gamma\rightarrow(\exists w \leq 2\cdot(t^*\#\ell(s)))(\forall x \leq |\ell(s)|)A(x,\dot{\beta}(x,|t^*|,t,w))),\Delta}$$

where ℓ is in τ and s in L_2. By the induction hypothesis there is a $Q^{i,(|\dot{\tau}|)}$-definable g in $FP^{\Sigma^p_i}(wit,|(|\dot{\tau}|)|)$ such that

$$\hat{T}^{i,|\tau|}_2 \vdash Wit^{i+1}_\Gamma(w,\vec{a},b) \supset Wit^{i+1}_{(\forall x\leq|\ell(s)|)(\exists y\leq t)A\vee\Delta}(g(w,\vec{a}),\vec{a}).$$

For this case, it suffices to notice that the predicates

$$Wit^{i+1}_{(\forall x\leq|\ell(s)|)(\exists y\leq t)A}$$

and

$$Wit^{i+1}_{(\exists w \leq 2\cdot(t^{\cdot}\#|\ell(s)|))(\forall x \leq |s|)A}$$

are the same. Hence, if we let $f = g$ then

$$\hat{T}_2^{i,|\tau|} \vdash Wit^{i+1}_{\Gamma}(w,\vec{a},b) \supset Wit^{i+1}_{(\exists w \leq 2\cdot(t^{\cdot}\#\ell(s)))(\forall x \leq |\ell(s)|)A \vee \Delta}(f(w,\vec{a}),\vec{a}).$$

This completes all possible cases and the proof. □

Theorem VIII.B.4 ($i \geq 1$) *Suppose*

$$\hat{T}_2^{i+1,||\tau||}+\hat{\Pi}^b_i\text{-}REPL^{|\tau|} \vdash \Gamma \rightarrow \Delta$$

where Γ *and* Δ *are cedents of formulas in*

$$LE\hat{\Sigma}^b_{i+1} \cup L|A|_{|\tau|}\hat{\Sigma}^b_{i+1} \cup LE|A|_{|\tau|}\hat{\Pi}^b_i.$$

Let $\vec{a}$ *be the free variables in this sequent.*

Then there is a $FP^{\Sigma^p_i}(wit, ||\tau|^{\#}|)$ *multifunction* f *which is* $Q^{i,|\tau|^{\#}}$*-defined in* $\hat{T}_2^{i,|\tau|^{\#}}$ *such that:*

$$\hat{T}_2^{i,|\tau|^{\#}} \vdash Wit^{i+1}_{\wedge\Gamma}(w,\vec{a}) \supset Wit^{i+1}_{\vee\Delta}(f(w,\vec{a}),\vec{a}).$$

Proof: This is proved by induction on the number of sequents in an

$$\hat{T}_2^{i+1,||\tau||}+\hat{\Pi}^b_i\text{-}REPL^{|\tau|}$$

proof of $\Gamma \rightarrow \Delta$. By cut elimination, we can assume all the sequents in the proof are in

$$LE\hat{\Sigma}^b_{i+1} \cup L|A|_{|\tau|}\hat{\Sigma}^b_{i+1} \cup LE|A|_{|\tau|}\hat{\Pi}^b_i.$$

We handle all cases of this witnessing argument as in Theorem VIII.B.3 above except for the ($\hat{\Sigma}^b_{i+1}$-$IND^{||\tau||}$) case which we handle as in Theorem VI.D.2. □

Corollary VIII.B.5 ($i \geq 1$)

(a) The theory $\hat{C}_2^{i,|\tau|}$ *is* $\hat{\Sigma}_{i+1}^b$*-conservative over* $\hat{T}_2^{i,|\tau|}$.

(b) The theory $\hat{T}_2^{i+1,||\tau||}+\hat{\Pi}_i^b$*-REPL*$^{|\tau|}$ *is* $\hat{\Sigma}_{i+1}^b$*-conservative over* $\hat{T}_2^{i,|\tau|^\#}$ *and also over* $\hat{T}_2^{i+1,||\tau||}$.

(c) The theory R_2^{i+1} *is* $\hat{\Sigma}_{i+1}^b$*-conservative over* $\hat{R}_2^{i+1}$.

Proof: (a) Suppose $\hat{C}_2^{i,|\tau|} \vdash (\exists x \leq t)A(x,\vec{a})$ where A is $\hat{\Pi}_i^b$. Then by Theorem VIII.B.3.

$$\hat{T}_2^{i,|\tau|} \vdash Wit^{i+1}_{(\exists x \leq t)A}(f(x,\vec{a}),\vec{a}).$$

By Lemma VIII.B.1.

$$\hat{T}_2^{i,|\tau|} \vdash Wit^{i+1}_{(\exists x \leq t)A}(w,\vec{a}) \supset (\exists x \leq t)A(x,\vec{a}).$$

So

$$\hat{T}_2^{i,|\tau|} \vdash (\exists x \leq t)A(x,\vec{a}).$$

(b) Follows from Theorem VIII.B.4 by the same argument as in (a). Recall by Theorem II.G.8, $\hat{T}_2^{i,|\tau|^\#} \subseteq \hat{T}_2^{i+1,||\tau||}$.

(c) Follows from the $\tau = \{id\}$ case of (b) and Theorem II.E.1.

□

Corollary VIII.B.6 ($i \geq 1$)

(a) The theory $\hat{C}_2^{i,|\tau|}$ *is* $B(\hat{\Sigma}_{i+1}^b)$*-conservative over* $\hat{T}_2^{i,|\tau|}$.

(b) The theory $\hat{T}_2^{i+1,||\tau||}+\hat{\Pi}_i^b$*-REPL*$^{|\tau|}$ *is* $B(\hat{\Sigma}_{i+1}^b)$*-conservative over* $\hat{T}_2^{i,|\tau|^\#}$ *and also over* $\hat{T}_2^{i+1,||\tau||}$.

(c) The theory R_2^{i+1} *is* $B(\hat{\Sigma}_{i+1}^b)$*-conservative over* $\hat{R}_2^{i+1}$.

Proof: By Remark VIII.B.2, we can use the method of Theorem VII.B.1 to prove the above result. □

Note the above corollary does not imply $\hat{T}_2^{i,|\tau|} = \hat{C}_2^{i,|\tau|}$ since $\hat{T}_2^{i,|\tau|}$ cannot necessarily prove any $\hat{\Pi}_i^b$-$REPL^m$ axiom is equivalent to a $B(\hat{\Sigma}_{i+1}^b)$-formula. Similarly, the above result does not necessarily imply R_2^i equals $\hat{R}_2^i$.

We now briefly consider the $\hat{\Sigma}_{i+k}^b$-definable functions of $\hat{C}_2^{i,|\tau|}$ for k greater than 1. Since $\hat{C}_2^{i,|\tau|}$ contains $EBASIC$, it can certainly define the functions in $FP^{\Sigma_i^p}(wit, 1)$. For the converse, consider any proof of a sequent of formulas in

$$LE\hat{\Sigma}_{i+k}^b \cup L|A|_{|\tau|}\hat{\Sigma}_{i+1}^b \cup LE|A|_{|\tau|}\hat{\Pi}_i^b.$$

For all formulas not in $LE\hat{\Sigma}_{i+k}^b \backslash \hat{\Pi}_{i+k-1}^b$, we can let the witness predicate just be the formula itself. Otherwise, we define the witness predicate as Wit^{i+k} where either the definition of Wit^{i+k} is from earlier in this section or from the $\hat{\Sigma}_i^b$-definability section (they will both be equivalent for the remaining cases).

Theorem VIII.B.7 ($i \geq 1, k \geq 2$) *Suppose* $\hat{C}_2^{i,|\tau|} \vdash \Gamma \rightarrow \Delta$ *where the formulas in* Γ *and* Δ *are cedents of formulas in*

$$LE\hat{\Sigma}_{i+k}^b \cup L|A|_{|\tau|}\hat{\Sigma}_{i+1}^b \cup LE|A|_{|\tau|}\hat{\Pi}_i^b.$$

Let $\vec{a}$ *be the free variables in this sequent. Then there is a* $Q^{i,cl}$*-definable in* $\hat{C}_2^{i,|\tau|}$. $FP^{\Sigma_{i+k-1}^p}(wit, 1)$ *multifunction* f *such that:*

$$\hat{C}_2^{i,|\tau|} \vdash Wit_{\wedge\Gamma}^{i+k}(w, \vec{a}) \supset Wit_{\vee\Delta}^{i+k}(f(w, \vec{a}), \vec{a}).$$

When $i = 0$ *there is a* $FP^{\Sigma_{k-1}^p}(wit, 1)$ *multifunction* f *such that*

$$\mathbf{N} \models Wit_{\wedge\Gamma}^{k}(w, \vec{a}) \supset Wit_{\vee\Delta}^{k}(f(w, \vec{a}), \vec{a}).$$

Proof: All the cases can be handled in essentially the same way as in the $\hat{\Sigma}_{i-1}^b$-witnessing argument. The only case where there is a slight difference is ($\hat{\Pi}_i^b$ – $REPL^{|\tau|}$:case). In this case you actually need $\hat{\Pi}_i^b - REPL^{|\tau|}$ to argue in $\hat{C}_2^{i,|\tau|}$ that

a witness multifunction for the top sequent in such an inference will be a witness multifunction for the lower sequent. □

From the above theorem the next theorem and its two corollaries follow by the same type of proofs as in Chapter VI.

Theorem VIII.B.8 *($i \geq 0, k \geq 2$) The $\hat{\Sigma}^b_{i+k}$-definable multifunctions of $\hat{C}^{i,\tau}_2$ are precisely the class $FP^{\Sigma^p_{i+k-1}}(wit, 1)$.*

Corollary VIII.B.9 *($i \geq 0, k \geq 2$) The $\hat{\Delta}^b_{i+k}$-predicates of $\hat{T}^{i,\tau}_2$ are precisely the predicates in $P^{\Sigma^p_{i+k-1}}(1)$.*

Corollary VIII.B.10 *($i \geq 1, k \geq 2$) The theory $\hat{C}^{i,\tau}_2$ proves its $\hat{\Delta}^b_{i+k}$-predicates can be written in the form*

$$\vee^n_{v=0}[A(x, v) \wedge \neg B(x, v+1)].$$

where A and B are $\hat{\Sigma}^b_{i+k-1}$-formulas and p is a polynomial.

One last interesting question about prenex replacement theories is the following: Does T^i_2 contain $\hat{C}^{i,|\tau|}_2$ for any τ? Obviously, since $T^i_2 = \hat{T}^{i,\{id\}}_2$, it contains the theories $\hat{T}^{i,|\tau|}_2$ for all τ. Yet, even though $\hat{C}^{i,|\tau|}_2$ is $B(\hat{\Sigma}^b_{i+1})$-conservative over $\hat{T}^{i,|\tau|}_2$, it seems difficult to prove T^i_2 contains $\hat{C}^{i,|\tau|}_2$ for any τ.

Chapter IX

Single-valuedness in $\hat{T}_2^{i,|\tau|}$ and $\hat{C}_2^{i,|\tau|}$

In this chapter we investigate the functions (as opposed to multifunctions) definable in the theories $\hat{T}_2^{i,|\tau|}$ and $\hat{T}_2^{i,\tau}$. We begin by investigating the relationship between bounded comprehension axioms and bounded replacement axioms. Then we define a notion of a τ-bounded function. We show $\hat{T}_2^{i,|\tau|}$ and $\hat{T}_2^{i,\tau}$ can prove the multifunctions defined using $\hat{\Delta}_{i+1}^b$-$COMP^{|\tau|}$ axioms are single-valued. As a converse we show for $j \leq i+1$ every τ-bounded $\hat{\Sigma}_{i+1}^b$-definable function in $\hat{T}_2^{i,\tau}$ and $\hat{T}_2^{i,|\tau|}$ can be defined using a $\hat{\Delta}_j^b$-$COMP^{|\tau|}$ axiom. This enables us to give a characterization for $j \leq i+1$ the $\hat{\Sigma}_j^b$-definable τ-bounded functions of $\hat{T}_2^{i,|\tau|}$ and $\hat{T}_2^{i,\tau}$ in terms of parallel computations of $\hat{\Delta}_j^b$-predicates. We suggest some characterizations of these classes. In particular, we show the $\hat{\Sigma}_i^b$-definable functions of $\hat{R}_2^i$ are precisely the function in $FNC^{\Sigma_i^p}$. Our results are mainly for the case where $i > 0$. In the last two sections we investigate a weaker notion than $\hat{\Sigma}_1^b$-definability, $\hat{\Sigma}_{1,|\tau|}^b$-definability, and show some results about the $\hat{\Sigma}_{1,|\tau|}^b$-definable functions of $\tilde{C}_2^{0,|\tau|}$, a subtheory of $\hat{C}_2^{0,|\tau|}$.

IX.A Replacement and comprehension axioms

In this section, we investigate the relationship between comprehension axioms and replacement axioms. We will use the results of this section in the next section where we address the issue of single-valuedness in bounded arithmetic theories and we will also use them in the last section of this chapter where we characterize the $\hat{\Sigma}^b_{1,|\tau|}$-definable functions of $\bar{C}_2^{0,|\tau|}$.

We begin with a lemma which shows $EBASIC$+*open-REPL*$^{|\tau|}$ can take the transpose of a $(|\ell| \times 2)$ matrix where $\ell \in \tau$.

Lemma IX.A.1 *Let r, s and t be L_2-terms and ℓ a term in τ.*
Define $m := \max(r^*, t^*)$ and $m' := 2 \cdot m\#\ell(s)$ and let $M(i, x, w, w')$ be the formula

$$\dot{\beta}(i, |m|, t, \dot{\beta}(x, 2 \cdot |m|, 2^{2\cdot|m|}, w)) = \dot{\beta}(x, |t^*|, t, \dot{\beta}(i, |m'|, t^*\#\ell(s), w')).$$

*The theory $EBASIC$+*open-REPL*$^{|\tau|}$ proves*

$$(\forall w)(\exists w' \leq 2^{2\cdot|m'|})(\forall x \leq |\ell(s)|)(M(1, x, w, w') \wedge M(2, x, w, w')).$$

Proof: It trivial that $EBASIC$ proves

$$(\forall x)(\exists y \leq t))(\dot{\beta}(1, |m|, t, \dot{\beta}(x, 2 \cdot |m|, 2^{2\cdot|m|}, w)) = y).$$

and also

$$(\forall x)(\exists z \leq r))(\dot{\beta}(2, |m|, t, \dot{\beta}(x, 2 \cdot |m|, 2^{2\cdot|m|}, w)) = z).$$

The result then follows from *open-REPL*$^{|\tau|}$ and pairing. □

Theorem IX.A.2 ($i \geq 0$) *The theory $T := EBASIC$+$\hat{\Pi}^b_i$-*REPL*$^{|\tau|}$ proves the $\hat{\Sigma}^b_{i+1}$-*REPL*$^{|\tau|}$ axioms. Hence, $\hat{C}_2^{i,|\tau|}$ proves the $\hat{\Sigma}^b_{i+1}$-*REPL*$^{|\tau|}$ axioms.*

Proof: The second sentence follows since $\hat{C}_2^{i,|\tau|}$ contains T. So we prove the first statement. Let $A(x, y) := (\exists z \leq t')B(x, y, z)$ be a $\hat{\Sigma}^b_{i+1}$-formula. The formula

$$(\forall x \leq |\ell(s)|)(\exists y \leq t)A(x, y)$$

is thus the formula

$$(\forall x \leq |\ell(s)|)(\exists y \leq t)(\exists z \leq r)B(x, y, z).$$

Here ℓ is suppose to be a term in τ. Let m be $\max r^*, t^*$. Using pairing this formula is provably equivalent in T to

$$(\forall x \leq |\ell(s)|)(\exists y' \leq 2^{2\cdot|m|})B(x, \dot{\beta}(1, |m|, t, y'), \dot{\beta}(2, |m|, s, y')).$$

By $\hat{\Pi}^b_i$-$REPL^{|\tau|}$ this formula is equivalent to

$$(\exists w' \leq 2 \cdot (2^{2\cdot|m|}\#\ell(s))(\forall x \leq |\ell(s)|)$$
$$B(x, \dot{\beta}(1, |m|, t, \dot{\beta}(x, 2 \cdot |m|, 2^{2\cdot|m|}, w'), \dot{\beta}(2, |m|, r, \dot{\beta}(x, 2 \cdot |m|, 2^{2\cdot|m|}, w')).$$

Let m' equal $2 \cdot m\#\ell(s)$. Using Lemma IX.A.1, the theory T can prove this implies

$$(\exists w' \leq 2^{2\cdot|m'|})(\forall x \leq |\ell(s)|)$$
$$B(x, \dot{\beta}(x, |t^*|, t, \dot{\beta}(1, |m'|, t^*\#\ell(s), w')), \dot{\beta}(x, |r^*|, r, \beta(2, |m'|, 2(r^*\#\ell(s)), w'))).$$

Undoing the pairing, T can show this implies

$$(\exists w \leq 2(t^*\#\ell(s))(\exists v \leq 2(r^*\#\ell(s))(\forall x \leq |\ell(s)|)B(x, \dot{\beta}(x, |t^*|, t, w), \dot{\beta}(x, |r^*|, r, v)).$$

Finally, using $\hat{\Pi}^b_i$-$REPL^{|\tau|}$ the theory T proves this implies

$$(\exists w \leq 2 \cdot (t^*\#\ell(s))(\forall x \leq |\ell(s)|)B(x, y, \dot{\beta}(x, |t^*|, t, w)).$$

□

Corollary IX.A.3 ($i \geq 1$) *The theory* $T := S^i_2$+Σ^b_{i+1}-$REPL^{\{id\}}$ *is* $B(\hat{\Sigma}^b_{i+1})$-*conservative over* S^i_2.

Proof: First note using $\hat{\Sigma}^b_{i+1}$-$REPL^{\{|id|\}}$ and pairing one can prove every Σ^b_{i+1}-formula is provably equivalent to a $\hat{\Sigma}^b_{i+1}$-formula. So $EBASIC$+$\hat{\Sigma}^b_{i+1}$-$REPL^{\{id\}}$ proves Σ^b_{i+1}-$REPL^{\{|id|\}}$. By Theorem IX.A.2, $\hat{C}^{i,\{|id|\}}_2$ can prove $\hat{\Sigma}^b_{i+1}$-$REPL^{\{id\}}$

and since $\hat{C}_2^{i,\{|id|\}}$ is $B(\hat{\Sigma}_{i+1}^b$-conservative over S_2^i by Corollary VIII.B.6 and Theorem II.E.1 this gives the result. □

We use Theorem IX.A.2 to prove the next theorem about comprehension axioms.

Theorem IX.A.4 $(i \geq 0)$ $\hat{C}_2^{i,|\tau|}$ *proves any* $\hat{\Delta}_{i+1}^b$-$COMP^{|\tau|}$ *axiom.*

Proof: Let $A(j,x)$ be $\hat{\Delta}_{i+1}^b$ with respect to $\hat{C}_2^{i,|\tau|}$. It is easy to see that $\hat{C}_2^{i,|\tau|}$ proves

$$(\forall x)(\forall j \leq |\ell(s)|)(\exists y \leq 1)((A(j,x) \wedge y = 1) \vee (\neg A(j,x) \wedge y = 0)$$

where ℓ is an iterm in τ. The formula inside the scope of the leftmost universals is provably equivalent to a $\hat{\Sigma}_{i+1}^b$-formula since A is a $\hat{\Delta}_{i+1}^b$-predicate. By Theorem IX.A.2, the theory $\hat{C}_2^{i,|\tau|}$ proves

$$(\exists y \leq 2 \cdot (1\#\ell(s)))(\forall j \leq |\ell(s)|)[(A(j,x) \wedge \dot{\beta}(j,|1|,1,y)) = 1) \\ \vee(\neg A(j,x) \wedge \dot{\beta}(j,|1|,1,y) = 0))]$$

The theory $EBASIC$ can prove $\dot{\beta}(j,|1|,1,y) = \hat{\beta}(j,|1|,y)$ which is the definition of $Bit(j,y)$. Hence, the theorem follows. □

We will use the next corollary when we discuss the single-valued functions of $\hat{T}_2^{i,|\tau|}$.

Corollary IX.A.5 $(i \geq 1)$ *The theory* $\hat{T}_2^{i,|\tau|}$ *proves the* $\hat{\Delta}_{i+1}^b$-$COMP^{|\tau|}$ *axioms.*

Proof: By Theorem IX.A.4, the theory $\hat{C}_2^{i,|\tau|}$ proves any $\hat{\Delta}_{i+1}^b$-$COMP^{|\tau|}$ axiom. Any $\hat{\Delta}_{i+1}^b$-$COMP^{|\tau|}$ axiom of $\hat{T}_2^{i,|\tau|}$ is provably equivalent to a $\hat{\Sigma}_{i+1}^b$-formula in $\hat{T}_2^{i,|\tau|}$. Hence, by Corollary VIII.B.6 the theory $\hat{T}_2^{i,|\tau|}$ proves this axiom. □

This corollary has the following interesting converse.

Theorem IX.A.6 ($i \geq 1$) *The theory* $\hat{T}_2^{i,|\tau|}$ *is the same theory as*

$$T := EBASIC + open\text{-}IND^{|\tau|} + \hat{\Sigma}_i^b\text{-}COMP^{|\tau|}$$

Proof: That T is contained in $\hat{T}_2^{i,|\tau|}$ follows from Corollary IX.A.5. Let $A(x)$ be a $\hat{\Sigma}_i^b$-formula and consider the $IND_{A,|\ell|}$ axiom. The $IND_{A,|\ell|}$ axiom is implied by

$$A(0) \wedge (\forall z \leq |\ell(x)|)(A(z) \supset A(Sz)) \supset (\forall z \leq |\ell(x)|)A(x) \qquad \text{(IX.1)}$$

where ℓ is in τ. Now T proves

$$(\exists y)(\forall z \leq |\ell(z)|)(A(z) \Leftrightarrow Bit(z, y))$$

and by $open\text{-}IND^{|\tau|}$

$$Bit(0, y) \wedge (\forall z \leq |\ell(x)|)(Bit(z, y) \supset Bit(Sz, y)) \supset (\forall z \leq |\ell(x)|)Bit(z, y).$$

Together these imply (IX.1) and the theorem. □

IX.B Comprehension and single-valuedness

The general question of what are $\hat{\Sigma}_i^b$-definable functions in $\hat{T}_2^{i,|\tau|}$ or $\hat{T}_2^{i,\tau}$ seems hard. Nevertheless, the next definition allows us to answer an interesting portion of this problem.

Definition IX.B.1 *A function* $f(x)$ *is* τ*-bounded if* $f(x) \leq \ell(t(x))$ *for some* L_2*-term* t *and some* τ*-iterm* ℓ.

Lemma IX.B.2 *The theory* $\hat{T}_2^{0,|\tau|}$ *proves the following bit-extensionality axioms* $(BITEX_\ell)$*:*

$$(\forall i < |\ell(a)|)(Bit(a, i) = Bit(b, i)) \supset LSP(a, |\ell(a)|) = LSP(b, |\ell(b)|)$$

where ℓ *is in* τ*. We call the collection of these axioms for any* $\ell \in \tau$ *the* τ*-*$BITEX$ *axioms.*

Proof: This is easily proved by IND^{ℓ}_{A} on the following formula $A(c)$ which is provably equivalent to a $\hat{\Pi}^b_0$-formula in $\hat{T}^{0,|\tau|}_2$:

$$(\forall i < |\ell(a)|)(i \leq c \wedge Bit(a,i) = Bit(b,i)) \supset$$
$$LSP(a,|\ell(a)|) = LSP(b,|\ell(b)|).$$

□

We now give a class of τ-bounded functions definable in $\hat{T}^{i,|\tau|}_2$ and $\hat{T}^{i,\tau}_2$.

Theorem IX.B.3 $(i \geq 1)$

Let $B(i,x)$ be a $\hat{\Delta}^b_{i+1}$-predicate in $\hat{T}^{i,\tau}_2$ and let $\ell \in \tau$. Then

$$\hat{T}^{i,|\tau|}_2 \vdash (\forall x)(\exists! y)[y \leq \ell(v) \wedge (\forall i < |\ell(v)|)(B(i.x) \equiv Bit(i,y))].$$

Let $B(i.x)$ be a $\hat{\Delta}^b_{i+1}$-predicate in $\hat{T}^{i,|\tau|}_2$ and let $\ell \in \tau$. Then

$$\hat{T}^{i,|\tau|}_2 \vdash (\forall x)(\exists! y)[y \leq \ell(v) \wedge (\forall i < |\ell(v)|)(B(i,x) \equiv Bit(i,y))].$$

Proof: Existence of a y follows from Corollary IX.A.5. Uniqueness follows from Lemma IX.B.2. □

Given this theorem the next obvious question is: Can every τ-bounded function in $\hat{T}^{i,|\tau|}_2$ or $\hat{T}^{i,\tau}_2$ be written in this way? The answer is yes. We first show for $j \leq i$ that every τ-bounded $\hat{\Sigma}^b_j$-definable function of $\hat{T}^{i,|\tau|}_2$ and $\hat{T}^{i,\tau}_2$ can be defined in this way. Then we show the $\hat{\Sigma}^b_{i+1}$-case.

Theorem IX.B.4 $(i \geq j \geq 1)$

(1) Every τ-bounded $\hat{\Sigma}^b_j$-definable function of $\hat{T}^{i,\tau}_2$ is definable as

$$(\forall x)(\exists! y)[y \leq \ell(v) \wedge (\forall n < |\ell(v)|)(B(n,x) \equiv Bit(n,y))].$$

for some B which is $\hat{\Delta}^b_j$ in $\hat{T}^{i,\tau}_2$ and for some ℓ in τ.

(2) Every τ-bounded $\hat{\Sigma}^b_j$-definable function of $\hat{T}^{i,|tau|}_2$ is definable as

$$(\forall x)(\exists! y)[y \leq \ell(v) \wedge (\forall n < |\ell(v)|)(B(n.x) \equiv Bit(n.y))].$$

for some B which is $\hat{\Delta}^b_j$ in $\hat{T}^{i,|\tau|}_2$ and for some ℓ in τ.

Proof: Since the same proof works in both cases we only show the $\hat{T}^{i,|\tau|}_2$ case. That we can use any $\hat{\Delta}^b_j$-predicate to define a τ-bounded function in $\hat{T}^{i,|\tau|}_2$ in this manner is a consequence of Theorem IX.B.3. On the other hand, let A be a $\hat{\Sigma}^b_j$-formula. Suppose $\hat{T}^{i,|\tau|}_2$ defines a function f by proving $(\forall x)(\exists z)A(x,z)$ and also $A(x,y) \wedge A(x,z) \supset z = y$. Then for $y \leq k$ we can define the predicate $A_k(x.n)$ which computes the nth bit of y satisfying A as either

$$A^{\Sigma}_k(x,n) := n < |k| \wedge (\exists y \leq k)(A(x,y) \wedge Bit(n.y) = 1)$$

or

$$A^{\Pi}_k(x,n) := n < |k| \wedge (\forall y \leq k)(A(x,y) \supset Bit(n.y) = 1).$$

The theory $EBASIC$ proves A^{Σ}_k is a equivalent to a $\hat{\Sigma}^b_j$-formula and A^{Π}_k is equivalent to a $\hat{\Pi}^b_j$-formula. For $\ell(v)$ in τ, the theory $\hat{T}^{i,|\tau|}_2$ proves $A^{\Sigma}_{\ell(v)}(x.n) \supset A^{\Pi}_{\ell(v)}(x.n)$ and proves $A^{\Pi}_{\ell(v)}(x,n) \supset A^{\Sigma}_{\ell(v)}(x,n)$. This can be done using the existence and uniqueness condition of f which are provable in $\hat{T}^{i,|\tau|}_2$. So the predicate $A_{\ell(v)}$ is $\hat{\Delta}^b_j$ with respect to $\hat{T}^{i,|\tau|}_2$. Now by $\hat{\Sigma}^b_j$-$IND^{|\tau|}$, the theory $\hat{T}^{i,|\tau|}_2$ proves

$$y \leq \ell(v) \wedge (\forall n < |\ell(v)|)(A_{\ell(v)}(x,n) \equiv Bit(i,y)) \supset (y \leq \ell(v) \wedge A(x.y)).$$

Likewise, using $\hat{\Pi}^b_j$-$IND^{|\tau|}$ and Theorem II.G.11, the theory $\hat{T}^{i,|\tau|}_2$ proves

$$y \leq \ell(v) \wedge A(x,y) \supset [y \leq \ell(v) \wedge (\forall n < |\ell(v)|)(A_{\ell(v)}(x,n) \equiv Bit(n,y))].$$

Thus, $(\forall x)(\exists! y)(y \leq \ell(v) \wedge A(x,y))$ is provably equivalent in $\hat{T}^{i,|\tau|}_2$ to

$$(\forall x)(\exists! y)(y \leq \ell(v) \wedge (\forall n < |\ell(v)|)(A_{\ell(v)}(x,n) \equiv Bit(n.y))).$$

So we have established the theorem. □

Theorem IX.B.5 ($i \geq 1$) *Every τ-bounded $\hat{\Sigma}^b_{i-1}$-definable functions of $\hat{T}^{i,\tau}_2$ (resp. $\hat{T}^{i,|\tau|}_2$) is definable as*

$$(\forall x)(\exists! y)[y \leq \ell(v) \wedge (\forall n < |\ell(v)|)(B(n,x) \equiv Bit(n,y))].$$

for some B which is $\hat{\Delta}^b_{i+1}$ with respect to $\hat{T}^{i,\tau}_2$ (resp. $\hat{T}^{i,|\tau|}_2$) and for some ℓ in τ.

Proof: Since the same proof works in both cases we show only the $\hat{T}^{i,|\tau|}_2$ case. That we can use any $\hat{\Delta}^b_{i+1}$-predicate to define a τ-bounded function in $\hat{T}^{i,|\tau|}_2$ in this manner is a consequence of Theorem IX.B.3. On the other hand, let A be a $\hat{\Sigma}^b_{i+1}$-formula. Suppose $\hat{T}^{i,|\tau|}_2$ defines a function g by proving $(\forall x)(\exists z)A(x,z)$ and also $A(x,y) \wedge A(x,z) \supset z = y$. By Theorem VI.D.2 there is a $Q^{i,(|\dot{\tau}|)}$-defined multifunction f such that $\hat{T}^{i,|\tau|}_2$ proves $Wit^{i+1}_A(f(x),x)$. By our definition of witness this implies $\hat{T}^{i,|\tau|}_2$ proves $A(x,\beta(1,f(x)))$. Since $\hat{T}^{i,|\tau|}_2$ proves $A(x,y) \wedge A(x,z) \supset z = y$, it can prove $\beta(1,f(x))$ is single-valued and so $\beta(1,f(x)) = g$. From the $Q^{i,(|\dot{\tau}|)}$-definition of f the theory $\hat{T}^{i,|\tau|}_2$ can prove the following formula instead of $(\forall x)(\exists z)A(x,z)$ to define g

$$\begin{aligned}(\forall x)(\exists y \leq t_f)(\exists v_f \leq \ell_f(s_f(x)))[&\\ &(\exists w_f \leq t_f)(\beta(1,Out_f(w_f)) = y \wedge A_f(x,w_f,v_f))\\ &\wedge\neg(\exists v'_f \leq \ell_f(s_f(x)))(\exists w'_f \leq t_f)(v'_f > v_f \wedge A_f(x,w'_f,v'_f))].\end{aligned}$$

where A_f is a $\hat{\Sigma}^b_i$-formula. Consider the two formulas $A^{\Sigma}(n,x)$

$$\begin{aligned}(\exists v_f \leq \ell_f(s_f(x)))[(\exists w_f \leq t_f)(Bit(n,\beta(1,Out_f(w_f))) = 1 \wedge A_f(x,w_f,v_f))&\\ \wedge\neg(\exists v'_f \leq \ell_f(s_f(x)))(\exists w'_f \leq t_f)(v'_f > v_f \wedge A_f(x,w'_f,v'_f))]&\end{aligned}$$

and $A^{\Pi}(n,x)$

$$\begin{aligned}\neg(\exists v_f \leq \ell_f(s_f(x)))[(\exists w_f \leq t_f)(Bit(n,\beta(1,Out_f(w_f))) = 0 \wedge A_f(x,w_f,v_f))&\\ \wedge\neg(\exists v'_f \leq \ell_f(s_f(x)))(\exists w'_f \leq t_f)(v'_f > v_f \wedge A_f(x,w'_f,v'_f))]&\end{aligned}$$

The theory $\hat{T}^{i,|\tau|}_2$ proves A^{Σ} is equivalent to a $\hat{\Sigma}^b_i$-formula and A^{Π} is equivalent to a $\hat{\Pi}^b_i$-formula. Further since $\hat{T}^{i,|\tau|}_2$ proves g is single-valued $\hat{T}^{i,|\tau|}_2$ proves $A^{\Sigma} \Leftrightarrow A^{\Pi}$.

So the predicate $A^*(n,x)$ that the nth bit of $g(x)$ is 1 is $\hat{\Delta}^b_{i+1}$ with respect to $\hat{T}^{i,\tau}_2$. Now if g is τ-bounded it can be bounded by some term $\ell(t(x))$ for ℓ in τ. By Theorem IX.B.3. the theory $\hat{T}^{i,|\tau|}_2$ proves

$$(\forall x)(\exists! y)[y \leq \ell(t) \wedge (\forall n < |\ell(t)|)(A^*(n,x) \equiv Bit(n,y))].$$

That the function defined by the above is the same as g follows from τ-$BITE.\Sigma$.

□

Definition IX.B.6 *Let $\mathcal{C}$ be a class of predicates. A function $f(x)$ is in τ-PFC (τ-parallel function $\mathcal{C}$) iff its output is bounded $\ell(x) \in \tau$ and its ith bit is computed by $B(i,x) \in \mathcal{C}$.*

Corollary IX.B.7

($i \geq 1$) The class of τ-bounded $\hat{\Sigma}^b_{i+1}$-definable functions of $\hat{T}^{i,\tau}_2$ is precisely the class τ-$PFP^{\Sigma^p_i}(|\tau|)$.

($i \geq 1$) The class of τ-bounded $\hat{\Sigma}^b_{i+1}$-definable functions of both $\hat{T}^{i,|\tau|}_2$ and $\hat{C}^{i,|\tau|}_2$ is precisely the class τ-$PFP^{\Sigma^p_i}(||\tau||)$.

Proof: This follows from Theorem IX.B.5 since by Corollary VI.E.5 the $\hat{\Delta}^b_{i+1}$-predicates of $\hat{T}^{i,\tau}_2$ and $\hat{T}^{i,|\tau|}_2$ are respectively $P^{\Sigma^p_i}(|\tau|)$ and $P^{\Sigma^p_i}(||\tau||)$. □

Definition IX.B.8 *For a class of multifunctions Ψ, we write $S\Psi$ for is the restriction to $0-1$ functions.*

Corollary IX.B.9

($i > 1$) The class of τ-bounded $\hat{\Sigma}^b_i$-definable functions of $\hat{T}^{i,|\tau|}_2$ is precisely the class τ-$PFP^{\Sigma^p_i}(|\tau^{\#}|)$.

($i \geq 1$) The class of τ-bounded $\hat{\Sigma}^b_i$-definable functions of $\hat{T}^{i,|\tau|}_2$ is precisely the class τ-$PF((SB^{|\tau|}_{i,2}) = 0)$.

($i \geq 1$) *The class of* τ*-bounded* $\hat{\Sigma}^b_i$*-definable functions of* $\hat{T}^{i,\tau}_2$ *is precisely the class* τ-$PF((S\pi LS^{B_{i,2}}_{\tau}) = 0)$.

Proof: These statements all follow from Theorem IX.B.4. The $\hat{\Delta}^b_i$-predicates of $\hat{T}^{i,|\tau|}_2$ for $i > 1$ are precisely $P^{\Sigma^p_i}(|\tau^{\#}|)$ by Corollary VI.E.1 and Corollary VI.E.5. That the $\hat{\Delta}^b_i$-predicates of $\hat{T}^{i,|\tau|}_2$ and $\hat{T}^{i,\tau}_2$ for $i \geq 1$ will be respectively $(SB^{|\tau|}_{i,2}) = 0$ and $(S\pi LS^{B_{i,2}}_{\tau}) = 0$ can be easily proven from our characterization of the multi-functions for these classes. □

Corollary IX.B.10

($i \geq 1$) *The class of* τ*-bounded* $\hat{\Sigma}^b_{i+1}$*-definable functions of* $\hat{T}^{i,|\tau|}_2$ *is precisely the class* τ-$PF(\hat{\Sigma}^b_{i+1} \cap_{|\tau|} \hat{\Pi}^b_{i+1})$.

($i > 1$) *The class of* τ*-bounded* $\hat{\Sigma}^b_i$*-definable functions of both* $\hat{T}^{i,|\tau|}_2$ *and* $\hat{C}^{i,|\tau|}_2$ *is precisely the class* τ-$PF(\hat{\Sigma}^b_i \cap_{|\tau^{\#}|} \hat{\Pi}^b_i)$.

Proof: These statements follows from Theorem IX.B.4, Theorem IX.B.5, and Corollary VII.C.7. □

IX.C Single-valuedness in S^i_2 and R^{i+1}_2

In this section, we use the results of the last section to show the $\hat{\Sigma}^b_{i+1}$-definable functions of S^i_2 and R^{i+1}_2 are the circuit classes $(FNC^1)^{\Sigma^p_i}$ and $(FNC)^{\Sigma^p_i}$ respectively. We begin with some definition needed to define these classes. Our basis for the circuit classes we consider will always be 0, 1, $\wedge$, $\vee$, $\neg$.

Definition IX.C.1 *An* oracle circuit C_n *on the n-variables,* $x_1, \ldots x_n$ *is a directed acyclic graph whose sources are labelled with either* 0, 1, *or* x_i *for some* $1 \leq i \leq n$, *whose internal nodes are labelled with* $\wedge$, $\vee$, $\neg$, *or* $\mathcal{O}$, *and whose sinks are labelled with distinct natural numbers. We require also the* $\wedge$ *and* $\vee$ *labelled*

nodes have fan-in 2, the $\neg$ *labelled nodes have fan-in 1, and all the oracle nodes* $\mathcal{O}$ *have the same fan-in* $f(n) \geq n$. *Inputs lines to an oracle gates are labelled* $0, \ldots f(n)-1$. *Further we require that if a sink is labelled* i *then for each* $j < i$ *there is a sink labelled* j. *We call source nodes of a circuit* inputs, *internal nodes of a circuit* gates, *and the sink nodes of a circuit* outputs.

Definition IX.C.2 *The* size *of an oracle circuit is the number of its nodes. We assign a depth to the nodes of an oracle circuit as follows: inputs,* $\wedge$, $\vee$, *and* $\neg$ *gates all have depth* 1, *oracle gates with fan-in* $f(n)$ *have depth* $|f(n)|$ *The* depth *of an oracle circuit is maximal sum of the depths along any of its directed paths.*

Definition IX.C.3 *Let* A *be an oracle set. A family of oracle circuits* $\{C_n\}$ *computes a function* $f : \mathbf{N} \mapsto \mathbf{N}$ *as follows: An input* x *is evaluated on the circuit* $C_{|x|}$ *starting at the inputs according to the usual rules of propositional logic. An oracle gate on inputs* $a_0, \ldots a_{f(n)}$ *outputs* 1 *iff* $a = \sum_{i=0}^{f(n)-1} a_i \cdot 2^i$ *is in* A. *The output node labelled* j *corresponds to the* j*th bit of the output of* f *on* x.

Since the circuit classes we are dealing with are all bigger than FP we will only require the following weak form of uniformity. By a logspace function we mean a function computed on a machine with three tapes a read-only input tape, a write-only output tape and whose use is restricted to be the log of the input length.

Definition IX.C.4 *A family of oracle circuits* $\{C_n\}$ *is* logspace uniform *is there is a logspace function which on input* n *outputs* C_n.

It should be obvious that any logspace uniform circuit is polynomial size. Other stronger notions of uniformity such as U_{E^*} are discussed in Ruzzo [44]. All of these notions will be equivalent for the classes we will consider, essentially the same proofs as we do go through; however, U_{E^*} uniformity would require several more definitions.

Definition IX.C.5

($i \geq 1$) The class $(FNC^1)^{\Sigma_i^p}$ is the class of functions computed by log depth logspace uniform families of circuits with an oracle for a set in Σ_i^p.

($i \geq 1$) The class $FNC^{\Sigma_i^p}$ is the class of functions computed by poly-log depth logspace uniform families of circuits with an oracle for a set in Σ_i^p.

($i \geq 1$) The class $(NC^1)^{\Sigma_i^p}$ is the class of predicates computed by $0-1$ valued functions in $(FNC^1)^{\Sigma_i^p}$.

($i \geq 1$) The class $NC^{\Sigma_i^p}$ is the class of predicates computed by $0-1$ valued functions in $FNC^{\Sigma_i^p}$.

We define the classes FNC, FNC^1, NC, and NC^1 similarly to the above except without access to oracles gates. We chose logspace uniformity partly because Allen [2] has shown that the Σ_1^b-definable functions of R_2^1 are logspace uniform FNC. Thus, S_2^1 and R_2^1 can define the functions in the class logspace uniform FNC^1 and FNC.

Bloch [8] shows the Σ_{i+1}^b-definable functions of S_2^i are precisely the class $(FNC^1)^{\Sigma_i^p}$. He calls this class $\square_{i,2}^c$, however. Selman [45] is a good survey of what is known about this class. He defines a class $PF_{tt}^{\Sigma_i^p}$ which is essentially equivalent to $(FNC^1)^{\Sigma_i^p}$ and shows that if

$$(FNC^1)^{\Sigma_i^p} = FP^{\Sigma_i^p}(\log n)$$

then $RP = NP$. Here RP is random polynomial time. The oracles for functions in the class $FP^{\Sigma_i^p}(\log n)$ do not return witnesses. It is unknown to the author if $(FNC^1)^{\Sigma_i^p} = FP^{\Sigma_i^p}$ implies the collapse of the polynomial hierarchy. Less is known about the class $FNC^{\Sigma_i^p}$ although there is some discussion in Bloch [8]. The next lemma is due to Bloch [8].

Lemma IX.C.6 *A function $f(x)$ is in $(FNC^1)^{\Sigma_i^p}$ (resp. $FNC^{\Sigma_i^p}$) iff its bit-graph $Bit(j, f(x))$ is in $(NC^1)^{\Sigma_i^p}$ (resp. $NC^{\Sigma_i^p}$).*

Proof: To compute the jth bit of a function f in $(FNC^1)^{\Sigma_i^p}$ just compose a multiplexer with the circuit for f. The resulting circuit will be in $(NC^1)^{\Sigma_i^p}$. Suppose for each $j \leq |f(x)|$ the predicate $Bit(j, f(x))$ was in $(NC^1)^{\Sigma_i^p}$ then if we just output these circuits in parallel we have a circuit in $(FNC^1)^{\Sigma_i^p}$ computing f. □

Theorem IX.C.7

($i \geq 1$) The $\hat{\Sigma}^b_{i+1}$-definable functions of S^i_2 are precisely the class $(FNC^1)^{\Sigma_i^p}$.

($i \geq 1$) The $\hat{\Sigma}^b_{i+1}$-definable functions of R^{i+1}_2 are precisely the class $(FNC)^{\Sigma_i^p}$.

Proof: Our method of proof will be similar to that of Buss and Hay [10]. By Corollary IX.B.10, we know the $\{id\}$-bounded $\hat{\Sigma}^b_{i+1}$-definable functions of S^i_2 will be precisely the class $\{id\}$-$PF(\hat{\Sigma}^b_{i+1} \cap_{\{|id|\}} \hat{\Pi}^b_{i+1})$ and the $\{id\}$-bounded $\hat{\Sigma}^b_{i+1}$-definable functions of $\hat{R}^{i+1}_2 \preceq_{B(\hat{\Sigma}^b_{i+1})} R^{i+1}_2$ will be the class $\{id\}$-$PF(\hat{\Sigma}^b_{i+1} \cap_{\{2^{p(||id||)}\}} \hat{\Pi}^b_{i+1})$. Since the $\{id\}$-bounded definable functions of these theories will just be the definable functions of these theories, we need to show

$$\{id\}\text{-}PF(\hat{\Sigma}^b_{i+1} \cap_{\{|id|\}} \hat{\Pi}^b_{i+1}) = (FNC^1)^{\Sigma_i^p}$$

and

$$\{id\}\text{-}PF(\hat{\Sigma}^b_{i+1} \cap_{\{2^{p(||id||)}\}} \hat{\Pi}^b_{i+1}) = FNC^{\Sigma_i^p}$$

to show the theorem. In view of the definitions of PFP and Lemma IX.C.6, it suffices to show

$$\hat{\Sigma}^b_{i+1} \cap_{\{|id|\}} \hat{\Pi}^b_{i+1} = (NC^1)^{\Sigma_i^p}$$

and

$$\hat{\Sigma}^b_{i+1} \cap_{\{2^{p(||id||)}\}} \hat{\Pi}^b_{i+1} = NC^{\Sigma_i^p}.$$

By Corollary VII.C.7, the formulas $\hat{\Sigma}^b_{i+1} \cap_{\{|id|\}} \hat{\Pi}^b_{i+1}$ are $\hat{\Delta}^b_{i+1}$ with respect to S^i_2 and so can be written in the form

$$(\exists v \leq |s(x)|)[A(x, v) \wedge \neg B(x, v)]$$

where A and b are $\hat{\Sigma}_i^b$ and s is an L_2-term. Similarly, the $\hat{\Delta}_{i+1}^b$-predicates of $\hat{R}_2^{i+1,1} \preceq_{B(\hat{\Sigma}_{i+1}^b)} R_2^{i+1}$ can be written in the form

$$(\exists v \leq 2^{p(|s(x)|)})[C(x,v) \wedge \neg D(x,v)]$$

where p is a polynomial, s an L_2-term and C and D are $\hat{\Sigma}_i^b$-fomulas. In the S_2^i case, let F be some formula of the above type. Let $A \oplus B$ be the Σ_i^p-oracle which contains $2^{2|m|}+v2^{|m|+1}+2x+1$ if $A(x,v)$ and contains $2^{2|m|}+v2^{|m|+1}+2x$ if $B(x,v)$. Here m is the max of x and $s(x)$. We can define an $(NC^1)^{\Sigma_i^p}$ circuit family which computes the value of F as follows. For each $v \leq |s(x)|$ we have a gate A_v which is an $A \oplus B$ oracle gate with the low order and high order line set to 1 and with v hard-wired into the lines beginning with the $2^{|m|+1}$ one. We define B_v similarly except the low order line is set to 0. In the rest of the circuit we AND the A_v's with the B_v's and take the balanced OR over all these subcircuits. It is not hard to see this family of circuits will compute F. These circuits are log-depth so will be in $(NC^1)^{\Sigma_i^p}$.

This shows $\hat{\Sigma}_{i+1}^b \cap_{\{|id|\}} \hat{\Pi}_{i+1}^b \subseteq (NC^1)^{\Sigma_i^p}$. A similar argument shows $\hat{\Sigma}_{i+1}^b \cap_{\{2^{p(|id|)}\}} \hat{\Pi}_{i+1}^b \subseteq NC^{\Sigma_i^p}$. We now show the opposite direction. To begin for an oracle gate in a circuit we define its rank to be the maximum number of oracle gates on a path to the gate in question. In the case of an $(NC^1)^{\Sigma_i^p}$ family of circuits $\{C_n\}$ the ranks of oracle gates can be bounded by a constant since each has depth $|f(n)| \geq |n|$. Here n will always mean $|x|$. For a $NC^{\Sigma_i^p}$ family of circuits the ranks of oracle gates can be bounded by $c \log^e n + d$ from some fixed c, e, d. Let $\{C_n\}$ be a family of circuits in $NC^{\Sigma_i^p}$ of size bounded by $p(n)$ a polynomial and of rank bounded by a function $k(n)$ of the form $c|n|^e + d$. Suppose $\{C_n\}$ makes use of the Σ_i^p oracle $A(a)$. This oracle is equivalent to some $\hat{\Sigma}_i^b$-formula $(\exists w \leq t)B(a,w)$ where B is $\hat{\Pi}_i^b$. Consider sums of integers of the form

$$v = \sum_{j=0}^{k(|x|)} v_j 2^{j \cdot p(|x|)}$$

We will write $v \prec v'$ for the $\hat{\Sigma}^b_0$-formula

$$(\forall m < j)(\hat{\beta}(m, p(|x|), v) = \hat{\beta}(m, p(|x|), v') \wedge$$
$$\hat{\beta}(m+1, p(|x|), v) < \hat{\beta}(m+1, p(|x|), v'))$$

If $w = \sum_{j=0}^{l} w_j 2^{j \cdot p(|x|)}$ where $l \leq p(|x|)$ and $p(|x|) \geq |t^*|$, we define $Q(w, x)$ as follows Q evaluates $C_{|x|}$ on input $|x|$ as normal except rather than evaluating oracle gates by making queries to $A(a)$ it insteads checks if there is a w_j in w such that $B(a, w_i)$ holds. It is not hard to see $Q(w, x)$ is equivalent to a $\hat{\Pi}^b_i$-formula in R^{i-1}_2 since by Allen [2] NC-circuit evaluation is $\hat{\Delta}^b_1$ with respect to R^1_2. Define $r(w, x)$ so that $\hat{\beta}(j, p(|x|), r)$ is equal to the number of rank j queries satisfied by w in the evaluation of $C_{|x|}$ according to Q.

Thus, x will be accepted by the circuit class $\{C_n\}$ iff

$$(\exists v \leq p(|x|)\#k(|x|))[(\exists w)(Q(w, x) \wedge v = r(w, x))$$
$$\wedge \neg(\exists v' \leq p(|x|)\#k(|x|))(\exists w')(Q(w', x) \wedge v \prec r(v', x))]$$

Both w and w' in the above can be bounded by $p(|x|)\#t^*(x)$ so the above is a predicate in $\hat{\Sigma}^b_{i+1} \cap_{\{2^{p(|1\#d|)}\}} \hat{\Pi}^b_{i+1}$. This completes our proof that

$$\hat{\Sigma}^b_{i+1} \cap_{\{2^{p(|1\#d|)}\}} \hat{\Pi}^b_{i+1} = NC^{\Sigma^p_i}.$$

The argument that $\hat{\Sigma}^b_{i+1} \cap_{\{|id|\}} \hat{\Pi}^b_{i+1} \supseteq (NC^1)^{\Sigma^p_i}$ is similar and works because k in this case will be a constant. □

Note the second half of the above proof can be used to show R^{i+1}_2 can actually $\hat{\Sigma}^b_i$-define the circuits in $FNC^{\Sigma^p_i}$ as opposed to some function class which turns out to be equivalent to $FNC^{\Sigma^p_i}$.

IX.D The $\hat{\Sigma}^b_1$-functions of $\bar{C}^{0,\{|\tau|\}}_2$

The results of this section were developed in a series of e-mail exchanges between myself and Jan Johannsen. We give a slight refinement of his paper [28]

where he develops a bounded arithmetic theory $\bar{R}_2^0$ whose Σ_1^b-definable functions are functions computable by uniform constant depth threshold circuits, the class FTC^0. We show the $\hat{\Sigma}_1^b$-consequences of $\hat{C}_2^{0,\{|id|\}}$ are also the class FTC^0 and, in general, the $\hat{\Sigma}_{1,|\tau|}^b$-definable functions of $\bar{C}_2^{0,|\tau|}$ are the class FTC_τ^0 which we define. In the next section, we show $FTC_{|\tau|}^0 \subsetneq FTC_{\{id\}}^0$. We will show in Chapter X that $\bar{C}_2^{0,|\tau|} = R_2^1$ implies the collapse of the polynomial hierarchy. In particular, this implies if $\hat{C}_2^{0,\{|id|\}} = R_2^1$ then the polynomial hierarchy collapses. This gives some evidence, albeit circuitous, that $TC^0 \neq NC$.

We begin by defining what we mean by $\hat{\Sigma}_{i,|\tau|}^b$ and $\bar{C}_2^{0,|\tau|}$.

Definition IX.D.1

We define $\hat{\Sigma}_{i,|\tau|,k}^b$ to be the subset of $\hat{\Sigma}_{i,k}^b$ containing formulas whose innermost sharply bounded quantifier is bounded by a term in $|\tau|$. We write $\hat{\Sigma}_{i,|\tau|}^b$ for $\hat{\Sigma}_{i,|\tau|,2}^b$. We define $\hat{\Pi}_{i,|\tau|,k}^b$ to be the subset of $\hat{\Pi}_{i,k}^b$ containing formulas whose innermost sharply bounded quantifier is bounded by a term in $|\tau|$. We write $\hat{\Pi}_{i,|\tau|}^b$ for $\hat{\Pi}_{i,|\tau|,2}^b$.

So the $\hat{\Sigma}_{i,|id|}^b$-formulas are the usual $\hat{\Sigma}_i^b$-formulas. At the other extreme $\hat{\Sigma}_{i,|cl|}^b$-formulas are of the form $(\exists x \leq t)open$. These formulas are usually called E_i (see Wilmers [51]). It is unknown whether $\hat{\Sigma}_i^b$-formulas are as expressive a class of formulas as E_i-formulas. The question of whether $\hat{\Sigma}_1^b = E_1$ can be thought of as the question of whether or not a bounded version of the Matijasevič Davis Robinson Putnam Theorem holds. Recall the MRDP Theorem says $\Sigma_1 = \exists_1$ and implied that there was no recursive procedure to solve Diophantine equations. Here $\exists_1$ means the set of formulas in the language of arithmetic with a block of existential quantifiers followed by an open formula. Some work on the model theoretic implications of the MRDP Theorem to bounded arithmetic can be found in Kaye [32]. Adleman and Manders [1] have studied bounded version of the MRDP Theorem. They show a bounded form of MRDP Theorem which says a set A is in $\mathcal{E}_n$ for $n \geq 3$ of the Grzegorczyk Hierarchy iff it is of the form:

$$A = \{x | (\exists \vec{y} \leq f(x)) p(x, \vec{y}) = 0\}$$

where p is a polynomial and f is in $\mathcal{E}_n$ (see Börger [9] for a proof and relevant definitions). However, since $\mathcal{E}_3$ contains all elementary functions: in particular, it contains $f(x) = 2 \uparrow x =$ a stack of 2's x high, this is not quite as bounded as our situation. They leave the $\hat{\Sigma}^b_1 = E_1$? question open. They show $(\exists x)(\exists y)(ax^2 + by + c)$ is NP-complete: however, to show $\hat{\Sigma}^b_1 = E_1$ we would need to be able to represent the reduction of NP-problems to this one also as an open formula. Gaifman and Dimitracopoulos have have shown the MRDP Theorem is provable in $I\Sigma_0$+exp. It can also be shown that if the MRDP theorem is provable in S_k then $NP = co\text{-}NP$ [24].

Definition IX.D.2

The theory $\bar{T}^{i,|\tau|}_2$ *is the theory* $EBASIC$+$\hat{\Sigma}^b_{i,|\tau|}$-$IND^\tau$.

The theory $\bar{C}^{i,|\tau|}_2$ *is the theory*

$$EBASIC\text{+}open\text{-}IND^{|\tau|}\text{+}\hat{\Pi}^b_{i,|\tau|}\text{-}REPL^{|\tau|}.$$

From the definitions we have $S^i_2 = \hat{T}^{i,\{|id|\}}_2 = \bar{T}^{i,\{|id|\}}_2$ and $\hat{C}^{i,\{|id|\}}_2 = \bar{C}^{i,\{|id|\}}_2$. The same proofs as used earlier in this thesis imply the next lemma.

Lemma IX.D.3 $(i \geq 0)$

$\bar{C}^{i,|\tau|}_2 \vdash \bar{T}^{i,|\tau|}_2$.

$\bar{C}^{i,|\tau|}_2 = \bar{C}^{i,(|\dot{\tau}|)}_2$

$\bar{T}^{i,|\tau|}_2$ *proves the* $\hat{\Sigma}^b_{i,|\tau|}$-$REPL^{|\tau|}$ *axioms.*

$\bar{T}^{i,|\tau|}_2 = \bar{T}^{i,(|\dot{\tau}|)}_2$.

$\bar{T}^{i,|\tau|}_2$ *proves the* $\hat{\Pi}^b_{i,|\tau|}$-$IND^{|\tau|}$ *axioms.*

The third statement has essentially the same proof as Theorem IX.A.2. We now work towards defining the classes FTC^0_τ.

Definition IX.D.4 *Suppose* $h_0(n,\vec{x})$, $h_1(n,\vec{x}) \leq 1$. *A function* f *is defined by concatenation recursion on notation (CRN) from* g, h_0, *and* h_1 *if*

$$\begin{aligned} f(0,\vec{x}) &= g(\vec{x}) \\ f(2n,\vec{x}) &= 2\cdot F(n,\vec{x}) + h_0(n,\vec{x}), \text{ provided } n \neq 0 \\ f(2n+1,\vec{x}) &= 2\cdot F(n,\vec{x}) + h_1(n,\vec{x}) \end{aligned}$$

Let ℓ *be a term in* τ *and suppose* $g(n,\vec{x}) \leq t(\vec{x})$ *and* s *are functions. Then*

$$\sum_{n=0}^{|\ell(a)|} g(n,\vec{x})\cdot 2^{n\cdot|t^*|}$$

is called a $|\tau|$*-sum.*

We will show later that $\{|id|\}$-sums are roughly equivalent in strength to CRN; however, weaker versions of CRN do not seem as strong as their corresponding $|\tau|$-sums versions.

Definition IX.D.5 *The function class* FTC^0 *is the class of function consisting of* 0, $i_k^n(x_1,\ldots x_n) = x_k$, $s_0(x) = 2x$, $s_1(x) = 2x+1$, $\cdot$, $\#$, $|x|$, *Bit and which is closed under composition and* CRN.

The function class FTC^0_τ *is the class of function consisting of the functions of* L_2 *and which is closed under composition and* $|\tau|$*-sums.*

That FTC^0 as defined above is the class of functions computable by uniform constant depth threshold circuits is shown in Clote and Takeuti [20]. The class TC^0 of predicates in FTC^0 is considered interesting since it is one of the weakest reasonable class of predicates which might equal to NP. As far as the relation between FTC^0 and FTC^0_τ, we will show $FTC^0 = FTC^0_{\{id\}}$. To show this, however, we first prove some lemmas.

Lemma IX.D.6

1. *If $f(i,x)$ is in FTC^0_τ so is the characteristic function of*

$$(\forall i \leq |\ell(a)|)(f(i.x) = 0)$$

for all ℓ in τ.

2. *The characteristic function of every $|\tau|$-sharply bounded L_2-formula is in FTC^0_τ.*

3. *The characteristic function of every sharply bounded L_2-formula is in FTC^0.*

Proof: The second statement follows from the first and the fact FTC^0_τ contains $K_=$. $K_\leq$, $K_\wedge$. and $K_\neg$. The third statement's proof is similar to the second statement and can be found in Clote [18]. To see the first statement let $g(x)$ be

$$\sum_{i=0}^{|\ell(a)|-1} K_=(f(i,x),0) \cdot 2^i.$$

Then $\chi_{(\forall i \leq |\ell(a)|)(f(i.x)=0)}$ can be defined as

$$K_\wedge(K_=(g(x), 2^{|\ell(a)|} \dot{-} 1), K_=(f(|\ell(a)|,x),0)).$$

□

Lemma IX.D.7 *Let f be a function in FTC^0_τ and $\ell \in \tau$. Then the function*

$$(\mu i \leq |\ell(x)|)[f(i,x) = 0]$$

is also in FTC^0_τ.

Proof: The proof is the same as Theorem VIII.A.4. □

Lemma IX.D.8 *Let ℓ be a term in τ. Then $\lfloor |a|/|b| \rfloor$ is contained in FTC^0 and $\lfloor |\ell(a)|/|\ell(b)| \rfloor$ is contained in FTC^0_τ.*

Proof: By Lemma IX.D.7 and Lemma IX.D.6 we can define

$$\lfloor |\ell(a)|/|\ell(b)| \rfloor := (\mu n \leq |\ell(a)|)[|\ell(a)| < (n+1)|\ell(b)|]$$

and

$$\lfloor |a|/|b| \rfloor := (\mu n \leq |a|)[|a| < (n+1)|b|].$$

□

We are now ready to show $FTC^0 = FTC^0_{id}$.

Theorem IX.D.9 *The classes FTC^0 and $FTC^0_{\{id\}}$ are the same class of functions.*

Proof: It is not hard to see each of the base functions of FTC^0 can be defined by some term in L_2. On the other hand, Clote [18] shows the Σ^b_0-predicates are computable in FTC^0 so the base functions of $FTC^0_{\{id\}}$ are in FTC^0. So it suffices to show FTC^0 is closed under $\{|id|\}$-sums and $FTC^0_{\{id\}}$ is closed under CRN. Suppose we want to define f by CRN from $g(x)$ and $h_1(n,x), h_2(n,x)$ functions in $FTC^0_{\{id|\}}$ using $|\tau|$-sums. To do this define $t(a,x)$ to be

$$\sum_{n=0}^{|a|} cond(mod2(MSP(a, |a| \dot{-} n)), h_0(n,x), h_1(n,x))2^n$$

and let $f(a,x)$ be $g(x) + t(a,x) \cdot 2^{|g|}$. On the other hand, suppose we want to define the $|\tau|$-sum

$$f(a,x) := \sum_{n=0}^{|\ell(a)|} h(n,x)2^{n|s^*(x)|}$$

using CRN where $h(n,x) \leq s(x)$ are functions in FTC^0 . We use CRN to compute the bits of f from the most significant bit to the least significant bit. The function

$$t(i,a,x) := |a| \dot{-} \lfloor |i|/|s^*(x)| \rfloor$$

allows us to determine which term in f we are computing the bits from. The function

$$p(i,x) := |s^*(x)| \dot{-} (|i| \dot{-} \lfloor |i|/|s^*(x)| \rfloor |s^*(x)|) \dot{-} 1$$

gives us the position within a term. Define the function f' by CRN in the following way:

$$f'(2i+1,x) = f'(2i,x) = 2f(i,x) + Bit(p(i,x), h(t(i,a,x),x)).$$

Then the desired f is $f'(a\#s^*(x), x)$. $\square$

We need the next lemma to show $\bar{T}_2^{0,|\tau|}$ can $\hat{\Sigma}^b_{0,|\tau|}$-define the functions in FTC^0_τ.

Lemma IX.D.10 *The theory $\bar{T}_2^{0,|\tau|}$ proves the following block-extensionality axioms ($BLKEX_\ell$):*

$$(\forall i < |\ell(a)|)(\hat{\beta}(i, |d|, a) = \hat{\beta}(i, |d|, b) \supset LSP(a, |\ell(a)||d|) = LSP(b, |\ell(b)||d|)$$

where ℓ is in τ. We call the collection of these axioms for any $\ell \in \tau$ the τ-$BLKEX$ axioms.

Proof: This is easily proved by IND^ℓ_A on the following formula $A(c)$ which is provably equivalent to a $\hat{\Pi}^b_{0,|\tau|}$-formula in $\bar{T}_2^{0,|\tau|}$:

$$(\forall i < |\ell(a)|)(i \leq c \wedge \hat{\beta}(i, |d|, a) = \hat{\beta}(i, |d|, b)) \supset$$
$$LSP(a, |\ell(a)||d|) = LSP(b, |\ell(b)||d|).$$

$\square$

Notice when $d = 1$ then the $BLKEX_\ell$ axiom is the $BITEX_\ell$ axiom. So the τ-$BLKEX$ axioms imply the τ-$BITEX$ axioms. Our proof above is a variant of a proof first given in Johannsen [27].

We are now ready to show the $\hat{\Sigma}^b_1$-definable functions of $\bar{C}_2^{i,|\tau|}$ are the functions in FTC^0_τ.

Theorem IX.D.11 *The $\bar{C}_2^{0,|\tau|}$ can $\hat{\Sigma}^b_1$-define the functions in FTC^0_τ.*

Proof: The L_2-base functions are obviously $\hat{\Sigma}^b_{1,|\tau|}$-definable in $\bar{C}_2^{0,|\tau|}$. So it suffices to show the $\hat{\Sigma}^b_{1,|\tau|}$-definable functions of $\bar{C}_2^{0,|\tau|}$ are closed under $|\tau|$-sums. Suppose $f(i,x)$ is $\hat{\Sigma}^b_{1,|\tau|}$-defined in $\bar{C}_2^{0,|\tau|}$ by the formula $A_f(i,x,y)$ with y bounded by $s(i,x)$ and we want the sum $\sum_{i=0}^{|\ell(a)|-1} f(i,x) \cdot 2^{i|s^*|}$. Now $\bar{C}_2^{0,|\tau|}$ proves

$$(\forall i < |\ell(a)|)(\exists! y \leq s(i,x)+1) A_f(i,x,y) \wedge y \leq s.$$

Thus, since $A_f \wedge y \leq s$ is provably equivalent to a $\hat{\Sigma}^b_{1,|\tau|}$-formula by $\hat{\Sigma}^b_{1,|\tau|}$-$REPL^{|\tau|}$ using Lemma IX.D.3, the theory $\bar{C}^{0,|\tau|}_2$ proves there is a w less than $2{\cdot}((s^*{+}1)\#\ell(y))$ such that:

$$(\forall i \leq |\ell(y)|)(A_f(i, \dot{\beta}(i, |s^*+1|, s+1, w)) \wedge \dot{\beta}(i, |s^*+1|, s+1, w) \leq s).$$

The value w is the desired sum and it can be proven unique by τ-$BLKEX$ axioms. □

To prove the converse of Theorem IX.D.11, we work with sequent calculus formulations of $\bar{C}^{0,|\tau|}_2$. So the $\hat{\Pi}^b_{0,|\tau|}$-$REPL^{|\tau|}$ becomes the rule of inference:

$$\frac{\Gamma \rightarrow (\forall x \leq |\ell(s)|)(\exists y \leq t)A(x,y), \Delta}{\Gamma \rightarrow (\exists w \leq 2 \cdot (t^* \# \ell(s)))(\forall x \leq |\ell(s)|)A(x, \dot{\beta}(x, |t^*|, t, w))), \Delta}$$

for A in $\hat{\Pi}^b_{0,|\tau|}$ and ℓ in τ. We define the witness predicate in the same way as in Chapter VIII and prove the following witnessing theorem.

Theorem IX.D.12 *Suppose*

$$\bar{C}^{0,|\tau|}_2 \vdash \Gamma \rightarrow \Delta$$

where Γ *and* Δ *are cedents of formulas in*

$$LE\hat{\Sigma}^b_{1,|\tau|} \cup L|A|_{|\tau|}\hat{\Sigma}^b_{1,|\tau|} \cup LE|A|_{|\tau|}\hat{\Pi}^b_{0,|\tau|}.$$

Let $\vec{a}$ *be the free variables in this sequent.*

Then there is a FTC^0_τ *function* f *which is* $\hat{\Sigma}^b_{1,|\tau|}$*-defined in* $\bar{C}^{0,|\tau|}_2$ *such that:*

$$\bar{C}^{0,|\tau|}_2 \vdash Wit^1_{\wedge\Gamma}(w, \vec{a}) \supset Wit^1_{\vee\Delta}(f(w, \vec{a}), \vec{a}).$$

Proof: This is proved by induction on the number of sequents in an $\bar{C}^{0,|\tau|}_2$ proof of $\Gamma \rightarrow \Delta$. By cut elimination, we can assume all the sequents in the proof are in

$$LE\hat{\Sigma}^b_{1,|\tau|} \cup L|A|_{|\tau|}\hat{\Sigma}^b_{1,|\tau|} \cup LE|A|_{|\tau|}\hat{\Pi}^b_{0,|\tau|}.$$

Most of the cases are similar to previous witnessing arguments we have done. So we only show the ($\forall$: right) case. the *open-IND*$^{|\tau|}$ case and the $\hat{\Pi}^b_{0,|\tau|}$-*REPL*$^{|\tau|}$ case.

(**$\forall$:right case**) Suppose we have the inference:

$$\frac{b \leq t, \Gamma \rightarrow A(b), \Delta}{\Gamma \rightarrow (\forall x \leq t) A(x), \Delta}$$

By the induction hypothesis there is a FTC^0_τ function g such that

$$\bar{C}_2^{0,|\tau|} \vdash Wit^1_{b \leq t \wedge \Gamma}(w, \vec{a}, b) \supset Wit^1_{A \vee \Delta}(g(w, \vec{a}, b), \vec{a}, b).$$

By cut-elimination, $(\forall x \leq t) A(x)$ is either in $L|A|_{|\tau|}\hat{\Pi}^b_{0,|\tau|}$ or is in $|A|_{|\tau|}\hat{\Sigma}^b_{1,|\tau|}$. So $t = |\ell(s)|$ for some term ℓ in τ. In the first case, let y be $(\mu i \leq |\ell(s)|)\neg A(i)$ and define f to be $g(w, \vec{a}, y)$. This is in FTC^0_τ be Lemma IX.D.6 and Lemma IX.D.7.

It is not hard to see that

$$\bar{C}_2^{0,|\tau|} \vdash Wit^1_\Gamma(w, \vec{a}) \supset Wit^1_{(\forall x \leq |\ell(s)|) A \vee \Delta}(f(w, \vec{a}), \vec{a}).$$

In the second case, $(\forall x \leq t) A(x)$ is really of the form

$$(\forall x \leq |\ell(s)|)(\exists y \leq t') B(x, y)$$

where B is a $\hat{\Pi}^b_{0,|\tau|}$-formula. Since Wit^1_A is provably equivalent to $\hat{\Pi}^b_{0,|\tau|}$-formula in *EBASIC*. its characteristic function $\chi_{Wit^1_A}$ is in FTC^0_τ. Let k be the multifunction

$$k(w, \vec{a}) = (\mu j < |\ell(s)|)[\neg \chi_{Wit^1_A}(\beta(1, g(w, \vec{a}, j)), \vec{a}, j) = 0]$$

Now define $f(w, \vec{a})$ from k as follows:

$$f(w, \vec{a}) = cond(K^-_=(k, |\ell(s)|), \sum_{j=0}^{|\ell(s)-1|} \beta(1, g(w, \vec{a}, j) \cdot 2^{j \dot{+} |(t')^-|}, \beta(2, g(w, \vec{a}, k))$$

It is not hard to see that

$$\bar{C}_2^{0,|\tau|} \vdash Wit^1_\Gamma(w, \vec{a}) \supset Wit^1_{(\forall x \leq |\ell(s)|) A \vee \Delta}(f(w, \vec{a}), \vec{a}).$$

(*open-$IND^{(|\tau|)}$* **case)** Suppose we have the inference

$$\frac{A(b), \Gamma \rightarrow A(Sb), \Delta}{A(0), \Gamma \rightarrow A(|\ell(s)|), \Delta}$$

where A is an open formula, ℓ is in τ, and s is in L_2. By the induction hypothesis there is a FTC^0_τ function g such that

$$\bar{C}_2^{0,|\tau|} \vdash Wit^1_{A(b)\wedge\Gamma}(w, b, \vec{a}) \supset Wit^1_{A(Sb)\vee\Delta}(g(w, b, \vec{a}). b. \vec{a}).$$

From our definition of the Wit^i predicate in Chapter VIII and Lemma IX.D.6. we know FTC^0_τ contains $\chi_{Wit^1_{\vee\Delta}}$, the characteristic function of this formula. Define

$$f(w. \vec{a}) := g(w. (\mu y \leq |\ell(s)|)(\neg\chi_{Wit^1_{\vee\Delta}}(\beta(2, g(w, y, \vec{a})). y. \vec{a}) = 0). \vec{a})$$

The idea is $f(w. \vec{a})$ runs g on the least value y less than $|\ell(s)|$ that produces a witness for Δ. If no such value exists then it must be the case that $A(|\ell|)$ holds and so as A is open the cedent is trivially witnessed. From this it is not hard to show:

$$\bar{C}_2^{0,|\tau|} \vdash Wit^1_{A(0)\wedge\Gamma}(w. \vec{a}) \supset Wit^1_{A(|\ell(r)|)\vee\Delta}(f(w. \vec{a}). \vec{a}).$$

($\hat{\Pi}^b_{0,|\tau|} - REPL^{|\tau|}$**:case)** Suppose we have the inference:

$$\frac{\Gamma \rightarrow (\forall x \leq |\ell(s)|)(\exists y \leq t)A(x, y), \Delta}{\Gamma \rightarrow (\exists w \leq 2 \cdot (t^* \# \ell(s)))(\forall x \leq |\ell(s)|)A(x, \dot{\beta}(x, |t^*|, t. w))). \Delta}$$

where ℓ is in τ and s in L_2. By the induction hypothesis there is a FTC^0_τ function g such that

$$\bar{C}_2^{0,|\tau|} \vdash Wit^1_\Gamma(w, \vec{a}, b) \supset Wit^1_{(\forall x \leq |\ell(s)|)(\exists y \leq t).A\vee\Delta}(g(w, \vec{a}). \vec{a}).$$

For this case, it suffices to notice that the predicates

$$Wit^1_{(\forall x \leq |s|)(\exists y \leq t).A}$$

and

$$Wit^1_{(\exists w \leq 2\cdot(t^* \# 2^{|s|}))(\forall x \leq |s|).A}$$

are the same. Hence, if we let $f = g$ then

$$\bar{C}_2^{0,|\tau|} \vdash Wit^1_\Gamma(w, \vec{a}, b) \supset Wit^1_{(\exists w \leq 2\cdot(t^* \# \ell(s)))(\forall x \leq |s|).A \vee \Delta}(f(w, \vec{a}), \vec{a}).$$

This completes the cases and the proof. □

Corollary IX.D.13

The $\hat{\Sigma}^b_{1,|\tau|}$-definable functions of $\bar{C}_2^{0,|\tau|}$ are the class FTC^0_τ.

The $\hat{\Sigma}^b_1$-definable functions of $\hat{C}_2^{0,\{|id|\}}$ are FTC^0.

The $\hat{\Sigma}^b_{1,|cl|}$-definable functions of $EBASIC$ are the class of L_2-terms.

Proof: The first statement follows from Theorem IX.D.12 when one takes Γ to be the empty cedent and Δ to be the formula defining the function in question. The second statement is a consequence of the first statement when $\tau = \{id\}$ and the fact $FTC^0 = FTC^0_{\{id\}}$. The last statement is a consequence of the first statement when $\tau = cl$. □

Remark IX.D.14 In view of Corollary IX.D.13 for the $i = 0$ case of Theorem VIII.B.8 one can actually prove if $\hat{C}_2^{0,|id|}$ proves $\Gamma \rightarrow \Delta$ is a sequent of $\hat{\Sigma}^b_k$-formula $k > 1$ then there is a $Q^{i,cl}$-definable in $\hat{C}_2^{0,|id|}$, $FP^{\Sigma^p_{k-1}}(wit, 1)$ multifunction f such that:

$$\hat{C}_2^{i,|id|} \vdash Wit^k_{\wedge\Gamma}(w, \vec{a}) \supset Wit^k_{\vee\Delta}(f(w, \vec{a}), \vec{a}).$$

Corollary IX.D.15 *If $EBASIC$ proves $(\exists y)A(x, y)$ where A is a $E_1 = \hat{\Sigma}^b_{1,|cl|}$-formula then there is a term $t(x)$ in L_2 such that $EBASIC$ proves $A(x, t(x))$.*

In particular, if f is a term in L_2 and $EBASIC$ proves $(\exists y)(f(x, y) = 0)$ then there is a term $t(x)$ such that $EBASIC$ proves $f(x, t(x)) = 0$.

Proof: Since FTC^0_{cl} is just the functions in L_2 this corollary is a consequence of Corollary IX.D.13. One can also prove this corollary from Herbrand's Theorem and the fact L_2-terms can express any open formula. □

Remark IX.D.16 This suggests a weaker program than trying to show $\hat{\Sigma}^b_1 \supsetneq E_1$. Try to show $\hat{\Sigma}^b_1$ is different from E_1 for stronger and stronger theories. In particular, the above corollary shows the E_1-definable functions of $EBASIC$ are just L_2-terms. We know from Chapter V that the $\hat{\Sigma}^b_1$-definable multifunctions of $EBASIC$ are the class $B_{1,2}$. Consider $\lfloor \frac{|x|}{3} \rfloor$. We can express $\lfloor \frac{|x|}{3} \rfloor$ in $B_{1,2}$ with the multifunction $(Wy \leq |x|)(t_A = 0)$ where t_A is an L_2-term equal to zero iff

$$3y = |x| \vee 3y + 1 = |x| \vee 3y + 2 = |x|.$$

Using the axiom $a + b \leq a + c \Leftrightarrow b \leq c$ and equality axioms $EBASIC$ can prove only one of $3y = x$, $3y+1 = x$, and $3y+2 = x$ can hold. Suppose $y < z$. $EBASIC$ can use the axiom

$$a \geq S0 \supset (a \cdot b \leq a \cdot c \Leftrightarrow b \leq c)$$

to argue that $3y + i = x$ and $3z + j = x$ cannot both hold where $i, j \leq 2$. Thus, $EBASIC$ proves the value returned by $(Wy \leq |x|)(t_A = 0)$ is unique. It seems likely that $\lfloor \frac{|x|}{3} \rfloor$ cannot be expressed by a L_2-term and so is not E_1-definable, although at this point the author is unable to prove this.

IX.E $FTC^0_{|\tau|} \subsetneq FTC^0_{\{id\}}$

In this section, we prove $FTC^0_{|\tau|} \subsetneq FTC^0_{\{id\}}$. Our method is based on the proof in Johannsen [26] that R^0_2 does not Σ^b_1-define $\lfloor \frac{x}{3} \rfloor$.

Definition IX.E.1 *The function $\#_B(x)$ returns the number of alternations between 1 and 0 in reading the binary number x from left to right. We start the counting of this number at 1 so $\#_B(1) = 1$.*

As an example, let x be the binary number 1110011 then $\#_B(x) = 3$. Since the number of alternations in x's binary notation is always going to be less than the length of x we have the following easy lemma.

Lemma IX.E.2 *If $y \leq x$ then $\#_B(y) \leq |x|$.*

Proof: This follows since $\#_B(y) \leq |y| \leq |x|$. □

To prove our results we study the way $\#_B(f(x_1, \ldots, x_n))$ depends on $\#_B(x_i)$ where f is in $FTC^0_{|\tau|}$.

Lemma IX.E.3 *Let $g \leq t$. The following inequalities hold:*

(a) $\#_B(|x|) \leq ||x||$

(b) $\#_B(\lfloor \frac{1}{2}x \rfloor) \leq \#_B(x)$

(c) $\#_B(MSP(x,i)) \leq \#_B(x)$

(d) $\#_B(Sx) \leq \#_B(x) + 1$

(e) $\#_B(x\#y) = 2$

(f) $\#_B(x + y) \leq 4 \cdot (\#_B(x) + \#_B(y))$

(g) $\#_B(x \dot{-} y) \leq 4 \cdot (\#_B(x) + \#_B(y) + 1) + 1 \leq 7 \cdot (\#_B(x) + \#_B(y))$

(h) $\#_B(x \cdot y) \leq 14 \cdot 2^{3|\#_B(x)+\#_B(y)|} \cdot (\#_B(x) + \#_B(y))$

(i) $\#_B(\sum_{n=0}^{|\ell(a)|} g(n, \vec{x}) \cdot 2^{n \cdot |t^*|}) \leq |\ell(a)| + \sum_{n=0}^{|\ell(a)|} \#_B(g(n, \vec{x}))$

(j) $\#_B((Wi \leq |t(x)|)(f(x,z) = 0)) \leq ||t(x)||$

Proof:

(a) This follows from Lemma IX.E.2

(b) Since $\lfloor \frac{1}{2}x \rfloor$ chops off the low order bit of x the number of alternations can at most stay the same.

(c) This follows by similar reasoning to (b).

(d) If the low order bits of x is 0 then adding 1 can increase the number of alternations by at most one since only this bit will be flipped. Otherwise, adding 1 will toggle the low order block of 1's in x and carry the 1 to the 0 to its left. Again, at most increasing the number of alternations by 1.

(e) The number $x\#y$ is a 1 followed by $|x||y|$ zeros.

(f) First, notice that adding 2^i to or subtracting 2^i from x can only increase the number of blocks in x by at most 2. Since the blocks of 1's in y can be represented as expressions of the from $2^{j+i} - 2^i$, when we perform the addition we get at most 4 blocks in the new number for every block of 1's in y. So the new number has fewer than $\#_B(x) + 4\#_B(y)$ blocks.

(g) This follows from (f) since if $x \geq y$ then

$$x \dot{-} y = (2^{|x|+1} - 1 - ((2^{|x|+1} - 1 - x) + y))$$

and $2^{|x|+1} - 1 - x$ has at most one more block then x and

$$(2^{|x|+1} - 1 - ((2^{|x|+1} - 1 - x) + y))$$

has at most one more block then $(2^{|x|+1} - 1 - x) + y$.

(h) Consider multiplying x by a block of 1's $2^{i+j} - 2^i$. This gives $x \cdot 2^{i+j} - x2^i$ which is the substraction of two number each with at most one more alternation than x. So we get less than $14 \cdot (\#_B(x) + 1)$ by (g). There are fewer than $\#_B(y)$ blocks of 1's in y. To compute $\#_B(x \cdot y)$ we need to add together fewer $\#_B(y)$ numbers with fewer than $14 \cdot (\#_B(x) + 1)$ blocks. If we do this in a balanced fashion then by (f) we get fewer than $8^{|\#_B(y)|}(14 \cdot (\#_B(x) + 1))$ blocks from which the bound follows.

(i) For each term in the sum we get $\#_B(g(n, \vec{x}))$ blocks with potentially a lead block of zeros.

(j) Follows from (a).

□

Lemma IX.E.4 *If $f(\vec{x}) \in FTC^0_{|\tau|}$ and $\#_B(x_i) \leq ||x_i||$ then $\#_B(f(\vec{x})0 \leq c\cdot(||x_1||+ \cdots + ||x_n||)^d$ for some fixed integers c and d.*

Proof: This follows from Lemma IX.E.3. (Remember $FTC^0_{|\tau|}$ has sums of length at most $||\ell(a)||$ where ℓ is in τ.) □

Lemma IX.E.5 *The function $\lfloor \frac{x}{3} \rfloor$ is definable in $FTC^0_{\{id\}}$.*

Proof: First we note that the binary representation of 1/3 is $.10101\cdots$. So $\lfloor \frac{2^{2|x|}+2}{3} \rfloor$ can be computed as $g(x) = \sum_{i=0}^{|x|} 2^i 2^i$. So $\lfloor \frac{x}{3} \rfloor$ can be defined as

$$MSP(g(x) \cdot x, 2 \cdot |x| + 2).$$

□

Theorem IX.E.6 *The function $\lfloor \frac{x}{3} \rfloor$ is not definable in $FTC^0_{|\tau|}$. Hence, $FTC^0_{|\tau|} \subsetneq FTC^0_{\{id\}}$.*

Proof: That $\lfloor \frac{x}{3} \rfloor$ is in $FTC^0_{\{id\}}$ is Lemma IX.E.5. To see $\lfloor \frac{x}{3} \rfloor$ is not definable in $FTC^0_{|\tau|}$ we use Lemma IX.E.4. Consider $\lfloor \frac{2^{|x|+1}-1}{3} \rfloor$ which is a number of length $|x| - 1$ of the form $1010\cdots$. Hence,

$$\#_B(\lfloor \frac{2^{|x|+1}-1}{3} \rfloor) = |x| - 1.$$

Thus, f does not define $\lfloor \frac{x}{3} \rfloor$. □

Theorem IX.E.7 *The following relation holds $\bar{C}_2^{0,|\tau|} \subsetneq \bar{C}_2^{0,\{id\}} = \hat{C}_2^{0,\{id\}}$.*

Proof: Using a combination of our results in Chapters III,IV,V and our result of this chapter, one can show the $\hat{\Sigma}_1^b$-definable multifunctions of $\bar{C}_2^{i,|\tau|}$ are the

closure of $B_{1,2}$ under composition and $||\tau||$-sums. By Lemma IX.E.3. in particular statement (j). we have

$$\#_B(f(\vec{x})0 \leq c \cdot (||x_1|| + \cdots + ||x_n||)^d$$

for any f in this class. So the same proof as in Theorem IX.E.6 gives the result. □

It would be nice to refine the $\#_B$ concept to show $\hat{\Sigma}^b_1$-definability is different from E_1-definability in $EBASIC$. Unfortunately, the author is not sure how to do this. One would like try to show if $\#_b(x_i) \leq |||x_i|||$ and $\#_b(|x_i|) \leq |||x_i|||$ then

$$\#_b(t(x)) \leq c \cdot (|||x_1||| + \cdots + |||x_n|||)^d$$

when t is an L_2-term. However, $\#_B(|x \dot{-} y|)$ in general can be near $||x||$.

Chapter X

Collapses and oracle separations

This chapter gives some evidence that certain relationships do not hold between the various bounded arithmetic theories we have been considering. In the first section we use a result of Chang and Kadin [30, 17] to show if $T_2^i = \hat{T}_2^{i+1,|\tau|}$ or if $T_2^i = \hat{C}_2^{i+1,|\tau|}$ or if $\hat{C}_2^{i,|\tau|} = \hat{T}_2^{i+1,|\tau'|}$ where τ contains at least one unbounded iterm then $\Sigma_{i+3}^p = \Pi_{i+3}^p$. It was already known from Krajíček, Pudlak, and Takeuti [35] that if $T_2^i = S_2^{i+1}$ the polynomial hierarchy collapses to the $(i+2)$nd level. Buss [15] and Zambella [52] showed that if $T_2^i = S_2^{i+1}$ then T_2^i proves the polynomial hierarchy collapses to the $(i+3)$rd level. Both of these results make use of Herbrand's theorem and some combinatorics; whereas, our result is implied by our witnessing argument characterizations of the $\dot{\Delta}_{i+2}^b$-predicates of these theories. It is not hard to generalize Krajíček, Pudlak, and Takeuti [35] combinatorics to get the first two statements to imply the hierarchy collapses; however, the third statement seems harder to show. So we feel our method is of independent interest. After the section on hierarchy collapses, the rest of the chapter is devoted to showing there is an oracle X such that $P^{\Sigma_i^p(X)}(\{\{||\dot{\ell}||\}\})$ is contained in but not equal to $P^{\Sigma_i^p(X)}(\{|\ell|\})$ where ℓ is a nondecreasing, unbounded iterm. This result implies many oracle separations. Some of these separations were obtained independently by Arnold Beckmann in his Ph.D. thesis [5] using "dynamic ordinal analysis" which is a different technique than ours.

X.A Hierarchy collapses

In this section, we will use brackets in expressions like $P^{\Sigma_i^p}[k]$ to denote at most k queries to a Σ_i^p-oracle and continue using parentheses such as $P^{\Sigma_i^p}(k)$ to mean $O(k)$ queries. In the combination of the two papers, Chang and Kadin [30, 17] it is shown that

$$P^{\Sigma_i^p}[k] = P^{\Sigma_i^p}[k+1]$$

implies $\Sigma_{i+3}^p = \Pi_{i+3}^p$. Here k is a fixed number. Let ℓ be a nondecreasing, unbounded iterm. We will show that the class $P^{\Sigma_i^p}(\{|\ell|\})$ has complete problems. Thus, if

$$P^{\Sigma_i^p}(\{|\ell|\}) = P^{\Sigma_i^p}(1)$$

then in fact

$$P^{\Sigma_i^p}(\{|\ell|\}) = P^{\Sigma_i^p}[k]$$

for some fixed k and so

$$P^{\Sigma_i^p}[k] = P^{\Sigma_i^p}[k+1]$$

implying the hierarchy collapses to the $(i+3)$rd level. Let τ be a set of iterms containing ℓ. Then the $\hat{\Delta}_{i+2}^b$-predicates of $\hat{T}_2^{i+1,|\tau|}$ contain those predicates in $P^{\Sigma_i^p}(\{|\ell|\})$. Similarly, the $\hat{\Delta}_{i+2}^b$-predicates of T_2^i contain those predicates in $P^{\Sigma_i^p}(1)$. So if $T_2^i = \hat{T}_2^{i+1,|\tau|}$ the polynomial hierarchy collapses to the $(i+3)rd$-level. By the same argument, we get $T_2^i = \hat{C}_2^{i+1,|\tau'|}$ implies the hierarchy collapses to the $(i+3)$rd level and likewise $\hat{C}_2^{i,|\tau|} = \hat{T}_2^{i+1,|\tau'|}$ implies the hierarchy collapses to the $(i+3)$rd level. We now show that the $P^{\Sigma_i^p}(\{|\ell|\})$ has complete problems.

Theorem X.A.1 $(i \geq 1)$ *The class $P^{\Sigma_i^p}(\{|\ell|\})$ has problems which are complete under polynomial-time many-one reductions.*

Proof: A polynomial time many-one reduction is a polynomial time function f from one set A to another set B such that $x \in A$ iff $f(x) \in B$. Let A be any set

in $P^{\Sigma_i^p}(\{|\ell|\})$. Consider the set K:

$$\{\langle e, x, y, 1^s\rangle | \text{The machine coded by } e \text{ accepts } x \text{ with fewer than } \ell(y) \text{ queries to } SAT_i \text{ and in fewer than } s \text{ steps.}\}$$

Here SAT_i is the problem of determining whether a closed quantified boolean formula of i alternations the outermost block being an exists block is valid. It is known to be Σ_i^p-complete (see Theorem 17.10 Papadimitriou [37]). We first show that K is in $P^{\Sigma_i^p}(\{|\ell|\})$. To do this let M be the machine which on input $\langle e, x, y, 1^s\rangle$ simulates e on x for s steps. If e does not accept by s steps or if at any time attempts more than $|\ell(y)|$ queries then M rejects. Otherwise M accepts. Since $\ell(y) \leq \ell(\langle e, x, y, 1^s\rangle)$ (where we are using our pairing function from before to make this quadruple), this machine runs in polynomial time making fewer than $|\ell(\langle e, x, y, 1^s\rangle)|$ queries to a Σ_i^p oracle. So it is in $P^{\Sigma_i^p}(\{|\ell|\})$.

Now we reduce $A \in P^{\Sigma_i^p}(\{|\ell|\})$ to K. Without loss of generality we can assume membership in A can be computed by a machine M making fewer than $|\ell(h(x))|$ queries to SAT_i and running in time $p(|x|)$ where h is an L_2-term. Consider the function

$$f(x) = \langle e_M, x, h(x), 1^{p(|x|)}\rangle.$$

Here e_M is a coding for the machine M and is fixed for all x. Certainly, this function is polynomial time and $f(x) \in K$ iff $x \in A$ so K is a complete problem for $P^{\Sigma_i^p}(|\ell(x)|)$. □

Corollary X.A.2 ($i \geq 0$) *The following statements imply* $\Sigma_{i+3}^p = \Pi_{i+3}^p$:

(a) $T_2^i = \hat{T}_2^{i+1,|\tau'|}$

(b) $T_2^i = \hat{C}_2^{i+1,|\tau'|}$

(c) $\hat{C}_2^{i,|\tau|} = \hat{T}_2^{i+1,|\tau'|}$.

where τ and τ' are two sets of items such that τ' contains at least one nondecreasing, unbounded item.

Proof: Let ℓ be the unbounded iterm in τ'. The above statements follow from the discussion at the beginning of this section, the fact $P^{\Sigma_i^p}(\{|\ell|\})$ has complete problems, Corollary VII.A.3, Corollary VIII.B.9, Corollary VI.E.5, and Corollary VIII.B.6. □

The $i = 0$ case of the last equality is interesting since the $\hat{\Sigma}_1^b$-definable functions of $\hat{C}_2^{0,\{|id|\}}$ is the class FTC^0. If $\hat{C}_2^{0,\{|id|\}} = R_2^1$ or S_2^1 then the polynomial hierarchy collapses. So this gives some indirect evidence that the classes TC^0 and NC are not equal.

X.B Oracle results

For rest of this chapter, we will work towards showing there is an oracle X for which $P^{\Sigma_i^p(X)}(\{\{||\dot{\ell}||\}\})$ is contained in but not equal to $P^{\Sigma_i^p(X)}(\{|\ell|\})$ where ℓ is a nondecreasing, unbounded iterm. An easy modification to Corollary VI.E.5 implies the $\hat{\Delta}_{i+1}^b(\alpha)$-predicates of $\hat{T}_2^{i,\{|\ell|\}}$ are $P^{\Sigma_i^p(\alpha)}(\{\{||\dot{\ell}||\}\})$ and those of $\hat{T}_2^{i,\{\ell\}}$ are $P^{\Sigma_i^p(\alpha)}(\{\{|\dot{\ell}|\}\})$. Thus, our separation shows $\hat{T}_2^{i,\{|\ell|\}}(\alpha) \subsetneq \hat{T}_2^{i,\{\ell\}}(\alpha)$ where α is a new 1-ary predicate symbol we add to the language of bounded arithmetic without defining equations. This follows since there is a model of these theories where α is interpreted as X. By Corollary II.G.14, this shows $\hat{T}_2^{i,\tau'}(\alpha) \subsetneq \hat{T}_2^{i,\tau}(\alpha)$ for any τ' whose iterms are surpassed by $|\ell|$ and for any τ containing a term surpassing ℓ. This result also shows these theories are separated by a $\hat{\Delta}_{i+1}^b(\alpha)$-predicate. We define $W \subseteq_K V$ to mean $W \cap K \subseteq V \cap K$. We define $\subsetneq_K$ in a similar manner. With a slight change to Corollary VIII.B.6 one can show $\hat{C}_2^{i,\tau}(\alpha)$ is $B(\hat{\Sigma}_{i+1}^b(\alpha))$-conservative over $\hat{T}_2^{i,\tau}(\alpha)$. So our oracle separation will show

$$\hat{T}_2^{i,\tau'}(\alpha) \subseteq \hat{C}_2^{i,\tau'}(\alpha) \subsetneq_{\hat{\Delta}_{i+1}^b(\alpha)} \hat{T}_2^{i,\tau}(\alpha) \subseteq \hat{C}_2^{i,\tau}(\alpha).$$

As two particular cases of this result we get

$$\hat{T}_2^{i,m+1}(\alpha) \subseteq \hat{C}_2^{i,m+1}(\alpha) \subsetneq_{\hat{\Delta}_{i+1}^b(\alpha)} \hat{T}_2^{i,m}(\alpha) \subseteq \hat{C}_2^{i,m}(\alpha)$$

and

$$\hat{R}_2^i(\alpha) \subseteq R_2^i(\alpha) \subsetneq_{\hat{\Delta}_{i+1}^b(\alpha)} S_2^i(\alpha) \subsetneq_{\hat{\Delta}_{i+1}^b(\alpha)} T_2^i(\alpha).$$

The $\hat{\Delta}_{i+1}^b$-predicates of T_2^{i-1} for $i > 1$ are $P^{\Sigma_i^p}(1)$ by Corollary VII.A.3. Generalizing this result to where we have α in the language, we can use our oracle to give us $T_2^{i-1}(\alpha) \not\supseteq_{\hat{\Delta}_{i+1}^b(\alpha)} \hat{T}_2^{i,\tau}(\alpha)$ for any τ containing an unbounded, nondecreasing iterm. On the other hand, consider the theory $\hat{T}_2^{i,\{\ell\}}(\alpha)$ versus $\hat{T}_2^{i+1,\{|\ell|\}}(\alpha)$. The $\hat{\Delta}_{i+1}^b$-consequences of the former will be the class $P^{\Sigma_i^p(\alpha)}(\{|\ell|\})$ and of the latter $P^{\Sigma_i^p(\alpha)}(\{||\dot{\ell}||\})$, so $\hat{T}_2^{i+1,\{||\ell||\}}(\alpha) \subsetneq_{\hat{\Delta}_{i+1}^b(\alpha)} \hat{T}_2^{i,\{\ell\}}(\alpha)$. That is, the $\hat{\Delta}_{i+1}^b$-consequences of $\hat{T}_2^{i+1,\{||\ell||\}}(\alpha)$ will be contained in but not equal to the $\hat{\Delta}_{i+1}^b$-consequences of $\hat{T}_2^{i,\{\ell\}}(\alpha)$ In particular, this shows

$$T_2^i(\alpha) \not\subseteq \hat{R}_2^{i+1}(\alpha)$$

and by Corollary VIII.B.6 for $i \geq 1$,

$$T_2^i(\alpha) \not\subseteq R_2^{i+1}(\alpha).$$

X.C The oracle separation

Let ℓ be a nondecreasing, unbounded iterm. Our method of oracle construction closely follows [33]. By Corollary VI.E.6, every predicate in $P^{\Sigma_i^p}(\{|\ell|\})$ can be written in the form

$$(\exists v \leq \ell(s(x)))[A(x, v) \wedge \neg B(x, v+1)]$$

where A and B are in Σ_i^p, and s is an L_2-term. (The converse of this statement is also true. This is because with $|\ell|$ many queries to a Σ_i^p oracle one can binary search for a value v such that A held and B did not.) It is not hard to generalize this statement to show every $P^{\Sigma_i^p(X)}(\{|\ell|\})$ predicate, where X is an oracle set, can be written in the form

$$(\exists v \leq \ell(s(x)))[A(x, v, X) \wedge \neg B(x, v+1, X)]$$

where A and B are in $\Sigma_i^p(X)$, and s is an L_2-term. So the problem of showing $P^{\Sigma_i^p(X)}(\{||\dot{\ell}||\})$ and $P^{\Sigma_i^p(X)}(\{|\ell|\})$ are not equal reduces to giving a problem which can be solved by predicates of the form

$$(\exists v \leq \ell(s(x)))[A(x, v, X) \wedge \neg B(x, v+1, X)]$$

where A and B are $\Sigma_i^p(X)$ and s is an L_2, but which cannot be solved by predicates of the form

$$(\exists v \leq (2^{||\ell(s'(x))||^d})[C(x, v, X) \wedge \neg D(x, v+1, X)]$$

on infinitely many inputs where C and D are $\Sigma_i^p(X)$, d is a constant.

We now define such a problem. For the remainder of the chapter we assume ℓ is of the form $\ell'(2^{|id|})$ where ℓ' is a nondecreasing, unbounded item. Although the new predicate symbol α is 1-ary we will use pairing to feed it inputs of higher arity.

Definition X.C.1

1. *For $i \geq 1$ we define the following $\Sigma_i^b(\alpha)$-formulas*

   (a) $\Psi_1^\ell(x, v, \alpha) := v = 0 \vee (\exists y_1 < \left(\frac{x \log(x))^{1/2})}{2}\right))\alpha(\langle x, v, y_1\rangle)$

   (b) $\Psi_2^\ell(x, v, \alpha) := v = 0 \vee (\exists y_1 < x)(\forall y_2 < (x \log(x))^{1/2})\alpha(\langle x, v, y_1, y_2\rangle)$

   (c)

   $$\begin{aligned}\Psi_i^\ell(x, v, \alpha) \;:=\; & v = 0 \vee (\exists y_1 < x)(\forall y_2 < x) \cdots (Q_{i-1} y_{i-1} < x) \\ & (Q_i y_i < \left(\frac{i \cdot x \cdot \log(x)}{2}\right)^{1/2})\alpha(\langle x, v, y_1, \ldots, y_i\rangle)\end{aligned}$$

   where Q_{i-1} is a $\forall$ if i is odd and an $\exists$ otherwise. Likewise, Q_i is a $\exists$ if i is odd and an $\forall$ otherwise.

2. *For $i \geq 1$ we define the predicate*

   $$\begin{aligned}& P_i^\ell(x, \alpha) := \\ & \quad (\exists v < \ell(x))[(\Psi_i^\ell(x, v, \alpha) \wedge v = 1 mod 2 \wedge \\ & \quad \neg(\exists v' < \ell(x))(v' > v \wedge \Psi_i^\ell(x, v', \alpha))]\end{aligned}$$

The x which appears in the inputs to α will be used later in our diagonalization argument. The formulas $P_i^\ell(x,\alpha)$ will be true if the maximal v satisfying $\Psi_i^\ell(x,v,\alpha)$ is odd. Given the definition of P_i^ℓ and the remarks at beginning of this section, it is not hard to see the next lemma is true.

Lemma X.C.2 *($i \geq 1$) The predicate $P_i^\ell(x,\alpha)$ is in $P^{\Sigma_i^p(\alpha)}(|\ell|)$ for all $\alpha \subset \omega$.*

To separate $P^{\Sigma_i^p(X)}(\{||\dot{\ell}||\})$ and $P^{\Sigma_i^p(X)}(|\ell|)$ we will be working with propositional translations of the above problem. The virtue of propositional translations is that they allow us to apply results from Boolean circuit complexity to help solve our problem. For any fixed number k we will use the next definition to give a propositional translation of the first order formula $P_i^\ell(k,\alpha)$.

Definition X.C.3 *Let $n := (i \cdot k\log(k)/2)^{1/2}$. We define the propositional translations $\overline{\Psi}_i(k,v)$ and $\overline{P}_i^{\ell,k}$ of the formulas $\Psi_i^\ell(k,v,\alpha)$ and $P_i^\ell(k,X)$.*

1. *The variables in $\overline{\Psi}_i^\ell(k,v)$ are of the form*

$$p_{v,y_1,y_2,\ldots,y_{i-1},y_i}$$

for $v < \ell(k)$ and, for every $(i-1)$-tuple $y_1, y_2, \ldots, y_{i-1} < k$ and for each $y_i < n$.

2. *We define the circuit $\overline{\Psi}_i^\ell(k,v)$ to be*

$$\bigvee_{y_1=0}^{k} \bigwedge_{y_2=0}^{k} \bigvee_{y_3=0}^{k} \cdots \bigtimes_{y_{i-1}=0}^{k} \bigtimes_{y_i=0}^{n} p_{v,y_1,\ldots,y_i}$$

where $\bigtimes_{y_{i-1}=0}^{k}$ is $\bigwedge_{y_{i-1}=0}^{k}$ if i is odd and an $\bigvee_{y_{i-1}=0}^{k}$ otherwise. Likewise, $\bigtimes_{y_i=0}^{k}$ is a $\bigvee_{y_i=0}^{k}$ if i is odd and an $\bigwedge_{y_i=0}^{k}$ otherwise.

3. *The circuit $\overline{P}_i^{\ell,k}$ is*

$$\bigvee_{v<\ell(k),\ v \text{ odd}} \left(\overline{\Psi}_i(k,v) \wedge \bigwedge_{v<v'<\ell(k)} \neg\overline{\Psi}_i(k,v')\right).$$

The essential idea of the above translation is that atomic formulas of the form $\alpha(\langle k, v, y_1, y_2\rangle)$ get translated as propositional variables $p_{v,y_1,\ldots,y_i}$ then existential quantifiers are translated as OR's and universal quantifiers are translated as AND's. Notice no atoms of the form $p_{0,y_1,\ldots,y_i}$ appear in $\overline{P}_i^{\ell,k}$. This makes sense since if the maximal v satisfying $\Psi_i^\ell(k, v, \alpha)$ is 0 then $P_i^\ell(k, \alpha)$ will be false. Under the truth assignment given in the next easily verifiable lemma we would also get that $\overline{P}_i^{\ell,k}$ is false.

Lemma X.C.4 $(i \geq 1, k \geq 0)$

1. *Let $\ell \in \tau$. The circuit $\overline{\Psi}_i^\ell(k, v)$ computes the truth value of $\Psi_i^\ell(k, v, \alpha)$ under the assignment*

$$p_{v,y_1,\ldots,y_i} = \begin{cases} 1 & \text{if } \langle k, v, y_1, \ldots, y_i\rangle \in \alpha \\ 0 & \text{otherwise} \end{cases}$$

2. *under the same assignment the circuit $\overline{P}_i^{\ell,k}$ computes the value of the predicate $P_i^\ell(k, \alpha)$.*

The next definition introduces a technical concept needed to apply a result of Hastad [25].

Definition X.C.5 1. *Let $(B_j)_j$ be a partition of the atoms of $\overline{P}_i^{\ell,k}$ into $\ell(k)\cdot k^{i-1}$ classes of the form*

$$\left\{ p_{v,y_1,\ldots,y_{i-1},y_i} \middle| y_i < \left(\frac{i \cdot k \log(k)}{2}\right)^{1/2} \right\}$$

one for every choice of $y_1, \ldots y_{i-1} < k$, $v < \ell(k)$.

2. *Let $0 < q < 1$ be a real number. A probability space R_q^+ of random restrictions is a space of restrictions ρ determined by the following process*

(a) Let

$$s_j := \begin{cases} * & \text{with probability } q \\ 0 & \text{with probability } 1 - q \end{cases}$$

(b) and for every atom $p \in B_j$ *let*

$$\rho(p) := \begin{cases} s_j & \text{with probability } q \\ 1 & \text{with probability } 1-q \end{cases}$$

3. *A probability space* R_q^- *is defined in the same way as* R_q^+ *except the roles of* 0 *and* 1 *are interchanged.*

4. *For any* $\rho \in R_q^+$, $g(\rho)$ *is a further restriction and renaming of the atoms defined for each* j *as follows:*

   (a) for j *such that* $s_j = *$ *let* $p_j = p_{v,y_1,\ldots,y_{i-1},y_i}$ *be the atom from* B_j *given value* $*$ *by* ρ *for the least value of* y_i.

   (b) $g(\rho)$ *gives value 1 to all* $p \in B_j$, $p \neq p_j$ *such that* $\rho(p) = *$.

   (c) $g(\rho)$ *renames* p_j *to* $p_{v,y_1,\ldots,y_{i-1}}$.

5. *For* $\rho \in R_q^-$, $g(\rho)$ *is is defined as in (4) except interchanging the roles of* 0 *and* 1.

6. *For* G *a circuit with atoms among those of the circuit* $\overline{P}_i^{\ell,k}$, *let* G^ρ *denote the circuit obtained from* G, *by performing the restriction* ρ *followed by the restriction* $g(\rho)$. *Note that the atoms of* G^ρ *will now be among the atoms of* $\overline{P}_i^{\ell,k}$.

The next lemma is one of two results we will use from Hastad [25].

Lemma X.C.6 *Let* $q := (2i\log(k)/k)^{1/2}$ *and assume* k *is sufficiently large. Then the following three conditions hold.*

1. *Let* G *be a depth 2 subcircuit of* $\overline{P}_i^{\ell,k}$: *That is,* G *is either an OR of AND's of size* $< (i \cdot k\log(k)/2)^{1/2}$ *or is an AND of OR's of size* $< (i \cdot k\log(k)/2)^{1/2}$. *Pick* ρ *at random from* R_q^+, *if* G *is an OR of ANDs, and from* R_q^-, *if it is an AND of ORs. With probability at least*

$$1 - \frac{1}{3}k^{-i+1}$$

G^ρ is an OR (resp. an AND) of at least $((i-1)\cdot k\log(k)/2)^{1/2}$ different atoms.

2. *($i \geq 3$) Pick ρ at random from R_q^+ for i even and from R_q^- for i odd. With probability at least two-thirds the circuit $(\overline{P}_i^{\ell,k})^\rho$ is $\overline{P}_{i-1}^{\ell,k}$ after a suitable renaming of variables.*

3. *($i = 2$) Pick ρ at random from R_q^+. With probability at least two-thirds the circuit $(\overline{P}_2^{\ell,k})^\rho$ is $\overline{P}_1^{\ell,n}$ after a suitable renaming of variables, where n is $(k\log(k)/2)^{1/2}$.*

Proof: We sketch the parts of the proof following [34, 12].

(1) Consider G an OR of ANDs and let $\rho \in R_q^+$ (the case where G is an AND of ORs is similar). An AND gate of G corresponds to a class B_j of atoms and after ρ takes the value s_j with probability at least

$$\begin{aligned} 1-(1-q)^{|B_j|} &= 1-\left(1-\left(\frac{2i\log(k)}{k}\right)^{1/2}\right)^{\left(\frac{ik\log(k)}{k}\right)^{1/2}} \\ &> 1-e^{-i\log k} > 1-\frac{1}{6}k^{-i}. \end{aligned}$$

Thus, with probability at least $1-\frac{1}{6}m^{-i+1}$ this is true of all m ANDs in G. The expected number of ANDs assigned the values s_j and then further assigned $*$ rather than 0 by ρ is $k\cdot q = (2ik\log(k))^{1/2}$. In fact, with probability at least

$$1-\frac{1}{6}k^{-i}$$

we get at least $((i-1)k\log(k))/2)^{1/2}$ s_j's assigned. To see this let r_u be the probability that exactly u of the ANDs are assigned value $*$ by ρ. Then r_u is the binomial coefficient

$$\binom{k}{u}q^u(1-q)^{k-u} = \binom{k}{u}\left(\frac{2i\log(k)}{k}\right)^{\frac{1}{2}u}\left(1-\frac{2i\log(k)}{k}\right)^{k-u}$$

For $u \leq (ik\log(k))^{\frac{1}{2}}$ it holds that $r_u/r_{u-1} \geq \sqrt{2}$. Also for k sufficiently large,

$k \geq 49i \log k$. As $r_{ik\log(k))^{\frac{1}{2}}} < 1$. we get the following estimate

$$\begin{aligned}
\sum_{u=0}^{(\frac{1}{2}ik\log(k))^{\frac{1}{2}}} r_u &\leq r_{(\frac{1}{2}ik\log(k))^{\frac{1}{2}}} \sum_{u=0}^{\infty} 2^{-\frac{1}{2}u} \\
&< 4r_{(\frac{1}{2}ik\log(k))^{\frac{1}{2}}} \\
&\leq 4(\sqrt{2})^{-(1-2^{-1/2})(ik\log(k))^{1/2}} r_{(\frac{1}{2}ik\log(k))^{\frac{1}{2}}} \\
&\leq 4(\sqrt{2})^{-(1-2^{-1/2})(i(49i\log(k))\log(k))^{1/2}} r_{(\frac{1}{2}ik\log(k))^{\frac{1}{2}}} \\
&\leq 4(\sqrt{2})^{-(1-2^{-1/2})(7i\log(k))} \\
&\leq \frac{1}{6}m^{-i}
\end{aligned}$$

So with probability at least

$$1 - \frac{1}{3}k^{-i+1}$$

the circuit G^ρ is an OR of at least $((i-1)k\log(k)/2)^{1/2}$ different atoms.

(2) There are $\ell(k)k^{i-2}$ subcircuits of depth 2 is $\overline{P}_i^{\ell,k}$. By our assumption $\ell(k) \leq k$, and (1), with probability at least

$$1 - \frac{1}{3}\ell(k)k^{-1} \geq \frac{2}{3}$$

all of them are restricted by ρ as described in the conclusion of (1). Thus, after renaming the atoms, $(\overline{P}_i^{\ell,k})^\rho$ becomes $\overline{P}_{i-1}^{\ell,k}$.

(3) When $i = 2$, the circuit $\overline{\Psi_i}(k, v)$ is an AND of size $(k\log(k))^{1/2}$ corresponding to the k classes B_j. By (1) with probability at least (5/6) they are all assigned the value the value s_j. Further, s_j is $*$ with probability at least (5/6) for at least $(k\log(k))^{1/2}$ of these ANDs. □

The next definition gives a notion a truth table reducibility which we will use to represent propositional translations of predicates in $P^{\Sigma_i^p(\alpha)}(\{||\dot{\ell}||\})$.

Definition X.C.7

1. *A Boolean circuit is called* $\Sigma_{i,k}^{S,t}$ *if*

   (a) it has depth $i+1$ *and its top gate is an OR.*

(b) OR's and AND's gates alternate in levels.

(c) it has at most S gates at each level greater than 2.

(d) its bottom gates have arity at most t.

(e) the inputs to its bottom gates are the atoms or negated atoms of $\overline{P}_i^{\ell,k}$.

2. *A $tt^{||\ell||}$-reducibility of type (i,k,d) is a Boolean formula of the form*

$$f(w_1,\ldots,w_m)$$

in $m \leq 2^{(||\ell(k)||)^d}$ variables together with $\Sigma_{i,k}^{S,t}$-circuits $E_1,\ldots,E_m$ where $S = 2^{(\log k)^d}$, and $t = \log(S)$.

3. *A $tt^{||\ell||}$-reducibility D of type (i,k,d) computes a function of the atoms of $\overline{P}_i^{\ell,k}$ in the following way: First evaluate $w_j := E_j$ on the atoms and then evaluate $f(w_1,\ldots,w_m)$.*

Let $S = 2^{(\log k)^d}$ for some constant d. Suppose one has a $\Sigma_i^b(\alpha)$ formula $A(\vec{x})$. For a fixed input $\vec{k}$ one can translate $A(\vec{k})$ into propositional formula $\bar{A}(\vec{k})$ as follows:

(1) If $A(\vec{k})$ is of the form $t(\vec{k}) \leq s(\vec{k})$ or $t(\vec{k}) = s(\vec{k})$ then $\bar{A}(\vec{k})$ is either $\top$ or *bot* according to the value of the atomic formula on input k.

(2) If $A(\vec{k})$ is of the form $\alpha(\langle\vec{k}\rangle)$ where y_i are bounds variables then $\bar{A}(\vec{k})$ is $p_{\vec{k}}$.

(3) If $A(\vec{k})$ is of the form $B \circ C$ where $\circ$ is a binary connective then $\bar{A}(\vec{k})$ is $\bar{B} \circ \bar{C}$.

(4) If $A(\vec{k})$ is of the form $\neg B$ then $\bar{A}(\vec{k})$ is $\neg\bar{B}$.

(5) If $A(\vec{k})$ is of the form $(\exists y \leq t(\vec{k}))B(\vec{k},y)$ where d is a fixed integer then $\bar{A}(\vec{k})$ is $\vee_{j=0}^{t(\vec{k})}\bar{B}(\vec{k},j)$.

(6) If $A(\vec{k})$ is of the form $(\forall y \leq t(\vec{k}))B(\vec{k},y)$ where d is a fixed integer then $\bar{A}(\vec{k})$ is $\wedge_{j=0}^{t(\vec{k})}\bar{B}(\vec{k},y)$.

Assume $X(\langle\vec{k}\rangle)$ is an oracle set which is false if $\vec{k}$ is not of the form $\langle k, r, y_1, \ldots, y_n\rangle$. It is not hard to modify the quantifier bounds of a $\Sigma_i^b(X)$-formula A so that a $\Sigma_{i,k}^{S,\log(S)}$-circuit can be used to compute the value of $A(k)$ under this translation and under the truth assignment $p_{\vec{k}} = \top$ iff $\langle\vec{k}\rangle \in X$. Given this if A and B are in $\Sigma_i^b(X)$, then it follows there is a $tt^{\|\ell\|}$-reducibility of type (i, k, d) computing the value of

$$(\exists v \leq \ell(k))[A(k, v, X) \wedge \neg B(k, v+1, X)].$$

We now prove some lemmas designed to show the limitations on $tt^{\|\ell\|}$-reducibilities. This will allow us to derive our separation results.

Lemma X.C.8 *Let G be an AND of OR's of size $\leq t$ with atoms among those of $\overline{P}_i^{\ell,k}$. Pick ρ randomly from R_q^+ or from R_q^-.*

Then with probability at least

$$1 - (6qt)^s$$

the circuit G^ρ can be written as an OR of ANDs of size $< s$.

The same is valid for the probability of the switching an OR of AND's into an AND of OR's.

The proof of the above lemma can be found in Hastad [25].

Lemma X.C.9 *Let $q := (2i\log(k)/k)^{1/2}$ and let D be a $tt^{\|\ell\|}$-reducibility of type (i, k, d). Pick ρ at random from R_q^+ or from R_q^-.*

Then with probability at least a $\frac{1}{2}$

$$D^\rho := \langle f; E_1^\rho, \ldots, E_m^\rho\rangle$$

is a $tt^{\|\ell\|}$-reducibility of type $(i-1, k, d)$.

Proof: Let $t = s = (\log k)^d$ and apply Lemma X.C.8. The probability that a depth 2 subcircuit of any E_j fails to be switched is at most

$$(6qt)^t = \left(6\left(\frac{2i\log(k)}{k}\right)^{1/2}(\log k)^d\right)^{(\log k)^d} < 2^{2\cdot(\log k)^d}$$

for large enough k.

There are fewer than $(\log k)^d \cdot 2^{(\log k)^d}$ such depth 2 subcircuits, so with probability at least

$$1 - (\log k)^d \cdot 2^{-(\log k)^d} > 1/2$$

all of them are switched. The switched subcircuits can be combined with the level 3 gates, reducing the depth of the E_j's by 1. □

Lemma X.C.10 *Let D be a $tt^{\|\ell\|}$-reducibility of type (i, k, d) computing the predicate $P_i^\ell(k, X)$ for all $X \subseteq \omega$.*

Then there is a $tt^{\|\ell\|}$-reducibility of type $(1, k, d)$ computing the predicate $P_1^\ell((k\log(k)/2)^{1/2}, Y)$ for every $Y \subseteq \omega$.

Proof: By Lemma X.C.4, the predicate $P_i^\ell(k, X)$ is computed by the circuit $\overline{P}_i^{\ell,k}$. Lemma X.C.6 and Lemma X.C.9 imply that a random restriction ρ (drawn from R_q^+ if i is even and R_q^- if i odd) has greater than 1/6 chance of simultaneously converting $\overline{P}_i^{\ell,k}$ into $\overline{P}_{i-1}^{\ell,k}$ and converting D into a $tt^{\|\ell\|}$-reducibility of type $(i-1, k, d)$. Since this probability is nonzero, there is some ρ which does this conversion. Applying this conversion $(i-1)$-times (for the last iteration use Lemma X.C.6 (3)) proves the lemma. □

Lemma X.C.11 $(i \geq 1)$ *For fixed d and sufficiently large k there is no $tt^{\|\ell\|}$-reducibility of type (i, k, d) correctly computing the predicate $P_i^\ell(k, X)$ for all $X \in \omega$).*

Proof: In view of Lemma X.C.10, it suffices to show no $tt^{\|\ell\|}$-reducibility of type $(1, k, d)$ correctly computes $P_1^\ell((k\log(k)/2)^{1/2}, Y)$ for every $Y \in \omega$.

To begin, let $n := (k\log(k)/2)^{1/2}$, $t := \log(k)^d$, and let

$$D = \langle f; E_1, \ldots, E_m \rangle$$

be a $tt^{\|\ell\|}$-reducibility of type $(1, k, d)$. So $m \leq 2^{\|\ell(k)\|^c}$. Here E_i are $\Sigma_{1,k}^{2^{(\log k)^d},(\log k)^d}$-circuits. For simplicity write P for $\overline{P}_1^n$.

In our argument, we will be working with ordered triples $\langle k, v, y_1 \rangle$ where the k is the fixed k in the statement of the lemma. For a finite set X of ordered triples $\langle k, v, y_1 \rangle$, we write $\max_p(X)$ for $p = 1, 2, 3$ to denote the largest value of the pth coordinate appearing in any ordered triple in X. We define $\min_p(X)$ similarly. We shall construct a sequence of sets of numbers X_s^+, X_s^-, I_s satisfying

1. $X_s^+ \cap X_s^- = \emptyset$ and for any number $\langle k, v, y_1 \rangle$ in X_s^+ we have $v < 2s$.

2. $|X_s^-| \leq s$ and $|X_s^+ \cup X_s^-| \leq st$.

3. $I_s \subseteq \{1, \ldots, m\}$ and $|I_s| = s$.

4. for every $Y \subseteq \omega$ such that

$$X_s^+ \subseteq Y \wedge X_s^- \cap Y = \emptyset$$

we have

$$E_j^Y = 1$$

for all $j \in I_s$. Here E_j^Y denotes the circuit E_j evaluated according to Y where evaluated according to Y means a propositional variable p_{v,y_1} is true iff $\langle k, v, y_1 \rangle \in Y$.

We begin with $X_0^+ := X_0^- := I_0 = \emptyset$. For stage $s+1$, assume we have X_s^+, X_s^-, I_s satisfying the conditions stated.

Set $Y := X_s^+$. So by condition (4), $E_j^Y = 1$ for all $j \in I_s$. Consider the following three cases:

(a) $D^Y = 1$ but $\max_2(Y)$ is 0 mod2, or $D^Y = 0$ but $\max_1(Y)$ is 1 mod2. In this case STOP.

(b) $D^Y = 1$ and $\max_2(Y)$ is 1 mod2. Consider the set

$$Y = \{\langle k, v, y_1 \rangle \mid$$
$$\max_2(X_s^+) < v < \ell(2^t), y_1 \leq 2^t, v = 0 \text{ mod2}, \langle k, v, y_1 \rangle \notin X_s^- \}$$

By condition (1), (2) and (3), the set Y' is nonempty since

$$2s \leq 2m \leq 2 \cdot 2^{||\ell(k)||^c} \leq 2^{||\ell(k)||^{c+1}} < \ell(k) \leq \ell(2^{(\log k)^d}) = \ell(2^t)$$

for sufficiently large k. That $2^{||\ell(k)||^{c+1}} < \ell(k)$ for sufficiently large k follows since $\ell(k)$ is unbounded and nondecreasing. That $\ell(k) \leq \ell(2^{(\log k)^d})$ follows since ℓ is nondecreasing. There are two subcases:

(b1) It is possible to add some element $\langle k, v, y_1 \rangle \in Y'$ to Y' to form

$$Y'' := Y' \cup \{\langle k, v, y_1 \rangle\}$$

such that $D^{Y''} = D^{Y'} = 1$.

In this subcase set $X^+_{s+1} := X^+_s \cup \{\langle k, v, y_1 \rangle\}$ and $X^-_{s+1} := X^-_s$ and STOP.

(b2) There is no $\langle k, v, y_1 \rangle \in Y'$ with property (b1).

Take $\langle k, v, y_1 \rangle$ in Y' such that $v = min_2(Y')$ and such that $\langle k, v, y'_1 \rangle$ in Y' implies $y_1 \leq y'_1$. Since (b1) does not apply the circuit D evaluated according to $Y' \cup \{\langle k, v, y_1 \rangle\}$ changes value. There are two subsubcases: (1) some E_{j_0} for $j_0 \notin I_s$ received new value 1. (2) some E_{j_0} for $j_0 \notin I_s$ received new value 0. In the first case, we set set $X^+_{s+1} := X^+_s \cup \{\langle k, v, y_1 \rangle\}$. As the circuit E_{j_0} is an $\Sigma^{2^t,t}_{1,n}$-circuit, it is an OR of ANDs. One of the ANDs of E_{j_0} must have become true. Add the indices of all negatively occurring atoms of E_{j_0} to X^-_s to form X^-_{s+1}. This is correct since if they were in X^+_s then the AND in E_{j_0} could not have evaluated to 1. Similarly, all the positive atoms necessary to make this AND true must be in X^+_{s+1}. In the second case, we want to make sure E_{j_0} stays equal to 1 so we set $X^+_{s+1} = X_s$. The element $\langle k, v, y_1 \rangle$ must occur negatively in one of E_{j_0}'s ANDs, so we form X^-_{s+1} by adding to X^-_s the element $\langle k, v, y_1 \rangle$ and the at most t negatively occuring elements in this AND. Notice in both cases $|X^+_{s+1}| < s+1$ and $|X^+_{s+1} \cup X^-_{s+1}| < st + t = (s+1)t$. Also notice $min_2(Y')$ is at most $max_2(X^+_s) + 2$. Since the total

number of elements in $X_s^+ \cup X_s^-$ is less than st there will always be y_1's such that for each sized $v > max_2(X_s^+)$ there is a tuple $\langle k, v, y_1 \rangle$ in Y.

Let $I_{s+1} := I_s \cup \{j_0\}$ and go to $s+2$.

It is easy to check that the new sets X_{s+1}^+, X_{s+1}^-, and I_{s+1} fulfill conditions (1)-(4).

(c) $D^Y = 0$ and $\max_1(Y)$ is even. In this case, let

$$Y = \{\langle k, v, y_1 \rangle \mid \max_2(X_s^+) < v < \ell(2^t), y_1 \leq 2^t, v = 1 \bmod 2, \langle k, v, y_1 \rangle \notin X_s^-\}$$

and proceed analogously to case (b).

If the construction has not terminated by stage s, then $I_s \subsetneq I_{s+1}$. Thus, by condition (3) the construction must halt eventually.

Let $Y := X_s^+$ for the final s. If during the construction only step (b) or (c) ever apply then D^Y does not agree with P^Y because condition (4) would imply the circuit was constant, yet for sufficiently large k that there are elements $\langle k, v, y_1 \rangle$, $\langle k, v', y_1' \rangle$ in Y such that $v := 0 \bmod 2$ and such that $v' := 1 \bmod 2$. If (a) ever applies then we are also done. Thus, the lemma follows. □

Theorem X.C.12 ($i \geq 1$) *There is a recursive oracle X such that*

$$P^{\Sigma_i^p(X)}(\{||\dot{\ell}||\}) \subsetneq P^{\Sigma_i^p(X)}(\{|\ell|\})$$

Proof: We construct the oracle $X \subseteq \omega$ such that the predicate $P_i^\ell(x, X)$ is not in $P^{\Sigma_i^p(X)}(\{|\ell(|\dot{id}|)|\})$.

By an easy extension to Corollary VI.E.6, any $P^{\Sigma_i^p(X)}(\{||\dot{\ell}||\})$ predicate can be written in the form

$$(\exists v \leq 2^{||\ell||^d})[C(x, v, X) \wedge \neg D(x, v+1, X)] \tag{X.1}$$

where C and D are $\Sigma_i^p(X)$-formulas and d is a constant. Let $F_j^{||\ell||}$, j=0,1, ... enumerate all such predicates in $P^{\Sigma_i^p(X)}(||\ell||)$. We shall consider successive j's and build X in stages to ensure that $F_j^{||\ell||}$ is not equivalent to the predicate $P_i^\ell(x, X)$.

Let X_s be the approximation of X constructed in the first s stages and let $s+1$ be the index of the predicate $F_{s+1}^{\|\ell\|}$ to be considered next. Choose $k := k_{s-1}$ so large that all numbers considered in the first s stages are small with respect to k. As we have mentioned earlier, for each fixed number k, formulas of the form (X.1) can be computed by a $tt^{\|\ell\|}$-reducibility D in a straightforward way. Let $D_{s+1}^{\|\ell\|}$ be the reducibility computing $F_{s+1}^{\|\ell\|}$. In the $\Sigma_{i,k}^{S,\log(S)}$-circuits of $D_{s+1}^{\|\ell\|}$ evaluate the atoms with indices corresponding to "$n \in \alpha$" according to A_s and set to 0 all atoms whose indices are not of the form $\langle k, v, y_1, \ldots, y_i \rangle$.

This leaves us with a $tt^{\|\ell\|}$-reducibility of type (i, k, d), which cannot compute $P_i^{\ell}(k, Y)$ correctly for all $Y \subset \omega$ by Lemma X.C.11. Since a finite Y for which the reducibility fails was constructed in Lemma X.C.11 whose elements were coding of triples the first coordinate always fixed at the value k, we can take $X_{s-1} = X_s \cup Y$ and the reducibility will fail for X_{s+1}. Hence, formula $F_{s+1}^{\|\ell\|}$ will not be equivalent to $P_i^{\ell}(x, X_{s+1})$. So $F_{s+1}^{\|\ell\|}$ will not be equivalent to $P_i^{\ell}(x, X)$ where $X = \bigcup_s X_s$.

Proceed to $s+2$.

This completes the proof. □

The next corollaries follow from the above theorem and the discussion at the beginning of this section.

Corollary X.C.13 *Suppose τ surpasses ℓ is a nondecreasing, unbounded item and suppose τ' is surpassed by $|\ell|$. Then:*

1. $\hat{T}_2^{i,\tau'}(\alpha) \subseteq \hat{C}_2^{i,\tau'}(\alpha) \subsetneq_{\hat{\Delta}_{i+1}^b(\alpha)} \hat{T}_2^{i,\tau}(\alpha) \subseteq \hat{C}_2^{i,\tau}(\alpha)$.
2. $T_2^{i-1}(\alpha) \not\supseteq_{\hat{\Delta}_{i+1}^b(\alpha)} \hat{T}_2^{i,\tau}(\alpha)$.
3. $\hat{T}_2^{i+1,\{\|\|\ell\|\|\}}(\alpha) \subsetneq_{\hat{\Delta}_{i+1}^b(\alpha)} \hat{T}_2^{i,\{\ell\}}(\alpha)$.

From the above general result it follows:

Corollary X.C.14 $(i \geq 1, m \geq 0)$

1. $\hat{R}_2^i(\alpha) \subseteq R_2^i(\alpha) \subsetneq_{\Delta_{i+1}^b(\alpha)} S_2^i(\alpha) \subsetneq_{\Delta_{i-1}^b(\alpha)} T_2^i(\alpha)$.

2. $\hat{T}_2^{i,m+1}(\alpha) \subseteq \hat{C}_2^{i,m+1}(\alpha) \subsetneq_{\Delta_{i+1}^b(\alpha)} \hat{T}_2^{i,m}(\alpha) \subseteq \hat{C}_2^{i,m}(\alpha)$.

3. $T_2^i(\alpha) \not\subseteq R_2^{i+1}(\alpha)$.

4. $T_2^i(\alpha) \not\supseteq \hat{T}_2^{i+1,m}(\alpha)$.

5. $T_2^i(\alpha) \not\supseteq R_2^{i+1}(\alpha)$.

6. $\hat{T}_2^{i,m}(\alpha) \not\subseteq \hat{T}_2^{i+1,m+2}(\alpha)$.

Appendix

The intention of this appendix is to put some of the principle results of this thesis into pictures or tables in one place in such a way as to be more easily digestible.

The next corollary summarizes the consequences of our general results to the well-studied theories R_2^i, S_2^i, and T_2^i.

Corollary A.15

(a)

$$\begin{array}{ccccc} \hat{T}_2^{i,\{2^{p(|x|)}\}} \preceq_{B(\hat{\Sigma}_{i+1}^b)} & R_2^{i+1} & \subseteq & S_2^{i+1} \subseteq T_2^{i+1} \\ & \cup| & & \curlyvee| B(\Sigma_{i+1}^b) \\ & \wr & \tilde{S}_2^i & \subseteq & \tilde{T}_2^i \\ & & \curlyvee| B(\hat{\Sigma}_{i+1}^b)^+ & & \curlyvee| B(\hat{\Sigma}_{i+1}^b)^+ \\ & R_2^i \subseteq & S_2^i & \subseteq & T_2^i \end{array}$$

(b) $T_2^{i-1}(\alpha) \not\supseteq_{\hat{\Delta}_{i+1}^b(\alpha)} R_2^i(\alpha) \subsetneq_{\hat{\Delta}_{i+1}^b(\alpha)} S_2^i(\alpha) \subsetneq_{\hat{\Delta}_{i+1}^b(\alpha)} T_2^i(\alpha)$

(c) $R_2^i(\alpha) \subsetneq_{\hat{\Delta}_i^b(\alpha)} T_2^{i-1}(\alpha)$

(d) $T_2^{i-1} = R_2^i$ *implies* $\Sigma_{i+3}^p = \Pi_{i+3}^p$.

A '$*$' beside an inclusion indicates a new result. A '$+$' beside an inclusion indicates Σ_i^b-conservative was previously known. The '$\sim$' above the S and T means the theory with Σ_{i+1}^b-$REPL^{\{|id|\}}$ added. The notation $T_1 \subseteq_\Psi T_2$ means the Ψ-consequences of T_1 are contained in T_2. The notation $T_1 \preceq_\Psi T_2$ means the $T_1 \subset T_2$ and the Ψ consequences of T_2 and provable in T_1.

Proof: The above results follow as special cases of our general results listed below and Theorem II.E.1 which shows $\hat{S}_2^i = S_2^i$ and $\hat{T}_2^i = T_2^i$. We also use the fact that $\tilde{S}_2^i = \hat{C}_2^{i,\{|id|\}}$ by Theorem II.E.1 and Theorem VIII.A.1. Lastly, we use the fact that S_2^{i+1} proves Σ_{i+1}^b-$REPL^{\{|id|\}}$, so $T_2^i \preceq_{B(\hat{\Sigma}_{i+1}^b)} S_2^{i+1}$ implies $T_2^i \preceq_{B(\hat{\Sigma}_{i+1}^b)} \tilde{T}_2^i$

□

The diagram in the corollary below summarizes the principle structural relationships between $\hat{T}_2^{i,\tau}$ and $\hat{C}_2^{i,|\tau|}$ we have established in this thesis.

Corollary A.16

(a)

$$\begin{array}{rll} \hat{T}_2^{i+1,\|\tau\|} \preceq_{B(\hat{\Sigma}^b_{i+1})} & \hat{T}_2^{i+1,\|\tau\|} \cup \hat{C}_2^{i,|\tau|} \\ & \cap| \\ & \hat{T}_2^{i+1,|\tau|} \preceq_{B(\hat{\Sigma}^b_{i+2})} \hat{C}_2^{i+1,|\tau|} \\ & \curlyvee| B(\hat{\Sigma}^b_{i+1}) \\ \hat{T}_2^{i,\tau} = \hat{T}_2^{i,\dot{\tau}} \subseteq & \hat{T}_2^{i,\tau^\#} \end{array}$$

(b) $\hat{T}_2^{i,\{\ell(|id|)\}}(\alpha) \subsetneq_{\hat{\Delta}^b_{i+1}(\alpha)} \hat{T}_2^{i,\{\ell\}}(\alpha)$

(c) $T_2^{i-1}(\alpha) \not\supseteq_{\hat{\Delta}^b_{i+1}(\alpha)} \hat{T}_2^{i,\{\ell\}}(\alpha)$

(d) $\hat{T}_2^{i+1,\{|\ell(|id|)|\}}(\alpha) \subsetneq_{\hat{\Delta}^b_{i+1}(\alpha)} \hat{T}_2^{i,\{\ell\}}(\alpha)$

In the above, ℓ is a nondecreasing unbounded iterm.

Proof: (a) This follows from Theorem II.G.7, Theorem II.G.8, Theorem II.G.11, Theorem VII.B.1, and Corollary VIII.B.6.

(b), (c), (d) follow from Corollary X.C.13. □

We also show in Corollary X.A.2 the following equalities imply the collapse of the polynomial hierarchy.

Corollary A.17 ($i \geq 0$) *The following statements imply $\Sigma^p_{i+3} = \Pi^p_{i+3}$:*

(a) $T_2^i = \hat{T}_2^{i+1,|\tau'|}$

(b) $T_2^i = \hat{C}_2^{i+1,|\tau'|}$

(c) $\hat{C}_2^{i,|\tau|} = \hat{T}_2^{i+1,|\tau'|}$.

where τ and τ' are two sets of iterms such that τ' contains at least one nondecreasing, unbounded iterm.

Another result we prove in Corollary VI.E.6 and Corollary VII.C.7 is the following.

Corollary A.18 ($i \geq 1$) *The theory $\hat{T}_2^{i,\tau}$ proves its $\hat{\Delta}^b_{i+1}$-predicates can be written*

in the form

$$(\exists v \leq \ell(s(x)))[A(x, v) \wedge \neg B(x, v+1)].$$

where A *and* B *are* $\hat{\Sigma}^b_i$*-formulas and* ℓ *is a* $\hat{\tau}$*-term and* s *is an* L_2*-term. Furthermore, every* $\hat{\Sigma}^b_{i+1} \cap_{|\tau|} \hat{\Pi}^b_{i+1}$*-formula is* $\hat{\Delta}^b_{i+1}$ *with respect to* $\hat{T}^{i,|\tau|}_2$.

The corollary below presents our results concerning multifunctions definable in R^i_2, S^i_2 and T^i_2.

Corollary A.19

	$\hat{\Sigma}^b_i$	$\hat{\Sigma}^b_{i+1}$	$\hat{\Sigma}^b_{i+k}(k \geq 2)$
T^i_2	$\pi LS^{FP^{\Sigma^p_{i-1}}(wit,1)}_{\{id\}}$	$FP^{\Sigma^p_i}(wit, poly)$	$FP^{\Sigma^p_{i+k-1}}(wit, 1)$
S^i_2	$\pi LS^{FP^{\Sigma^p_{i-1}}(wit,1)}_{\{\|id\|\}}$	$FP^{\Sigma^p_i}(wit, \log)$	$FP^{\Sigma^p_{i+k-1}}(wit, 1)$
R^i_2	$\pi LS^{FP^{\Sigma^p_{i-1}}(wit,1)}_{\{\|\|id\|\|\}}$	$FP^{\Sigma^p_i}(wit, \log\log)$	$FP^{\Sigma^p_{i+k-1}}(wit, 1)$

	$\hat{\Delta}^b_i$	$\hat{\Delta}^b_{i+1}$	$\hat{\Delta}^b_{i+k}(k \geq 2)$
T^i_2	$\pi LS^{FP^{\Sigma^p_{i-1}}(wit,1)}_{\{id\}}$ *rel'ns*	Δ^p_{i+1}	$P^{\Sigma^p_{i+k-1}}(1)$
S^i_2	$\pi LS^{FP^{\Sigma^p_{i-1}}(wit,1)}_{\{\|id\|\}}$ *rel'ns*	$P^{\Sigma^p_i}(\log)$	$P^{\Sigma^p_{i+k-1}}(1)$
R^i_2	$\pi LS^{FP^{\Sigma^p_{i-1}}(wit,1)}_{\{\|\|id\|\|\}}$ *rel'ns*	$P^{\Sigma^p_i}(\log\log)$	$P^{\Sigma^p_{i+k-1}}(1)$

Proof: These results follow from Corollary VI.E.2, Corollary VI.E.4, Corollary VI.E.5, Theorem VII.A.2, and Corollary VII.A.3. By relations we mean $0-1$ valued functions. □

The corollary below presents our results concerning multifunctions definable in $\hat{T}^{i,\tau}_2$ and $\hat{C}^{i,|\tau|}_2$.

Corollary A.20

	$\hat{\Sigma}^b_i$	$\hat{\Sigma}^b_{i+1}$	$\hat{\Sigma}^b_{i+k}(k \geq 2)$
$\hat{T}^{i,\tau}_2$	$\pi LS^{FP^{\Sigma^p_{i-1}}(wit,1)}_{\tau}$	$FP^{\Sigma^p_i}(wit, \|\tau\|)$	$FP^{\Sigma^p_{i+k-1}}(wit, 1)$
$\hat{C}^{i,\|\tau\|}_2$	$\pi LS^{FP^{\Sigma^p_{i-1}}(wit,1)}_{\|\tau\|}$	$FP^{\Sigma^p_i}(wit, \|\|\tau\|\|)$	$FP^{\Sigma^p_{i+k-1}}(wit, 1)$

	Δ_i^b	$\hat{\Delta}_{i-1}^b$	$\hat{\Delta}_{i+k}^b (k \geq 2)$
$\hat{T}_2^{i,\tau}$	$\pi LS_\tau^{FP^{\Sigma_{i-1}^p}(wit.1)}$ *rel'ns*	$P^{\Sigma_i^p}(\|\tau\|)$	$P^{\Sigma_{i+k-1}^p}(1)$
$\hat{C}_2^{i,\|\tau\|}$	$\pi LS_{\|\tau\|}^{FP^{\Sigma_{i-1}^p}(wit.1)}$ *rel'ns*	$P^{\Sigma_i^p}(\|\|\tau\|\|)$	$P^{\Sigma_{i+k-1}^p}(1)$

Proof: As with the last corollary, these results follow from Corollary VI.E.2, Corollary VI.E.4, Corollary VI.E.5, Theorem VII.A.2, and Corollary VII.A.3. By relations we mean $0-1$ valued functions. □

We list below some of the single-valuedness results proven in this thesis. Our results imply the Buss [14] result that the Σ_i^b-definable functions of T_2^{i-1} and S_2^i are the class $FP^{\Sigma_i^p}$. It should be noted that (d) was previously proven in Bloch [8].

Corollary A.21

(a) $(i \geq 1)$ *The class of* τ*-bounded* $\hat{\Sigma}_{i+1}^b$*-definable functions of* $\hat{T}_2^{i,\tau}$ *is the class* τ-$PFP^{\Sigma_i^p}(|\tau|)$.

(b) $(i \geq 1)$ *The class of* τ*-bounded* $\hat{\Sigma}_{i+1}^b$*-definable functions of both* $\hat{T}_2^{i,|\tau|}$ *and* $\hat{C}_2^{i,|\tau|}$ *is precisely the class of* τ*-bounded functions in* τ-$PFP^{\Sigma_i^p}(||\tau||)$.

(c) $(i > 1)$ *The class of* τ*-bounded* $\hat{\Sigma}_i^b$*-definable functions of both* $\hat{T}_2^{i,|\tau|}$ *and* $\hat{C}_2^{i,|\tau|}$ *is precisely the class of* τ*-bounded functions in* τ-$PF(\hat{\Sigma}_i^b \cap_{|\tau\#|} \hat{\Pi}_i^b)$.

(d) $(i \geq 1)$ *The* $\hat{\Sigma}_{i+1}^b$*-definable functions of* S_2^i *are precisely the class* $(FNC^1)^{\Sigma_i^p}$.

(e) $(i \geq 1)$ *The* $\hat{\Sigma}_{i+1}^b$*-definable functions of* R_2^{i+1} *are precisely the class* $(FNC)^{\Sigma_i^p}$.

(f) The $\hat{\Sigma}_{1,|\tau|}^b$*-definable functions of* $\bar{C}_2^{0,|\tau|}$ *are the class* FTC_τ^0.

Proof: These results follow from Corollary IX.B.7, Corollary IX.B.10, Theorem IX.C.7, and Corollary IX.D.13. □

The next table lists the principle relationships between the various axioms schemas introduced in this thesis.

Corollary A.22 ($i \geq 0$) *The following axiom schema are equivalent in the presence of EBASIC:*

(a)

$$\begin{array}{ccccc}
\hat{\Pi}^b_{i+1}\text{-}REPL^{|\tau|} & \Longleftrightarrow & \hat{\Pi}^b_{i+1}\text{-}REPL^{(|\tau|)} & \Longleftrightarrow & \hat{\Sigma}^b_{i+2}\text{-}REPL^{|\tau|} \\
\Downarrow (*) & & & & \\
\hat{\Sigma}^b_{i-1}\text{-}IND^{|\tau|} & \Longleftrightarrow & \hat{\Sigma}^b_{i+1}\text{-}COMP^{|\tau|}(*) & \Longrightarrow & \hat{\Pi}^b_i\text{-}REPL^{|\tau|} \\
\Downarrow & & & & \\
\hat{\Delta}^b_{i+1}\text{-}IND^{\tau^\#} & \Longleftrightarrow & \hat{\Sigma}^b_i\text{-}IND^{\tau^\#} & \Longleftrightarrow & \hat{\Pi}^b_i\text{-}IND^{\tau^\#} \\
\Downarrow & & & & \\
\hat{\Sigma}^b_i\text{-}IND^{\tau} & \Longleftrightarrow & \hat{\Sigma}^b_i\text{-}IND^{\dot{\tau}} & \Longleftrightarrow & \hat{\Pi}^b_i\text{-}IND^{\dot{\tau}} \\
\Downarrow & & & & \\
\hat{\Sigma}^b_i\text{-}IND^{|\tau|} & & & &
\end{array}$$

A '$*$' indicates the additional presence of open-$IND^{|\tau|}$.

(b)

$$\begin{array}{ccccc}
\hat{\Sigma}^b_{i+1}\text{-}IND^{\tau} & \Longleftrightarrow & \hat{\Sigma}^b_{i+1}\text{-}MIN^{\tau} & \Longleftrightarrow & \hat{\Pi}^b_i\text{-}MIN^{\tau} \\
\Updownarrow & & & & \\
\hat{\Sigma}^b_{i+1}\text{-}MAX^{\tau} & \Longleftrightarrow & \hat{\Pi}^b_i\text{-}MAX^{\tau} & &
\end{array}$$

(c) $\hat{\Sigma}^b_{i+2} \cap_{|\tau|} \hat{\Pi}^b_{i+2}\text{-}IND^{|\tau|} \Longleftrightarrow \hat{\Delta}^b_{i+2}\text{-}IND^{|\tau|} \Longleftrightarrow \hat{\Sigma}^b_{i+1}\text{-}IND^{|\tau|}$

Proof: (a) follows from Theorem II.G.8. Theorem II.G.11. Theorem II.G.10. Theorem II.G.7. Theorem VII.C.9. Theorem VIII.A.1. Theorem IX.A.2. and Theorem IX.A.6.

(b) follows from Lemma III.C.4.

(c) follows from Corollary VII.C.7 and Corollary VII.C.6 □

Index

Bibliography

[1] L. Adleman and K. Manders. Computational complexity of decision procedures for polynomials. In *Proceedings 16th Annual IEEE International Symposions on Foundations of Computer Science*, pages 169–177. Berkeley, 1975.

[2] B. Allen. Arithmetizing uniform NC. *Annals of Pure and Applied Logic*, 53:1–50, 1991.

[3] J.L. Balcazár, J. Diaz, and J. Gabarró. *Structural Complexity I.* Springer-Verlag, 1988.

[4] J.L. Balcazár, J. Diaz, and J. Gabarró. *Structural Complexity II.* Springer-Verlag, 1990.

[5] A. Beckmann. *Separating fragments of bounded arithmetic.* PhD thesis. Universität Münster, 1996.

[6] S. Bloch. *Divide and Conquer in Parallel Complexity and Proof Theory.* PhD thesis. U.C. San Diego, 1993.

[7] S. Bloch. On parallel hierarchies and R_k^i. In D. Leivant, editor. *Logic and Computational Complexity*, LNCS 960, pages 52–76. Springer-Verlag, 1995.

[8] S. Bloch. On parallel hierarchies and R_k^i. Submitted Annals of Pure and Applied Logic., 1996.

[9] E. Börger. *Computability, Complexity, Logic.* North-Holland, 1989.

[10] S. R. Buss and L. Hay. On truth-table reducibility to SAT. *Information and Computation*, 91(1):86–102, March 1991.

[11] S. R. Buss and A. Ignjatović. Unprovability of consistency statements in fragments of bounded arithmetic. CMU-PHIL 43, Carnegie Mellon University, November 1993.

[12] S. R. Buss and J. Krajíček. An application of Boolean complexity to separation problems in bounded arithmetic. *Proceedings of the London Mathematical Society*, 69(3):1-21, 1994.

[13] S.R. Buss. *Bounded Arithmetic.* Bibliopolis. Napoli. 1986.

[14] S.R. Buss. Axiomatizations and conservation results for fragments of bounded arithmetic. *Contemporary Mathematics.* 106:57–83. 1990.

[15] S.R. Buss. Relating the bounded arithmetic and polynomial time hierarchies. *Annals of Pure and Applied Logic.* 75:67–77, 1995.

[16] S.R. Buss. J. Krajíček, and G. Takeuti. Provably total functions in bounded arithmetic theories R^i_3, U^i_2, and V^i_2. In P. Clote and J. Krajíček, editors. *Arithmetic, Proof Theory and Computational Complexity,* pages 116–161. Oxford Science Publications. 1993.

[17] R. Chang and J. Kadin. The boolean hierarchy and the polynomial hierarchy: a closer connection. In *Proceedings Fifth Annual Structures in Complexity Conference.* pages 169–178, 1990.

[18] P. Clote. On polynomial size Frege proofs of certain combinatorial principles. In P. Clote and J. Krajíček, editors. *Arithmetic, Proof Theory and Computational Complexity.* pages 162–193. Oxford Science Publications. 1993.

[19] P. Clote and G. Takeuti. Bounded arithmetic for NC. Alogtime. L and NL. *Annals of Pure and Applied Logic.* 56:73–177. 1992.

[20] P. Clote and G. Takeuti. First order bounded arithmetic and small boolean circuit complexity classes. In P. Clote and J. Remmel. editors. *Feasible Mathematics II,* pages 154–218. Birkhauser. 1995.

[21] S. A. Cook. The complexity of theorem proving procedures. In *Proceedings of the 3-th ACM Symposium on the Theory of Computation.* pages 151–158. ACM Press. 1971.

[22] H.B. Enderton. *A Mathematical Introduction to Logic.* Academic Press. 1972.

[23] M. R. Garey and D. S. Johnson. *Computers and Intractibility: A Guide to the theory of NP-completeness.* W.H. Freeman and Company. 1979.

[24] P. Hájek and P. Pudlák. *Metamathematics of First-Order Arithmetics.* Springer-Verlag. 1993.

[25] J. Hastad. Almost optimal lower bounds for small depth circuits. In *Proceedings of the Eighteenth Annual ACM Symposium on theory of Computing.* pages 6 20. 1987.

[26] J. Johannsen. On the weakness of sharply bounded polynomial induction. In *Proceedings of Gödel 1993.* pages 223–230. Springer-Verlag. 1993.

[27] J. Johannsen. A note on sharply bounded arithmetic. *Archive for Mathematical Logic.* 33:159–165. 1994.

[28] J. Johannsen. A bounded arithmetic theory for constant depth threshold circuits. In *Proceedings of Gödel 1996*, pages 224–234. Springer LNL 6, 1996.

[29] D. S. Johnson, C. M. Papadimitriou, and M. Yannakakis. How easy is local search? *Journal of Computer and System Science*, pages 79–100, 1988.

[30] J. Kadin. The polynomial time hierarchy collapses if the boolean hierarchy collapses. *SIAM Journal on Computing*, 17(6):1263–1282, August 1988.

[31] R. Kaye. *Models of Peano Arithmetic*. Oxford Science Publications, 1991.

[32] R. Kaye. Open induction, Tennbaum phenomena, and complexity theory. In P. Clote and J. Krajíček, editors, *Arithmetic, Proof Theory and Computational Complexity*, pages 222–237. Oxford Science Publications, 1993.

[33] J. Krajíček. Fragments of bounded arithmetic and bounded query classes. *Transactions of the American Mathematical Society*, 338(2):587–598, August 1993.

[34] J. Krajíček. *Bounded Arithmetic, Propositional Logic and Complexity Theory*. Cambridge University Press, 1995.

[35] J. Krajíček, P. Pudlák, and G. Takeuti. Bounded arithmetic and the polynomial hierarchy. *Annals of Pure and Applied Logic*, 42:143–155, 1991.

[36] P. Odifreddi. *Classical recursion theory : the theory of functions and sets of natural numbers*. North-Holland, 1989.

[37] C. M. Papadimitriou. *Computational Complexity*. Addison-Wesley, 1994.

[38] C. M. Papadimitriou and M. Yannakakis. Optimization,approxiamtion and complexity classes. In *Proceedings of the 20th Annual ACM Symposium on theory of Computing*, pages 229–234, 1988.

[39] R. Parikh. Existence and feasibility in arithmetic. *Journal of Symbolic Logic*, 36:494–508, 1971.

[40] J. Paris, A. Wilkie, and A. Woods. Provability of the pigeonhole principle and the existence of infinitely many primes. *Journal of Symbolic Logic*, 53:1235–1244, 1988.

[41] A.A. Razborov. Bounded arithmetic and lower bounds in Boolean complexity. In P. Clote and J. Remmel, editors, *Feasible Mathematics II*, pages 344–386. Birkhauser, 1995.

[42] A.A. Razborov. Lower bounds for propositional proofs and independence results in bounded arithmetic. In *Proceedings of 20th International Symposium on the Mathematical Foundations of Computer Science*, page 105. Springer-Verlag, 1995.

[43] A.A. Razborov and S. Rudich. Natural proofs. In *Proceedings of the 26th Annual ACM Symposium on theory of Computing*, pages 204–213. ACM Press, 1994.

[44] W.L. Ruzzo. On uniform circuit complexity. *Journal of Compute and System Science*, 22:365–383, 1981.

[45] A. Selman. Much ado about functions. In S. Homer and J.-Y. Cai, editors, *11th Annual IEEE Conference on Computational Complexity*, pages 198–212. IEEE Comput. Soc. Press, 1996.

[46] R. I. Soare. *Recursively enumerable sets and degrees : a study of computable functions and computably generated sets*. Springer-Verlag, 1987.

[47] L. J. Stockmeyer. The polynomial hierarchy. *Theoretical Computer Science*, 3:1–22, 1976.

[48] G. Takeuti. *Proof theory*. North-Holland, 1975.

[49] G. Takeuti. *RSUV* isomorphisms. In P. Clote and J. Krajíček, editors, *Arithmetic, Proof Theory and Computational Complexity*, pages 364–386. Oxford Science Publications, 1993.

[50] D. van Dalen. *Logic and Structure. Third Edition*. Springer-Verlag, 1991.

[51] G.M. Wilmers. Bounded existential induction. *Journal of Symbolic Logic*, 50:72–90, 1985.

[52] D. Zambella. Notes on polynomially bounded arithmetic. *Journal of Symbolic Logic*, 61:942–966, 1996.