# Structure and Definability in General Bounded Arithmetic Theories

Chris Pollett

*Department of Mathematics and Computer Science, Clark University, Worcester, MA 01610 cpollett@aleph0.clarku.edu*

The bounded arithmetic theories $R^i_2$, $S^i_2$, and $T^i_2$ are closely connected with complexity theory. This paper is motivated by the questions: what are the $\Sigma^b_{i+1}$-definable multifunctions of $R^i_2$? and when is one theory conservative over another? To answer these questions we consider theories $\hat{R}^i_2$, $\hat{S}^i_2$, and $\hat{T}^i_2$ where induction is restricted to prenex formulas. We also define $\hat{T}^{i,\tau}_2$ which has induction up to the 0 or 1-ary $L_2$-terms in the set $\tau$. We show $\hat{S}^i_2 = S^i_2$ and $\hat{T}^i_2 = T^i_2$ and for $i > 1$, $\hat{R}^i_2 \preceq_{B(\hat{\Sigma}^b_i)} R^i_2$. We show that the $\hat{\Sigma}^b_{i+1}$-multifunctions of $\hat{T}^{i,\tau}_2$ are $FP^{\Sigma^p_i}(wit, |\tau|)$ and that those of $\hat{R}^i_2$ are $FP^{\Sigma^p_i}(wit, \log\log)$. For $\hat{\Sigma}^b_{i+k+2}$-definability we get $FP^{\Sigma^p_{i+k+1}}(wit, 1)$ for all these theories. Write $2^{\dot{\tau}}$ for the set of terms $2^{\min(\ell(x),|t(x)|)}$ where $\ell$ is a finite product of terms in $\tau$ and $t \in L_2$. We prove $\hat{T}^{i,2^{\dot{\tau}}}_2 \preceq_{B(\hat{\Sigma}^b_{i+1})} \hat{T}^{i+1,\tau}_2$ and we show $\hat{T}^{i,\tau}_2 \vdash \hat{\Delta}^b_{i+1}\text{-}IND^\tau$ provided $\tau \subseteq O_2(|id|)$. This gives a proof theoretic proof that $S^i_2 \vdash \Delta^b_{i+1}\text{-}LIND$ and $\hat{R}^i_2 \vdash \hat{\Delta}^b_{i+1}\text{-}LLIND$ solving an open problem. For $\tau \subseteq O_2(|id|)$, we define $\hat{C}^{i,\tau}_2$ using weak replacement axioms and show $\hat{T}^{i,\tau}_2 \preceq_{B(\hat{\Sigma}^b_{i+1})} \hat{C}^{i,\tau}_2$. 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 $\tau'$ has an unbounded term then $PH = B(\Sigma^p_{i+2})$. We separate $P^{\Sigma^p_i(A)}(\{||\ell||\})$ from $P^{\Sigma^p_i(A)}(\{||\ell||^2\})$ for behaved $\ell$ and deduce theory separations. We lastly introduce a notion of a model separating two theories and derive some consequences.

*Key words:* bounded arithmetic, complexity theory, multivalued functions, conservation results, oracle separations
*1991 MSC:* 03F30, 68Q15

## 1 Introduction

Three families of bounded arithmetic theories, $R^i_2$ , $S^i_2$, and $T^i_2$, were developed in Buss [7], Allen [1],Clote-Takeuti [11], and Takeuti [28]. These theories

have been studied because of their close connection to computational complexity. It is known that the $\Sigma^b_i$-definable functions of $S^i_2$ are $FP^{\Sigma^p_{i-1}}$, those functions computable in polynomial time with access to a $\Sigma^p_{i-1}$-oracle [7]. The $\Sigma^b_1$-definable functions of $R^1_2$ are the circuit class $FNC$. It is also known for $i > 1$ that $S^i_2$ is $\Sigma^b_i$-conservative over $T^{i-1}_2$. Krajíček [17] shows that the $\Sigma^b_i$-definable multifunctions of $S^{i-1}_2$ are $FP^{\Sigma^p_{i-1}}(wit, \log)$, those multifunctions computed by Turing machines running in polynomial time with only logarithmically many queries to a $\Sigma^p_{i-1}$-oracle such that if the oracle answers '1' to a query it also supplies a poly-size witness string.

These results reveal a trend that was the original motivation for this paper. $T^{i-1}_2$, $S^{i-1}_2$ and $R^{i-1}_2$ are axiomatized with respectively the usual, log length, and log log length induction for $\Sigma^b_{i-1}$-formulas and, in going from $\Sigma^b_i$-definability in $T^{i-1}_2$ versus $S^{i-1}_2$ we go from poly to log many queries to a $\Sigma^p_{i-1}$-oracle. One would guess that the $\Sigma^b_i$-definable multifunctions of $R^{i-1}_2$ are $FP^{\Sigma^p_{i-1}}(wit, \log\log)$. However, the usual witnessing argument fails for the $(\forall : right)$ case. Nevertheless, if one restricts the inductions in the definition of $R^i_2$ to prenex formulas then the $\Sigma^b_i$-definable multifunctions are $FP^{\Sigma^p_{i-1}}(wit, \log\log)$. So the natural question becomes is prenex $R^i_2$, which we call $\hat{R}^i_2$, equal to $R^i_2$? As $R^1_2$ is related to $FNC$ this question seems very relevant. Although one can show that the prenex versions of $T^i_2$ and $S^i_2$ are equal to their non-prenex counterparts it seems difficult to establish this for $R^i_2$. This is because the normal recursive doubling trick used to show that $R^i_2$ can prove quantifier replacement axioms cannot easily be done in $\hat{R}^i_2$. We show in this paper, however, that $R^i_2$ is $B(\hat{\Sigma}^b_i)$-conservative over $\hat{R}^i_2$ where $B$ stands for Boolean combinations and $\hat{\Sigma}^b_i$ stands for prenex $\Sigma^b_i$.

Another motivating question was whether $R^i_2$ is $\Sigma^b_i$-conservative over $S^{i-1}_2$. This is a reasonable conjecture since $S^i_2$ is $\Sigma^b_i$-conservative over $T^{i-1}_2$ from Buss [8]. Buss, Krajíček, and Takeuti [10] were not able to solve this problem but did show that if the theories had a slightly faster growth rate function $\#_3$ in the language then the result held. This paper takes up this question in the prenex setting and gives a general condition for one bounded arithmetic theory to be conservative over another. We consider theories $\hat{T}^{i,\tau}_2$ where $\tau$ is a set of 1-ary terms up to which $\hat{T}^{i,\tau}_2$ has $\hat{\Sigma}^b_i$ induction. Let $2^{\dot{\tau}}$ denote the set of terms $2^{\min(\ell(x),|x|)}$ where $\ell$ is a finite product of terms in $\tau$. We prove $\hat{T}^{i+1,\tau}_2$ is $B(\hat{\Sigma}^b_i)$-conservative over $\hat{T}^{i-1,2^{\dot{\tau}}}_2$ provided $\tau \subseteq O_2(|id|)$. Roughly, $O_2(|id|)$ is the set of 0 and 1-ary terms $\ell$ such that for any $x$ our base theory can prove $\ell(x) \leq |t(x)|$ where $t \in L_2$. Since the prenex versions of $T^i_2$ and $S^i_2$ are the same as the non-prenex versions this result can be used to show $S^i_2$ is $B(\hat{\Sigma}^b_i)$-conservative over $T^{i-1}_2$ a slight strengthening of Buss [8]. For $R^i_2$ using a modification of this result we get $R^i_2$ is $B(\hat{\Sigma}^b_i)$-conservative over $\hat{R}^i_2$. Then using the $\tau = \{||id||\}$ case of our result we get $\hat{R}^i_2$ is $B(\hat{\Sigma}^b_i)$-conservative over $\hat{T}^{i-1,\{2^{p(||id||)}\}}_2$. Here $id(a) = a$ is the identity function and $\{2^{p(||id||)}\}$ stands for terms of the form

$2^{p(||id||)}$ where $p$ is some polynomial. Let $|id|_0 := id$ and $|id|_m := ||id|_{m-1}|$. In general, our conservation result can be used to determine the $\hat{\Sigma}^b_{i-j}$-definable multifunctions of $\hat{T}^{i,\{|id|_m\}}_2$ provided $m \geq i > j \geq 0$. As an example one can use our conservation result to show $\hat{T}^{i,\{|||id|||\}}_2 \succeq_{B(\hat{\Sigma}^b_i)} \hat{T}^{i-1,\{2^{p(|||id|||)}\}}_2 \succeq_{B(\hat{\Sigma}^b_{i-1})} \hat{T}^{i-2,\{2^{2^{p(|||id|||)}}\}}_2$ and then by a general argument we can characterise the latter's $\hat{\Sigma}^b_{i-1}$-definable multifunctions.

One reason to study bounded arithmetic as opposed to just structural complexity theory is to try to show independence of questions like $P = NP$? from some sizeable portion of mathematics. It is known that if the bounded arithmetic hierarchy $S_2 = \cup_i S^i_2$ collapses, then so does the polynomial hierarchy [19,9]. However, it is unknown what does the failure of the bounded arithmetic hierarchy to collapse imply about the polynomial hierarchy. At our present state of knowledge, the noncollapse of the bounded arithmetic hierarchy could imply the collapse of the polynomial hierarchy question is independent of $S_2$. The theory $S_2$ can formulate facts about the density of primes, variants of Ramsey's theorem, and can formalise many arguments used to show circuit lower bounds [25,22,24]. So this would be a non-trivial independence result. Nevertheless, it should be easier to separate bounded arithmetic theories than to separate the polynomial hierarchy. This is because bounded arithmetic theories have a good deal more structure than mere complexity classes. For a bounded arithmetic theory $T$ not only can one examine its $\Sigma^b_i$-definability functions, or $\Delta^b_i$-predicates for various $i$ but also examine definability of subclasses which restrict how these functions are defined or how these proofs of $\Delta^b_i$ness are carried out. In fact, we give an example in Remark 78 of two bounded arithmetic theories with the same $\hat{\Sigma}^b_j$-definable multifunctions for all $j$ yet are not known to be equal. This is because the same multifunctions can be defined in each theory using different formulas and at least one of the two theories cannot prove these formulas are equivalent. Thus, it is interesting to study more restrictive classes of definability in that it might inspire separation techniques.

Since a distinction apparently arises at the prenex versus non-prenex level, this seems like a natural setting for such an investigation. We show in this paper that every $\hat{\Sigma}^b_i$-definable multifunction of $\hat{T}^{i,\tau}_2$ is provably equivalent to a multifunction of a particular syntactic form. Similarly, every $\hat{\Delta}^b_i$-predicate in $\hat{T}^{i,\tau}_2$ is provably equivalent to a formula of a particular syntactic form. As an application of this we give a proof theoretic proof that $S^i_2$ admits $\Delta^b_{i+1}$-induction. This solves open question (10) of Clote and Krajíček [12]. Further restricting this syntactic characterisation might be helpful in the development of separation results. The last section of this paper gives some oracle separations based on our syntactic characterisations. We show that the complexity characterisation of the $\hat{\Delta}^b_{i+2}$-predicates of $T^i_2$ and $\hat{T}^{i+1,\tau}_2$ where $\tau$ has at least one unbounded term will not yield separation results for these theories unless

the polynomial hierarchy is infinite. It should be mentioned that showing the noncollapse of the bounded arithmetic hierarchy is by no means the only way to obtain independence results in bounded arithmetic. Some independence results have already been obtained using interpolation methods. Perhaps the most cleanly stated of these is Widgersen's corollary to Razborov [26]: $S^2_2(\alpha)$ does not prove the existence of pseudo-random number generators.

Although it is probably difficult to separate the bounded arithmetic hierarchy, one might ask whether there is a relativised world where $S_2 \supsetneq S^i_2$ for all $i$ yet the polynomial hierarchy collapses? We say *a model $M$ separates the theories $A$ and $B$ with respect to $\hat{\Delta}^b_i(\alpha)$-predicates* if: (a) $M$ models $A$ and $B$; (b) the $\hat{\Delta}^b_i(\alpha)$-predicates of $A$ are $\Psi_A$ and those of $B$ are $\Psi_B$; (c) $M \models \Psi_A \neq \Psi_B$. We conjecture there is a single model $M$ separating $S^i_2(\alpha)$ for all $i$ with respect to $\hat{\Delta}^b_2(\alpha)$-consequences yet $M \models PH(\alpha) = \Sigma^p_2(\alpha)$. Krajíček [17]'s oracle $X$ shows $(\mathbb{N}, X)$ where $X$ interprets $\alpha$ separates $S^i_2(\alpha)$ from $T^i_2(\alpha)$ for all $i$ and $(\mathbb{N}, X) \models PH(\alpha) \uparrow$. Improved lower bound results for constant-depth Frege systems might establish our conjecture. At the end of this paper, we exhibit an oracle $X$ such that for all $i$ there is a term $\ell$ for which $(\mathbb{N}, X)$ separates $\hat{T}^{i,\{\ell\}}_2(\alpha)$ from $\hat{T}^{i,\{|\ell|\}}_2(\alpha)$ for $\hat{\Delta}^b_2(\alpha)$-predicates yet $(\mathbb{N}, X) \models PH(\alpha) = \Delta^p_2(\alpha)$.

We now outline the format of this paper. In Section 2, we introduce various arithmetic theories. Our base theory is $EBASIC$ which extends $BASIC$ from Buss [7] with axioms for $MSP$ and $\dot{-}$ as well as three open axioms that allow a form of pairing. We define $\hat{T}^{i,\tau}_2$ and also the classical bounded arithmetic theories $R^i_2$, $S^i_2$, $T^i_2$. We discuss some useful properties a set $\tau$ of 1-ary terms can have, then try to justify the three open axioms we selected for $EBASIC$ by showing $R^0_2$ can prove them. Next we give results about the quantifier replacement axioms are available in our theories. In Section 3, we show that for $i \geq 1$ the $\hat{\Sigma}^b_{i+1}$-definable multifunctions of $\hat{T}^{i,\tau}_2$ are $FP^{\Sigma^p_i}(wit, |\tau|)$. We show that $\hat{T}^{i,2^{\dot{\tau}}}_2 \preceq_{\hat{\Sigma}^b_{i+1}} \hat{T}^{i+1,\tau}_2$ provided $\tau \subseteq O_2(|id|)$. We then give applications of these results to $EBASIC$ and $\hat{R}^i_2$. In Section 5 we characterise the $\hat{\Sigma}^b_{i+k}$-definable multifunctions of $\hat{T}^{i,\tau}_2$ for $k > 1$ as $FP^{\Sigma^p_{i+k-1}}(wit, 1)$. We show that $\hat{T}^{i,2^{\dot{\tau}}}_k \preceq_{B(\hat{\Sigma}^b_{i+1})} \hat{T}^{i+1,\tau}_k$ provided $\tau \subseteq O_2(|id|)$. This implies $T^i_2 \preceq_{B(\hat{\Sigma}^b_{i+1})} S^{i+1}_2$. We then show that $\hat{T}^{i,\tau}_2$ proves $\hat{\Delta}^b_{i+1}$-$IND^\tau$ and that $\hat{T}^{i,2^{\dot{\tau}}}_2$ proves $\hat{\Delta}^b_{i+1}$-$IND^{2^{\dot{\tau}}}$ provided $\tau \subseteq O_2(|id|)$. In Section 6 we develop $\hat{C}^{i,\tau}_2$ defined as $EBASIC$+*open*-$IND^\tau$+$\hat{\Sigma}^b_i$-$REPL^\tau$. We show that $\hat{T}^{i,\tau}_2 \preceq_{B(\hat{\Sigma}^b_{i+1})} \hat{C}^{i,\tau}_2$ provided $\tau \subseteq O_2(|id|)$. We also show for $i \geq 1$ that $\hat{R}^{i+1}_2 \preceq_{B(\hat{\Sigma}^b_{i+1})} R^{i+1}_2$. In general, we show for $i \geq 1$ that $\hat{T}^{i+1,||\tau||}_2 \preceq_{B(\hat{\Sigma}^b_{i+1})} \hat{T}^{i+1,||\tau||}_2 + \hat{\Pi}^b_i$-$REPL^{|\tau|}$. At the end of Section 6 we give some tables summarising the results proven to this point. The last section shows some collapse and oracle separations 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 $\tau$ contains an unbounded iterm then $PH = B(\Sigma^p_{i+2})$. These results can be viewed

as showing that the property of being $\hat{\Delta}^b_{i+2}$ is not a powerful enough notion to separate theories with even very weak $\hat{\Sigma}^b_{i+1}$ induction from $T^i_2$. We then construct an oracle $X$ which separates $P^{\Sigma^p_i(X)}(\{||\ell||\})$ from $P^{\Sigma^p_i(X)}(\{||\ell||^2\})$ where $\ell$ is a nondecreasing, unbounded iterm. Separations for theories with an undefined predicate symbol are then derived. Lastly, the notion of models separating theories is discussed.

## 2 Preliminaries

The language of bounded arithmetic, $L_2$, contains the non-logical symbols: 0, $S$, $+$, $\cdot$, $\leq$, $\dot{-}$, $\lfloor \frac{1}{2}x \rfloor$, $|x|$, $MSP(x,i)$ and $\#$. 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 is greater than zero and zero otherwise, $\lfloor \frac{1}{2}x \rfloor$ is $x$ divided by 2 rounded down, and $|x|$ is $\lceil \log_2(x+1) \rceil$, that is, the length of $x$ in binary notation. $MSP(x,i)$ stands for 'most significant part' and is intended to mean $\lfloor x/2^i \rfloor$. 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 numeral 2 in $S^i_2$ denotes the presence of $\#_2$ in the language; a 3 would indicate the presence of $\#_2$ and $\#_3$, etc. $L_k$ is the language including $\#_j$ for $2 \leq j \leq k$. The exponential function is not provably total in bounded arithmetic so we need the function $\#$ to do sequence coding.

$BASIC$ consists of all substitution instances of a finite set of quantifier free axioms for the non-logical symbols of $L_2$. These axioms are listed in Buss [7] with the exception of the axioms for $MSP$ and $\dot{-}$ which are listed in Takeuti [28]. For $k \geq 2$, $BASIC_k$ is $BASIC$ plus the additional axioms $|x\#_j y| = |x|\#_{j-1}|y|$ where $2 < j \leq k$.

We enlarge the syntax of first-order logic 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 that of $(\exists x \leq t)$ is $(\exists x)(x \leq t \wedge \cdots)$. A formula is *bounded* if all its quantifiers are bounded. A quantifier of the form $(\forall x \leq |t|)$ or of the form $(\exists x \leq |t|)$ 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.

We define the bounded arithmetic hierarchy as follows: $\Sigma^b_0 = \Pi^b_0$ is the class of all sharply bounded formulas. $\Sigma^b_i$ is the least class containing $\Pi^b_{i-1}$, closed under conjunction, disjunction, sharply bounded universal quantifiers, and bounded existential quantifiers. Similarly, $\Pi^b_i$ is the least class containing $\Sigma^b_{i-1}$, 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 $\Sigma^b_i$-formulas describe

exactly predicates in $\Sigma_i^p$. Similarly, $\Pi_i^b$-formulas correspond to $\Pi_i^p$-predicates. This correspondence is proven in Buss [7].

We define the prenex bounded arithmetic hierarchy as follows: $\hat{\Sigma}_0^b$ are those formulas of the form $(\exists x \leq |s|)\phi$ and $\hat{\Pi}_0^b$ are those formulas of the form $(\forall x \leq |s|)\phi$ where $\phi$ is an open formula. $\hat{\Sigma}_i^b$ are those formulas of the form $(\exists x \leq t)\phi$ where $\phi \in \hat{\Pi}_{i-1}^b$-formula. $\hat{\Pi}_i^b$ are those formulas of the form $(\forall x \leq t)\phi$ where $\phi \in \hat{\Sigma}_{i-1}^b$. For $i \geq 1$, the sets described by $\hat{\Sigma}_i^b$-formulas and $\Sigma_i^b$-formulas are equivalent. In Section 2, we show various bounded arithmetic theories prove this equivalence. Similarly, sets described by $\hat{\Pi}_i^b$-formulas and $\Pi_i^b$-formulas are equivalent. We call any formula in $\bigcup_i \hat{\Sigma}_i^b \cup \hat{\Pi}_i^b$ a *prenex formula.*

The classes of $L_k$-formulas $\Sigma_{i,k}^b$ , $\Pi_{i,k}^b$ , $\hat{\Sigma}_{i,k}^b$ , and $\hat{\Pi}_{i,k}^b$ mutatis mutandis.

### *2.1 Defining functions and frequently used $L_2$-terms*

Let $\Psi$ be a set of formulas. A theory $T$ can $\Psi$-*define a multifunction* $f(x)$, if there is a $\Psi$-formula $A_f(x,y)$ such that $T \vdash \forall x \exists y A_f(x,y)$ and $\mathbb{N} \models A_f(x,y) \Leftrightarrow f(x) = y$. If $T$ proves $y$ is unique then we say $T$ $\Psi$-*defines the function* $f$. We will be interested in $\Sigma_i^b$ and $\hat{\Sigma}_i^b$-definability. Our notion of $\Sigma_i^b$-definable multifunction was called *strongly* $\Sigma_i^b$-definable in Buss, Krajíček, and Takeuti [10]. A predicate is $\Delta_i^b$ with respect to $T$ if it is provably equivalent in $T$ to both a $\Sigma_i^b$-formula and a $\Pi_i^b$-formula. A predicate is $\hat{\Delta}_i^b$ with respect to $T$ if it is provably equivalent to both a $\hat{\Sigma}_i^b$-formula and a $\hat{\Pi}_i^b$-formula. By adding a trivial universal quantifier to the outside of a $\hat{\Sigma}_i^b$-formula one can show that a given $\hat{\Sigma}_i^b$-formula is logically equivalent to a $\hat{\Pi}_{i+1}^b$-formula, and by adding a trivial sharply bounded formula in front of the matrix of a $\hat{\Sigma}_i^b$-formula one shows the same $\hat{\Sigma}_i^b$-formula is equivalent to a $\hat{\Sigma}_{i+1}^b$-formula. i.e., the $\hat{\Sigma}_0^b$-formula $(\exists x \leq |y|)(x = z \vee \neg(x = z))$ is equivalent to the $\hat{\Sigma}_1^b$-formula $(\exists x \leq |y|)(\forall w \leq |y|)(x = z \vee \neg(x = z))$. Hence, any $\hat{\Sigma}_i^b$-formula is $\hat{\Delta}_{i+1}^b$ with respect to any theory. Also, any $\hat{\Pi}_i^b$-formula is $\hat{\Delta}_{i+1}^b$ with respect to any theory. Below are some functions $BASIC$ can *open*-define:

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

$$\max(x,y) := cond(K_{\leq}(x,y), y, x)$$

$$\min(x,y) := cond(K_{\leq}(x,y), x, y)$$

Notice all of the above definitions are actually $L_2$-terms. The $k$ and the $n$ in $2^{k\cdot|y|^n}$ are fixed integers. Taking products of terms $2^{k\cdot|s|^n}$ we can construct terms representing $2^{p(|s|)}$ where $p$ is any polynomial. We use the predicate $x < y$ as an abbreviation for $Sx \leq y$. The above definitions are all $L_2$-terms so can be used freely in an $L_2$-formula without increasing its quantifier complexity. It is a theorem of Buss [7] that once we can $\Sigma^b_1$-define a function $f$ in a bounded arithmetic theory we can add the function symbol to the theory without changing the $\Sigma^b_i$ or $\Pi^b_i$-consequences of the theory $i \geq 1$. A similar result holds for adding $\Delta^b_1$-predicate symbols [7]. We will not need this more general result, however.

$\hat{\beta}$ and $\dot{\beta}$ allow some sequence manipulation in our theories. Roughly, $\hat{\beta}(x, |t|, w)$ projects out the $x$th block (starting with a 0th block) of $|t|$ bits from $w$. $\dot{\beta}(x, |t|, s, w)$ returns the minimum of $\hat{\beta}(x, |t|, w)$ and $s$. The term $cond(x, y, z)$ returns $z$ if $x$ is non-zero and $y$ otherwise.

**Remark 1** *For this paper, $A \supset B$ is as an abbreviation for $\neg A \vee B$. In transforming formulas into prenex ones we use the fact that $\neg\forall x\neg$ and $\exists x$ are logically equivalent. This allows us to push negations inward into a formula.*

### *2.2 Bounded arithmetic theories*

This section introduces a variety of bounded arithmetic theories. First, we need some definitions.

**Definition 2** *Given $t \in L_k$ we define a monotonic term $t^*$ called the* dominator for $t$ *by induction on the complexity of $t$. $t = t^*$ if $t$ is constant or a variable. 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 $f^*$.*

**Definition 3** *A set $\tau$ of* 0- *and* 1*-ary terms in $L_k$ is called a set of* $k$-iterms *($k$-induction terms). We call* 2-iterms *just* iterms. *If $\ell_1$ and $\ell_2$ are $k$-iterms then $\ell_2$* k-surpasses *$\ell_1$, if $BASIC_k \vdash (\forall x)(\ell_1(x) < \ell_2(t(x)))$ where $t \in L_k$. When $k$ is understood we just write surpass for $k$-surpass. We use the suggestive notation $O_k(\ell)$ to denote the class of all $k$-iterms surpassed by $\ell$.*

*Let $\tau$ be a set of iterms. The $\Psi$-$IND^\tau$ axioms are the axioms $IND^\ell_\alpha$:*

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

*where* $\alpha \in \Psi$ *and* $\ell \in \tau$. *We write* $IND^{\tau}_{\alpha}$ *for the set of axioms* $IND^{\ell}_{\alpha}$ *for* $\ell \in \tau$.

$\Psi$-$REPL^{\tau}$ *where* $\tau \subseteq O_2(|id|)$ *are the axioms* $REPL^{\ell}_{\alpha,s,t}$:

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

*where* $\alpha \in \Psi$, $\ell \in \tau$, *and* $s,t \in L_k$. *We write* $REPL^{\tau}_{\alpha}$ *for the set of axioms* $REPL^{\ell}_{\alpha,s,t}$ *for* $\ell \in \tau$.

As an example, let $id(a) = a$. Then $\{id\}$ is a set of iterms and $\Psi$-$IND^{\{id\}}$ is the usual induction for $\Psi$-formulas. Other common sets of iterms are $\{|id|\}$, $\{||id||\}$ or $\{|id|_m\}$ where $|id|_0 = id$ and $|id|_m = ||id|_{m-1}|$. We often write $IND$, $LIND$ and $LLIND$ instead of $IND^{\{id\}}$, $IND^{\{|id|\}}$, and $IND^{\{||id||\}}$. The set $\{|id|_m\}$ for fixed $m$ is just a singleton set; however, we will consider sets of iterms such as $\{2^{p(||id||)}\}$ or $\{2^{2^{p(|||id|||)}}\}$ where $p$ is any polynomial. $\Psi$-$REPL^{\{|id|\}}$ will be denoted $\Psi$-$REPL$. $\hat{\Sigma}^b_i$-$REPL$ is useful for converting $\Sigma^b_i$-formulas into $\hat{\Sigma}^b_i$-formulas. Notice we write $|\tau|$ to denote terms of the form $|\ell|$ for $\ell \in \tau$. Let $cl_k$ denote the closed iterms in $L_k$. We write $cl$ for $cl_2$. So the $\hat{\Sigma}^b_i$-$IND^{cl}$ axioms are provable in $BASIC$. As another example of choices of $\tau$ consider $\tau$ defined as $\{1\#(MSP(x, \lfloor \frac{1}{2}|x| \rfloor)\}$. This grows approximately as $2^{|\sqrt{x}|}$ which is a potentially interesting growth rate between $id$ and $|id|$. Iterms need not be monotonic. Below we show this does not have pathological consequences.

**Theorem 4** *Let* $\Psi$ *be closed under term substitution. Let* $\neg\Psi$ *denote negations of formulas in* $\Psi$. *Then* $BASIC$+$\Psi$-$IND^{\tau}$ *proves* $\neg\Psi$-$IND^{\tau}$.

**PROOF.** Both directions are the same. Let $A \in \neg\Psi$. Then $\neg A(y \dot{-} x)$ is equivalent to a $\Psi$-formula and using $\Psi$-$IND^{\tau}$ on this formula gives us $IND^{\tau}_A$. $\square$

**Definition 5** $(i \geq 0)$ $T^i_2$, $S^i_2$ *and* $R^i_2$ *are respectively the theories* $BASIC$+$\Sigma^b_i$-$IND$, $BASIC$+$\Sigma^b_i$-$LIND$, *and* $BASIC$+$\Sigma^b_i$-$LLIND$.

$\hat{T}^i_2$, $\hat{S}^i_2$, *and* $\hat{R}^i_2$ *are defined similarly except with* $\hat{\Sigma}^b_i$ *induction axioms. We define* $LIOpen$ *to be* $BASIC$+*open-*$LIND$.

**Theorem 6** $(i \geq 0)$ $R^i_2 \subseteq S^i_2 \subseteq T^i_2$ *and* $\hat{R}^i_2 \subseteq \hat{S}^i_2 \subseteq \hat{T}^i_2$.

**PROOF.** Both statements are proved similarly. 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 $(\forall x)A(|x|)$ implies $(\forall x)A(||x||)$. $\square$

In addition to the above theories, we consider the following theories in later sections:

**Definition 7** *$EBASIC = EBASIC_2$ is the theory obtained from $BASIC$ by adding the following three axioms:*

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

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

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

*$EBASIC_k$ is the theory obtained by adding the above three axioms to $BASIC_k$.*

**Definition 8** *($i \geq 0$) Let $\tau$ be a set of $k$-iterms. We define $\hat{T}_k^{i,\tau}$ to be*

$$EBASIC_k{+}\hat{\Sigma}^b_{i,k}\text{-}IND^\tau$$

*and $\hat{C}_k^{i,\tau}$ to be $EBASIC_k{+}open\text{-}IND^\tau{+}\hat{\Pi}^b_{i,k}\text{-}REPL^\tau$.*

The $C$ in $\hat{C}_k^{i,\tau}$ is for collection axiom, another name used for the replacement axioms in bounded arithmetic. $\hat{C}_2^{i,\tau}$ appears in Section 4 and is discussed in detail in Section 6. The additional axioms in $EBASIC$ allow a form of pairing in theories where it would be difficult to define. It is not obvious that $R_2^0$ proves the $EBASIC$ axioms and we devote some time to proving this in a later subsection. Next, however, we discuss some properties of iterms.

### *2.3 Properties of iterms*

In this subsection we introduce some properties of iterms. We first give two definitions which will allow us to present our conservation result.

**Definition 9** *Let $\tau$ be a set of iterms. Then the closure of $\tau$ under products, denoted $\dot{\tau}$, is $\cup_i \sigma_i$ where $\sigma_0 = \tau \cup cl$ and*

$$\sigma_{i+1} = \sigma_i \cup \{\ell_1(s(x)) \cdot \ell_2(t(x)) \ \mid \ell_1, \ell_2 \in \sigma_i, s, t \in L_2\}.$$

*We write $(|\dot{\tau}|)$ for the product closure of $|\tau|$.*

**Definition 10** *Let $\tau$ be a set of iterms. We write $2^\tau$ to denote the set of iterms $2^{\min(\ell(x),|t(x)|)}$ where $\ell \in \tau$, $t(x) \in L_2$. We define $2 \uparrow 0(\tau)$ to be $\tau$ and for $i > 0$, $2 \uparrow i(\tau)$ is $2^{2\uparrow i-1(\tau)}$.*

We now present a couple results which will be useful in comparing the relative strength of two theories $\hat{T}_2^{i,\tau}$ and $\hat{T}_2^{i,\tau'}$ in terms of their iterms.

**Theorem 11** *Let $\Psi$ be closed under $(\forall x \leq t)$. If $\ell_1$ and $\ell_2$ are iterms and $\ell_2$* k-surpasses *$\ell_1$, then*

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

**PROOF.** Let $A(a) \in \Psi$. Then $B(b) := (\forall x \leq b)A(x) \in \Psi$. $EBASIC$ proves $A(0)$ implies $B(0)$ and $(\forall x)(A(x) \supset A(Sx))$ implies $(\forall x)(B(x) \supset B(Sx))$. The surpass condition together with $(\forall x)B(\ell_2(x))$ imply $(\forall x)A(\ell_1(x))$. So, $EBASIC{+}IND_B^{\{\ell_2\}}$ implies $IND_A^{\{\ell_1\}}$. $\square$

**Corollary 12** $(i \geq 0)$ *Let $\tau$ and $\tau'$ be sets of k-iterms such that every $\ell \in \tau$ is surpassed by some $\ell' \in \tau'$ then $\hat{T}_k^{i,\tau} \subseteq \hat{T}_k^{i,\tau'}$.*

**PROOF.** We argue in the next subsection that the three axioms added to $EBASIC$ over $BASIC$ allow a form of pairing. Given this, the formulas provably equivalent to $\hat{\Pi}_{i,k}^b$-formulas in $\hat{T}_k^{i,\tau'}$ satisfy the conditions of Theorem 11. As every $\ell \in \tau$ is surpassed by some $\ell' \in \tau'$, $\hat{T}_k^{i,\tau'}$ proves $\hat{\Pi}_{i,k}^b\text{-}IND^\tau$ and, thus, by Theorem 4 it also proves $\hat{\Sigma}_{i,k}^b\text{-}IND^\tau$. $\square$

Corollary 12 shows the power of $\hat{T}_2^{i,\{\ell\}}$ where $\ell$ might not be monotonic since $\hat{T}_2^{i,\{\ell\}}$ is contained in any $\hat{T}_2^{i,\tau}$ which has terms which surpass $\ell$ (for instance, $T_2^i$) and it contains any $\hat{T}_2^{i,\{\ell'\}}$ involving a monotonic $\ell'$ which $\ell$ surpasses.

### *2.4 Pairing in LIOpen*

In this subsection, we show $LIOpen := BASIC{+}open\text{-}LIND$ has a form of pairing. This allows us to increase the class of formulas we know $\hat{R}_2^i$, $\hat{S}_2^i$, and $\hat{T}_2^i$ prove equivalent to $\hat{\Sigma}_i^b$-formulas. This is useful as these theories prove their induction schemes for any formula provably equivalent to a $\hat{\Sigma}_i^b$-formula. We also begin our justification of our choice of $EBASIC$ axioms. For results about $LIOpen$ to be useful for all of $\hat{R}_2^i$, $\hat{S}_2^i$, and $\hat{T}_2^i$ we show that $\hat{R}_2^0 \supseteq LIOpen$.

**Theorem 13** $LIOpen \subseteq \hat{R}_2^0$.

**PROOF.** Let $A(x) \in open$, $B(b) := (\forall x \leq |c|)(A(x) \supset A(\min(x + 2^b, |c|)))$. For simplicity we write $2^b$ for $2^{\min(||c||,b)}$. As $B \in \hat{\Pi}_0^b$, by Theorem 4, $\hat{R}_2^0$ proves $LLIND_B$. $\hat{R}_2^0$ also proves $(\forall x)(A(x) \supset A(Sx))$ implies $B(0)$. Further, $\hat{R}_2^0$ proves $B(b) \supset B(Sb)$ and $B(||c||) \supset (A(0) \supset A(|c|))$. So $\hat{R}_2^0 \vdash (\forall x)(A(x) \supset A(Sx)) \supset (A(0) \supset A(|c|))$. $\square$

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

**Lemma 14** *$LIOpen$ proves $b < 2^{|d|} \supset MSP(a \cdot 2^{|d|} + b, |d|) = a$.*

**PROOF.** Recall the axioms for $MSP$ in $BASIC$ are $MSP(a, 0) = a$ and $MSP(a, i+1) = \lfloor \frac{1}{2} MSP(a, i) \rfloor$. It suffices to prove the following in $LIOpen$

$$a \leq b \supset MSP(a, |d|) \leq MSP(b, |d|) \tag{1}$$

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

$$MSP(a \cdot 2^{|d|}, |d|) = a. \tag{3}$$

To prove (1) consider $A(j) := a \leq b \supset MSP(a, j) \leq MSP(b, j)$. The first axiom for $MSP$ implies $A(0)$. Then $A(j) \supset A(j+1)$ follows from the second axiom. So $LIOpen$ proves $A(|d|) := a \leq b \supset MSP(a, |d|) \leq MSP(b, |d|)$. For (2), let $B(j)$ be the formula

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

Now $B(0)$ follows from the first axiom for $MSP$ and $B(j) \supset B(Sj)$ follows from the second axiom for $MSP$ as well as the axiom for $\lfloor \frac{1}{2} x \rfloor$. Hence, by $LIND_B$, $LIOpen$ proves $B(|d|)$ which implies $MSP(a \cdot 2^{|d|} + 2^{|d|} \dot{-} 1, |d|) = a$.

Finally for (3), let $C(j)$ be the formula $MSP(a \cdot 2^{|d|}, j) = a \cdot 2^{|d| \dot{-} j}$. As with $B(j)$, the theory $LIOpen$ proves $C(|d|)$ and in turn $MSP(a \cdot 2^{|d|}, |d|) = a$. Combining the facts (1), (2), (3) 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 $b < 2^{|d|}$. $\square$

One can generalise the above argument to show:

**Corollary 15**

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

This was the first of the three axioms we added to $BASIC$. The next theorem shows $LIOpen$ has a form of pairing. It also shows $LIOpen$ proves the second new axiom of $EBASIC$.

**Theorem 16** *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 $MSP(LSP(w, Sx \cdot |d|), x \cdot |d|)$. If $a = 0$ the theorem is trivial, so assume $a > 0$. From the axioms for $MSP$ one sees that

*LIOpen* proves $\hat{\beta}(0, |d|, a \cdot 2^{|d|} + b)$ is $LSP(a \cdot 2^{|d|} + b, |d|)$. The definition of $LSP$ implies $LSP(a \cdot 2^{|d|} + b, |d|)$ is

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

As $a > 0$, *LIOpen* proves this is $a \cdot 2^{|d|} + b \dot{-} MSP(a \cdot 2^{|d|} + b, |d|) \cdot 2^{|d|}$. If $b < 2^{|d|}$ then by Lemma 14 *LIOpen* proves this is just $b$. Now consider $\hat{\beta}(1, |d|, a \cdot 2^{|d|} + b)$ by definition this function is

$$MSP(LSP(a \cdot 2^{|d|} + b, 2 \cdot |d|), |d|). \tag{4}$$

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

$$a \cdot 2^{|d|} + b \dot{-} MSP(a \cdot 2^{|d|} + b, 2 \cdot |d|) \cdot 2^{min(|a \cdot 2^{|d|} + b|, 2 \cdot |d|)}. \tag{5}$$

As $a < 2^{|d|}$ 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 an induction as in Lemma 14, *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 (5) is equal to $a \cdot 2^{|d|} + b$. So $\hat{\beta}(1, |d|, a \cdot 2^{|d|} + b)$ which by definition is equation (4) is equal to $a$ by Lemma 14. $\square$

**Lemma 17** *Let* $m = \max(s(a), t(a, s))$ *and let* $t^+ := t(a, \dot{\beta}(0, |m|, s(a), w))$ *where* $s(a), t(a, b) \in L_2$. *Then LIOpen and EBASIC prove:*

*(a)* $(\exists w \leq 2^{2 \cdot |m|}) A(\dot{\beta}(0, |m|, s, w), \dot{\beta}(1, |m|, t^+, w))$
$\Leftrightarrow (\exists x \leq s)(\exists y \leq t) A(x, y)$
*(b)* $(\forall w \leq 2^{2 \cdot |m|}) A(\dot{\beta}(0, |m|, s, w), \dot{\beta}(1, |m|, t^+, w))$
$\Leftrightarrow (\forall x \leq s)(\forall y \leq t) A(x, y)$.

**PROOF.** Both statements are proven in the same way so we only prove the first. 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 16, *LIOpen* proves

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

Existentially quantifying $b \cdot 2^{2\cdot|m|} + a$ then universally quantifying $a$ and $b$, *LIOpen* proves

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

For the other direction *LIOpen* can derive

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

Existentially quantifying the terms $\dot{\beta}(1,|m|,t^+,c)$ and $\dot{\beta}(0,|m|,s,c)$ then universally quantifying $c$, we get

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

□

Lemma 17 enables *EBASIC* to show a bounded formula is equivalent to a formula where blocks of like bounded quantifiers have been collapsed into single bounded quantifiers. The next remark shows how bounded $L_k$-formulas can be prenexified.

**Remark 18** *Let $A(a)$ and $B(y)$ be $L_k$-formulas such that $y$ does not appear in $A$. We recall some useful tautologies*

*(i)* $(\forall y \leq t)(A(a) \wedge B(y)) \Leftrightarrow A(a) \wedge (\forall y \leq t)B(y)$
*(ii)* $(\exists y \leq t)(A(a) \wedge B(y)) \Leftrightarrow A(a) \wedge (\exists y \leq t)B(y)$
*(iii)* $(\forall y \leq t)(A(a) \vee B(y)) \Leftrightarrow A(a) \vee (\forall y \leq t)B(y)$
*(iv)* $(\exists y \leq t)(A(a) \vee B(y)) \Leftrightarrow A(a) \vee (\exists y \leq t)B(y)$.

We therefore have induction in $\hat{R}^i_2$, $\hat{S}^i_2$ and $\hat{T}^i_2$ for any formula equivalent to a $\hat{\Sigma}^b_i$-formula using Lemma 17 and Remark 18.

### *2.5 Replacement axioms available in prenex theories*

In this subsection we show the class of provably $\hat{\Sigma}^b_i$-formulas in $\hat{T}^{i,\tau}_2$ is closed under a form of sharply bounded quantification. We first need a next technical lemma which shows *LIOpen* proves the third axiom of *EBASIC*.

**Lemma 19** *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 that $\hat{\beta}(i, |a|, w) = \hat{\beta}(i, |a|, LSP(w, k))$. 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

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

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 $MSP(LSP(w, Si \cdot |a|), Si \cdot |a|) = 0$. $\Box$

**Theorem 20** ($i \geq 1$) *$\hat{S}^i_2$ proves $\hat{\Pi}^b_{i-1}$-REPL, $\hat{R}^i_2$ proves $\hat{\Pi}^b_{i-1}$-$REPL^{\{||id||\}}$, and EBASIC proves $\hat{\Pi}^b_{i-1}$-$REPL^{\{cl\}}$. In general, $\hat{T}^{i,\tau}_2$ proves $\hat{\Pi}^b_{i-1}$-$REPL^{\{\tau\}}$ provided $\tau \subseteq O_2(|id|)$.*

**PROOF.** This proof is essentially the same as the proof that was used in Buss [7] to show the theory $S^i_2$ has $\Sigma^b_i$-*REPL*. $\Box$

**Remark 21** *Having replacement for $\hat{\Pi}^b_{i-1}$-formulas implies replacement for both $\hat{\Pi}^b_{i-2}$ and $\hat{\Sigma}^b_{i-2}$-formulas, since adding dummy quantifiers to formulas in the latter two classes makes them into $\hat{\Pi}^b_{i-1}$-formulas. This quantifier padding also shows if a theory $\hat{\Sigma}^b_i$-defines a function it also $\hat{\Sigma}^b_{i+k}$-defines that function.*

One can improve Theorem 20 for $\hat{R}^i_2$ in the following way.

**Theorem 22** ($i \geq 0$) *Let $\tau$ be a set of iterms.*

*(i)* $\hat{T}^{i,\tau}_2 = \hat{T}^{i,\dot{\tau}}_2$
*(ii)* $\hat{T}^{i,\tau}_2 \vdash \hat{\Pi}^b_{i-1}$-$REPL^{\dot{\tau}}$ *provided* $\tau \subseteq O_2(|id|)$.
*(iii)* $\hat{R}^i_2 \vdash \hat{\Pi}^b_{i-1}$-$REPL^{\{||\dot{id}||\}}$.

**PROOF.** The proofs of (i) and (ii) are made by similar speed-up arguments so we will only show (ii) below. (iii) follows from (ii). We now prove (ii). The set $\dot{\tau}$ is defined inductively. Since $\sigma_0 = \tau \cup cl$, by Theorem 20,

$\hat{T}^{i,\tau}_2$ proves the $\hat{\Pi}^b_{i-1} - REPL^{\sigma_0}$ axioms. Assume $\hat{T}^{i,\tau}_2$ proves the $\hat{\Pi}^b_{i-1} - REPL^{\sigma_i}$ axioms and consider the axiom

$$(\forall x \leq \ell_1(v(a)) \cdot \ell_2(t(a)))(\exists y \leq s(x,a))A(x,y,a) \Leftrightarrow$$
$$(\exists w \leq 2 \cdot (m\#2^{\ell_1(v)\cdot\ell_2(t)}))(\forall x \leq \ell_1(v) \cdot \ell_2(t)))A(x, \dot{\beta}(x, |m|, s, w), a))$$

where $\ell_1, \ell_2 \in \sigma_i$ and $t, v \in L_2$ and where $m$ is short for $s^*(\ell_1(v(a)) \cdot \ell_2(t(a)), a)$. Let

$$X = (\forall x \leq \ell_1(v(a)) \cdot \ell_2(t(a)))(\exists y \leq s)A(x,y)$$
$$Y(u) = (\exists w \leq 2 \cdot (m\#2^{\ell_1(v(a))\cdot\ell_2(t(a))}))(\forall x \leq u \cdot \ell_2(t))A(x, \dot{\beta}(x, |m|, s, w))$$

We want to show $\hat{T}_2^{i,\tau} \vdash X \Leftrightarrow Y(\ell_1(v(a)))$. That $\hat{T}_2^{i,\tau} \vdash Y(\ell_1(v(a))) \supset X$ is obvious. The formula $Y(u)$ is equivalent to a $\hat{\Sigma}_i^b$-formula. Hence, $\hat{T}_2^{i,\tau}$ proves $IND_Y^{\ell_1}$. We also have $\hat{T}_2^{i,\tau} \vdash X \supset Y(0)$, and by $REPL_{A(x,y),s,t}^{\ell_2}$, we have $\hat{T}_2^{i,\tau} \vdash X \supset Y(1)$. We use $REPL_{A(x+u\cdot\ell_2(t(a)),y),s,t}^{\ell_2}$ to show $X \supset (u < \ell_1(v(a)) \wedge Y(u) \supset Y(Su))$. Thus, $\hat{T}_2^{i,\tau}$ prove $X \supset Y(\ell_1(v(a)))$. $\square$

### *2.6 Equivalence results*

Another application of Theorem 20 is the following theorem.

**Theorem 23** *($i \geq 1$) $S_2^i = \hat{S}_2^i$, $T_2^i = \hat{T}_2^i$, and $R_2^i = \hat{R}_2^i + \hat{\Pi}_{i-1}^b$-$REPL$.*

**PROOF.** We can convert any $\Sigma_i^b$-formula to a $\hat{\Sigma}_i^b$-formula using Lemma 17, Remark 1, Remark 18, Remark 21, and $\hat{\Pi}_{i-1}^b$-$REPL$. Hence, the above prenex theories can prove their induction schemes for any $\Sigma_i^b$-formula. $\square$

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

**Theorem 24** *($i \geq 2$) $\hat{R}_2^i$ proves the $\hat{\Pi}_{i-2}^b$-$REPL$ axioms and $\hat{T}_2^{i,||\tau||}$ proves the $\hat{\Pi}_{i-2}^b$-$REPL^{|\tau|}$ axioms.*

**PROOF.** This proof was used by Allen [1] to show $R_2^i$ proves $\Sigma_i^b$-replacement. Let $A \in \hat{\Pi}_{i-2}^b$. Let $X := (\forall x \leq |t|)(\exists y \leq s(x,a))A(x,y)$ and let $Y := (\exists w \leq 2 \cdot (t\#m))(\forall x \leq |t|)(A(x, \dot{\beta}(x, |m|, s(x,a), w)))$ where $m = s^*(|t|, a)$. 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

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

$\hat{R}^i_2$ can prove this is equivalent to a $\hat{\Pi}^b_i$-formula. (Note we are counting sharply bounded quantifiers in the number of quantifier alternations.) So by Lemma 4, $\hat{R}^i_2$ proves $LLIND_Z$. It is trivial that $\hat{R}^i_2$ proves $X \supset Z(0)$. Also $\hat{R}^i_2$ proves $X \wedge Z(j) \supset Z(Sj)$. Together with $LLIND_Z$ this implies $X \supset Z(||t||)$. As $\hat{R}^i_2$ proves $Z(||t||) \supset Y$, this completes the proof. The general case is similar. □

**Definition 25** *Let $\tau \subseteq O_2(|id|)$. We write $\Sigma^b_{0,\tau}(\Psi)$ or $\Pi^b_{0,\tau}(\Psi)$ to denote the smallest class containing $\Psi$ and closed under Boolean operations and $(\exists y \leq \ell(t))$ where $\ell \in \dot{\tau}$ and $t \in L_2$. For $i > 0$, we write $\Sigma^b_{i,\tau}(\Psi)$ for the smallest class containing $\Pi^b_{i-1,\tau}(\Psi)$ where, and quantifications of the form $(\exists x \leq t)$ and $(Qx \leq \ell(t))$ where $\ell \in \dot{\tau}$ and $t \in L_2$. $\Pi^b_{i,\tau}(\Psi)$ is defined mutatis mutandis. We write $\Sigma^b_i(\Psi)$ for $\Sigma^b_{i,\{|id|\}}(\Psi)$.*

**Theorem 26** $(i \geq 1)$ *Let $\tau \subseteq O_2(|id|)$. $\hat{T}^{i,\tau}_2$ proves any $\phi \in \Sigma^b_{1,\tau}(\hat{\Sigma}^b_{i-1})$ equivalent to some formula in $\hat{\Sigma}^b_i$. So $\hat{T}^i_2$ proves $IND^\tau_\phi$. In particular, $\hat{R}^i_2$ proves any $\phi \in \Sigma^b_{1,\{||id||\}}(\hat{\Sigma}^b_{i-1})$ equivalent to some formula in $\hat{\Sigma}^b_i$. Further for $i \geq 2$, we can replace $\Sigma^b_{1,\{||id||\}}(\hat{\Sigma}^b_{i-1})$ in the above with $\Sigma^b_{1,\{||id||\}}(\Sigma^b_{i-1})$.*

**PROOF.** The $\hat{T}^{i,\tau}_2$ result follows from Lemma 17 and Theorem 22. We then use Theorem 24 and the proof of Theorem 23 to show for $i \geq 2$ that $\hat{R}^i_2$ proves every $\Sigma^b_{i-1}$-formula is equivalent to a $\hat{\Sigma}^b_{i-1}$-formula. □

Theorem 26 has content even for $EBASIC$ since $EBASIC$ is equal to $\hat{T}^{i,cl}_2$.

**Theorem 27** $(i \geq 1)$ *$\hat{R}^i_2$ proves the $\hat{\Delta}^b_i$-$IND^{2^{\{||\dot{id}||\}}}$ axioms and hence, the $\hat{\Delta}^b_i$-$LIND$ axioms. In general, $\hat{T}^{i,\tau}_2$ proves the $\hat{\Delta}^b_i$-$IND^{2^{\dot{\tau}}}$ axioms.*

**PROOF.** Let $A(x)$ be $\hat{\Delta}^b_i$ in $\hat{T}^{i,\tau}_2$. Let $A_\Sigma(x) \in \hat{\Sigma}^b_i$ and $A_\Pi(x) \in \hat{\Pi}^b_i$ be equivalent to $A(x)$. $\hat{T}^{i,\tau}_2$ proves $(\forall x \leq 2^{\min(\ell(c),|c|)})(A_\Sigma(x) \supset A_\Pi(\min(x + 2^b, 2^{\min(\ell(c),|c|)})))$ is equivalent to a $\hat{\Pi}^b_i$-formula where $\ell \in \dot{\tau}$. Call this formula $B(b)$ and perform the same proof as in Theorem 13. □

Note if $\tau \not\subseteq O_2(|id|)$, then the min's which occur in terms in $2^{\dot{\tau}}$ will kick-in and we will not get a full exponential speed-up.

**Corollary 28** $(i \geq 1)$ *$\hat{S}^{i-1}_2 \subseteq \hat{R}^i_2$. In general, $\hat{T}^{i-1,2^{\dot{\tau}}}_2 \subseteq \hat{T}^{i,\tau}_2$. If $i \geq 2$, $S^{i-1}_2 \subseteq \hat{R}^i_2$.*

**PROOF.** The corollary follows from Theorem 23 and Theorem 27. □

### *2.7 Another pairing function*

We define another pairing function that we use in our witnessing arguments.

Let $B = 2^{|\max(x,y)|+1}$. So $B$ will be longer than either $x$ or $y$. Hence, we can code pairs as $\langle x, y\rangle := (2^{|\max(x,y)|}+y)\cdot B+(2^{|\max(x,y)|}+x)$. To project out the coordinates from an ordered pairs we use $\beta(1, w) := \hat{\beta}(0, \lfloor\frac{1}{2}|w|\rfloor \dot{-} 1, \hat{\beta}(0, \lfloor\frac{1}{2}|w|\rfloor, w))$ and $\beta(2, w) := \hat{\beta}(0, \lfloor\frac{1}{2}|w|\rfloor \dot{-} 1, \hat{\beta}(1, \lfloor\frac{1}{2}|w|\rfloor, w))$ which returns the left and right coordinate of the pair $w$. (The real Gödel beta function projects out $\beta(i, w)$, the $i$th element of a sequence $w$. However, as we never use this function we allow the suggestive notation.) To check if $w$ is a pair we use $ispair(w) :=$

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

The above 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 $\beta(2, w) = y$.

## 3 Machine classes and definability in prenex theories

We now give characterisations of the $\hat{\Sigma}^b_{i+1}$-definable multifunctions of $\hat{T}^{i,\tau}_2$ analogous to Krajíček [17]'s characterization of the $\Sigma^b_{i+1}$-multifunctions of $S^i_2$ as $FP^{\Sigma^p_i}(wit, \log)$. We show $\hat{T}^{i,2^{\dot{\tau}}}_2 \preceq_{\hat{\Sigma}^b_{i+1}} \hat{T}^{i+1,\tau}_2$ provided $\tau \subseteq O_2(|id|)$. Lastly, we give a syntactic characterisation of the $\hat{\Delta}^b_{i+1}$-predicates of $\hat{T}^{i,\tau}_2$.

### *3.1 Technical tools*

**Definition 29** *A* multifunction *is a set $f \subseteq \mathbb{N} \times \mathbb{N}$ such that for all $x \in \mathbb{N}$ there exists $\langle x, y\rangle \in f$. We express $\langle x, y\rangle \in f$ as $f(x) = y$. We write $f \circ g$ for the composition of $f$ and $g$ and define $(f \circ g)(x) = z$ if there is a $y \in \mathbb{N}$ 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 that $f(x) = y$.*

**Definition 30** *If $f(x) = y$ is a multifunction defined in $T$ by a predicate $A_f(x, y)$ where $y$ is provably bounded by $t$, then by the expression $T \vdash B(f(x))$ for some formula $B$ we mean $T \vdash (\exists y \leq t(x))(A_f(x, y) \wedge B(y))$.*

**Definition 31**

*A multifunction $f$ is defined by $\tau$-bounded primitive recursion ($BPR_k^\tau$) from $g$ and $h$, $t, r \in L_k$, and $\ell \in \tau$ if*

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

*We write $BPR^\tau$ for $BPR_2^\tau$.*

Before we define the class $FP^{\Sigma_i^p}(wit, |\tau|)$, we need to discuss the witness oracle machine model we will use. One natural choice would be to have a deterministic, three tape machine with a work tape, an oracle tape, and an oracle response tape. Queries would be written on the oracle tape and whenever a query state was entered, the answer '1' or '0' would appear in one step on the oracle response tape and the oracle response tape head would be on this symbol. In the case of a '1' answer, a dollar sign would be placed after the '1' followed by a witness to the correctness of the oracle response. An initial configuration of such a machine would have the input $x$ on the work tape and the other tapes blank. The output of such a machine would be the content of its work tape when a halt state is entered. Let us call these kinds of machines *witness oracle Turing machines* ($WOTM$). These machines, although natural, are not completely adequate for our purposes. The problem is that a theory $T_2^{i,\tau}$ can in general only effectively reason about sequences of lengths it has induction up to. For $\tau$ with slow growing terms, this can easily be sublinear, hence, the computations these theories can reason about will be sublinear time. We, thus, want our machine model to be able to handle sublinear time computations, yet have these computations still produce polynomial length outputs. We do two things to get around this problem. First, we change the initial configuration so that the run-time bound of the computation is initially written on the work tape, the input $x$ is written on the oracle tape followed by a dollar sign, and the oracle response tape is blank except for a dollar sign in the second square. The run-time bound on the work tape allows us to use it as a clock for the computation. The $x$ on the oracle tape allows us to have queries about the whole input and not have to worry about the linear time it would take to copy it from the work tape. The second modification we make is we view the oracle response tape after the dollar sign as being partitioned into blocks of squares of some size $r(x)$ where $x$ is the input and where $r \in L_2$. When a halt state is entered, we now define the output of the machine as being the contents of the first such block. Since witnesses to '1' answers can be polynomial in length, we have solved our problem. Call this kind of machine a $BWOTM$ for *blocked-$WOTM$*. We will discuss the relationship between these two models after the next definitions.

**Definition 32** *($i \geq 1$) $F[|\tau|]_2^{\Sigma_i^p}(wit)$ is the class of multifunctions $f$ computed*

*by a BWOTM $M$ which on input $x$ runs in time $|\ell_M(h(x))|$ for some $\ell_M \in \dot{\tau}$ and $h \in L_2$ and which makes queries to an $\Sigma_i^p$-oracle.*

Since $cl \in \dot{\tau}$ the machines in this class can always make at least $O(1)$ many queries. Depending on $\ell$ and $h$ it is possible for two different inputs of the same length to an $F[|\tau|]_2^{\Sigma_i^p}(wit)$ machine to have different run-time bounds. We put $|\cdot|$ outside the $\ell(h(x))$ to keep our notation and some of our arguments simpler. To avoid this issue one can consider the subclass of $F[|\tau|]_2^{\Sigma_i^p}(wit)$ of machines with $h$ is of the form $g(2^{|x|})$.

**Definition 33** *$FP^{\Sigma_i^p}(wit, |\tau|)$ is the class of multifunctions computable by polynomial time $WOTM$s which use fewer than $|\ell(h)|$ witness queries to a $\Sigma_i^p$-oracle in for some $\ell \in \dot{\tau}$ and $h \in L_2$. $P^{\Sigma_i^p}(|\tau|)$ is the class of predicates in $FP^{\Sigma_i^p}(wit, |\tau|)$ computable by $WOTM$'s that do not look at the witnesses returned by the oracle. $FP^{\Sigma_i^p}(wit, s)$ and $P^{\Sigma_i^p}(s)$ for some single function $s$ are the classes where the number of queries on inputs of length $n$ is bounded by $O(s(n))$.*

In the first definition above $|\tau|$ 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 third definition there is a single bound on the number queries which is a function of the length of the input. 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 our definitions above what we call $FP^{\Sigma_i^p}(wit, log)$ is what Buss, Krajicek, and Takeuti [10] call *strong-*$FP^{\Sigma_i^p}(wit, log)$. Given the restricted nature of the class $F[|\tau|]_2^{\Sigma_i^p}(wit)$, the next result, which is based on a result in [10], is somewhat surprising.

**Theorem 34** $(i \geq 1)$ $F[|\tau|]_2^{\Sigma_i^p}(wit) = FP^{\Sigma_i^p}(wit, |\tau|)$.

**PROOF.** Let $M \in F[|\tau|]_2^{\Sigma_i^p}(wit)$. We give a machine $N \in FP^{\Sigma_i^p}(wit, |\tau|)$ accepting the same language. On input $x$, $N$ computes $|\ell(h(x))|$, where $\ell \in \dot{\tau}$ and $h \in L_2$, and then begins simulating $M$. After $M$ halts, it writes as its output the contents of the first block of $M$'s oracle tape. Now suppose $M \in FP^{\Sigma_i^p}(wit, |\tau|)$ with number of queries bounded by $|\ell(h)|$ for $\ell \in \dot{\tau}$ and $h \in L_2$. We can assume the number of tape squares changed on any tape during $M$'s computation $x$ is less than $|x|^r$ for some fixed $r$. Consider the following procedure on an $F[|\tau|]_2^{\Sigma_i^p}(wit)$ machine $N$.

**Input** $x\$$ /* The \$ immediately follows $x$ on the query tape.*/
**For** $j = 1, \ldots, |\ell(h(x))|$
    /* $|\ell(h(x))|$ = max. # of queries in $M$. The counter is implemented on the work tape. The instructions below are for the query tape.*/

**If** $j \neq 1$ **then** move right on oracle tape.
**Write** 1 on oracle tape.
Ask oracle:
"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 dollar sign?"$*/$
Enter query state.
**If** square under oracle response head $= 0$ **Write** 0 on oracle tape
**End For**

The run-time of $N$ is bounded by some constant times $|\ell(h)|$ so will be less than some iterm in $\dot{\tau}$. To see that the above oracle query is $\Sigma_i^p$ let $(\exists z \leq t)A(q,z)$ be $M$'s oracle. A $\Sigma_i^p$ machine can guess a sequence of configurations of $M$ on $x$ and verify that the first configuration is a valid initial configuration and subsequent non-oracle configurations follow from their immediate predecessors. In the case of an oracle query, the $\Sigma_i^p$ machine checks that the query answer matched what $N$ said it was. In the case of a '1' answer we check also that the witness $z$ returned satisfies $A(q,z)$. This is a $\Pi_{i-1}^p$ query so a $\Sigma_i^p$ machine can do it. Since $N$ is choosing '1' answers greedily we do not have to verify '0' answers are correct. The oracle's encoding for each step of $M$'s computation has length $3|x|^r$ where the first $|x|^r$ blocks are used to encode the contents of $M$'s work tape, the second $|x|^r$ squares are used to encode the state of $M$'s oracle tape, and the last $|x|^r$ square used to encode the contents of $M$'s oracle response tape. We require that the encoding of steps of $M$ is right to left so that the last step of $M$'s computation appears to the right of the dollar sign of the oracle response tape. We use $|x|^r$ as our block size for $N$'s oracle tape. The output of the above $N$ 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 $M$. $\Box$

### *3.2 Defining machine classes in prenex theories*

We now use Theorem 34 to show $\hat{T}_2^{i,\tau}$ can $\hat{\Sigma}_{i+1}^b$-define $FP^{\Sigma_i^p}(wit, |\tau|)$. Notice this will show $EBASIC$ can $\hat{\Sigma}_{i+1}^b$-define $FP^{\Sigma_i^p}(wit, 1)$ since $\hat{T}_2^{i,cl} = EBASIC$. In particular, this shows $EBASIC$ can $\hat{\Sigma}_2^b$-define $FP^{NP}(wit, 1)$ which contains $FP$. This is not as surprising as it may at first seem. Since all the theories we are considering are classical they can prove excluded middle for any formula. Hence,for any $\hat{\Sigma}_1^b$-formula $A(x,y)$, $EBASIC$ can prove

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

which is equivalent in $EBASIC$ to a $\hat{\Sigma}_2^b$-formula and is one witness query to an $NP$ oracle. With a single such query one can guess a polynomial time com-

putation, so already one has $FP$. $EBASIC$ can prove its $\hat{\Sigma}^b_2$-multifunctions closed under composition and one can view the content of Theorem 34 in this case as saying the class $FP^{NP}(wit, 1)$ reduces to a finite composition of $NP$ witness queries. This said, $EBASIC$'s ability to prove properties of it $\hat{\Sigma}^b_2$-definable multifunctions is severely limited since it does not have induction.

**Theorem 35** *($i \geq 1$) $\hat{T}^{i,\tau}_2$ can $\hat{\Sigma}^b_{i+1}$-define the $FP^{\Sigma^p_i}(wit, |\tau|)$ multifunctions.*

**PROOF.** By Theorem 34, it suffices to show $\hat{T}^{i,\tau}_2$ can $\hat{\Sigma}^b_{i+1}$-define any $M \in F[|\tau|]^{\Sigma^p_i}_2(wit)$. Suppose $M(x) \in F[|\tau|]^{\Sigma^p_i}_2(wit)$ uses oracle $\Omega(q)$ and runs in time $|\ell(h)|$ for $\ell \in \dot{\tau}$ and $h \in L_2$. We write this $\Sigma^p_i$-oracle as $(\exists z \leq t(q))B(z, q)$ where $B \in \hat{\Pi}^b_{i-1}$ and $t \in L_2$.

An instantaneous description ($ID$) of $M$ is a 7-tuple (the notion of 7-tuple is defined using composition of ordered pairs) of the form: $\langle u, x, o, w, t^q_L, t^W_L, t^W_R \rangle$. 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, $t^q_L$ is a number which after deleting the most significant bit represents the contents of the query tape to the left of the dollar sign, $t^W_L$ is a number which after deleting the most significant bit represents the visited squares to the left of work tape head, and $t^W_R$ is a number which after deleting the most significant bit represents the visited squares to the right of the work tape head. Notice in view of the proof of Theorem 34 we do not have to worry about the head on the oracle tape moving left, also we can assume the oracle response tape is read-only.

Following [10] we define a *precomputation* of $M$ to be a sequence of ID's 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 sequence's 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, 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 $|\ell(h(x))|$ for some $\ell \in \dot{\tau}$, and $h \in L_2$, we can write a formula checking if a number codes a precomputation with a single quantifier of the form $(\forall j \leq |\ell(h(x))|)$.

A *Q-computation* is a precomputation in which the '1' answers are correct for the oracle $\Omega$ but the '0' answers are not required to be correct. We define $QComp_M(w, x, v)$ to be the following formula:

$QComp_M(w, x, v) :=$ $w$ is a precomputation of $M(x)$ and

$(\forall j \leq |\ell(h(x))|)(\mathit{YAns}(w,j) \Leftrightarrow \mathit{Bit}(|\ell(h(x))| \dot{-} j, v) = 1)$
and $(\forall j \leq |\ell(h(x))|)(\mathit{Bit}(|\ell(h(x))| \dot{-} j, v) = 1 \supset$
$\mathit{CorrectYes}(w,j))$

Here $\mathit{YAns}(w,j)$ says the first oracle square of the $j$th $ID$ in precomputation $w$ was '1'. It can be defined with an open formula using $\dot{\beta}$ and using projections of the pairing function. $\mathit{CorrectYes}(w,j)$ is just the predicate $\mathit{QueryState}(j) \supset B(z,q)$, where $q$ is the contents of oracle tape at time $j$ and $z$ is the minimum of $t(q)$ and the witness on the oracle tape at time $j$. $\mathit{QueryState}(j)$ is true iff $M$ was in a query state at time $j-1$ (time $j-1$ since the oracle responds in the step after a query was entered), this can be checked with an open formula. Both $z$ and $q$ can be defined as $L_2$-terms so $\mathit{CorrectYes}(w,j)$ is a $\hat{\Pi}^b_{i-1}$-formula. Hence, $\mathit{QComp}_M$ is provably equivalent in $\hat{T}^{i,\tau}_2$ to a $\hat{\Pi}^b_{i-1}$-formula. Since the number of distinct $ID$s in a computation of $M$ on input $x$ is bounded by $|\ell(h(x))|$, $v$ in $\mathit{QComp}_M$ can be bounded by $\ell'(h) := 2^{|\ell(h(x))|} \in 2^{\dot{\tau}}$. This also bounds 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 $ID$s. Since these $ID$s contain oracle witnesses $t$ need not be sharply bounded. As $\mathit{QComp}_M$ is provably equivalent to a $\hat{\Pi}^b_{i-1}$-formula, $\Psi := (\exists w \leq t)\mathit{QComp}_M(w,x,v)$ is provably equivalent to a $\hat{\Sigma}^b_i$-formula. However, if $v = 0$ then $\mathit{QComp}_M$ is equivalent to a $\hat{\Pi}^b_0$-formula in $EBASIC$ using Lemma 17 and noticing the bound on the pair can be bounded by a term of the form $|q|$. So $\hat{T}^{1,\tau}_2$ proves there is a precomputation of $x$ with all the oracle answers 0 using $IND^{\tau}_{\mathit{QComp}_M(w,x,0)}$. Thus, $\hat{T}^{1,\tau}_2 \vdash (\exists w \leq t)\mathit{QComp}_M(w,x,0)$. Let $A(u)$ be

$$(\exists v \leq \ell'(h(x)))(\exists w \leq t)(\mathit{QComp}_M(w,x,v) \wedge v \geq u).$$

We just showed $A(0)$. 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 22, we either have $A(\ell'(h(x)))$ or $(\exists u < \ell'(h(x)))(A(u) \wedge \neg A(u+1))$. Hence, there is a maximal $v \leq \ell'(h(x))$ for which $(\exists w \leq t)\mathit{QComp}_M(w,x,v)$ holds. All of the '1' answers in $v$ must be correct since $\mathit{QComp}_M$ holds. We argue that $\hat{T}^{i,\tau}_2$ proves all the 0 answers must also be correct. Suppose the $j$th '0' was incorrect. We could change it to a '1' and set the lower order bits to '0', thus, making a number $v' > v$. Now from $\exists w \mathit{QComp}_M(w,x,v)$ we can show

$$\hat{T}^{1,\tau}_2 \vdash (\exists w')\mathit{QComp}_M(w',x,v')$$

by letting $w'$ be $w$ up to the $j$th query, then coding a '1' with a valid witness on the response tape for the $j$th query and then coding $M$'s computation where all the answers to subsequent queries are '0'.

Therefore, $\hat{T}^{i,\tau}_2$ proves $M(x)$ has a computation with correct oracle responses. Define $\mathit{Out}(w,x)$ using $\beta$ and $MSP$ to take a precomputation $w$ and output the contents of the first block of the witness string. For $i \geq 1$, $\hat{T}^{i,\tau}_2$ proves:

$$(\forall x)(\exists y)(\exists v \le \ell'(h'(x)))[$$
$$(\exists w \le t)(Out(w,x) = y \wedge QComp_M(w,x,v))$$
$$\wedge\neg(\exists v' \le \ell'(h'(x)))(\exists w' \le t)(v' > v \wedge QComp_M(w',x,v')]$$

and the formula inside the $(\exists y)$ is equivalent to a $\hat{\Sigma}^b_{i+1}$-formula using Theorem 26, Remark 18, and Lemma 17. $\Box$

### *3.3 Query definability*

To prove the converse of the above theorem we need that $\hat{T}^{i,\tau}_2$ can $\hat{\Sigma}^b_{i+1}$-define the composition of $FP^{\Sigma^p_i}(wit, |\tau|)$ functions in a "nice" way. First, we make precise our definition of "nice".

**Definition 36** *A multifunction $f(x) = y$ is $Q^{i,\tau}$-defined in $T$ by a formula*

$$B(x,y) := (\exists v \le \ell(s(x)))[(\exists w \le t)(Out(w,x) = y \wedge A(x,w,v))$$
$$\wedge\neg(\exists v' \le \ell(s(x)))(\exists w' \le t)(v' > v \wedge A(x,w',v'))].$$

*where $A \in \hat{\Pi}^b_{i-1}$, $Out(w,x), s \in L_2$, and $\ell \in \tau$ if $\mathbb{N} \models B(x,y) \Leftrightarrow f(x) = y$ and $T \vdash (\forall x)(\exists y \le t)B$. In addition, $A(x,w,0)$ must be provable equivalent to a $\hat{\Pi}^b_0$-formula in $T$ and $T$ must prove $(\exists w \le t)A(x,w,0)$. The formula $B$ is called a $Q^{i,\tau}$-*definition *of $f$.*

Buss [8] gives a variant of $Q^{i,\tau}$-definition. The formula $B(x,y)$ in the above definition is equivalent to a $\hat{\Sigma}^b_{i+1}$-formula in $\hat{T}^{i,\tau}_2$ so if $f$ is $Q^{i,\dot{\tau}}$-defined in $\hat{T}^{i,\tau}_2$, it will also be $\hat{\Sigma}^b_{i+1}$-defined in $\hat{T}^{i,\tau}_2$. The proof of Theorem 35 shows any $f \in FP^{\Sigma^p_i}(wit, |\tau|)$ is $Q^{i,\dot{\tau}}$-definable in $\hat{T}^{i,\tau}_2$. However, it is unclear from this whether given an $f \in FP^{\Sigma^p_i}(wit, |\tau|)$ which is $\hat{\Sigma}^b_{i+1}$-definable in $\hat{T}^{i,\tau}_2$ by $A_f(x,y)$ that $\hat{T}^{i,\tau}_2$ can prove $A_f(x,y)$ equivalent to a $Q^{i,\dot{\tau}}$-definition.

**Lemma 37** *If a multifunction $f(x) = y$ has a $Q^{i,\dot{\tau}}$-definition, then $f \in FP^{\Sigma^p_i}(wit, |\tau|)$. The predicate $f(x) = 1$ is computable in $P^{\Sigma^p_i}(|\tau|)$.*

**PROOF.** Let

$$B(x,y) := (\exists v \le \ell(s(x)))[(\exists w \le t)(Out(w,x) = y \wedge A(x,w,v))$$
$$\wedge\neg(\exists v' \le \ell(s(x)))(\exists w' \le t)(v' > v \wedge A(x,w',v'))].$$

where $A \in \hat{\Pi}^b_{i-1}$, $Out(w,x), s \in L_2$, and $\ell \in \dot{\tau}$ be a $Q^{i,\dot{\tau}}$-definition of $f$. Using the $\Sigma^p_i$-query $[(\exists w \le t)A(x,w,v)?]$, one can binary search for a maximal $v \le \ell(s(x))$ such that $(\exists w \le t)A(x,w,v)$ holds, then compute and output

$Out(w,x)$ from the witness $w$ returned by the query. This takes $\log(\ell(s(x))$ queries which will be $O(\ell'(h(x)))$ queries for some $\ell' \in |\tau|$ and $h \in L_2$. In the $f(x) = 1$ case, one finds a maximal $v$ in the same manner (this does not require a witness oracle), and then for this $v$ make the $\Sigma_i^p$-query does $[(\exists w \leq t)(A(x,w,v) \wedge Out(w,x) = 1)?]$. $\Box$

**Lemma 38** ($i \geq 1$) *The theory $\hat{T}_2^{i,\tau}$ proves its $Q^{i,\dot{\tau}}$-definable multifunctions are closed under composition.*

**PROOF.** Suppose $f$ and $g$ are $Q^{i,\dot{\tau}}$-definable in $\hat{T}_2^{i,\tau}$ where $f$ is defined by proving $B_f :=$

$$
\begin{array}{l}
(\forall x)(\exists y \leq t_f)(\exists v_f \leq \ell_f(s_f(x))))[ \\
(\exists w_f \leq t_f)(Out_f(w_f,x) = y \wedge A_f(x,w_f,v_f)) \\
\wedge\neg(\exists v'_f \leq \ell_f(s_f(x))))(\exists w'_f \leq t_f)(v'_f > v_f \wedge A_f(x,w'_f,v'_f))].
\end{array}
$$

and $g$ is defined by proving $B_g$ similarly. To define $h = g \circ f$, we define $C_h := (\forall x)(\exists y \leq t_g(t_f(x))D_h$ where $D_h$ is

$$
\begin{array}{l}
(\exists v_f \leq \ell_f(s_f(x))))(\exists v_g \leq \ell_g(s_g(t_f(x))))[(\exists w_f \leq t_f)(\exists w_g \leq t_g(t_f(x))) \\
(Out_g(w_g,x) = y \wedge v_g \leq Out(w_f,x) \wedge A_f(x,w_f,v_f) \wedge \\
A_g(Out(w_f,x),w_g,v_g)) \\
\wedge\neg(\exists v'_f \leq \ell(s_f(x)))(\exists v'_g \leq \ell_g(s_g(t_f(x)))))(\exists w'_f \leq t_f)(\exists w'_g \leq t_g(t_f(x)))( \\
(v'_f > v_f \vee (v'_f = v_f \wedge v'_g > v_g \wedge v'_g \leq Out(w'_f,x))) \wedge A_f(x,w'_f,v'_f) \wedge \\
A_g(Out(w'_f,x),w'_g,v'_g))].
\end{array}
$$

Since $\hat{T}_2^{i,\tau}$ proves $B_g$ and $B_f$, it proves $C_h$. Now $C_h$ can be converted into the desired $B_h$ using Theorem 26 and pairing. In the pairing we bound the size of $\langle v_f, v_g \rangle$ by $(\ell_f(s_f) \cdot \ell_g(s_g))^3 \in \dot{\tau}$ then use *cond* to guarantee $v_f \leq \ell_f(s_f)$ and $v_g \leq \ell_g(s_g)$. Using the fact that when $v_f$ and $v_g$ are 0, $A_f$ and $A_g$ will be equivalent to $\hat{\Pi}_0^b$-formulas, it is not hard to check when $v_h$ is 0, $A_h$ will be equivalent to a $\hat{\Pi}_0^b$-formula in $\hat{T}_2^{i,\tau}$ and $\hat{T}_2^{i,\tau} \vdash (\exists w_h \leq t_h)A_h$. Thus, $h$ is $Q^{i,\dot{\tau}}$-definable in $\hat{T}_2^{i,\tau}$. $\Box$

**Lemma 39** ($i \geq 1$) *Let $\tau \subseteq O_2(|id|)$. The theory $\hat{T}_2^{i,2^{\dot{\tau}}}$ proves its $Q^{i,2^{\dot{\tau}}}$-definable multifunctions are closed under $BPR_2^{\dot{\tau}}$.*

**PROOF.** Recall $f$ is defined by $BPR_2^{\dot{\tau}}$ from $g$, $h$, $F$, $k$, and $r$ if

$$F(0,\mathbf{x}) = g(\mathbf{x})$$

$$F(n+1,\mathbf{x}) = \min(h(n,\mathbf{x},F(n,\mathbf{x})), r(n,\mathbf{x}))$$
$$f(n,\mathbf{x}) = F(\ell(k(n,\mathbf{x})),\mathbf{x})$$

where $r,k \in L_2$ and $\ell \in \dot{\tau}$. Suppose $g,h$ are $Q^{i,2^{\dot{\tau}}}$-definable in $\hat{T}_2^{i,2^{\dot{\tau}}}$. Let $h'(n,\mathbf{x},z)$ be $\min(h(n,\mathbf{x},z), r(n,\mathbf{x}))$. This is $Q^{i,2^{\dot{\tau}}}$-definable by Lemma 38. Let $g$ be defined by proving

$$\begin{aligned}&(\forall \mathbf{x})(\exists y \le t_g)(\exists v_g \le \ell_g(s_g))[\\ &(\exists w_g \le t_g)(Out_g(w_g,\mathbf{x}) = y \wedge A_g(\mathbf{x},w_g,v_g))\\ &\wedge\neg(\exists v_g' \le \ell_g(s_g))(\exists w_g' \le t_g)(v_g' > v_g \wedge A_g(\mathbf{x},w_g',v_g'))].\end{aligned}$$

where $\ell_g \in 2^{\dot{\tau}}$ and let $h'$ be defined by proving

$$\begin{aligned}&(\forall n,\mathbf{x},z)(\exists y \le t_h')(\exists v_{h'} \le \ell_{h'}(s_{h'}))[\\ &(\exists w_{h'} \le t_{h'})(Out_{h'}(w_{h'},n,\mathbf{x}) = y \wedge A_{h'}(n,\mathbf{x},z,w_{h'},v_{h'})) \wedge\\ &\neg(\exists v_{h'}' \le \ell_{h'}(s_{h'}(n,\mathbf{x},z)))(\exists w_{h'}' \le t_{h'})(v_{h'}' > v_{h'} \wedge A_{h'}(n,\mathbf{x},z,w_{h'}',v_{h'}'))].\end{aligned}$$

where $\ell_{h'}$ is in $2^{\dot{\tau}}$. Without loss of generality we can assume $\ell_g(s_g(\mathbf{x})) \le \ell_{h'}(s_{h'}(0,\mathbf{x}))$ for all $\mathbf{x}$. Define $m_t$ to be $t_{h'}^*(n,\mathbf{x},r(n,\mathbf{x}))$ and define $m_s$ to be $\ell_{h'}(s_{h'}^*(n,\mathbf{x},r(n,\mathbf{x}),m_t))$. Let $A_f(n,\mathbf{x},w,v)$ be

$$\begin{aligned}&A_g(\mathbf{x},\hat{\beta}(0,|m_t|,w),\hat{\beta}(0,|m_s|,v)) \wedge (\forall j < |\ell(k(n,\mathbf{x}))|)\\ &A_{h'}(j,\mathbf{x},Out_{h'}(\hat{\beta}(j,|m_t|,w),n,\mathbf{x}),\hat{\beta}(Sj,|m_t|,w),\dot{\beta}(Sj,|m_s|,\ell_{h'}(s_{h'}),v))\end{aligned}$$

As $A_g, A_{h'} \in \hat{\Pi}_{i-1}^b$, $\hat{T}_2^{i,2^{\dot{\tau}}}$ proves $A_f$ is equivalent to a $\hat{\Pi}_{i-1}^b$-formula. Notice when $v$ is 0, $A_f$ will be equivalent to a $\hat{\Pi}_0^b$-formula using pairing and the fact that $A_g$ and $A_{h'}$ will be equivalent to $\hat{\Pi}_0^b$-formulas in this case by the definition of $Q^{i,2^{\dot{\tau}}}$-definability. So $\hat{T}_2^{i,2^{\dot{\tau}}}$ can prove $(\exists w_f \le 2\cdot 2^{\ell(k)\cdot|m_t|})A_f(n,\mathbf{x},w_f,0)$ from the $Q^{i,2^{\dot{\tau}}}$-properties of $A_g$ and $A_{h'}$. Using $\hat{\Sigma}_i^b$-$IND^{2^{\dot{\tau}}}$ on $A(u) :=$

$$(\exists v_f \le 2\cdot 2^{\ell(k)\cdot|m_s|})(\exists w_f \le 2\cdot 2^{\ell(k)\cdot|m_t|})(A_f(n,\mathbf{x},w_f,v_f) \wedge v_f \ge u)$$

as we did in Theorem 35, $\hat{T}_2^{i,2^{\dot{\tau}}}$ can define $f$ by proving

$$\begin{aligned}&(\forall n,\mathbf{x})(\exists y \le r)(\exists v_f \le 2\cdot 2^{\ell(k)\cdot|m_s|})[\\ &(\exists w_f \le 2\cdot 2^{\ell(k)\cdot|m_t|})(Out_f(w_f,n,\mathbf{x}) = y \wedge A_f(n,\mathbf{x},w_f,v_f)) \wedge\\ &\neg(\exists v_f' \le 2\cdot 2^{\ell(k)\cdot|m_s|})(\exists w_f' \le 2\cdot 2^{\ell(k)\cdot|m_t|})(v_f' > v_f \wedge A_f(n,\mathbf{x},w_f',v_f'))].\end{aligned}$$

Here $Out_f(w_f,n,\mathbf{x})$ is $Out_{h'}(\hat{\beta}(\ell(k(n,x)),|m_t|,w_{h'}),n,\mathbf{x})$. Since $\ell \in \dot{\tau}$ and since $m_s$ is in $2^{\dot{\tau}}$, the term $2\cdot 2^{\ell(k)\cdot|m_s|}$ is boundable by a term in $2^{\dot{\tau}}$. $\square$

The next lemma shows closure under a slightly different recursion scheme.

**Lemma 40** *($i \geq 1$) Let $\tau \subseteq O_2(|id|)$. The $Q^{i,2^{\dot{\tau}}}$-definable multifunctions of $\hat{T}_2^{i,2^{\dot{\tau}}}$ are closed under:*

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

*where $g, h$ are $Q^{i,2^{\dot{\tau}}}$-definable , $r, t \in L_2$ and $\ell \in \dot{\tau}$.*

**PROOF.** To define $f$ we first define $f'$ with

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

where $m = r^*(\ell(t),\mathbf{x})$. From $f'$ we define $f$ as $\hat{\beta}(\min(n,\ell(t)),|m|,f'(n,\mathbf{x}))$. $\square$

## 4 The sequent calculus and cut-elimination

Until now we have not specified the deduction system in which we perform $\hat{T}_2^{i,\tau}$ and $\hat{C}_2^{i,\tau}$ proofs. To show the converse of Theorem 35; however, we work in the sequent calculus reformulating the induction and replacement axioms as rules of inference. Buss [7] or Takeuti [27] describe the sequent calculus.

**Definition 41**

*A $\Psi$-$IND^\tau$ inference is an inference:*

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

*where $b$ is an eigenvariable and must not appear in the lower sequent, $t \in L_k$, $\ell \in \tau$, and $A \in \Psi$.*

*Let $\tau \subseteq O_2(|id|)$. A $\Psi$-$REPL^\tau$ inference is an inference of the form:*

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

*where* $A \in \Psi$, $\ell \in \tau$, $s, t \in L_k$, *and* $m := t^*(\ell(s), a)$.

Buss [7] has shown that one gets the same theory if one formulates $S^i_2$ or $T^i_2$ with induction axioms or induction rules. The same sorts of proof work in the $\hat{T}^{i,\tau}_2$ and $\hat{C}^{i,\tau}_2$ case [23].

Given a set $\Psi$ of prenex formulas let $L\Psi$ be the formulas which can be made into $\Psi$-formulas by padding the left hand side with zero or more dummy quantifiers. The next result is the primary reason why we use the sequent calculus and why we formulate $\hat{T}^{i,\tau}_2$ and $\hat{C}^{i,\tau}_2$ with rules of inference. The proof relies on cut-elimination and is the same as in the $S^i_2$ and $T^i_2$ case which are in Buss [7]. We write $A_\tau$ to mean a quantifier $(\forall x \leq \ell(t))$ where $\ell \in \tau$ and $t \in L_2$. Similarly, we write $E_\tau$ to mean a quantifier $(\exists x \leq \ell(t))$ where $\ell \in \tau$ and $t \in L_2$. We write $A$ and $E$ for $A_{\{id\}}$ and $E_{\{id\}}$. So an $EA_{\{|id\}}\hat{\Sigma}^b_1$-formula would look like $(\exists x \leq t)(\forall y \leq |s|)A$ where $A$ is a $\hat{\Sigma}^b_1$-formula.

**Theorem 42** $(i \geq 0, k \geq 1)$

*Let* $\Psi \supseteq L\hat{\Sigma}^b_{i,k}$ *be closed under subformulas and under* $L_k$*-term substitutions. Let* $\Gamma \to \Delta$ *be a sequent of* $\Psi$*-formulas provable in* $EBASIC_k$ *or* $\hat{T}^{i,\tau}_k$*. Then* $\Gamma \to \Delta$ *has a proof in which only* $\Psi$*-formulas occur.*

*Suppose* $\tau \subseteq O_2(|id|)$*. Let* $\Psi$ *containing* $LA_\tau\hat{\Sigma}^b_{i+1} \cup LEA_\tau\hat{\Pi}^b_i$ *be closed under subformulas and closed under* $L_k$*-term substitutions. Let* $\Gamma \to \Delta$ *be a sequent of* $\Psi$*-formulas provable in* $\hat{C}^{i,\tau}_k$*. Then* $\Gamma \to \Delta$ *has a proof in which only* $\Psi$*-formulas occur.*

In particular, Theorem 42 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.

### *4.1 The witness predicate*

Let $T$ be one of $EBASIC_2$, $\hat{T}^{i,\tau}_2$, or $\hat{C}^{i,\tau}_2$. By Parikh's Theorem [21], $T$ can $\hat{\Sigma}^b_m$-define a function $f$ if and only if there is a $\hat{\Sigma}^b_m$-formula $A_f(x, y)$ and a term $t \in L_2$ such that $T$ proves $(\forall x)(\exists! y \leq t)A_f(x, y)$. For a multifunction one does not have to show uniqueness. An $E\hat{\Sigma}^b_m$-formula is a formula $(\exists y \leq t)A$ where $A \in \hat{\Sigma}^b_m$. We define a witness predicate as follows.

If $A(\mathbf{a}) \in L\hat{\Pi}^b_{m-1}$ or $A(\mathbf{a}) \in L\hat{\Sigma}^b_{m-1}$ then $Wit^m_A(w, \mathbf{a}) := w = 0 \wedge A(\mathbf{a})$.

If $A(\mathbf{a})$ is $(\exists x \leq t(\mathbf{a}))B$ and $A \in \hat{\Sigma}^b_m$ then $Wit^m_A(w, \mathbf{a}) := w \leq t(\mathbf{a}) \wedge B(w, \mathbf{a})$.

If $A(\mathbf{a})$ is $(\exists x_1 \leq t_1)(\exists x_2 \leq t_2)B$ and $A \in E\hat{\Sigma}^b_m$ then

$$Wit^m_A(w, \mathbf{a}) := ispair(w) \wedge \beta(1, w) \leq t_1 \wedge \beta(2, w) \leq t_2 \wedge B(\beta(1, w), \beta(2, w), \mathbf{a}).$$

Thus, $Wit^m_A$ is equivalent in $EBASIC$ to a $\hat{\Pi}^b_{m-1}$-formula or a $\hat{\Sigma}^b_{m-1}$-formula. The witness predicate above is simplified from Buss [7]. The simplification arises because we are in the prenex setting. From the definition of witness the next useful properties follow:

**Lemma 43** ($m \geq 1$) *If $A(\mathbf{a}) \in LE\hat{\Sigma}^b_m$, then: (a) $EBASIC \vdash Wit^m_A(w, \mathbf{a}) \supset A(\mathbf{a})$. (b) There is a $t_A$ so that $EBASIC \vdash A(\mathbf{a}) \Leftrightarrow (\exists w \leq t_A(\mathbf{a}))Wit^m_A(w, \mathbf{a})$. (c) For $t_A$, $EBASIC \vdash Wit^m_A(w, \mathbf{a}) \supset w \leq t_A$.*

**PROOF.**

(a) This statement is immediate from the definition of $Wit^m_A$.

(b) If $A \in \hat{\Sigma}^b_m$ 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 is bounded by $2^{2\cdot(|\max(t_1,t_2)|+1)}$.

(c) Follows from (b) and the definition of $Wit^m_A$. In particular, the definition of *ispair* forces any pair for a witness to be unique. □

For a cedent $\Gamma = \{A_1, \ldots, A_n\}$ 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 in defining witnesses for $Wit^m_{\wedge\Gamma}$ and $Wit^m_{\vee\Gamma}$.

We define $Wit^m_{\wedge\Gamma}(w, \mathbf{a})$ by induction. If $\Gamma = \emptyset$, define $Wit^m_{\wedge\Gamma}(w, \mathbf{a})$ to be $w = 0$. If $\Gamma = \{A\}$ then $Wit^m_{\wedge\Gamma}(w, \mathbf{a})$ is $Wit^m_A(w, \mathbf{a})$. If $\Gamma = \{A_1, \ldots, A_n\}$, let $\Gamma'$ be $\{A_2, \ldots A_n\}$ and set $Wit^m_{\wedge\Gamma}(w, \mathbf{a})$ to be $Wit^m_{A_1}(\beta(1, w), \mathbf{a}) \wedge Wit^m_{\wedge\Gamma'}(\beta(2, w), \mathbf{a})$.

We now define $Wit^m_{\vee\Gamma}(w, \mathbf{a})$. If $\Gamma = \emptyset$, define $Wit^m_{\vee\Gamma}(w, \mathbf{a})$ to be $\neg(0 = 0)$. If $\Gamma = \{A\}$ then $Wit^m_{\vee\Gamma}(w, \mathbf{a})$ is $Wit^m_A(w, \mathbf{a})$. If $\Gamma = \{A_1, \ldots A_n\}$, let $\Gamma'$ be $\{A_2 \ldots A_n\}$ and define $Wit^m_{\vee\Gamma}(w, \mathbf{a})$ to be $Wit^m_{A_1}(\beta(1, w), \mathbf{a}) \vee Wit^m_{\vee\Gamma'}(\beta(2, w), \mathbf{a})$ where $t_{A_j}$ are from Lemma 43.

From the above definition $EBASIC$ proves $Wit^m_{\wedge\Gamma}$ is equivalent to a formula of the form $A \wedge \neg B$ and $Wit^m_{\vee\Gamma}$ is equivalent to a formula of the form $C \vee \neg D$ where $A, B, C, D \in \hat{\Sigma}^b_{m-1}$. From this it is not hard to show these predicates are $Q^{m-1,cl}$-definable in $EBASIC$.

**Lemma 44** ($m \geq 1$) *Let $\Gamma, \Delta$ be cedents of $LE\hat{\Sigma}^b_m$-formulas with free variables $\mathbf{a}$. There is a term $t_\Gamma$ such that $EBASIC \vdash Wit^m_{\wedge\Gamma}(w, \mathbf{a}) \supset w \leq t_\Gamma$ and*

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

*There is also a term* $t_\Gamma$ *such that*

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

*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 pairs, and by the bounds for witnesses for formulas given by Lemma 43. □

The pairing function and $\beta$-functions of the last section are computable in $FP^{\Sigma^p_i}(wit, |\tau|)$ and are $Q^{i,\dot{\tau}}$-definable in $\hat{T}^{i,\tau}_2$.

### *4.2 Some witnessing arguments*

We use a witnessing argument to prove the converse of Theorem 35.

**Theorem 45** ($i \geq 1$) *Suppose* $\hat{T}^{i,\tau}_2 \vdash \Gamma \rightarrow \Delta$ *where* $\Gamma$ *and* $\Delta$ *are cedents of* $LE\hat{\Sigma}^b_{i+1} \cup L\hat{\Sigma}^b_i$ *formulas with free variables among* $\mathbf{a}$. *Then there is a* $Q^{i,\dot{\tau}}$*-defined in* $\hat{T}^{i,\tau}_2$ *multifunction* $f \in FP^{\Sigma^p_i}(wit, |\tau|)$ *such that:*

$$\hat{T}^{i,\tau}_2 \vdash Wit^{i+1}_{\wedge\Gamma}(w, \mathbf{a}) \supset Wit^{i+1}_{\vee\Delta}(f(w, \mathbf{a}), \mathbf{a}).$$

The meaning of $Wit^{i+1}_{\vee\Delta}(f(w, \mathbf{a}), \mathbf{a})$ is interpreted using Definition 30.

**PROOF.** This is proved by induction on the number of sequents in an $\hat{T}^{i,\tau}_2$ proof of $\Gamma \rightarrow \Delta$. By cut elimination, we 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 case the witness predicate is the original formula. So we choose $f$ to be the constant zero function. To define $f$ for logical inferences, cut inferences, structural inferences, ($\exists$:right) or ($\forall$:left) is relatively simple and can be found in similar arguments in Krajíček [18]. 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 hypothesis there is a $Q^{i,\dot{\tau}}$-definable $g \in FP^{\Sigma_i^p}(wit, |\tau|)$ such that

$$\hat{T}_2^{i,\tau} \vdash Wit^{i+1}_{b \leq t \wedge A \wedge \Gamma}(w, \mathbf{a}, b) \supset Wit^{i+1}_{\vee\Delta}(g(w, \mathbf{a}, b), \mathbf{a}, b).$$

There are three subcases to consider. In each case, we need to determine a value for $b$ and then run $g$ on that value. In the first case, $(\exists x \leq t)A(x) \in E\hat{\Sigma}^b_{i+1}$. If $w$ witnesses $(\exists x \leq t)A(x) \wedge \Gamma$, 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 $f(w, \mathbf{a}) := g(\langle\langle 0, \beta(2, \beta(1, w)), \beta(2, w)\rangle\rangle, \mathbf{a}, \beta(1, \beta(1, w)))$. Then

$$\hat{T}_2^{i,\tau} \vdash Wit^{i+1}_{(\exists x \leq t)A \wedge \Gamma}(w, \mathbf{a}) \supset Wit^{i+1}_{\vee\Delta}(f(w, \mathbf{a}), \mathbf{a}).$$

In the second case, $(\exists x \leq t)A(x) \in \hat{\Sigma}^b_{i+1}$. If $w$ witnesses $(\exists x \leq t)A(x) \wedge \Gamma$, then $\beta(1, w)$ is a value for $b$ such that $A(b)$ holds. Let

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

Then

$$\hat{T}_2^{i,|\tau|} \vdash Wit^{i+1}_{(\exists x \leq t)A \wedge \Gamma}(w, \mathbf{a}) \supset Wit^{i+1}_{\vee\Delta}(f(w, \mathbf{a}), \mathbf{a}).$$

The last subcase is when $(\exists x \leq t)A(x) \in L\hat{\Sigma}^b_i$ or $(\exists x \leq t)A(x) \in L\hat{\Sigma}^b_{i-1}$. Define $f$ as above except rather than use $\beta(1, \beta(1, w))$ or $\beta(1, w)$ for $b$ use the multifunction which queries a witness oracle about $(\exists x \leq t)A(x)$. If the latter is satisfiable then the oracle returns a value satisfying it. Notice $\beta(1, \beta(1, w))$ in $f$ in this case is 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 hypothesis there is a $Q^{i,\dot{\tau}}$-definable $g \in FP^{\Sigma_i^p}(wit, |\tau|)$ such that

$$\hat{T}_2^{i,\tau} \vdash Wit^{i+1}_{b \leq t \wedge \Gamma}(w, \mathbf{a}, b) \supset Wit^{i+1}_{A \vee \Delta}(g(w, \mathbf{a}, b), \mathbf{a}, b).$$

By cut-elimination, $(\forall x \leq t)A(x) \in L\hat{\Pi}^b_i$. Thus, $(\exists x \leq t)\neg A(x) \in \Sigma^p_i$. So we can ask an oracle for a value $b \leq t$ such that $\neg(A(b))$ holds. If such a value exists set $f(w, \mathbf{a}) = g(\langle 0, w\rangle, \mathbf{a}, b)$. If no such value exists we let $f(w, \mathbf{a}) = \langle 0, 0\rangle$ since $(\forall x \leq t)A(x)$ must be a valid $L\hat{\Pi}^b_i$-formula.

**($\hat{\Sigma}^b_i$-$IND^\tau$ case)** Suppose for an $\ell \in \tau$ and $r \in L_2$ we have the inference

$$\frac{A(b), \Gamma \rightarrow A(Sb), \Delta}{A(0), \Gamma \rightarrow A(\ell(r(c, \mathbf{a}))), \Delta}$$

then by hypothesis there is a $Q^{i,\dot{\tau}}$-definable $g \in FP^{\Sigma_i^p}(wit, |\tau|)$ such that

$$\hat{T}_2^{i,\tau} \vdash Wit^{i+1}_{A(b)\wedge\Gamma}(w, b, \mathbf{a}) \supset Wit^{i+1}_{A(Sb)\vee\Delta}(g(w, b, \mathbf{a}), b, \mathbf{a}).$$

Let $f \in FP^{\Sigma_i^p}(wit, |\tau|)$ do the following: First, $f$ computes $v = \ell(r(c, \mathbf{a}))$ and queries $[A(v)]$? If the answer is '1' then $f$ outputs the witness. If $A(v)$ is valid any value will witness it and hence the succedent will be witnessed. If the answer was 'No', $f$ queries $[A(0)?]$. If it receives 'No' as a reply it outputs 0; the antecedent will be false. If the reply was '1', then $f$ binary searches for a $d \leq v$ such that $A(d)$ but not $A(Sd)$. This takes $O(|v|)$ many queries to $A(d)$. $\hat{T}_2^{i,\tau}$ can prove by a $\hat{\Sigma}_i^b$-$IND^\tau$ using $(\exists w \leq t)QComp_{M_f}(w, x, v)$ for the $M_f$ that does this computation that the value returned by $f$ is such that $A(d)$ but not $A(Sd)$. Using this value of $d$, $f$ can run $g(w, \mathbf{a}, d)$ 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,

$$\hat{T}_2^{i,\tau} \vdash Wit^{i+1}_{A(0)\wedge\Gamma}(w, \mathbf{a}) \supset Wit^{i+1}_{A(\ell(r))\vee\Delta}(f(w, \mathbf{a}), \mathbf{a}).$$

This completes the cases that remained to be shown and the proof. $\Box$

Notice if we had tried to carry out the above argument in $EBASIC$+$\Sigma_i^b$-$IND^\tau$, then in the $(\forall : right)$ case $A$ could be a $\Sigma^b_{i+1}\backslash\Pi^b_i$ formula if $t$ were of the form $|s|$. So our argument above would not work. In fact, for $\tau$ containing terms of slower growth rate than $|id|$ it seems hard to come up with a witness function for the lower sequent in this case.

**Theorem 46** $(i \geq 1)$ *Let $\tau \subseteq O_2(|id|)$. Suppose $\hat{T}_2^{i+1,\tau} \vdash \Gamma \to \Delta$ where $\Gamma$ and $\Delta$ are cedents of $LE\hat{\Sigma}^b_{i+1}$-formulas with free variables among $\mathbf{a}$. Then there is an $f \in FP^{\Sigma_i^p}(wit, \dot{\tau})$ which is $Q^{i,2^{\dot{\tau}}}$-defined in $\hat{T}_2^{i,2^{\dot{\tau}}}$ such that:*

$$\hat{T}_2^{i,2^{\dot{\tau}}} \vdash Wit^{i+1}_{\wedge\Gamma}(w, \mathbf{a}) \supset Wit^{i+1}_{\vee\Delta}(f(w, \mathbf{a}), \mathbf{a}).$$

**PROOF.** This is proved by induction on the number of sequents in a $\hat{T}_2^{i+1,\tau}$ proof of $\Gamma \to \Delta$. By cut elimination, we assume all the sequents in the proof are in $LE\hat{\Sigma}^b_{i+1}$. All cases except for the $(\hat{\Sigma}^b_{i+1}$-$IND^\tau)$ case are as in Theorem 45. We now do this last case.

**($\hat{\Sigma}^b_{i+1}$-$IND^\tau$ case)** Suppose we have

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

where $\ell \in \tau$ and $s \in L_2$. We assume $\mathbf{a}$ contains all free variables except $b$ in the upper and lower sequent. By hypothesis there is a $Q^{i,2^{\dot{\tau}}}$-definable

$g \in FP^{\Sigma_i^p}(wit, \dot{\tau})$ such that

$$\hat{T}_2^{i,2^{\dot{\tau}}} \vdash Wit^{i+1}_{A(b)\wedge\Gamma}(w, b, \mathbf{a}) \supset Wit^{i+1}_{A(Sb)\vee\Delta}(g(w, b, \mathbf{a}), b, \mathbf{a}).$$

Informally, the idea to witness the lower sequent is the following: run $g$ on $w$ a witness for $A(0), \Gamma$. Either this witnesses $A(Sb)$ or it witnesses $\Delta$. In the latter case, we are done. In the former case, we run $g$ on the witness just produced for $A(S0)$ together with $\beta(2, w)$ which is supposed to be a witness for $\wedge\Gamma$. We keep repeating this process until we get a witness for $\Delta$ or we finally get a witness for $A(\ell(s))$. More formally, using Lemma 40, we $Q^{i,2^{\dot{\tau}}}$-define a function $f$ by $BPR_2^{\dot{\tau}}$ in the following way. First, we let

$$k(v, w, \mathbf{a}) = cond(Wit^{i+1}_{\vee\Delta}(\beta(2, v), \mathbf{a}), w, v).$$

This is $Q^{i,2^{\dot{\tau}}}$-definable in $\hat{T}_2^{i,2^{\dot{\tau}}}$ by the comments after the definition of the witness predicate, Lemma 38 and since $L_2$-terms are easily $Q^{i,2^{\dot{\tau}}}$-definable in $\hat{T}_2^{i,2^{\dot{\tau}}}$. Then we define

$$\begin{aligned} F(0, w, \mathbf{a}) &= \langle \beta(1, w), 0 \rangle \\ F(b+1, w, \mathbf{a}) &= min(k(F(b, w, \mathbf{a}), g(\beta(1, F(b, w, \mathbf{a})), \beta(2, w), \mathbf{a})), \\ &\qquad t_{A(Sb)\vee(\vee\Delta)}(b, \mathbf{a}) \\ f(u, w, \mathbf{a}) &= F(\min(u, \ell(s)), w, \mathbf{a}). \end{aligned}$$

Recall $t_{A(Sb)\vee(\vee\Delta)}(b, \mathbf{a})$ is the term bounding witness size for $A(Sb) \vee (\vee\Delta)$ by Lemma 44. $f$ will be in $FP^{\Sigma_i^p}(wit, \dot{\tau})$ by Lemma 37. Now

$$\hat{T}_2^{i,2^{\dot{\tau}}} \vdash Wit^{i+1}_{A(0)\wedge\Gamma}(w, \mathbf{a}) \supset Wit^{i+1}_{A(0)\vee\Delta}(f(0, w, \mathbf{a}), \mathbf{a}). \tag{6}$$

Also, it is not hard to show

$$\hat{T}_2^{i,2^{\dot{\tau}}} \vdash Wit^{i+1}_{A(0)\wedge\Gamma}(w, \mathbf{a}) \wedge Sb \leq \ell(s) \wedge Wit^{i+1}_{A(b)\vee\Delta}(f(b, w, \mathbf{a}), b, \mathbf{a}) \supset Wit^{i+1}_{A(Sb)\vee\Delta}(f(Sb, w, \mathbf{a}), Sb, \mathbf{a}). \tag{7}$$

We show this implies

$$\hat{T}_2^{i,2^{\dot{\tau}}} \vdash Wit^{i+1}_{A(0)\wedge\Gamma}(w, \mathbf{a}) \supset Wit^{i+1}_{A(\ell(s))\vee\Delta}(f(\ell(s), w, \mathbf{a}), \mathbf{a}).$$

First, we $Q^{i,2^{\dot{\tau}}}$-define $h$ by $BPR_2^{\dot{\tau}}$ as:

$$\begin{aligned} H(0, w, \mathbf{a}) &= f(0, w, \mathbf{a}) \\ H(b+1, w, \mathbf{a}) &= f(b+1, w, \mathbf{a}) \cdot 2^{(b+1)\cdot|m|} + H(b, w, \mathbf{a}) \\ h(w, \mathbf{a}) &= H(\ell(s(\mathbf{a})), w, \mathbf{a}) \end{aligned}$$

where min's have been deleted for readability and where $m = t^*_{A(Sb)(\ell(s),\mathbf{a})\vee\bigvee\Delta}$. There are $L_2$-terms bounding the above sum. Now let $h$ be $Q^{i,2^{\dot\tau}}$-defined by $B_h(w,\mathbf{a},w')$. From (7) above

$$\hat T_2^{i,2^{\dot\tau}} \vdash B_h(w,\mathbf{a},w') \wedge Wit^{i+1}_{A(0)\wedge\Gamma}(w,\mathbf{a}) \wedge Sb \le \ell(s)$$

$$\wedge Wit^{i+1}_{A(b)\vee\Delta}(\hat\beta(b,|m|,w'),b,\mathbf{a}) \supset Wit^{i+1}_{A(Sb)\vee\Delta}(\hat\beta(Sb,|m|,w'),Sb,\mathbf{a}).$$

By $\hat\Pi^b_i$-$IND^{2^{\dot\tau}}$ on $Wit^{i+1}_{A(b)\vee\Delta}(\hat\beta(b,|m|,w'),b,\mathbf{a})$ and by (6), this implies

$$\hat T_2^{i,2^{\dot\tau}} \vdash B_h(w,\mathbf{a},w') \wedge Wit^{i+1}_{A(0)\wedge\Gamma}(w,\mathbf{a}) \supset$$
$$Wit^{i+1}_{A(\ell(s))\vee\Delta}(\dot\beta(\ell(s),|m|,w'),\ell(s),\mathbf{a}).$$

Hence, from the definition of $h$, $\hat T_2^{i,2^{\dot\tau}}$ proves

$$\hat T_2^{i,2^{\dot\tau}} \vdash Wit^{i+1}_{A(0)\wedge\Gamma}(w,\mathbf{a}) \supset Wit^{i+1}_{A(\ell(s))\vee\Delta}(f(\ell(s),w,\mathbf{a}),\mathbf{a}).$$

□

### *4.3 Implications of the witnessing argument*

We end this section with some corollaries of the above theorems.

**Corollary 47** *($i > 1$) Suppose $\tau \subseteq O_2(|id|)$.*

$$\hat T_2^{i-1,2^{\dot\tau}} \preceq_{\hat\Sigma^b_i} \hat T_2^{i,\tau} = \hat T_2^{i,\dot\tau}.$$

*We thus have: (1) $T_2^{i-1} \preceq_{\hat\Sigma^b_i} S_2^i$ and (2) $\hat T_2^{i-1,2^{\{p(||id||)\}}} \preceq_{\hat\Sigma^b_i} \hat R_2^i$.*

**PROOF.** Suppose $\hat T_2^{i,\tau} = \hat T_2^{i,\dot\tau}$ proves $A(\mathbf{a}) \in \hat\Sigma^b_i$. By Theorem 46, $\hat T_2^{i-1,2^{\dot\tau}}$ proves $Wit^i_A(f(w,\mathbf{a}),\mathbf{a})$ where $f \in FP^{\Sigma^p_{i-1}}(wit,\dot\tau)$. So by Lemma 43, $\hat T_2^{i-1,2^{\dot\tau}} \vdash A$. (1) follows if $\tau = \{|id|\}$. $\hat T_2^{i-1,2^{(\{|\dot id|\})}}$ has induction up to terms of the form $2^{p(|s|)}$ which could also be the bound in the conclusion of a IND inference. (2) follows if $\tau = \{||id||\}$. □

**Corollary 48** *($i \ge 1$) A multifunction $f$ is $\hat\Sigma^b_{i+1}$-definable in $\hat T_2^{i,\tau}$ iff $f \in FP^{\Sigma^p_i}(wit,|\tau|)$. So the $\hat\Sigma^b_{i+1}$-definable multifunctions of $T_2^i$, $S_2^i$, $\hat R_2^i$, $EBASIC$ are $FP^{\Sigma^p_i}(wit,poly)$, $FP^{\Sigma^p_i}(wit,\log)$, $FP^{\Sigma^p_i}(wit,\log\log)$, and $FP^{\Sigma^p_i}(wit,1)$.*

**PROOF.** For the 'if' direction use Theorem 35. Otherwise, by Theorem 45 when we take $\Gamma$ empty and $\Delta$ to be an $E\hat{\Sigma}^b_{i+1}$-formula $(\exists y \leq t(x))A(x,y)$ provable in $\hat{T}^{i,\tau}_2$, there is a $Q^{i,\dot{\tau}}$-defined, $FP^{\Sigma^p_i}(wit, |\tau|)$ multifunction $f$ such that $\hat{T}^{i,\tau}_2 \vdash\!\!\rightarrow Wit^{i+1}_{(\exists y \leq t)A}(x, f(x))$. By the definition of witness we have $\hat{T}^{i,\tau}_2 \vdash\!\!\rightarrow A(x, \beta(1, f(x)))$. So $\beta(1, f(x))$ give at least one value such that $A(x,y)$ holds. Let $M$ be the machine for $\beta(1, f(x))$. Using $M$ we will construct a machine $M'$ in $FP^{\Sigma^p_i}(wit, |\tau|)$ such that $M'(x) = y$ iff $A(x,y)$ holds. Suppose $A(x,y)$ is of the form $(\exists z \leq s)B(x,y,z)$ where $B \in \hat{\Pi}^b_i$. Then $M'$ does the following: (1) Run $M$ on $x$ and obtain its output $y_0$. (2) Ask the queries $(\exists y \leq t)(y = y)$ and $(\exists z \leq s)(z = z)$. Let $y_1$ and $z_1$ be the oracle responses. (3) Ask the $\hat{\Sigma}^b_i$-query $\neg B(x, y_1, z_1)$. If the answer is '1' output $y_0$. Otherwise, output $y_1$. $M'$ will be in $FP^{\Sigma^p_i}(wit, |\tau|)$ since $M$ is. The purpose of step (2) is to nondeterministically get values for $y_1$ and $z_1$. If these values happen to witness $(\exists y \leq t)A$ then $y_1$ is output, otherwise $y_0$ is output.

The other results follow from the $\hat{T}^{i,\tau}_2$ result and Definition 33. We are using the fact that $|||x|||$ is in $\Theta(\log\log(|x|))$. $\square$

The $T^i_2$ result was essentially known from Buss [8] and the $S^i_2$ result follows from Krajíček [18] using the construction of $M'$ from $M$ which was in Buss, Krajíček, Takeuti [10].

**Corollary 49** *($i \geq 1$) The $\hat{\Delta}^b_{i+1}$-predicates of $\hat{T}^{i,\tau}_2$ are $P^{\Sigma^p_i}(|\tau|)$. So the $\hat{\Delta}^b_{i+1}$-predicates of $T^i_2$, $S^i_2$, $\hat{R}^i_2$, and $EBASIC$ are $P^{\Sigma^p_i}$, $P^{\Sigma^p_i}(\log)$, $P^{\Sigma^p_i}(\log\log)$, and $P^{\Sigma^p_i}(1)$ respectively.*

**PROOF.** Suppose $f \in P^{\Sigma^p_i}(|\tau|) \subset FP^{\Sigma^p_i}(wit, |\tau|)$. Now $f$ can be computed by some $M_f \in F[|\tau|]^{\Sigma^p_i}_2(wit)$ in the manner of the proof of Theorem 34. We can change the definition of $BWOTM$ slightly for predicates so that instead of the output being the first block of the witness on the oracle response tape it is instead just the response of the last query the machine makes. A machine $M'$ defined in this way could compute $f(x)$ by operating like $M_f$ on $x$ until $M_f$ halts and then asking the one additional query: "Is there a valid computation of $M_f$ on the input $x$ with the queries answered by the string to the right of the dollar sign and where the first block of the witness on the oracle response tape is '1'?" Essentially, the same proof as Theorem 35 shows $\hat{T}^{i,\tau}_2$ can define $M'$ as $B(x,y) :=$

$$\begin{aligned}(\exists v \leq \ell(h(x)))[&(\exists w \leq t)(Out(v,x) = y \wedge QComp_{M'}(w,x,v)) \\ &\wedge \neg(\exists v' \leq \ell(h(x)))(\exists w' \leq t)(v' > v \wedge QComp_{M'}(w',x,v')]\end{aligned}$$

where $QComp_{M'}$ is $\hat{\Pi}^b_{i-1}$, $Out, h \in L_2$ and $\ell \in \tau$. Here $Out$ is an $L_2$-term computing the bit value of the last oracle query from $v$. So $B(x,y)$ is equivalent

to a $\hat{\Sigma}^b_{i+1}$-formula in $\hat{T}^{i,\tau}_2$. Also $\hat{T}^{i,\tau}_2$ proves $(\exists! y \leq 1)B(x,y)$ since by the proof of Theorem 35 it can show any $v$ such that the above predicate holds must be unique. So $\hat{T}^{i,\tau}_2 \vdash B(x,1) \Leftrightarrow \neg B(x,0)$. Both $B(x,1)$ and $\neg B(x,0)$ are equivalent to $f(x)$ outputting '1' and the former is equivalent to a $\hat{\Sigma}^b_{i+1}$-formula and the latter is equivalent to a $\hat{\Pi}^b_{i+1}$-formula.

For the other direction, suppose $A$ is $\hat{\Delta}^b_{i+1}$ in $\hat{T}^{i,\tau}_2$. Let $A_\Sigma \in \hat{\Sigma}^b_{i+1}$ and $A_\Pi \in \hat{\Pi}^b_{i+1}$ be equivalent to $A$. Consider $B(x,y) :=$

$$(\neg A_\Pi(x) \wedge y = 0) \vee (A_\Sigma(x) \wedge y = 1).$$

Certainly, $\hat{T}^{i,\tau}_2$ proves $(\forall x)(\exists y \leq 1)B(x,y)$. By Remark 1 and Theorem 26, $\hat{T}^{i,\tau}_2$ proves $(\exists y \leq 1)B(x,y)$ is equivalent to a $E\hat{\Sigma}^b_{i+1}$-formula. So by Theorem 45 there is a $g \in FP^{\Sigma^p_i}(wit, |\tau|)$ such that $\hat{T}^{i,\tau}_2 \vdash Wit^i_B(x, g(x))$. The definition witness predicate implies

$$\hat{T}^{i,\tau}_2 \vdash B(x, \beta(1, g(x))). \tag{8}$$

Let $f(x) = \beta(1, g(x))$. As $g$ is $Q^{i,\dot{\tau}}$-definable in $\hat{T}^{i,\tau}_2$, this theory proves $f$ can be defined with

$$\begin{aligned}(\exists v \leq \ell(s(x)))[&(\exists w \leq t)(\beta(1, Out(w,x)) = y \wedge C(x,w,v)) \\ &\wedge \neg(\exists v' \leq \ell(s(x)))(\exists w' \leq t)(v' > v \wedge C(x,w',v'))]\end{aligned}$$

where $C \in \hat{\Sigma}^b_i$, $Out, s \in L_2$, ($Out$ is supposed to return the output of $g$) and $\ell \in \dot{\tau}$. The definition of $B$ implies $f(x) = 1 \Leftrightarrow B(x,1) \Leftrightarrow A(x)$ and the predicate $f(x) = 1$ will be in $P^{\Sigma^p_i}(|\tau|)$ by essentially the same argument used in Lemma 37. $\Box$

The $T^i_2$ result above was known from Buss [8] and the $S^i_2$ result is similar to a result in Krajíček [18].

**Corollary 50** *($i \geq 1$) $\hat{T}^{i,\tau}_2$ 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 $A, B \in \hat{\Sigma}^b_i$, $\ell \in \dot{\tau}$ and $s \in L_2$.*

**PROOF.** From the proof of Corollary 49 every $\hat{\Delta}^b_{i+1}$-predicate in $\hat{T}^{i,\tau}_2$ is equivalent to a formula

$$\begin{aligned}(\exists v \leq \ell(s(x)))[&(\exists w \leq t)(\beta(1, Out(w,x)) = 1 \wedge C(x,w,v)) \\ &\wedge \neg(\exists v' \leq \ell(s(x)))(\exists w' \leq t)(v' > v \wedge C(x,w',v'))].\end{aligned}$$

where $C \in \hat{\Sigma}^b_i$. This formula in turn is provably equivalent to

$$(\exists v \leq \ell(s(x)))[(\exists w \leq t)(\beta(1, Out(w,x)) = 1 \wedge C(x,w,v)) \\ \wedge \neg(\exists v' \leq \ell(s(x)))(\exists w' \leq t)(v' \geq v+1 \wedge C(x,w',v'))].$$

Let $A(x,v)$ be a $\hat{\Sigma}^b_i$-formula provably equivalent to

$$(\exists w \leq t)(\beta(1, Out(w,x)) = 1 \wedge C(x,w,v))$$

and let $B(x,v+1)$ be a $\hat{\Sigma}^b_i$-formula provably equivalent to

$$(\exists v' \leq \ell(s(x)))(\exists w' \leq t)(v' \geq v+1 \wedge C(x,w',v')).$$

□

Corollary 50 is similar to a result of Buss-Hay [5] where they show predicates in $P^{\Sigma^p_i}(\log)$ can be written in the form $(\exists v \leq |s(x)|)(A(x,v) \wedge \neg B(x,v))$ where $A$ and $B$ are $\Sigma^b_i$. Our result shows the $\hat{\Delta}^b_{i+1}$-predicates of $S^i_2$ which are also $P^{\Sigma^p_i}(\log)$ can be written in this form provably in $S^i_2$. In the $\hat{T}^{i,cl}_2 = EBASIC$ case of Corollary 50, the outermost existential is bounded by a constant so can be replaced by a disjunction.

**Remark 51** *The results above generalise to the theories $T^{i,\tau}_k$ for $k \geq 2$.*

**Remark 52** *Given the last remark, by Corollary 47 for $i \geq 1$ and $k \geq m \geq 0$, $\hat{T}^{i,\{|id|_m\}}_{k+2} \preceq_{\hat{\Sigma}^b_{i,k+2}} \hat{T}^{i+1,\{|id|_{m+1}\}}_{k+2}$. This is true by Corollary 12 since $EBASIC_{k+2}$ can prove any term in $2^{\{|id|_{m+1}\}}$ is $k+2$-surpassed by $|id|_m$.*

In [10] it was shown that $S^i_3 \preceq_{\Sigma^b_{i+1,3}} R^{i+1}_3$, by the above we have $S^i_3 \preceq_{\hat{\Sigma}^b_{i+1,3}} \hat{R}^{i+1}_3$, thus, $\hat{R}^{i+1}_3 \preceq_{\hat{\Sigma}^b_{i+1,3}} R^{i+1}_3$. In Section 6 we show for $k \geq 0$, $\hat{R}^{i+1}_{k+2} \preceq_{\hat{\Sigma}^b_{i+1,k+2}} R^{i+1}_{k+2}$.

## 5 Applications of the witnessing argument

In this section we give some applications of the results of the last section.

### *5.1 The $\hat{\Sigma}^b_{i+k}$-definable multifunctions of prenex theories*

We now discuss the $\hat{\Sigma}^b_{i+k}$-definable multifunctions of $\hat{T}^{i,\tau}_2$ where $k \geq 2$. To make sure the reader is not confused we stress we are talking about $\hat{\Sigma}^b_{i+k,2}$ not $\hat{\Sigma}^b_{i,k}$.

A first observation on $\hat{\Sigma}^b_{i+k}$-definability in $\hat{T}^{i,\tau}_2$ is that since $EBASIC \subseteq \hat{T}^{i,\tau}_2$, these theories can $\hat{\Sigma}^b_{i+k}$-define any $f$ in $FP^{\Sigma^p_{i+k-1}}(wit, 1)$. A second observation is that $FP^{\Sigma^p_i}(wit, |\tau|) \subseteq FP^{\Sigma^p_{i+k-1}}(wit, 1)$ for $k \geq 2$ as with a single query to a $\Sigma^p_{i+1}$ witness oracle one can ask for a witness of the sequence of steps in a computation of any $M \in FP^{\Sigma^p_i}(wit, |\tau|)$. Using this witness one can read off the final output of $M$.

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 $\hat{T}^{i,\tau}_2$. All cases can be handled as in the $EBASIC = \hat{T}^{i+k,cl}_2$ version of Theorem 45 except we now also have a $\hat{\Sigma}^b_i$-$IND^\tau$ inference case (this is where the $L\hat{\Sigma}^b_i$-formulas may come from). Recall how this case was handled in the $\hat{T}^{i,\tau}_2$ version of Theorem 45. Given

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

where $\ell \in \tau$ and $r \in L_2$, 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 composed with the machine that would provide a witness for the top sequent. By hypothesis we assume the top sequent is witnessed with some $g \in FP^{\Sigma^p_{i+k-1}}(wit, 1)$. Since $FP^{\Sigma^p_i}(wit, |\tau|)$ is contained in $FP^{\Sigma^p_{i+k-1}}(wit, 1)$, this whole case can be handled by a machine in $FP^{\Sigma^p_{i+k-1}}(wit, 1)$. Thus, the following result holds.

**Theorem 53** *($i \geq 1, k \geq 2$) Suppose $\hat{T}^{i,\tau}_2 \vdash \Gamma \rightarrow \Delta$ where $\Gamma$ and $\Delta$ are cedents of $LE\hat{\Sigma}^b_{i+k} \cup L\hat{\Sigma}^b_i$-formulas with free variables among $\mathbf{a}$. Then there is a $Q^{i+k-1,cl}$-definable in $\hat{T}^{i,\tau}_2$, $FP^{\Sigma^p_{i+k-1}}(wit, 1)$ multifunction $f$ such that:*

$$\hat{T}^{i,\tau}_2 \vdash Wit^{i+k}_{\bigwedge\Gamma}(w, \mathbf{a}) \supset Wit^{i+k}_{\bigvee\Delta}(f(w, \mathbf{a}), \mathbf{a}).$$

*When $i = 0$ there is a $f \in FP^{\Sigma^p_{k-1}}(wit, 1)$ such that*

$$\mathbb{N} \models Wit^{k}_{\bigwedge\Gamma}(w, \mathbf{a}) \supset Wit^{k}_{\bigvee\Delta}(f(w, \mathbf{a}), \mathbf{a}).$$

For the $i = 0$ case we can 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 the next theorem and its corollaries follow by the same type of proofs as in Section 4.3 and Section 5.2.

**Theorem 54** *($i \geq 0, k \geq 2$) A multifunction $f$ is a $\hat{\Sigma}^b_{i+k}$-definable multifunction of $\hat{T}^{i,\tau}_2$ if and only if $f \in FP^{\Sigma^p_{i+k-1}}(wit, 1)$.*

**Corollary 55** *($i \geq 0, k \geq 2$) The $\hat{\Delta}^b_{i+k}$-predicates of $\hat{T}^{i,\tau}_2$ are $P^{\Sigma^p_{i+k-1}}(1)$.*

**Corollary 56** *($i \geq 1, k \geq 2$) The theory $\hat{T}_2^{i,\tau}$ proves its $\hat{\Delta}_{i+k}^b$-predicates can be written in the form*

$$\vee_{v=0}^{n}[A(x, S^v(0)) \wedge \neg B(x, S^{v+1}(0))].$$

*where $A, B \in \hat{\Sigma}_{i+k-1}^b$ and $n$ is a fixed integer. Here $S^0(0) = 0$ and $S^{v+1}(0) = S(S^v(0))$.*

It should be stressed that although $EBASIC$, $\hat{T}_2^{i,|\tau|}$, and $\hat{T}_2^{i,\tau}$ all have the same $\hat{\Sigma}_{i+k}^b$-definable multifunctions, it does not seem to be the case that either $EBASIC$ or $\hat{T}_2^{i,|\tau|}$ can carry out the witnessing argument needed to show they have the same $\hat{\Sigma}_{i+k}^b$-definable functions as $\hat{T}_2^{i,\tau}$. This is because neither of these theories seems to be able to simulate the $\hat{\Sigma}_i^b$-$IND^\tau$ case of the $\hat{T}_2^{i,\tau}$ witnessing argument which required $\hat{\Sigma}_i^b$-$IND^\tau$ to prove.

### *5.2 A strengthened conservation result*

We begin with the following result.

**Theorem 57** *($i \geq 1, k \geq 0$) Let $\tau \subseteq O_2(|id|)$. The $\hat{T}_{k+2}^{i+1,\dot{\tau}}$ is conservative over $\hat{T}_{k+2}^{i,2^{\dot{\tau}}}$ with respect to Boolean combinations of $\hat{\Sigma}_{i+1,k+2}^b$-formulas. That is, $\hat{T}_{k+2}^{i,2^{\dot{\tau}}} \preceq_{B(\hat{\Sigma}_{i+1,k+2}^b)} \hat{T}_{k+2}^{i+1,\dot{\tau}}$ and, in particular, $T_2^i \preceq_{B(\hat{\Sigma}_{i+1}^b)} S_2^{i+1}$ and $S_3^i \preceq_{B(\hat{\Sigma}_{i+1,3}^b)} \hat{R}_3^{i+1}$.*

**PROOF.** Suppose $\hat{T}_{k+2}^{i+1,\dot{\tau}} \vdash A(\mathbf{a}) \in B(\hat{\Sigma}_{i+1,k+2}^b)$. Then $A$ is tautologically equivalent to a formula of the form $\wedge_n \vee_j A_{nj}$ where each $A_{nj}$ is either a $\hat{\Sigma}_{i+1,k+2}^b$-formula or a $\hat{\Pi}_{i+1,k+2}^b$-formula. So $\hat{T}_{k+2}^{i+1,\dot{\tau}}$ proves each disjunct $\vee_j A_{nj}$. Consider one such disjunct $\vee_j A_{nj}$. Let $\Delta_n$ be the cedent of $\hat{\Sigma}_{i+1,k+2}^b$-formulas in this disjunct and let $\Gamma_n$ be the $\hat{\Sigma}_{i+1,k+2}^b$-formulas that are equivalent to the negations of $\hat{\Pi}_{i+1,k+2}^b$-formulas in this disjunct. Hence, $\hat{T}_{k+2}^{i+1,\dot{\tau}}$ proves $\Gamma_n \rightarrow \Delta_n$. Now this sequent can be proved with a proof such that all formulas are $L\hat{\Sigma}_{i+1,k+2}^b \cup L\hat{\Sigma}_{i,k+2}^b$. By Lemma 43

$$\hat{T}_{k+2}^{i,2^{\dot{\tau}}} \vdash \wedge\Gamma_n \supset (\exists w \leq t_{\Gamma_n}) Wit_{\wedge\Gamma_n}^{i+1}(w, \mathbf{a})$$

and

$$\hat{T}_{k+2}^{i,2^{\dot{\tau}}} \vdash (\exists w \leq t_{\Delta_n}) Wit_{\vee\Delta_n}^{i+1}(w, \mathbf{a}) \supset \vee\Delta_n.$$

We then carry out the witnessing argument of Remark 52 to show

$$\hat{T}_{k+2}^{i,2^{\dot{\tau}}} \vdash (\exists w \leq t_{\Gamma_n}) Wit_{\wedge\Gamma_n}^{i+1}(w, \mathbf{a}) \supset (\exists w \leq t_{\Delta_n}) Wit_{\vee\Delta_n}^{i+1}(w, \mathbf{a})$$

Hence, $\hat{T}^{i,2^{\dot{\tau}}}_{k+2} \vdash \Gamma_n \to \Delta_n$. Thus, $\hat{T}^{i,2^{\dot{\tau}}}_{k+2}$ proves $\vee_j A_{nj}$. So $\hat{T}^{i,2^{\dot{\tau}}}_{k+2}$ proves $A(\mathbf{a})$.

The remaining parts of the theorem are special cases of the first statement. □

The proof of Theorem 57 was adapted from the proof in Buss [8] that

$$T^i_2 + \Sigma^b_i\text{-}REPL \preceq_{B(\Sigma^b_{i+1})} S^{i+1}_2.$$

Below are two interesting corollary of the above theorem.

**Corollary 58** *($i \geq 1, m \geq n \geq 0, k \geq 2$) Let $\tau \subseteq O_2(|id|_m)$. Then*

$$\hat{T}^{i+n,2\uparrow(m-n)(\dot{\tau})}_k \preceq_{B(\hat{\Sigma}^b_{i+n+1,k})} \hat{T}^{i+m,\tau}_k.$$

*So by Corollary 49, the $\hat{\Delta}^b_{i+n+1}$-predicates of $\hat{T}^{i+m,\tau}_2$ are $P^{\Sigma^p_{i+n}}(wit, |2\uparrow(m-n)(\dot{\tau})|)$, provided $\tau \subseteq O_2(|id|_m)$.*

**PROOF.** This follows from Theorem 57 since

$$\begin{aligned}
&\hat{T}^{i+n,2\uparrow(m-n)(\dot{\tau})}_k \preceq_{B(\hat{\Sigma}^b_{i+n+1,k})} \hat{T}^{i+n+1,2\uparrow(m-n-1)(\dot{\tau})}_k \preceq_{B(\hat{\Sigma}^b_{i+n+2,k})} \\
&\cdots \preceq_{B(\hat{\Sigma}^b_{i+m-1,k})} \hat{T}^{i+m-1,2^{\dot{\tau}}}_k \preceq_{B(\hat{\Sigma}^b_{i+m,k})} \hat{T}^{i+m,m}_k.
\end{aligned}$$

We are using here the easily observed result that every iterm in $2^{(2^{\dot{\tau}})}$ is surpassed by some iterm in $2^{2^{\dot{\tau}}}$. □

By the same reasoning as Remark 52, the above corollary yields:

**Corollary 59** *($i \geq 1, k \geq m \geq n \geq 0$) Let $\hat{T}^{i,m}_k$ denote $\hat{T}^{i,\{|id|_m\}}_k$. Then $\hat{T}^{i+n,n}_{k+2} \preceq_{B(\hat{\Sigma}^b_{i+n+1,k+2})} \hat{T}^{i+m,m}_{k+2}$. In particular, $\hat{T}^i_{k+2} \preceq_{B(\hat{\Sigma}^b_{i+1,k+2})} \hat{T}^{i+m,m}_{k+2}$.*

### *5.3 $\hat{\Delta}^b_{i+1}$-$IND^{\dot{\tau}}$*

We now give a proof theoretic proof that $S^i_2$ proves $\Delta^b_{i+1}$-$LIND$. This was previously shown in Buss, Krajíček, and Takeuti [10] using a model theoretic argument of Ressayre that $S^i_2 \preceq_{\Sigma^b_i} S^i_2 + \Sigma^b_{i+1}\text{-}REPL^{\{|id|\}}$. We use two known results: (1) the result of Buss [8] that $S^i_2$ proves $\Sigma^b_0(\Sigma^b_i)$-$LIND$ and (2) the witnessing argument for $\Sigma^b_i$-formulas in Krajíček [18]. Once we have shown $S^i_2$ proves $\Delta^b_{i+1}$-$LIND$, we show $\hat{T}^{i,\tau}_2$ proves $\Sigma^b_{0,\tau}(\hat{\Sigma}^b_i)$-$IND^{\dot{\tau}}$ provided $\tau \subseteq O_2(|id|)$. We use this together with Corollary 49 and our proof method for

$S^i_2$ to show that $\hat{T}^{i,\tau}_2$ proves $\hat{\Delta}^b_{i+1}$-$IND^{\dot{\tau}}$. In particular, 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 75, we give a proof theoretic proof that $S^i_2 \preceq_{B(\hat{\Sigma}^b_{i+1})} S^i_2 + \hat{\Pi}^b_i$-$REPL^{\{|id|\}}$. Together with the $\hat{\Delta}^b_{i+1}$-$LIND$ result this suffices to show $S^i_2$ proves $\Delta^b_{i+1}$-$LIND$ without relying on results not in this paper. The $\hat{R}^i_2$ result and the general result are new.

**Theorem 60** *($i \geq 1$) $S^i_2$ proves the $\Delta^b_{i+1}$-$LIND$ axioms.*

**PROOF.** By Buss [8], $S^i_2$ proves $\Sigma^b_0(\Sigma^b_i)$-$LIND$. Let $A$ be $\Delta^b_{i+1}$ with respect to $S^i_2$. Let $A_\Pi \in \Pi^b_{i+1}$ and let $A_\Sigma \in \Sigma^b_{i+1}$ be equivalent to $A$ in $S^i_2$. Consider $B(\mathbf{x}, y) :=$

$$(\neg A_\Pi(\mathbf{x}) \wedge y = 0) \vee (A_\Sigma(\mathbf{x}) \wedge y = 1).$$

Certainly, $S^i_2$ proves $(\forall \mathbf{x})(\exists y \leq 1) B(\mathbf{x}, y)$. Thus, by the witnessing theorem in [17] (which is similar to the $\tau = \{|id|\}$ case of Theorem 45), there is a $g \in FP^{\Sigma^p_i}(wit, \log)$ such that $S^i_2 \vdash Wit^{i+1}_{(\exists y \leq 1)B}(g(\mathbf{x}), \mathbf{x})$. So by the definition of the witness predicate, $S^i_2 \vdash Wit^{i+1}_B(\beta(2, g(\mathbf{x})), \mathbf{x}, \beta(1, g(\mathbf{x})))$ and also $S^i_2 \vdash Wit^{i+1}_B(w, \mathbf{x}, y) \supset B(\mathbf{x}, y)$. Thus, $S^i_2$ proves $B(\mathbf{x}, \beta(1, g(\mathbf{x})))$. Let $f(\mathbf{x}) = \beta(1, g(\mathbf{x}))$. Then $S^i_2$ proves $f(x) = 1 \Leftrightarrow A(x)$. This $f$ can be defined in $S^i_2$ using almost the same notion of $Q^{i,\{|id|\}}$-definition that we used in Section 3. That is, it can be defined with a formula of the form:

$$\begin{aligned} y \leq 1 \wedge (\exists v \leq p(|s(x)|))[&(\exists w \leq t)(Out(w, x) = y \wedge A(x, w, v)) \\ &\wedge \neg(\exists v' \leq p(|s(x)|))(\exists w' \leq t)(v' > v \wedge A(x, w', v'))]. \end{aligned}$$

where $A \in \Pi^b_{i-1}$ and where $s, Out \in L_2$. But this is a $\forall\Sigma^b_0(\Sigma^b_i)$-formula, so $S^i_2$ proves $LIND_{f(x)=1}$. As $S^i_2$ proves $f(x) = 1 \Leftrightarrow A(x)$, we also have $S^i_2$ proves $LIND_A$. Hence, $S^i_2$ proves $\Delta^b_{i+1}$-$LIND$. $\square$

We now modify the above to show $\hat{R}^i_2$ proves $\hat{\Delta}^b_i$-$LLIND$ and also that $\hat{T}^{i,\tau}_2$ proves $\hat{\Delta}^b_{i+1}$-$IND^{\dot{\tau}}$ provided $\tau \subseteq O_2(|id|)$. We first show $\hat{T}^{i,\tau}_2$ proves $\Sigma^b_{0,\tau}(\hat{\Sigma}^b_i)$-$IND^{\dot{\tau}}$. For this we use the next two theorems, which are modified from Buss [8]. First, we define a bit comprehension axiom.

**Definition 61** *Let $\tau \subseteq O_2(|id|)$. The $\Psi$-$COMP^\tau$ are the axioms $COMP^\ell_\alpha$:*

$$(\exists w)(\forall x \leq \ell(b))(\alpha(v, x) \Leftrightarrow Bit(x, w) = 1).$$

*where $\alpha \in \Psi$ and $\ell \in \tau$.*

**Theorem 62** *($i \geq 1$) Let $\tau \subseteq O_2(|id|)$. The theory $\hat{T}^{i,\tau}_2$ proves the $\hat{\Sigma}^b_i$-$COMP^{\dot{\tau}}$ axioms.*

**PROOF.** By the usual speed-up techniques it suffices to show $\hat{T}_2^{i,\tau}$ proves the $\hat{\Sigma}_i^b$-$COMP^\tau$ axioms. Let $A \in \hat{\Sigma}_i^b$. Define $B(n,v) :=$

$$(\exists w < 2^{S\ell(b)})(\exists w' \leq 2^{S(|w|)|w|})[(\forall j \leq |w|)(\hat{\beta}(0,|w|,w') = Bit(0,w) \wedge$$
$$\hat{\beta}(j+1,|w|,w') = \hat{\beta}(j,|w|,w') + Bit(j+1,w)) \wedge \hat{\beta}(|w|,|w|,w') = n$$
$$\wedge(\forall x \leq \ell(b))(Bit(x,w) = 1 \supset A(v,x))].$$

The first two lines of the above 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 26, $B$ is equivalent to a $\hat{\Sigma}_i^b$-formula. Further, $\hat{T}_2^{i,\tau} \vdash \neg B(\ell(b)+2,v)$, so it follows from $\hat{\Sigma}_i^b$-$IND^\tau$ that

$$\hat{T}_2^{i,\tau} \vdash (\exists n \leq \ell(b)+1)(B(n,v) \wedge \neg B(n+1,v)).$$

Thus, $\hat{T}_2^{i,\tau}$ proves there is a maximal $n$ such that $B(n,v)$ holds. The $w$ whose existence is asserted for this $n$ has bit $x$ turned on if and only if $A(v,x)$. $\square$

**Theorem 63** *($i \geq 1$) Let $\tau \subseteq O_2(|id|)$. Then $\hat{T}_2^{i,\tau}$ proves $\Sigma^b_{0,\tau}(\hat{\Sigma}_i^b)$-$IND^\tau$. In particular, $\hat{R}_2^i$ proves $\Sigma^b_{0,\{||id||\}}(\hat{\Sigma}_i^b)$-$LLIND$.*

**PROOF.** Using Remark 18, any $A(b,\mathbf{v}) \in \Sigma^b_{0,\tau}(\hat{\Sigma}_i^b)$ can be written as

$$(Q_1 x_1 \leq \ell_1(r_1)) \cdots (Q_n x_n \leq \ell_n(r_n)) B(A_1,\ldots,A_s).$$

where $A_j \in \hat{\Sigma}_i^b$, $\ell_i \in \dot{\tau}$, $r_i \in L_2$, and $B(A_1,\ldots,A_s)$ denotes a Boolean combination of $A_1,\ldots,A_s$. We assume $r_j$'s variables are among $\mathbf{v}$. By modifying Theorem 62, $\hat{T}_2^{i,\tau}$ proves there are $w_1,\ldots,w_s$ such that

$$(\forall x_1 \leq \ell_1(r_1)) \cdots (\forall x_n \leq \ell_n(r_n))[Bit(\langle \mathbf{x} \rangle, w_j) \Leftrightarrow A_j(\mathbf{x},\mathbf{v})].$$

Here $\langle \mathbf{x} \rangle$ denotes an $n$-tuple $\langle x_1,\ldots,x_n \rangle$. Thus, given $w_1,\ldots,w_s$, $A$ is equivalent to a $\hat{\Delta}_1^b$-formula. The theorem follows as $\hat{T}_2^{i,\tau}$ can thus prove $IND^\tau_A$. $\square$

The above two theorems show that $\hat{R}_2^i$ can prove $\hat{\Delta}^b_{i+1}$-$LLIND$ axioms and $\hat{T}_2^{i,\tau}$ can prove $\hat{\Delta}^b_{i+1}$-$IND^\tau$ axioms provided $\tau \subseteq O_2(|id|)$.

**Corollary 64** *($i \geq 1$) Let $\tau \subseteq O_2(|id|)$. $\hat{R}_2^i$ proves $\hat{\Delta}^b_{i+1}$-$LLIND$ and $\hat{T}_2^{i,\tau}$ proves $\hat{\Delta}^b_{i+1}$-$IND^\tau$.*

**PROOF.** The proof is the same as in Theorem 60. Given a $\hat{\Delta}^b_{i+1}$ in $\hat{T}_2^{i,\tau}$ predicate $B$, it is equivalent to a predicate $f(x) = 1$ of the form

$$(\exists v \leq \ell(s(x)))[(\exists w \leq t)(Out(w,x) = 1 \wedge A(x,w,v))$$
$$\wedge\neg(\exists v' \leq \ell(s(x)))(\exists w' \leq t)(v' > v \wedge A(x,w',v'))].$$

where $A \in \hat{\Pi}^b_{i-1}$, $\ell \in \dot{\tau}$. This is a $\Sigma^b_{0,\tau}(\hat{\Sigma}^b_i)$-formula so by Theorem 63, $\hat{T}^{i,\tau}_2$ can prove $IND^\tau_{f(x)=1}$. So we have $IND^\tau_B$. $\Box$

Another corollary of the proof of Theorem 63 is:

**Corollary 65** *($i \geq 1$) Let $\tau \subseteq O_2(|id|)$. The $\Sigma^b_{0,\tau}(\hat{\Sigma}^b_i)$-formulas are $\hat{\Delta}^b_{i+1}$ with respect to $\hat{T}^{i,\tau}_2$. The $\Sigma^b_{0,\{||id||\}}(\hat{\Sigma}^b_i)$-formulas are $\hat{\Delta}^b_{i+1}$ with respect to $\hat{R}^i_2$.*

**PROOF.** Let $A$ be as in the proof of Theorem 63. Let $B_j := Bit(\langle \mathbf{x} \rangle, w_j)$. For the $w_j$'s used in that proof, $\hat{T}^{i,\tau}_2$ proves $A' :=$

$$(Q_1 x_1 \leq \ell_1(r_1)) \cdots (Q_n x_n \leq \ell_n(r_n))B(B_1, \ldots, B_s)$$

equivalent to $A$. Using $REPL^\tau$ and working from the innermost quantifier out, $\hat{T}^{i,\tau}_2$ can prove $A'$ equivalent to a $\hat{\Sigma}^b_1$-formula $C(B_1, \ldots, B_s)$ and also to a $\hat{\Pi}^b_1$-formula $D(B_1, \ldots, B_s)$. For these particular $w_j$'s, $\hat{T}^{i,\tau}_2$ proves

$$C(A_1, \ldots, A_s) \Leftrightarrow C(B_1, \ldots, B_s) \Leftrightarrow D(B_1, \ldots, B_s) \Leftrightarrow D(A_1, \ldots, A_s) \Leftrightarrow A.$$

Finally, $C(A_1, \ldots, A_s)$ is equivalent if a $\hat{\Sigma}^b_{i+1}$-formula and $D(A_1, \ldots, A_s)$ is equivalent to a $\hat{\Pi}^b_{i+1}$-formula in $\hat{T}^{i,\tau}_2$. $\Box$

**Corollary 66** *($i \geq 1$) Let $\tau \subseteq O_2(|id|)$. The theory $\hat{T}^{i,\tau}_2$ proves the $\Sigma^b_{0,\tau}(\hat{\Sigma}^b_i)$-formulas can be written in the form*

$$(\exists v \leq \ell(s(x)))[A(x,v) \wedge \neg B(x, v+1)]$$

*where $A, B \in \hat{\Sigma}^b_i$, $\ell \in \dot{\tau}$ and $s \in L_2$.*

**PROOF.** This follows from Theorem 50 and Corollary 65. $\Box$

The author does not know if for arbitrary set of iterms $\tau$, whether $\hat{T}^{i,\tau}_2$ proves $\hat{\Delta}^b_{i+1}$-$IND^\tau$, but the next theorem gives additional $\tau$'s for which this result holds.

**Theorem 67** *($i \geq 1$) Let $\tau \subseteq O_2(|id|)$. $\hat{T}^{i,2^{\dot{\tau}}}_2 \vdash \hat{\Delta}^b_{i+1}$-$IND^{2^{\dot{\tau}}}$.*

**PROOF.** Let $A$ be $\hat{\Delta}^b_{i+1}$ in $\hat{T}^{i,2^{\dot{\tau}}}_2$. Let $A_\Sigma \in \hat{\Sigma}^b_{i+1}$ and $A_\Pi \in \hat{\Pi}^b_{i+1}$ be equivalent to $A$ in $\hat{T}^{i,2^{\dot{\tau}}}_2$. Let $\ell \in \tau$, $t \in L_2$. Then

$$A_\Pi(0) \wedge (\forall x \leq 2^{\min(\ell(b),|t(b)|)})(A_\Sigma \supset A_\Pi) \supset A_\Sigma(\ell(b))$$

is a $\hat{\Sigma}^b_{i+1}$-formula. Since $\hat{T}^{i+1,\tau}_2$ proves the $\hat{\Delta}^b_{i+1}$-$IND^{2^{\dot{\tau}}}$ axioms by Theorem 27 and Theorem 22 we have $\hat{T}^{i+1,\tau}_2 \vdash IND^{2^{\min(\ell(b),|t(b)|)}}_A$. But then by Theorem 57, $\hat{T}^{i,2^{\dot{\tau}}}_2 \vdash IND^{2^{\min(\ell(b),|t(b)|)}}_A$. $\square$

## 6 Prenex replacement theories

We now study $\hat{C}^{i,\tau}_2$, which we defined in Section 2. Let $\tau \subseteq O_2(|id|)$. We show $\hat{T}^{i,\tau}_2 \preceq_{B(\hat{\Sigma}^b_{i+1})} \hat{C}^{i,\tau}_2$. Our proof is then used to show for $i \geq 1$ that $\hat{T}^{i+1,||\tau||}_2 \preceq_{B(\hat{\Sigma}^b_{i+1})} \hat{T}^{i+1,||\tau||}_2 + \hat{\Pi}^b_i$-$REPL^{|\tau|}$. This shows that $\hat{R}^{i+1}_2 \preceq_{B(\hat{\Sigma}^b_{i+1})} R^{i+1}_2$ for $i \geq 1$. We delayed this section until now as our witness predicate is different from earlier sections and we did not want to cause undue confusion by switching between two types of witness predicate.

### *6.1 Preliminaries*

We begin with the following theorem.

**Theorem 68** *($i \geq 0$) Let $\tau \subseteq O_2(|id|)$. Then $\hat{C}^{i,\tau}_2 \vdash \hat{T}^{i,\tau}_2$.*

**PROOF.** The proof is the same as the proof in Buss [7] that $S^i_2$ is contained in $S^1_2$+$\Sigma^b_{i+1}$-$REPL$. $\square$

To show $\hat{T}^{i,\tau}_2 \preceq_{B(\hat{\Sigma}^b_{i+1})} \hat{C}^{i,\tau}_2$ we first show $\hat{T}^{i,\tau}_2 \preceq_{\hat{\Sigma}^b_{i+1}} \hat{C}^{i,\tau}_2$. We need to show that $FP^{\Sigma^p_i}(wit, |\tau|)$ is closed under a certain kind of parallel computation.

**Theorem 69** *($i \geq 1$) Let $\ell \in O_2(|id|)$ and $\ell \in O_2(\ell_2)$ for some $\ell_2 \in \dot{\tau}$. Let $f(j, \mathbf{x})$ be $Q^{i,\dot{\tau}}$-definable in $\hat{T}^{i,\tau}_2$ and suppose $f$ is bounded by $t^*(\mathbf{x}) \in L_2$ for $j \leq \ell(h(\mathbf{x}))$, $h \in L_2$. Then:*

*(a) $f_\ell(\mathbf{x}) = \sum_{j=0}^{\ell-1} f(j, \mathbf{x}) \cdot 2^{j \cdot |t^*|}$ is $Q^{i,\dot{\tau}}$-definable in $\hat{T}^{i,\tau}_2$.*

*(b) $\hat{T}^{i,\tau}_2$ proves $\hat{\beta}(j, |t^*|, f_\ell(\mathbf{x})) = f(j, \mathbf{x})$ where this is translated into the language of $L_2$ using Definition 30 and where $f_\ell$ is interpreted using the $Q^{i,\dot{\tau}}$-definition from (a).*

**PROOF.** For (a) suppose $f$ is $Q^{i,\dot{\tau}}$-defined by

$$B(j,\mathbf{x},y) := (\exists v \le s(r(\mathbf{x})))[(\exists w' \le q)(Out(w',j,\mathbf{x}) = y \wedge A(j,\mathbf{x},w',v)) \\ \wedge\neg(\exists v' \le s(r(\mathbf{x})))(\exists w'' \le q)(v' > v \wedge A(j,\mathbf{x},w'',v'))]$$

where $s \in \dot{\tau}$, $q, r \in L_2$. Notice we are assuming that $r$ does not depend on $j$. We can do this without loss of generality since we are only considering values $j \le \ell(h(\mathbf{x}))$. Define $C(u) := (\exists w \le 2 \cdot (\ell(h)\#t^*))(\forall j \le \ell(h))D$ where $D$ is

$$(\exists v \le s(r))(A(j,\mathbf{x},\dot{\beta}(j,|t^*|,q,w),v) \wedge v \ge \hat{\beta}(j,|s(r)|,u)).$$

$\hat{T}_2^{i,\tau}$ proves $C$ is a $\hat{\Sigma}_i^b$-formula by Lemma 17 and Theorem 22 since $A$ is $\hat{\Sigma}_i^b$ and since $\ell$ is both $O_2(|id|)$ and $\ell \in O_2(\ell_2)$ for some $\ell_2 \in \dot{\tau}$. Using the properties of $Q^{i,\dot{\tau}}$-definition when $v$ is 0, the theory $\hat{T}_2^{i,\tau}$ proves $A$ equivalent to a $\hat{\Pi}_0^b$-formula. Also, $\hat{T}_2^{i,\tau}$ proves $(\forall j \le \ell(h))(\exists w' \le q)A(j,\mathbf{x},w',0)$. So using $\hat{\Pi}_0^b$-$REPL^{\{\ell\}}$, the theory $\hat{T}_2^{i,\tau}$ proves $C(0)$. The theory $\hat{T}_2^{i,\tau}$ also proves $\neg C(2 \cdot (s(r) \cdot \ell(h)) + 1)$. Using $IND_C^{\dot{\tau}}$, we thus have

$$(\exists u \le 2 \cdot (s(r) \cdot \ell(h)))(C(u) \wedge \neg C(u+1)). \tag{9}$$

$\hat{T}_2^{i,\tau}$ proves for this $u$ and for each $j \le \ell(s)$ there is not a $v' \ge \hat{\beta}(j,|s(r)|,u))$ such that we could satisfy $A$ with $v'$ and some other $w'$. (If there were such a $v'$ we could modify $u$ to obtain a larger value for $u$ such that $C$ held.) So $\hat{T}_2^{i,\tau}$ proves $Out(\dot{\beta}(j,|t^*|,q,w),j,\mathbf{x})$ is an output of $f(j,\mathbf{x})$. Using $\hat{\Sigma}_1^b$-$IND^{\tau}$, the theory $\hat{T}_2^{i,\tau}$ can define a function $g$ which given $w$ produces a $y$ such that $\hat{\beta}(j,|t^*|,y) = Out(\dot{\beta}(j,|t^*|,q,w),j,\mathbf{x})$ for all $j \le \ell(h)$. A $\hat{\Sigma}_1^b$-defined function is trivially $Q^{i,\dot{\tau}}$-defined in $\hat{T}_2^{i,\tau}$. So we can define $f_\ell$ using Lemma 38, where we use (9) to $Q^{i,\dot{\tau}}$-define a multifunction outputting $w$ and then compose it with $g$. The statement (b) above is easily verified from our $Q^{i,\dot{\tau}}$-definition. □

We also need the $Q^{i,\dot{\tau}}$-definable multifunctions of $\hat{T}_2^{i,\tau}$ are closed under $\dot{\tau}$-bounded $\mu$-operator.

**Theorem 70** *($i \ge 1$) Let $\tau \in O_2(|id|)$ and let $f$ be a $Q^{i,\dot{\tau}}$-definable multifunctions of $\hat{T}_2^{i,\tau}$. 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

$$g(j,x) := cond((\exists n < \ell(x))(n < j \wedge f(n,x) = 0), 1, 0).$$

Define $(\mu i < \ell(x))[f(i,x) = 0]$ to be $|\sum_{j=0}^{\ell(x)-1} g(j,x) \cdot 2^j| \dot{-} 1$. The condition in the *cond* is equivalent to a $\Sigma^b_{0,\tau}(\hat{\Sigma}^b_i)$-formula since $f(n,x) = 0 \Leftrightarrow B(n,x,0)$ where $B$ is the $Q^{i,\dot{\tau}}$-definition of $f$. So it will be $Q^{i,\dot{\tau}}$-defined in $\hat{T}^{i,\tau}_2$ by Corollary 65, Corollary 49, and Theorem 35. $\Box$

### *6.2 Witnessing arguments for replacement theories*

We use a witnessing argument to show $\hat{T}^{i,\tau}_2 \preceq_{\hat{\Sigma}^b_{i+1}} \hat{C}^{i,\tau}_2$ provided $\tau \subseteq O_2(|id|)$. By Theorem 42, a free-cut free $\hat{C}^{i,\tau}_2$-proof of an $E\hat{\Sigma}^b_{i+1}$-formula has formulas in $LE\hat{\Sigma}^b_{i+1} \cup LA_\tau\hat{\Sigma}^b_{i+1} \cup LEA_\tau\hat{\Pi}^b_i$. Our witness predicate is as before except with the three additional cases:

If $A(\mathbf{a}) \in A_\tau\hat{\Pi}^b_i$ then $Wit^{i+1}_A(w,\mathbf{a}) := w = 0 \wedge A$.

If $A(\mathbf{a})$ is of the form $(\exists x \leq t(\mathbf{a}))B$ where $A \in \hat{\Sigma}^b_{i+1} \cup EA_\tau\hat{\Pi}^b_i$ then

$$Wit^{i+1}_A(w,\mathbf{a}) := b \leq t(\mathbf{a}) \wedge B(b,\mathbf{a}).$$

If $A(\mathbf{a})$ is $(\forall x \leq \ell(s))(\exists y \leq t)B$ where $A \in A_\tau\hat{\Sigma}^b_{i+1}$, then

$$Wit^{i+1}_A(w,\mathbf{a}) :=$$
$$w \leq 2 \cdot (t^*(\ell(s),\mathbf{a})\#\ell(s)) \wedge (\forall x \leq |\ell(s)|)B(\dot{\beta}(x, |t^*(\ell(s),\mathbf{a})|, t(x,\mathbf{a}),\mathbf{a}).$$

For the above definitions, the analog of Lemma 43 is:

**Lemma 71** *($i \geq 1$) Let $\tau \subseteq O_2(|id|)$ and let $A \in LE\hat{\Sigma}^b_{i+1} \cup LA_\tau\hat{\Sigma}^b_{i+1} \cup LEA_\tau\hat{\Pi}^b_i$ with free variables $\mathbf{a}$. Then: $EBASIC \vdash Wit^{i+1}_A(w,\mathbf{a}) \supset A(\mathbf{a})$ and there is a term $t_A$ such that*

$$\hat{C}^{i,\tau}_2 \vdash A(\mathbf{a}) \Leftrightarrow (\exists w \leq t_A(\mathbf{a}))Wit^{i+1}_A(w,\mathbf{a}). \tag{10}$$

*For this $t_A$, we also have $EBASIC \vdash Wit^{i+1}_A(w,\mathbf{a}) \supset w \leq t_A$.*

**Remark 72** *If $A \in LE\hat{\Sigma}^b_{i+1}$ then (10) requires only $EBASIC$ to prove.*

We extend the definition of witness for a formula to a definition for witness for a cedent as before. A lemma similar to the above also holds for cedents.

**Theorem 73** *($i \geq 1$) Let $\tau \subseteq O_2(|id|)$. Suppose $\hat{C}^{i,\tau}_2 \vdash \Gamma \rightarrow \Delta$ where $\Gamma$ and $\Delta$ are cedents of formulas in $LE\hat{\Sigma}^b_{i+1} \cup LA_\tau\hat{\Sigma}^b_{i+1} \cup LEA_\tau\hat{\Pi}^b_i$ with free variables*

*among* $\mathbf{a}$. *Then there is a* $f \in FP^{\Sigma_i^p}(wit, |\tau|)$ *which is* $Q^{i,\dot{\tau}}$*-defined in* $\hat{T}_2^{i,\tau}$ *such that:*

$$\hat{T}_2^{i,\tau} \vdash Wit^{i+1}_{\wedge\Gamma}(w, \mathbf{a}) \supset Wit^{i+1}_{\vee\Delta}(f(w, \mathbf{a}), \mathbf{a}).$$

**PROOF.** This is proved by induction on a $\hat{C}_2^{i,\tau}$ proof of $\Gamma \to \Delta$. By cut elimination, we assume the sequents in the proof are in $LE\hat{\Sigma}^b_{i+1} \cup LA_\tau\hat{\Sigma}^b_{i+1} \cup LEA_\tau\hat{\Pi}^b_i$. Almost all cases are handled as in the witnessing argument for $\hat{T}_2^{i,\tau}$. However, the $\forall$ : cases change, and we have an additional case for $REPL^\tau$-inferences.

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

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

By hypothesis there is a $Q^{i,\dot{\tau}}$-definable $g$ such that

$$\hat{T}_2^{i,\tau} \vdash Wit^{i+1}_{A(t)\wedge\Gamma}(w, \mathbf{a}) \supset Wit^{i+1}_{\vee\Delta}(g(w, \mathbf{a}), \mathbf{a}).$$

The definition of $Wit^{i+1}$ implies

$$\hat{T}_2^{i,\tau} \vdash Wit^{i+1}_{t\leq s\wedge(\forall x\leq s)A(x)\wedge\Gamma}(w, \mathbf{a}) \supset t \leq s \wedge Wit^{i+1}_{(\forall x\leq s)A(x)\wedge\Gamma}(\beta(2, w), \mathbf{a}).$$

By cut-elimination, $(\forall x \leq s)A(x)$ is in $LA_\tau\hat{\Pi}^b_i$ or in $A_\tau\hat{\Sigma}^b_{i+1}$. In the first case, define $f$ to be $f(w, \mathbf{a}) := g(\langle 0, \beta(2, \beta(2, w))\rangle, \mathbf{a})$. This function is $Q^{i,\dot{\tau}}$-definable in $\hat{T}_2^{i,\tau}$ and also

$$\hat{T}_2^{i,\tau} \vdash Wit^{i+1}_{t\leq s\wedge(\forall x\leq s)A(x)\wedge\Gamma}(w, \mathbf{a}) \supset Wit^{i+1}_{\vee\Delta}(f(w, \mathbf{a}), \mathbf{a}).$$

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 $\ell \in \tau$ and $A$ is of the form $(\exists y \leq v(x, \mathbf{a}))B$ where $B \in \hat{\Pi}^b_i$. Let $h(w, \mathbf{a}) := \langle \dot{\beta}(t, |v^*(\ell(s'), \mathbf{a})|, v(t, \mathbf{a}), \beta(1, \beta(2, w))), \beta(2, \beta(2, w))\rangle$. Then by the definition of witness,

$$\hat{T}_2^{i,\tau} \vdash Wit^{i+1}_{t\leq s\wedge(\forall x\leq s)A(x)\wedge\Gamma}(w, \mathbf{a}) \supset Wit^{i+1}_{A(t)\wedge\Gamma}(h(w, \mathbf{a}), \mathbf{a})$$

and $f(w, \mathbf{a}) := g(h(w, \mathbf{a}), \mathbf{a})$ has the desired witnessing properties.

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

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

By hypothesis there is a $Q^{i,\dot{\tau}}$-definable $g \in FP^{\Sigma_i^p}(wit, |\tau|)$ such that

$$\hat{T}_2^{i,\tau} \vdash Wit^{i+1}_{b \leq t \wedge \Gamma}(w, \mathbf{a}, b) \supset Wit^{i+1}_{A \vee \Delta}(g(w, \mathbf{a}, b), \mathbf{a}, b).$$

By cut-elimination, $(\forall x \leq t)A(x)$ is in $LA_\tau \hat{\Pi}_i^b$ or is in $A_\tau \hat{\Sigma}_{i+1}^b$. In the first case, $(\exists x \leq t)\neg A(x)$ is a $\Sigma_i^p$-predicate. So we can ask an oracle for a value $b \leq t$ such that $\neg A(b)$ holds. If such a value exists set $f(w, \mathbf{a}) = g(\langle 0, w\rangle, \mathbf{a}, b)$. If no such value exists let $f(w, \mathbf{a}) = \langle 0, 0\rangle$ since $(\forall x \leq t)A(x)$ would be a valid $LA_\tau \hat{\Pi}_i^b$-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 $B \in \hat{\Pi}_i^b$. By the comment just before Lemma 44, $Wit_A^{i+1}$ as a $0-1$ valued function is $Q^{i,\dot{\tau}}$-definable in $\hat{T}_2^{i,\tau}$. Let $k$ be

$$k(w, \mathbf{a}) = (\mu j \leq \ell(s))[\neg Wit_A^{i+1}(\beta(1, g(w, \mathbf{a}, j)), \mathbf{a}, j) = 0].$$

By Theorem 70, Lemma 37, and Lemma 38, $k$ is $Q^{i,\dot{\tau}}$-defined in $\hat{T}_2^{i,\tau}$ and in $FP^{\Sigma_i^p}(wit, |\tau|)$. Define $f(w, \mathbf{a}) :=$

$$cond(K_=(k, \ell(s)+1), \langle \sum_{j=0}^{\ell(s)} \beta(1, g(w, \mathbf{a}, j)) \cdot 2^{j \cdot |(t')^*(\ell(s), \mathbf{a})|}, 0\rangle, g(w, \mathbf{a}, k).$$

Using Theorem 69, $\hat{T}_2^{i,\tau} \vdash Wit_\Gamma^{i+1}(w, \mathbf{a}) \supset Wit^{i+1}_{(\forall x \leq \ell(s))A \vee \Delta}(f(w, \mathbf{a}), \mathbf{a})$.

**($\hat{\Pi}_i^b - REPL^\tau$:case)** Suppose we have the inference:

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

where $\ell \in \tau$ and $s \in L_2$. By hypothesis there is a $g \in FP^{\Sigma_i^p}(wit, |\tau|)$ which is $Q^{i,\dot{\tau}}$-definable in $\hat{T}_2^{i,\tau}$ such that

$$\hat{T}_2^{i,\tau} \vdash Wit_\Gamma^{i+1}(w, \mathbf{a}) \supset Wit^{i+1}_{(\forall x \leq \ell(s))(\exists y \leq t)A \vee \Delta}(g(w, \mathbf{a}), \mathbf{a}).$$

Notice that $Wit^{i+1}_{(\forall x \leq \ell(s))(\exists y \leq t)A}$ and $Wit^{i+1}_{(\exists w \leq 2 \cdot (t^*(\ell(s)) \# 2^{\min(\ell(s), |s|)}))(\forall x \leq \ell(s))A}$ are the same. Hence, if we let $f = g$ then

$$\hat{T}_2^{i,|\tau|} \vdash Wit_\Gamma^{i+1}(w, \mathbf{a}, b) \supset Wit^{i+1}_{(\exists w \leq 2 \cdot (t^*(\ell(s)) \# 2^{\min(\ell(s), |s|)}))(\forall x \leq \ell(s))A \vee \Delta}(f(w, \mathbf{a}), \mathbf{a}).$$

This completes the remaining cases and the proof. $\Box$

**Theorem 74** *($i \geq 1$) If $\hat{T}_2^{i+1, ||\tau||} + \hat{\Pi}_i^b\text{-}REPL^{|\tau|} \vdash \Gamma \rightarrow \Delta$ where $\Gamma$ and $\Delta$ are cedents of formulas in*

$$LE\hat{\Sigma}_{i+1}^b \cup LA_{|\tau|}\hat{\Sigma}_{i+1}^b \cup LEA_{|\tau|}\hat{\Pi}_i^b.$$

*with free variables among* $\mathbf{a}$*, then there is a* $f \in FP^{\Sigma_i^p}(wit, (||\dot{\tau}||))$ *which is* $Q^{i,2^{(||\dot{\tau}||)}}$*-defined in* $\hat{T}_2^{i,2^{(||\dot{\tau}||)}}$ *such that:*

$$\hat{T}_2^{i,2^{(||\dot{\tau}||)}} \vdash Wit^{i+1}_{\wedge\Gamma}(w, \mathbf{a}) \supset Wit^{i+1}_{\vee\Delta}(f(w, \mathbf{a}), \mathbf{a}).$$

**PROOF.** This is proved by induction on the number of sequents in an

$$\hat{T}_2^{i+1,||\tau||}{+}\hat{\Pi}_i^b\text{-}REPL^{|\tau|}$$

proof of $\Gamma \to \Delta$. By cut elimination, we assume all the sequents in the proof are in $LE\hat{\Sigma}^b_{i+1} \cup LA_{|\tau|}\hat{\Sigma}^b_{i+1} \cup LEA_{|\tau|}\hat{\Pi}^b_i$. We handle all cases of this witnessing argument as in Theorem 73 above except for the ($\hat{\Sigma}^b_{i+1}$-$IND^{||\tau||}$) case which we handle as in Theorem 46. $\Box$

**Corollary 75** $(i \geq 1)$

*(a)* $\hat{T}_2^{i,\tau} \preceq_{B(\hat{\Sigma}^b_{i+1})} \hat{C}_2^{i,\tau}$ *provided* $\tau \subseteq O_2(|id|)$.

*(b)* $\hat{T}_2^{i,2^{(||\dot{\tau}||)}} \preceq_{B(\hat{\Sigma}^b_{i+1})} \hat{T}_2^{i+1,||\tau||} \preceq_{B(\hat{\Sigma}^b_{i+1})} \hat{T}_2^{i+1,||\tau||}{+}\hat{\Pi}_i^b\text{-}REPL^{|\tau|}$.

*(c)* $\hat{R}_2^{i+1} \preceq_{B(\hat{\Sigma}^b_{i+1})} R_2^{i+1}$.

*(d)* $S_2^i \preceq_{B(\hat{\Sigma}^b_{i+1})} S_2^i{+}\Pi_i^b\text{-}REPL^{\{|id|\}}$.

**PROOF.** By Remark 72 and the method of Theorem 57 it suffices to show $\hat{\Sigma}^b_{i+1}$-conservativety. (a) Suppose $\hat{C}_2^{i,\tau} \vdash (\exists x \leq t)A(x, \mathbf{a})$ where $A$ is $\hat{\Pi}^b_i$. Then by Theorem 73, $\hat{T}_2^{i,\tau} \vdash Wit^{i+1}_{(\exists x \leq t)A}(f(x, \mathbf{a}), \mathbf{a})$. By Lemma 71,

$$\hat{T}_2^{i,\tau} \vdash Wit^{i+1}_{(\exists x \leq t)A}(w, \mathbf{a}) \supset (\exists x \leq t)A(x, \mathbf{a}).$$

So $\hat{T}_2^{i,\tau} \vdash (\exists x \leq t)A(x, \mathbf{a})$.

(b) Follows from Theorem 74 by the same argument as in (a). Recall that by Theorem 27, $\hat{T}_2^{i,2^{(||\dot{\tau}||)}} \subseteq \hat{T}_2^{i+1,||\tau||}$.

(c) Follows from the $\tau = \{id\}$ case of (b) and Theorem 23.

(d) Follows from the $\tau = \{id\}$ case of (a) and since $S_2^i$ proves every $\Pi^b_i$-formula is equivalent to a $\hat{\Pi}^b_i$-formula. In [23], this result was strengthened to $S_2^i{+}\Sigma^b_{i+1}$-$REPL^{\{|id|\}}$ is $B(\hat{\Sigma}^b_{i+1})$-conservative over $S_2^i$. $\Box$

The above corollary does not imply that $\hat{T}_2^{i,\tau} = \hat{C}_2^{i,\tau}$ since $\hat{T}_2^{i,\tau}$ does not necessarily prove that any $\hat{\Pi}_i^b$-$REPL^\tau$ axiom is equivalent to a $B(\hat{\Sigma}_{i+1}^b)$-formula. Similarly, the above result does not imply $R_2^i$ equals $\hat{R}_2^i$.

We now consider $\hat{\Sigma}_{i+k}^b$-definability in $\hat{C}_2^{i,\tau}$ for $k > 1$ and where $\tau \subseteq O_2(|id|)$. Since $EBASIC \subseteq \hat{C}_2^{i,\tau}$, it can define the multifunctions in $FP^{\Sigma_{i+k-1}^p}(wit, 1)$. For the converse, consider any proof of a sequent of formulas in

$$LE\hat{\Sigma}_{i+k}^b \cup LA_\tau\hat{\Sigma}_{i+1}^b \cup LEA_\tau\hat{\Pi}_i^b.$$

For formulas not in $E\hat{\Sigma}_{i+k}^b \cup \hat{\Sigma}_{i+k}^b$, we let the witness predicate just be the formula itself. Otherwise, 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 $\hat{\Sigma}_{i+1}^b$-definability section (they will both be equivalent for the remaining cases).

**Theorem 76** *($i \geq 1, k \geq 2$) Let $\tau \subseteq O_2(|id|)$. If $\hat{C}_2^{i,\tau} \vdash \Gamma \rightarrow \Delta$ where the formulas in $\Gamma$ and $\Delta$ are cedents of formulas in $LE\hat{\Sigma}_{i+k}^b \cup LA_\tau\hat{\Sigma}_{i+1}^b \cup LEA_\tau\hat{\Pi}_i^b$ with free variables among $\mathbf{a}$, then there is a $f \in FP^{\Sigma_{i+k-1}^p}(wit, 1)$ which is $Q^{i+k-1,cl}$-definable in $\hat{C}_2^{i,\tau}$ such that:*

$$\hat{C}_2^{i,\tau} \vdash Wit_{\wedge\Gamma}^{i+k}(w, \mathbf{a}) \supset Wit_{\vee\Delta}^{i+k}(f(w, \mathbf{a}), \mathbf{a}).$$

*When $i = 0$ there is a $f \in FP^{\Sigma_{k-1}^p}(wit, 1)$ such that*

$$\mathbb{N} \models Wit_{\wedge\Gamma}^{k}(w, \mathbf{a}) \supset Wit_{\vee\Delta}^{k}(f(w, \mathbf{a}), \mathbf{a}).$$

**PROOF.** All the cases are handled in the same way as in the $\hat{\Sigma}_{i+1}^b$-witnessing argument except the ($\hat{\Pi}_i^b - REPL^\tau$: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, the next theorem and its corollaries follow by the type of proof used in Section 3.

**Theorem 77** *($i \geq 0, k \geq 2$) Let $\tau \subseteq O_2(|id|)$. The $\hat{\Sigma}_{i+k}^b$-definable multifunctions of $\hat{C}_2^{i,\tau}$ are precisely the class $FP^{\Sigma_{i+k-1}^p}(wit, 1)$. The $\hat{\Delta}_{i+k}^b$-predicates of $\hat{C}_2^{i,\tau}$ are precisely the predicates in $P^{\Sigma_{i+k-1}^p}(1)$ and can be written in the form*

$$\vee_{v=0}^n[A(x, S^v(0)) \wedge \neg B(x, S^{v+1}(0))]$$

*where $A, B \in \hat{\Sigma}_{i+k-1}^b$ and $n$ is a fixed integer. Here $S^0(0) = 0$ and $S^{v+1}(0) = S(S^v(0))$.*

**Remark 78** *From the above theorem it follows that the $\hat{\Sigma}^b_j$-definable multifunctions of $\hat{T}^{i,\tau}_2$ and $\hat{C}^{i,\tau}_2$ are the same for all $j$ and yet these theories are not as far as we know equal. This is the example mentioned in the introduction.*

One last interesting question about prenex replacement theories is the following: Does $T^i_2$ contain $\hat{C}^{i,\tau}_2$ for some $\tau$ containing an unbounded iterm? Obviously, since $T^i_2 = \hat{T}^{i,\{id\}}_2$, it contains the theories $\hat{T}^{i,\tau}_2$ for all $\tau \subseteq O_2(|id|)$. 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 some $\tau$ containing an unbounded term.

### *6.3 Summary of structural and definability results*

This subsection contains two tables summarising the principle definability and structural results obtained so far in this paper.

| | $\hat{\Delta}^b_{i+1-j}$ $(i > j \geq 0)$ | $\hat{\Delta}^b_{i+k}$ $(i \geq 1, k > 1)$ |
|---|---|---|
| $\hat{T}^{i,\tau}_2$ | $P^{\Sigma^p_i}(\|2 \uparrow j(\tau)\|)$ if $\tau \subseteq O_2(\|id\|_j)$ | $P^{\Sigma^p_{i+k-1}}(1)$ |
| $\hat{C}^{i,\tau}_2$ | $P^{\Sigma^p_i}(\|2 \uparrow j(\tau)\|)$ if $\tau \subseteq O_2(\|id\|_j)$ | $P^{\Sigma^p_{i+k-1}}(1)$ |
| | and $\tau \subseteq O_2(\|id\|)$ | |
| $T^i_2$ | $P^{\Sigma^p_i}$ if $j = 0$ | $P^{\Sigma^p_{i+k-1}}(1)$ |
| $S^i_2$ | $P^{\Sigma^p_i}(\log)$ | $P^{\Sigma^p_{i+k-1}}(1)$ |
| | $P^{\Sigma^p_{i-1}}$ if $j = 1, i > 1$ | |
| $R^i_2$ | $P^{\Sigma^p_i}(\log\log)$ $j = 0$ | $P^{\Sigma^p_{i+k-1}}(1)$ |
| | $P^{\Sigma^p_{i-1}}(\log^{O(1)})$ $j = 1$ | |
| $EBASIC$ | $P^{\Sigma^p_{i-j}}(O(1))$ | $P^{\Sigma^p_{i+k-1}}(1)$ |

The corresponding $\hat{\Sigma}^b_{i+1}$-definability results are obtained by adding an 'F' in front of a class and a 'wit' inside the parentheses. The above table follows from Corollary 49 and Corollary 58.

| General Result ($i \geq 1$, $\tau \subseteq O_2(\lvert id\rvert)$) | Application ($i \geq 1$) |
|---|---|
| $\hat{T}_2^{i,\{\ell\}} \subseteq \hat{T}_2^{i,\{\ell'\}}$ if $\ell \in O_2(\ell')$ | $\hat{R}_2^i \subseteq S_2^i \subseteq T_2^i$ |
| $\hat{T}_2^{i,2^{\dot{\tau}}} \preceq_{B(\hat{\Sigma}_{i+1}^b)} \hat{T}_2^{i+1,\tau}$ | $T_2^i \preceq_{B(\hat{\Sigma}_{i+1}^b)} S_2^{i+1}$ |
| | $\hat{T}_2^{i,2^{\{\lvert\lvert i\dot{d}\rvert\rvert\}}} \preceq_{B(\hat{\Sigma}_{i+1}^b)} \hat{R}_2^i$ |
| $\hat{T}_2^{i+1,\lvert\lvert\tau\rvert\rvert} \preceq_{B(\hat{\Sigma}_{i+1}^b)} \hat{T}_2^{i+1,\lvert\lvert\tau\rvert\rvert} + \hat{\Pi}_i^b\text{-}REPL^{\lvert\tau\rvert}$ | $\hat{R}_2^i \preceq_{B(\hat{\Sigma}_{i+1}^b)} R_2^i$ |
| $\hat{C}_2^{i-1,\tau} \subseteq \hat{T}_2^{i,\tau} \preceq_{B(\hat{\Sigma}_{i+1}^b)} \hat{C}_2^{i,\tau}$ | $S_2^i \preceq_{B(\hat{\Sigma}_{i+1}^b)} S_2^i + \hat{\Pi}_i^b\text{-}REPL$ |
| $\hat{T}_2^{i,\tau} \vdash \hat{\Sigma}_i^b\text{-}COMP^{\dot{\tau}}$ | $S_2^i \vdash \hat{\Sigma}_i^b\text{-}COMP^{\{\lvert i\dot{d}\rvert\}}$ |
| | $R_2^i \vdash \hat{\Sigma}_i^b\text{-}COMP^{\{\lvert\lvert i\dot{d}\rvert\rvert\}}$ |
| $\hat{T}_2^{i,\tau} \vdash \hat{\Delta}_{i+1}^b\text{-}IND^{\tau}$ | $S_2^i \vdash \hat{\Delta}_{i+1}^b\text{-}LIND$ |
| | $R_2^i \vdash \hat{\Delta}_{i+1}^b\text{-}LLIND$ |
| $\hat{T}_2^{i,2^{\dot{\tau}}} \vdash \hat{\Delta}_{i+1}^b\text{-}IND^{2^{\dot{\tau}}}$ | $T_2^i \vdash \hat{\Delta}_{i+1}^b\text{-}IND$ |
| $\hat{T}_2^{i,\tau} \vdash \Sigma_{0,\tau}^b(\hat{\Sigma}_i^b) \subseteq \hat{\Delta}_{i+1}^b$ | $S_2^i \vdash \Sigma_0^b(\hat{\Sigma}_i^b) \subseteq \hat{\Delta}_{i+1}^b$ |
| | $R_2^i \vdash \Sigma_{0,\{\lvert\lvert id\rvert\rvert\}}^b(\hat{\Sigma}_i^b) \subseteq \hat{\Delta}_{i+1}^b$ |
| $\hat{T}_2^{i,\tau} \vdash \forall A \in \hat{\Delta}_{i+1}^b \exists A' \in E_\tau(\hat{\Sigma}_i^b \wedge \hat{\Pi}_i^b)(A \Leftrightarrow A')$ | |

By the last line in the table, we mean Corollary 50. By $\hat{T}_2^{i,\tau} \vdash \Sigma_{0,\tau}^b(\hat{\Sigma}_i^b) \subseteq \hat{\Delta}_{i+1}^b$ we mean Corollary 65. The remaining lines in the above table follow from Corollary 12, Theorem 57, Corollary 75, Theorem 20, Theorem 62, Corollary 64, and Theorem 67.

## 7 Collapses and oracle separations

This section gives evidence that certain relationships do not hold between the bounded arithmetic theories we have been considering. We 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 $\tau, \tau' \subseteq O_2(\lvert id\rvert)$ and $\tau'$ contains at least one unbounded iterm then $PH = B(\Sigma_{i+2}^p)$. It was known from Krajíček, Pudlak, and Takeuti [19] that if $T_2^i = S_2^{i+1}$ the polynomial hierarchy collapses to the $(i+2)$nd level. Buss [9] and Zambella [29] 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 characterisations of the $\hat{\Delta}_{i+2}^b$-predicates of these theories. One can generalise Krajíček, Pudlak, and Takeuti [19]'s combinatorics to get the first two statements imply the hierarchy collapses; however, the third statement seems harder to show. We then devote a couple subsections to giving an oracle $X$ such that $P^{\Sigma_i^p(X)}(\{\lvert\lvert\ell\rvert\rvert\})$

is contained in but not equal to $P^{\Sigma_i^p(X)}(\{||\ell||^2\})$ where $\ell$ is a nondecreasing, unbounded iterm. This result implies many oracle separations. Some of these results were obtained independently by Arnold Beckmann in his Ph.D. thesis [2] using a technique called "dynamic ordinal analysis". Lastly, we give a result concerning models separating theories.

### *7.1 Hierarchy collapses*

In this subsection, we use brackets in expressions like $P^{\Sigma_i^p}[k]$ to denote at most $k$ queries to a $\Sigma_i^p$-oracle and use parentheses such as $P^{\Sigma_i^p}(k)$ to mean $O(k)$ queries. From Hemaspaadra, Hemaspaadra, and Hempel [14,15] and Buhrman and Fortnow [4] it is known that $P^{\Sigma_i^p}[k] = P^{\Sigma_i^p}[k+1]$ implies $PH = B(\Sigma_{i+2}^p)$. Here $k$ is a fixed number. Let $\ell$ 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 $B(\Sigma_{i+2}^p)$. Let $\tau$ be a set of iterms containing $\ell$. Then the $\hat{\Delta}_{i+2}^b$-predicates of $\hat{T}_2^{i+1,\tau}$ contain $P^{\Sigma_{i+1}^p}(\{|\ell|\})$. Similarly, the $\hat{\Delta}_{i+2}^b$-predicates of $T_2^i$ are $P^{\Sigma_{i+1}^p}(1)$. So if $T_2^i = \hat{T}_2^{i+1,\tau}$ the polynomial hierarchy collapses to $B(\Sigma_{i+2}^p)$. By the same argument if $\tau, \tau' \subseteq O_2(|id|)$ where the $\ell$ above is in $\tau$, we get $T_2^i = \hat{C}_2^{i+1,\tau}$ implies the hierarchy collapses to $B(\Sigma_{i+2}^p)$ and likewise $\hat{C}_2^{i,\tau'} = \hat{T}_2^{i+1,\tau}$ implies the hierarchy collapses to $B(\Sigma_{i+2}^p)$ where $\tau'$ contains an unbounded iterm. We now show that the $P^{\Sigma_i^p}(\{|\ell|\})$ has complete problems.

**Theorem 79** ($i \geq 1$) *Let $\ell$ be a nondecreasing, unbounded iterm. $P^{\Sigma_i^p}(\{|\ell|\})$ has problems complete under polynomial-time many-one reductions.*

**PROOF.** It is not hard to see that the set $K$:

$$\{\langle e, x, y, 1^s\rangle | \text{The machine coded by } e \text{ accepts } x \text{ with fewer than } |\ell(y)| \text{ queries to } SAT_i \text{ and in fewer than } s \text{ steps.}\}$$

is $P^{\Sigma_i^p}(\{|\ell|\})$-complete. 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. □

**Corollary 80** ($i \geq 0$) *The following statements imply $PH = B(\Sigma_{i+2}^p)$: (a) $T_2^i = \hat{T}_2^{i+1,\tau'}$, (b) $T_2^i = \hat{C}_2^{i+1,\tau'}$, and (c) $\hat{C}_2^{i,\tau} = \hat{T}_2^{i+1,\tau'}$ where $\tau, \tau' \subseteq O_2(|id|)$ are two sets of iterms and $\tau'$ has a nondecreasing, unbounded iterm.*

**PROOF.** These statements follow from the discussion at the beginning of this section, the fact $P^{\Sigma_i^p}(\{|\ell|\})$ has complete problems, Corollary 55, Theorem 77, Corollary 49, and Corollary 75. □

One can view this as saying that the complexity characterisation of the $\hat{\Delta}^b_{i+2}$-predicates of $T^i_2$ and $\hat{T}^{i+1,\tau}_2$ where $\tau$ has an unbounded iterm will not separate these theories unless the polynomial hierarchy is infinite.

The results of Hemaspaandra, Hemaspaandra, Hempel [14,15] and Buhrman Fortnow [4] are based on the easy-hard arguments of Kadin [16] and are of a simplistic enough nature that they might be formalizable in $T^i_2$. This would give a provable collapse to $B(\Sigma^p_{i+2})$ if $T^i_2 = \hat{T}^{i+1,\tau'}_2$.

The $i = 0$ case of the equality (c) is interesting since the $\hat{\Sigma}^b_1$-definable functions of $\hat{C}^{0,\{|id|\}}_2$ are $FTC^0$ [23], functions computable by constant-depth threshold circuits. If $\hat{C}^{0,\{|id|\}}_2 = R^1_2$ or $S^1_2$ then the polynomial hierarchy collapses. So this gives some indirect evidence that $TC^0$ and $NC$ are not equal.

### *7.2 Oracle results*

We now give an oracle $X$ for which $P^{\Sigma_i^p(X)}(\{||\ell||\}) \subsetneq P^{\Sigma_i^p(X)}(\{||\ell||^2\})$ where $\ell$ is a nondecreasing, unbounded iterm. The relativisation of Corollary 49 implies the $\hat{\Delta}^b_{i+1}(\alpha)$-predicates of $\hat{T}^{i,\{|\ell|\}}_2(\alpha)$ are $P^{\Sigma_i^p(\alpha)}(\{||\ell||\})$ and those of $\hat{T}^{i,\{2^{||\ell||^2}\}}_2(\alpha)$ are $P^{\Sigma_i^p(\alpha)}(\{||\ell||^2\})$. So our oracle implies $\hat{T}^{i,\{|\ell|\}}_2(\alpha) \subsetneq \hat{T}^{i,\{2^{||\ell||^2}\}}_2(\alpha)$ where $\alpha$ is a new 1-ary predicate symbol added to $L_2$ without defining equations. This follows since $(\mathbb{N}, X)$ where $X$ interprets $\alpha$ models $\hat{T}^{i,\{|\ell|\}}_2(\alpha)$. So $\hat{T}^{i,\{|\ell|\}}_2(\alpha)$'s $\hat{\Delta}^b_{i+1}(\alpha)$-predicates are not all of $P^{\Sigma_i^p(\alpha)}(\{||\ell||^2\})$, yet $\hat{T}^{i,\{2^{||\ell||^2}\}}_2$'s are. By Corollary 12, this shows $\hat{T}^{i,\tau'}_2(\alpha) \subsetneq \hat{T}^{i,\tau}_2(\alpha)$ for any set $\tau'$ surpassed by $|\ell|$ and for any $\tau$ containing a term surpassing $2^{||\ell||^2}$. This result also shows these theories are separated by a $\hat{\Delta}^b_{i+1}(\alpha)$-predicate. We define $W \subseteq_{\hat{\Delta}^b_i(\alpha)} V$ to mean the $\hat{\Delta}^b_i(\alpha)$ predicates of $W$ are contained in the $\hat{\Delta}^b_i(\alpha)$ predicates of $V$. We define $\subsetneq_{\hat{\Delta}^b_i(\alpha)}$ in a similar manner. Taking $\ell$ to be $id$ the previous argument then gives

$$S^i_2(\alpha) \subsetneq_{\hat{\Delta}^b_{i+1}(\alpha)} \hat{T}^{i,2^{\{||\dot{x}||\}}}_2(\alpha) \preceq_{B(\hat{\Sigma}^b_{i+1}(\alpha))} R^{i+1}_2(\alpha).$$

The relativisation of Corollary 75 shows $\hat{C}^{i,\tau}_2(\alpha)$ is $B(\hat{\Sigma}^b_{i+1}(\alpha))$-conservative over $\hat{T}^{i,\tau}_2(\alpha)$ provided $\tau \subseteq O_2(|id|)$. So for $\tau, \tau'$ as above, our oracle separation shows

$$\hat{T}^{i,\tau'}_2(\alpha) \preceq_{B(\hat{\Sigma}^b_{i+1}(\alpha))} \hat{C}^{i,\tau'}_2(\alpha) \subsetneq_{\hat{\Delta}^b_{i+1}(\alpha)} \hat{T}^{i,\tau}_2(\alpha) \subseteq \hat{C}^{i,\tau}_2(\alpha).$$

We get that the $\hat{\Delta}^b_{i+1}(\alpha)$-predicates of $\hat{C}^{i,\tau}_2(\alpha)$ will actually be contained in $\hat{T}^{i,\tau}_2(\alpha)$ because of the first conservation and since $\hat{T}^{i,\tau'}_2(\alpha) \subsetneq \hat{T}^{i,\tau}_2(\alpha)$. Noticing $||x|| \leq 2^{|||x|||^2} \leq |x| \leq 2^{||x||^2} \leq x$ for large enough $x$ and using the relativisation of Corollary 75(c), our $\hat{T}^{i,\{|\ell|\}}_2(\alpha)$ versus $\hat{T}^{i,\{2^{||\ell||^2}\}}_2(\alpha)$ argument implies for $i \geq 1$:

$$\hat{R}^i_2(\alpha) \subseteq R^i_2(\alpha) \subsetneq_{\hat{\Delta}^b_{i+1}(\alpha)} S^i_2(\alpha) \subsetneq_{\hat{\Delta}^b_{i+1}(\alpha)} T^i_2(\alpha).$$

The $\hat{\Delta}^b_{i+1}(\alpha)$-predicates of $T^{i-1}_2(\alpha)$ for $i > 1$ are $P^{\Sigma^p_i(\alpha)}(1)$ by Corollary 55. Our oracle thus gives us $T^{i-1}_2(\alpha) \not\supseteq_{\hat{\Delta}^b_{i+1}(\alpha)} \hat{T}^{i,\tau}_2(\alpha)$ for any $\tau$ containing an unbounded, nondecreasing iterm. Now consider $\hat{T}^{i,\{\ell\}}_2(\alpha)$ versus $\hat{T}^{i+1,\{||\ell||\}}_2(\alpha)$. By Corollary 49 and Corollary 58, the $\hat{\Delta}^b_{i+1}(\alpha)$-predicates of the former are $P^{\Sigma^p_i(\alpha)}(\{|\ell|\})$ and of the latter are $P^{\Sigma^p_i(\alpha)}(\{||\dot{\ell}||\})$, so $\hat{T}^{i+1,\{||\ell||\}}_2(\alpha) \subsetneq_{\hat{\Delta}^b_{i+1}(\alpha)} \hat{T}^{i,\{\ell\}}_2(\alpha)$. Containment follows, since by conservation the $\hat{\Delta}^b_{i+1}(\alpha)$-predicates of $\hat{T}^{i+1,\{||\ell||\}}_2(\alpha)$ are those of $\hat{T}^{i,2^{\{||\dot{\ell}||\}}}_2(\alpha)$ which is contained in $\hat{T}^{i,\{\ell\}}_2(\alpha)$. The strictness of the inclusion follows from our oracle result since any term in $\{||\dot{\ell}||\}$ is $O(|\ell|^{1/2})$. For $i \geq 1$, using $T^i_2 = \hat{T}^{i,\{id\}}_2$ this result shows $\hat{R}^{i+1}_2(\alpha) \subsetneq_{\hat{\Delta}^b_{i+1}(\alpha)} T^i_2(\alpha)$ and by Corollary 75, $R^{i+1}_2(\alpha) \subsetneq_{\hat{\Delta}^b_{i+1}(\alpha)} T^i_2(\alpha)$.

### *7.3 The oracle separation*

Let $\ell$ be a nondecreasing, unbounded iterm. So any term in $|\{\dot{\ell}\}|$ can be bounded by some term of the form $e \cdot |\ell(s)|$ where $e$ is fixed $s \in L_2$. Our oracle construction follows [17]. By Corollary 50 and Corollary 49, a predicate in $P^{\Sigma^p_i}(\{||\ell||\})$ can be written as

$$(\exists v \leq e \cdot |\ell(s(x))|)[A(x,v) \wedge \neg B(x,v+1)]$$

where $A, B \in \Sigma^p_i$, and $s \in L_2$ and $e$ is fixed. The converse also holds by applying Corollary 65 and Corollary 49 to formulas of this kind. One can relativise these results to show any predicate is in $P^{\Sigma^p_i(X)}(\{||\ell||\})$, where $X$ is an oracle set, if and only if it can be written as

$$(\exists v \leq e \cdot |\ell(s(x))|)[A(x,v,X) \wedge \neg B(x,v+1,X)]$$

where $A, B \in \Sigma^p_i(X)$ and $s \in L_2$ and $e$ is fixed. So the problem of showing $P^{\Sigma^p_i(X)}(\{||\ell||\}) \subsetneq P^{\Sigma^p_i(X)}(\{||\ell||^2\})$ reduces to giving a problem solvable by predicates of the form

$$(\exists v \leq 2^{f \cdot ||\ell(s(x))||^2})[A(x,v,X) \wedge \neg B(x,v+1,X)]$$

where $A, B \in \Sigma_i^p(X)$ and $s \in L_2$ and $f$ is fixed, but unsolvable by predicates of the form

$$(\exists v \leq |\ell(t)|)[C(x, v, X) \wedge \neg D(x, v+1, X)]$$

where $C, D \in \Sigma_i^p(X)$.

We now define such a problem. Henceforth, we assume $\ell$ is of the form $\ell'(2^{|id|})$ where $\ell'$ is a nondecreasing, unbounded iterm. Although the new predicate symbol $\alpha$ is 1-ary we can use pairing to feed it inputs of higher arity.

**Definition 81**

*(i)* $(i \geq 1)$ *We define the* $\Sigma_i^b(\alpha)$*-formulas*

*(a)* $\Psi_1(x, v, \alpha) := v = 0 \vee (\exists y_1 < \left(\frac{x \log(x)}{2}\right)^{1/2})\alpha(\langle x, v, y_1\rangle)$

*(b)* $\Psi_2(x, v, \alpha) := v = 0 \vee (\exists y_1 < x)(\forall y_2 < (x \log(x))^{1/2})\alpha(\langle x, v, y_1, y_2\rangle)$

*(c)*

$$\begin{aligned}\Psi_i(x, v, \alpha) := v = 0 \vee (\exists y_1 < x)(\forall y_2 < x) \cdots (Q_{i-1} y_{i-1} < x) \\ (Q_i y_i < \left(\frac{i \cdot x \cdot \log(x)}{2}\right)^{1/2})\alpha(\langle x, v, y_1, \ldots, y_i\rangle)\end{aligned}$$

*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.*

*(ii)* $(i \geq 1)$ *we define*

$$\begin{aligned}P_i^\ell(x, \alpha) := (\exists v < 2^{||\ell(x)||^2})[(\Psi_i(x, v, \alpha) \wedge v = 1 mod 2 \wedge \\ \neg(\exists v' < 2^{||\ell(x)||^2})(v' > v \wedge \Psi_i(x, v', \alpha))]\end{aligned}$$

$P_i^\ell(x, \alpha)$ is true if the maximal $v$ satisfying $\Psi_i(x, v, \alpha)$ is odd. We have modified the definition of $\Psi_i$ above from Krajíček [18] and so have not entirely directly adapted the problem used there to separate $S_2^i(\alpha)$ from $T_2^i(\alpha)$. We did this to simplify our proof of Lemma 86 and because Lemma 91 seemed harder to show using a more direct adaptation of that paper's problem. The next lemma follows from the definition of $P_i^\ell$ and the relativisations of Corollary 65 and Corollary 49.

**Lemma 82** $(i \geq 1)$ $P_i^\ell(x, \alpha) \in P^{\Sigma_i^p(\alpha)}(\{||\ell||^2\})$ *for all* $\alpha \subset \omega$.

To separate $P^{\Sigma_i^p(X)}(\{||\ell||\})$ and $P^{\Sigma_i^p(X)}(\{||\ell||^2\})$ we use propositional translations $P_i^\ell(x, \alpha)$. These translations allow us to apply results from Boolean circuit complexity to help solve our problem.

**Definition 83** *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* $\Psi_i(k, v, \alpha)$ *and* $P_i^\ell(k, X)$.

*(i) The variables in* $\overline{\Psi}_i(k,v)$ *are of the form*

$$p_{v,y_1,y_2,\ldots,y_{i-1},y_i}$$

*for* $v < 2^{||\ell(k)||^2}$ *and, for every* $(i-1)$*-tuple* $y_1, y_2, \ldots, y_{i-1} < k$ *and for each* $y_i < n$.

*(ii) We define the circuit* $\overline{\Psi}_i(k,v)$ *to be*

$$\bigvee_{y_1=0}^{k-1} \bigwedge_{y_2=0}^{k-1} \bigvee_{y_3=0}^{k-1} \cdots \bigbigvee_{y_{i-1}=0}^{k-1} \bigbigwedge_{y_i=0}^{n-1} p_{v,y_1,\ldots,y_i}$$

*where* $\bigbigvee_{y_{i-1}=0}^{k-1}$ *is* $\bigwedge_{y_{i-1}=0}^{k-1}$ *if* $i$ *is odd and an* $\bigvee_{y_{i-1}=0}^{k-1}$ *otherwise. Likewise,* $\bigbigwedge_{y_i=0}^{n-1}$ *is a* $\bigvee_{y_i=0}^{n-1}$ *if* $i$ *is odd and an* $\bigwedge_{y_i=0}^{n-1}$ *otherwise.*

*(iii) The circuit* $\overline{P}_i^{\ell,k}$ *is*

$$\bigvee_{v<2^{||\ell(k)||^2},\ v\ odd} \Big(\overline{\Psi}_i(k,v) \wedge \bigwedge_{v<v'<2^{||\ell(k)||^2}} \neg\overline{\Psi}_i(k,v')\Big).$$

The idea of the above is that atomic formulas $\alpha(\langle k, v, y_1, \ldots, y_i\rangle)$ are translated as propositional variables $p_{v,y_1,\ldots,y_i}$, existential quantifiers are translated as OR's, and universal quantifiers are translated as AND's. 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 $\Psi_i(k,v,\alpha)$ is 0 then $P_i^\ell(k,\alpha)$ will be false. From this discussion, the next lemma is easily verified.

**Lemma 84** $(i \geq 1, k \geq 0)$ *Let* $\ell \in \tau$. *The circuit* $\overline{P}_i^{\ell,k}$ *computes the value of* $P_i^\ell(k,\alpha)$ *under the assignment*

$$p_{v,y_1,\ldots,y_i} = \begin{cases} 1 \text{ if } \langle k, v, y_1, \ldots, y_i\rangle \in \alpha \\ \\ 0 \text{ otherwise} \end{cases}$$

The next definition is needed to apply a result of Hastad [13].

**Definition 85** *(i) Let* $(B_j)_j$ *be a partition of the atoms of* $\overline{P}_i^{\ell,k}$ *into* $2^{||\ell(k)||^2} \cdot k^{i-1}$ *classes of the form*

$$\Big\{p_{v,y_1,\ldots,y_{i-1},y_i}\Big| y_i < \Big(\frac{i \cdot k\log(k)}{2}\Big)^{1/2}\Big\}$$

*one for every choice of* $y_1, \ldots y_{i-1} < k$, $v < 2^{||\ell(k)||^2}$.

*(ii)* *Let $0 < q < 1$ be a real number. A probability space $R_q^+$ of random restrictions is a space of restrictions $\rho$ 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*

$$\rho(p) := \begin{cases} s_j & \text{with probability } q \\ 1 & \text{with probability } 1-q \end{cases}$$

*(iii)* *$R_q^-$ is defined in the same way as $R_q^+$ except the roles of 0 and 1 are interchanged.*
*(iv)* *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 $\rho$ 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 $p_{v,y_1,\ldots,y_{i-1}}$.*
*(v)* *For $\rho \in R_q^-$, $g(\rho)$ is is defined as in (iv) except interchanging the roles of 0 and 1.*
*(vi)* *For $G$ a circuit with atoms among those of $\overline{P}_i^{\ell,k}$, let $G^\rho$ denote the circuit obtained from $G$, by performing the restriction $\rho$ followed by the restriction $g(\rho)$. The atoms of $G^\rho$ are among those of $\overline{P}_{i-1}^{\ell,k}$.*

The next lemma is one of two results we use from Hastad [13].

**Lemma 86** *Let $q := (2i\log(k)/k)^{1/2}$ and assume $k$ is sufficiently large. Then the following three conditions hold.*

*(i)* *Let $G$ be a depth 2 subcircuit of $\overline{P}_i^{\ell,k}$: So $G$ 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 $\rho$ 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 $1 - \frac{1}{3}k^{-i+1}$ $G^\rho$ is an OR (resp. an AND) of at least $((i-1) \cdot k\log(k)/2)^{1/2}$ different atoms.*
*(ii)* *($i \geq 2$) Pick $\rho$ 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.*

**PROOF.** We sketch this following Krajíček [18] and Buss and Krajicek [6].

(i) The proof of this is the same as Lemma 10.4.7 (i) in Krajíček [18].

(ii) There are $2^{||\ell(k)||^2} \cdot k^{i-2}$ different subcircuits of depth 2 in $\overline{P}_i^{\ell,k}$. By our assumption $2^{||\ell(k)||^2} \leq k$, and (i), with probability

$$(1 - \frac{1}{3}k^{-i+1})^{2^{||\ell(k)||^2} \cdot k^{i-2}} \geq 1 - \frac{1}{3}2^{||\ell(k)||^2} \cdot k^{-1} \geq \frac{2}{3}$$

all of them are restricted by $\rho$ as described in the conclusion of (i). The first inequality holds by looking at the series expansion of the first term. Thus, after renaming the atoms, $(\overline{P}_i^{\ell,k})^\rho$ becomes $\overline{P}_{i-1}^{\ell,k}$. $\square$

We now give a notion a truth table reducibility which we use to represent propositional translations of predicates in $P^{\Sigma_i^p(\alpha)}(\{||\ell||\})$.

**Definition 87**

*(i) 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 $\overline{P}_i^{\ell,k}$.*

*(ii) A $tt^{||\ell||}$-reducibility of type $(i,k,d)$ is a Boolean formula of the form*

$$f(w_1, \ldots, w_m)$$

*in $m \leq e \cdot |\ell(k)|$ variables where $e$ is fixed together with $\Sigma_{i,k}^{S,t}$-circuits $E_1, \ldots, E_m$ where $S = 2^{(\log k)^d}$, and $t = \log(S)$.*

*(iii) 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 a fixed $d$. Suppose one has a $A(\mathbf{x}) \in \Sigma_i^b(\alpha)$. For a fixed $\mathbf{k}$ one translates $A(\mathbf{k})$ into propositional formula $\bar{A}(\mathbf{k})$ as follows:

(1) If $A(\mathbf{k})$ is $t(\mathbf{k}) \leq s(\mathbf{k})$ or $t(\mathbf{k}) = s(\mathbf{k})$ then $\bar{A}(\mathbf{k})$ is either $\top$ or $\bot$ according to the value of the atomic formula on input $\mathbf{k}$.
(2) If $A(\mathbf{k})$ is $\alpha(\langle \mathbf{k} \rangle)$ then $\bar{A}(\mathbf{k})$ is $p_{\mathbf{k}}$.
(3) If $A(\mathbf{k})$ is $B \circ C$ where $\circ$ is a binary connective then $\bar{A}(\mathbf{k})$ is $\bar{B} \circ \bar{C}$.
(4) If $A(\mathbf{k})$ is $\neg B$ then $\bar{A}(\mathbf{k})$ is $\neg \bar{B}$.
(5) If $A(\mathbf{k})$ is $(\exists y \leq t(\mathbf{k}))B(\mathbf{k}, y)$ then $\bar{A}(\mathbf{k})$ is $\vee_{j=0}^{t(\mathbf{k})} \bar{B}(\mathbf{k}, j)$.
(6) If $A(\mathbf{k})$ is of the form $(\forall y \leq t(\mathbf{k}))B(\mathbf{k}, y)$ then $\bar{A}(\mathbf{k})$ is $\wedge_{j=0}^{t(\mathbf{k})} \bar{B}(\mathbf{k}, y)$.

One can modify the quantifier bounds of a prenexification of a $\Sigma_i^b(X)$-formula $A$ so that a $\Sigma_{i,k}^{S,\log(S)}$-circuit can be used to compute $A(k)$ under this translation and under the truth assignment $p_{\mathbf{k}} = \top$ iff $\langle \mathbf{k} \rangle \in X$. If $A, B \in \Sigma_i^b(X)$ and $e$

is fixed, then it follows there is a $tt^{||\ell||}$-reducibility of type $(i,k,d)$ computing the value of $(\exists v \leq e\cdot|\ell(k)|)[A(k,v,X)\wedge\neg B(k,v+1,X)]$. We now prove some lemmas that show the limitations on $tt^{||\ell||}$-reducibilities.

**Lemma 88** *Let $G$ be an AND of OR's of size $\leq t$ with atoms among those of $\overline{P}_i^{\ell,k}$. Pick $\rho$ randomly from $R_q^+$ or from $R_q^-$.*

*Then with probability at least $1-(6qt)^s$ the circuit $G^\rho$ can be written as an OR of ANDs of size $< s$.*

*This is also the probability of switching an OR of AND's to an AND of OR's.*

The proof of the above lemma is in Hastad [13].

**Lemma 89** *Let $q := (2i\log(k)/k)^{1/2}$ and let $D$ be a $tt^{||\ell||}$-reducibility of type $(i,k,d)$. Pick $\rho$ at random from $R_q^+$ or from $R_q^-$. Then with probability at least a half, $D^\rho := \langle f; E_1^\rho,\ldots,E_m^\rho\rangle$ is a $tt^{||\ell||}$-reducibility of type $(i-1,k,d)$.*

**PROOF.** Let $t = s = (\log k)^d$ and apply Lemma 88. The probability that a depth 2 subcircuit of any $E_j$ fails to be switched is at most

$$(6qt)^t = \Big(6\Big(\frac{2i\log(k)}{k}\Big)^{1/2}(\log k)^d\Big)^{(\log k)^d} < 2^{-f\cdot(\log k)^{d+1}}$$

for large enough $k$ and some sufficiently small constant $f$.

There are fewer than $e\cdot|\ell(k)|\cdot(2^{(\log k)^d})^{i-2} \leq 2^{i\cdot(\log k)^d}$ such depth 2 subcircuits, so with probability at least

$$1-2^{i\cdot(\log k)^d - f\cdot(\log k)^{d+1}} > 1/2$$

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. $\Box$

**Lemma 90** *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 $P_1^\ell(k,Y)$ for every $Y\subseteq\omega$.*

**PROOF.** By Lemma 84, $P_i^\ell(k,X)$ is computed by $\overline{P}_i^{\ell,k}$. Lemma 86 and Lemma 89 imply a random restriction $\rho$ (drawn from $R_q^+$ if $i$ is even and $R_q^-$ if $i$ odd) has greater than a 1/6 chance of both converting $\overline{P}_i^{\ell,k}$ into $\overline{P}_{i-1}^{\ell,k}$ and converting $D$ into a $tt^{||\ell||}$-reducibility of type $(i-1,k,d)$. As this is nonzero, some $\rho$ does this conversion. Applying this conversion $(i-1)$-times proves the lemma. $\Box$

**Lemma 91** ($i \geq 1$) *For fixed $d$ and large enough $k$ no $tt^{||\ell||}$-reducibility of type $(i,k,d)$ computes $P_i^\ell(k,X)$ for all $X \subseteq \omega$.*

**PROOF.** In view of Lemma 90, it suffices to show no $tt^{||\ell||}$-reducibility of type $(1,k,d)$ computes $P_1^\ell(k,Y)$ for all $Y \subseteq \omega$.

Let $t := \log(k)^d$, and let $D = \langle f; E_1, \ldots, E_m \rangle$ be a $tt^{||\ell||}$-reducibility of type $(1,k,d)$. So $m \leq e \cdot |\ell(k)|$. Here $E_i$ are $\Sigma_{1,k}^{2^{(\log k)^d},(\log k)^d}$-circuits. For simplicity write $P$ for $\overline{P}_1^k$.

We work with triples $\langle k, v, y_1 \rangle$ where $k$ is as in the statement of the lemma. For a finite set $X$ of triples $\langle k, v, y_1 \rangle$, we write $\max_p(X)$ for $p = 1, 2, 3$ for the largest value of the $p$th coordinate in any triple in $X$. We define $\min_p(X)$ similarly. We construct a sequence of sets $X_s^+$, $X_s^-$, $I_s$ 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 set $X_0^+ := X_0^- := I_0 = \emptyset$. For stage $s+1$, assume $X_s^+$, $X_s^-$, $I_s$ satisfy the conditions stated.

Set $Y := X_s^+$. By (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 $\max_2(Y)$ is 1 mod2. In this case STOP.
(b) $D^Y = 1$ and $\max_2(Y)$ is 1 mod2. Consider the set

$$V = \{\langle k, v, y_1 \rangle \mid \max_2(X_s^+) < v < 2^{||\ell(k)||^2},$$
$$y_1 \leq ((k \log k)/2)^{1/2}, v = 0 \text{ mod2}, \langle k, v, y_1 \rangle \notin X_s^-\}$$

The upper bounds on $v$ and $y_1$ are the largest values these indices have in variables in $P$. By condition (1), (2) and (3), the set $V$ is nonempty since

$$2s \leq 2m \leq 2 \cdot e \cdot |\ell(k)| \leq 2^{||\ell(k)||^2}$$

for sufficiently large $k$ and since $\ell(k)$ is unbounded. There are two subcases:

(b1) It is possible to add some element $\langle k, v, y_1 \rangle \in V$ 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 $\langle k, v, y_1\rangle \in V$ with property (b1). Take $\langle k, v, y_1\rangle$ in $V$ such that $v = min_2(V)$ and such that $\langle k, v, y'_1\rangle$ in $V$ 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. So either: (1) some $E_{j_0}$ for $j_0 \notin I_s$ received new value 1, or (2) some $E_{j_0}$ for $j_0 \notin I_s$ received new value 0. In the first case, we set $X^+_{s+1} := X^+_s \cup \{\langle k, v, y_1\rangle\}$. As the circuit $E_{j_0}$ is an $\Sigma^{2^t,t}_{1,k}$-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 this AND in $E_{j_0}$ 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 occurring elements in this AND. Notice in both cases $|X^+_{s+1}| \leq s+1$ and $|X^+_{s+1} \cup X^-_{s+1}| \leq st + t = (s+1)t$. Since for sufficiently large $k$

$$|X^+_s \cup X^-_s| < st \leq m \cdot (\log k)^d \leq e|\ell(k)|(\log k)^d < (\frac{k \log k}{2})^{1/2}$$

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 $V$. So $min_2(V)$ is at most $max_2(X^+_s)+2$, since either $\max_2(X^+_s)+1$ or $\max_2(X^+_s)+2$ is 1mod2 and there will be tuples in $V$ with these values of $v$. Thus in both cases of (b2) condition (1) will be satisfied since for any $\langle k, v, y_1\rangle \in X^+_{s+1}$ we have $v \leq \min_2(V) \leq \max(X^+_s)+2 \leq 2s+2 = 2(s+1)$. 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

$$V = \{\langle k, v, y_1\rangle \mid \max_2(X^+_s) < v < 2^{||\ell(k)||^2},$$
$$y_1 \leq ((k \log k)/2)^{1/2}, v = 1 \bmod 2, \langle k, v, y_1\rangle \notin X^-_s\}$$

and proceed analogously to case (b).

If the construction has not terminated by stage $s$, then $I_s \subsetneq I_{s+1}$. Thus, by (3) the construction must halt eventually.

Let $Y := X^+_s$ for the final $s$. If during the construction only step (b) or (c) 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 $v := 0$ mod2 and such that $v' := 1$ mod2. If (a) ever applies then we are also done. □

**Theorem 92** $(i \geq 1)$ *There is an $X$ so that $P^{\Sigma_i^p(X)}(\{||\ell||\}) \subsetneq P^{\Sigma_i^p(X)}(\{||\ell||^2\})$*

**PROOF.** We construct $X \subseteq \omega$ such that $P_i^\ell(x, X) \notin P^{\Sigma_i^p(X)}(\{||\ell||\})$. By an easy extension to Corollary 50, any $P^{\Sigma_i^p(X)}(\{||\ell||\})$ predicate can be written as $A := (\exists v \leq e \cdot |\ell|)[C(x, v, X) \wedge \neg D(x, v+1, X)]$ where $C, D \in \Sigma_i^p(X)$ and $e$ is fixed. Let $F_j^{||\ell||}$, j=0,1, ... enumerate all such predicates. We consider successive $j$'s and build $X$ in stages to ensure that $F_j^{||\ell||} \neq P_i^\ell(x, X)$.

Let $X_s$ be the approximation of $X$ constructed by stage $s$ 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 stated before, for each fixed $k$, formulas of the form $A$ can be computed by a $tt^{||\ell||}$-reducibility $D$ in a straightforward way. Let $D_{s+1}^{||\ell||}$ be the reducibility computing $F_{s+1}^{||\ell||}$. Evaluate indices corresponding to "$n \in \alpha$" with $k' < k$ according to $X_s$ and otherwise, set to 0 all atoms whose indices are not of the form $\langle k, v, y_1, \ldots, y_i \rangle$.

This leaves a $tt^{||\ell||}$-reducibility of type $(i, k, d)$, which cannot compute $P_i^\ell(k, Y)$ for all $Y \subset \omega$ by Lemma 91. A finite $Y$ for which the reducibility fails was constructed in Lemma 91, take $X_{s+1} = X_s \cup Y$ and the reducibility fails for $X_{s+1}$. Hence, $F_{s+1}^{||\ell||} \neq P_i^\ell(x, X_{s+1})$. So $F_{s+1}^{||\ell||} \neq P_i^\ell(x, X)$ where $X = \bigcup_s X_s$.

Proceed to $s+2$. $\square$

The next corollaries follow from the above theorem and the discussion in Section 7.2.

**Corollary 93** *Suppose $\ell' \in \tau$ surpasses $2^{||\ell||^2}$ and is a nondecreasing, unbounded iterm and suppose $\tau'$ is surpassed by $|\ell|$. Then:*

*(i)* $\hat{T}_2^{i,\tau'}(\alpha) \subseteq \hat{C}_2^{i,\tau'}(\alpha) \subsetneq_{\hat{\Delta}_{i+1}^b(\alpha)} \hat{T}_2^{i,\tau}(\alpha) \subseteq \hat{C}_2^{i,\tau}(\alpha)$.

*(ii)* $T_2^{i-1}(\alpha) \not\supseteq_{\hat{\Delta}_{i+1}^b(\alpha)} \hat{T}_2^{i,\tau}(\alpha)$.

*(iii)* $\hat{T}_2^{i+1,\{||\ell||\}}(\alpha) \subsetneq_{\hat{\Delta}_{i+1}^b(\alpha)} \hat{T}_2^{i,2^{\{|\dot{\ell}|\}}}(\alpha)$.

*(iv)* $\hat{T}_2^{i,\{|\ell|\}}(\alpha) \subsetneq_{\hat{\Delta}_{i+1}^b(\alpha)} \hat{T}_2^{i,2^{\{||\dot{\ell}||\}}} \preceq_{B(\hat{\Sigma}_{i+1}^b(\alpha))} \hat{T}_2^{i+1,\{||\ell||\}}(\alpha)$.

**Corollary 94** $(i \geq 1, m \geq 0)$

*(i)* $\hat{R}_2^i(\alpha) \subseteq R_2^i(\alpha) \subsetneq_{\hat{\Delta}_{i+1}^b(\alpha)} S_2^i(\alpha) \subsetneq_{\hat{\Delta}_{i+1}^b(\alpha)} T_2^i(\alpha)$.

*(ii)* $T_2^{i-1}(\alpha) \not\supseteq_{\hat{\Delta}_{i+1}^b(\alpha)} \hat{T}_2^{i,\{|id|_m\}}(\alpha)$.

*(iii)* $\hat{R}_2^{i+1}(\alpha) \subsetneq_{\hat{\Delta}_{i+1}^b(\alpha)} T_2^i(\alpha)$.

*(iv)* $R_2^{i+1}(\alpha) \subsetneq_{\hat{\Delta}_{i+1}^b(\alpha)} T_2^i(\alpha)$.

*(v)* $S_2^i(\alpha) \subsetneq_{\hat{\Delta}_{i+1}^b(\alpha)} \hat{T}_2^{i,2^{\{||id||\}}} \preceq_{B(\hat{\Sigma}_{i+1}^b(\alpha))} R_2^{i+1}(\alpha)$.

### *7.4 Models separating theories*

Recall from the introduction that a model $M$ separates the theories $A$ and $B$ with respect to $\hat{\Delta}_i^b(\alpha)$-predicates if: (a) $M$ models $A$ and $B$. (b) The $\hat{\Delta}_i^b(\alpha)$-predicates of $A$ are $\Psi_A$ and those of $B$ are $\Psi_B$. (c) $M \models \Psi_A \neq \Psi_B$.

**Theorem 95** *There is an oracle $X$ such that for all $i \geq 1$ there is an $\ell$ for which $(\mathbb{N}, X)$ separates $\hat{T}_2^{i,\{\ell\}}(\alpha)$ from $\hat{T}_2^{i,\{|\ell|\}}(\alpha)$ for $\hat{\Delta}_2^b(\alpha)$-predicates yet $(\mathbb{N}, X) \models PH(\alpha) = \Delta_2^p(\alpha)$.*

**PROOF.** Buhrman and Torenvliet [3] give an oracle $X$ for which $NEXP^X \subseteq P^{NP^X}$. So $(\mathbb{N}, X) \models NEXP(\alpha) = PH(\alpha) = P^{NP}(\alpha)$. Mocas [20] shows $P^{NP}(n^k) \subsetneq NEXP$ and this relativizes. Now consider $\hat{T}_2^{i,\{|id|_i\}}(\alpha)$ versus $\hat{T}_2^{i,\{|id|_{i-1}\}}(\alpha)$. For all $i \geq 1$, $\hat{T}_2^{i,\{|id|_{i-1}\}}(\alpha) \supseteq T_2^1(\alpha)$ so its $\hat{\Delta}_2^b(\alpha)$-predicates contain $P^{NP}(\alpha)$. By Corollary 58, however, one sees the $\hat{\Delta}_2^b(\alpha)$-predicates of $\hat{T}_2^{i,\{|id|_i\}}(\alpha)$ have subpolynomially many queries to an $NP(\alpha)$-oracle. In particular, they are contained in $P^{NP}(n^2)(\alpha)$. So by the Burhman and Torenvliet result and the Mocas result $(\mathbb{N}, X)$ separates $\hat{T}_2^{i,\{|id|_{i-1}\}}(\alpha)$ from $\hat{T}_2^{i,\{|id|_i\}}(\alpha)$ with respect to $\hat{\Delta}_2^b(\alpha)$-predicates. □

## 8 Acknowledgements

This paper consists of both a revision and extension of some of the results from the author's dissertation [23]. The author would first and foremost like to thank his advisor Sam Buss whose assistance throughout the creative process was invaluable. The author would like to thank Steve Fenner, Lance Fortnow, and Steve Homer for the references Buhrman and Torenvliet [3] and Mocas [20] and would also like to thank Lane Hemaspaandra and Harold Hempel for pointing out the literature after Kadin [16]. The author would also like to thank Jan Johannsen for his constructive suggestions on an earlier version of this paper.

## References

[1] B. Allen. Arithmetizing uniform NC. *Annals of Pure and Applied Logic*, 53:1–50, 1991.

[2] A. Beckmann. *Separating fragments of bounded arithmetic.* PhD thesis, Universität Münster, 1996.

[3] H. Buhrman and L. Torenvliet. On the cutting edge of relativization: The resource bounded injury method. In *ICALP 1994*, pages 263–273. Springer-Verlag in Lecture Notes in Computer Science 820, 1994.

[4] H Burhman and L. Fortnow. Two queries. TR 96-20, University of Chicago, Department of Computer Sciencee, September 1996.

[5] S. R. Buss and L. Hay. On truth-table reducibility to SAT. *Information and Computation*, 91(1):86–102, March 1991.

[6] 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.

[7] S.R. Buss. *Bounded Arithmetic.* Bibliopolis, Napoli, 1986.

[8] S.R. Buss. Axiomatizations and conservation results for fragments of bounded arithmetic. *Contemporary Mathematics*, 106:57–83, 1990.

[9] S.R. Buss. Relating the bounded arithmetic and polynomial time hierarchies. *Annals of Pure and Applied Logic*, 75:67–77, 1995.

[10] 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.

[11] P. Clote and G. Takeuti. Bounded arithmetic for NC, Alogtime, L and NL. *Annals of Pure and Applied Logic*, 56:73–177, 1992.

[12] S. A. Cook. Feasibly constructive proofs and the propositional calculus. In *Proceedings of the 7-th ACM Symposium on the Theory of Computation*, pages 83–97, 1975.

[13] 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.

[14] E. Hemaspaandra, L. Hemaspaandra, and H. Hempel. A downward translation in the polynomial hierarchy. In *Proceedings of the 14th Annual Symposium on Theoretical Aspects of Computer Science*, pages 319–328, 1997.

[15] E. Hemaspaandra, L. Hemaspaandra, and H. Hempel. Translating equality downwards. TR 97-657, University of Rochester, Department of Computer Science, April 1997.

[16] J. Kadin. The polynomial time hierarchy collapses if the boolean hierarchy collapses. *SIAM Journal on Computing*, 17(6):1263–1282, August 1988.

[17] J. Krajíček. Fragments of bounded arithmetic and bounded query classes. *Transactions of the American Mathematical Society*, 338(2):587–598, August 1993.

[18] J. Krajíček. *Bounded Arithmetic, Propositional Logic and Complexity Theory.* Cambridge University Press, 1995.

[19] J. Krajíček, P. Pudlák, and G. Takeuti. Bounded arithmetic and the polynomial hierarchy. *Annals of Pure and Applied Logic*, 42:143–155, 1991.

[20] S. Mocas. *Separating Exponential time classes from polynomial time classes.* PhD thesis, Northeastern University, 1997.

[21] R. Parikh. Existence and feasibility in arithmetic. *Journal of Symbolic Logic*, 36:494–508, 1971.

[22] 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.

[23] C. Pollett. *Arithmetic Theories with Prenex Normal Form Induction.* PhD thesis, University of California, San Diego, 1997.

[24] P. Pudlak. Ramsey's theorem in bounded arithmetic. In *Computer Science Logic '90, LNCS533*, pages 308–317. Springer-Verlag, 1990.

[25] 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.

[26] 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.

[27] G. Takeuti. *Proof theory.* North-Holland, 1975.

[28] G. Takeuti. *RSUV* isomorphisms. In P. Clote and J. Krajíček, editors, *Arithmetic, Proof Theory and Computational Complexity*, pages 364–386. Oxford Science Publications, 1993.

[29] D. Zambella. Notes on polynomially bounded arithmetic. *Journal of Symbolic Logic*, 61:942–966, 1996.