Conservative Fragments of S^1_2 and R^1_2

Chris Pollett
214 MacQuarrie Hall
Department of Computer Science
San Jose State University
1 Washington Square, San Jose CA 95192
pollett@cs.sjsu.edu

September 20, 2009– Draft

Abstract

Conservative subtheories of R^1_2 and S^1_2 are presented. For S^1_2, a slight tightening of Jeřábek's result [18] that $T^0_2 \preceq_{\forall\Sigma^{\mathsf{b}}_1} S^1_2$ is presented: It is shown that T^0_2 can be axiomatised as *BASIC* together with induction on sharply bounded formulas of one alternation. Within this $\forall\Sigma^{\mathsf{b}}_1$-theory, we define a $\forall\Sigma^{\mathsf{b}}_0$-theory, T^{-1}_2, for the $\forall\Sigma^{\mathsf{b}}_0$-consequences of S^1_2. We show T^{-1}_2 is weak by showing it cannot Σ^{b}_0-define division by 3. We then consider what would be the analogous $\forall\hat{\Sigma}^{\mathsf{b}}_1$-conservative subtheory of R^1_2 based on Pollett [24]. It is shown that this theory, $T^{0,\{2^{(||\mathrm{id}||)}\}}_2$, also cannot Σ^{b}_0-define division by 3. On the other hand, we show that $S^0_2 + open_{\{||id||\}}$-$COMP$ is a $\forall\hat{\Sigma}^{\mathsf{b}}_1$-conservative subtheory of R^1_2. Finally, we give a refinement of Johannsen and Pollett [21] and show that $\hat{C}^0_2$ is $\forall\hat{\Sigma}^{\mathsf{b}}_1$-conservative over a theory based on $open_{\mathrm{cl}}$-comprehension.

Mathematics Subject Classification: 03F30, 68Q15
Keywords: bounded arithmetic, independence results

1 Introduction

One of the fundamental problems in bounded arithmetic is to separate the theories S^j_2, $j \geq 0$ defined in Buss [6]. It is known that if $S^j_2 = S^{j+1}_2$ then the polynomial hierarchy collapses to Σ^p_{j+2} [16]. From this it follows that if $S_2 = \cup_k S^k_2 \neq S^j_2$ for all j then S_2 does not prove the collapse of the polynomial hierarchy. It is hoped that separating these theories might be easier than separating the polynomial hierarchy but nevertheless shed insight into the complexity problem. In this paper, we explore an approach to separating bounded arithmetic theories by looking at their $\hat{\Sigma}^{\mathsf{b}}_1$ and sharply bounded fragments.

In order to appreciate the difficulty in separating bounded arithmetic theories it is useful to consider what would be involved in separating theories via some notion of definability. Here an arithmetic theory T can Ψ-define a function f if there is a formula A_f in Ψ such that $T \vdash \forall \mathbf{x} \exists ! y A_{(}\vec{x}, y)$ and $\mathbb{N} \models \forall \mathbf{x} A_f(\mathbf{x}, f(\mathbf{x}))$. For example, a classic result of Buss [6] is that the Σ^{b}_1-definable functions of S^1_2 are precisely the polynomial time computable functions, FP, and the Σ^{b}_2-definable functions of S^2_2 are the polynomial time functions with access to an NP oracle, FP^{NP}. It is unlikely that looking at Σ^{b}_2-definable or larger will help in separating these theories as even the base theory, $BASIC$, for any of these systems can Σ^{b}_2-define any polynomial time function which makes $O(1)$ queries to an NP-oracle [24]. So to separate theories using Σ^{b}_i-definability for $i \geq 2$ would be at least as hard as solving open complexity theory problems. For Σ^{b}_1-definability the situation also seems difficult. It is known the Σ^{b}_1-definable multifunctions of S^2_2 are projections of multifunctions in PLS, the class of polynomial local search problems. This class contains FP. Proofs of Σ^{b}_i-definability generally also give one characterizations of the $\hat{\Delta}^b_i$-relations, those formulas which are provably equivalent to both a Σ^{b}_i and $\hat{\Pi}^{\mathsf{b}}_i$ formula. In the S^1_2 versus S^2_2 case one gets P versus PLS and we know $\mathsf{P} \subseteq \mathsf{PLS} \subseteq \mathsf{NP}$. So it seems this approach is at least as hard as separating P from NP. For $j \geq 2$, separating S^j_2 from S^{j+1}_2 only becomes harder. So for all of these theories the best results known are relativized separations of theories $S^j_2(\alpha)$ where α is a predicate symbol.

There are two main kinds of outright separations results known for arithmetic theories contained in S_2: (1) Separations based on a Σ^{b}_1-formula. (2) Separations based on a open or sharply bounded formula. As an example of the first kind, one can show $\hat{\Sigma}^{\mathsf{b}}_1$-definability in S^0_2 is different from S^1_2 basically because the function class one gets for S^0_2 is strictly contained in FP and can be shown not to contain $\lfloor \frac{x}{3} \rfloor$. Shepherdson's very early weak arithmetic paper [28], gives an example of the second kind of separation. Shepherdson studied the relationship between the open axiom of induction versus the open rule of induction for various languages of arithmetic. For each language up to the language $=$, 0, $S(x) := x+1$, $P(x) := \max(x-1, 0)$, $+$, $\cdot$, $\lfloor \frac{x}{n} \rfloor$, for some fixed $n \in \mathbb{N}$ he showed the open rule of induction is equivalent to a finite number of additional axioms. He was unable to do this when

$\dot{-}$ was added to the language; however, he was able to give a recursive model for the theory based on the axiom of induction in this language. This model consisted of elements of the form:

$$a_p t^{p/q} + a_{p-1} t^{p-1/q} + \cdots + a_1 t^{1/q} + b$$

where t is indeterminate, $p \geq 0$, $q > 0$, and $b \geq 0$ are integers and each a_i is a real algebraic number. Using this model, Shepherdson showed open statements like $y^2 \neq 2x^2 \vee x = 0$ are not provable using the open axiom of induction. The reason we say either open or sharply bounded formulas for this kind of separation, is that by adding a sharply bounded μ-operator symbol to the language one can often make a conservative extension of one's theory. The sharply bounded formulas in the resulting theory will then each be equivalent to an open formula. In terms of separations this makes the problem only marginally more difficult as it is known that in several common languages of bounded arithmetic that the sharply bounded formulas express predicates strictly contained in P [22].

If only because known outright separations of theories within S_2 have been obtained via Σ^{b}_1- and sharply bounded formulas, it is important to get a good characterization of these formulas for the theories S^j_2, $j \geq 1$. And in the last several years a good deal of progress has been made on this problem [13], [17], [27], [2], [3]. Shepherdson's paper though shows that building simple pathological models of open or sharply bounded fragments of arithmetic might be simpler than for more powerful theories. Some evidence of this is given by the more recent results can be found in Boughattas and Ressayre [5] and Boughattas and Kołodziejczyk [4].

In this paper, we look at $\forall\Sigma^{\mathsf{b}}_1$ and sharply bounded fragments of theories with the goal of making progress on the question of whether the theory R^1_2 is equal to S^1_2. As was mentioned above, the $\hat{\Delta}^b_1$-predicates of S^1_2 are precisely the P relations. It is also known that the $\hat{\Delta}^b_1$-predicates of R^1_2 are precisely the uniform NC relations [1],[29]. I.e., those relation computable by logspace uniform polylog depth, polynomial sized circuit families. The P versus NC question has been open for more than twenty years. So the R^1_2 versus S^1_2 is likely to be non-trivial to solve. Nevertheless, if one formulates S^1_2 and R^1_2 over the base theory using prenex formulas, then S^1_2 can be formulated as having $\hat{\Sigma}^{\mathsf{b}}_1$ length induction, and R^1_2 can be formulated as having $\hat{\Sigma}^{\mathsf{b}}_1$-length-length induction together with collection for $\hat{\Sigma}^{\mathsf{b}}_1$-formulas. If one drops collection, the $\hat{\Sigma}^{\mathsf{b}}_1$-definable multifunctions of the resulting theory were given in Pollett [24]. These multifunctions seem to be significantly weaker than NC as evidenced by [24], [5] so there is some hope the resulting theory could be directly separated from both R^1_2 and S^1_2. Another reason why the R^1_2 versus S^1_2 problem is a potentially viable candidate for separation, is that Jeřábek [18] has given a good characterization of the Σ^{b}_1-consequences of S^1_2 as the theory T^0_2 which has induction for sharply bounded formulas. So separations based on using the more restricted structure of T^0_2 or its analog for R^1_2 might be possible.

This paper examines a good candidate for a $\forall\hat{\Sigma}^{\mathsf{b}}_1$-conservative sub-theory of R^1_2 and then in turn tries to find a $\forall\hat{\Sigma}^{\mathsf{b}}_0$-subtheory of this. As Pollett [24] has shown that $T_2^{i,\{2^{(||\mathrm{id}||)}\}}$, which over the base theory has induction on $\hat{\Sigma}^{\mathsf{b}}_i$-formulas up to terms of the form $2^{p(||x||)}$ for some polynomial p, is $\forall\hat{\Sigma}^{\mathsf{b}}_{i+1}$-conservative under R^{i+1}_2 for $i \geq 1$, $T_2^{0,\{2^{(||\mathrm{id}||)}\}}$ seems like such a candidate. We denote by $T^{0,\tau}_2$ the theory which has sharply bounded induction up to terms from a set τ of nondecreasing 0- or 1-ary terms. It is straightforward to come up with a theory of $T^{0,\tau}_2$'s $\hat{\Sigma}^{\mathsf{b}}_0$-consequences: One restricts the cut-rule in the sequent calculus formulation of $T^{0,\tau}_2$ to only allow $\hat{\Sigma}^{\mathsf{b}}_0$-formulas to occur as either the principal or side formulas. Using cut-elimination, one can show this theory, which we will call $T^{-1,\tau}_2$, is $\hat{\Sigma}^{\mathsf{b}}_0$-conservative under $T^{0,\tau}_2$. This result applies to both $T_2^{i,\{2^{(||\mathrm{id}||)}\}}$ and T^0_2 and makes progress towards understanding the $\hat{\Sigma}^{\mathsf{b}}_0$-consequences of R^1_2. We would like to argue that $T^{-1,\tau}_2$ is weak enough that it could be potentially useful in separations. As a first step to seeing this we use a witnessing argument and Johannsen's [19] block-counting technique to show this theory cannot $\hat{\Sigma}^{\mathsf{b}}_1$-define divisibility by 3, so this theory is strictly weaker than $T^{0,\tau}_2$. Unfortunately, this same block counting technique shows that $T_2^{0,\{2^{(||\mathrm{id}||)}\}}$ is not $\forall\Sigma^{\mathsf{b}}_1$-conservative under R^1_2.

Although $T_2^{0,\{2^{(||\mathrm{id}||)}\}}$ does not turn out to be $\forall\Sigma^{\mathsf{b}}_1$-conservative under R^1_2, by examining Jeřábek's proof of the T^0_2 result, we are able to come up with theories which correspond to the $\forall\hat{\Sigma}^{\mathsf{b}}_1$-consequences of R^1_2. The key step in Jeřábek's proof is showing that if a Σ^{b}_0 formula ϕ is safe for bit recursion then T^0_2 can prove the following comprehension scheme:

$$\exists! w(|w| \leq |a| \wedge (\forall i < |a|)(i \in w \Leftrightarrow \phi(i, w))).$$

This safety condition is that all occurrences of w in ϕ occur inside a subformula of the form $t > i \wedge t \in w$ for some term t not containing w. This allows ϕ to have access to the string w that is being defined provided that access is to bits to the left of the ones that have yet to be fixed. We come up with a similar notion for open formulas and we define a class $open_\tau$ of *open*-formulas which are w-restricted-by-intervals of recursion depth τ. Unlike Jeřábek's notion our condition on *open*-formulas is specifically tailored to the kinds of recursions that need to be handled in the witnessing argument. This would presumably allow further tweaks of our class to handle other theories we do not consider such as theories for logspace or other complexity classes. We show the theory $R[1,\tau] := \mathit{LIOpen}{+}\mathit{BB}\hat{\Pi}^{\mathsf{b}}_0{+}\hat{\Sigma}^{\mathsf{b}}_1\text{-}\mathit{IND}^\tau$ is $\forall\hat{\Sigma}^{\mathsf{b}}_1$-conservative over $\mathit{TComp}^\tau := \mathit{LIOpen}{+}\hat{\Pi}^{\mathsf{b}}_0\text{-}\mathit{IND}^\tau{+}\mathit{open}_\tau\text{-}\mathit{COMP}$. We give a normal form for proofs of this conservativity involving only one use of comprehension. Here *LIOpen* is *BASIC* together with length-induction for *open*-formulas. From this result we are able to show, T^0_2 can be alternately defined by restricting the induction axioms to sharply bounded formula of only one alternation. We are also able to give a theory $\mathit{TComp}^{\{||id||\}}$ for the $\forall\hat{\Sigma}^{\mathsf{b}}_1$-consequences of R^1_2. Finally, we can tighten the characterization of the $\forall\hat{\Sigma}^{\mathsf{b}}_1$-consequences of $\hat{C}^0_2$, a theory for constant depth threshold circuits given in Johannsen and Pollett [20][21], to the theory consisting of *LIOpen* together with $\mathit{open}_{\mathrm{cl}}$-comprehension axioms. Very recently, L. A. Kołodziejczyk, Phuong Nguyen and Neil Thapen [14] have come up with a local improvement principle characterization of the $\forall\Sigma^{\mathsf{b}}_0$-consequences of S^1_2. Their development is in a second-order theory and they use the RSUV isomorphism to obtain their results.

This paper is organized as follows: In the next section we present the bounded arithmetic theories used in this paper. Then we present our results about $\forall\hat{\Sigma}^{\mathsf{b}}_0$-theories and separations via block-counting. We next define our comprehension theories and do bootstrapping on these theories to show simple facts they can prove. The paper concludes with our comprehension conservativety results.

2 Preliminaries

This paper assumes some knowledge of bounded arithmetic such as may be found in Buss [6], Hájek and Pudlák [12], Krajíček [15], or Cook and Nguyen [8]. This section will briefly fix some of the notations and definitions we will need for the remainder of the paper. To start we will be interested in the language L_2 which consists of 0, S, $+$, $x \dot{-} y := \max(0, x-y)$, '$\cdot$', $\mathrm{MSP}(x,y) := \lfloor \frac{x}{2^y} \rfloor$, $|x|$, $x\#y := 2^{|x||y|}$ and $\leq$. We will use as our base theory the 12 open axioms for *BASIC* given in Jeřábek [18] together with the two axioms from Allen [1] for $x \dot{-} y$:

$$x \dot{-} y = 0 \Leftrightarrow x \leq y. \tag{1}$$

$$x \leq y \supset (x \dot{-} y) + y = x \tag{2}$$

It will turn out to be convenient to have limited subtraction in the language so that we can do sequence coding directly using terms.

In the language L_2 we will consider various hierarchies of formulas. For an L_2-formula, a quantifier of the form $(\forall x \leq t)$ or $(\exists x \leq t)$ where t is a term not containing x is called a *bounded quantifier.* A quantifier of the form $(\forall x \leq |t|)$ or of the form $(\exists x \leq |t|)$ is called *sharply bounded* and a formula is *sharply bounded* if all its quantifiers are. The bounded formulas of L_2 are classified into hierarchies Σ^{b}_i and Π^{b}_i by counting alternations of quantifiers, ignoring sharply-bounded quantifiers. Formally, a Σ^{b}_0 (Π^{b}_0) formula is one in which all quantifiers are sharply-bounded. The $\Sigma^{\mathsf{b}}_{i+1}$ (Π^{b}_{i+1}) formulas contain the $\Sigma^{\mathsf{b}}_i \cup \Pi^{\mathsf{b}}_i$ formulas and are closed under $\neg A$, $A \supset B$, $B \wedge C$, $B \vee C$, sharply-bounded quantification, and bounded existential (universal) quantification, where A is Π^{b}_{i+1} $(\Sigma^{\mathsf{b}}_{i+1})$ and B and C are $\Sigma^{\mathsf{b}}_{i+1}$ (Π^{b}_{i+1}). In Pollett [24] prenex hierarchies of formulas $\hat{\Sigma}^{\mathsf{b}}_i$ and $\hat{\Pi}^{\mathsf{b}}_i$ were developed. Let $\hat{\Sigma}^{\mathsf{b}}_{-1} = \hat{\Pi}^{\mathsf{b}}_{-1}$ be the *open*-formulas. A formula is $\hat{\Sigma}^{\mathsf{b}}_i$ (resp. $\hat{\Pi}^{\mathsf{b}}_i$ if it is in $\Sigma^{\mathsf{b}}_i \setminus \Pi^{\mathsf{b}}_{i-1}$ (resp. $\hat{\Pi}^{\mathsf{b}}_i \setminus \hat{\Sigma}^{\mathsf{b}}_{i-1}$) and consists exactly $i+1$ bounded quantifiers, the innermost being sharply bounded, followed by an *open* matrix. If a theory is strong enough to prove the $BB\hat{\Sigma}^{\mathsf{b}}_i$ axioms (defined below), then it can be proven in this theory [24] that any Σ^{b}_i-formula is equivalent to a $\hat{\Sigma}^{\mathsf{b}}_i$-formula. A similar result holds for Π^{b}_i and $\hat{\Pi}^{\mathsf{b}}_i$-formulas. For this paper we will be interested in the theories R^1_2 and S^1_2 which can prove $\hat{\Sigma}^{\mathsf{b}}_1$-collection. Sometimes the structure of $\hat{\Sigma}^{\mathsf{b}}_i$ and $\hat{\Pi}^{\mathsf{b}}_i$ will be a little too fixed for our purposes. Given a class of formulas Ψ, we write $L\Psi$ for those formulas which can be made into Ψ formulas by adding "dummy" quantifers. For example, we are interested in classes like $L\hat{\Sigma}^{\mathsf{b}}_i$. We will also write expressions like $E\Psi$ (resp. $A\Psi$) to indicate a formula consisting of a bounded existential (resp. universal) quantifier followed by a Ψ-formula. We write E_τ or A_τ if we want to indicate that the quantifier has a bound coming from terms in τ.

We formulate our theories in the sequent calculus deduction system LKB of Buss [6] which extends the usual sequence calculus LK to directly handle bounded quantifiers. We consider theories where we extend the different $BASIC$ axioms above by various inductions schemas:

Definition 1 *Let τ be a collection of* 0 *or* 1*-ary terms. A Ψ-IND^τ inference is an inference:*

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

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

The formulas A in the above we call the *principal formulas* of the inference; all other other formulas are considered *side formulas.* Define $|x|_0 = x$, and $|x|_{m+1} = ||x|_m|$. Let $\mathrm{id}(x) := x$ be the identity function. The notations *IND*, *LIND*, *LLIND* will be used instead of $\mathit{IND}^{\{\mathrm{id}\}}$, $\mathit{IND}^{\{|\mathrm{id}|\}}$, and $\mathit{IND}^{\{||\mathrm{id}||\}}$. *BASIC* formulated in *LKB* extended by Ψ-IND^τ inferences, without any restrictions on cut, proves the same theorems as *BASIC* together with the following Ψ-IND^τ axioms [6],[24]:

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

where A is from Ψ and ℓ is from τ.

Definition 2 ($i \geq 0$) *The theories T^i_2, S^i_2, R^i_2 are BASIC+Σ^{b}_i-IND and BASIC+Σ^{b}_i-LIND, BASIC+Σ^{b}_i-LLIND respectively.*
We define $S_2 := \cup_i S^i_2$.

That S^i_2 and T^i_2 can be equivalently defined using $\hat{\Sigma}^{\mathsf{b}}_i$-induction schemas rather than Σ^{b}_i-schemas was shown in Pollett [24]. From Buss [6], it is it known for $i \geq 0$ that

$$S^i_2 \subseteq T^i_2 \subseteq S^{i+1}_2.$$

In the remainder of this section we recall the pairing function from Clote and Takeuti [10], and the coding scheme from Pollett [24]. Pairing and coding will be need to present our collection axioms. Our approach is not quite the same as these earlier papers in that we will define a function $\mathrm{BLK}(a, b, w)$ used to project out b bits starting at bit position a from w, which does not occur in those papers, but which will be useful in later sections.

Definition 3 *Given a term $t \in L_2$ we define a monotonic term t^+ as follows: If t is constant or a variable, then $t = t^+$. If t is $f(s)$, where f is a unary function symbol, then t^+ is $f(s^+)$. If t is $s_1 \circ s_2$ for $\circ$ a binary operation other than $\dot{-}$ or MSP, then t^+ is $s^+_1 \circ s^+_2$. Lastly, if t is $s_1 \dot{-} s_2$ or $\mathrm{MSP}(s_1, s_2)$, then t^+ is s^+_1.*

It is easily proved in $BASIC$+*open*-$LIND$ that t^+ is monotonic, and $t \leq t^+$.

The following terms will be used frequently below. Let

$$\begin{aligned}
2^{|x|} &:= 1\#x \\
\mathrm{mod2}(x) &:= x \dot{-} 2\cdot\lfloor\frac{1}{2}x\rfloor \\
\mathrm{BIT}(i,x) &:= \mathrm{mod2}(\mathrm{MSP}(x,i)) \\
2^{\min(x,|y|)} &:= \mathrm{MSP}(2^{|y|}, |y| \dot{-} x) \\
\mathrm{cond}(x,y,z) &:= 1 \dot{-} x\cdot y + (1 \dot{-} (1 \dot{-} x))\cdot z \\
\mathrm{LSP}(x,i) &:= x \dot{-} 2^{\min(i,|x|)}\cdot\mathrm{MSP}(x,i) \\
\mathrm{BLK}(a,b,w) &:= \mathrm{MSP}(\mathrm{LSP}(w,a+b),a) \\
\beta_a(i,w) &:= \mathrm{BLK}(i\cdot a,a,w)
\end{aligned}$$

so that $LSP(x,|y|)$ returns the number consisting of the last $|y|$ bits of x, and if w codes a sequence $\langle b_1,\ldots,b_\ell\rangle$ with $|b_i|\leq|a|$ for all i, then $\beta_a(w,i)=b_i$. The code for this sequence is simply the number w whose binary representation consists of a 1 followed by the binary representations of the b_i concatenated, each padded with zeroes to be of exact length $|a|$. If we set $\mathrm{bd}(a,s) := 2(2a\#2s)$, then $\mathrm{bd}(a,s)$ is thus a bound on the code for a sequence of length $|s|$ with each item bounded by a.

We also define a pairing operation that does not rely on an explicitly mentioned bound. Let $B=2^{|\max(x,y)|}$. Pairs are coded as $\langle x,y\rangle := (B+y)\cdot 2B+(B+x)$. The terms $(w)_1 := \beta_{\lfloor\frac{1}{2}|w|\rfloor\dot{-}1}(0,\beta_{\lfloor\frac{1}{2}|w|\rfloor}(0,w))$ and $(w)_2 := \beta_{\lfloor\frac{1}{2}|w|\rfloor\dot{-}1}(0,\beta_{\lfloor\frac{1}{2}|w|\rfloor}(1,w))$, project out the left and right coordinates from an ordered pair. To check if w is a pair we use the formula

$$\mathrm{ispair}(w) := \mathrm{BIT}(\lfloor\frac{1}{2}|w|\rfloor \dot{-} 1, w) = 1 \wedge 2\cdot|\max((w)_1,(w)_2)|+2=|w|\ .$$

Definition 4 *For a class of formulas Ψ, the collection inference $BB\Psi$ (sometimes called Ψ-replacement) is*

$$\frac{\Gamma\rightarrow(\exists y\leq t(x))A(x,y),\Delta}{\Gamma\rightarrow(\exists w\leq\mathrm{bd}(t^+(|s|),s))(\forall x\leq|s|)\beta_{t^+(|s|)}(x,w)\leq t(x)\wedge A(x,\beta_{t+(|s|)}(x,w)),\Delta}$$

for each $A(x,y)\in\Psi$.

Pollett [24] gives an alternative formulation of R^i_2 as $BASIC$+$\hat{\Sigma}^{\mathsf{b}}_i$-$LLIND$+$BB\hat{\Sigma}^{\mathsf{b}}_i$ which we will make use of in a latter section.

3 Σ_0^{b}-theories and Σ_∞^τ-witnessing

In this section, we examine deduction systems which are sharply bounded in nature. We give one system which characterizes the $\forall\Sigma_0^{\mathsf{b}}$-consequences of T_2^0. We also give an upper bound on definability in such theories.

Definition 5 *The theory $T_2^{-1,\tau}$ is the theory whose consequences can be derived in the LKB deduction system with BASIC axioms and allowing $\hat{\Sigma}_0^{\mathsf{b}}$-IND$^\tau$ rules of inference with only $\hat{\Sigma}_0^{\mathsf{b}}$-side formulas. We write T_2^{-1} as a shorthand for $T_2^{-1,\{id\}}$.*

We next show that $T_2^{0,\tau}$ is $\forall\Sigma_0^{\mathsf{b}}$-conservative over $T_2^{-1,\tau}$ in the sense of the following two theorems.

Theorem 1 *Suppose $T_2^{0,\tau}$ proves $A(\mathbf{a})$ where A is a Σ_0^{b} formula, then $T_2^{-1,\tau}$ proves $A(\mathbf{a})$.*

Proof. If $T_2^{0,\tau}$ proves a Σ_0^{b}-formula A, then A has free-cut free sequent calculus proof [6]. But such a proof will only involve Σ_0^{b}-formulas, so would constitute a $T_2^{-1,\tau}$ proof. □

We have only formulated $T_2^{-1,\tau}$ as a deduction system, and have not given an axiomatization of this theory. To show we are accurately capturing the $\forall\hat{\Sigma}_0^{\mathsf{b}}$-consequences of $T_2^{0,\tau}$ we need to show that whenever something is provable in $T_2^{-1,\tau}$ then it also follows from the $\forall\Sigma_0^{\mathsf{b}}$-consequences of $T_2^{0,\tau}$.

Theorem 2 *Suppose $T_2^{-1,\tau}$ proves a formula $A(\mathbf{a})$, then there is a finite set of Σ_0^{b}-formulas Γ provable in $T_2^{0,\tau}$ such that $\Gamma \vdash A(\mathbf{a})$.*

Proof. Let G be the set of open sequents in a free-cut free $T_2^{-1,\tau}$ proof P of $A(\mathbf{a})$, a Σ_0^{b}-formula. Each sequent $\Omega \to \Lambda$ in G has a $T_2^{-1,\tau}$ proof, and this same proof is also a $T_2^{0,\tau}$ proof. It is also immediate that the open formula $\bigwedge\!\!\!\bigwedge \Omega \supset \bigvee\!\!\!\bigvee \Lambda$ is provable in $T_2^{0,\tau}$ and implies the sequent $\Omega \to \Lambda$. Let Γ be the set of open formulas constructed in this manner from the sequents in G. Given the definition of $T_2^{-1,\tau}$, the sequents of P not in G are all derived by structural, logical, or quantifier inferences. If we took as a set of axioms the set of first open sequents on any path back through the proof P from $\to A$ to the leaves, then $\to A$ follows from these axioms and these axioms are implied by Γ. □

Since S_2^1 is Σ_1^{b}-conservative over T_2^0 it is immediately follows that:

Corollary 1 *The $\forall\Sigma^{\mathsf{b}}_0$ theorems of S^1_2 are precisely the theorems of T^{-1}_2.*

For the rest of this section we work towards an upper bound with regard to definability in $T^{-1,\tau}_2$. We work in a general set-up which will allow us to derive the results of the next section as well. By $(\mu i \leq t(\mathbf{a}))(f(i,\mathbf{a}) = 0)$ (bounded μ-operator), we mean the function which returns the least $i \leq t$ such that $f(i,\mathbf{a}) = 0$ if such an i exists and returns $i+1$ otherwise.

Definition 6 *Let τ be a collection of nondecreasing 0 to 1-ary terms, with at least one term ℓ such that BASIC proves $\forall x \geq S^n(0)\ell(x) \geq |x|$ for some n. A Σ^τ_∞* formula *is a bounded formula, all of whose bounded quantifiers have bounding terms of the form $\ell(t)$ where $\ell \in \tau$ and t is a term. The class $\mathcal{A}\Sigma^\tau_\infty$ is defined to be the smallest function algebra which contains the L_2-terms, and is closed under composition and $(\mu i \leq \ell(t))(f = 0)$ for $\ell \in \tau$, t is a term, and $f \in \mathcal{A}\Sigma^\tau_\infty$.*

The condition on containing at least one ℓ which grows faster than $|x|$, is to ensure the Σ^τ_∞ formulas contain the Σ^{b}_0-sets. We also have

Lemma 1 *Given A in Σ^τ_∞ there is an function $f_A \in \mathcal{A}\Sigma^\tau_\infty$ such that $f_A = 0$ iff A holds.*

Proof. This is proven by induction on the complexity of A. Given any atomic formula $s \leq t$, we can define $f_{s\leq t}$ as $1 \dot{-} ((t+1) \dot{-} s)$. To handle A which is a boolean combination of subformulas for which we already have defining functions, we can build f_A, using the functions $K_\wedge(b,c) := b + c$ and $K_\neg(b) := 1 \dot{-} b$. For A of the form $\forall x \leq \ell(t)B$, we define

$$f_A := (\mu x \leq \ell(t))(f_B = 0) \dot{-} \ell(t).$$

Finally, for A of the form $\exists x \leq \ell(t)B$ we rewrite this as $\neg\forall x \leq \ell(t)\neg B$. □

A bounding term and witness predicate for Σ^τ_∞-formulas are now defined.

- If $A(\mathbf{a}) \in \Sigma^\tau_\infty$ then $t_A = 0$ and $WIT^\tau_A(w,\mathbf{a}) := A(\mathbf{a}) \wedge w = 0$.
- If $A(\mathbf{a}) \in E\Sigma^\tau_\infty \setminus \Sigma^\tau_\infty$ is of the form $\exists x \leq tB(x,\mathbf{a})$ where $B(x,\mathbf{a})$ is from Σ^τ_∞, then $t_A := t^+_A$ and

$$WIT^\tau_A(w,\mathbf{a}) := w \leq t \wedge WIT^\tau_B(w,\mathbf{a})\ .$$

The following lemma is immediate from Σ^τ_∞ being witness suitable and from the definition of witness predicates:

Lemma 2 *If $A(\mathbf{a}) \in LE\Sigma^\tau_\infty$, then:*

(1) WIT^τ_A is a Σ^τ_∞-predicates.

(2) $BASIC \vdash \exists w \leq t_A(\mathbf{a})\, WIT^\tau_A(w, \mathbf{a}) \supset A(\mathbf{a})$.

The witness predicate is extended to a witness predicate on cedents using iterated pairing as was done in [6][25].

Definition 7 *A deduction system T is Σ^τ_∞-*suitable *if it is an extension of LKB, all of its axioms are Σ^τ_∞-formulas, free-cut free elimination can be carried out for T, and the new rules of inference in T only allow Σ^τ_∞-formulas in the lower sequent.*

Since $T_2^{-1,\tau}$ only allows induction inferences in which all the side-formulas are $\Sigma^{\mathsf{b}}_0 = \Sigma^{\{|\mathsf{id}|\}}_\infty$, it follows that $T_2^{-1,\tau}$ is $\Sigma^{\{|\mathsf{id}|\}}_\infty$-suitable. As another example, if one formulates $T_2^{0,\tau}$ with axioms for its induction principles rather than induction inferences, then the resulting theory will be Σ^τ_∞-suitable.

Theorem 3 *Let T be Σ^τ_∞-suitable. Suppose*

$$T \vdash \Gamma \rightarrow \Delta$$

where Γ and Δ are cedents of $LE\Sigma^\tau_\infty$-formulas. Let $\mathbf{a}$ *be the free variables in this sequent. Then there is a $\mathcal{A}\Sigma^\tau_\infty$ function f such that*

$$\mathbb{N} \models WIT^\tau_{\wedge\Gamma}(w, \mathbf{a}) \rightarrow WIT^\tau_{\vee\Delta}(f(w, \mathbf{a}), \mathbf{a}).$$

Proof. This is proven by induction on the number of sequents in an T-proof of $\Gamma \rightarrow \Delta$. By cut-elimination, we can assume all the sequents in the proof are in $LE\Sigma^\tau_\infty$. In the base case, the proof consists of sequent $\rightarrow A$ where A is a logical axiom, an equality axiom, a $BASIC$ axiom, or an axiom of T. Since T is Σ^τ_∞-suitable, in each of these cases the witness predicate is $A \wedge w = 0$. So we can choose f to be the zero function. The weak inferences, structural inferences, and cut can be handled in essentially the same way as in the S^i_2 case of the witnessing argument in Buss [6]. We show the ($\exists$ $\leq$:left), ($\exists$ $\leq$:right) cases, and T-rule cases — ($\forall$ $\leq$:left), ($\forall$ $\leq$:right) cases are handled similarly.

($\exists$:left case)

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

By hypothesis there is a $g \in \mathcal{A}\Sigma^\tau_\infty$ such that

$$\mathbb{N} \models \mathit{WIT}^\tau_{b \le t \wedge A \wedge (\wedge \Gamma)}(w, \mathbf{a}, b) \supset \mathit{WIT}^\tau_{\vee\Delta}(g(w, \mathbf{a}, b), \mathbf{a}, b).$$

There are two subcases. In each case, we need to determine a value for the free variable b and then run g using that value. First, suppose $(\exists x \le t)A(x) \in E\Sigma^\tau_\infty$. If w is a witness for $(\exists x \le t)A(x) \wedge \Gamma$, then $(w)_1$ is a value for b such that $A(b)$ holds. Let our new witness function be

$$f(w, \mathbf{a}) = g(\langle\langle 0, 0, (w)_2\rangle\rangle, \mathbf{a}, (w)_1).$$

This is in $\mathcal{A}\Sigma^\tau_\infty$ and fulfills the requirement that:

$$\mathbb{N} \models \mathit{WIT}^\tau_{(\exists x \le t) A \wedge (\wedge \Gamma)}(w, \mathbf{a}) \supset \mathit{WIT}^\tau_{\vee\Delta}(f(w, \mathbf{a}), \mathbf{a}).$$

The second case is when $(\exists x \le t)A(x) \in \Sigma^\tau_\infty$. In this case, let f_A be the function in $\mathcal{A}\Sigma^\tau_\infty$ which by Lemma 1 has the property that $f_A(x) = 0$ iff $A(x)$. We define f to be the same as in the above case except rather than use $(w)_1$ to give a value b we instead use the $\mathcal{A}\Sigma^\tau_\infty$ function $(\mu x \le t)[f_A(x) = 0]$ to give a value for b.

($\exists$:right case)

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

By hypothesis there is a $g \in \mathcal{A}\Sigma^\tau_\infty$ such that

$$\mathbb{N} \models \mathit{WIT}^\tau_{\wedge\Gamma}(w, \mathbf{a}) \supset \mathit{WIT}^\tau_{A(t) \vee (\vee \Delta)}(g(w, \mathbf{a}), \mathbf{a}).$$

The definition of WIT^τ implies

$$\mathbb{N} \models \mathit{WIT}^\tau_{t \le s \wedge (\wedge \Gamma)}(w, \mathbf{a}) \supset t \le s \wedge \mathit{WIT}^\tau_{\wedge\Gamma}((w)_2, \mathbf{a}).$$

If $(\exists x \le s)A(x) \in E\Sigma^\tau_\infty$ define $f := \langle t(\mathbf{a}), (g((w)_2, \mathbf{a}))_2\rangle$. Otherwise, define $f := g((w)_2, \mathbf{a}))$.

These functions are all $\mathcal{A}\Sigma^\tau_\infty$ and satisfy:

$$\mathbb{N} \models \mathit{WIT}^\tau_{t \le s \wedge (\wedge \Gamma)}(w, \mathbf{a}) \supset \mathit{WIT}^\tau_{(\exists x \le s) A(x) \vee (\vee \Delta)}(f(w, \mathbf{a}), \mathbf{a}).$$

(T-rule case) Suppose the lower sequent of a T-rule is $\Gamma \rightarrow \Delta$. Since the lower sequent of a T-rule involves only Σ^τ_∞-formulas, witnesses for both Γ and Δ can be directly built-up using pairing and 0. So the witness function can ignore its input and just output the appropriate witness pairing for Δ.

This completes all possible cases and the proof. □

Corollary 2 *The $\Sigma_{\infty}^{\{|id|\}}$-definable functions of T_2^{-1} and S_2^0 are contained in $\mathcal{A}\Sigma_{\infty}^{\{|id|\}}$. As $\Sigma_0^{\mathsf{b}} = \Sigma_{\infty}^{\{|id|\}}$, it follows both the Σ_0^{b}-definable functions of these theories are contained in $\mathcal{A}\Sigma_{\infty}^{\{|id|\}}$.*

Proof. Let T be either T_2^{-1} or S_2^0. If T can $\Sigma_{\infty}^{\{|id|\}}$-define a function f, then there is some $\Sigma_{\infty}^{\{|id|\}}$-formula $A_f(\mathbf{a}, b)$ defining its graph such that T proves $\forall \mathbf{x} \exists y A_f(\mathbf{x}, y)$. So Parikh's Theorem implies $T \vdash\longrightarrow \exists y \leq t A_f(\mathbf{a}, y)$ for some term t. So the result then follows from Theorem 3 taking Γ to be empty and Δ to be A_f. $\Box$

Essentially the same proof, but choosing $T = T_2^{0,\{2^{(||\mathrm{id}||)}\}}$, gives:

Corollary 3 *The $\Sigma_{\infty}^{\{2^{(||\mathrm{id}||)}\}}$-definable functions of $T_2^{0,\{2^{(||\mathrm{id}||)}\}}$ are contained in $\mathcal{A}\Sigma_{\infty}^{\{2^{(||\mathrm{id}||)}\}}$.*

4 Separations

We next use our witnessing result to prove a sequence of separations of bounded arithmetic theories. We first show that T_2^{-1} is a strictly weaker theory than T_2^0, then we show that R_2^1 is not $\forall\hat{\Sigma}_1^{\mathsf{b}}$-conservative over $T_2^{0,\{2^{(||\mathrm{id}||)}\}}$.

Definition 8 *The function $\#_B(x)$ returns the number of alternations between 1 and 0 in reading the binary number x from left to right. We start the counting of this number at 1 so $\#_B(1) = 1$.*

As an example, let x be the binary number 1010011 then $\#_B(x) = 5$. The following lemma is a consequence of Lemma 35 in Pollett [25] once one notices that $\#_B((\mu i \leq \ell(t(\mathbf{x}))(f = 0)) \leq |\ell(t^+(\mathbf{x}))|$.

In what follows, let ℓ', ℓ be either the pair $|x|$ and $2^{||x||^2}$ or the pair $2^{2^{|||x|||^2}}$ and $2^{|x|}$.

Lemma 3 *Suppose for every $\ell'' \in \tau$, $\ell''(x) \in O(\ell'(x))$. If $f(\mathbf{x}) \in \mathcal{A}\Sigma_{\infty}^{\tau}$ and $\#_B(x_i) \leq |\ell(x_i)|$ then $\#_B(f(\mathbf{x})) \leq c \cdot (|\ell'(x_1)| + \cdots + |\ell'(x_n)|)^d$ for some fixed integers c and d.*

Theorem 4 *Let τ, ℓ', and ℓ be as above. Then $\mathcal{A}\Sigma_{\infty}^{\tau}$ does not contain $\lfloor \frac{\ell(x) \dot{-} 1}{3} \rfloor$.*

Proof. Notice $\#_B(\ell(x) \dot{-} 1) = 1$, yet $\lfloor \frac{\ell(x) \dot{-} 1}{3} \rfloor$ is a number of length $|\ell(x)| - 1$ of the form $1010\cdots$. Hence, $\#_B(\lfloor y \rfloor) = |\ell(x)| - 1 > |\ell'(x)|^d$ for any fixed d provided x is large enough. So by Lemma 3, $\lfloor \frac{\ell(x) \dot{-} 1}{3} \rfloor$ is not in $\mathcal{A}\Sigma^{\tau}_{\infty}$. □

The choices of ℓ' and ℓ in the above are for expediency to the particular results we obtain below and could have been relaxed considerably while still having Theorem 4 hold.

Theorem 5 *Let ℓ be as above. The theory $T_2^{0,\{\ell\}}$ can prove:*

$$\exists z \leq \ell(x)(3 \cdot z = \ell(x) \vee 3 \cdot z + 1 = \ell(x) \vee 3 \cdot z + 2 = \ell(x)). \tag{3}$$

Proof. Consider the Σ_0^{b}-formula $A(y, x)$ defined as $B(\ell(x) \dot{-} y, x)$ where $B(y, x)$ is:

$$\begin{aligned} |y| \leq |\ell(x)| \wedge \forall i \leq |\ell(x)| \forall j \leq |\ell(x)| [j > i \supset \\ 3 \cdot \mathrm{MSP}(y, j) \geq MSP(\ell(x), j) \vee \\ 3 \cdot \mathrm{MSP}(y, j) + 1 = MSP(\ell(x), j) \vee \\ 3 \cdot \mathrm{MSP}(y, j) + 2 = MSP(\ell(x), j)] \end{aligned}$$

Then $A(0, x)$ holds, but $A(\ell(x), x)$ does not. So $T_2^{0,\{\ell\}}$ proves by Σ_0^{b}-IND^{ℓ} that $\exists y \leq \ell(x)(A(y, x) \wedge \neg A(Sy, x))$. It is not hard to see that Sy satisfies the existential in the formula (3). □

Corollary 4 *T_2^0 is not $E open$-conservative over T_2^{-1}.*

Proof. Consider the *Eopen* statement of Theorem 5 where $\ell := 2^{|x|}$. The theory $T_2^0 \supseteq T_2^{0,\{\ell\}}$ proves this statement. On the other hand, by Theorem 4 and Corollary 2, the theory T_2^{-1} does not. □

The same proof also gives:

Corollary 5 *Let ℓ and τ be as above. Then $T_2^{0,\{\ell\}}$ is not E_{ℓ}open-conservative over $T_2^{0,\tau}$. So $S_2^0 = T_2^{0,\{|id|\}} \subsetneq T_2^{0,\{2^{||x||^2}\}} \subseteq T_2^{0,\{2^{(||\mathrm{id}||)}\}}$.*

We now turn our attention to the R_2^1 versus $T_2^{0,\{2^{(||\mathrm{id}||)}\}}$ result.

Corollary 6

$T_2^{0,\{2^{(||\mathrm{id}||)}\}}$ cannot $\Sigma_{\infty}^{\{2^{(||\mathrm{id}||)}\}}$-define $\lfloor \frac{2^{|x|} \dot{-} 1}{3} \rfloor$.

R^1_2 is not $\forall\hat{\Sigma}^{\mathsf{b}}_1$-conservative over $T_2^{0,\{\mathit{2}^{(||\dot{\mathrm{id}}||)}\}}$ or any $T_2^{0,\tau}$ where τ is as above.

Proof. The first result follows from Theorem 4 and Corollary 2. For the second result, R^1_2 can $\hat{\Sigma}^{\mathsf{b}}_1$ define any function in uniform NC [29] and so can define $\lfloor \frac{x}{3} \rfloor$. Then observe $LE\Sigma_\infty^{\{\mathit{2}^{(||\dot{\mathrm{id}}||)}\}}$ contains $\hat{\Sigma}^{\mathsf{b}}_1$-formulas. □

5 Comprehension Theories and Bootstrapping

In this section, we examine how much needs to be added to $T_2^{0,\{\mathit{2}^{(||\dot{\mathrm{id}}||)}\}}$ in order to make it $\hat{\Sigma}^{\mathsf{b}}_1$-conservative under R^1_2. We will develop theories based on variants of *open*-comprehension axioms and prove these theories' definable functions are closed under various operations.

Definition 9 *Ψ-COMP axioms are substitution instances of the axioms $COMP_A$:*

$$(\exists w \le 2^{|a|})(\forall i \le |a|)\big(\mathrm{BIT}(i,w) = 1 \Leftrightarrow A(i,a,\mathbf{b})\big) \ .$$

where A is a Ψ-formula.

Definition 10 *Let LIOpen be the theory BASIC+open-LIND.*

Pollett [24] shows the next result which in turn implies the w given by the *open-COMP* rule is unique.

Lemma 4 *LIOpen proves the bit-extensionality axiom:*

$$|a| = |b| \wedge (\forall i \le |a|)\big(\mathrm{BIT}(i,a) = \mathrm{BIT}(i,b)\big) \supset a = b \ .$$

Notice the formula A in *open-COMP* does not involve w. This rules out situations which would contradict the existence of w such as $A(i,w) := \mathrm{BIT}(i,w) = 0$. We next consider one way to extend the *open-COMP* axioms to allow for the use of a w in A. To extend the comprehension axiom, we split up the string w we are defining into bit intervals. That a variable i defining a bit position of w belongs to such an interval can be expressed as an *open*-formula:

$$\mathrm{i} \in [\mathrm{a}, \mathrm{b}) \quad := \quad a \le i \wedge i < b$$

We are interested in intervals of the form: $\mathrm{i} \in [\mathrm{a}, \mathrm{a} + \mathrm{c} \cdot 2^{\min(\mathrm{b},|\mathrm{d}|)})$, which start at a bit position a and go for c blocks of b-bits. We will tend to suppress d when it is clear that $b \leq |d|$ for some d. Since we can only easily express divisibility by 2 as a term in our language, we will tend to use $\mathrm{i} \in [\mathrm{a}, \mathrm{a} + \mathrm{c} \cdot 2^{\min(\mathrm{b},|\mathrm{d}|)})$ where a is of the form $2^{||a'||}$ and b is of the form $||b'||$. Suppose we use an open formula $A(i, w, \mathbf{z})$ to define w. In our definition below, we will restrict A's access to w in one of three ways: (1) it makes no mention of w. (2) If we already had a way to mention w in $B(i, w, j, \mathbf{z})$ for $\mathrm{i} \in [0, 2^{||\mathrm{t}||})$ that allows for comprehension, and we consider those cases where $j \leq |s|$, then we allow A to be $B(i \dot{-} \lfloor \frac{i}{2^{||t||}} \rfloor \cdot 2^{||t||}, w, \lfloor \frac{i}{2^{||t||}} \rfloor, \mathbf{z})$ on $\mathrm{i} \in [0, |\mathrm{s}| \cdot 2^{||\mathrm{t}||})$. (3) We allow A access to w on a range $[0, 2^{||r^+||} + \ell \cdot 2^{||s^+||})$ if A meets the following criteria: (a) For A in the bit range $[0, 2^{||r^+||})$, A is given by some formula $B_0(j, w', \mathbf{b})$ where B_0 is a formula such that if w' has length less than $2^{||r^+||}$, we can do comprehension for B_0 with respect to this variable. (b) For A in the bit range $[2^{||r^+||}, 2^{||r^+||} + \ell \cdot 2^{||s^+||})$, A is defined using a formula $B_1(i, w', v', n, \mathbf{b})$ such that if w' has length less than $2^{||s^+||}$ we can do comprehension for B_1 with respect to w'. (c) For A in the bit range $[2^{||r^+||}, 2^{||r^+||} + 2^{||s^+||})$, we project out the $2^{||s^+||}$ bits from $[2^{||r^+||}, 2^{||r^+||} + 2^{||s^+||})$ and use these for w' and we use bits $[0, 2^{||r^+||})$ of w for v'. (d) For A in a bit range of the form $[2^{||r^+||} + j \cdot 2^{||s^+||}, 2^{||r^+||} + (j+1) \cdot 2^{||s^+||})$, we project out these bits from w and use them for w' and we project out the previous $2^{||s^+||}$ bits and use them for v'.

These conditions on A's access to w were tailored so that we could prove functions defined using comprehension had certain closure properties. Condition (2) will be used to show the comprehension-defined functions are closed under a kind of concatenation recursion and Condition (3) will be used to show the comprehension-defined functions are closed under a kind of bounded primitive recursion as well as composition. We now give a more precise definition of our conditions which will show that we can express the above using open formulas.

Definition 11 *Let τ be a set of nondecreasing 0 or 1-ary terms. An open-formula $A(i, w, \mathbf{b})$ is w-restricted-by-intervals to recursion depth τ if:*

(1) A does not involve w,

(2) A is of the form $\mathrm{i} \in [0, |\mathrm{s}| \cdot 2^{||\mathrm{t}||}) \wedge B(i \dot{-} \lfloor \frac{i}{2^{||t||}} \rfloor \cdot 2^{||t||}, \beta_{2^{||t||}}(\lfloor \frac{i}{2^{||t||}} \rfloor, w), \lfloor \frac{i}{2^{||t||}} \rfloor, \mathbf{b})$, where $B(i, w, a, \mathbf{b})$ is w-restricted-by-intervals to recursion depth τ, and s, t are terms not involving w or i.

(3) A is a disjunction of a formula

$$\mathrm{i} \in [0, 2^{||\mathrm{r}^+||}) \wedge B_0(i, \mathrm{BLK}(0, 2^{||r^+||} \dot{-} 1, w), \mathbf{b})$$

with a formula $C_1(r, s, \ell, B_1)$:

$$\begin{aligned}
&\mathrm{i} \in [2^{||\mathrm{r}^+||}, 2^{||\mathrm{r}^+||} + \ell \cdot 2^{||\mathrm{s}^+||}) \wedge \\
&\quad \big[\big(\lfloor \frac{i \dot{-} 2^{||r^+||}}{2^{||s^+||}} \rfloor = 0 \wedge B_1(i \dot{-} 2^{||r^+||}, \mathrm{BLK}(2^{||r^+||}, 2^{||s^+||} \dot{-} 1, w), \mathrm{BLK}(0, 2^{||r^+||} \dot{-} 1, w), 0, \mathbf{b})\big) \vee \\
&\quad \big(\lfloor \frac{i \dot{-} 2^{||r^+||}}{2^{||s^+||}} \rfloor > 0 \wedge B_1(i \dot{-} (2^{||r^+||} + \lfloor \frac{i \dot{-} 2^{||r^+||}}{2^{||s^+||}} \rfloor \cdot 2^{||s^+||}), \\
&\qquad\qquad \mathrm{BLK}(2^{||r^+||} + \lfloor \frac{i \dot{-} 2^{||r^+||}}{2^{||s^+||}} \rfloor \cdot 2^{||s^+||}, 2^{||s^+||} \dot{-} 1, w), \\
&\qquad\qquad \mathrm{BLK}(2^{||r^+||} + (\lfloor \frac{i \dot{-} 2^{||r^+||}}{2^{||s^+||}} \rfloor \dot{-} 1) \cdot 2^{||s^+||}, 2^{||s^+||} \dot{-} 1, w), \lfloor \frac{i \dot{-} 2^{||r^+||}}{2^{||s^+||}} \rfloor, \mathbf{b})\big)\big]
\end{aligned}$$

where $B_0(j, w', \mathbf{b})$, $B_1(j, w', v', n, \mathbf{b})$ are w'-restricted-by-intervals to recursion depth τ, and where r and s are terms not involving w or i, and $\ell(\mathbf{b})$ is from τ.

Let $open_\tau$ be the class of *open*-formulas which are w-restricted-by-intervals to recursion depth τ. For the remainder of this section, we assume that τ contains at least one term of growth rate provably in *BASIC* greater than or equal to $||x||$.

Definition 12 *Let $TComp^\tau$ be the theory $LIOpen$+$\hat{\Pi}^{\mathsf{b}}_0$-IND^τ+$open_\tau$-$COMP$.*

We will show $TComp^{\{||\mathrm{id}||\}}$ is $\forall\hat{\Sigma}^{\mathsf{b}}_1$-conservative under R^1_2.

Lemma 5 *Let $R[1, \tau] := LIOpen$+$BB\hat{\Pi}^{\mathsf{b}}_0$+$\hat{\Sigma}^{\mathsf{b}}_1$-$IND^\tau$. (1) $R[1, \tau]$ proves the $open_\tau$-$COMP$ axioms so contains $TComp^\tau$. (2) $BASIC$+$E_{\{|id|\}}A_{\{|id|\}}$-IND proves the $open_{\{|id|\}}$-$COMP$ axioms. (3) $LIOpen$ proves the w asserted by an $open_\tau$-$COMP$ axiom is unique.*

Proof. (1) This is proven by induction on the complexity of a given $open_\tau$-formula $A(i, w, \mathbf{b})$. To handle the base case we note that by unwinding definitions we have $\beta_1(i, w) = \mathrm{BIT}(i, w)$, and note that $R[1, \tau]$ proves

$$\forall i \leq |a| \exists! y \leq 1(A(i, w, \mathbf{b}) \Leftrightarrow y = 1 \wedge \neg A(i, w, \mathbf{b}) \Leftrightarrow y = 0)$$

Since A is open we can apply $BB\hat{\Pi}^{\mathsf{b}}_0$, to thus prove the desired $COMP_A$ axiom. Suppose A is defined by Definition 11 case (2). So A is of the form:

$$\mathrm{i} \in [0, |\mathrm{s}| \cdot 2^{||\mathrm{t}||}) \wedge B(i \dot{-} \lfloor \frac{i}{2^{||t||}} \rfloor \cdot 2^{||t||}, \beta_{2^{||t||}}(\lfloor \frac{i}{2^{||t||}} \rfloor, w), \lfloor \frac{i}{2^{||t||}} \rfloor, \mathbf{b}),$$

where by the induction hypothesis we can already prove $\mathit{COMP}_{B(i,w,n,\mathbf{b})}$. So $R[1,\tau]$ can prove

$$\forall n \leq |a| \exists w \leq 2^{|c|} \forall i \leq |c| \big(Bit(i,w) = 1 \Leftrightarrow B(i,w,n,\mathbf{b})\big)$$

The formula inside the existential is $\hat{\Pi}^{\mathsf{b}}_0$ since B is *open*, so by $BB\hat{\Pi}^{\mathsf{b}}_0$ we get:

$$\exists w' \leq \mathrm{bd}(c,a) \forall n \leq |a| \forall i \leq |c| \big(Bit(i, \beta_{|c|}(n,w')) = 1 \Leftrightarrow B(i, \beta_{|c|}(n,w'), n, \mathbf{b})\big)$$

so $R[1,\tau]$ proves comprehension for case (2) after substituting terms for a and c, and then merging the two universal quantifiers into one, everywhere replacing the two variables i and n by appropriate terms of the single merged variable. Finally, suppose $A(i,w,\mathbf{b})$ is defined by Definition 11 case (3). Let $t := 2^{2^{||r^+||} + \ell \cdot 2^{||s^+||}}$. Consider the $\hat{\Sigma}^{\mathsf{b}}_1$-formula $C(u)$:

$$\exists w \leq 2^{\min(2^{||r^+||}+(u+1)\cdot 2^{||s^+||}, |t|)} \forall i \leq |t| \big[\lfloor \frac{i \dot{-} 2^{||r^+||}}{2^{||s^+||}} \rfloor \leq u \supset \big(\mathrm{BIT}(i,w) \Leftrightarrow A(i,w,\mathbf{b})\big)\big]$$

The w asserted to exist by $C(0)$ consists of the $2^{||r^+||}$ given by B_0 concatenated with the $2^{||s^+||}$-bits of the first disjunct in C_1. Given the induction hypothesis we have comprehension for B_0 and B_1, so $R[1,\tau]$ can prove the existence of w in the $C(0)$ case. A similar argument shows $C(u) \supset C(Su)$. Thus by $\hat{\Sigma}^{\mathsf{b}}_1$-$\mathit{IND}^\tau$, $R[1,\tau]$ proves $C(\ell)$ and the w in this case is what is asserted by COMP_A axiom (as A is always false outside the specified interval).

(2) Let $T := \mathit{BASIC} + E_{\{|id|\}}A_{\{|id|\}}$-*IND* and let $A(i,w,\mathbf{b})$ be an $\mathit{open}_{\{|id|\}}$-formula. Consider the formula $\Psi(w)$:

$$\begin{gathered} |w| \leq |a| \wedge \forall i < |a| (\forall j < |a| (j > i \supset \\ (\mathrm{BIT}(j,w) = 1 \Leftrightarrow A(j,w,\mathbf{b}))) \supset (\mathrm{BIT}(i,w) = 1 \supset A(i,w,\mathbf{b}))). \end{gathered}$$

This is an $A_{\{|id|\}}E_{\{|id|\}}$-formula and T proves $\Psi(0)$ and $\neg\Psi(2^{|a|})$. Since by reverse induction one can show the $E_{\{|id|\}}A_{\{|id|\}}$-*IND* axioms imply the $A_{\{|id|\}}E_{\{|id|\}}$-*IND*, T proves the existence of a w such that $\Psi(w) \wedge \neg\Psi(Sw)$. That this w then satisfies the *COMP* axiom then follows by essentially the same argument as in Jeřábek [18] Lemma 4.2.

(3) Follows from Lemma 4. □

To establish our conservation result we next show certain definable functions of TComp^τ are closed under the operations needed to carry out a witnessing argument.

Definition 13 *We say a function f is* τ-comprehension-defined *if there is an open$_\tau$-formula, $A_f(i, w, \mathbf{x})$ and terms* $\mathrm{OUT}_f(w, \mathbf{x})$*, and t_f such that*

$$f(\mathbf{x}) = y \Leftrightarrow$$
$$(\exists w \leq 2^{|t_f(\mathbf{x})|})(\forall i \leq |t_f(\mathbf{x})|)\big(\mathrm{BIT}(i, w) = 1 \Leftrightarrow A_f(i, w, \mathbf{x}) \wedge \mathrm{OUT}_f(w, \mathbf{x}) = y\big)$$

Ignoring the complexity associated with the definition of *open*$_\tau$, the notion of τ-comprehension-defined is a marginally simpler variant of Jeřábek [18]'s notion of bit-recursively defined. It is possible in our setting because we have $\dot{-}$ in the language, and so the language supports projections of bits using terms.

Lemma 6 *TComp*$^\tau$ *can* $\hat{\Sigma}^{\mathsf{b}}_1$*-define the τ-comprehension defined functions.*

Proof. Let $f(\vec{x})$ be τ-comprehension defined via $A_f(i, w, \mathbf{x}) \in$ *open*$_\tau$ and terms $\mathrm{OUT}_f(w, \mathbf{x})$, t_f. Let $B_f(i, w, \mathbf{x})$ be the formula

$$\big(\mathrm{BIT}(i, w) = 1 \Leftrightarrow A_f(i, w, \mathbf{x})\big).$$

By Lemma 5 (3) and using *open*$_\tau$*-COMP*, *TComp*$^\tau$ proves:

$$(\exists! w \leq 2^{|t_f(\mathbf{x})|})(\forall i \leq |t_f(\mathbf{x})|) B_f\ .$$

Let

$$C_f(i, w, \mathbf{x}) := \big(B_f(i, w, \mathbf{x}) \wedge \mathrm{OUT}_f(w, \mathbf{x}) = \mathrm{OUT}_f(w, \mathbf{x})\big).$$

Certainly, *TComp*$^\tau$ proves $B_f(i, w, \mathbf{x}) \Leftrightarrow C_f(i, w, \mathbf{x})$. So *TComp*$^\tau$

$$(\exists! w \leq 2^{|t_f(\mathbf{x})|})(\forall i \leq |t_f(\mathbf{x})|) C_f\ .$$

Using this and ($\exists$: *right*) inference it can therefore prove:

$$(\exists y)(\exists w \leq 2^{|t_f(\mathbf{x})|})(\forall i \leq |t_f(\mathbf{x})|)\big(\mathrm{BIT}(i, w) = 1 \Leftrightarrow A_f(i, w, \mathbf{x}) \wedge \mathrm{OUT}_f(w, \mathbf{x}) = y\big).$$

Uniqueness of y can then be proven from the uniqueness of w which in turn follows by bit-extensionality. □

Lemma 7 *Let $\phi_f(\mathbf{x}, y)$ denote the whole formula used to τ-comprehension define the function f. For any term $s(\mathbf{x})$, there is a $\phi_s(\mathbf{x}, y)$ such that BASIC proves $\phi_s(\mathbf{x}, s(\mathbf{x}))$.*

Proof. Define A_s as $0 = 1$, so $w = 0$ will witness the existential. Then take $\mathrm{OUT}_s(w, \mathbf{x})$ to be $s(\mathbf{x})$ and $t_s = s^+$. The statement trivially follows. □

Lemma 8 *The τ-comprehension-defined functions are closed under composition.*

Proof. We show the single parameter case, and leave the general case to the reader. Suppose $f(x)$ and $g(y)$ are τ-comprehension-defined where f is defined by

$$(\exists w \leq 2^{|t_f(x)|})(\forall i \leq |t_f(x)|)\big(\mathrm{BIT}(i,w) = 1 \Leftrightarrow A_f(i,w,x) \wedge \mathrm{OUT}_f(w,x) = y\big)$$

and g is defined by

$$\exists w' \leq 2^{|t_g(y)|})(\forall i \leq |t_g(y)|)\big(\mathrm{BIT}(i,w') = 1 \Leftrightarrow A_g(i,w',y) \wedge \mathrm{OUT}_g(w',y) = z\big)$$

To define $h = g \circ f$, notice if $A_g(i,w',y)$ is w'-restricted-by-intervals to recursion depth τ, so is $B_1(i,w,w',x) := A_g(i,w',\mathrm{OUT}_f(\mathrm{BLK}(0,2^{||t_f^+||},w),x))$, simply because the argument inserted into the third parameter does not involve w'. Notice we do not make use of the parameter n of B_1 from Definition 11. Then define the *open*$_\tau$-formula $A_{g\circ f}$ as the disjunction:

$$\mathrm{i} \in [0,2^{||\mathrm{t}_\mathrm{f}^+||}) \wedge A_f(i,\mathrm{BLK}(0,2^{||t_f^+||},w),x) \vee C_1(t_f,t_g,1,B_1)$$

Here A_f plays the role of B_0 in Definition 11 case (3). Since $\ell = 1$, only the $\lfloor \frac{i \dot{-} 2^{||t_f^+||}}{2^{||t_g^+||}} \rfloor = 0$ disjunct of C_1 ever applies. Finally, define $\mathrm{OUT}_h(w,x)$ as

$$\mathrm{OUT}_g(BLK(2^{||t_f^+||},|t_g^+| \dot{-} 1,w),\mathrm{OUT}_f(\mathrm{BLK}(0,|t_f^+|,w))$$

and $t_h(|x,y|)$ as $2^{|t_f^+|+|t_g^+|}$. □

We next argue *open*$_\tau$-*COMP* implies the τ- comprehension-defined functions are closed under the following recursion scheme:

Definition 14 *Suppose $h_0(n,\mathbf{b})$, $h_1(n,\mathbf{b}) \leq 1$. A function f is defined by concatenation recursion on notation (CRN) from g, h_0, and h_1 if*

$$\begin{aligned} f(0,\mathbf{b}) &= g(\mathbf{b}) \\ f(2n,\mathbf{b}) &= 2 \cdot f(n,\mathbf{b}) + h_0(n,\mathbf{b}), \ \textit{provided } n \neq 0 \\ f(2n+1,\mathbf{b}) &= 2 \cdot f(n,\mathbf{b}) + h_1(n,\mathbf{b}) \end{aligned}$$

Lemma 9 *The τ-comprehension-defined functions are closed under CRN.*

Proof. Suppose that f is defined by CRN from $g(\mathbf{b})$ and $h_0(n, \mathbf{b}), h_1(n, \mathbf{b})$, where g, h_0, h_1 are τ-comprehension defined in $TComp^\tau$. Define $u(a, \mathbf{b})$ to be

$$\sum_{n=0}^{|a|} \mathrm{cond}(\mathrm{BIT}(|a| \dot{-} n, a), h_0(n, \mathbf{b}), h_1(n, \mathbf{b})) \cdot 2^n \ ,$$

then $f(a, \mathbf{b}) = g(\mathbf{b}) \cdot 2^{|u(a,\mathbf{b})|} + u(a, \mathbf{b})$. It suffices to show the sum $u(a, v)$ is τ-comprehension-defined, since then $f(a, \mathbf{b})$ will be by composition.

Notice

$$k(n, a, \mathbf{b}) := \mathrm{cond}(\mathrm{BIT}(|a| \dot{-} n, a), h_0(n, \mathbf{b}), h_1(n, \mathbf{b}))$$

is τ-comprehension-defined by composition. Let $A_k(i, w, n, a, \mathbf{b})$, $\mathrm{OUT}_k(w, n, a, \mathbf{b})$, t_k be used in its definition. So $u(a, \mathbf{b})$ is equal to the sum $\sum_{n=0}^{|a|-1} k(n, a, \mathbf{b}) \cdot 2^n$. A witness string w for this sum can be defined from the concatenation of the witnesses w_n for $A_k(i, w_n, n, a, \mathbf{b})$ for each value of $0 \leq n < |a|$, followed by a string y which concatenates the values of $\mathrm{OUT}_k(w_n, n, a, \mathbf{b})$. The formula

$$A_{k'} := \mathrm{i} \in [0, |\mathrm{a}| \cdot 2^{||\mathrm{t_k}||}) \wedge A_k(i \dot{-} \lfloor \frac{i}{2^{||t_k||}} \rfloor, \beta_{2^{||t_k||}}(\lfloor \frac{i}{2^{||t_k||}} \rfloor, w), \lfloor \frac{i}{2^{||t_k||}} \rfloor, a, \mathbf{b})$$

is w-restricted-by-intervals to recursion depth τ by case (2) of Definition 11. So the function k' which returns the concatenation of the w_n's, can be defined using this formula, setting $t_{k'}(a, \mathbf{b}) = 2^{2^{||t_k^+(|a|,a,\mathbf{b})||}|a|}$, and setting $\mathrm{OUT}_{k'} := w$. If v were the output of $k'(a, \mathbf{b})$ then

$$A_t(n, v, a, \mathbf{b}) := \mathrm{OUT}_k(\mathrm{BLK}(n \cdot 2^{||t_k||}, |t_k|, v), n, a, \mathbf{b}) = 1$$

holds if $k(n, a, \mathbf{b})$ is 1. Using *open*-comprehension (i.e., case (1) of Definition 11) we can *open*$_\tau$-comprehension define a function $t(v, a, \mathbf{b})$ which given v computes a string w' such that

$$\forall n \leq |a|(\mathrm{BIT}(n, w') \Leftrightarrow A_t(n, v, a, \mathbf{b})).$$

So by composition $u(a, \mathbf{b}) = t(k'(a, \mathbf{b}), a, \mathbf{b})$ is τ-comprehension defined. □

Another ingredient we need in order to prove our conservation result is closure under the following recursion scheme useful for witnessing induction rules:

Definition 15 *The function f is defined by τ-*bounded primitive recursion *(BPR^τ) from functions g, h, t, and r if*

$$\begin{array}{rcl} F(0,\mathbf{b}) & = & g(\mathbf{b}) \\ F(n+1,\mathbf{b}) & = & \min(h(n,\mathbf{b},F(n,\mathbf{b})),r(n,\mathbf{b})) \\ f(n,\mathbf{b}) & = & F(\ell(k(n,\mathbf{b})),\mathbf{b}) \end{array}$$

for some $r, k \in L_2$ and $\ell \in \tau$.

Lemma 10 *The τ-comprehension-defined functions are closed under BPR^τ.*

Proof. Suppose f is defined by BPR^τ from g, h, F, k, and r as in the above definition. Suppose g, h are τ-comprehension-definable. Let $h'(n,\mathbf{b},z)$ be $\min(h(n,\mathbf{b},z),r(n,\mathbf{b}))$. This is τ-comprehension-definable by Lemma 8. Let g be defined by

$$(\exists w \le 2^{|t_g(\mathbf{b})|})(\forall i \le |t_g(\mathbf{b})|)\big(\mathrm{BIT}(i,w)=1 \Leftrightarrow A_g(i,w,\mathbf{b}) \wedge \mathrm{OUT}_g(w,\mathbf{b})=y\big)$$

and let h' be defined by proving

$$\begin{array}{l}(\exists w \le 2^{|t_{h'}(n,\mathbf{b},z)|})(\forall i \le |t_{h'}(n,\mathbf{b},z)|)\big(\\ \qquad \mathrm{BIT}(i,w)=1 \Leftrightarrow A_{h'}(i,w,n,\mathbf{b},z) \wedge \mathrm{OUT}_{h'}(w,n,\mathbf{b},z)=y\big)\end{array}$$

Since $z \le r(n,\vec{b})$ we can choose a term $t_{h'}$ that bounds w which only depends on n and $\mathbf{b}$. We can also find monotonic terms $t_{\mathrm{OUT}g}(\mathbf{b})$ and $t_{\mathrm{OUT}h'}(n,\mathbf{b})$ which bound the output sizes of g and h'. In the same way as we argued in the closure under CRN proof when discussing the functions k' and t, we can find a formula $A_{g'}(i,w,\mathbf{b})$ which is w-restricted-by-intervals to recursion depth τ, and such that $A_g(i,\mathrm{BLK}(0,|t_g|,w),\mathbf{b})$ and

$$\mathrm{OUT}_g(\mathrm{BLK}(0,|t_g|,w),\mathbf{b}) = \mathrm{BLK}(2^{||t_g||},|t_{\mathrm{OUT}g}|,w)$$

hold whenever $A_{g'}(i,w,\mathbf{b})$ holds. Let $t_{g'}$ be an appropriate bounding term. Similarly, we can find a formula $A_{h''}(i,w,\mathbf{b},z)$ which is w-restricted-by-intervals to recursion depth τ such that $A_{h'}(i,\mathrm{BLK}(0,|t_{h'}|,w),n,\mathbf{b},z)$ and

$$\mathrm{OUT}_{h'}(\mathrm{BLK}(0,|t_{h'}|,w),n,\mathbf{b},z) = \mathrm{BLK}(2^{||t_{h'}||},|t_{\mathrm{OUT}h'}|,w)$$

hold whenever $A_{h''}(i,w,n,\mathbf{b},z)$ holds. We define an $open_\tau$-formula A_f using Definition 11 case 3, where we set $B_0(j,w',\mathbf{b}) := A_g(j,w',\mathbf{x})$ and set the r of Definition 11 to t_g. We then set

$$\begin{array}{l}B_1(j,w',v',n,\mathbf{b}) := \\ \qquad A_{h''}\big(j,v',n,\mathbf{b},cond(n,\mathrm{BLK}(2^{||t_g||},|t_{\mathrm{OUT}g}|,w'),\mathrm{BLK}(2^{||t_{h'}||},|t_{\mathrm{OUT}h'}|,w')))\end{array}$$

We set $t_f := 2^{2^{||t^+_{h''}||}|\ell|}$. Finally, to complete the definition of f set $\mathrm{OUT}_f(w, n, \mathbf{b})$ to be the term

$$\mathrm{BLK}(2^{||g'||} + (\ell - 1)2^{||t^+_{h''}||} + 2^{||t_{h'}||}, |t_{\mathrm{OUT}h'}|, w).$$

□

Given that the comprehension-defined functions contain the L_2-terms, are closed under composition, and are closed under CRN, the next two lemmas are proven as in Lemma 6 in Clote [9] and Lemma 4 in Johannsen and Pollett [21].

Lemma 11 *Let t be a τ-comprehension defined. (1) $TComp^\tau$ proves $(\mu i \leq |a|)(t(x, a) = 0)$ is τ-comprehension-defined. (2) Given any Σ^{b}_0-formula A its graph χ_A is τ-comprehension-defined.*

Lemma 12 $\min(\lfloor \frac{a}{b} \rfloor, |c|)$ *is τ-comprehension-defined.*

Closure under CRN allows one to show closure under certain kinds of sums which will be useful in our witnessing argument to handle R^1_2's quantifier inferences. Suppose $g(n, \mathbf{x}) \leq t(\mathbf{x})$ and s, t are terms. Then a *length-sum* is a sum of the form

$$\sum_{n=0}^{|s|} g(n, \mathbf{x}) \cdot 2^{n \cdot |t^+|} \ .$$

Lemma 13 *The τ-comprehension-defined functions are closed under length-sums.*

Proof. Suppose we want to define the length-sum

$$f(a, x) := \sum_{n=0}^{|a|} h(n, x) 2^{n|s^+(x)|}$$

where $h(n, x) \leq s(x)$ is comprehension defined and $s(x)$ is a term. We use Lemma 9 and use CRN to compute the bits of f from the most significant bit to the least significant bit. The function

$$t(i, a, x) := |a| \dot{-} \lfloor |i| / |s^+(x)| \rfloor$$

(definable using μ) allows us to determine which term in f we are computing the bits from. The function

$$p(i, x) := |s^+(x)| \dot{-} (|i| \dot{-} \lfloor |i| / |s^+(x)| \rfloor |s^+(x)|) \dot{-} 1$$

gives us the position within a term. Define the function f' by CRN in the following way:

$$\begin{aligned} f'(0,a,x) &= \mathrm{BIT}(p(0,x), h(t(0,a,x),x)) \\ f'(2i+1,a,x) &= f'(2i,a,x) = 2f'(i,a,x) + \mathrm{BIT}(p(i,x), h(t(i,a,x),x)). \end{aligned}$$

Then the desired $f(a,x)$ is $f'(2^{|a||s^+(x)|+|h(|a|,x)|\dot{-}2}, a, x)$. The expression in the first component of f' is easily defined using $\cdot$, $\#$, and MSP. $\square$

In closing this section, we remark that if a function f is τ-comprehension defined by one of the closure conditions mentioned in this section, then given a witness w for the formula defining f, and given witnesses for the defining formulas of the functions from which f is defined, then the theory $\mathit{LIOpen}{+}\hat{\Pi}^{\mathsf{b}}_0\text{-}\mathit{IND}^\tau$ suffices to prove that OUT_f definitionally follows from the OUT terms used to define f. The kind of arguments needed to show these facts will be illustrated by the induction case of the witnessing argument in the next section.

6 A $\forall\hat{\Sigma}^{\mathsf{b}}_1$-conservation result

We are now in a position to prove a witnessing theorem that will yield the conservation results between our comprehension theories and S^1_2, R^1_2, and $\hat{C}^0_2$. In order to do this, we extend the definition of the $\mathit{WIT}^{\{|id|\}}_A$ predicate to the handle the case where $A(\mathbf{a})$ is of the form $(\forall x \leq |s|)B(x,\mathbf{a})$ where $B(x,\mathbf{a}) \in E\Sigma^{\{|id|\}}_\infty$. To keep the notation under control, for the remainder of this section we will write WIT_A rather than $\mathit{WIT}^{\{|id|\}}_A$. For this new case, we set $t_A := bd(t^+_B(|s|), s)$ and

$$\mathit{WIT}_A(w,\mathbf{a}) := w \leq t_A \wedge (\forall x \leq |s|)\, \mathit{WIT}_B(\beta_{t_A}(x,w), x, \mathbf{a}))\ .$$

Given a comprehension defined function f via A_f, t_f, and OUT_f, let ψ_f denote the following formula

$$(\forall i \leq |t_f(\mathbf{x})|)(\mathrm{BIT}(i,w) = 1 \Leftrightarrow A_f(i,w,\mathbf{x})).$$

Theorem 6 *Let* $R[1,\tau] := \mathit{LIOpen}{+}\mathit{BB}\hat{\Pi}^{\mathsf{b}}_0{+}\hat{\Sigma}^{\mathsf{b}}_1\text{-}\mathit{IND}^\tau$ *and let* $T[0,\tau] := \mathit{LIOpen}{+}\hat{\Pi}^{\mathsf{b}}_0\text{-}\mathit{IND}^\tau$*. Suppose* $R[1,\tau] \vdash \Gamma \rightarrow \Delta$ *where* Γ *and* Δ *are cedents of* $LA_{\{|id|\}}E\hat{\Pi}^{\mathsf{b}}_0$*-formulas with free variables among* $\mathbf{a}$*. Then there is a* τ*-comprehension-defined function* f *such that:*

$$T[0,\tau] \vdash \psi_f(v,w,\mathbf{a}) \wedge \mathit{WIT}_{\wedge\Gamma}(w,\mathbf{a}) \supset \mathit{WIT}_{\vee\Delta}(\mathrm{OUT}_f(v,w,\mathbf{a}),\mathbf{a}).$$

Proof. Here we use v to denote the variable that would be existentially quantified over if ψ_f were a subformula of a *COMP* axiom. Theorem 6 is proven by induction on the number of sequents in a $R[1,\tau]$ proof of $\Gamma \rightarrow \Delta$. By cut-elimination, we can assume all the sequents in the proof are $LA_{\{|id|\}}E\hat{\Pi}^{\mathsf{b}}_0$. We formulate *open-LIND* as a $\hat{\Pi}^{\mathsf{b}}_0$-axiom. As the corresponding witness formula can be witnessed by setting $w = 0$, we can easily handle this case. Most of the other cases are similar to previous witnessing arguments so we only show the ($\forall$: right) case, $\hat{\Sigma}^{\mathsf{b}}_1$-$IND^\tau$ case and the $BB\hat{\Pi}^{\mathsf{b}}_0$ case.

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

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

By the induction hypothesis there is a τ-comprehension defined function g such that

$$T[0,\tau] \vdash \psi_g(v, w, \mathbf{a}) \wedge \mathit{WIT}_{b \leq t \wedge (\wedge\Gamma)}(w, \mathbf{a}, b) \supset \\ \mathit{WIT}_{A \vee (\vee\Delta)}(\mathrm{OUT}_g(v, w, \mathbf{a}, b), \mathbf{a}, b) \ .$$

By cut-elimination, $(\forall x \leq t)A(x)$ is a $LA_{\{|id|\}}E\hat{\Pi}^{\mathsf{b}}_0$-formula, so t must be of the form $t = |s|$. There are two case: where A is $\hat{\Pi}^{\mathsf{b}}_0$ and where A is $A_{\{|id|\}}E\hat{\Pi}^{\mathsf{b}}_0$. In the first case, let y be $(\mu i \leq |s|)(\neg A(i))$ and define f to be $g(\langle 0, w\rangle, \mathbf{a}, y)$. The 0 in the ordered pair is since $\mathit{WIT}_{b \leq t}(w, b) := b \leq t \wedge w = 0$. This is τ-comprehension defined by Lemma 11 and it is not hard to show that

$$T[0,\tau] \vdash \psi_f(v', w, \mathbf{a}) \wedge \mathit{WIT}_{\wedge\Gamma}(w, \mathbf{a}) \supset \mathit{WIT}_{\forall x \leq |s| \ A \vee (\vee\Delta)}(\mathrm{OUT}_f(v', w, \mathbf{a}), \mathbf{a}) \ .$$

In the second case, since WIT_A is a $\hat{\Pi}^{\mathsf{b}}_0$-formula, its characteristic function χ_{WIT_A} is comprehension defined. Let k be the function

$$k(w, \mathbf{a}) = (\mu j < |s|)[\neg \mathit{WIT}_A((g(\langle 0, w\rangle, \mathbf{a}, j))_1, \mathbf{a}, j)] \ .$$

Let $t' := (t_A(t))^+$ where $t_{A(x)}$ is from Lemma 2. Now define $f(w, \mathbf{a})$ from k using cond as follows:

$$f(w, \mathbf{a}) = \begin{cases} \langle \sum_{j=0}^{|s|} (g(\langle 0, w\rangle, \mathbf{a}, j))_1 \cdot 2^{j \cdot |t'|}, 0\rangle & \text{if } k(w, \mathbf{a}) = |s| + 1 \\ \langle 0, (g(\langle 0, w\rangle, \mathbf{a}, k(w, \mathbf{a})))_2\rangle & \text{otherwise} \end{cases} \ ,$$

then

$$T[0,\tau] \vdash \psi_f(v', w, \mathbf{a}) \wedge \mathit{WIT}_{\Gamma}(w, \mathbf{a}) \supset \mathit{WIT}_{\forall x \leq |s| \ A \vee (\vee\Delta)}(\mathrm{OUT}_f(v', w, \mathbf{a}), \mathbf{a}) \ .$$

($\hat{\Sigma}^{\mathsf{b}}_1$-$IND^{\tau}$ case) Suppose we have the inference

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

where A is an $\hat{\Sigma}^{\mathsf{b}}_1$-formula and s is a term. We assume $\mathbf{a}$ contains all free variables except b in the upper and lower sequent. By the induction hypothesis there is a comprehension defined function g such that

$$\begin{aligned} T[0,\tau] \vdash \psi_g(v, w, \mathbf{a}) \wedge \mathit{WIT}_{A(b)\wedge(\wedge\Gamma)}(w, b, \mathbf{a}) \supset \\ \mathit{WIT}_{A(Sb)\vee(\vee\Delta)}(\mathrm{OUT}_g(v, w, b, \mathbf{a}), b, \mathbf{a}). \end{aligned}$$

Informally, the idea to witness the lower sequent is the following: run g on w a witness for $A(0), \Gamma$. Either this witnesses $A(S0)$ or it witnesses Δ. In the latter case, we are done. In the former case, we run g on the witness just produced for $A(S0)$ together with $(w)_2$ which is supposed to be a witness for Γ. We keep repeating this process until we get a witness for Δ or we finally get a witness for $A(\ell(s))$. More formally, using Lemma 10, we τ-comprehension-define a function f by BPR^{τ} in the following way. First, we let

$$k(v, w, \mathbf{a}) = \mathit{cond}(\mathit{WIT}_{\vee\Delta}((v)_2, \mathbf{a}), w, v).$$

This is τ-comprehension-definable by Lemma 8, Lemma 7, and Lemma 11. We would like to define f by the following recursion

$$\begin{aligned} F(0, w, \mathbf{a}) &= \langle (w)_1, 0\rangle \\ F(Sb, w, \mathbf{a}) &= \min(k(F(b, w, \mathbf{a}), g((F(b, w, \mathbf{a}))_1, (w)_2, \mathbf{a})), t_{A(Sb)\vee(\vee\Delta)}(b, \mathbf{a})) \\ f(u, w, \mathbf{a}) &= F(\min(u, \ell(s)), w, \mathbf{a}). \end{aligned}$$

which is not exactly that of Lemma 10. To solve this problem, let $F'(b, w, \mathbf{a}, H)$ be an abbreviation for

$$\min(k(\beta_{|m|}(b, H(b, w, \mathbf{a})), g((\beta_{|m|}(b, H(b, w, \mathbf{a})))_1, (w)_2, \mathbf{a})), t_{A(Sb)\vee(\vee\Delta)}(b, \mathbf{a})).$$

in the following definition

$$\begin{aligned} H(0, w, \mathbf{a}) &= \langle (w)_1, 0\rangle \\ H(Sb, w, \mathbf{a}) &= F'(b, w, \mathbf{a}, H) \cdot 2^{(b+1)\cdot|m|} + H(b, w, \mathbf{a}) \\ h(w, \mathbf{a}) &= H(\ell(s(\mathbf{a})), w, \mathbf{a}) \end{aligned}$$

where min's have been suppressed for readability and where $m = t^{+}_{A(Sb)(\ell(s),\mathbf{a})\vee\bigvee\Delta}$, a term bounding the witness size for $A(Sb) \vee (\vee\ \Delta)$. Then $f(u, w, \mathbf{a}) =$

$\beta_{|m|}(min(u, \ell(s)), h(w, \mathbf{a}))$. So both f and h will be τ-comprehension defined by Lemma 10. We would like to show

$$T[0, \tau] \vdash \psi_f(v, w, \mathbf{a}) \wedge \mathit{WIT}_{A(0) \wedge \Gamma}(w, \mathbf{a}) \supset \mathit{WIT}_{A(\ell(s)) \vee \Delta}(\mathrm{OUT}_f(v, \ell(s), w, \mathbf{a}), \mathbf{a}).$$

To see this notice as $f(u, w, \mathbf{a}) = \beta_{|m|}(min(u, \ell(s)), h(w, \mathbf{a}))$ we have both

$$\begin{aligned} T[0, \tau] \vdash \psi_h(v, w, \mathbf{a}) \wedge \mathit{WIT}_{A(0) \wedge (\wedge\Gamma)}(w, \mathbf{a}) \supset \\ \mathit{WIT}_{A(0) \vee (\vee\Delta)}(\beta_{|m|}(0, \mathrm{OUT}_h(v, w, \mathbf{a})), b, \mathbf{a}) \end{aligned}$$

since $f(0, w, \mathbf{a})$ is a witness for $A(0)$, and

$$\begin{aligned} T[0, \tau] \vdash \psi_h(v, w, \mathbf{a}) \wedge \mathit{WIT}_{A(0) \wedge \Gamma}(w, \mathbf{a}) \wedge Sb \leq \ell(s) \wedge \\ \mathit{WIT}_{A(b) \vee (\vee\Delta)}(\beta_{|m|}(b, \mathrm{OUT}_h(v, w, \mathbf{a})), b, \mathbf{a}) \supset \\ \mathit{WIT}_{A(Sb) \vee (\vee\Delta)}(\beta_{|m|}(Sb, \mathrm{OUT}_h(v, w, \mathbf{a})), Sb, \mathbf{a}). \end{aligned}$$

By $\hat{\Pi}^{\mathsf{b}}_0$-IND^τ on $\mathit{WIT}_{A(b) \vee (\vee\Delta)}(\beta_{|m|}(b, \mathrm{OUT}_h(v, w, \mathbf{a})), b, \mathbf{a})$, this implies

$$\begin{aligned} T[0, \tau] \vdash \psi_h(v, w, \mathbf{a}) \wedge \mathit{WIT}_{A(0) \wedge (\wedge\Gamma)}(w, \mathbf{a}) \supset \\ \mathit{WIT}_{A(\ell(s)) \vee (\vee\Delta)}(\beta_{|m|}(\ell(s), \mathrm{OUT}_h(v, w, \mathbf{a})), \ell(s), \mathbf{a}). \end{aligned}$$

Hence, as

$$\beta_{|m|}(\ell(s), \mathrm{OUT}_h(v, w, \mathbf{a})) = \mathrm{OUT}_f(v, \ell(s), w, \mathbf{a})$$

and $\psi_f = \psi_h$ we have

$$T[0, \tau] \vdash \psi_f(v, w, \mathbf{a}) \wedge \mathit{WIT}_{A(0) \wedge (\wedge\Gamma)}(w, \mathbf{a}) \supset \mathit{WIT}_{A(\ell(s)) \vee (\vee\Delta)}(\mathrm{OUT}_f(v, \ell(s), w, \mathbf{a}), \mathbf{a}).$$

($BB\hat{\Pi}^{\mathsf{b}}_0$:case) Suppose we have the inference:

$$\frac{\Gamma \rightarrow (\forall x \leq |s|)(\exists y \leq t) A(x, y), \Delta}{\Gamma \rightarrow (\exists v \leq bd(t^+(|s|), s))(\forall x \leq |s|)(\beta_{t^+(|s|)}(x, v) \leq t \wedge A(x, \beta_{t^+(|s|)}(x, v))), \Delta}$$

where s, t are terms and $A(x, y) \in \hat{\Pi}^{\mathsf{b}}_0$. By the induction hypothesis there is a τ-comprehension defined function g such that

$$T[0, \tau] \vdash \psi_g(v, w, \mathbf{a}) \wedge \mathit{WIT}_{\wedge\Gamma}(w, \mathbf{a}, b) \supset \mathit{WIT}_{\forall x \leq |s|\, \exists y \leq t\, A \vee (\vee\Delta)}(\mathrm{OUT}_g(v, w, \mathbf{a}), \mathbf{a})\ .$$

For this case, it suffices to notice that the predicates

$$\mathit{WIT}_{\forall x \leq |s|\, \exists y \leq t\, A}$$

and

$$\mathit{WIT}_{\exists v \leq \mathrm{bd}(t^+(|s|), s)\, \forall x \leq |s|\, (\beta_{t^+(s(|x|))}(x, v) \leq t \wedge A)}$$

are the same. Hence, if we let $f = g$ then

$$T[0,\tau] \vdash \psi_f(v,w,\mathbf{a}) \wedge \mathit{WIT}_{\wedge\Gamma}(w,\mathbf{a},b) \supset \mathit{WIT}_{\exists w\leq bd(t^+,s)\,\forall x\leq|s|\,A\vee(\vee\Delta)}(\mathrm{OUT}_f(v,w,\mathbf{a}),\mathbf{a}).$$

This completes the cases and the proof. □

Let cl denote the set of closed terms.

Corollary 7 *(1) $R[1,\tau]$ is $\forall\hat{\Sigma}^{\mathsf{b}}_1$-conservative over $TComp^{\tau}$. (2) S^1_2 is $\forall\hat{\Sigma}^{\mathsf{b}}_1$-conservative over $BASIC$+$E_{\{|id|\}}A_{\{|id|\}}$-IND. (3) R^1_2 is $\forall\hat{\Sigma}^{\mathsf{b}}_1$-conservative over $TComp^{\{||id||\}}$. (4) $\hat{C}^0_2$ is $\forall\hat{\Sigma}^{\mathsf{b}}_1$-conservative over $TComp^{\{\mathrm{cl}\}}$.*

Proof. For (1) we first note that $R[1,\tau]$ contains $TComp^{\tau}$ by Lemma 5 (1). Suppose $R[1,\tau]$ proves $\forall\mathbf{x}A(\mathbf{x})$. Then by Theorem 6, $T[0,\tau]$ proves

$$\psi_f(v,w,\mathbf{a}) \wedge \mathit{WIT}_{\emptyset}(w,\mathbf{a}) \rightarrow \mathit{WIT}_A(\mathit{OUT}_f(v,w,\mathbf{a}),\mathbf{a})$$

for some τ-comprehension defined function f. Setting $w = 0$ witnesses the empty cedent. Further using an ($\exists$: *right*) and the fact $(\exists w)\,\mathit{WIT}_A \supset A$ gives us:

$$\psi_f(v,0,\mathbf{a}) \rightarrow A(\mathbf{a}).$$

Now v only appears in the formula $\psi_f(v,0,\mathbf{a})$ in this sequent so we can existentially quantify over it and cut this against the corresponding $open_{\tau}$-*COMP* axiom to give the result.

(2), (3), (4) follow from (1) using Lemma 5 and setting τ to be respectively: $\{|id|\}$, $\{||id||\}$, and cl, noting for any formula A that *BASIC* proves $\mathit{IND}^{\mathrm{cl}}_A$. □

The proof of Corollary 7 (1) gives the following result.

Corollary 8 *If $TComp^{\tau}$ proves a $L\hat{\Sigma}^{\mathsf{b}}_1$-formula A, then there is $open_{\tau}$-formula B, such that $T[0,\tau]$ proves $COMP_B \supset A$.*

We note $TComp^{\{||id||\}}$ can τ-comprehension define the graph of an Σ^{b}_0 formula. As the τ-comprehension defined functions are closed under sharply bounded μ-operator, and $TComp^{\{||id||\}}$ can proves basic facts about this, $TComp^{\{||id||\}}$ proves the Σ^{b}_0-*LIND* axioms, so contains S^0_2. On the other hand, S^0_2 contains *LIOpen* and proves the $\hat{\Pi}^{\mathsf{b}}_0$-*LLIND* axioms, so we have have established:

Corollary 9 *R^1_2 is $\forall\hat{\Sigma}^{\mathsf{b}}_1$-conservative over $TComp^{\{||id||\}} = S^0_2$+$open_{\{||id||\}}$-COMP.*

7 Acknowledgements

The author would like to thank Leszek Kołodziejczyk for his feedback on an earlier draft of this paper.

References

[1] B. Allen. Arithmetizing Uniform NC. *Annals of Pure Applied Logic.* Vol.53 Iss. 1. 1991. pp. 1–50.

[2] A. Beckmann and S.R. Buss. Polynomial Local Search in the Polynomial Hierarchy and Witnessing in Fragments of Bounded Arithmetic Preliminary Manuscript. 2008.

[3] A. Beckmann and S.R. Buss. Characterising Definable Search Problems in Bounded Arithmetic via Proof Notations Preliminary Manuscript. 2009.

[4] S. Boughattas and L. A. Kołodziejczyk. The strength of sharply bounded induction requires MSP. To appear *Annals of Pure and Applied Logic.* 2009.

[5] S. Boughattas and J.P. Ressayre Bootstrapping I. To appear *Annals of Pure and Applied Logic.* 2009.

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

[7] S.R. Buss and J. Krajíček. An application of Boolean complexity to separation problems in bounded arithmetic. *Proceedings of the London Mathematical Society.* Vol. 69. 1994. pp. 1–21.

[8] S. Cook and P. Nguyen. *Logical Foundations of Proof Complexity.* To appear in Perspectives in Logic, Cambridge University Press.

[9] P. Clote. Polynomial size Frege proofs of certain combinatorial principles In P. Clote and J. Krajíček, eds., *Arithmetic, Proof Theory and Computational Complexity.* Oxford Science Publications. 1993.

[10] P. Clote and G. Takeuti. First-order bounded arithmetic and small boolean circuit complexity classes. In P. Clote and J. Remmel, eds., *Feasible Mathematics II.* Birkhauser. Boston. 1995. pp. 154–218.

[11] S. Cook and A. Kolokova. A second-order system for polytime reasoning based on Grädel's theorem *Annals of Pure and Applied Logic*. Vol. 124. Dec. 2003. pp. 193–231.

[12] P. Hájek and P. Pudlák. *Metamathematics of First-Order Arithmetics.* Springer-Verlag, 1993.

[13] J. Hanika. Search Problems and Bounded Arithmetic. Ph.D. Thesis. Charles University. 2004.

[14] L. A. Kołodziejczyk, Phuong Nguyen and Neil Thapen. The provably total NP search problems of weak second order arithmetic. Preliminary manuscript. 2009.

[15] J. Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory, volume 60 of Encyclopedia of Mathematics and its Applications.* Cambridge University Press. Cambridge. 1995.

[16] J. Krajíček, P. Pudlák, and G. Takeuti. Bounded arithmetic and polynomial hierarchy. *Annals of Pure and Applied Logic*. Vol. 52. 1991. pp.143–154.

[17] J. Krajíček, A. Skelley, and N. Thapen. NP search problems in low fragments of bounded arithmetic. *Journal of Symbolic Logic*. Vol. 72. Iss. 2. 2007. pp. 649–672.

[18] E. Jeřábek. The strength of sharply bounded induction. *Mathematical Logic Quarterly*. Vol. 52. 2006. No. 6. pp. 613–624.

[19] J. Johannsen. On Sharply Bounded Length Induction. In *Proc. of Computer Science Logic '95.* Paderborn 1995. Springer LNCS 1092. 1996. pp. 362–367.

[20] J. Johannsen and C. Pollett. On Proofs about Threshold Circuits and Counting Hierarchies. In *Proceedings of Thirteenth IEEE Symposium on Logic in Computer Science*. pp.444–452.

[21] J. Johannsen and C. Pollett. On the Δ_1^b-bit-comprehension rule. In Sam Buss, Petr Hájek, and Pavel Pudlák, eds., *Logic Colloquium '98.* ASL Lecture Notes in Logic. 2000. pp. 262–279.

[22] S.-G. Mantzivis. Circuits in Bounded Arithmetic, Part I. *Annals of Mathematics and Artificial Intelligence*. Vol. 6. 1991. pp. 127–156.

[23] R. Parikh. Existence and feasibility in arithmetic. *Journal of Symbolic Logic*. Vol. 36. 1971. pp. 494–508.

[24] C. Pollett. Structure and definability in general bounded arithmetic theories. *Annals of Pure and Applied Logic*. Vol. 100. October 1999. pp. 189–245.

[25] C. Pollett. Multifunction algebras and the provability of $\mathsf{PH}\downarrow$. *Annals of Pure and Applied Logic*. Vol. 104. July 2000. pp. 279–303.

[26] C. Pollett. On the Bounded Version of Hilbert's Tenth Problem. *Archive for Mathematical Logic*. Vol. 42. No. 5. 2003. pp. 469–488.

[27] P. Pudlák. Fragments of Bounded Arithmetic and the lengths of proofs. *Journal of Symbolic Logic*. Vol. 73. Iss. 4. 2008. pp. 1389–1406.

[28] J.C. Shepherdson. Non-standard models for fragments of number theory. *Proceedings of the 1963 International Symposium at Berkeley on the Theory of Models*. North-Holland. Amsterdam. 1965. pp. 342–358.

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