On the Finite Axiomatizability of $\forall\hat{\Sigma}^{\mathsf{b}}_1(\hat{R}^1_2)$

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

September 3, 2016– Draft

Abstract

The question of whether the bounded arithmetic theories S^1_2 and R^1_2 are equal is closely connected to the complexity question of whether P is equal to NC. In this paper, we examine the still open question of whether the prenex version of R^1_2, $\hat{R}^1_2$, is equal to S^1_2. We give new dependent choice-based axiomatizations of the $\forall\hat{\Sigma}^{\mathsf{b}}_1$-consequences of S^1_2 and $\hat{R}^1_2$. Our dependent choice axiomatizations give new normal forms for the $\hat{\Delta}^b_1$-consequences of S^1_2 and $\hat{R}^1_2$. We use these axiomatizations to give an alternative proof of the finite axiomatizability of $\forall\hat{\Sigma}^{\mathsf{b}}_1(S^1_2)$ and to show new results such as $\forall\hat{\Sigma}^{\mathsf{b}}_1(R'^1_3)$ is finitely axiomatized and that there is a finitely axiomatized theory, TUC, containing $\hat{S}^0_2$ and contained in $\hat{R}^1_2$. On the other hand, we show that our theory for $\forall\hat{\Sigma}^{\mathsf{b}}_1(\hat{R}^1_2)$ splits into a natural infinite hierarchy of theories. We give a diagonalization result that stems from our attempts to separate the hierarchy for $\forall\hat{\Sigma}^{\mathsf{b}}_1(\hat{R}^1_2)$.

Mathematics Subject Classification: 03F30, 68Q15
Keywords: bounded arithmetic, finite axiomatizations

1 Introduction

The theories S^1_2 and R^1_2 are two of the more well-studied bounded arithmetic theories. The $\hat{\Sigma}^{\mathsf{b}}_1$-definable functions of S^1_2 are known to be P, the polynomial time computable functions, and those of R^1_2 to be the functions in NC, functions corresponding to uniform poly-size, poly-log depth circuit families. The question of whether or not these two theories are equal seems to be hard and connected to the important question of whether the feasibly computable functions as captured by P correspond to the feasibly parallelizable functions as captured by NC. Some success has been had in separating weaker bounded arithmetic theories from S^1_2. The present paper follows in this tradition and attempts to characterize the $\forall\hat{\Sigma}^{\mathsf{b}}_1$-consequences of the prenex version of R^1_2, $\hat{R}^1_2$, in a way that would be useful in separating it from S^1_2.

The theories S^i_2 and R^i_2 are formulated over a base theory $BASIC$, consisting of a finite set of open axioms for the symbols of arithmetic, and add to this theory either length or length-length induction for Σ^{b}_i-formulas, those formulas which correspond to the class NP for $i = 1$ or $\mathsf{NP}^{\Sigma^{\mathsf{p}}_{i-1}}$ for $i > 1$. Pollett [24] shows that the theory with four lengths induction for prenex Σ^{b}_1 formulas ($\hat{\Sigma}^{\mathsf{b}}_1$ formulas) is strictly weaker than S^1_2. This was later improved by Boughattas and Ressayre [3] via a model theoretical approach to three lengths induction; however, the language of their result no longer has MSP. For this paper, we will consider the finite axiomatizability of the $\forall\hat{\Sigma}^{\mathsf{b}}_1$ consequences of the prenex version of R^1_2, $\hat{R}^1_2$, versus that of S^1_2. Garlík [11] has shown via an ultraproduct construction that $\hat{R}^1_2$ is weaker than R^1_2 under the assumption that one-way permutations exist and are computable in R^1_2, but no unconditional separation of these theories is known.

One common approach to separating complexity classes and logical theories is via some kind of diagonalization argument. Even if diagonalization by itself does not directly succeed, it can sometimes be combined with a strong "if-pigs-could-fly" hypothesis to provide a separation or lower bound. An example of this is the research on lower bounds for satisfiability started by Fortnow [10]. A first step in being able to perform a diagonalization argument is often to come up with a universal predicate for the functions, theorems, etc. of the class one is trying to separate from. This is also often needed when one is trying to show a logical theory is finitely axiomatized.

Finitely axiomatizability results for theories S^i_2 and R^i_2 for $i \geq 2$ were shown in Krajíček and Pudlák [14] and Pollett [22]. Cook and Kolokolova [9] show that the $\forall\hat{\Sigma}^{\mathsf{b}}_1$ consequences of S^1_2 are finitely axiomatized. Their result was shown via a second-order theory V_1-Horn whose theorems are isomorphic to these consequences. That paper was part of a larger program begun by Zambella, Cook, Nguyen, and others to give nice second-order bounded arithmetic theories for computational complexity classes. We give here a new proof of this result directly in S^1_2. It is unknown if the $\forall\hat{\Sigma}^{\mathsf{b}}_1$ consequences of R^1_2 or $\hat{R}^1_2$ are finitely axiomatized, and showing that they are not could be an approach to separating these theories from S^1_2.

This paper presents finite axiomatizations of S^1_2 and R'^1_3 that start with the base theory *EBASIC*, a variant of Buss' base theory *BASIC*, (in the ${R'}^1_3$ case, with the extra growth function $\#_3$ defined later) and an axiom we call BITMIN for bit minimization. We show that *EBASIC* together with BITMIN is close to capturing all of $\hat{S}^0_2$ in the sense that $\hat{S}^0_2$ can prove this theory, and if we allow a certain kind of unsafe term substitution into a BITMIN axiom, one can prove any $\hat{\Pi}^{\mathsf{b}}_0$-*LIND* axiom. To $B := \mathit{EBASIC}+$BITMIN we add a single axiom, UC, a universal term bit comprehension axiom. We show $\mathit{TUC} := B + UC$ contains $\hat{S}^0_2$ and is contained in S^1_2 and R^1_2. We show *TUC* together with a length bounded dependent choice principle exactly captures $\forall\hat{\Sigma}^{\mathsf{b}}_1(S^1_2)$. The main work in this result is showing that this theory can intentionally reason about the usual functional closure properties needed to carry out a Buss witnessing argument for conservativity. If rather than consider our length-bounded dependent choice principle, we work in a language with the growth function $\#_3$ and add a (length length) bounded dependent choice principle, then we get a theory for the $\forall\hat{\Sigma}^{\mathsf{b}}_1$ consequences of ${R'}^1_3 := \hat{R}^1_3 + UC$. Given our definitions $\hat{R}^1_3 \subseteq {R'}^1_3 \subseteq R^1_3$. To get the ${R'}^1_3$ result mentioned above, we have to be a little more careful in our handling of the universal predicates that we consider. This is because with just length-length-bounded $\hat{\Sigma}^{\mathsf{b}}_1$ induction and not $\hat{\Sigma}^{\mathsf{b}}_1$ bounded collection, it is hard to express the sharply bounded μ-operator in a way that will both work in our witnessing arguments and in our universal predicates.

When we remove $\#_3$ from the language, $\forall\hat{\Sigma}^{\mathsf{b}}_1(S^1_2)$ is finitely axiomatizable, but $\forall\hat{\Sigma}^{\mathsf{b}}_1(\hat{R}^1_2)$ is axiomatizable as $\hat{S}^0_2$ together with a union over k of instances of (length-length)^k bounded dependent choice principles. Although at this point we cannot show this hierarchy over k is infinite, we are able to get a normal form for the $\hat{\Delta}^b_1$ consequences of S^1_2 and $\hat{R}^1_2$ based on these principles. We argue these normal forms lend themselves to diagonalization arguments which we feel might be a component to an argument which does separate these theories. We prove a very weak diagonalization result which can be viewed as an analog of a combination time-space hierarchy based on the number of # symbols appearing in terms in our normal forms. Unlike usual hierarchy results of languages which are framed in terms Turing machines, our hierarchy is somewhat interesting as it has a more algebraic flavor.

This paper is organized as follows: In the next section we present the bounded arithmetic theories S^i_2, R^i_2 and their prenex variants. We then present the BITMIN axiom, our bounded dependent choice principles, and our $\hat{S}^0_2$ result. We next do a witnessing argument to show $\forall\hat{\Sigma}^{\mathsf{b}}_1$ conservativity results between our bounded dependent choice theories and S^1_2 and $\hat{R}^1_2$. This argument also implies our $\hat{\Delta}^b_1$ normal form results. We then prove our finite axiomatization results. Finally, we conclude the paper with our diagonalization result.

2 Preliminaries

The reader interested in an introductory treatment of bounded arithmetic can consult any of the books: Buss [4], Hájek and Pudlák [12], Krajíček [13], or Cook and Nguyen [6]. In this section, we fix the notations and definitions needed for this paper. To start the language L_2 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 $\leq$. MSP is perhaps the least familiar of these functions, it roughly shifts and removes the y least significant bits from x. The base theory, *EBASIC*, is as defined in Pollett [23] and consists of the axioms for *BASIC* from Buss [4], together with a total of seven additional axioms regarding $\dot{-}$ (the axioms for these as in Allen [1]), MSP, and block of bits projections. These seven additional axioms are used to show finite pairings and block of bits projections work as expected in this base theory. Let L_3 be L_2 expanded with an additional function symbol $\#_3$ intended to mean $x\#_3 y := 2^{|x|\#|y|}$. We define $EBASIC_3$ to be *EBASIC* together with additional axioms $|x\#_3 y| = S(|x|\#|y|)$ and $z < x\#_3 y \Leftrightarrow |z| < |x\#_3 y|$. It should be pointed out that the theories S^i_2 and R^i_2 as defined in the papers where they were originally introduced can prove the *EBASIC* axioms that were not in these original definitions [23], the added *EBASIC* axioms are only important for some of the weaker theories we consider.

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 $SIB0$ (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 [23] 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 $\hat{\Sigma}^{\mathsf{b}}_i \setminus \hat{\Pi}^{\mathsf{b}}_{i-1}$ (resp. $\hat{\Pi}^{\mathsf{b}}_i \setminus \hat{\Sigma}^{\mathsf{b}}_{i-1}$) and consists of 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 [23] 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. 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" quantifiers. 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 [4] which extends the usual sequence calculus *LK* to directly handle bounded quantifiers. We consider theories where we extend the different *EBASIC* 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:*

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

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 $IND^{\{\mathrm{id}\}}$, $IND^{\{|\mathrm{id}|\}}$, and $IND^{\{||\mathrm{id}||\}}$. *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 [4],[23], IND^{ℓ}_{A}:

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

where A is from Ψ and ℓ is from τ. When referring to a particular induction axiom, we will write $LIND_A$ for IND^{ℓ}_{A} when $\ell = |id|$ and $LLIND_A$ when $\ell = ||id||$.

Definition 2 ($i \geq 0$) *The theories T^i_2, S^i_2, R^i_2, $T^{i,\tau}_2$ are $BASIC$+Σ^{b}_i-IND, $BASIC$+Σ^{b}_i-$LIND$, $BASIC$+Σ^{b}_i-$LLIND$, and $BASIC$+Σ^{b}_i-IND^τ respectively.*

We define $S_2 := \cup_i S^i_2$.

Let $\hat{T}^i_2$, $\hat{S}^i_2$, $\hat{R}^i_2$, $\hat{T}^{i,\tau}_2$ denote the theories above but where we only have the defining induction scheme for $\hat{\Sigma}^{\mathsf{b}}_i$-formulas. By Pollett [23], for $i > 0$ for

$\hat{T}^i_2 = T^i_2$ and $\hat{S}^i_2 = S^i_2$; however, R^i_2 and $\hat{R}^i_2$ are not known to be the same theory. It is also known for $i \geq 0$ that

$$S^i_2 \subseteq T^i_2 \subseteq S^{i+1}_2 \text{ and } \hat{R}^i_2 \subseteq R^i_2 \subseteq S^i_2 \subseteq \hat{R}^{i+1}_2.$$

In the remainder of this section we recall the pairing function from Clote and Takeuti [8], and the coding scheme from Pollett [23]. Pairing and coding will be needed to present our collection axioms.

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* MSP(s_1, s_2)*, then t^+ is s_1^+.*

By induction on the complexity of t, *BASIC* + *open-LIND* can show t^+ is monotonic, and $t \leq t^+$. Let $k > 0$ be a fixed natural number. Below are some frequently used L_2-terms:

$$\begin{array}{rcl}
x^0 & := & 1 \\
x^k & := & x^{k-1} \\
2^{|x|^0} & := & 1 \\
2^{|x|^k} & := & 2^{|x|^{k-1}} \# x \\
\mathrm{mod2}(x) & := & x \dot{-} 2 \cdot \lfloor \frac{1}{2} x \rfloor \\
\mathrm{BIT}(i, x) & := & \mathrm{mod2}(\mathrm{MSP}(x, i)) \\
2^{\min(x, |y|)} & := & \mathrm{MSP}(2^{|y|}, |y| \dot{-} x) \\
\mathrm{cond}(x, y, z) & := & (1 \dot{-} x) \cdot y + (1 \dot{-} (1 \dot{-} x)) \cdot z \\
\mathrm{LSP}(x, i) & := & x \dot{-} 2^{\min(i, |x|)} \cdot \mathrm{MSP}(x, i) \\
\mathrm{BLK}(a, b, w) & := & \mathrm{MSP}(\mathrm{LSP}(w, a + b), a) \\
\beta_a(i, w) & := & \mathrm{BLK}(i \cdot a, a, w)
\end{array}$$

For any polynomial p, we can define a term $2^{p(|x|)}$ using the first four definitions above. Intuitively, LSP(x, i), the least significant part of x, returns the last i bits of x, BLK(a, b, w) projects out a bits from w starting with the bth bit, and $\beta_a(i, w)$ projects out the ith block of a many bits from w. Given a sequence of values b_i with $b_i < 2^{|a|}$, we say a number w codes the sequence $\langle b_0, \ldots, b_{\ell-1} \rangle$ with block size $|a|$ if for all i, $\beta_{|a|}(i, w) = b_i$. Notice $a \# s = 2^{|a||s|}$ is a bound on a number w coding a sequence of length $\ell = |s|$ with each item $b_i < 2^{|a|}$. Over *EBASIC* using length induction, one can show that any two numbers coding $|s|$ many values $b_i < 2^{|a|}$ must agree on their lower order $|a||s|$ bits.

We will make use of 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

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

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

$$\frac{\Gamma \rightarrow (\exists y \leq t(x))A(x,y), \Delta}{\Gamma \rightarrow (\exists w \leq 2^{|t^+(|s|)|(|s|+1)})(\forall x \leq |s|)\beta_{|t^+(|s|)|}(x,w) \leq t(x) \wedge A(x, \beta_{|t^+(|s|)|}(x,w)), \Delta}$$

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

Pollett [23] gives an alternative formulation of R^i_2 as *EBASIC*+$\hat{\Sigma}^{\mathsf{b}}_i$-*LLIND*+$BB\hat{\Sigma}^{\mathsf{b}}_i$ which we will make use of in a later section.

3 $\hat{\Sigma}^{\mathsf{b}}_1$ sub-theories of S^1_2 and $\hat{R}^1_2$

We are now in a position to define our sub-theories for the $\forall\hat{\Sigma}^{\mathsf{b}}_1$-consequences of S^1_2 and $\hat{R}^1_2$. In the following, we will tend to use $\hat{S}^0_2$ as our base theory, however, later when we try to get our finite axiomatization results, we will use *EBASIC* together with the BITMIN axiom:

Definition 5 BITMIN *is the axiom*

$$(\exists i \leq |a|)\text{LEASTON}(i, a)$$

where LEASTON(i, a) *is:*

$$\begin{gathered}(\forall j < i)[(i < |a| \supset \text{BIT}(i,a) = 1 \wedge \text{BIT}(j,a) = 0) \wedge \\ (i = 0 \supset a = 1) \wedge (i = |a| \supset (\forall k < |a|)\text{BIT}(k,a) = 0)].\end{gathered}$$

It turns out that *EBASIC*+BITMIN is very closely related to the theory $\hat{S}^0_2$. In order to see this, we need the following lemma.

Lemma 1 *Let A be an open formula. There is a term K_A such that*

$$EBASIC \vdash K_A = 1 \Leftrightarrow A \textit{ and } EBASIC \vdash K_A = 0 \Leftrightarrow \neg A.$$

Proof. This is proven by induction on the logical complexity of the formula A. For the purposes of our argument, we will treat $A \supset B$ as an abbreviation for $\neg A \vee B$ and $A \vee B$ as an abbreviation for $\neg(\neg A \wedge \neg B)$. Given an atomic formula $s \leq t$, we can define the term $K_{s \leq t}$ as $1 \dot{-} ((s+1) \dot{-} t)$. Using the axioms for $+$ and $\dot{-}$, *EBASIC* proves this formula is non-zero if and only if the inequality $s \leq t$ holds. For the non-base case, if A is an open formula its top logical connective will be one of $\wedge$ or $\neg$. By defining $K_{\wedge}(b, c) := b \cdot c$ and $K_{\neg}(b) := 1 \dot{-} b$, and using the induction hypothesis on subformulas, we can naturally get a term K_A which *EBASIC* proves is non-zero if and only if A holds. □

Given terms $s(c, b)$, $t(i, |c|, s(c, b), b)$, let $\mathrm{BITMIN}_{s,t}$ denote the axiom where we "roughly" substitute t for the free variable a in BITMIN and where we use $s(c, b)$ rather than $|a|$ for the number bits we are doing minimization over. That is, $\mathrm{BITMIN}_{s,t}$ is $(\exists i \leq |s(c, b)|)\mathrm{LEASTON}(i, t)$ where $\mathrm{LEASTON}(i, t)$ is

$$(\forall j < i)(i < |s(c, b)| \supset \mathrm{BIT}(i, t(i, |c|, s(c, b), b)) = 1 \wedge \mathrm{BIT}(j, t(j, |c|, s(c, b), b)) = 0) \wedge$$
$$(i = 0 \supset t(0, |c|, s(c, b), b) = 1) \wedge (i = |s(c, b)| \supset (\forall k < |s(c, b)|)\mathrm{BIT}(k, t(k, |c|, s(c, b), b)) = 0).$$

Lemma 2

1. *$\hat{S}^0_2$ proves* BITMIN*, and for any term $s(c, b)$, $t(i, |c|, s(c, b), b)$, it proves* $\mathrm{BITMIN}_{s,t}$*.*

2. *Given any $\hat{\Pi}^{\mathsf{b}}_0$-formula A, there are terms $s_A(c, b)$, $t_A(i, |c|, s(c, b), b)$ such that*
$$\mathit{EBASIC} + \mathrm{BITMIN}_{s_A,t_A} \vdash \mathit{LIND}_A.$$

Proof. For (1), we note BITMIN is just a special case of $\mathrm{BITMIN}_{s,t}$ where $s(c, b) := b$ and $t(i, |c|, s(c, b), b) := b$. So it suffices to show $\hat{S}^0_2$ proves $\mathrm{BITMIN}_{s,t}$ for arbitrary terms $s(c, b)$, $t(i, |c|, s(c, b), b)$. To do this, consider the $\hat{\Pi}^{\mathsf{b}}_0$-formula $B(j, c, b)$:

$$(\forall k < |s(c, b)|)(k < j \supset \mathrm{BIT}(k, t(k, |c|, s(c, b), b)) = 0).$$

EBASIC proves $B(0, b)$. So by $\hat{\Pi}^{\mathsf{b}}_0$-*LIND*, $\exists j < |d|(B(j, c, b) \wedge \neg B(S(j), c, b))$ or

$$\forall j < |d|(\mathrm{BIT}(j, t(j, |c|, s(c, b), b)) = 0).$$

where d is a free variable that we may substitute with $s(c, b)$. If we do this, The i asserted by $\mathrm{BITMIN}_{s,t}$ is $S(j)$ in the former case and $i = |s(c, b)|$ in the latter case. This shows $\hat{S}^0_2$ proves $\mathrm{BITMIN}_{s,t}$.

For (2), we make use of the term K_B given by Lemma 1. Let A be $\hat{\Pi}^{\mathsf{b}}_0$-formula. By adjusting the sharply bounded term, we can show any $\hat{\Pi}^{\mathsf{b}}_0$-formula is equivalent to one where the bounded quantifier uses a strict inequality. So we assume A is of the form $\forall m < |t(j,b)|B(j,m,b)$, where B is open. We want to show EBASIC+BITMIN$_{s_A,t_A}$ proves LIND_A for some L_2 terms s_A, t_A. Here j is the induction variable. The conclusion of LIND_A is equivalent to $\forall m < |t(|c|,b)|B(|c|,m,b)$ for some free variable c. Take $s_A(c,b) := 2 \cdot \max(c, t^+(|c|,b))$, and to shorten things further, write d for $s_A(c,b)$. Since we have the MSP function but not the general division function in the language, it will be convenient to work with $2^{||d||}$ rather than $|d|$. We will define a formula $B'(i,b,d)$ where we imagine i as running over values less than $(2^{||d||})^2$, $2^{||d||}$ blocks of $2^{||d||}$ numbers. We can use the terms $BNum(i,d) := \lfloor \frac{i}{2^{||d||}} \rfloor$ and $Pos(i,d) := i \dot{-} 2^{||d||} \cdot \lfloor \frac{i}{2^{||d||}} \rfloor$ to determine which block and which position in that block i has. We imagine $BNum(i,d)$ as playing the role of j in the original formula B and $Pos(i,d)$ as playing the role of m. Given this, define $B'(i,|c|,d,b)$:

$$\begin{gathered}(Pos(i,d) < |t(BNum(i,d),b)| \wedge B(BNum(i,d),Pos(i,d),b)) \vee \\ Pos(i,d) \geq |t(BNum(i,d),b)| \vee BNum(i,d) \geq |c|\end{gathered}$$

Since we have defined bit minimization to hunt for the least on bit, let $B'' := \neg B'$. Write $2^{\min(i,(2^{||d||})^2)}$ for the more complicated substitution instance of $2^{\min(x,|y|)}$, given by the expression $2^{\min(\min(i,(2^{||d||})^2),|d\#d\#d|)}$. Let $t_A(i,|c|,s_A(c,b),b) = t_A(i,|c|,d,b)$ be $2^{\min(i,(2^{||d||})^2)} \cdot K_{B''}(i,|c|,d,b)$ and consider BITMIN$_{s_A,t_A}$. The $2^{\min(i,(2^{||d||})^2)}$ factor in the previous occurs because in the bit minimization axiom we look at the ith bit of $t_A(i,b)$ to see if it is 0 or 1; whereas, $K_{B''}(i,|c|,d,b)$ by itself only returns 0 or 1 and so will typically have nothing at its ith bit. Unwinding our definitions in EBASIC, we have for $0 \leq i < 2^{||d||}$, LEASTON(i,t_A) implies $\neg A(0,b)$. Similarly, for $2^{||d||} \leq i < (2^{||d||})^2$, LEASTON$(i,t_A)$ implies $\exists j A(j,b) \wedge \neg A(S(j),b)$ for $j = BNum(i,d) - 1$, and for any greater i, LEASTON(i,t_A) implies $\forall j < |d| A(j,b)$, so LEASTON(i,t_A) implies $\forall m < |t(|c|,b)|B(|c|,m,b)$. Hence, BITMIN$_{s_A,t_A}$ over EBASIC implies LIND_A. □

To define the bounded dependent choice axioms which will serve as a basis for the new theories considered in this paper, we define the equation $a = \mu j < |b|(t(j,\mathbf{c}) > 0)$ for some term t to mean the formula:

$$\begin{aligned}(\forall i \leq |b|)[((a < |b| \wedge i < a) \supset t(a,\mathbf{c}) > 0 \wedge t(i,\mathbf{c}) = 0) \\ \wedge (a = |b| \supset (\forall k < |b|)(t(k,\mathbf{c}) = 0))]\end{aligned}$$

It asserts that a is the least value of j less than $|b|$ such that $t(j,\mathbf{c}) > 0$

or $a = |b|$ and for all values of j less than $|b|$, $t(k, \mathbf{c}) = 0$. This sharply bounded μ-operation is one of the functions definable in S^0_2. The theories we are about to give extend S^0_2 with the ability to define certain kinds of arithmetic computation sequences where one of the allowed operations to perform in one step is based on this μ-operation. By pulling the sharply bounded formulas to the front and using pairing, the above formula can be made into a $\hat{\Pi}^{\mathsf{b}}_0$-formula.

Definition 6 *Let τ be a set of 1-ary nondecreasing terms $\ell(x) \leq |x|$, let $k \in \mathbb{N}$. We write τ-BDC for the theory consisting of $\hat{S}^0_2$ together with axioms $BDC[\ell, t_{init}, t_{sel}, t_{rec}, t_\mu, b]$ of the form:*

$$\begin{aligned}(\exists w \leq 2^{\ell(b)\cdot(|b|+1)})(\forall i < \ell(b))[(&\beta_{|b|}(0, w) = \min(t_{init}(\mathbf{a}), b) \wedge \\ &(t_{sel}(\beta_{|b|}(i, w), i, \mathbf{a}) > 0 \supset \beta_{|b|}(i+1, w) = \min(t_{rec}(\beta_{|b|}(i, w), i, \mathbf{a}), b)) \wedge \\ &(t_{sel}(\beta_{|b|}(i, w), i, \mathbf{a}) = 0 \supset \beta_{|b|}(i+1, w) = \mu j < |b|(t_\mu(j, \beta_{|b|}(i, w), \mathbf{a}) > 0))].\end{aligned}$$

where $\ell \in \tau$ and t_{init}, t_{sel}, t_{rec}, t_μ are L_2 terms.

Here *BDC* stands for *bounded dependent choice*, the name coming from the discussion in Clote Takeuti [8] concerning the set theory principle which inspired their weak successive nomination (WSN) rule. In English, a *BDC* axiom roughly asserts the existence of a computation sequence of **length** $\ell(b)$ made up of blocks of length $|b|$, the first block having value $t_{init}(\mathbf{a})$, and subsequent blocks being computed from previous ones as the minimum of a maximum **width** value, b, and either t_{rec} or $\mu j < |b|(t_\mu > 0)$ applied to the previous block. The term t_{sel} is used to select between these two cases. Let id denote the identity function. We will show that the $\forall\hat{\Sigma}^{\mathsf{b}}_1$-consequences of S^1_2 and $\hat{R}^1_2$ correspond to $\{|\mathrm{id}|\}$-*BDC* and $\cup_m\{||\mathrm{id}||^m\}$-*BDC* respectively. Towards that end, we first observe the following relationships between our theories.

Lemma 3

1. $\{||\mathrm{id}||\}$-*BDC* $\subseteq$ $\{||\mathrm{id}||^2\}$-*BDC* $\subseteq \cdots \cup_m\{||\mathrm{id}||^m\}$-*BDC* $\subseteq \{|\mathrm{id}|\}$-*BDC*.
2. $\cup_m\{||\mathrm{id}||^m\}$-*BDC* $\subseteq \hat{R}^1_2$ *and* $\{|\mathrm{id}|\}$-*BDC* $\subseteq S^1_2$.

Proof. For (1), given a term $t_{rec}(y, i, \mathbf{a})$, using the cond function we can make a term $t'_{rec}(y, i, \mathbf{a})$ which is equal to t_{rec} for $i \leq \ell(b)$ and is equal to y otherwise. To ensure only t'_{rec} is used for $i > \ell$, we can use cond to define t'_{sel}, a version of t_{sel}, which is equal to t_{sel} for $i \leq \ell$ and is 1 otherwise. Let $t'_\mu := t_\mu$. So if $\ell = ||id||^m$, given an instance of $\{||\mathrm{id}||^m\}$-*BDC* that uses terms t_{init}, t_{sel}, t_{rec} and t_μ, we can in this way create an equivalent instance of $\{||\mathrm{id}||^{m+1}\}$-*BDC* using t_{init}, t'_{sel}, t'_{rec} and t'_μ.

For (2), from Theorem 22 (i) in Pollett [23] it is known $\hat{R}^1_2$ can prove $\hat{\Sigma}^{\mathsf{b}}_1$ induction up to terms of the form $||t||^m$. Using this, given an instance $A(||b||^m) := BDC[||id||^m, t_{init}, t_{sel}, t_{rec}, t_\mu, b]$ of a $\{||\mathrm{id}||^m\}$-*BDC* axiom, $\hat{R}^1_2$ can prove $A(0)$ as this just asserts there exists a $w \leq 2^{||b||^m \cdot (|b|+1)}$ such that $\beta_{|b|}(0, w) = t_{init}(\mathbf{a})$, and so one could take $w = t_{init}(\mathbf{a})$ to satisfy this. Also, $\hat{R}^1_2$ proves $A(j) \supset A(S(j))$, as a witness for $A(S(j))$ could be had by concatenating onto a witness w for $A(j)$ either the minimum of b and t_{rec} or t_μ depending on whether t_{sel} was 0 or not. Hence, by using $||id||^m$ induction, $\hat{R}^1_2$ can prove $A(||b||^m)$. The S^1_2 result is proven in a similar fashion. □

Let τ be a set of 1-ary nondecreasing terms, $\ell(x) \leq |x|$ and let $r(\mathbf{a})$ be an L_2 term. If we view w as a sequence of $|r^+|$-bit long blocks. To get the last block of bits from this sequence, define

$$\mathrm{LAST}(w, r) = \min(\beta_{|r^+|}(\lceil |w|/|r^+| \rceil - 1, w), r).$$

We say a function $f(\mathbf{a}) = y$ in a bounded arithmetic theory T is τ-*bounded choice defined* if there is a formula $\psi_f(w, \mathbf{a}, r)$ of the form:

$$\begin{aligned}&(\forall i < \ell(r^+))[(\beta_{|r^+|}(0, w) = \min(t_{init}(\mathbf{a}), r) \wedge \\ &\quad (t_{sel}(\beta_{|r^+|}(i, w), i, \mathbf{a}) > 0 \supset \beta_{|r^+|}(i+1, w) = \min(t_{rec}(\beta_{|r^+|}(i, w), i, \mathbf{a}), r)) \wedge \\ &\quad (t_{sel}(\beta_{|r^+|}(i, w), i, \mathbf{a}) = 0 \supset \beta_{|r^+|}(i+1, w) = (\mu j < |r^+|)(t_\mu(j, \beta_{|r^+|}(i, w), \mathbf{a}) > 0))].\end{aligned}$$

where $\ell \in \tau$, $r(\mathbf{a})$ and $t_{init}(\mathbf{a})$, $t_{sel}(v, i, \mathbf{a})$, $t_{rec}(v, i, \mathbf{a})$, $t_\mu(j, v, \mathbf{a})$ are terms, and if there is a term $\mathrm{OUT}_f(v, \mathbf{a})$, computing from the last block v of w the output of f, such that T proves

$$\forall \mathbf{a} \exists ! y \leq 2^{|r^+|} \exists ! w \leq 2^{\ell(r^+) \cdot (|r^+|+1)} \psi_f(w, \mathbf{a}, r) \wedge \mathrm{OUT}_f(\mathrm{LAST}(w, r), \mathbf{a}) = y$$

and

$$\mathbb{N} \models \exists w \leq 2^{\ell(r^+) \cdot (|r^+|+1)} \psi_f(w, \mathbf{a}, r) \wedge \mathrm{OUT}_f(\mathrm{LAST}(w, r), \mathbf{a}) = f(\mathbf{a}).$$

We call r the **width term** of the definition. It puts an upper bound on the values which can appear in the sequence w. The term ℓ governs the length of the sequence, so we call $\ell(r^+)$ the **length term** of the definition.

We will prove our conservativity results using a witnessing argument. To do this, we first develop some closure properties for the class of functions τ-*BDC* can τ-bounded choice define.

Lemma 4

1. *If τ-BDC can τ-bounded choice define a function f using width term r and the term $q > r$ and $q^+ > r^+$ for all inputs, then it can τ-bounded choice define the function f using q as the width term.*

2. *If τ-BDC can τ-bounded choice define a function f using length term ℓ and the term $\ell' \in \tau$, for all inputs $\ell' > \ell$, then it can τ-bounded choice define the function f using ℓ' as the length term.*

Proof. For (1), suppose f is τ-bounded choice defined via terms r, t_{init}, t_{sel}, t_{rec}, and t_μ. Let w be the witness string one gets and let OUT_f be the term used to project out f from w. Let t'_{rec} be the term $t_{rec}(\min(y, r), i, \mathbf{a})$. Let w' be a witness to ψ_f which exists by bounded dependent choice. Using $\hat{\Pi}^{\mathsf{b}}_0$-*LIND*, τ-*BDC* can show for each $i \leq \ell(r^+)$ that $\beta_{|q^+|}(i, w') = \beta_{|r^+|}(i, w)$. We can define t''_{rec} from t'_{rec} and t''_μ from t_μ, using cond so that for for $i < \ell(r^+)$ that their output is before, and for $i \geq \ell(r^+)$ their effect on the sequence is an identity step. This handles that $\ell(q^+)$ is potentially larger than $\ell(r^+)$. Given the above, we can use the same OUT_f to τ-bounded choice define f. The same idea of using cond can also be used to show (2). □

Lemma 5 *Let τ be a set of 1-ary nondecreasing terms such that for any terms $\ell, \ell' \in \tau$ there is a term ℓ'' such that $1 + \ell + \ell' \leq \ell''$ for inputs larger than some $n \in \mathbb{N}$, provably in τ-BDC. Then τ-BDC proves its τ-bounded choice defined functions are closed under composition.*

Proof. Let f and g be τ-bounded choice defined in τ-*BDC* via terms r_f, $t_{f,init}$, $t_{f,sel}$, $t_{f,rec}$, $t_{f,\mu}$, OUT_f, ℓ_f, r_g, $t_{g,init}$, $t_{g,sel}$, $t_{g,rec}$, $t_{g,\mu}$, and OUT_g, ℓ_g where ℓ_f and ℓ_g are from τ. Let $\ell_{f\circ g} \in \tau$ be such that $1 + \ell_f + \ell_g \leq \ell_{f\circ g}$ for inputs larger than some n. Define $t_{f\circ g,init} := t_{f,init}(\mathbf{a})$ and $r_{f\circ g} := r_g^+ + \mathrm{OUT}_g^+ + r_f^+(\mathrm{OUT}_g^+)$. Notice $r_{f\circ g} = r_{f\circ g}s^+$ follows from this definition. This is useful for when we later try to use a *BDC* axioms which has a single bounding parameter b where bounded choice makes use of both bounding terms r and r^+. Let *op* be one of *sel*, *rec*, or μ. Using cond, we can define a term $t_{f\circ g,op}$ which outputs, the minimum of $t_{g,op}$ and r_g when $i \leq \ell_g$, then for $i = \ell_g + 1$ either outputs $t_{init,g}$ where $\mathrm{OUT}_g(\mathrm{LAST}(\beta_{\ell_g|r^+_{f\circ g}|}(0, w), r_f))$ has been substituted in the slot being composed or 1 depending of if *op* is *rec* or *op* is μ or *sel*, then outputs the minimum of $t_{f,op}(i - \ell_g - 1)$ and $r_f(\mathrm{OUT}_g(\mathrm{LAST}(w, r)))$ for $\ell_g + 1 < i \leq 1 + \ell_f + \ell_g$. The factor $\beta_{\ell_g|r^+_{f\circ g}|}(0, w)$ corresponds to that part of the computation sequence w computing g. Using these $t_{f\circ g,op}$, $\ell_{f\circ g}$, and OUT_f in the definition of τ-bounded choice define, we define the composition for inputs greater than $n \in \mathbb{N}$. To handle values less than or equal to n, note that in these cases the $f \circ g$ is a finite number of compositions of $t_{g,op}$, OUT_g, $t_{f,op}$, OUT_g. This could actually be carried out by a term t' in the language. So we take $\mathrm{OUT}_{f \circ g}$ to be the term which uses cond to check if $i \leq n$ and if so computes t'; otherwise, it computes OUT_f. Using an $BDC[\ell_{f\circ g}, t_{f\circ g,init}, t_{f\circ g,sel}, t_{f\circ g,rec}, t_{f\circ g,\mu}, r_{f\circ g}]$ axiom, τ-*BDC* can prove the existence of the computation sequence satisfying the τ-bounded choice defining $\hat{\Pi}^{\mathsf{b}}_0$-formula $\psi_{f\circ g}$. Given such a computation sequence $w_{f\circ g}$, as well as sequences w_f, w_g satisfying ψ_f and ψ_g, τ-*BDC* can prove using $\hat{\Pi}^{\mathsf{b}}_0$-*LIND* that the output of the $\ell_g + 1$ step of $w_{f\circ g}$ matches the value of g and that the final output of $f \circ g$ computed via our definition matches value as computed from w_g, and hence, also show uniqueness. □

Lemma 6 *Let cl denote the closed terms in the language. Let s be a term, and let A be a $\hat{\Pi}^{\mathsf{b}}_0$-formula. $\hat{S}^0_2$ can show that s is cl-bounded choice defined. Further, $\hat{S}^0_2$ can* cl*-bounded choice define $(\mu y < |a|)[s(y, a, \mathbf{b}) > 0]$ and K_A (the graph of A).*

Proof. Given a term $s(\mathbf{a})$, to show it can be cl-bounded choice defined, let ψ_s be

$$\begin{aligned}(\forall i < 2)[&\beta_{|s^+|}(0, w) = \min(s(\mathbf{a}), s(\mathbf{a})) \wedge \\ &(S0 > 0 \supset \beta_{|s^+|}(i+1, w) = \min(s(\mathbf{a}), s(\mathbf{a}))) \wedge \\ &(S0 = 0 \supset (\mu j < |s^+|)(s(\mathbf{a}) > 0))].\end{aligned}$$

I.e., $t_{sel} := S(0)$, $t_{rec} = t_\mu := s(\mathbf{a})$ and $r = s$. Then just take $\mathrm{OUT}_s := s$. Notice the term $S(0)$ is always greater than 0, so only the first clause ever applies. Notice also Out_s is allowed to ignore the LAST term and just calculate based on the inputs.

To define $f := (\mu y < |a|)[s(y, a, \mathbf{b}) > 0]$, let $\ell = 2$, $r := a$, $t_{init} := t_{sel} := 0$, $t_{rec} := 0$, and $t_\mu(j, a, \mathbf{b}) := s(j, a, \mathbf{b})$. Finally, set $\mathrm{OUT}_f(v, a, \mathbf{b}) := v$. So a witness string w of length 2 will code a sequence beginning with 0 followed $(\mu y \leq |a|)[s(y, a, \mathbf{b}) > 0]$, so $\mathrm{OUT}_f(\mathrm{LAST}(w, a), a, \mathbf{b}) = (\mu y < |a|)[s(y, a, \mathbf{b}) > 0]$, the desired value. $\hat{S}^0_2$ can prove a witness string exists since in this case ℓ is a closed term and so it can build w inductively as it only has to do so for finitely many steps. It uses the *LIND* axioms to construct the minimization for the next step after the first step.

Next given a $\hat{\Pi}^{\mathsf{b}}_0$-formula $A = (\forall y \leq |s(\mathbf{a})|)B(y, \mathbf{a})$, to define K_A, we first let K_B be the term for B from Lemma 1. Using Lemma 5, we can define K_A as $K_=((\mu y < |s(\mathbf{a})| + 1)[K_B(y, \mathbf{a}) > 0], |s(\mathbf{a})| + 1)$ where $K_=$ is defined in terms of the $K_\leq$ and $K_\wedge$ we defined in Lemma 1. □

Definition 7 *A function f is defined by τ-bounded primitive recursion, BPR^{τ}, from functions g, h, t, and r if*

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

for some terms r, t and $\ell \in \tau$.

Lemma 7

1. *$\{|\mathrm{id}|\}$-BDC proves its $\{|\mathrm{id}|\}$-bounded choice defined functions are closed under $BPR^{\{|\mathrm{id}|\}}$.*

2. *$\cup_k\{||id||^k\}$-BDC proves its $\cup_k\{||\mathrm{id}||^k\}$-bounded choice defined functions are closed under $BPR^{\cup_k\{||\mathrm{id}||^k\}}$.*

Proof. Both of these statements are proven in essentially the same way, so we show only the harder second statement. For (2), let f be defined by $BPR^{\{||\mathrm{id}||^k\}}$ for some fixed $k > 0$ via $\cup_m\{||\mathrm{id}||^m\}$-bounded choice defined functions g, h, terms t and r, and where the ℓ term in the recursion is $||\mathrm{id}||^k$. Assume g and h are $\cup_m\{||\mathrm{id}||^m\}$-bounded choice defined via $t_{g,init}$, $t_{g,sel}$, $t_{g,rec}$, $t_{g,\mu}$, OUT_g, $\ell_g := ||id||^{k'}$, $t_{h,init}$, $t_{h,sel}$, $t_{h,rec}$, $t_{h,\mu}$, and OUT_h, $\ell_h := ||id||^{k''}$. Using Lemma 4, without loss of generality, we assume that $k = k' = k''$, i.e., that $\ell = \ell_g = \ell_h$. The idea is to unwind the bounded primitive recursion as a sequence of compositions and use an argument similar to Lemma 5. We will use the power of 2, $2^{k|||id|||}$, which satisfies for inputs greater than 0: $2 \cdot ||id||^k \geq 2^{k|||id|||} \geq$ so we can use MSP rather than division in what follows. Pick $\ell_f \in \cup_m\{||\mathrm{id}||^m\}$ such that

$$\ell_f := ||id||^{k'''} >= (||id||^k+1)+(||id||^k+1)\cdot 2^{k|||id|||} = (||id||^k+1)(2^{k|||id|||}+1)$$

for all inputs larger than some fixed natural number. The first $||id||^k + 1$ in the above definition comes from the length needed to handle the computation of g, the remaining $(||id||^k+1)\cdot 2^{k|||id|||}$ factor comes from the length needed to compute the recursions made with h. Let

$$r_f := r^+(||t(n,x)||^k, x) + r_g^+ + r_h^+ + \mathrm{OUT}_g^+(r_g^+) + \mathrm{OUT}_h^+(r_h^+).$$

So r_f will be larger than any of the maximum values r, r_g^+, r_h^+, OUT_g and OUT_h used in any of the intermediate compositions needed to unwind the recursion. Also, notice $r_f = r_f^+$. Using Lemma 4 (1), we can $\cup_m\{||\mathrm{id}||^m\}$-bounded choice define g, h, using r^f rather than r^g and r^h. Set $t_{f,init} := t_{g,init}$. Let *op* be one of *sel*, *rec*, μ. Using cond, we can define a term $t_{f,op}$ whose output depends on a fixed list of cases (we suppress arguments of terms which do not change):

1. For $i \leq ||r_f^+||^k$, it outputs the minimum of $t_{g,op}$ and r_g.

2. For $i = ||r_f^+||^k{+}1$, it either outputs $t_{h,init}$ with $\mathrm{OUT}_g(\mathrm{LAST}(\beta_{\ell_g|r_f^+|}(0, w), r_f))$ appropriately substituted, or 1, depending on whether *op* is *rec* or *op* is μ or *sel*.

3. For $||r_f^+||^k + 1 < i \leq (||r_f^+||^k + 1)(2^{k|||r_f^+|||} + 1)$, let j abbreviate $\lfloor (i - ||r_f^+||^k - 1)/2^{k|||r_f^+|||})\rfloor$.

   (a) For i such that $(j + 1) \cdot (\ell_h + 1) < i \leq (j + 1) \cdot (\ell_h + 1) + \ell_h$, it outputs the minimum of $t_h(i \dot{-} j \cdot (\ell_h + 1))$ and $r_h(i \dot{-} j \cdot (\ell_h + 1))$.

   (b) For $i = (j{+}1){\cdot}(\ell_h{+}1)$, it outputs the minimum of $\mathrm{OUT}_h(\mathrm{LAST}(\beta_{\ell_h|r_f^+|}(j + 1, w), r_h))$ and $r(j)$.

   (c) For values i, $(j + 1) \cdot (\ell_h + 1) < i \leq (j + 1) \cdot 2^{k|||id|||}$, let $t_{f,op}$ be the identity function.

4. For $i > (||r_f^+||^k + 1)(2^{k|||r_f^+|||} + 1)$, let $t_{f,op}$ be the identity function.

Notice in the above, $\ell_g \cdot |r_f^+| := ||r_f^+||^k \cdot |r_f^+|$ and $\ell_h \cdot |r_f^+| := ||r_f^+||^k \cdot |r_f^+|$ are used in β to project out the whole subsequences corresponding to computing g or one application of h, then LAST is applied to get the final element of this subsequence. Using

$$BDC[\ell_f, t_{f,init}, t_{f,sel}, t_{f,rec}, t_{f,\mu}, r_f^+],$$

$\cup_k\{||id||^k\}$-*BDC* can prove the existence of the computation sequence w_f satisfying the $\{\ell_f\}$-bounded choice defining, $\hat{\Pi}_0^{\mathsf{b}}$-formula ψ_f corresponding to the terms $\ell_f, t_{f,init} t_{f,sel}, t_{f,rec}, t_{f,\mu}, r_f^+$. Given w_f, as well as the sequences, w_g, $w_{h,j}$, satisfying ψ_g and ψ_h ($w_{h,j}$ correspond to h taking as the input of the j step of the recursion), $\cup_k\{||id||^k\}$-*BDC* can prove using $\hat{\Pi}_0^{\mathsf{b}}$-*LIND* that the output of the $\ell_g + 1$ step of w_f matches the value of g, the interim j steps correspond to $w_{h,j}$ and that the final output of f computed via our definition matches the value the value as computed from w_h, ℓ. □

4 $\forall\hat{\Sigma}^{\mathsf{b}}_1$-conservativity

In this section, we give a witnessing argument to establish $\forall\hat{\Sigma}^{\mathsf{b}}_1$-conservativity between the theories $\{|\mathrm{id}|\}$-BDC and $\cup_k\{||\mathrm{id}||^k\}$-$BDC$ and S^1_2 and $\hat{R}^1_2$. To begin we introduce our witness predicate as follows:

If $A(\mathbf{a}) \in L\hat{\Pi}^{\mathsf{b}}_0$, define $WIT_A(w, \mathbf{a}) := w = 0 \wedge A(\mathbf{a})$.

If $A(\mathbf{a})$ is $(\exists x \leq t(\mathbf{a}))B$ and $A \in \hat{\Sigma}^{\mathsf{b}}_1$, define $WIT_A(w, \mathbf{a}) := w \leq t(\mathbf{a}) \wedge B(w, \mathbf{a})$.

Finally, if $A(\mathbf{a})$ is $(\exists x_1 \leq t_1)(\exists x_2 \leq t_2)B$ and $A \in E\hat{\Sigma}^{\mathsf{b}}_1$, define

$$\begin{aligned} WIT_A(w, \mathbf{a}) \quad := \quad & ispair(w) \wedge \beta(1, w) \leq t_1 \wedge \beta(2, w) \leq t_2 \wedge \\ & B(\beta(1, 2), \beta(2, w), \mathbf{a}). \end{aligned}$$

Thus, if $A \in LE\hat{\Sigma}^{\mathsf{b}}_1$ then WIT_A is equivalent in $\hat{S}^0_2$ to a $\hat{\Pi}^{\mathsf{b}}_0$-formula. The witness predicate above is simplified from Buss [4]. The simplification arises because we are in the prenex setting. From the definition of witness the next useful properties follow:

Lemma 8 *If $A(\mathbf{a}) \in LE\hat{\Sigma}^{\mathsf{b}}_1$, then:*

(a) $\hat{S}^0_2 \vdash WIT_A(w, \mathbf{a}) \supset A(\mathbf{a})$.

(b) There is a t_A so that $\hat{S}^0_2 \vdash A(\mathbf{a}) \Leftrightarrow (\exists w \leq t_A(\mathbf{a}))\, WIT_A(w, \mathbf{a})$.

(c) For t_A, $\hat{S}^0_2 \vdash WIT_A(w, \mathbf{a}) \supset w \leq t_A$.

Proof. (a) This statement is immediate from the definition of WIT_A.
(b) If $A \in \hat{\Sigma}^{\mathsf{b}}_1$ 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_A. In particular, the definition of *ispair* forces any pair for a witness to be unique. □

As the deductive system of our theories is the sequent calculus LKB of Buss [4], we need to extend our witness predicate definition to cedents. Given a cedent $\Gamma = \{A_1, \ldots, A_n\}$, we write $\wedge\,\Gamma$ (resp. $\vee\,\Gamma$) to denote the conjunction (resp. disjunction) of its formulas. Let $w = \langle\langle w_1, \cdots, w_n\rangle\rangle$ denote pairings of the form $\langle w_1, \langle w_2, \cdots, \langle w_{n-1}, w_n\rangle \cdots\rangle\rangle$.

We define $WIT_{\wedge\Gamma}(w, \mathbf{a})$ (resp. $WIT_{\vee\Gamma}(w, \mathbf{a})$) by induction:

1. If $\Gamma = \emptyset$, define $WIT_{\wedge\Gamma}(w, \mathbf{a})$ (resp. $WIT_{\vee\Gamma}(w, \mathbf{a})$) to be $0 = 0$ (resp. $\neg(0 = 0)$).

2. If $\Gamma = \{A\}$, define $WIT_{\wedge\Gamma}(w, \mathbf{a})$ and $WIT_{\vee\Gamma}(w, \mathbf{a})$ to be $WIT_A(w, \mathbf{a})$.

3. If $\Gamma = \{A_1, \ldots, A_n\}$, let Γ' be $\{A_2, \ldots A_n\}$ and set $WIT_{\wedge\Gamma}(w, \mathbf{a})$ (resp. $WIT_{\vee\Gamma}(w, \mathbf{a})$) to be
$WIT_{A_1}(\beta(1, w), \mathbf{a}) \wedge WIT_{\wedge\Gamma'}(\beta(2, w), \mathbf{a})$,
(resp. $WIT_{A_1}(\beta(1, w), \mathbf{a}) \wedge w_1 \leq t_{A_1}) \vee WIT_{\vee\Gamma'}(\beta(2, w), \mathbf{a})$).

Both $WIT_{\wedge\Gamma}$ and $WIT_{\vee\Gamma}$ are equivalent to $\hat{\Pi}^{\mathsf{b}}_0$-formulas in $\hat{S}^0_2$.

Lemma 9 *Let Γ, Δ be cedents of $LE\hat{\Sigma}^{\mathsf{b}}_1$-formulas with free variables $\mathbf{a}$. There is a term t_Γ such that $\hat{S}^0_2 \vdash WIT_{\wedge\Gamma}(w, \mathbf{a}) \supset w \leq t_\Gamma$ and $\hat{S}^0_2 \vdash WIT_{\vee\Gamma}(w, \mathbf{a}) \supset w \leq t_\Gamma$.*

We also have

$$\hat{S}^0_2 \vdash (\exists w \leq t_\Gamma)\, WIT_{\wedge\Gamma}(w, \mathbf{a}) \to (\exists w \leq t_\Delta)\, WIT_{\vee\Delta}(w, \mathbf{a})$$

if and only if $\hat{S}^0_2 \vdash \Gamma \to \Delta$.

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 8. □

Theorem 1

1. *Suppose $S^1_2 = \hat{S}^1_2 \vdash \Gamma \to \Delta$ where Γ and Δ are cedents of $LE\hat{\Sigma}^{\mathsf{b}}_1$-formulas. Let $\mathbf{a}$ be the free variables in this sequent. Then there is an $\{|id|\}$-choice defined in $\{|\mathrm{id}|\}$-BDC function f such that:*

$$\{|\mathrm{id}|\}\text{-}BDC \vdash \psi_f(v, w, \mathbf{a}, r_f) \wedge WIT_{\wedge\Gamma}(w, \mathbf{a}) \supset \\ WIT_{\vee\Delta}(\mathrm{OUT}_f(\mathrm{LAST}(v, r_f), w, \mathbf{a}), \mathbf{a}).$$

2. *Suppose $\hat{R}^1_2 \vdash \Gamma \to \Delta$ where Γ and Δ are cedents of $LE\hat{\Sigma}^{\mathsf{b}}_1$-formulas. Let $\mathbf{a}$ be the free variables in this sequent. Then there is an $\cup_k\{||id||^k\}$-choice defined in $\cup_k\{||\mathrm{id}||^k\}$-BDC function f such that:*

$$\cup_k\{||\mathrm{id}||^k\}\text{-}BDC \vdash \psi_f(v, w, \mathbf{a}, r_f) \wedge WIT_{\wedge\Gamma}(w, \mathbf{a}) \supset \\ WIT_{\vee\Delta}(\mathrm{OUT}_f(\mathrm{LAST}(v, r_f), w, \mathbf{a}), \mathbf{a}).$$

Proof. In both cases, Theorem 1 is proven by induction on the number of sequents in the proof of $\Gamma \to \Delta$. By cut-elimination, we can assume all the sequents in the proof are $LE\hat{\Sigma}^{\mathsf{b}}_1$. Both of the statements are proven in the essentially same way, so we only prove (2). Further, most of the other cases are similar to previous witnessing arguments and rely on closure under composition of the class of witnessing functions and Lemma 6, so we only show the base case, ($\forall$: right) case, $\hat{\Sigma}^{\mathsf{b}}_1$-*LLIND* case as these highlight the use of the closure properties of the *BDC* axioms.

(Base case) In the base case, an $\hat{R}^1_2$- proof consists of a *BASIC* axiom, a logical axiom, or an equality axiom. The formulas in the $\hat{R}^1_2$ proof of $\Gamma \to \Delta$ will all be open and so the witness predicate for them will have the form $w = 0 \wedge A(\mathbf{a})$. A witness to a formula is thus just 0, and a witness to $WIT_{\vee\Delta}$ will be just a fixed number of pairings of 0's, so witnessable by a closed term. Hence, f is $\cup_k\{||id||^k\}$-choice defined by Lemma 6 and

$$\cup_k\{||\mathrm{id}||^k\}\text{-}BDC \vdash \psi_f(v, w, \mathbf{a}, r_f) \wedge WIT_{\wedge\Gamma}(w, \mathbf{a}) \supset \\ WIT_{\vee\Delta}(\mathrm{OUT}_f(\mathrm{LAST}(v, r_f), w, \mathbf{a}), \mathbf{a})$$

will follow from this and the axiom we are trying to witness itself.

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

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

By the induction hypothesis there is a $\cup_k\{||id||^k\}$-bounded choice defined function g such that

$$\cup_k\{||\mathrm{id}||^k\}\text{-}BDC \vdash \psi_g(v, w, b, \mathbf{a}, r_g) \wedge WIT_{b\leq t\wedge(\wedge\Gamma)}(w, b, \mathbf{a}) \supset \\ WIT_{A\vee(\vee\Delta)}(\mathrm{OUT}_g(\mathrm{LAST}(v, r_g), w, b, \mathbf{a}), b, \mathbf{a}) \; .$$

By cut-elimination, $(\forall x \leq t)A(x)$ is a $\hat{\Pi}^{\mathsf{b}}_0$-formula, so t must be of the form $t = |s|$ and A is an open formula. Let y be $(\mu i < |s| + 1)(K_{\neg A}(i) > 0)$ (using Lemma 1) and define f to be $g(\langle 0, w\rangle, \mathbf{a}, y)$. The 0 in the ordered pair is the witness to $WIT_{b\leq t}(w, b, \mathbf{a}) := b \leq t(\mathbf{a}) \wedge w = 0$. The function f is $\cup_k\{||id||^k\}$-bounded choice defined by Lemma 6 and Lemma 5 and it is not hard to show that

$$\cup_k\{||\mathrm{id}||^k\}\text{-}BDC \vdash \psi_f(v', w, \mathbf{a}) \wedge WIT_{\wedge\Gamma}(w, \mathbf{a}) \supset \\ WIT_{\forall x\leq|s|\; A\vee(\vee\Delta)}(\mathrm{OUT}_f(\mathrm{LAST}(v', r_f), w, \mathbf{a}), \mathbf{a}) \; .$$

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

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

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

$$\cup_k\{||\mathrm{id}||^k\}\text{-}BDC \vdash \psi_g(v, w, b, \mathbf{a}) \wedge \mathit{WIT}_{A(b)\wedge(\wedge\Gamma)}(w, b, \mathbf{a}) \supset \\ \mathit{WIT}_{A(Sb)\vee(\vee\Delta)}(\mathrm{OUT}_g(v, w, b, \mathbf{a}), b, \mathbf{a}).$$

Informally, the idea to witness the lower sequent is the following: Run g on w a witness for $A(0), \Gamma$. Either this witnesses $A(S(0))$ or it witnesses Δ. In the latter case, we are done. In the former case, we run g on the witness just produced for $A(S(0))$ 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 $A(||s||)$. More formally, using Lemma 7, we bounded choice define a function f by $BPR^{\{||id||\}}$ in the following way. First, we let

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

This is $\cup_k\{||\mathrm{id}||^k\}$ bounded choice definable by Lemma 6 and Lemma 5. We would like to define f by the following recursion

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

which is not exactly that of Lemma 7. 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

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

where min's have been suppressed for readability and where $m = t^{+}_{A(Sb)(||s||,\mathbf{a})\vee\bigvee\Delta}$, a term bounding the witness size for $A(Sb) \vee (\vee\,\Delta)$. Then $f(u, w, \mathbf{a}) = \beta_{|m|}(\mathit{min}(u, ||s||), h(w, \mathbf{a}))$. So both f and h will be bounded choice defined by Lemma 7. We would like to show

$$\cup_k\{||\mathrm{id}||^k\}\text{-}BDC \vdash \psi_f(v, w, \mathbf{a}) \wedge \mathit{WIT}_{A(0)\wedge\Gamma}(w, \mathbf{a}) \supset \\ \mathit{WIT}_{A(||s||)\vee\Delta}(\mathrm{OUT}_f(\mathrm{LAST}(v, r_f), ||s||, w, \mathbf{a}), \mathbf{a}).$$

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

$$\cup_k\{||\mathrm{id}||^k\}\text{-}BDC \vdash \psi_h(v, w, \mathbf{a}) \wedge \mathit{WIT}_{A(0)\wedge(\wedge\Gamma)}(w, \mathbf{a}) \supset \\ \mathit{WIT}_{A(0)\vee(\vee\Delta)}(\beta_{|m|}(0, \mathrm{OUT}_h(\mathrm{LAST}(v, r_h), w, \mathbf{a})), \mathbf{a})$$

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

$$\cup_k\{||\mathrm{id}||^k\}\text{-}BDC \vdash \psi_h(v, w, \mathbf{a}) \wedge \mathit{WIT}_{A(0)\wedge\Gamma}(w, \mathbf{a}) \wedge Sb \leq ||s|| \wedge \\ \mathit{WIT}_{A(b)\vee(\vee\Delta)}(\beta_{|m|}(b, \mathrm{OUT}_h(\mathrm{LAST}(v, r_h), w, \mathbf{a})), b, \mathbf{a}) \supset \\ \mathit{WIT}_{A(Sb)\vee(\vee\Delta)}(\beta_{|m|}(Sb, \mathrm{OUT}_h(\mathrm{LAST}(v, r_h), w, \mathbf{a})), Sb, \mathbf{a}).$$

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

$$\cup_k\{||\mathrm{id}||^k\}\text{-}BDC \vdash \psi_h(\mathrm{LAST}(v, r_h), w, \mathbf{a}) \wedge \mathit{WIT}_{A(0)\wedge(\wedge\Gamma)}(w, \mathbf{a}) \supset \\ \mathit{WIT}_{A(||s||)\vee(\vee\Delta)}(\beta_{|m|}(||s||, \mathrm{OUT}_h(\mathrm{LAST}(v, r_h), w, \mathbf{a})), ||s||, \mathbf{a}).$$

Hence, as

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

and $\psi_f = \psi_h$ we have

$$\cup_k\{||\mathrm{id}||^k\}\text{-}BDC \vdash \psi_f(v, w, \mathbf{a}) \wedge \mathit{WIT}_{A(0)\wedge(\wedge\Gamma)}(w, \mathbf{a}) \supset \\ \mathit{WIT}_{A(||s||)\vee(\vee\Delta)}(\mathrm{OUT}_f(\mathrm{LAST}(v, r_f), ||s||, w, \mathbf{a}), \mathbf{a}).$$

□

Corollary 1 *The following conservation results hold:*

1. S^1_2 *is* $\forall\hat{\Sigma}^{\mathsf{b}}_1$*-conservative over* $\{|\mathrm{id}|\}$*-BDC.*
2. $\hat{R}^1_2$ *is* $\forall\hat{\Sigma}^{\mathsf{b}}_1$*-conservative over* $\cup_k\{||\mathrm{id}||^k\}$*-BDC.*

Proof. Both statements are proven in the same way, so we show only the first. First, $\{|\mathrm{id}|\}$-*BDC* is contained in S^1_2 by Lemma 3. Suppose $\hat{S}^1_2$ proves $\forall x(\exists y \leq t)B(x, y, \mathbf{c})$ where B is $\hat{\Pi}^{\mathsf{b}}_0$. Then $\hat{S}^1_2$ proves $(\exists y \leq t)B(a, y, \mathbf{c})$ where a is free, so by Theorem 1 and the definitions of witnesses for sequents, $\{|\mathrm{id}|\}$-*BDC* will prove:

$$\psi_f(v, a, \mathbf{c}) \supset \mathit{WIT}_{(\exists y \leq t)B}(\mathrm{OUT}_f(\mathrm{LAST}(v, r_f), a, \mathbf{c}), a, \mathbf{c})$$

for some $\{|\mathrm{id}|\}$ choice defined function f. By the definitions of $\{|\mathrm{id}|\}$ choice defined, $\{|\mathrm{id}|\}$-*BDC* proves $\exists v \psi_f(v, a, \mathbf{c})$, where v is bounded by Parikh's Theorem. So combined with Lemma 8, this shows $\{|\mathrm{id}|\}$-*BDC* proves $(\exists y \leq t)B(a, y, \mathbf{c})$, and hence, $\forall x(\exists y \leq t)B(x, y, \mathbf{c})$. □

A formula $A(\mathbf{a})$ is $\hat{\Delta}_1^b$ with respect to a theory T, if there exists a $\hat{\Sigma}_1^{\mathsf{b}}$ formula A_Σ and a $\hat{\Pi}_1^{\mathsf{b}}$ formula A_Π and

$$T \vdash A(\mathbf{a}) \Leftrightarrow A_\Sigma(\mathbf{a}) \Leftrightarrow A_\Pi(\mathbf{a}).$$

Corollary 2 *Let T be S_2^1 or $\hat{R}_2^1$. Then T proves every $\hat{\Delta}_1^b$-formula is equivalent to a $\hat{\Sigma}_1^{\mathsf{b}}$-formula of the form $C(\mathbf{a}, 1)$ and to a $\hat{\Pi}_1^{\mathsf{b}}$-formula equivalent to $\neg C(\mathbf{a}, 0)$ where $C(\mathbf{a}, b)$ is:*

$$\begin{aligned}(\exists w \leq 2^{\ell(r^+)|r^+ + 1|})(\forall i < \ell(r^+)))[(\beta_{|r^+|}(0, w) = \min(t_{init}(\mathbf{a}), r(\mathbf{a})) \wedge \\ (t_{sel}(i, \mathbf{a}) > 0 \supset \beta_{|r^+|}(i + 1, w) = \min(t_{rec}(\beta_{|r^+|}(i, w), i, \mathbf{a}), r(\mathbf{a}))) \wedge \\ (t_{sel}(i, \mathbf{a}) = 0 \supset \beta_{|r^+|}(i + 1, w) = \mu j < |r^+|(t_\mu(j, \beta_{|r^+|}(i, w), \mathbf{a}) > 0)) \wedge \\ \mathrm{BIT}(0, \mathrm{LAST}(w, r(\mathbf{a}))) = b].\end{aligned}$$

where is $\ell := |id|$ when $T = S_2^1$, and ℓ is of the form $||id||^k$ for some k when $T = \hat{R}_2^1$, and where r, t_{init}, t_{sel}, t_{rec}, t_μ, OUT *are L_2 terms.*

Proof. In what follows ℓ will be either $|id|$ or $||id||^k$ for some fixed k. Suppose A is $\hat{\Delta}_1^b$ in T. Let $A_\Sigma \in \hat{\Sigma}_1^{\mathsf{b}}$ and $A_\Pi \in \hat{\Pi}_1^{\mathsf{b}}$ be provably equivalent to A in T. Consider $B(x, y) :=$

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

Then T proves $(\forall x)(\exists y \leq 1)B(x, y)$. Further, $(\exists y \leq 1)B(x, y)$ is equivalent to a $E\hat{\Sigma}_1^{\mathsf{b}}$-formula. So by Theorem 1 there is an ℓ bounded choice definable g such that $T \vdash \psi_g(x, y) \supset \mathit{WIT}_{(\exists y \leq 1)B}(x, y)$. This implies

$$T \vdash \psi_g(x, y) \supset B(x, (y)_1).$$

Let $f(x) = (g(x))_1$. Since g is ℓ bounded choice definable, by closure under composition and L_2 terms, f will be ℓ bounded choice definable. Further, the definition of B implies $f(x) = 1 \Leftrightarrow B(x, 1) \Leftrightarrow A(x)$. To get the form of our definition exactly as in the statement of the Corollary, we can replace the $\mathrm{OUT}(\mathrm{LAST}(w, r(\mathbf{a})), \mathbf{a}) = 1$ in ℓ-bounded choice definition of f with $\mathrm{BIT}(0, \mathrm{LAST}(w, r(\mathbf{a})), \mathbf{a}) = 1$ by tacking onto the sequence w given with at least one more block which computes the most significant bit of $\mathrm{OUT}(\mathrm{LAST}(w, r(\mathbf{a})), \mathbf{a})$, then copies this value for the remaining blocks, adjusting r to handle this slightly longer sequence. □

5 Finite Axiomatizability

Next we show our finitely axiomatization results. As we mentioned in the introduction it was previously shown by Cook and Kolokolova [9] that the $\forall\hat{\Sigma}^{\mathsf{b}}_1$-consequences of S^1_2 are finitely axiomatized. Their proof goes through a second-order theory V_1-HORN. We will give a completely first-order argument for this as well as results concerning axiomatizations of variants of $\hat{R}^1_2$. We begin by considering how to encode terms.

By Parikh's Theorem [21], if a bounded theory $T \vdash \exists y A(\mathbf{a}, y)$ then $T \vdash \exists y \leq t(\mathbf{a}) A(\mathbf{a}, y)$ for some term t. Recall $\#$ is the fastest growing function in our language. If t does not contain $\#$, then for some fixed $n > 0$ and $\sum_i a_i > n$, $t(\mathbf{a}) \leq 2^{|\sum_i a_i|^2}$. Let $C_\#(t)$ denote the number of occurences of $\#$ in the term t, the **smash complexity of** t. Then, in general, for large enough inputs, $t(\mathbf{a}) \leq 2^{|\sum_i a_i|^{C_\#(t)+1}}$. As the $\#$ function grows more slowly than the exponential function, we have to be a careful in defining our encoding. We can code a fixed term t as a number e_t according to some choice of encoding, and an expression like $2^{|\sum_i a_i|^{C_\#(t)+1}}$ would then bound the output of t based on inputs $\mathbf{a}$. Moreover, for a reasonable encoding $C_\#(t) + 1 \leq |e_t|$. Since we would like to use encoding e in some of our formulas as a free variable, we imagine adding a second free variable z to our formulas. If a fixed number e_t is the encoding of a term t, we set $z_t = 2^{(|\sum_i a_i|)^{C_\#(t)+1}}$ as the value for z. Finally, the computation sequences w that $\cup_k\{||id||^k\}$-BDC and R^1_2 can easily manipulate involve length length many steps, not length many steps. To get around this in a way that still works in the fixed term t and code e_t case, we use a code E such that the first decode operation is to take the length $e = |E|$. In this set up, we will have $C_\#(t) + 1 \leq |e_t| \leq ||E_t||$.

Lemma 10 *Let $n \in \mathbb{N}$. $\cup_k\{||id||^k\}$-BDC can $\cup_k\{||id||^k\}$ bounded choice define and$\{|id|\}$-BDC can $\{|id|\}$ bounded choice define a function* $\mathrm{term}(E, z, a_1, \ldots a_n)$ *such that for any fixed n-ary term t there is an $e_t = |E_t|$, where if we let $z_t = 2^{|\sum_i a_i|^{C_\#(t)+1}}$ and ψ_{term}, $\mathrm{OUT}_{\mathrm{term}}$ be from either of these bounded choice definitions, then $\hat{S}^0_2$ proves:*

$$\forall \mathbf{a} \exists w \leq 2^{|e_t| \cdot |E_t + z_t|} \psi_{\mathrm{term}}(w, E_t, z_t, \mathbf{a}, 2^{|E_t+z_t|}) \wedge \\ \mathrm{OUT}_{\mathrm{term}}(\mathrm{LAST}(w, 2^{|E_t+z_t|}), E_t, \mathbf{a}, 2^{|E_t+z_t|}) = t(\mathbf{a}).$$

Proof. The $\{|id|\}$ bounded choice definition in $\{|id|\}$-BDC will follow from the $\cup_k\{||id||^k\}$ bounded choice definition using Lemma 4. Throughout our proof will use e to abbreviate $|E|$. The $r_{\mathrm{term}}(E, z, \mathbf{a})$ in the $\cup_k\{||id||^k\}$

bounded choice definition will be $2^{|E+z|}$ and we will take $\ell = ||id||$. In the choice definition, the witness string would hence be bounded by $2^{||r^+_{\text{term}}||\cdot|r^+_{\text{term}}|} = 2^{||E+z||\cdot|E+z|}$ where $||r^+_{\text{term}}|| = ||E+z|| \geq ||E|| = |e|$. We can use the techniques of Lemma 4 to pad our computation sequences to the longer lengths to meet this definition rather than the bound implied by generalizing the $\hat{S}^0_2$ result mentioned above. To show the $\hat{S}^0_2$ result we develop a coding scheme for terms in our language. First, we fix codes for 0, for the seven function symbols of L_2, and for the variables $a_1, \ldots a_n$. We use $\ulcorner\urcorner$ around a symbol to denote the code for that symbol. I.e., $\ulcorner + \urcorner$ is the code for $+$. We choose our coding so that all codes require less than $|m|$ bits, where $m \geq 10+n$. We choose 0 to code $\ulcorner NOP \urcorner$, meaning no operation, and 1 to code $\ulcorner INIT \urcorner$, meaning initialize the computation stack. Given the code for $\ulcorner NOP \urcorner$ is 0, if one tries to project out operations beyond the end of a code, one naturally just projects outs $\ulcorner NOP \urcorner$'s. The code for a term t is a number E such that $e = |E|$ can be viewed as a sequence of blocks of length $|m|$ that write out t in postfix order. So $s_1 + s_2$ would be coded as the three blocks $\ulcorner s_1 \urcorner \ulcorner s_2 \urcorner \ulcorner + \urcorner$. To make our definition below a little easier we require all term codes to have $\ulcorner INIT \urcorner$ in the first, low-order, $|m|$ bit block. Given this coding, we next define $t_{\text{term},init}$, $t_{\text{term},sel}$, $t_{\text{term},rec}$, $t_{\text{term},\mu}$, needed for the bounded choice definition. First, we define $t_{\text{term},init} := 0$ and $t_{\text{term},sel} := t_{\text{term},\mu} := 1$. Since $t_{\text{term},sel} = 1$, we will only make use of $t_{\text{term},rec}$ and not $t_{\text{term},\mu}$ in computing a witnessing computation w for the $\cup_k\{||id||^k\}$ bounded choice definition. The block-size $|b|$ used in the witnessing computation will be $|r^+_{\text{term}}| = |E+z| \geq |z|$. In the case of a term t, the value $|E_t + z_t| \geq |z_t|$ will be greater than or equal to the number of bits needed to represent any intermediate computation of t by the discussion proceeding the lemma. We imagine the ith block as coding the ith state of a stack used to compute the postfix computation of term represented by e. The total number of blocks needed to carry out this computation is less than $|e|$, hence our bound on w in the statement of the lemma. We divide the stack in turn into blocks of size $2^{\lfloor \frac{1}{2}||b|| \rfloor}$, with the 0th block being the top of the stack. Using cond we can define the output of $t_{rec}(u, i, E, \mathbf{a}, b)$, where we are especially interested when $u = \beta_{|b|}(i, w)$ and $b = r_{\text{term}}$, by cases as follows:

1. If $i = 0$ or $\beta_{|m|}(i, e) = \ulcorner INIT \urcorner$, $t_{rec}(u, i, E, \mathbf{a}, b) = 0$. This initializes the stack.

2. If $\beta_{|m|}(i, e) = \ulcorner NOP \urcorner$, $t_{\text{term},rec}(u, i, E, \mathbf{a}, b) = u$.

3. If $\beta_{|m|}(i, e) = \ulcorner a_j \urcorner$, $1 \leq j \leq n$, then $t_{\text{term},rec}(u, i, E, \mathbf{a}, b) := a_j + u \cdot$

$2^{2^{\lfloor \frac{1}{2}||b||\rfloor}}$. The effect here is to push a_j onto the stack.

4. If $\beta_{|m|}(i,e) = \ulcorner 0 \urcorner$, then $t_{\mathrm{term},rec}(u,i,E,\mathbf{a},b) := 0 + u \cdot 2^{2^{\lfloor \frac{1}{2}||b||\rfloor}}$. The effect here is to push 0 onto the stack.

5. If $\beta_{|m|}(i,e) = \ulcorner S \urcorner$, then $t_{\mathrm{term},rec}(u,i,E,\mathbf{a},b) := (\beta_{2^{\lfloor \frac{1}{2}||b||\rfloor}}(0,u)+1) + \mathrm{MSP}(u, 2^{\lfloor \frac{1}{2}||b||\rfloor}) \cdot 2^{2^{\lfloor \frac{1}{2}||b||\rfloor}}$. This pops the top of the stack, adds 1, and pushes the result onto the stack.

$$\cdots$$

6. If $\beta_{|m|}(i,e) = \ulcorner \# \urcorner$, then $t_{\mathrm{term},rec}(u,i,E,\mathbf{a},b) :=$

$$(\beta_{2^{\lfloor \frac{1}{2}||b||\rfloor}}(0,u) \# (\beta_{2^{\lfloor \frac{1}{2}||b||\rfloor}}(1,u)) + \mathrm{MSP}(u, 2 \cdot 2^{\lfloor \frac{1}{2}||b||\rfloor}) \cdot 2^{2^{\lfloor \frac{1}{2}||b||\rfloor}}.$$

This pops the top two elements off the stack, computes their #, and pushes the result onto the stack.

To complete our choice definition, we define $\mathrm{OUT}_{\mathrm{term}}(u,\mathbf{a}) := \beta_{2^{\lfloor \frac{1}{2}||b||\rfloor}}(0,u)$, which returns the top of the stack. Given these definitions, by induction on the complexity of t (a fixed finite number), $\hat{S}^0_2$ can show:

$$\forall \mathbf{a} \exists w \leq 2^{|e_t|\cdot|E_t+z_t|} \psi_{\mathrm{term}}(w, E_t, z_t, \mathbf{a}, 2^{|E_t+z_t|}) \wedge$$
$$\mathrm{OUT}_{\mathrm{term}}(\mathrm{LAST}(w, 2^{|E_t+z_t|}), E_t, \mathbf{a}, 2^{|E_t+z_t|}) = t(\mathbf{a}).$$

□

We next want to isolate a finitely axiomatized theory T such that $\hat{S}^0_2 \subseteq \mathrm{T} \subseteq R^1_2$. The idea is to use Lemma 2. Given a $\hat{\Pi}^{\mathsf{b}}_0$ formula A, let s_A and t_A be the terms from Lemma 2. Suppose we had a new axiom that asserts the existence of a string y whose ith bit for $i \leq |s_A|$ is on if and only if $t_A(i,b) > 0$. Using the string y_A in the BITMIN axiom would then imply the $\mathrm{BITMIN}_{s_A,t_A}$ axiom and, hence, $LIND_A$. This new axiom together with *EBASIC* and BITMIN would thus imply $\hat{S}^0_2$. The discussion motivates the following axiom:

Definition 8 *Let* $\mathrm{bd}(E,z) = 2^{||E||\cdot|E+z|}$. *Define* $UC(E,d,a,\mathrm{bd}(E,z))$ *to be the axiom*

$$(\exists y \leq 2^{|d|})(\exists w \leq \mathrm{bd}(E,z)\#(2d))\mathrm{TERMCOMP}(E,z,d,a,y,w)$$

where TERMCOMP *is:*

$$\forall k \leq |d| \psi_{\mathrm{term}}(\beta_{|\mathrm{bd}(E,z)|}(k,w), E, k, a, r_{\mathrm{term}}) \wedge$$
$$\mathrm{BIT}(k, \mathrm{OUT}_{\mathrm{term}}(\mathrm{LAST}(\beta_{|\mathrm{bd}(E,z)|}(k,w), r_{\mathrm{term}}), E, k, a, r_{\mathrm{term}})) = \mathrm{BIT}(k,y).$$

Using pairing, UC is provably equivalent to a $\hat{\Sigma}^{\mathsf{b}}_1$-formula. Let $TUC := EBASIC$+BITMIN+UC. So TUC is finitely axiomatized. Moreover, we have:

Lemma 11 $\hat{S}^0_2 \subseteq TUC \subseteq R^1_2$.

Proof. The discussion prior to the definition shows the first containment where we take a substitution instance of UC with $d = s_A$, $E = E_{t_A}$ and $z = z_{t_A}$. To see the $TUC \subseteq R^1_2$, first note that by Lemma 10 and by Lemma 4, $\hat{S}^0_2 \subseteq R^1_2$ proves:

$$(\forall k \leq |d|)(\exists w' \leq \mathrm{bd}(E,z))\psi_{\mathrm{term}}(w', E, k, a, r_{\mathrm{term}}).$$

So by $BB\hat{\Sigma}^{\mathsf{b}}_1$, R^1_2 proves:

$$(\exists w \leq \mathrm{bd}(E,z)\#(2d))(\forall k \leq |d|)\psi_{\mathrm{term}}(\beta_{|\mathrm{bd}(E,z)|}(k,w), E, k, a, r_{\mathrm{term}}). \quad (1)$$

Let $A(j, 2^{\min(b,|d|)})$ be the formula

$$\begin{aligned}&(\exists y \leq 2^{\min(b,|d|)})(\exists w \leq \mathrm{bd}(E,z)\#(2d))(\forall k \leq |d|)[\\ &\quad \psi_{\mathrm{term}}(\beta_{|\mathrm{bd}(E,z)|}(k,w), E, k, a, r_{\mathrm{term}}) \wedge\\ &\quad (j \leq k \wedge k \leq j + b \wedge j + b \leq |d| \supset\\ &\quad \mathrm{BIT}(k, \mathrm{OUT}_{\mathrm{term}}(\mathrm{LAST}(\beta_{|\mathrm{bd}(E,z)|}(k,w), r_{\mathrm{term}}), E, k, a, r_{\mathrm{term}})) = \mathrm{BIT}(k,y))]\end{aligned}$$

Notice using pairing, $A(j, 2^{\min(b,|d|)})$ is provably equivalent in R^1_2 to a $\hat{\Sigma}^{\mathsf{b}}_1$ formula. Roughly, the formula A asserts the existence of a string whose bits match the jth through $j+b$th of the string y asserted to exist by the UC axiom. Also, $A(j, 2^{\min(0,|d|)})$ follows easily from (1). Further, $A(j, 2^{\min(b,|d|)})$ and $A(j + 2^{\min(b,|d|)}, 2^{\min(b,|d|)})$, imply $A(j, 2^{\min(S(b),|d|)})$, so the result follows by $\hat{\Sigma}^{\mathsf{b}}_1$-*LLIND*. □

Remark 1 *By using our pairing function multiple times, we can define terms for triples, and, in general, n-tuples. For any term $t(a_0, ..., a_n)$, the term $t'(u) = t((u)_0, \ldots, (u)_n)$ satisfies $t(a_0, \ldots, a_n) = t'(\langle a_0, \ldots, a_n\rangle)$. Further, this is provable in $\hat{S}^0_2$. Using this idea, we can show over $\hat{S}^0_2$, and hence over TUC, that*

$$BDC[t_{init}(\mathbf{a}), t_{sel}(v, i, \mathbf{a}), t_{rec}(v, i, \mathbf{a}), t_{\mu}(j, v, \mathbf{a}), b]$$

is equivalent to an axiom

$$BDC[t'_{init}(\langle\mathbf{a}\rangle), t'_{sel}(v, i, \langle\mathbf{a}\rangle), t'_{rec}(v, i, \langle\mathbf{a}\rangle), t'_{\mu}(j, v, \langle\mathbf{a}\rangle), b]$$

where we have suitably modified the original terms. So in terms of axiomatizing τ-BDC, it suffices to only consider BDC axioms with one free variable (parameters i, j, v in the terms above will always be used for bound variable in BDC axioms). This same idea can also be applied to the BDC$'$ axioms we will describe in a moment.

In what follows, we assume that our *BDC* axiom have a single parameter a rather than a vector $\mathbf{a}$. In order to get our finite axiomatization results, we need to modify our *BDC* axioms so that the way in which the μ operator is computed is more directly recorded in the witness string. To this end, we next formulate a variant of the *BDC* axiom:

Definition 9 *Let τ be a collection of 1-ary nondecreasing terms. Define $\tau-$ BDC$'$ to be the theory consisting of TUC together with BDC$'[\ell, t_{init}, t_{sel}, t_{rec}, t_\mu, b]$ axioms:*

$$
\begin{aligned}
&(\exists w \leq 2^{\ell(b)\cdot|b|})(\exists w' \leq 2^{\ell(b)|b'|})(\forall i < \ell(b))[\\
&\quad (\beta_{|b|}(0, w) = \min(t_{init}(a), b) \wedge \beta_{|b'|}(0, w') = 0) \wedge\\
&\quad (t_{sel}(\beta_{|b|}(i, w), i, a) > 0 \supset \beta_{|b|}(i+1, w) = \min(t_{rec}(\beta_{|b|}(i, w), i, a), b) \wedge\\
&\qquad \wedge\, \beta_{|b'|}(i, w') = 0) \wedge\\
&\quad (t_{sel}(\beta_{|b|}(i, w), i, a) = 0 \supset (\mathrm{ispair}(\beta_{|b'|}(i, w')) \wedge\\
&\qquad \mathrm{TERMCOMP}(E_{t_\mu}, z_{t_\mu}, b, \langle \beta_{|b|}(i, w), a\rangle, (\beta_{|b'|}(i, w'))_1, (\beta_{|b'|}(i, w'))_2) \wedge\\
&\qquad \mathrm{LEASTON}(\beta_{|b|}(i+1, w), (\beta_{|b'|}(i, w')))_1)))].
\end{aligned}
$$

where $\ell \in \tau$, and t_{sel}, t_{rec}, t_μ are L_2-terms. Here E_{t_μ} is the fixed code for the term t_μ, $z_{t_\mu} = 2^{|a|^{C\#(t_\mu)+1}}$, and $b' = 2^{2\cdot|\mathrm{bd}(E_{t_\mu}, z_{t_\mu})\#2b|+1}$.

The clause beginning with $\beta_{|b|}(0, w)$ and the one beginning with $t_{sel}(\beta_{|b|}(i, w), i, a) > 0$ above correspond to the same clauses in a *BDC* axiom except that we also assert a second string w' has $\beta_{|b|}(0, w') = 0$ or $\beta_{|b|}(i, w') = 0$. Here the string w' is used to store the computations related to doing a μ operation, and neither of these clauses concerns a μ-operation. The third clause, beginning with $t_{sel}(\beta_{|b|}(i, w), i, a) = 0$, concerns a μ computation step. In a *BDC* axiom the μ-operation is over values less than $|b|$. Here we imagine the ith block of bits of w' is a pair, the first component being a string of length $2^{|b|}$ recording in its jth bit whether $t_\mu(j, a) > 0$, and the second component being a computation sequence of length $\mathrm{bd}(E_{t_\mu}, z_{t_\mu})\#2b > 2^{|b|}$, computing the value of $t_\mu(j, a)$. So the length of this pair is bounded by $2 \cdot |\mathrm{bd}(E_{t_\mu}, z_{t_\mu})\#2b| + 1$.

Define R'^1_2 to be $\hat{R}^1_2 + UC$. From this definition and Lemma 11, we have $\hat{R}^1_2 \subseteq R'^1_2 \subseteq R^1_2$. For $\hat{S}^1_2$, since $R^1_2 \subseteq \hat{S}^1_2 = S^1_2$, $\hat{S}^1_2 + UC = \hat{S}^1_2 = S^1_2$.

Theorem 2

1. $\cup_k\{||id||^k\}$*-BDC* $\subseteq \cup_k\{||id||^k\}$*-BDC'*.

2. R'^1_2 *is* $\forall\hat{\Sigma}^{\mathsf{b}}_1$*-conservative over* $\cup_k\{||id||^k\}$*-BDC'*.

Proof. For (1), TUC can prove using $LIND$ on the $\hat{\Pi}^{\mathsf{b}}_0$ matrices of

$$BDC'[||id||^m, t_{init}, t_{sel}, t_{rec}, t_\mu, b] \text{ and } BDC[||id||^m, t_{init}, t_{sel}, t_{rec}, t_\mu, b],$$

that when one projects out blocks of size $|b|$ from a witness w for outer existential in the former they match projections of size $|b|$ bits of a witness for existential in the latter. As part of the induction step of the $LIND$ a secondary $LIND$ is used to show that the blocks of w' give pairs correctly computing μ step of the BDC axiom.

For (2), consider any $A := BDC'[||id||^m, t_{init}, t_{sel}, t_{rec}, t_\mu, b]$. Using pairing, A is provably equivalent to a $\hat{\Sigma}^{\mathsf{b}}_1$-formula. Let $B(i, w, w', a, b)$ be the formula inside the $(\forall i < ||b||^m)$ quantifier of A. Let $A'(k, a, b)$ be the formula where we replace $B(i, w, w', a, b)$ in A with $i \leq k \supset B(i, w, w', a, b)$. R'^1_2 proves $A'(0, a, b)$ because w just needs to contain t_{init} and w' can be 0. Given witnesses for w and w' for $A'(k, a, b)$, then depending on the value of t_{sel}, we can either use t_{rec} or the UC axiom to concatenate on a string to witness $A'(S(k), a, b)$. Hence, using $LLIND$ with speed-up of induction, R'^1_2 proves $A'(||b||^m, a, b)$ which in turn implies A. So R'^1_2 contains $\cup_k\{||id||^k\}$-BDC'. Now suppose R'^1_2 proves some $\hat{\Sigma}^{\mathsf{b}}_1$ formula $C(\mathbf{a})$. Then this proof will involve some finite number of substitution instances of the UC axiom, call these $UC_1, \ldots, UC_m$. So $\hat{R}^1_2$ proves $UC_1, \ldots, UC_m \to C(\vec{a})$ and so by Theorem 1, there is a $\cup_k\{||id||^k\}$-choice defined in $\cup_k\{||\mathrm{id}||^k\}$-$BDC$ function f such that:

$$\cup_k\{||\mathrm{id}||^k\}\text{-}BDC \vdash \psi_f(v, w, a) \wedge WIT_{\wedge UC_j}(w, a) \supset$$
$$WIT_C(\mathrm{OUT}_f(\mathrm{LAST}(v, r_f), a), a).$$

Using the UC axiom, $\cup_k\{||id||^k\}$-BDC' proves that there exists a w witnessing $WIT_{\wedge UC_j}(w, a)$, from which it can prove there is a witness to WIT_C. It then follows that $\cup_k\{||id||^k\}$-BDC' proves C by Lemma 8. □

Lemma 12 *There exist* $\hat{\Sigma}^{\mathsf{b}}_1$*-formulas* $U(E, z, a, b)$ *and* $U_k(E, z, a, b)$*,* $k > 0$*, such that for any term* t *defined as a 4-tuple* $\langle t_{init}(a), t_{sel}(v, i, a), t_{rec}(v, i, a), t_\mu(j, v, a)\rangle$ *the following hold:*

1. *TUC proves there is a code $E_t \in \mathbb{N}$ and bound z_t such that $U(E_t, z_t, a, b) \supset BDC'[|\mathrm{id}|, t_{init}, t_{sel}, t_{rec}, t_\mu, b]$.*

2. *TUC proves there is a code $E_t \in \mathbb{N}$ and bounds z_t, b such that $U_k(E_t, z_t, a, b) \supset BDC'[||id||^k, t_{init}, t_{sel}, t_{rec}, t_\mu, b]$.*

Proof. Both results are proven in the same way, so we show only (2). Let $t^\star_{op} = \min(t_{op}, b)$ for $op = init, sel, rec$. Let $t^\star_\mu$ be defined via cond to be t_μ for $j < |b|$ and be 1 otherwise. Using the $\star$ variants of our original terms will help guarantee that we bound completed computation steps by b appropriately in what follows. Consider the 4-tuple term $t := \langle t^\star_{init}, t^\star_{sel}, t^\star_{rec}, t^\star_\mu \rangle(i, j, v, a, b)$, where (i, j, v, a, b) list all of its parameters. Let E_t denote the code for t and let e_t abbreviate $|E_t|$. In Lemma 10, we would set $z_t = 2^{|i+j+v+a+b|^{C_{\#}(t)+1}}$. As $i, j, v \leq b$, for this lemma we will use $z_t = 2^{|4b+a|^{C_{\#}(t)+1}}$. For this lemma, E_t will almost be the code for the 4-tuple you would get using Lemma 10; however, we will slightly modify what is used for the $t^\star_\mu$ component of the 4-tuple as explained later. Let m be the number of distinct code symbols as given by Lemma 10. Let $t_{\mathrm{term},init}$, $t_{\mathrm{term},sel}$, $t_{\mathrm{term},rec}$, $t_{\mathrm{term},\mu}$ be the terms used in the bounded choice definition of $\mathrm{term}(E, z, a_1, a_2, a_3, a_4, a_5)$. We will rename the variables in t as $a_1 = i$, $a_2 = j$, $a_3 = v$, and $a_4 = a$, $a_5 = b$, we will use i, j, v from now on to refer to the variables in $t_{\mathrm{term},op}$. We define U_k as a conjunction $U'_k \wedge U''_k \wedge U'''_k$ where U'_k, U''_k and U'''_k will all be BDC' axioms. We define U'_k as $BDC'[||id||^k, t'_{init}, t'_{sel}, t'_{rec}, t'_\mu, b']$ where $b' = 2^{|E+z|}$ and using terms t'_{init}, t'_{sel}, t'_{rec}, t'_μ which we shall now describe. Set $u = \lceil |e|/|m| \rceil + 2$. So $u - 1$ is greater than the number of non-NOP operations in a computation of $e = |E|$. Let $t'_{init} = 0$. Using cond, we define t'_{sel}, t'_{rec}, t'_μ by cases as follows:

1. If $i < u - 1$, then

   $$\begin{aligned} t'_{init} &:= t_{\mathrm{term},init}(E, z, 0, 0, 0, a_4, a_5, b'), \\ t'_{sel} &:= 1, \text{ and} \\ t'_{rec} &:= t_{\mathrm{term},rec}(v, i, E, z, 0, 0, 0, a_4, a_5, b') \end{aligned}$$

   We will use these values of i when $E = E_t$, $z = z_t$ to compute the value $t^\star_{init}$, in the first component of the output 4-tuple.

2. If $i = u - 1$, let $out = \mathrm{OUT}_{\mathrm{term}}(\beta_{|b'|}(i, w), E, z, \mathbf{a}, b')$. So if $E = E_t$, $(out)_1$ computes $t^\star_{init}$. For this i, we set $t'_{sel} := 1$ and $t'_{rec} := \langle 0, (out)_1 \rangle$. For higher i's, t'_{rec} will continue to output pairs, the first coordinate

will represent intermediate computations in computing t, the second coordinate will represent the output of the last full computation of t.

3. If $u \leq i < u \cdot ||b'||^k$ and $i \mod u < u - 1$, then let $a_1 = \lfloor i/u \rfloor - 1$. Let v represent a pair, the first coordinate being an intermediate computation, the second, the value of the last full computation of t. Set $a_3 = (v)_2$, $a_4 = a$, $a_5 = b$. Define

   $$\begin{aligned} t'_{sel} &:= 1, \text{ recall we defined } t_{\text{term},sel} \text{ to be 1 in Lemma 10,} \\ t'_{rec} &:= \langle t_{\text{term},rec}((v)_1, i, E, z, \mathbf{a}, b'), (v)_2 \rangle. \end{aligned}$$

   So in these steps when $E = E_t$, intermediate computations of $t^\star_{sel}$ and $t^\star_{rec}$ are computed. It should be noted we will also be computing $t^\star_{init}$ and $t^\star_\mu$ but ignoring them.

4. If $i < u \cdot ||b'||^k$ and $i \mod u = u - 1$, then let v be a pair as above, use a_1, a_3, and *out* for $\lfloor i/u \rfloor - 1$, $(v)_2$, and $\text{OUT}_{\text{term}}(\beta_{|b'|}(i, w), E, z, \mathbf{a}, b')$ respectively. Let $a_4 = a$, $a_5 = b$. So when $E = E_t$, $z = z_t$, $(out)_2$ would be the value of $t^\star_{sel}(a_3, a_1, a_4, a_5)$ and $(out)_3$ would be $t^\star_{rec}(a_3, a_1, a_4, a_5)$. Define $t'_{sel} := (out)_2$ and $t'_{rec} := (out)_3$. To handle the case where $(out)_2 = 0$, consider the open formula

   $$A := (j)_1 = 0 \wedge t^\star_\mu((j)_2, a_3, a_4) > 0$$

   This formula is true when there is an ordered pair whose first coordinate is 0 and whose second coordinate makes t_μ nonzero. If a sharply bounded number makes t_μ nonzero, then this pair is sharply bounded too (albeit with slightly bigger bound). Define t'_μ to be $K_{\neg A}$. The computation of t'_μ is handled by the TERMCOMP clause of the BDC' axiom using a separate witness string w', the result of the computation though is $\beta_{|b'|}(i + 1, w)$ and in this case would be a pair $\langle 0, j' \rangle$ such that $t_\mu(j', a_3, a_4) > 0$. Recall earlier, we mentioned we would slightly tweak the code E_t for t. What we meant was, when giving the code E_t for t, we use t'_μ rather than $t^\star_\mu$ in the 4-tuple.

5. If $i \geq u \cdot ||b'||^k$, we don't want the witness strings w and w' to contain any additional information. To ensure this we set $t'_{sel} = 1$, $t'_{rec} = 0$, and $t'_\mu = 0$.

We note when $E = E_t$, $z = z_t$

$$u \cdot ||b'||^k = (\lceil |e_t|/|m| \rceil + 2)||b'||^k < |e_t| \cdot ||b'||^k = |e_t||E_t + z_t|$$

so all cases will apply in $U'_k = BDC'[||id||^k, t'_{init}, t'_{sel}, t'_{rec}, t'_\mu, 2^{|E_t+z_t|}]$. Let ψ_{U_k} be the $\hat{\Pi}^{\mathsf{b}}_0$-subformula of this axiom and let ψ_t be the $\hat{\Pi}^{\mathsf{b}}_0$-subformula corresponding to $BDC'[||id||^k, t_{init}, t_{sel}, t_{rec}, t_\mu, b]$. Given a witness w_1 to the outer existential of U'_k and a witness w_2 to the outer existential of

$$BDC'[||id||^k, t_{init}, t_{sel}, t_{rec}, t_\mu, b],$$

TUC can use length induction to prove $\beta_{|b'|}((i+1)\cdot u-1, w_1) = \beta_{|b|}(i+1, w_2)$. By itself, this does not prove that U'_k implies a witness w_2 for ψ_t. However, we can define $t''_{init} := 0$, $t''_{sel} := t''_\mu := 1$ and define t''_{rec} to be the concatenation of the second coordinate from the $(i+1)\cdot u - 1$th block of $|b'|$ bits of w using a block size of $|b|$ onto whatever was the previous value. If we define $U''_k = BDC'[||id||^k, t''_{init}, t''_{sel}, t''_{rec}, t''_\mu, b']$, this second axiom would allow us to prove the existence of w_2 from w_1. We can handle the conversion problem for the second existential of $BDC'[||id||^k, t_{init}, t_{sel}, t_{rec}, t_\mu, b]$ in the same fashion using one more BDC' axiom U'''_k completing the proof. □

Lemma 13 *S^1_2 proves the formula $U(E, z, a, b)$ and for each $k \geq 1$, R'^1_2 proves the formula $U_k(E, z, a, b)$.*

Proof. By the proof of Lemma 12, U is a conjunction of $\{|\mathrm{id}|\}$-BDC' axioms so provable in $\{|\mathrm{id}|\}$-BDC' and, hence, by Lemma 3 provable in S^1_2. Similarly, the lemma also shows U_k is conjunction of $\{||\mathrm{id}||^k\}$-BDC' axioms and, hence, provable in $\{||\mathrm{id}||^k\}$-BDC' and R'^1_2. □

Theorem 3

1. *$\forall\hat{\Sigma}^{\mathsf{b}}_1(S^1_2)$ can be finitely axiomatized as TUC+U.*
2. *$\forall\hat{\Sigma}^{\mathsf{b}}_1(R'^1_2)$ can be axiomatized as TUC+$\cup_k U_k$.*

Proof. This follows from Remark 1, Theorem 2, Lemma 12, and Lemma 13. □

6 Towards Separations

In view of Theorem 3, we know that if $\hat{R}^1_2 = S^1_2$, then $\forall\hat{\Sigma}^{\mathsf{b}}_1(\hat{R}^1_2)$ and $\forall\hat{\Sigma}^{\mathsf{b}}_1(R'^1_2)$ will be finitely axiomatized. It also follows that if we could show that for all k, there is a $k' > k$ such that $\{||id||^k\}$-$BDC' \subsetneq \{||id||^{k'}\}$-$BDC'$, then $\forall\hat{\Sigma}^{\mathsf{b}}_1(R'^1_2)$ would not be finitely axiomatized and $\hat{R}^1_2 \subseteq R'^1_2 \subsetneq S^1_2$. If we define $x\#_3 y := 2^{|x|\#|y|}$ and add axioms for this symbol to our language, we obtain theories $\hat{R}^1_3$, R'^1_3, S^1_3, and $\{||id||^k\}$-BDC'_3. The proof of Theorem 3 generalizes to this setting by making a few minor changes: First, let $C_{\#_3}(t)$ be the number of occurrences of $\#_3$ in term t. In Lemma 10, we would set $z_t = 2^{2^{||\sum_i a_i||^{C_{\#_3}(t)+1}}}$ to handle the higher growth rates that might occur in intermediate computations, we would also add a clause to t_{rec} to handle $\#_3$. The changed value of z_t would then be propagated through the remaining lemmas and theorems of the section and, otherwise, there would be no other substantive changes. In this language, however, there is a term $t(x)$ such $||t(x)|| = ||x||^k$, and so $\{||id||\}$-$BDC'_3 = \cup_k\{||id||^k\}$-$BDC'_3$ and we have:

Theorem 4 *$\forall\hat{\Sigma}^{\mathsf{b}}_1(R'^1_3)$ can be finitely axiomatized as TUC_3+$U_{1,3}$.*

Here TUC_3 and $U_{1,3}$ are the generalizations of the theory TUC and the axiom U_1 from the previous section to handle $\#_3$. That is, TUC_3 is $EBASIC_3$+BITMIN+UC and $U_{1,3}$ is obtained from U_1 by adding adding another clause in Lemma 10 to handle $\#_3$. In the introduction, we mentioned it is hard to express the sharply bounded μ-operator in a way that will both work in our witnessing arguments and in our universal predicates in connection with the R'^1_3 above. This problem was dealt with in our results without $\#_3$, and hence in our results with $\#_3$, by using the BDC' axioms in which μ-computation steps are expanded rather than the BDC axioms.

The result above highlights that if separations exists between $\{||id||^k\}$-BDC' and $\{||id||^{k'}\}$-BDC' for $k' > k$ that the proof will be sensitive to the choice of base functions.

On the other hand, our normal forms and predicate U_k are sufficient to give us some limited diagonalization results. We generalize the notion of the smash complexity to Corollary 2 normal form predicates A, by defining the $C_\#(A)$ to be the sum of the smash complexities of its defining terms r^+, t_{sel}, t_{rec}, and t_μ and the power of $||id||^m$ used in the normal form.

Theorem 5 *For any $k > 0$, there is a $\hat{\Delta}^b_1$-predicate in R'^1_2, which if it is a $\hat{\Delta}^b_1$-predicate in $\hat{R}^1_2$, then it is a $\hat{\Delta}^b_1$-predicate in $\hat{R}^1_2$ of smash complexity greater than k.*

Proof. Let $C(a)$ be a $\hat{\Delta}^b_1$-predicate in $\hat{R}^1_2$ of smash complexity k and let r, t_{init}, t_{sel}, t_{rec}, and t_μ be the terms of its normal form. Let E_t be the code for the 4-tuple computed by the terms other than r where we modify them to compute $\min(t_{op}, r)$ for $op = init, sel, rec$ and for $op = \mu$ to compute t_μ for $j < |r^+|$ and 1 otherwise. By Lemma 5, Lemma 12 and the proof of Theorem 2, $U_k(E_t, z_t, a, r^+(a))$ implies $BDC[||id||^k, t_{init}, t_{sel}, t_{rec}, t_\mu, r]$ where $e_t =$

E_t and $z_t = 2^{|4r^+(a)+a|^{C_\#(t)+1}} = 2^{|4r^+(a)+a|^{k+1}}$. Since $C_\#(r) \leq k$, by at most tweaking E_t slightly as per Lemma 4, we can replace r with $2^{|a|^{k+1}} \geq a$ and use $z_t = 2^{|a|^{(k+1)^2}+5} \geq 2^{|4r^+(a)+a|^{k+1}}$ in U_k and still imply $BDC[||id||^k, t_{init}, t_{sel}, t_{rec}, t_\mu, r]$. This same choice of z_t can be used for any formula $C(a)$ of smash complexity k. So we have a single formula

$$U(E,a) := U_k(E, 2^{|a|^{(k+1)^2}+5}, a, 2^{|a|^{k+1}}),$$

such that for any smash complexity k formula $C(a)$, there is a term t such that $U(E_t, a)$ implies the BDC axiom corresponding to the normal form of $C(a)$. Moreover, a witness w to the outer existential of the U'_k component of the U_k axiom above has blocks corresponding to each of the blocks in the BDC axiom, and the 0th bit of w in the last block would be 1 only if the witness to BDC's axiom's existential has a last block with 0th bit equal to 1. Let $A(E, a, c)$ be the formula which has $c = 1$ if bit 0 of the last block of U'_k is 0 and vice-versa. R'^1_2 proves $\exists! y \leq 1 A(E, a, c)$ and that $A(E, a, 1) \Leftrightarrow \neg A(E, a, 0)$, so $A(E, a, 1)$ is $\hat{\Delta}^b_1$ in R'^1_2. Our reasoning above shows for any $C(a)$ of smash complexity of k is equivalent to $\neg A(E_t, a, 1)$ for some term t. If $A(E, a, 1)$ had smash complexity k, then we could find a code for it, E_{t_A}, and the truth or falsity of $A(E_{t_A}, E_{t_A}, 1)$ would be contradictorily defined. □

References

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

[2] S. Boughattas and L. A. Kołodziejczyk. The strength of sharply bounded induction requires MSP. *Annals of Pure and Applied Logic.* Vol. 161. 2010. pp. 504-510.

[3] S. Boughattas and J.P. Ressayre. Bootstrapping I. *Annals of Pure and Applied Logic.* Vol. 161. 2010. pp. 511-533.

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

[5] 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.

[6] S. Cook and P. Nguyen. *Logical Foundations of Proof Complexity.* Perspectives in Logic, Cambridge University Press. 2010.

[7] 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.

[8] 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.

[9] 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.

[10] L. Fortnow. Time-space tradeoffs for satisfiability. *Journal of Computer and System Sciences.* Vol. 60. Iss. 2. Apr. 2000. pp. 337–253.

[11] M. Garlík. Construction of models of bounded arithmetic by restricted reduced powers. To appear.

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

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

[14] J. KrajíčekP. Pudlák. Quantified propositional calculi and fragments of bounded arithmetic. *Zeitschr. f. Math. Logic und Grundlagen d. Math..* Vol. 36. 1990. pp. 29–46.

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

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

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

[18] J. Johannsen. A model-theoretic property of sharply bounded formulae, with some applications. *Mathematical Logic Quarterly.* Vol. 44. No. 2. pp. 205–215, 1998.

[19] 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.

[20] J. Johannsen and C. Pollett. On the Δ^b_1-bit-comprehension rule. In Sam Buss, Petr Hájek, and Pavel Pudlák, eds., *Logic Colloquium '98*. ASL Lecture Notes in Logic. 2000. pp. 262–279.

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

[22] C. Pollett. A Propositional Proof System For R^i_2. In P. W. Beame, S. R. Buss eds., *Proof Complexity and Feasible Arithmetics*. DIMACS Series in Math. and Theoretical Computer Science. Vol. 39. 1998. pp. 253–278.

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

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