A Note on Bootstrapping Intuitionistic Bounded Arithmetic

SAMUEL R. BUSS*

Department of Mathematics
University of California, San Diego†

Abstract

This paper, firstly, discusses the relationship between Buss's definition and Cook and Urquhart's definition of BASIC axioms and of IS_2^1. The two definitions of BASIC axioms are not equivalent; however, each intuitionistically implies the law of the excluded middle for quantifier-free formulas. There is an elementary proof that the definitions of IS_2^1 are equivalent which is not based on realizability or functional interpretations.

Secondly, it is shown that any negated positive consequence of S_2^1 is also a theorem of IS_2^1. Some possible additional axioms for IS_2^1 are investigated.

1. Introduction and Definitions

In [1, 2] we introduced a hierarchy of formal theories of arithmetic called collectively Bounded Arithmetic; these theories were shown to have a very close connection to the computational complexity of polynomial time, the levels of the polynomial hierarchy, polynomial space and exponential time. Of particular interest is theory called S_2^1 which has proof-theoretic strength closely linked to polynomial time computability. Later we introduced an intuitionistic version of this theory called IS_2^1 and proved a feasibility result for this theory based on a realizability interpretation using a notion of

*Supported in part by NSF Grants DMS-8701828 and DMS-8902480.
†E-mail address: sbuss@ucsd.edu.

polynomial time functionals [3]. Recently, Cook and Urquhart [7, 6] have given an alternative definition of IS_2^1. They also gave an improved treatment of polynomial time functionals, introduced new powerful theories using lambda calculus, strengthened the feasibility results for IS_2^1, and reproved the 'main theorem' for S_2^1 as a corollary of their results for IS_2^1.

The work in the first part of this paper was motivated by an desire to clarify the relationship between these two definitions of IS_2^1; more precisely, while reading Cook and Urquhart's paper I tried to verify their assertion that the bootstrapping argument for S_2^1 could be followed to bootstrap their version of IS_2^1. As it turned out, there is a general reason why their assertion in true (Corollary 12) and it was not necessary to trace the bootstrapping argument step-by-step to formalize it in IS_2^1. We show below that the BASIC axioms of Cook and Urquhart are not equivalent to the BASIC axioms of Buss; however, we also give an elementary proof that the different definitions of IS_2^1 are equivalent (a fact already proved by Cook and Urquhart based on their Dialectica interpretation).

In the last part of this paper we show that S_2^1 is conservative over IS_2^1 in the following sense: If A is a positive formula and B is an $H\Sigma_1^b$ formula and if $S_2^1 \vdash A \supset B$ then IS_2^1 also proves $A \supset B$. This generalises the fact that S_2^1 and IS_2^1 have the same $H\Sigma_1^b$-definable functions. As a corollary, if A is a positive formula and $S_2^1 \vdash \neg A$ then $IS_2^1 \vdash \neg A$. An intuitionistic theory IS_2^{1+} which is apparently stronger that IS_2^1 is defined by allowing PIND on formulas of the form $A(b) \vee B$ where $A \in H\Sigma_1^b$ and B is an arbitrary formula in which the induction variable b does not appear. The theory IS_2^{1+} is shown in [5] is shown to be the intuitionistic theory which is valid in every S_2^1-normal Kripke model; we prove here a proof-theoretic theorem needed in [5].

We presume familiarity with the first part of chapter 2 of Buss [2], with the definitions of IS_2^1 in Buss [3] and in section 1 of Cook-Urquhart [7], and with the sequent calculus. The realizability and functional interpretations of IS_2^1 are not needed.

Buss [2] and Cook-Urquhart [7] use a finite set of BASIC axioms which form a base theory to which induction axioms are later added. However, the two definitions of BASIC are different; for reference, we list all 32 BASIC axioms of Buss and all 21 BASIC axioms of Cook and Urquhart in a table below.

We briefly review some definitions; see [2, 3, 7] for the full definitions. A *bounded* quantifier is one of the form $(Qx \leq t)$ and it is *sharply bounded* if t is of the form $|s|$. A *(sharply) bounded formula* is one in which every quantifier is (sharply) bounded. The class $\Sigma_0^b = \Pi_0^b = \Delta_0^b$ is the set of sharply bounded formulas. The classes Σ_i^b and Π_i^b are sets of bounded formulas defined by counting alternations of bounded quantifiers, ignoring the sharply bounded quantifiers. The class $H\Sigma_1^b$ of *hereditarily* Σ_1^b formulas is the set of formulas A such that each subformula of A is Σ_1^b. A *positive* formula is one that contains no implication or negation signs. A formula is Σ_1^{b+} if and only if it is positive and is Σ_1^b. Clearly every Σ_1^{b+}-formula is $H\Sigma_1^b$.

We now define two variants of IS_2^1, denoted IS_2^1B and IS_2^1CU in this paper. We shall actually prove they are equivalent and hence the preferred name for either theory is just IS_2^1. IS_2^1B is the theory called IS_2^1 in [3] and called IS_2^1B by Cook-Urquhart [7], whereas IS_2^1CU is the theory called IS_2^1 in [7]. Both theories are formulated with PIND axioms which are (universal closures of) axioms of the form

$$A(0) \land (\forall x)(A(\lfloor \tfrac{1}{2}x \rfloor) \supset A(x)) \supset (\forall x)A(x).$$

Definition The theory IS_2^1B is the intuitionistic theory which has axioms

(a) All formulas of the form

$$B_1 \land B_2 \land \cdots \land B_k \supset B_{k+1}$$

with each B_i a $H\Sigma_1^b$-formula, which are consequences of the (classical) theory S_2^1,

(b) The PIND axioms for each $H\Sigma_1^b$ formula A.

Buss's BASIC axioms	Cook-Urquhart's BASIC axioms
(B-1) $y \leq x \supset y \leq Sx$	
(B-2) $\neg x = Sx$	(CU-1) $x = Sx \supset A$
(B-3) $0 \leq x$	(CU-2) $0 \leq x$
(B-4) $x \leq y \wedge \neg x = y \leftrightarrow Sx \leq y$	(CU-3) $x \leq y \supset (x = y \vee Sx \leq y)$
(B-5) $\neg x = 0 \supset \neg 2x = 0$	
(B-6) $y \leq x \vee x \leq y$	(CU-6) $y \leq x \vee x \leq y$
(B-7) $x \leq y \wedge y \leq x \supset x = y$	(CU-5) $x \leq y \wedge y \leq x \supset x = y$
(B-8) $x \leq y \wedge y \leq z \supset x \leq z$	(CU-4) $x \leq y \wedge y \leq z \supset x \leq z$
(B-9) $\lvert 0\rvert = 0$	(CU-7) $\lvert 0\rvert = 0$
(B-10) $\neg x = 0 \supset \lvert 2x\rvert = S(\lvert x\rvert)\wedge$	(CU-8) $1 \leq x \supset \lvert 2x\rvert = S(\lvert x\rvert)$
$\lvert S(2x)\rvert = S(\lvert x\rvert)$	(CU-9) $\lvert S(2x)\rvert = S(\lvert x\rvert)$
(B-11) $\lvert 1\rvert = 1$	
(B-12) $x \leq y \supset \lvert x\rvert \leq \lvert y\rvert$	(CU-10) $x \leq y \supset \lvert x\rvert \leq \lvert y\rvert$
(B-13) $\lvert x\#y\rvert = S(\lvert x\rvert \cdot \lvert y\rvert)$	(CU-11) $\lvert x\#y\rvert = S(\lvert x\rvert \cdot \lvert y\rvert)$
(B-14) $0\#y = 1$	(CU-12) $1\#1 = 2$
(B-15) $\neg x = 0 \supset 1\#(2x) = 2(1\#x)\wedge$	
$1\#(S(2x)) = 2(1\#x)$	
(B-16) $x\#y = y\#x$	(CU-13) $x\#y = y\#x$
(B-17) $\lvert x\rvert = \lvert y\rvert \supset x\#z = y\#z$	
(B-18) $\lvert x\rvert = \lvert u\rvert + \lvert v\rvert \supset$	(CU-14) $\lvert x\rvert = \lvert u\rvert + \lvert v\rvert \supset$
$x\#y = (u\#y)\cdot(v\#y)$	$x\#y = (u\#y)\cdot(v\#y)$
(B-19) $x \leq x + y$	
(B-20) $x \leq y \wedge \neg x = y \supset$	
$S(2x) \leq 2y \wedge \neg S(2x) = 2y$	
(B-21) $x + y = y + x$	
(B-22) $x + 0 = x$	(CU-15) $x + 0 = x$
(B-23) $x + Sy = S(x + y)$	(CU-16) $x + Sy = S(x + y)$
(B-24) $(x + y) + z = x + (y + z)$	(CU-17) $(x + y) + z = x + (y + z)$
(B-25) $x + y \leq x + z \leftrightarrow y \leq z$	(CU-18) $x + y \leq x + z \leftrightarrow y \leq z$
(B-26) $x \cdot 0 = 0$	(CU-19) $x \cdot 1 = x$
(B-27) $x \cdot (Sy) = (x \cdot y) + x$	
(B-28) $x \cdot y = y \cdot x$	
(B-29) $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$	(CU-20) $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
(B-30) $1 \leq x \supset (x \cdot y \leq x \cdot z \leftrightarrow y \leq z)$	
(B-31) $\neg x = 0 \supset \lvert x\rvert = S(\lvert\lfloor\frac{1}{2}x\rfloor\rvert)$	(CU-21) $x = (\lfloor\frac{1}{2}x\rfloor + \lfloor\frac{1}{2}x\rfloor)\vee$
(B-32) $x = \lfloor\frac{1}{2}y\rfloor \leftrightarrow (2x = y \vee S(2x) = y)$	$x = S(\lfloor\frac{1}{2}x\rfloor + \lfloor\frac{1}{2}x\rfloor)$

Definition The theory IS^1_2CU is the intuitionistic theory which has axioms

(a) The BASIC axioms of Cook and Urquhart,

(b) The PIND axioms for each Σ^{b+}_1 formula A.

Similar definitions can be formulated for intuitionistic theories IS^i_2; however, we shall only consider the case $i = 0$ since the complications in 'bootstrapping' apply mainly to BASIC and IS^1_2. V. Harnik [8] has generalized Cook and Urquhart's work to IS^i_2 for $i > 1$.

I wish to thank Stephen Cook and Alasdair Urquhart for making their unpublished notes on bootstrapping IS^1_2CU available to me.

2. Consequences of the BASIC Axioms

We shall show that both formulations of the BASIC axioms imply the law of the excluded middle for atomic formulas. However, the two formulations are **not** equivalent: Buss's BASIC axioms imply Cook-Urquhart's BASIC axioms but not vice-versa. For the rest of this paper we let BBASIC denote the 32 BASIC axioms of Buss and CUBASIC denote the 21 BASIC axioms of Cook and Urquhart.

Proposition 1 *The following formulas are intuitionistic consequences of both BBASIC and CUBASIC:*

(a) $x \le x$

(b) $x \le Sx$

(c) $\neg Sx \le x$

(d) $Sx \le y \supset \neg y \le x$

(e) $0 \ne Sx$

We are adopting the convention that a formula with free variables is a consequence of a theory iff its generalization (universal closure) is. So "$x = x$" means "$(\forall x)(x = x)$", etc.

Proof Formula (a) follows from (B-6) or (CU-6). Formula (b) follows from (a) and (B-1), while (B-1) follows from (CU-15), (CU-16), (CU-18) and (CU-2). Formula (c) follows from (b), (B-7) and (B-2) or, equivalently, from (b), (CU-5) and (CU-1). Formula (d) follows from (c) and either (B-8) or (CU-4). Finally (e) follows from (a), (b), (B-8) or (CU-4), and (c). $\square$

Theorem 2 *(Cook-Urquhart [7]) CUBASIC intuitionistically implies the law of the excluded middle for atomic formulas.*

Proof The axiom (CU-6) states that $x \leq y \vee y \leq x$; this plus (CU-3) intuitionistically implies $x = y \vee Sx \leq y \vee Sy \leq x$. Now formulas (d) and (a) imply $x = y \vee \neg x = y$. Also from (CU-6) and (CU-3) we get $y \leq x \vee x = y \vee Sx \leq y$; so by (d) and (a) and equality axioms, $y \leq x \vee \neg y \leq x$. $\square$

The BBASIC axioms were originally formulated for a classical theory so no attempt was made to ensure that they were appropriate for intuitionistic theories; however, the next theorem shows that the BBASIC axioms do indeed imply the law of the excluded middle for atomic formulas.

Theorem 3 *BBASIC intuitionistically implies the law of the excluded middle for atomic formulas.*

Proof We prove a series of claims:

Claim (B-i): BBASIC intuitionistically implies $x \leq y \leftrightarrow Sx \leq Sy$ and $x = y \leftrightarrow Sx = Sy$.

Proof: Note that (B-22), (B-23) and (B-21) imply that $S0 + x = Sx$. Now $x \leq y \leftrightarrow Sx \leq Sy$ follows from (B-25). From this, (B-6) and (B-7) imply $x = y \leftrightarrow Sx = Sy$.

Claim (B-ii): BBASIC intuitionistically implies $x + x \le y + y \supset x \le y$.

Proof: It is easy to prove that $x + x = 2 \cdot x$ and $y + y = 2 \cdot y$ using (B-26)-(B-28). Now the claim follows from axiom (B-30) since by (b) of Proposition 1, $1 \le 2$.

Claim (B-iii): BBASIC intuitionistically implies $x + x \le y + y + 1 \supset x \le y$.

Proof: Now we need to show that $2 \cdot x \le 2 \cdot y + 1 \supset x \le y$. Let's argue informally intuitionistically from BBASIC. By (B-6) either $Sy \le x$ or $x \le Sy$ or both. If $Sy \le x$ then $Sy + Sy \le x + x \le y + y + 1$ and hence $S(y + y + 1) \le y + y + 1$ which contradicts formula (c) of Proposition 1. So $x \le Sy$. (This a valid intuitionistic use of proof-by-contradiction.) Now $x \ne Sy$, else $x = Sy$ implies $Sy \le x$ which we just showed implied $S(y + y + 1) \le y + y + 1$. (Again, it is intuitionistically valid to prove $x \ne Sy$ by assuming $x = Sy$ and obtaining a contradiction; however, it would not be valid to prove $x = Sy$ by deriving a contradiction from $x \ne Sy$.) Thus $x \le Sy \wedge x \ne Sy$ so $Sx \le Sy$ by (B-4) and thus $x \le y$ by (B-*i*).

Claim (B-iv): BBASIC intuitionistically implies

$$y \le x \wedge x \le Sy \supset x = y \vee x = Sy.$$

Proof: To prove this, note that axiom (B-32) implies that either $y = \lfloor \frac{1}{2} y \rfloor + \lfloor \frac{1}{2} y \rfloor$ or $y = S(\lfloor \frac{1}{2} y \rfloor + \lfloor \frac{1}{2} y \rfloor)$. Let's first assume that the first case holds. Another use of axiom (B-32) shows that $\lfloor \frac{1}{2}(Sy) \rfloor = \lfloor \frac{1}{2} y \rfloor$. Now we further split into two subcases depending on whether $x = \lfloor \frac{1}{2} x \rfloor + \lfloor \frac{1}{2} x \rfloor$ or $x = \lfloor \frac{1}{2} x \rfloor + \lfloor \frac{1}{2} x \rfloor + 1$; one of these subcases holds by yet another use of (B-32). In either subcase we can use Claim (B-*ii*) or (B-*iii*), respectively, to show that $\lfloor \frac{1}{2} y \rfloor \le \lfloor \frac{1}{2} x \rfloor$. A similar argument shows that $\lfloor \frac{1}{2} x \rfloor \le \lfloor \frac{1}{2} Sy \rfloor$. Hence $\lfloor \frac{1}{2} x \rfloor = \lfloor \frac{1}{2} y \rfloor$. Now by axiom (B-32) again, $x = y \vee x = Sy$.

For the second case, assume that $y = S(\lfloor \frac{1}{2} y \rfloor + \lfloor \frac{1}{2} y \rfloor)$. Then $Sy = S\lfloor \frac{1}{2} y \rfloor + S\lfloor \frac{1}{2} y \rfloor$ so $S\lfloor \frac{1}{2} y \rfloor = \lfloor \frac{1}{2}(Sy) \rfloor$. And $Sy \le Sx \le S(Sy)$. We can now use the first case to see that $Sx = Sy \vee Sx = S(Sy)$, thus by (B-i), $x = y \vee x = Sy$.

Claim (B-v): BBASIC intuitionistically implies $x \le y \vee \neg x \le y$.

Proof: By (B-6) twice, $x \le y \vee Sy \le x \vee (y \le x \wedge x \le Sy)$. By (B-$iv$), this implies $x \le y \vee Sy \le x \vee x = y \vee x = Sy$; so $x \le y \vee \neg x \le y$ by (a) and (d) of Proposition 1.

Claim (B-vi): BBASIC intuitionistically implies $x = y \vee x \ne y$.

Proof: By claim (B-v) twice, $(x \le y \wedge y \le x) \vee \neg x \le y \vee \neg y \le x$ and thus by axiom (B-7) and by (a) of Proposition 1, $x = y \vee x \ne y$.
Q.E.D. Theorem 3

Theorem 4 *BBASIC intuitionistically implies CUBASIC.*

Proof Because BBASIC and CUBASIC are (generalizations of) atomic formulas and because BBASIC intuitionistically implies the law of the excluded middle, it is actually sufficient to show that BBASIC classically implies CUBASIC. The only CUBASIC axioms that do not immediately follow from BBASIC are (CU-3) and (CU-12). (CU-3) is a classical consequence of (B-4) and thus follows by the law of the excluded middle for the formula $x = y$. (CU-12) is the axiom $1\#1 = 2$. To derive this, use (B-15) with $x = 1$ to show $1\#2 = 2 \cdot (1\#1)$ then use (B-18) with $x = 2$ and $u = v = y = 1$ to derive $2\#1 = (1\#1) \cdot (1\#1)$. Now by use of (B-16) and (B-28), $(1\#1)\#(1\#1) = (1\#1) \cdot 2$ and by using (B-30) twice, $1\#1 = 2$ is derived (note that $1\#1 \ne 0$ by (B-13), (B-11), and (B-12)). $\Box$

The converse to Theorem 4 does not hold; before we prove this we show that adding three additional axioms to CUBASIC is sufficient to make it equivalent to BBASIC.

Theorem 5 *Let* $\mathrm{CUBASIC}^+$ *be the the axioms of CUBASIC plus the axioms (B-21), (B-28) and (B-30). Then* $\mathrm{CUBASIC}^+$ *intuitionistically implies the*

BBASIC axioms.

Proof (B-1) follows from formula (b) of Proposition 1 and (CU-4). (B-4) is an immediate consequence of (CU-3) and (b) and (c) of Proposition 1. To show $\text{CUBASIC}^{+} \models \text{(B-5)}$, first note that $x \neq 0 \supset 1 \leq x$ by (CU-2) and (CU-3); hence $x \neq 0 \supset 0 \neq |2x|$ by (CU-8) and (e) of Proposition 1 and finally, by (CU-7), $x \neq 0 \supset 2x \neq 0$. Axiom (B-19) follows from (CU-15), (CU-18) and (CU-2). (B-10) and (B-11) are consequences of (CU-8) and (CU-9).

By (CU-11) and (e) of Proposition 1, $x\#y \neq 0$ is a consequence of CUBASIC^{+}. By (CU-14) with $x = u = v = 0$, $0\#y = (0\#y) \cdot (0\#y)$ and by (CU-19) and (B-30), $0\#y = 1$, which is (B-14). It is straightforward to derive (B-15) from (B-10), (B-11), (CU-12) and (CU-14). Also, (B-17) is implied by (CU-14) and the fact that $|0| = 0$ and $0\#z = 1$.

To derive (B-20), first use (B-28) and (CU-19) and (CU-20) to show that $S(2x) = x + x + 1$. Now, if $x \leq y \wedge x \neq y$ then by (B-4), $Sx \leq y$. And by (B-28) and (B-30), $2(Sx) \leq 2y$. Thus $S(2x) < 2(Sx) \leq 2y$.

(B-26) follows readily from (CU-19) and (CU-20); (B-27) is an immediate consequence of (CU-20) with the aid of $x \cdot 1 = x$ and $Sy = y + 1$. Finally to derive (B-32) from (CU-21) it will suffice to show that $x + x = y + y \supset x = y$. Suppose that $x + x = y + y$ and $x \neq y$; then w.l.o.g. $Sx \leq y$ and so (B-20) yields a contradiction. And (B-31) follows from (B-32), (CU-8) and (CU-9). $\square$

Theorem 6 *The CUBASIC axioms do not (classically) imply the BBASIC axioms.*

Proof We shall prove this by constructing a model of CUBASIC in which multiplication is not commutative, violating axiom (B-28). Let $\mathcal{M}$ be a model of S_2^1 in which exponentiation is not total and in which the function $x \mapsto 2^{|x|\#|x|}$ is total. Let M be the universe of $\mathcal{M}$. We shall say that $m \in M$ is *large* if and only if there is no $n \in M$ with $m = |n|$, i.e., m is large if and only if 2^m does not exist. An object is *small* if and only if it is not large. Note that the small elements are closed under $\#$ since $x \mapsto 2^{|x|\#|x|}$ is total. Let $\mathcal{N}$

be the substructure of $\mathcal{M}$ with universe N the set of objects that can be expressed as $a \cdot 2^b + c$ with b and c small and with 2^b large. Clearly $\mathcal{N}$ is well-defined as a substructure since N is closed under all the functions of CUBASIC. Since CUBASIC consists of universal formulas, $\mathcal{N} \models$ CUBASIC (since $\mathcal{M}$ is a model of CUBASIC).

Pick some fixed large $a_0 \in N$ which is not a power of two. Form a structure $\mathcal{N}^*$ from $\mathcal{N}$ with the same universe as $\mathcal{N}$ and with all functions and relations, other than multiplication, unchanged. For multiplication, any product of the form $a_0 \cdot (a \cdot 2^b + c)$ with c small and 2^b large is defined to be equal to $a_0 \cdot c$. Any other product $a \cdot b$ with $a \neq a_0$ is equal to its product in $\mathcal{N}$ (and in $\mathcal{M}$). It is easy to see that $\mathcal{N}^*$ still satisfies all the CUBASIC axioms: since a_0 is not small, (CU-11) still holds, and since a_0 is not a power of two, (CU-14) is unaffected. Obviously (CU-19) and (CU-20) hold in $\mathcal{N}^*$. But multiplication is not commutative in $\mathcal{N}^*$ so $\mathcal{N}$ is not a model of BBASIC. □

Another way that multiplication could have been defined in $\mathcal{N}^*$ would be to let $a_0 \cdot (a \cdot 2^b + c)$ be equal to $m \cdot a \cdot 2^b + a_0 \cdot c$ for some arbitrary m in M.

3. Equivalence of the Definitions of IS_2^1

Next we show that the two definitions IS_2^1CU and IS_2^1B of IS_2^1 are equivalent. There are three steps necessary for this: first, we must show that IS_2^1CU implies all the BBASIC axioms; second, that IS_2^1CU implies the $H\Sigma_1^b$-PIND axioms; and third, that IS_2^1CU implies all the axioms of IS_2^1B. All three of these steps are done by Cook and Urquhart in [7]; our new contribution here is to give a simple proof of the third step that does not depend on the realizability or functional interpretations of IS_2^1. Our simple proof for the third step allows one to reduce the bootstrapping of IS_2^1CU to the bootstrapping of S_2^1.

Theorem 7 *(Cook-Urquhart [7]) $IS_2^1CU \models BBASIC$. In fact, PIND on open formulas is sufficient to derive the BBASIC axioms from the CUBASIC axioms.*

Proof (Sketch) By Theorem 5 it will suffice to show that (B-21), (B-28) and

(B-30) are consequences of IS_2^1. We sketch the steps in the proof, leaving the details to the reader: (This derivation is only slightly different from Cook and Urquhart's original unpublished proof.)

1. Prove $0+x=x$ by PIND on x.
2. Prove $1+x=x+1$ by PIND on x.
3. Prove $x+y=y+x$ by PIND on x. This is (B-21).
4. Prove $x \cdot 0 = 0$. No PIND necessary, derive the equality $x+0 = x + x \cdot 0$ and use (CU-18).
5. Prove $0 \cdot x = 0$ by PIND on x.
6. Prove $(y+y) \cdot x = y \cdot x + y \cdot x$ by PIND on x.
7. Prove $(y+y+1) \cdot x = y \cdot x + y \cdot x + x$ by PIND on x.
8. Prove $x \cdot y = y \cdot x$ by PIND on x. This is (B-28).
9. Prove $x+x \le y+y \leftrightarrow x \le y$ without use of induction. This follows from the fact that if $x<y$ then $x+x<x+y=y+x<y+y$ which can be derived from (CU-18).
10. Prove $1 \le x \supset (x \cdot y \le x \cdot z \leftrightarrow y \le z)$ by PIND on x. This is (B-30).

$\square$

The next theorem is relatively simple to prove; see Lemma 1.3 through Theorem 1.7 of [7].

Theorem 8 *(Cook-Urquhart [7])*

(1) *IS_2^1CU proves $A \vee \neg A$ for A a Σ_0^b-formula.*

(2) *IS_2^1CU proves that every $H\Sigma_1^b$-formula is equivalent to a Σ_1^{b+}-formula.*

(3) *IS_2^1CU implies the $H\Sigma_1^b$-PIND axioms.*

The next lemma will aid in the proof that IS_2^1CU proves all the axioms of IS_2^1B.

Lemma 9 *The following are intuitionistically valid:*

(a) $A \supset A \vee B$

(b) $(A \vee C) \wedge (B \vee C) \supset (A \wedge B) \vee C$

(c) $(B \supset A \vee C) \supset (\neg A \wedge B \supset C)$

(d) $(A \vee \neg A) \supset (A \wedge B \supset C) \supset (B \supset \neg A \vee C)$

(e) $(B \supset A \vee C) \wedge (A \wedge B \supset C) \supset (B \supset C)$

(f) $(B \vee \neg B) \supset (B \wedge C \supset A \vee D) \supset (C \supset (B \supset A) \vee D)$

(g) $(C \supset A \vee D) \wedge (C \wedge B \supset D) \supset (C \wedge (A \supset B) \supset D)$

(h) $A(s) \wedge s \leq t \supset (\exists x \leq t)A(x)$

The proof of Lemma 9 is straightforward.

Theorem 10 *(Cook-Urquhart [7]) All axioms of IS_2^1B are consequences of IS_2^1CU.*

A generalization of Theorem 10 is presented in section below.

Proof Recall that S_2^1 is a classical theory of Bounded Arithmetic with the BBASIC axioms and Σ_1^b-PIND rules. We shall show that any sequent of $H\Sigma_1^b$-formulas which is a theorem of S_2^1 is also a consequence of IS_2^1CU. More precisely, if $\Gamma \longrightarrow \Delta$ is a sequent containing only $H\Sigma_1^b$-formulas and is a theorem of S_2^1 then the formula $(\bigwedge \Gamma) \supset (\bigvee \Delta)$ is a consequence of IS_2^1CU. (Frequently intuitionistic logic is formulated in the sequent calculus by restricting succedents to have only one formula; however, it still makes sense to talk about a sequent with more than one succedent formula being a theorem of an intuitionistic system. The way to do this is to think of the formulas in the succedent as being disjoined into a single formula.) By classical prenex operations, any Σ_1^b-formula is equivalent to an $H\Sigma_1^b$-formula so S_2^1 may be equivalently formulated with the $H\Sigma_1^b$-PIND rule instead of Σ_1^b-PIND. Thus if S_2^1 proves a sequent $\Gamma \longrightarrow \Delta$ containing only $H\Sigma_1^b$-formulas, then there is an S_2^1-proof in which every induction formula is a $H\Sigma_1^b$-formula. Now, by free-cut elimination, there is an S_2^1 proof of $\Gamma \longrightarrow \Delta$ such that every formula in the proof is an $H\Sigma_1^b$-formula.

Given an S_2^1 proof of $\Gamma \longrightarrow \Delta$ in which every formula is a $H\Sigma_1^b$-formula, we prove that every sequent in the proof is a theorem of IS_2^1CU by beginning at the initial sequents (axioms) and proceeding inductively on the number of inferences needed to derive a sequent. The initial sequents are logical axioms, equality axioms or BBASIC formulas and are consequences of IS_2^1CU by Theorem 7. For the induction step, suppose for example that a $\neg$*:right* inference

$$\frac{A, \Pi \longrightarrow \Lambda}{\Pi \longrightarrow \Lambda, \neg A}$$

has its upper sequent a theorem of IS_2^1CU; then since both A and $\neg A$ are $H\Sigma_1^b$-formulas, A is actually a Σ_0^b formula, and by Theorem 8(1) and Lemma 9(d), the lower sequent is also a theorem of IS_2^1. The fact that $\vee$*:right*, $\wedge$*:right*, $\neg$*:left*, *Cut*, $\supset$*:right*, $\supset$*:left*, and $\exists \leq$*:right* inferences preserve the property of being a theorem of IS_2^1 follows in a similar manner from Lemma 9(a)-(c),(e)-(h), respectively. The structural inferences and the other *left* inference rules are even easier to handle.

The $\forall \leq$*:right* and $H\Sigma_1^b$-PIND inference rules remain. Suppose that the upper sequent of

$$\frac{b \leq t, \Pi \longrightarrow A(b), \Lambda}{\Pi \longrightarrow (\forall x \leq t) A(x), \Lambda}$$

is a theorem of IS_2^1CU (recall b must not appear in the lower sequent). Since $(\forall x \leq t)A(x)$ is a $H\Sigma_1^b$-formula, the indicated quantifier must be sharply bounded and the term t must be of the form $t = |s|$. Then IS_2^1 also proves

$$b \leq t, \Pi, \left[(\forall x \leq |(\lfloor \tfrac{1}{2} b \rfloor)|) A(x) \vee \left(\bigvee \Lambda\right)\right] \longrightarrow \left[(\forall x \leq |b|) A(x) \vee \left(\bigvee \Lambda\right)\right]$$

and now it is easy to use $H\Sigma_1^b$-PIND on the formula in square brackets with respect to the variable b to show that the lower sequent of the $\forall \leq$*:right* inference is a theorem of IS_2^1CU.

Finally, suppose that the upper sequent of a $H\Sigma_1^b$-PIND inference

$$\frac{A(\lfloor \frac{1}{2}b \rfloor), \Pi \longrightarrow A(b), \Lambda}{A(0), \Pi \longrightarrow A(t), \Lambda}$$

is a theorem of IS_2^1CU. It follows that

$$\Pi, A(\lfloor \tfrac{1}{2}b \rfloor) \vee \left(\bigvee \Lambda\right) \longrightarrow A(b) \vee \left(\bigvee \Lambda\right)$$

is also a consequence of IS_2^1CU, from whence, by an intuitionistic use of $H\Sigma_1^b$-PIND,

$$\Pi, A(0) \vee \left(\bigvee \Lambda\right) \longrightarrow A(t) \vee \left(\bigvee \Lambda\right)$$

which intuitionistically implies the lower sequent of the inference.
Q.E.D. Theorem 10

Corollary 11 *(Cook-Urquhart [7]) The systems IS_2^1CU and IS_2^1B are equivalent.*

Corollary 12 *(Cook-Urquhart [7]) Any Σ_1^b-definable function of S_2^1 is Σ_1^{b+}-definable in IS_2^1CU.*

Corollary 13 *(Cook-Urquhart [7]) IS_2^1 is closed under Markov's Rule for $H\Sigma_1^b$-formulas. In other words, if A is an $H\Sigma_1^b$-formula and if $IS_2^1 \vdash \neg\neg A$ then $IS_2^1 \vdash A$.*

4. On the Choice of Axioms for IS_2^1

We have shown that although the BBASIC axioms and the CUBASIC axioms are not equivalent, the different definitions of IS_2^1 by Buss and by Cook and Urquhart are equivalent. It is worth asking what is the best or right definition of these systems. The original BASIC axioms (the BBASIC axioms) were defined to serve as a base theory for a number of theories of bounded arithmetic: we stated in [2] that any "sufficiently large" set of universal axioms would suffice as the BASIC axioms. Although the CUBASIC axioms are sufficient as a base theory for IS_2^1CU they may well not be strong anough for other (weaker) theories. Let us formulate five general criteria for the choice of BASIC axioms: (1) The BASIC axioms should be universal, true formulas. (2) The BASIC axioms should be strong enough to prove elementary facts about the non-logical symbols. (3) The BASIC axioms should not be too strong; for example, they should not state something equivalent to the consistency of Peano arithmetic. (4) Let I_m be a term with value equal to m and length linear in $|m|$. Then for any fixed term $t(\vec{x})$ there should be polynomial size BASIC proofs of $t(I_{\vec{n}}) = I_{t(\vec{n})}$ for all natural numbers $\vec{n}$. More generally, if $A(\vec{x})$ is a fixed Σ_1^b-formula then for all $\vec{n} \in \mathbb{N}$, if $A(\vec{n})$ is true there should be a free-cut free BASIC proof of $A(I_{\vec{n}})$. In addition, this statement should be formalizable in IS_2^1 or S_2^1 (this is Theorem 7.4 of [2]). (5) For every term $t(\vec{x})$, there should be a term $\sigma_t(\vec{x})$ such that the BASIC axioms imply (without induction) that

$$\forall \vec{x} \forall \vec{y} ((\bigwedge_{i=1}^{k} x_i \leq y_i) \supset t(\vec{x}) \leq \sigma_t(\vec{y})).$$

This fifth condition states that BASIC is a "sufficient" theory in the terminology of [4]. Note that the remark at the very end of section 2 can be used to show that the CUBASIC axioms are not sufficient. It is important that a theory be sufficient in order to be able to introduce new function symbols and use them freely in terms bounding quantifiers and it seems expedient that the BASIC axioms themselves be sufficient (without any induction). In addition, Theorem 4.10 of [2] seems to depend crucially on the fact that that BASIC axioms are sufficient.

Thus we prefer the BBASIC axioms, or equivalently and slightly more elegantly, the CUBASIC axioms plus (B-21), (B-28) and (B-30), over just the CUBASIC axioms.

Finally let's consider consider the axiomatizations of IS_2^1CU and IS_2^1B. Since IS_2^1CU proves that any $H\Sigma_1^b$-formula is equivalent to a Σ_1^{b+}-formula, the choice of $H\Sigma_1^b$-PIND versus Σ_1^{b+}-PIND is unimportant‡. Of more significance is the choice of non-induction axioms. The theory IS_2^1B is defined with a set of consequences of S_2^1 as its non-induction axioms, whereas, IS_2^1CU has just the CUBASIC axioms as non-induction axioms. In the former case, Buss thus required the "main theorem" for S_2^1 to prove that every definable function of IS_2^1B is polynomial time computable; but in the latter case, Cook

‡Cook and Urquhart use Σ_1^{b+}-formulas to simplify the bootstrapping.

and Urquhart are able to obtain the main theorem for S^1_2 as a corollary to their Dialectica interpretation of the intuitionistic systems. By using our simplified proof of Theorem 11 above, the main theorem for S^1_2 follows already from the corresponding theorem for IS^1_2B or IS^1_2CU without requiring the Dialectica interpretation. Thus Cook and Urquhart's use of BASIC axioms as a base theory is a nice improvement over using the sequents of $H\Sigma^b_1$-formulas which are consequences of S^1_2.

5. Conservation Results for S^1_2 over Intuitionistic Theories

In this section, an extension of IS^1_2 called IS^{1+}_2 is defined; actually, it is open whether IS^1_2 and IS^{1+}_2 are distinct. We are interested in IS^{1+}_2 because it allows a rather general extension of Theorem 10 and because IS^{1+}_2 arises naturally in the study of Kripke models for intuitionistic Bounded Arithmetic. First we state a generalization of Theorem 10 that still applies if IS^1_2.

Theorem 14

(a) *If A is a positive formula and $S^1_2 \vdash \neg A$ then $IS^1_2 \vdash \neg A$.*

(b) *If A is a positive formula and B is an $H\Sigma^b_1$-formula, then if $S^1_2 \vdash A \supset B$ then $IS^1_2 \vdash A \supset B$.*

Corollary 15 *A positive sentence is classically consistent with S^1_2 if and only if it is intuitionistically consistent with IS^1_2.*

Proof The proof of Theorem 14 is almost exactly like the proof the Theorem 10. First note that (b) implies (a) by taking B to be $0 = 1$, so it suffices to prove (b). By using free-cut elimination and by restricting induction in the S^1_2-proof to PIND on $H\Sigma^b_1$-formulas, there is an S^1_2-proof P of the sequent $A \longrightarrow B$ such that every formula in the antecedent of a sequent in P is either positive or an $H\Sigma^b_1$-formula and such that every formula in the succedent of a sequent in P is an $H\Sigma^b_1$-formula. Now the rest of the proof of Theorem 10 applies word-for-word. $\Box$

Definition An *$H\Sigma^{b*}_1$-formula with distinguished variable* b is a formula of the form $A(b, \vec{c}) \vee B(\vec{c})$ where A is an $H\Sigma^b_1$-formula, B is an arbitrary formula and b does not occur in $B(\vec{c})$. The variables $\vec{c}$ will act as parameters.

Definition IS^{1+}_2 is the intutionistic theory axiomatized as IS^1_2 plus the PIND axioms for $H\Sigma^{b*}_2$-formulas with respect to their distinguished variables.

Note that S^1_2 implies (classically) all the axioms of IS^{1+}_2 since it can classically consider the two cases $B(\vec{c})$ and $\neg B(\vec{c})$. However, we don't know if IS^1_2 implies IS^{1+}_2. The main reason for our interest in IS^{1+}_2 is that it is the intuitionistic theory which is valid in Kripke models in which every world is a classical model of S^1_2. This fact is proved in Buss [5] and depends crucially on the next theorem.

Definition Let A be a positive formula and let B be an arbitrary formula. The formula A^B is obtained from A by replacing every atomic subformula C of A by $(C \vee B)$. (We are using the conventions of Gentzen's sequent calculus: there are distinct free and bound variables and hence free variables in B can not become bound in A^B.)

Theorem 16 *Let A be a positive formula and suppose $S^1_2 \vdash \neg A$. Then, for any formula B, $IS^{1+}_2 \vdash A^B \supset B$.*

Proof As argued above, if $S^1_2 \vdash \neg A$ then there is a tree-like, free-cut free S^1_2-proof P of the sequent $A \longrightarrow$ in which every formula is either (a) in an antecedent, positive and an ancestor of the formula A in the endsequent, or (b) is an $H\Sigma^b_1$-formula which is an ancestor of a cut formula. Form another "proof" P^* by replacing every formula C in P of type (a) by the formula C^B, and, for any sequent in which such a replacement is made, adding the formula B to the succedent. P^* ends with the sequent $A^B \longrightarrow B$; although P^* is not quite a valid IS^{1+}_2-proof, we claim that all the "inferences" in P are sound for IS^{1+}_2.

To prove this claim, consider the ways that P^* may fail to be an IS^{1+}_2-proof. Initial sequents in P contain only atomic formulas, so in P^* each initial sequent is either (a) unchanged from P or (b) has at least one formula, say D, in the antecedent replaced by $D \vee B$ and has B added as an additional formula in the succedent. In either case, the initial sequent of P^* is a consequence of IS^{1+}_2 (and of IS^1_2). Just as in the proof of Theorem 10, any $\neg$*:right*, $\vee$*:right*, $\wedge$*:right*, $\neg$*:left*, *Cut*, $\supset$*:right*, $\supset$*:left*, $\exists\leq$*:left*, $\vee$*:left*, $\wedge$*:left* and structural inferences in P become IS^{1+}_2 sound "inferences" in P^*. It remains to consider the cases of $\forall\leq$*:right* and PIND. These latter two cases are handled similarly to the corresponding cases in the proof of Theorem 10. Suppose, for instance, that P contains the inference

$$\frac{b \leq t, \Pi \longrightarrow A(b), \Lambda}{\Pi \longrightarrow (\forall x \leq t) A(x), \Lambda}$$

where b is the eigenvariable and does not occur in the lower sequent. Since $(\forall x \le |t|)A(x)$ is an $H\Sigma_1^b$-formula, the indicated quantifier must be sharply bounded and $t = |s|$ for some term s. In P^*, this inference is either unchanged or becomes

$$\frac{b \le t, \Pi^* \longrightarrow A(b), \Lambda, B}{\Pi^* \longrightarrow (\forall x \le t)A(x), \Lambda, B}$$

where Π^* represents Π with one or more formulas C replaced by $C \vee B$. We claim that if the upper sequent of this latter "inference" is IS_2^{1+}-provable, then so is the lower inference. This is because if the upper sequent is provable, then IS_2^{1+} proves

$$b \le t, \Pi^*, \left[(\forall x \le |(\lfloor \tfrac{1}{2}b \rfloor)|)A(x) \vee (\bigvee \Lambda) \vee B\right] \longrightarrow \\ \longrightarrow [(\forall x \le |b|)A(x) \vee (\bigvee \Lambda) \vee B] .$$

The formula in square brackets is an $H\Sigma_1^{b*}$-formula since every formula in Λ is in $H\Sigma_1^b$-formula. Hence IS_2^{1+} can use its PIND axioms on this formula to prove the lower sequent.

Similarly, any induction inference in P corresponds to an IS_2^{1+}-sound inference in P^*; this is shown as in the proof of Theorem 10, except again the $(\bigvee \Lambda)$ may become $(\bigvee \Lambda) \vee B$.
Q.E.D. Theorem 16

There are several open problems regarding axiomatizations of IS_2^1. As noted above, we don't know if IS_2^{1+} is equivalent to IS_2^1. Also, S. Cook asked whether Π_1^{b+}-PIND is a consequence of IS_2^1. Current techniques (feasible realizability or functional interpretations) can not be used to show that Π_1^{b+}-PIND is *not* a consequence of IS_2^1 since the Π_1^{b+}-PIND axioms are polynomial-time realizable. Likewise, it is open whether the Σ_1^b-PIND axioms are consequences of IS_2^1. Again, the Σ_1^b-PIND axioms are polynomial-time realizable.

One final observation: if S_2^1 can prove that $\mathrm{P} = \mathrm{NP}$ then any bounded formula is IS_2^1-provably equivalent to a Σ_1^{b+}-formula and IS_2^1 would have

PIND and the law of the excluded middle for all bounded formulas. By S^1_2 proving $\mathrm{P} = \mathrm{NP}$ we mean that there is a Δ^b_1-definable, polynomial-time predicate which, provably in S^1_2, is equivalent to some NP-complete problem (such as SAT). Hence it is expected to be difficult to show that, say Π^{b+}_1-PIND is not a consequence of IS^1_2 since this would require proving that S^1_2 does not prove $\mathrm{P} = \mathrm{NP}$. Similarly, it is expected to be difficult to show that IS^1_2 is not equal to IS^2_2 or, more generally, to show that the hierarchy of intuitionistic theories of Bounded Arithmetic is proper.

References

[1] S. R. Buss, *The polynomial hierarchy and fragments of bounded arithmetic*, in Proceedings of the 17-th Annual ACM Symposium on Theory of Computing, 1985, pp. 285–290.

[2] ——, *Bounded Arithmetic*, Bibliopolis, 1986. Revision of 1985 Princeton University Ph.D. thesis.

[3] ——, *The polynomial hierarchy and intuitionistic bounded arithmetic*, in Structure in Complexity, Lecture Notes in Computer Science #223, Springer-Verlag, 1986, pp. 77–103.

[4] ——, *A conservation result concerning bounded theories and the collection axiom*, Proceedings of the American Mathematical Society, 100 (1987), pp. 709–716.

[5] ——, *On model theory for intuitionistic bounded arithmetic with applications to independence results*, in Feasible Mathematics: A Mathematical Sciences Institute Workshop held in Ithaca, New York, June 1989, Birkhäuser, 1990, pp. 27–47.

[6] S. A. Cook and A. Urquhart, *Functional interpretations of feasibly constructive arithmetic (extended abstract)*, in Proceedings of the 21-st Annual ACM Symposium on Theory of Computing, 1989, pp. 107–112. Synopsis of [7].

[7] ——, *Functional interpretations of feasibly constructive arithmetic*, Annals of Pure and Applied Logic, 63 (1993), pp. 103–200.

[8] V. Harnik, *Provably total functions of intuitionistic bounded arithmetic.* Typewritten manuscript, 1989.