Open induction in a bounded arithmetic for TC^0

Emil Jeřábek*

Institute of Mathematics of the Academy of Sciences

Žitná 25, 115 67 Praha 1, Czech Republic, email: jerabek@math.cas.cz

May 28, 2014

Abstract

The elementary arithmetic operations $+, \cdot, \leq$ on integers are well-known to be computable in the weak complexity class TC^0, and it is a basic question what properties of these operations can be proved using only TC^0-computable objects, i.e., in a theory of bounded arithmetic corresponding to TC^0. We will show that the theory VTC^0 extended with an axiom postulating the totality of iterated multiplication (which is computable in TC^0) proves induction for quantifier-free formulas in the language $\langle +, \cdot, \leq \rangle$ (*IOpen*), and more generally, minimization for Σ^b_0 formulas in the language of Buss's S_2.

1 Introduction

Proof complexity is sometimes presented as the investigation of a three-way correspondence between propositional proof systems, theories of bounded arithmetic, and computational complexity classes. In particular, we can associate to a complexity class C satisfying suitable regularity conditions a theory T such that on the one hand, the provably total computable functions of T of certain logical form define exactly the C-functions in the standard model of arithmetic, and on the other hand, T proves fundamental deductive principles such as induction and comprehension for formulas that correspond to C-predicates. In this sense T provides a formalization of C-feasible reasoning: we can interpret provability in T as capturing the idea of what can be demonstrated when our reasoning capabilities are restricted to manipulation of objects and concepts of complexity C. The complexity class corresponding to a "minimal" theory that proves a given logical or combinatorial statement can be seen as a gauge of its proof complexity. Then a particularly natural question is, given a function or predicate X, which properties of X can be proved by reasoning whose complexity does not exceed that of X, that is, in a theory corresponding to the complexity class for which X is complete.

*Supported by grant IAA100190902 of GA AV ČR, Center of Excellence CE-ITI under the grant P202/12/G061 of GA ČR, and RVO: 67985840. The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007–2013) / ERC grant agreement no. 339691.

The main theme of this paper is what we can feasibly prove about the basic integer arithmetic operations $+, \cdot, \leq$. The matching complexity class is TC^0: $+$ and $\leq$ are computable in $\mathrm{AC}^0 \subseteq \mathrm{TC}^0$, while $\cdot$ is in TC^0, and it is in fact TC^0-complete under AC^0 (Turing) reductions. (In this paper, all circuit classes like TC^0 are assumed DLOGTIME-uniform unless stated otherwise.) TC^0 also includes many other functions related to arithmetic. First, $+$ and $\cdot$ are also TC^0-computable on rationals or Gaussian rationals. An important result of Hesse, Allender, and Barrington [11] based on earlier work by Beame et al. [3] and Chiu et al. [7] states that integer division and iterated multiplication are TC^0-computable. As a consequence, one can compute in TC^0 approximations of functions presented by sufficiently nice power series, such as log, sin, or $x^{1/k}$, see e.g. Reif [26], Reif and Tate [27], Maciel and Thérien [22], and Hesse et al. [11].

The more-or-less canonical arithmetical theory corresponding to TC^0 is VTC^0 (see Cook and Nguyen [8]). This is a two-sorted theory in the setup of Zambella [33], extending the base AC^0-theory V^0 by an axiom stating the existence of suitable counting functions, which gives it the power of TC^0. VTC^0 is equivalent ($RSUV$-isomorphic) to the one-sorted theory Δ^b_1-CR by Johannsen and Pollett [19], which is in turn $\forall\exists\Sigma^b_1$-conservative under the theory C^0_2 [18].

VTC^0 can define addition and multiplication on binary integers, and it proves basic identities governing these operations, specifically the axioms of discretely ordered rings (DOR). We are interested in what other properties of integers expressible in the language $L_{OR} = \langle 0, 1, +, -, \cdot, \leq \rangle$ of ordered rings are provable in VTC^0, and in particular, whether the theory can prove induction for a nontrivial class of formulas. Note that we should not expect the theory to prove induction for bounded existential formulas, or even its weak algebraic consequences such as the Bézout property: this would imply that integer gcd is computable in TC^0, while it is not even known to be in NC. However, this leaves the possibility that VTC^0 could prove induction for *open* (quantifier-free) formulas of L_{OR}, i.e., that it includes the theory *IOpen* introduced by Shepherdson [29].

Using an algebraic characterization of open induction and a witnessing theorem for VTC^0, the provability of *IOpen* in this theory is equivalent to the existence of TC^0 algorithms for approximation of real or complex roots of constant-degree univariate polynomials whose soundness can be proved in VTC^0. The existence of such algorithms in the "real world" is established in [15], but the argument extensively relies on tools from complex analysis (Cauchy integral formula, ...) that are not available in bounded arithmetic, hence it is unsuitable for formalization in VTC^0 or a similar theory.

The purpose of this paper is to demonstrate that *IOpen* is in fact provable in a mild extension of VTC^0. The argument naturally splits into two parts. We first formalize by a direct inductive proof a suitable version of the Lagrange inversion formula (LIF), which was also the core ingredient in the algorithm in [15]. This allows us to compute approximations of a root of a polynomial f by means of partial sums of a power series expressing the inverse function of f, but only for polynomials obeying certain restrictions on coefficients. The second part of the argument is model-theoretic, using basic results from the theory of valued fields. The question whether a given DOR is a model of *IOpen* can be reduced to the question whether the completion of its fraction field under a valuation induced by its ordering is real-closed, and there is a simple criterion for recognizing real-closed valued fields. In our situation, LIF ensures the relevant field is henselian, which implies that the criterion is satisfied.

We do not work with VTC^0 itself, but with its extension $VTC^0 + IMUL$ including an axiom ensuring the totality of iterated multiplication. This theory corresponds to TC^0 just like VTC^0 does, as iterated multiplication is TC^0-computable. We need the extra axiom because it is not known whether VTC^0 can formalize the TC^0 algorithms for division and iterated multiplication of Hesse et al. [11], and this subtle problem is rather tangential to the question of open induction and root approximation. As explained in more detail in Section 3, the *IMUL* axiom is closely related to the integer division axiom *DIV* which is implied by *IOpen*, hence its use is unavoidable in one way or another. In terms of the original theory VTC^0, our results show that $VTC^0 \vdash IOpen$ if and only if $VTC^0 \vdash DIV$.

We can strengthen the main result if we switch from L_{OR} to the language of Buss's one-sorted theories of bounded arithmetic. By formalizing the description of bounded Σ^b_0-definable sets due to Mantzivis [23], $VTC^0 + IMUL$ can prove the *RSUV*-translation of Buss's theory T^0_2, and in fact, of the Σ^b_0-minimization schema. In other words, T^0_2 and Σ^b_0-*MIN* are included in the theory Δ^b_1-$CR + IMUL$.

2 Preliminaries

A structure $\langle D, 0, 1, +, -, \cdot, \leq\rangle$ is an *ordered ring* if $\langle D, 0, 1, +, -, \cdot\rangle$ is a commutative (associative unital) ring, $\leq$ is a linear order on D, and $x \leq y$ implies $x + z \leq y + z$ and $xz \leq yz$ for all $x, y, z \in D$ such that $z \geq 0$. If D is an ordered ring, D^+ denotes $\{a \in D : a > 0\}$. A *discretely ordered ring* (*DOR*) is an ordered ring D such that 1 is the least element of D^+. Every DOR is an integral domain. An *ordered field* is an ordered ring which is a field. A *real-closed field* (*RCF*) is an ordered field R satisfying any of the following equivalent conditions:

- Every $a \in R^+$ has a square root in R, and every $f \in R[x]$ of odd degree has a root in R.
- R has no proper algebraic ordered field extension.
- The field $R(\sqrt{-1})$ is algebraically closed.
- R is elementarily equivalent to $\mathbb{R}$.

(In a RCF, $\leq$ is definable in terms of the ring structure, thus we can also call a field $\langle R, +, \cdot\rangle$ real-closed if it is the reduct of a RCF.) The *real closure* of an ordered field F is a RCF $\tilde{F}^{\mathrm{real}} \supseteq F$ which is an algebraic extension of F. Every ordered field has a unique real closure up to a unique F-isomorphism.

The theory *IOpen* consists of the axioms of ordered rings and the induction schema

$$\varphi(0) \wedge \forall x\, (\varphi(x) \to \varphi(x+1)) \to \forall x \geq 0\, \varphi(x)$$

for open formulas φ (possibly with parameters). An *integer part* of an ordered field F is a discretely ordered subring $D \subseteq F$ such that every element of F is within distance 1 from an element of D. The following well-known characterization is due to Shepherdson [29].

Theorem 2.1 *Models of IOpen are exactly the integer parts of real-closed fields.* □

The criterion is often stated with the real closure of the fraction field of the model instead of a general real-closed field, but these two formulations are clearly equivalent, as an integer part D of a field R is also an integer part of any subfield $D \subseteq R' \subseteq R$.

In particular, models of *IOpen* are integer parts of their fraction fields. This amounts to provability of the division axiom

$$(DIV) \qquad \forall x > 0\, \forall y\, \exists q, r\, (y = qx + r \wedge 0 \leq r < x)$$

in *IOpen*. (The uniqueness of q and r holds in any DOR.)

We define AC^0 as the class of languages recognizable by a DLOGTIME-uniform family of polynomial-size constant-depth circuits using $\neg$ and unbounded fan-in $\wedge$ and $\vee$ gates, or equivalently, languages computable by an $O(\log n)$-time alternating Turing machine with $O(1)$ alternations, or by a constant-time CRAM with polynomially many processors [12]. If we represent an n-bit binary string w by the finite structure $\langle \{0, \dots, n-1\}, <, +, \cdot, P_w \rangle$, where $P_w(i)$ iff the ith bit of w is 1, then AC^0 coincides with FO (languages definable by first-order sentences). A language B is AC^0-*reducible* to a language A if B is computable by a DLOGTIME-uniform family of polynomial-size constant-depth circuits using unbounded fan-in $\wedge$, $\vee$, $\neg$, and A-gates. The class of languages AC^0-reducible to A is its AC^0-*closure*.

TC^0, originally introduced as a nonuniform class by Hajnal et al. [10], is defined for our purposes as the AC^0-closure of Majority. (Several problems TC^0-complete under AC^0 reductions are noted in Chandra et al. [6], any of these could be used in place of Majority.) Equivalently, TC^0 coincides with languages computable by $O(\log n)$-time threshold Turing machines with $O(1)$ thresholds, or by constant-time TRAM with polynomially many processors [25]. In terms of descriptive complexity, a language is in TC^0 iff the corresponding class of finite structures is definable in FOM, i.e., first-order logic with majority quantifiers [1].

In connection with bounded arithmetic, it is convenient to consider not just the complexity of languages, but of predicates $P(x_1, \dots, x_n, X_1, \dots, X_m)$ with several inputs, where X_i are binary strings as usual, and x_i are natural numbers written in unary. It is straightforward to generalize AC^0, TC^0, and similar classes to this context, see [8, §IV.3] for details. Likewise, we can consider computability of functions: if C is a complexity class, a unary number function $f(\vec{x}, \vec{X})$ is in FC if it is bounded by a polynomial in $\vec{x}$ and the lengths of $\vec{X}$, and its graph $f(\vec{x}, \vec{X}) = y$ is in C; a string function $F(\vec{x}, \vec{X})$ is in FC if the length of the output is polynomially bounded as above, and the bitgraph $G_F(\vec{x}, \vec{X}, y) \Leftrightarrow (F(\vec{x}, \vec{X}))_y = 1$ is in C. For simplicity, functions from FC will also be called just C-functions.

We will work with two-sorted (second-order) theories of bounded arithmetic in the form introduced by Zambella [33] as a simplification of Buss [5]. We refer the reader to Cook and Nguyen [8] for a general background on these theories as well as a detailed treatment of VTC^0, however, we include the main definitions here in order to fix our notation.

The language $L_2 = \langle 0, S, +, \cdot, \leq, \in, \|\cdot\| \rangle$ of second-order bounded arithmetic is a first-order language with equality with two sorts of variables, one for unary natural numbers, and one for finite sets thereof, which can also be interpreted as binary strings, or binary integers. The standard convention is that variables of the first sort are written with lowercase letters $x, y, z, \ldots$, and variables of the second sort with uppercase letters $X, Y, Z, \ldots$. While we adhere to this convention in the introductory material on the theories and their basic properties, we will not follow it in the less formal main part of the paper (we will mostly work with binary integers or rationals, and it looks awkward to write them all in uppercase). The symbols $0, S, +, \cdot, \leq$ of L_2 denote the usual arithmetic operations and relation on the unary sort; $x \in X$ is the elementhood predicate, and the intended meaning of the $\|X\|$ function is the least unary number strictly greater than all elements of X. This function is usually denoted as $|X|$, however (apart from the section on Buss's theories) we reserve the latter symbol for the absolute value on binary integers and rationals, which we will use more often. We write $x < y$ as an abbreviation for $x \leq y \wedge x \neq y$.

Bounded quantifiers are introduced by

$$\exists x \leq t\, \varphi \Leftrightarrow \exists x\, (x \leq t \wedge \varphi),$$
$$\exists X \leq t\, \varphi \Leftrightarrow \exists X\, (\|X\| \leq t \wedge \varphi),$$

where t is a term of unary sort not containing x or X (resp.). Universal bounded quantifiers, as well as variants of bounded quantifiers with strict inequalities, are defined in a similar way. A formula is Σ^B_0 if it contains no second-order quantifiers, and all its first-order quantifiers are bounded. The Σ^B_0-definable predicates in the standard model of arithmetic are exactly the AC^0 predicates. A formula is Σ^B_i if it consists of i alternating (possibly empty) blocks of bounded quantifiers, the first of which is existential, followed by a Σ^B_0 formula. We define Π^B_i formulas dually. Similarly, a formula is Σ^1_i (Π^1_i) if it consists of i alternating blocks of (possibly unbounded) quantifiers, the first of which is existential (universal, resp.), followed by a Σ^B_0 formula[1].

The theory V^0 in L_2 can be axiomatized by the basic axioms

$$\begin{aligned}
&x + 0 = x && x + Sy = S(x + y)\\
&x \cdot 0 = 0 && x \cdot Sy = x \cdot y + x\\
&Sy \leq x \to y < x && \|X\| \neq 0 \to \exists x\, (x \in X \wedge \|X\| = Sx)\\
&x \in X \to x < \|X\| && \forall x\, (x \in X \leftrightarrow x \in Y) \to X = Y
\end{aligned}$$

and the comprehension schema

$$(\varphi\text{-}\mathit{COMP}) \qquad \exists X \leq x\, \forall u < x\, (u \in X \leftrightarrow \varphi(u))$$

for Σ^B_0 formulas φ, possibly with parameters not shown (but with no occurrence of X). We denote the set X whose existence is postulated by φ-*COMP* as $\{u < x : \varphi(u)\}$. Using *COMP*, V^0 proves the induction and minimization schemata

$$(\varphi\text{-}\mathit{IND}) \qquad \varphi(0) \wedge \forall x\, \big(\varphi(x) \to \varphi(x+1)\big) \to \forall x\, \varphi(x),$$
$$(\varphi\text{-}\mathit{MIN}) \qquad \varphi(x) \to \exists y\, \big(\varphi(y) \wedge \forall z < y\, \neg\varphi(z)\big)$$

[1]Notice that bounded second-order quantifiers still count towards i, so these formula classes do not correspond in the one-sorted setting to the usual arithmetical hierarchy Σ^0_i, but to its restricted version where the formula after the main quantifier prefix is sharply bounded. We follow [8] in this usage; they only appear to define Σ^1_1, but we find it convenient to extend this notation to higher levels as well.

for Σ^B_0 formulas φ. In particular, V^0 includes $I\Delta_0$ on the unary number sort.

Let $\langle x, y\rangle$ be a V^0-definable pairing function on unary numbers, e.g., $\langle x, y\rangle = (x + y)(x + y + 1)/2 + y$. We define $X^{[u]} = \{x : \langle u, x\rangle \in X\}$; this provides an encoding of sequences of sets by sets. We can encode sequences of unary numbers by putting $X^{(u)} = \|X^{[u]}\|$ (this is easily seen to be a Σ^B_0-definable function). For convenience, we also extend the pairing function to (standard-length) k-tuples by $\langle x_1, \dots, x_{k+1}\rangle = \langle\langle x_1, \dots, x_k\rangle, x_{k+1}\rangle$, and we write $X^{[u_1,\dots,u_k]} = X^{[\langle u_1,\dots,u_k\rangle]}$, $X^{(u_1,\dots,u_k)} = X^{(\langle u_1,\dots,u_k\rangle)}$.

VTC^0 is the extension of V^0 by the axiom

$$\forall n, X\, \exists Y\, \bigl(Y^{(0)} = 0 \wedge \forall i < n\, \bigl((i \notin X \to Y^{(i+1)} = Y^{(i)}) \wedge (i \in X \to Y^{(i+1)} = Y^{(i)} + 1)\bigr)\bigr),$$

whose meaning is that for every set X there is a sequence Y supplying the counting function $Y^{(i)} = \operatorname{card}(X \cap \{0, \dots, i - 1\})$.

Let Γ be a class of formulas, and T an extension of V^0. A string function $F(\vec{x}, \vec{X})$ is a *provably total* Γ*-definable function* of T if its graph is definable in $\mathbb{N}$ by a formula $\varphi(\vec{x}, \vec{X}, Y) \in \Gamma$ such that $T \vdash \forall \vec{x}, \vec{X}\, \exists! Y\, \varphi(\vec{x}, \vec{X}, Y)$; similarly for number functions. If $\Gamma = \Sigma^1_1$, such functions are also called *provably total recursive functions* of T. Note that one function may have many different definitions that are not T-provably equivalent; some of them may be provably total, while other are not.

The provably total recursive functions of V^0 and VTC^0 are FAC^0 and FTC^0, respectively. Moreover, we can use these functions freely in the sense that if we expand the languages of the theories with the corresponding function symbols, the resulting conservative extensions of V^0 and VTC^0 (respectively) prove the comprehension and induction schemata for Σ^B_0 formulas of the expanded language; we will see more details in the next section.

Being AC^0, the ordering on binary integers is definable by a Σ^B_0 formula, and addition is provably total in V^0. Likewise, multiplication and iterated addition are provably total Σ^B_1-definable functions of VTC^0. In fact, as shown in [8], the natural Σ^B_0 definitions of $X < Y$ and $X + Y$ provably satisfy basic properties like commutativity and associativity in V^0, and similarly, there are natural definitions of $X \cdot Y$ and $\sum_{i<n} X^{[i]}$ provably total in VTC^0 such that VTC^0 proves their basic properties, including the inductive clauses

$$\sum_{i<0} X^{[i]} = 0,$$
$$\sum_{i<n+1} X^{[i]} = \sum_{i<n} X^{[i]} + X^{[n]}.$$

While Cook and Nguyen [8] normally use second-sort objects to denote nonnegative integers, it will be more convenient for us to make them represent all integers, which is easily accomplished by using one bit for sign. The definitions of $<$, $+$, $\cdot$, and $\sum_{i<n} X^{[i]}$ can be adapted in a straightforward way to this setting so that VTC^0 still proves their relevant properties, that is, the axioms of discretely ordered rings.

3 Iterated multiplication and division

As we already mentioned, it is not known whether VTC^0 can formalize the TC^0 algorithms of Hesse, Allender, and Barrington [11] for integer division and iterated multiplication. In particular, it is not known whether VTC^0 proves the sentence DIV (formulated for binary integers), which is a consequence of $IOpen$. This problem is rather tangential to the formalization of root finding, whence we bypass it by strengthening our theory appropriately.

It might seem natural just to work in the theory $VTC^0 + DIV$, however we will instead consider an axiom stating the totality of iterated multiplication in the following form:

$$(IMUL) \qquad \forall X, n\, \exists Y\, \forall i \le j < n\, \bigl(Y^{[i,i]} = 1 \wedge Y^{[i,j+1]} = Y^{[i,j]} \cdot X^{[j]}\bigr).$$

(The meaning is that for any sequence X of n binary integers, there is a triangular matrix Y with entries $Y^{[i,j]} = \prod_{k=i}^{j-1} X^{[k]}$.) One reason is simply that we need to use iterated multiplication at various places in the argument (in particular, to compute partial sums of power series), and we do not know whether $VTC^0 + DIV \vdash IMUL$. The more subtle reason is that we need the theory to be well-behaved in a certain technical sense that we will describe in more detail below, and it turns out that $VTC^0 + IMUL$ is the smallest well-behaved extension of $VTC^0 + DIV$.

Consider an extension $T \supseteq V^0$ proving that a particular polynomially bounded recursive (i.e., Σ^1_1-definable) function F is total, e.g. DIV or $IMUL$. While the most simplistic arguments employing F can get away with the mere fact that the value computed by F exists for a particular input, usually we need more than that. For example, we may want to use induction on a formula $\varphi(x)$ which involves F applied to an argument depending on x; since induction is obtained over V^0 by considering the least element of the set $\{x < a : \neg\varphi(x)\}$, we effectively need comprehension for (simple enough) formulas containing F, say, $\Sigma^B_0(F)$-$COMP$.

From a computational viewpoint, it is desirable that we can combine provably total recursive functions in various ways. For example, one of the basic TC^0 functions is iterated addition, and a natural way how we would like to apply it is to compute $\sum_{x<a} F(x)$ for a given provably total function F. More generally, we want the class of provably total recursive functions to be closed under AC^0 (or even TC^0 in our case) reductions, and as a simple special case, under *parallel repetition*: if we can compute a function $F(X)$, we want to be able to compute its *aggregate function* $F^*\colon \langle X_0, \dots, X_{n-1}\rangle \mapsto \langle F(X_0), \dots, F(X_{n-1})\rangle$ (where n is a part of the input). In more logical terms, it is desirable that T is closed under the *choice rule* Σ^B_0-AC^R: if $T \vdash \forall X\, \exists Y\, \varphi(X,Y)$, where $\varphi \in \Sigma^B_0$, then also $T \vdash \forall n\, \forall W\, \exists Z\, \forall i < n\, \varphi(W^{[i]}, Z^{[i]})$. This is a derived rule corresponding to the axiom of choice, also called replacement or bounded collection:

$$(\Sigma^B_0\text{-}AC) \qquad \forall i < n\, \exists Y \le m\, \varphi(i, Y, P) \to \exists Z\, \forall i < n\, \varphi(i, Z^{[i]}, P).$$

Unfortunately, none of the desiderata mentioned in the last two paragraphs hold automatically, even for theories of the simple form $V^0 + \forall X\, \exists! Y\, F(X) = Y$ (note that $VTC^0 + DIV$ is of such form): this axiom implies the totality of functions making a constant number of calls to F, but we cannot a priori construct functions involving an unbounded number of applications of F, such as the aggregate function F^*. However, Cook and Nguyen [8] show that the simple expedient of using F^* in the axiomatization instead of F leads to theories satisfying all the properties above.

Definition 3.1 Let $\delta(X, Y)$ be a Σ^B_0-formula such that V^0 proves

$$\delta(X,Y) \to \|Y\| \le t(X),$$
$$\delta(X,Y) \wedge \delta(X,Y') \to Y = Y'$$

for some term $t(X)$. The *Cook–Nguyen (CN) theory*[2] associated with δ is

$$V(\delta) = V^0 + \forall W, n\, \exists Z\, \forall i < n\, \delta(W^{[i]}, Z^{[i]}).$$

(That is, if F is a polynomially bounded function with an AC^0 graph defined by δ, which V^0 proves to be a partial function, then $V(\delta)$ is axiomatized by the statement that the aggregate function F^* is total.)

For example, VTC^0 can be formulated as a CN theory, as shown in [8, §IX.3].

Theorem 3.2 *Let $V(\delta)$ be a CN theory, and F the function whose graph is defined by δ.*

(i) The provably total Σ^1_1-definable (or Σ^B_1-definable) functions of $V(\delta)$ are exactly the functions in the AC^0-closure of F.

(ii) $V(\delta)$ has a universal definitional (and therefore conservative) extension $\overline{V(\delta)}$ in a language $L_{\overline{V(\delta)}}$ consisting of Σ^B_1-definable functions of $V(\delta)$. The theory $\overline{V(\delta)}$ has quantifier elimination for $\Sigma^B_0(L_{\overline{V(\delta)}})$-formulas, and it proves $\Sigma^B_0(L_{\overline{V(\delta)}})$-COMP, $\Sigma^B_0(L_{\overline{V(\delta)}})$-IND, and $\Sigma^B_0(L_{\overline{V(\delta)}})$-MIN.

(iii) $V(\delta)$ is closed under Σ^B_0-AC^R, and $V(\delta) + \Sigma^B_0$-AC is Π^1_2-conservative over $V(\delta)$.

Proof: (i) and (ii) are Theorems IX.2.3, IX.2.14, and IX.2.16 in Cook and Nguyen [8].

(iii): If $V(\delta) \vdash \forall X\, \exists Y\, \varphi(X,Y)$ with $\varphi \in \Sigma^B_0$, there is an $L_{\overline{V(\delta)}}$-term $G(X)$ such that $\overline{V(\delta)} \vdash \varphi(X, G(X))$ by Herbrand's theorem, as $\overline{V(\delta)}$ is a universal theory, and φ is equivalent to an open formula. Then $\overline{V(\delta)}$, hence $V(\delta)$, proves

$$\forall W, n\, \exists Z\, Z = \{\langle i, y\rangle : i < n, y \in G(W^{[i]})\}$$

using $\Sigma^B_0(L_{\overline{V(\delta)}})$-*COMP*.

The Π^1_2-conservativity of Σ^B_0-AC over $V(\delta)$ follows from the closure under Σ^B_0-AC^R by cut elimination. Alternatively, see [14, Thm. 4.19] for a model-theoretic proof generalizing the result of Zambella [33] for V^0. □

[2] In [8], $V(\delta)$ is denoted VC, where the complexity class C is the AC^0-closure of F, and it is called the minimal theory associated with C. We refrain from this terminology as the theory is not uniquely determined by the complexity class: it depends on the choice of the C-complete function F, and of a particular Σ^B_0-formula defining the graph of F in $\mathbb{N}$. In particular, both VTC^0 and $VTC^0 + IMUL$ are "minimal" theories for the same class (TC^0), and it would be rather confusing to call them as such.

Lemma 3.3

(*i*) *VTC*^{0} + *IMUL is a CN theory.*

(*ii*) *VTC*^{0} + *IMUL* ⊢ *DIV*.

Proof: (i): The main observation is that $VTC^0 + IMUL$ proves the totality of the aggregate function of iterated multiplication, that is,

$$(IMUL^*) \qquad \forall W, m, n\, \exists Z\, \forall k < m\, \forall i \le j < n\, \big(Z^{[k,i,i]} = 1 \land Z^{[k,i,j+1]} = Z^{[k,i,j]} \cdot W^{[k,j]}\big).$$

Given W, m, n, put $X = \{\langle nk + j, x\rangle : k < m, j < n, x \in W^{[k,j]}\}$ so that $X^{[nk+j]} = W^{[k,j]}$ for all $k < m$ and $j < n$, and let Y be as in ($IMUL$) for X, mn. Define

$$Z = \big\{\langle k, i, j, y\rangle : k < m, i \le j \le n, y \in Y^{[nk+i,nk+j]}\big\},$$

so that $Z^{[k,i,j]} = Y^{[nk+i,nk+j]}$ for $k < m$ and $i \le j \le n$. Then Z satisfies ($IMUL^*$).

Thus, $VTC^0 + IMUL = VTC^0 + IMUL^*$. The latter looks almost like a CN theory, except that the graph of the function specified in the axiom is not Σ^B_0, as it involves multiplication. (The official definition also does not allow an extra unary input, but this is benign as we could easily code X, n into a single set.) There are several ways how to get around this problem. For one, the whole machinery from [8, §IX.2] works fine if we take VTC^0 instead of V^0 as a base theory, and allow the use of $\Sigma^B_0(L_{\overline{VTC^0}})$ formulas. Alternatively, we can rewrite $IMUL$ to incorporate the definition of multiplication, say

$$\begin{aligned} (IMUL') \qquad & \forall X, n\, \exists Y, Z\, \forall i \le j < n\, \forall x < \|X\|\, \big(Y^{[i,i]} = 1 \land Z^{[i,j,0]} = 0 \land Z^{[i,j,\|X\|]} = Y^{[i,j+1]} \\ & \qquad \land \big(x \notin X^{[j]} \to Z^{[i,j,x+1]} = Z^{[i,j,x]}\big) \\ & \qquad \land \big(x \in X^{[j]} \to Z^{[i,j,x+1]} = Z^{[i,j,x]} + 2^x Y^{[i,j]}\big)\big), \end{aligned}$$

where + and multiplication by 2^x can be given easy Σ^B_0 definitions. Since the entries of Z can be expressed as products of suitable Σ^B_0-definable sequences of integers, one can show in the same way as above that $IMUL'$, as well as the axiom $IMUL'^*$ stating the totality of the corresponding aggregate function, is provable in $VTC^0 + IMUL$. Conversely, the CN theory $V^0 + IMUL'^*$ proves VTC^0 (as it implies the totality of usual multiplication), hence it is equivalent to $VTC^0 + IMUL$.

(ii) can be shown by formalizing the reduction from [3]. Assume that we want to find $\lfloor Y/X \rfloor$, where $X \ge 1$. Choose $n, m > 0$ such that $2^{n-1} \le X \le 2^n$ and $Y \le 2^m$, and put

$$Z = \sum_{i<m} (2^n - X)^i 2^{n(m-1-i)}.$$

An easy manipulation of the sum shows that $XZ = 2^{nm} - (2^n - X)^m$, hence

$$2^{nm} - 2^{(n-1)m} \le XZ \le 2^{nm}.$$

Put $Q = \lfloor YZ/2^{nm} \rfloor$. Then

$$2^{nm} Y \ge XYZ \ge 2^{nm} QX > XYZ - 2^{nm} X \ge 2^{nm}(Y - X - 1),$$

hence $QX \le Y \le (Q + 1)X$. □

The more complicated converse reduction of iterated multiplication to division was formalized in bounded arithmetic by Johannsen [17] (building on Johannsen and Pollett [18]), but in a different setting, so let us see what his result gives us here. Johannsen works with a one-sorted theory $C^0_2[div]$, whose language consists of the usual Buss's language for S_2 expanded with $\dot{-}$, MSP, and most importantly $\lfloor x/y \rfloor$. It is axiomatized by a suitable version of $BASIC$, the defining axiom for division, the quantifier-free $LIND$ schema, and the axiom of choice $BB\Sigma^b_0$ for Σ^b_0 formulas in the expanded language.

We claim that $C^0_2[div]$ is $RSUV$-isomorphic to the theory $VTC^0 + DIV + \Sigma^B_0\text{-}AC$. We leave the interpretation of the latter theory in $C^0_2[div]$ to the reader as we will not need it, and focus on the other direction. It is straightforward to translate the symbols of the language save division to the corresponding operations on binary integers, and prove the translation of $BASIC$ in VTC^0. Of course, DIV allows us to translate the division function and prove its defining axiom, hence the only remaining problem is with the $LIND$ and BB schemata. Here we have to be a bit careful, as Σ^b_0 (or even quantifier-free) formulas in the language of $C^0_2[div]$ do not translate to Σ^B_0 formulas in the language of V^0.

Let DIV^* denote the axiom stating the totality of the aggregate function of division, or rather, of its expanded version with witnesses for multiplication as in the proof of Lemma 3.3, so that $T = VTC^0 + DIV^*$ is a CN theory. By an application of choice, $VTC^0 + DIV + \Sigma^B_0\text{-}AC$ proves DIV^*. Let $\overline{T}$ be the universal conservative extension of T from Theorem 3.2, which includes function symbols for division and for TC^0 functions like multiplication. Since Σ^b_0 formulas in the language of $C^0_2[div]$ translate to $\Sigma^B_0(L_{\overline{T}})$ formulas, Theorem 3.2 implies that $\overline{T}$, and therefore $T \subseteq VTC^0 + DIV + \Sigma^B_0\text{-}AC$, proves the translation of open (or even Σ^b_0) $LIND$. As for the axiom of choice, every $\Sigma^B_0(L_{\overline{T}})$ formula is equivalent to a Σ^B_1 formula in the language of V^0, and $\Sigma^B_0\text{-}AC$ implies $\Sigma^B_1\text{-}AC$, hence the translation of $BB\Sigma^b_0$ is provable in $\overline{T} + \Sigma^B_0\text{-}AC$, and thus in $VTC^0 + DIV + \Sigma^B_0\text{-}AC$ by the conservativity of $\overline{T}$ over T.

This, together with provability of iterated multiplication in $C^0_2[div]$, implies the following:

Theorem 3.4 (Johannsen [17]) *$VTC^0 + DIV + \Sigma^B_0\text{-}AC$ proves $IMUL$.* □

Corollary 3.5 *$VTC^0 + IMUL = VTC^0 + DIV^*$ is the smallest CN theory including $VTC^0 + DIV$.*

Proof: Since $VTC^0 + DIV^*$ is a CN theory, Theorem 3.2 implies that $VTC^0 + DIV + \Sigma^B_0\text{-}AC$ is Π^1_2-conservative over $VTC^0 + DIV^*$, hence $VTC^0 + DIV^* \vdash IMUL$ by Theorem 3.4. Conversely, every CN theory (such as $VTC^0 + IMUL$, by Lemma 3.3) that proves DIV also proves DIV^*, using its closure under $\Sigma^B_0\text{-}AC^R$. □

Corollary 3.6 *$VTC^0 \vdash DIV$ if and only if $VTC^0 \vdash IMUL$.*

Proof: VTC^0 is a CN theory. □

The alert reader may have noticed that the reason why $IMUL$ yields a CN theory while this is unclear for DIV is not due to any deep property of iterated multiplication that would make it inherently better-behaved than division, but because we made it so by formulating the axiom in the slightly redundant form using a triangular matrix of partial products. There does not seem to be any particular reason we should expect to get a CN theory if we formulate the axiom more economically, using only a one-dimensional array consisting of the products $\prod_{j<i} X^{[j]}$. In view of this, the decision to axiomatize the theory using *IMUL* rather than DIV^* is mostly a matter of esthetic preference and convenience. Even in its triangular form, the *IMUL* axiom is a fairly natural rendering of the idea of computing iterated products, whereas the usage of an aggregate function in DIV^* is overtly a technical crutch. Moreover, we will be using iterated products more often than division, and while *DIV* has a straightforward proof in $VTC^0 + IMUL$ as indicated above, we would have to rely on the complicated argument from [17] to derive *IMUL* if we based the theory on DIV^*, making the main result of the paper less self-contained.

We mention another possibility for axiomatization of our theory, using the powering axiom

$$(POW) \qquad \forall X, n\, \exists Y\, \forall i < n \left(Y^{[0]} = 1 \wedge Y^{[i+1]} = Y^{[i]} \cdot X\right)$$

(here it makes no difference whether we use a linear or triangular array of witnesses) and its aggregate function version POW^*. Over VTC^0, we clearly have $IMUL \vdash POW^* \vdash POW$. The argument in Lemma 3.3 (ii) only needed the sequence of powers $(2^n - X)^i$, $i \leq m$ apart from VTC^0, hence it actually shows $POW \vdash DIV$. Since $VTC^0 + POW^*$ is a CN theory, this implies $VTC^0 + POW^* = VTC^0 + IMUL$. In fact, one can also show that $VTC^0 + POW = VTC^0 + DIV$ by formalizing the reduction of powering to division from [3]. The key point is that the result of a single division is enough to reconstruct the whole sequence of powers $X^0, \dots, X^n$, hence we do not need any aggregate functions. If $X < 2^k$ and $m = k(n+1) + 1$, let $2^{nm} = (2^m - X)Q + R$ with $R < 2^m - X$ using *DIV*, write $Q = \sum_{i<n} Y^{[i]} 2^{(n-1-i)m}$ with $Y^{[i]} < 2^m$, and put $Y^{[n]} = R$. Then one can show $Y^{[0]} = 1$ and

$$Y^{[j]} \leq 2^{kj} \wedge \forall i < j\, Y^{[i+1]} = XY^{[i]}$$

by induction on $j \leq n$. We leave the details to the interested reader.

Let us also mention that while it is unclear whether the soundness of the Hesse–Allender–Barrington algorithms for division and iterated multiplication is provable in VTC^0, it seems very likely that it is provable in $VTC^0 + IMUL$. If true, this would imply that $VTC^0 + IMUL$ is Π^1_1-axiomatizable over VTC^0 by the sentence asserting the soundness of the algorithm, and it can be formulated as a purely universal theory in the language of $\overline{VTC^0}$. A priori, the *IMUL* axiom is only $\forall\Sigma^B_1$.

Even though we do not know whether *IMUL* is provable in VTC^0 itself, we can place it reasonably low in the usual hierarchy of theories for small complexity classes: it is straightforward to show that $VTC^0 + IMUL$ is included in the theory VNC^2 (and even VTC^1, if anyone bothered to define such a theory) by formalizing the computation of iterated products by a balanced tree of binary products.

As stated in the Introduction, the provability of *IOpen* in VTC^0 or $VTC^0 + IMUL$ can be phrased in terms of TC^0 root-finding algorithms. There are several ways of expressing this connection precisely; one version reads as follows.

Proposition 3.7 *$VTC^0 + IMUL$ proves IOpen if and only if for every constant $d > 0$ there exist $L_{\overline{VTC^0+IMUL}}$-terms $R_-(A_0, \dots, A_d, X, Y, E)$ and $R_+(A_0, \dots, A_d, X, Y, E)$ such that the theory proves*

$$(1) \quad X < Y \wedge F(X) < 0 < F(Y) \wedge E > 0 \wedge Z_\pm = R_\pm(A_0, \dots, A_d, X, Y, E) \\ \to X < Z_- < Z_+ < Y \wedge Z_+ - Z_- < E \wedge F(Z_-) < 0 < F(Z_+),$$

where all second-sort variables are interpreted as binary rational numbers (fractions), and $F(X)$ denotes $A_d X^d + A_{d-1} X^{d-1} + \dots + A_0$.

Proof: Left-to-right: the statement that for every $A_0, \dots, A_d, X, Y, E$ there exist Z_-, Z_+ satisfying (1) is provable in *IOpen* (in the real closure of the model, there is a root of F between X and Y where F changes sign, and this root can be arbitrarily closely approximated from either side in the fraction field of the model using Theorem 2.1). By assumption, the same statement is also provable in $\overline{VTC^0 + IMUL}$. Since the latter is a universal theory whose terms are closed under definitions by cases, Herbrand's theorem implies that there are terms R_-, R_+ witnessing Z_-, Z_+.

Right-to-left: Let D be a DOR induced by a model of $VTC^0 + IMUL$, K its fraction field, and F a polynomial with coefficients in D. Since F can change sign only $\deg(F)$ times, a repeated use of (1) gives us elements $Z_0 < Z_1 < \dots < Z_k$ of K such that F has (in K) a constant sign on each interval $(-\infty, Z_0)$, (Z_k, ∞), and (Z_i, Z_{i+1}), except when $Z_{i+1} - Z_i < 1$. We have $D \vDash DIV$, hence we can approximate each Z_i in D within distance 1; it follows that in D, F is positive on a finite union of (possibly degenerate) intervals. Every L_{OR} open formula φ is equivalent to a Boolean combination of formulas of the form $F(X) > 0$, hence $\{X \in D : X \geq 0 \wedge \neg\varphi(X)\}$ is also a finite union of intervals, and as such it has a least element if nonempty. Thus, D satisfies induction for φ. □

Note that $L_{\overline{VTC^0+IMUL}}$-terms denote TC^0 algorithms (employing iterated multiplication), hence the gist of the conclusion of Proposition 3.7 is that $VTC^0 + IMUL$ proves the soundness of a TC^0 degree-d polynomial root-approximation algorithm for each d. The details can be varied; for example, we could drop X and Y, and make the algorithm output approximations to all real roots of the polynomial, or even complex roots. However, such modifications make it more difficult to state what exactly the "soundness" of the algorithm means.

4 Working in $VTC^0 + IMUL$

As we already warned the reader, the objects we work with most often in this paper are binary numbers (integer or rational), and we will employ common mathematical notation rather than the formal conventions used in [8]: in particular, we will typically denote numbers by lowercase letters (conversely, we will occasionally denote unary numbers by capital letters), and we will write x_i for the ith member of a sequence x (which may be a constant-length tuple, a variable-length finite sequence encoded by a set as in Section 2, or an infinite sequence given by a TC^0 function with unary input i). We do not distinguish binary and unary numbers in notation; we will either explicitly mention which numbers are unary, or it will be assumed from the context: unary natural numbers appear as indices and lengths of sequences, as powering exponents, and as bound variables in iterated sums $\sum_{i=0}^{n} x_i$ and products $\prod_{i=0}^{n} x_i$.

By Theorem 3.2, we can use $L_{\overline{VTC^0+IMUL}}$-function symbols (i.e., TC^0 algorithms) freely in the arguments. In particular, we can use basic arithmetic operations on integers, including iterated sums and products. Iterated sums satisfy the recursive identities

$$\sum_{i<0} x_0 = 0,$$
$$\sum_{i<n+1} x_i = \sum_{i<n} x_i + x_n,$$

and other basic properties can be easily proved by induction, for example

$$\begin{aligned} \sum_{i<n}(x_i + y_i) &= \sum_{i<n} x_i + \sum_{i<n} y_i, \\ \sum_{i<n} y x_i &= y \sum_{i<n} x_i, \\ \sum_{i<n+m} x_i &= \sum_{i<n} x_i + \sum_{i<m} x_{n+i}. \end{aligned} \tag{2}$$

In particular, $VTC^0 + IMUL$ proves that if π is a permutation of $\{0, \dots, n-1\}$, then

$$\sum_{i<n} x_i = \sum_{i<n} x_{\pi(i)}. \tag{3}$$

(In order to see this, show $\sum_{i<m} x_i = \sum_{i<n} x_{\pi(i)}[\pi(i) < m]$ by induction on $m \le n$ using (2), where $[\cdots]$ denotes the Iverson bracket.) This allows us to make sense of more general sums $\sum_{i\in I} x_i$ where the indices run over a TC^0-definable collection of objects (e.g., tuples of unary numbers) that can be enumerated by a subset of some $\{0, \dots, n-1\}$; the identity (3) shows that the value of such a sum is independent of the enumeration. For example, we can write

$$f(n) = \sum_{i+j=n} x_{i,j},$$

meaning a sum over all pairs of numbers $\langle i, j\rangle$ such that $i + j = n$. We can also prove the double counting identity

$$\sum_{i<n}\sum_{j<m} x_{i,j} = \sum_{\substack{i<n \\ j<m}} x_{i,j} = \sum_{j<m}\sum_{i<n} x_{i,j} \tag{4}$$

by first showing $\sum_{i<n}\sum_{j<m} x_{i,j} = \sum_{k<nm} x_{\lfloor k/m\rfloor, k \bmod m}$ by induction on n using (2), and then (3) implies that other enumerations of the same set of pairs give the same result. Likewise, we can show

$$\Big(\sum_{i<n} x_i\Big)\Big(\sum_{i<m} y_i\Big) = \sum_{\substack{i<n \\ j<m}} x_i y_j. \tag{5}$$

Iterated products can be treated the same way as sums, mutatis mutandis.

Rational numbers can be represented in $VTC^0 + IMUL$ as pairs of integers standing for fractions a/b, where $b > 0$. We will not assume fractions to be reduced, as we cannot compute integer gcd. Arithmetic operations can be extended to rational numbers in $VTC^0 + IMUL$ in the obvious way, for example

$$\sum_{i<n} \frac{a_i}{b_i} := \frac{\sum_{i<n} a_i \prod_{j \neq i} b_j}{\prod_{i<n} b_i}.$$

$VTC^0 + IMUL$ knows the rationals form an ordered field, being the fraction field of a DOR. The properties of iterated sums and products we established above for integers also hold for rationals.

Using iterated products, we can define factorials and binomial coefficients

$$n! = \prod_{i=1}^{n} i, \qquad \binom{n}{m} = \frac{n!}{m!(n-m)!}$$

for unary natural numbers $n \geq m$. A priori, $n!$ is a binary integer, and $\binom{n}{m}$ a binary rational; however, the definition easily implies the identities

$$\binom{n}{0} = \binom{n}{n} = 0, \qquad \binom{n+1}{m+1} = \binom{n}{m} + \binom{n}{m+1},$$

from which one can show by induction on n that $\binom{n}{m}$ is an integer for all $m \leq n$. We can also prove by induction on n the binomial formula

$$(x+y)^n = \sum_{i \leq n} \binom{n}{i} x^i y^{n-i}$$

for rational x, y. More generally, we can define the multinomial coefficients

$$\binom{n}{n_1, \dots, n_d} = \frac{n!}{n_1! \cdots n_d!} = \binom{n}{n_1} \binom{n - n_1}{n_2} \cdots \binom{n - n_1 - \cdots - n_{d-1}}{n_d}$$

for a standard constant d and unary $n = n_1 + \cdots + n_d$, and we can prove the multinomial formula

$$(x_1 + \cdots + x_d)^n = \sum_{n_1 + \cdots + n_d = n} \binom{n}{n_1, \dots, n_d} x_1^{n_1} \cdots x_d^{n_d} \tag{6}$$

by metainduction on d.

5 Lagrange inversion formula

The Lagrange inversion formula (LIF) is an expression for the coefficients of the (compositional) inverse $g = f^{-1}$ of a power series f. In this section, we will formalize in $VTC^0 + IMUL$ variants of LIF for the special case where f is a constant-degree polynomial; we first show that g inverts f as a formal power series, and then with the help of a suitable bound on the coefficients of g, we show that the series $g(w)$ is convergent for small enough w; this means that under some restrictions, partial sums of $g(-a_0)$ approximate a root of the polynomial $f(x) + a_0$.

LIF, specifically the equivalent identity (9), has a simple combinatorial interpretation in terms of trees which allows for a straightforward bijective proof. However, this proof relies on exact counting of exponentially many objects, and as such it cannot be formalized in $VTC^0 + IMUL$. In contrast, the inductive proof we give below proceeds by low-level manipulations of sums and products; while it lacks conceptual clarity, it is elementary enough to go through in our weak theory.

We introduce some notation for convenience. Let us fix a standard constant $d \geq 1$. We are going to work extensively with sequences $m = \langle m_2, \dots, m_d \rangle$ of length $d-1$ of unary nonnegative integers. We will use subscripts $i = 2, \dots, d$ to extract elements of the sequence as indicated, and we will employ superscripts (and primes) to label various sequences used at the same time; these do not denote exponentiation. If m^1 and m^2 are two such sequences, we define $m^1 + m^2$ and $m^1 - m^2$ coordinatewise (i.e., $(m^1 + m^2)_i = m^1_i + m^2_i$), we write $m^1 \leq m^2$ if $m^1_i \leq m^2_i$ for all $i = 2, \dots, d$, and $m^1 \lneq m^2$ if $m^1 \leq m^2$ and $m^1 \neq m^2$. We define the generalized Catalan numbers

$$C_m = \frac{\left(\sum_{i=2}^d i m_i\right)!}{\left(\sum_{i=2}^d (i-1) m_i + 1\right)! \prod_{i=2}^d m_i!}.$$

Theorem 5.1 *$VTC^0 + IMUL$ proves the following for every constant $d \geq 1$: let*

$$f(x) = x + \sum_{k=2}^d a_k x^k$$

be a rational polynomial, and let

$$g(w) = \sum_{n=1}^\infty b_n w^n$$

be the formal power series (with unary indices) defined by

$$b_n = \sum_{\sum_i (i-1) m_i = n-1} C_m \prod_{i=2}^d (-a_i)^{m_i}. \tag{7}$$

Then $f(g(w)) = w$ as formal power series.

Remark 5.2 The sum in (7) runs over sequences $m = \langle m_2, \dots, m_d \rangle$ satisfying the constraint $\sum_{i=2}^d (i-1) m_i = n-1$; since this implies $m_2, \dots, m_d < n$, there are at most n^{d-1} such sequences, hence the sum makes sense in $VTC^0 + IMUL$.

The power series identity $f(g(w)) = w$ in the conclusion of the theorem amounts to $b_1 = 1$, and the recurrence

$$b_n = \sum_{k=2}^d (-a_k) \sum_{n_1 + \dots + n_k = n} b_{n_1} \cdots b_{n_k} \qquad (n > 1). \tag{8}$$

Rather than developing a general theory of formal power series in $VTC^0 + IMUL$, we take this as a *definition* of $f(g(w)) = w$.

Proof: After plugging in the definition of b_n, both sides of (8) can be written as polynomials in $-a_2, \dots, -a_d$ with rational (actually, integer) coefficients by several applications of (5). Moreover, b_{n_j} contains only monomials $\prod_i (-a_i)^{m_i^j}$ with $\sum_i (i-1) m_i^j = n_j - 1$. Thus, the right-hand side contains monomials $\prod_i (-a_i)^{m_i}$ with $m_i = \sum_j m_i^j + \delta_i^k$, where δ_i^k is Kronecker's delta. We have $\sum_i (i-1) m_i = \sum_{i,j} (i-1) m_i^j + k - 1 = \sum_j (n_j - 1) + k - 1 = n - 1$, which is the same constraint as on the left-hand side. In order to prove (8), it thus suffices to show that the coefficients of the monomials $\prod_i (-a_i)^{m_i}$ satisfying $\sum_i (i-1) m_i = n-1$ are the same on both sides of (8). This is easily seen to be equivalent to the following identity for every sequence m:

$$C_m = \sum_{k=2}^{d} \sum_{m^1 + \dots + m^k = m - \delta^k} C_{m^1} \cdots C_{m^k} \qquad (m \neq \vec{0}). \tag{9}$$

(Here, we treat Kronecker's delta as the sequence $\delta^k = \langle \delta_2^k, \dots, \delta_d^k \rangle$.) We will prove (9) by induction on $\sum_i m_i$, simultaneously with the identities

$$\sum_{m' + m'' = m} \bigl(\textstyle\sum_i (i-1) m'_i + 1\bigr) C_{m'} C_{m''} = \bigl(\textstyle\sum_i i m_i + 1\bigr) C_m, \tag{10}$$

$$\sum_{m^1 + \dots + m^k = m} C_{m^1} \cdots C_{m^k} = \frac{\bigl(\sum_i i m_i + k - 1\bigr)!\, k}{\bigl(\sum_i (i-1) m_i + k\bigr)! \prod_i m_i!} \qquad (k = 1, \dots, d). \tag{11}$$

The reader may find it helpful to consider the following combinatorial explanation of the identities, even though it cannot be expressed in $VTC^0 + IMUL$. First, C_m counts the number of ordered rooted trees with $m_2, \dots, m_d$ nodes of out-degree $2, \dots, d$, respectively, and the appropriate number (i.e., $\sum_i (i-1) m_i + 1$) of leaves. Indeed, such a tree can be uniquely described by the sequence of out-degrees of its nodes in preorder. One checks easily that every string with $m_2, \dots, m_d$ occurrences of $2, \dots, d$, resp., and $\sum_i (i-1) m_i + 1$ occurrences of 0, has a unique cyclic shift that is a valid representation of a tree, so there are

$$\frac{1}{\sum_i i m_i + 1} \binom{\sum_i i m_i + 1}{\sum_i (i-1) m_i + 1, m_2, \dots, m_d} = C_m$$

such trees. The left-hand side of (11) thus counts k-tuples of trees with a prescribed total number of nodes of out-degree $2, \dots, d$; a similar argument as above shows their number equals the right-hand side (every string with the appropriate number of symbols of each kind has exactly k cyclic shifts that are concatenations of representations of k trees). The main identity (9) expresses that a tree with more than one node can be uniquely decomposed as a root of out-degree $k = 2, \dots, d$ followed by a k-tuple of trees. Finally, (10) expresses that a pair of trees t', t'' together with a distinguished leaf x of t' uniquely represent a tree t with a distinguished node x, namely the tree obtained by identifying the root of t'' with x.

Let us proceed with the formal proof by induction. Assume that (9), (10), and (11) hold for all m' such that $m' \lneq m$, we will prove them for m.

(9): If $m \neq \vec{0}$, we have

$$\sum_{k=2}^{d} \sum_{m^1+\cdots+m^k=m-\delta^k} C_{m^1}\cdots C_{m^k} = \sum_{\substack{k=2\\ m_k>0}}^{d} \frac{\left(\sum_i im_i - 1\right)!\, k}{\left(\sum_i (i-1)m_i + 1\right)! \prod_{i\neq k} m_i!\,(m_k-1)!}$$

$$= \frac{\left(\sum_i im_i - 1\right)!}{\left(\sum_i (i-1)m_i + 1\right)! \prod_i m_i!} \sum_{\substack{k=2\\ m_k>0}}^{d} km_k$$

$$= \frac{\left(\sum_i im_i\right)!}{\left(\sum_i (i-1)m_i + 1\right)! \prod_i m_i!} = C_m,$$

using (11) for $m - \delta^k \lneq m$.

(10): If $m = \vec{0}$, the statement holds. Otherwise, we have

$$\left(\sum_i im_i + 1\right)C_m$$

$$= C_m + \left(\sum_i im_i\right) \sum_{k=2}^{d} \sum_{m^1+\cdots+m^k=m-\delta^k} C_{m^1}\cdots C_{m^k}$$

$$= C_m + \sum_{k=2}^{d} \sum_{m^1+\cdots+m^k=m-\delta^k} \sum_{j=1}^{k} \left(\sum_i im_i^j + 1\right) C_{m^1}\cdots C_{m^k}$$

$$= C_m + \sum_{k=2}^{d} k \sum_{m^1+\cdots+m^k=m-\delta^k} \left(\sum_i im_i^k + 1\right) C_{m^1}\cdots C_{m^k} \tag{12}$$

$$= C_m + \sum_{k=2}^{d} k \sum_{m^1+\cdots+m^k+m''=m-\delta^k} \left(\sum_i (i-1)m_i^k + 1\right) C_{m^1}\cdots C_{m^k} C_{m''}$$

$$= C_m + \sum_{\substack{m'+m''=m\\ m'\neq\vec{0}}} C_{m''} \sum_{k=2}^{d} k \sum_{m^1+\cdots+m^k=m'-\delta^k} \left(\sum_i (i-1)m_i^k + 1\right) C_{m^1}\cdots C_{m^k}$$

$$= C_m + \sum_{\substack{m'+m''=m\\ m'\neq\vec{0}}} C_{m''} \sum_{k=2}^{d} \sum_{m^1+\cdots+m^k=m'-\delta^k} \sum_{j=1}^{k} \left(\sum_i (i-1)m_i^j + 1\right) C_{m^1}\cdots C_{m^k} \tag{13}$$

$$= C_m + \sum_{\substack{m'+m''=m\\ m'\neq\vec{0}}} C_{m''} \sum_{k=2}^{d} \sum_{m^1+\cdots+m^k=m'-\delta^k} \left(\sum_i (i-1)m'_i + 1\right) C_{m^1}\cdots C_{m^k}$$

$$= C_m + \sum_{\substack{m'+m''=m\\ m'\neq\vec{0}}} \left(\sum_i (i-1)m'_i + 1\right) C_{m''} C_{m'}$$

$$= \sum_{m'+m''=m} \left(\sum_i (i-1)m'_i + 1\right) C_{m'} C_{m''},$$

using (9) for m and $m' \leq m$, and (10) for $m^k \lneq m$. We derive line (12) by observing that the

k sums

$$\sum_{m^1+\dots+m^k=m-\delta^k} \bigl(\sum_i im_i^j + 1\bigr) C_{m^1} \cdots C_{m^k} \qquad (j = 1, \dots, k)$$

have the same value due to symmetry (i.e., by an application of (3)). Line (13) is similar.

(11): By metainduction on $k = 1, \dots, d$. The case $k = 1$ is the definition of C_m. Assuming the statement holds for k, we prove it for $k+1$ from the identity

$$\begin{aligned}
k\bigl(\textstyle\sum_i (i-1)m_i + k + 1\bigr) &\sum_{m^1+\dots+m^{k+1}=m} C_{m^1} \cdots C_{m^{k+1}} \\
&= k \sum_{m^1+\dots+m^{k+1}=m} \sum_{j=1}^{k+1} \bigl(\textstyle\sum_i (i-1)m_i^j + 1\bigr) C_{m^1} \cdots C_{m^{k+1}} \\
&= k(k+1) \sum_{m^1+\dots+m^{k+1}=m} \bigl(\textstyle\sum_i (i-1)m_i^{k+1} + 1\bigr) C_{m^1} \cdots C_{m^{k+1}} \\
&= k(k+1) \sum_{m^1+\dots+m^k=m} C_{m^1} \cdots C_{m^{k-1}} \sum_{m'+m''=m^k} \bigl(\textstyle\sum_i (i-1)m'_i + 1\bigr) C_{m'} C_{m''} \\
&= k(k+1) \sum_{m^1+\dots+m^k=m} \bigl(\textstyle\sum_i im_i^k + 1\bigr) C_{m^1} \cdots C_{m^k} \\
&= (k+1) \sum_{m^1+\dots+m^k=m} \sum_{j=1}^{k} \bigl(\textstyle\sum_i im_i^j + 1\bigr) C_{m^1} \cdots C_{m^k} \\
&= (k+1)\bigl(\textstyle\sum_i im_i + k\bigr) \sum_{m^1+\dots+m^k=m} C_{m^1} \cdots C_{m^k}
\end{aligned}$$

using (10) for $m^k \le m$. □

Lemma 5.3 *$VTC^0 + IMUL$ proves: let f, g be as in Theorem 5.1, and $a = \max\bigl\{1, \sum_i |a_i|\bigr\}$. Then $|b_n| \le (4a)^{n-1}$ for every n.*

Proof: We can estimate

$$\begin{aligned}
|b_n| &\le a^{n-1} \sum_{\sum_i (i-1)m_i = n-1} C_m \prod_{i=2}^{d} \bigl(a^{1-i}|a_i|\bigr)^{m_i} \\
&= \frac{a^{n-1}}{n} \sum_{\sum_i (i-1)m_i = n-1} \binom{n-1+\sum_i m_i}{n-1, m_2, \dots, m_d} \prod_{i=2}^{d} \bigl(a^{1-i}|a_i|\bigr)^{m_i} \\
&\le \frac{a^{n-1}}{n} \sum_{t=n-1}^{2(n-1)} \sum_{s+\sum_i m_i = t} \binom{t}{s, m_2, \dots, m_d} \prod_{i=2}^{d} \bigl(a^{-1}|a_i|\bigr)^{m_i} \\
&= \frac{a^{n-1}}{n} \sum_{t=n-1}^{2(n-1)} \Bigl(1 + a^{-1} \sum_{i=2}^{d} |a_i|\Bigr)^t \\
&\le a^{n-1} \Bigl(1 + a^{-1} \sum_{i=2}^{d} |a_i|\Bigr)^{2(n-1)} \le a^{n-1} 2^{2(n-1)}
\end{aligned}$$

using the multinomial formula (6). □

Example 5.4 The bound in Lemma 5.3 is reasonably tight even in the "real world". Let $a > 0$ be a real number, and put $f(x) = x - ax^2$. Then g is its inverse function $g(w) = (1 - \sqrt{1 - 4aw})/2a$, whose radius of convergence is the modulus of the nearest singularity, namely $1/4a$. Thus, for every $\varepsilon > 0$, $|b_n| \geq (4a - \varepsilon)^n$ for infinitely many n. In fact, the Stirling approximation for Catalan numbers gives $b_n = \Theta\big((4a)^n n^{-3/2}\big)$.

Theorem 5.5 *$VTC^0 + IMUL$ proves the following for every constant $d \geq 1$. Let $h(x) = \sum_{i=0}^{d} a_i x^i$ be a rational polynomial with linear coefficient $a_1 = 1$. Put $f = h - a_0$, let g and b_n be as in Theorem* 5.1*, $a = \max\big\{1, \sum_{i=2}^{d} |a_i|\big\}$, $\alpha = 4a|a_0|$, and let*

$$x_N = \sum_{n=1}^{N} b_n (-a_0)^n$$

denote the Nth partial sum of $g(-a_0)$ for every unary natural number N. If

$$|a_0| < \frac{1}{4a},$$

then

$$|x_N| \leq \frac{|a_0|}{1 - \alpha}, \tag{14}$$

$$|x_N - x_M| \leq \frac{|a_0|\alpha^{N-1}}{1 - \alpha}, \tag{15}$$

$$|h(x_N)| \leq N^d |a_0| \alpha^N \tag{16}$$

for every unary $M \geq N \geq 1$.

Proof: Lemma 5.3 gives

$$|x_N| \leq \sum_{n=1}^{N} |a_0|^n (4a)^{n-1} = |a_0| \sum_{n=0}^{N-1} \alpha^n \leq \frac{|a_0|}{1 - \alpha}.$$

The proof of (15) is similar. As for (16), we have

$$\begin{aligned} h(x_N) &= a_0 + \sum_{k=1}^{d} a_k \sum_{n_1, \dots, n_k = 1}^{N} b_{n_1} \cdots b_{n_k} (-a_0)^{n_1 + \dots + n_k} \\ &= \sum_{k=1}^{d} a_k \sum_{\substack{n_1, \dots, n_k = 1 \\ n_1 + \dots + n_k > N}}^{N} b_{n_1} \cdots b_{n_k} (-a_0)^{n_1 + \dots + n_k}, \end{aligned} \tag{17}$$

as

$$\sum_{k=1}^{d} a_k \sum_{n_1 + \dots + n_k = n} b_{n_1} \cdots b_{n_k} = \delta_n^1$$

for all $n \leq N$ by Theorem 5.1. Note that the inner sum in (17) is empty for $k = 1$, thus

$$\begin{aligned} |h(x_N)| &\leq \sum_{k=2}^{d} |a_k| \sum_{\substack{n_1,\dots,n_k=1 \\ n_1+\dots+n_k>N}}^{N} (4a)^{-k} \big(4a|a_0|\big)^{n_1+\dots+n_k} \\ &\leq \sum_{k=2}^{d} |a_k| \left(\frac{N}{4a}\right)^k \alpha^{N+1} \\ &\leq a \max\left\{\frac{N^2}{(4a)^2}, \frac{N^d}{(4a)^d}\right\} \alpha^{N+1} \\ &\leq \max\left\{\frac{N^2}{4}, \frac{N^d}{4^{d-1}}\right\} |a_0| \alpha^N \leq N^d |a_0| \alpha^N, \end{aligned}$$

using Lemma 5.3 and $a \geq 1$. □

Intuitively, the conclusion of Theorem 5.5 says that x_N is a Cauchy sequence with an explicit modulus of convergence whose limit is a root of h of bounded modulus.

6 Valued fields

Theorem 5.5 shows that $VTC^0 + IMUL$ can compute roots of polynomials of a special form, however it would still be rather difficult to extend it to a full-blown root-finding algorithm. We will instead give a model-theoretic argument using well-known properties of valued fields to bridge the gap between Theorem 5.5 and approximation of roots of general polynomials.

In order to prove $VTC^0 + IMUL \vdash IOpen$, it suffices to show that every model of $VTC^0 + IMUL$ is a model of $IOpen$. First, since $VTC^0 + IMUL \vdash DIV$, we can reformulate Theorem 2.1 in terms of fields.

Lemma 6.1 *Let D be a DOR, and F its fraction field. The following are equivalent.*

(i) $D \vDash IOpen$.

(ii) $D \vDash DIV$*, and F is a dense subfield of a RCF R.* □

The condition that F is dense in R means that elements of R can be well approximated in F, i.e., R cannot be too large, while the condition that R is real-closed (or at least contains the real closure $\tilde{F}^{\mathrm{real}}$) means that R cannot be too small, so these two conditions work against each other. One canonical choice of R is the smallest RCF extending F, i.e., $\tilde{F}^{\mathrm{real}}$. We obtain that a DOR $D \vDash DIV$ is a model of $IOpen$ iff F is dense in $\tilde{F}^{\mathrm{real}}$. However, it will be useful for us to consider another choice: it turns out that there exists the largest ordered field extension $\hat{F} \supseteq F$ in which F is dense, and a DOR $D \vDash DIV$ is a model of $IOpen$ iff $\hat{F}$ is real-closed.

The existence of $\hat{F}$ was shown by Scott [28]. One way to prove it is by generalization of the construction of $\mathbb{R}$ using Dedekind cuts. Consider pairs $\langle A, B\rangle$, where $F = A \cup B$, B has no smallest element, and

$$\inf\{b - a : a \in A, b \in B\} = 0.$$

One can show that the collection of all such cuts can be given the structure of an ordered field in a natural way, and it has the property needed of $\hat{F}$. However, we will use a different construction of $\hat{F}$ which may look more complicated on first sight, but has the advantage of allowing us to employ tools from the theory of valuations to explore its properties (such as being real-closed). It can be thought of as generalizing the construction of $\mathbb{R}$ by means of Cauchy sequences.

We refer the reader to [9] for the theory of valued fields, however we will review our notation and some basic facts below to make sure we are on the same page.

A *valuation* on a field K is a surjective mapping $v\colon K \twoheadrightarrow \Gamma \cup \{\infty\}$, where $\langle \Gamma, +, \leq \rangle$ is a totally ordered abelian group (called the *value group*), and v satisfies

(i) $v(a) = \infty$ only if $a = 0$,

(ii) $v(ab) = v(a) + v(b)$,

(iii) $v(a + b) = \min\{v(a), v(b)\}$,

where we put $\infty + \gamma = \gamma + \infty = \infty$ and $\gamma \leq \infty$ for every $\gamma \in \Gamma$. (Elements with large valuation should be thought of as being small; the order is upside down for historical reasons.) Valuations $v\colon K \to \Gamma \cup \{\infty\}$, $v'\colon K \to \Gamma' \cup \{\infty\}$ are *equivalent* if there is an ordered group isomorphism $f\colon \Gamma \to \Gamma'$ such that $v' = f \circ v$.

The *valuation ring* of v is

$$O = \{a \in K : v(a) \geq 0\},$$

with its unique *maximal ideal* being

$$I = \{a \in K : v(a) > 0\}.$$

The quotient field $k = O/I$ is called the *residue field*. If $a \in O$, we will denote its image under the natural projection $O \to k$ as $\overline{a}$.

More abstractly, a valuation ring for a field K is a subring $O \subseteq K$ such that $a \in O$ or $a^{-1} \in O$ for every $a \in K^\times$. Any such ring corresponds to a valuation: we take $\Gamma = K^\times/O^\times$ ordered by $aO^\times \leq bO^\times$ iff $b \in aO$, and define v as the natural projection $v(a) = aO^\times$. A valuation is determined uniquely up to equivalence by its valuation ring; thus, either of the structures $\langle K, v\rangle$ and $\langle K, O\rangle$ can be called a *valued field*. A valued field $\langle K', v'\rangle$ is an *extension* of $\langle K, v\rangle$ if K is a subfield of K', and $v \subseteq v'$. (In terms of valuation rings, the latter means $O = O' \cap K$.) A valuation (or valuation ring or valued field) is *nontrivial* if $\Gamma \neq \{0\}$, or equivalently, if $O \neq K$.

A valuation $v\colon K \to \Gamma \cup \{\infty\}$ induces a *topology* on K with basic open sets

$$B(a, \gamma) = \{b \in K : v(b - a) > \gamma\}, \qquad a \in K, \gamma \in \Gamma.$$

(Note that $B(a, \gamma) = B(a', \gamma)$ for any $a' \in B(a, \gamma)$.) This makes K a topological field, and as with any topological group, it also makes K a uniform space (with a fundamental system of entourages of the form $\{\langle a, b\rangle \in K^2 : v(a - b) > \gamma\}$ for $\gamma \in \Gamma$). Consequently, we have the notions of Cauchy nets, completeness, and completion; for the particular case of valued fields, they can be stated as follows. A *Cauchy sequence* in K is $\{a_\gamma : \gamma \in \Gamma\} \subseteq K$ such that $v(a_\gamma - a_\delta) > \min\{\gamma, \delta\}$ for every $\gamma, \delta \in \Gamma$. (Alternatively, it would be enough if Cauchy sequences were indexed over a cofinal subset of Γ.) Such a sequence converges to $a \in K$ if $v(a - a_\gamma) > \gamma$ for every $\gamma \in \Gamma$. The valued field $\langle K, v\rangle$ is *complete* if every Cauchy sequence in K converges. A *completion* of $\langle K, v\rangle$ is an extension $\langle \hat{K}, \hat{v}\rangle$ of $\langle K, v\rangle$ which is a complete valued field such that K is (topologically) dense in $\hat{K}$. (The last condition implies that $\hat{K}$ is an *immediate* extension of K, i.e., the natural embeddings $\Gamma \subseteq \hat{\Gamma}$ and $k \subseteq \hat{k}$ are isomorphisms.)

Theorem 6.2 ([9, Thm.2.4.3]) *Every valued field $\langle K, v\rangle$ has a completion, which is unique up to a unique valued field isomorphism identical on K.* □

Now we turn to the interaction of valuation and order [9, §2.2.2]. Let $\langle K, O\rangle$ be a valued field. If $\leq$ is an order on K (i.e., $\langle K, \leq\rangle$ is an ordered field) such that O is *convex* (i.e., $a \leq b \leq c$ and $a, c \in O$ implies $b \in O$), then an order is induced on the residue field k by $\bar{a} \leq \bar{b} \Leftrightarrow a \leq b$. Conversely, any order on k is induced from an order $\leq$ on K making O convex in this way. If Γ is 2-divisible, such a $\leq$ is unique, and can be defined explicitly by

$$a > 0 \quad \text{iff} \quad \exists b \in K\, (ab^2 \in O^\times \wedge \overline{ab^2} > 0).$$

In general, the structure of all such orders $\leq$ is described by the Baer–Krull theorem [9, Thm. 2.2.5]. Notice also that every convex subring of an ordered field is a valuation ring.

Lemma 6.3 *If $\langle K, \leq\rangle$ is an ordered field, and O a nontrivial convex subring of K, then the valuation topology on K coincides with the interval topology. In particular, a subset $X \subseteq K$ is topologically dense iff it is order-theoretically dense.*

Proof: The convexity of O implies that every $B(a, \gamma)$ is also convex. If $c \in (a, b)$, and $\gamma \geq v(c - a), v(c - b)$, then $c \in B(c, \gamma) \subseteq (a, b)$. On the other hand, if $c \in B(a, \gamma)$, pick $e > 0$ with $v(e) > \gamma$ (which exists as the valuation is nontrivial). Then $c \in (c - e, c + e) \subseteq B(a, \gamma)$. □

For any ordered field $\langle K, \leq\rangle$, the set of its bounded elements

$$O = \{a \in K : \exists q \in \mathbb{Q}^+\, (-q \leq a \leq q)\}$$

is a convex valuation ring for K with the set of infinitesimal elements

$$I = \{a \in K : \forall q \in \mathbb{Q}^+\, (-q \leq a \leq q)\}$$

being its maximal ideal. The corresponding valuation is the *natural valuation* induced by $\leq$. The residue field is an archimedean ordered field, and as such it can be uniquely identified with a subfield $k \subseteq \mathbb{R}$. Here is the promised construction of the largest dense extension of an ordered field.

Lemma 6.4 *Let $\langle K, \leq\rangle$ be a nonarchimedean ordered field, v its natural valuation, and $\langle \hat{K}, \hat{v}\rangle$ its completion. There is a unique order on $\hat{K}$ extending $\leq$ that makes $\hat{O}$ convex. Its natural valuation is $\hat{v}$, and it satisfies:*

(*i*) *$\hat{K}$ is an ordered field extension of K such that K is dense in $\hat{K}$.*

(*ii*) *If K' is any ordered field extension of K in which K is dense, there is a unique ordered field embedding of K' in $\hat{K}$ identical on K.*

Proof: Since $\hat{K}$ is an immediate extension of K, for every $a \in \hat{K}^\times$ there exists an $a_0 \in K^\times$ such that $aa_0^{-1} \in 1 + \hat{I}$, or equivalently, $\hat{v}(a - a_0) > \hat{v}(a) = v(a_0)$. Any order $\hat{\leq}$ on $\hat{K}$ extending $\leq$ such that $\hat{O}$ is convex (which implies $1 + \hat{I} \subseteq \hat{K}^+$) must satisfy

$$(18) \qquad a \mathrel{\hat{>}} 0 \quad \text{iff} \quad a_0 > 0,$$

which specifies it uniquely. On the other hand, we claim that (18) defines an order on $\hat{K}$. First, the definition is independent of the choice of a_0: if $a_1 \in K^\times$ is such that $aa_1^{-1} \in 1 + \hat{I}$, then $a_0 a_1^{-1} \in 1 + I$ is positive, whence a_0 and a_1 have the same sign. Clearly, exactly one of a and $-a$ is positive for any $a \in \hat{K}^\times$. Let $a, b \in \hat{K}^\times$, $a, b \mathrel{\hat{>}} 0$. Since $(ab)(a_0 b_0)^{-1} \in 1 + \hat{I}$, we have $ab \mathrel{\hat{>}} 0$. Also, $v(a_0 + b_0) = \min\{v(a_0), v(b_0)\}$ as they have the same sign, thus

$$\hat{v}\big((a + b) - (a_0 + b_0)\big) \geq \min\{\hat{v}(a - a_0), \hat{v}(b - b_0)\} > \min\{v(a_0), v(b_0)\} = v(a_0 + b_0).$$

This means we can take $a_0 + b_0$ for $(a + b)_0$, showing that $a + b \mathrel{\hat{>}} 0$.

If $a \mathrel{\hat{<}} b \mathrel{\hat{<}} c$, $a, c \in \hat{O}$, we may assume $(c - a)_0 = (c - b)_0 + (b - a)_0$ by the argument above, hence $(c - b)_0 + (b - a)_0 \in O$. Since $(c - b)_0, (b - a)_0 > 0$, this implies $(b - a)_0 \in O$, hence $b - a \in \hat{O}$, and $b \in \hat{O}$. Thus, $\hat{O}$ is convex under $\hat{\leq}$.

Since $\langle K, \leq\rangle$ is nonarchimedean, the valuations v and $\hat{v}$ are nontrivial. Thus, K is an order-theoretically dense subfield of $\hat{K}$ by Lemma 6.3, which shows (i). Also, in view of the convexity of $\hat{O}$, this implies that O is dense in $\hat{O}$, hence

$$\hat{O} = \{a \in \hat{K} : \exists q \in \mathbb{Q}^+ \, (-q \mathrel{\hat{\leq}} a \mathrel{\hat{\leq}} q)\},$$

i.e., $\hat{v}$ is the natural valuation of $\langle \hat{K}, \hat{\leq}\rangle$.

(ii): Let v' be the natural valuation on K', and $\langle \hat{K'}, \hat{v}'\rangle$ its completion. By Lemma 6.3, $\langle K, v\rangle$ is topologically dense in its complete extension $\langle \hat{K'}, \hat{v}'\rangle$, hence there is an isomorphism of $\langle \hat{K'}, \hat{v}'\rangle$ and $\langle \hat{K}, \hat{v}\rangle$ identical on K by Theorem 6.2. It restricts to an embedding $f \colon \langle K', v'\rangle \to \langle \hat{K}, \hat{v}\rangle$. For any $a \in K'$, we can see from (18) that $f(a) \mathrel{\hat{>}} 0$ implies $a_0 > 0$ for some $a_0 \in K^\times$ such that $aa_0^{-1} \in 1 + I'$, whence $a >' 0$. Thus, f is order-preserving. The uniqueness of f follows from the density of K in $\hat{K}$. □

(If K is archimedean, its natural valuation is trivial, hence the induced topology is discrete, and $\hat{K} = K$. However, the largest ordered field extension of K where K is dense is $\mathbb{R}$.)

We will rely on the following important characterization of real-closed fields in terms of valuations [9, Thm. 4.3.7].

Theorem 6.5 *Let $\langle K, \leq\rangle$ be an ordered field, and O a convex valuation ring of K. The following are equivalent.*

(*i*) *K is real-closed.*

(*ii*) Γ *is divisible,* k *is real-closed, and* O *is henselian.* $\square$

There are many equivalent definitions of henselian valuation rings or valued fields (cf. [9, Thm. 4.1.3]). It will be most convenient for our purposes to adopt the following one: a valuation ring O or a valued field $\langle K, O\rangle$ is *henselian* iff every polynomial $h(x) = \sum_{i=0}^{d} a_i x^i \in O[x]$ such that $a_0 \in I$ and $a_1 = 1$ has a root in I.

The basic intuition behind Theorem 6.5 is that in order to find a root a of a polynomial in K, we use the divisibility of Γ to get a ballpark estimate of a, we refine it to an approximation up to an infinitesimal relative error using the real-closedness of k, and then use the henselian property to compute a. Complications arise from interference with other roots of the polynomial.

It is well known that the completion of a henselian valued field is henselian. In fact, we have the following simple criterion, where we define a valued field $\langle K, O\rangle$ to be *almost henselian* if for every polynomial h as above, and every $\gamma \in \Gamma$, there is $a \in I$ such that $v(h(a)) > \gamma$. (Equivalently, $\langle K, O\rangle$ is almost henselian iff the quotient ring O/P is henselian for every nonzero prime ideal $P \subseteq O$ [31].)

Lemma 6.6 *The completion* $\langle \hat{K}, \hat{v}\rangle$ *is henselian iff* $\langle K, v\rangle$ *is almost henselian.*

Proof: First, we observe that if $h = \sum_{i=0}^{d} a_i x^i \in O[x]$ has $a_1 = 1$, then

$$v(h(b) - h(c)) = v(b - c) \tag{19}$$

for any $b, c \in I$. Indeed, if $b \neq c$, we have

$$\frac{h(b) - h(c)}{b - c} = a_1 + \sum_{i=2}^{d} a_i (b^{i-1} + b^{i-2}c + \cdots + c^{i-1}) \in 1 + I \subseteq O^{\times}.$$

Left to right: assume that $h = \sum_{i=0}^{d} a_i x^i \in O[x]$, $a_1 = 1$, $a_0 \in I$, and $\gamma \in \Gamma$. Without loss of generality, $\gamma \geq 0$. Since $\hat{K}$ is henselian, there is $\hat{a} \in \hat{I}$ such that $h(\hat{a}) = 0$. By the density of K in $\hat{K}$, we can find $a \in K$ such that $\hat{v}(a - \hat{a}) > \gamma$. Then $a \in I$, and $v(h(a)) > \gamma$ by (19).

Right to left: let $h = \sum_{i=0}^{d} a_i x^i \in \hat{O}[x]$ with $a_1 = 1$ and $a_0 \in \hat{I}$. For any $\gamma \in \Gamma$, $\gamma \geq 0$, we choose $a_{i,\gamma} \in K$ such that $\hat{v}(a_i - a_{i,\gamma}) > \gamma$, and put $h_\gamma = \sum_i a_{i,\gamma} x^i$. Then $h_\gamma \in O[x]$, $a_{0,\gamma} \in I$, and we could have picked $a_{1,\gamma} = 1$, hence by assumption, there is $b_\gamma \in I$ such that $v(h_\gamma(b_\gamma)) > \gamma$. By the choice of h_γ, this implies $\hat{v}(h(b_\gamma)) > \gamma$. Moreover, $v(b_\gamma - b_\delta) = \hat{v}(h(b_\gamma) - h(b_\delta)) > \min\{\gamma, \delta\}$ by (19), hence $\{b_\gamma : \gamma \geq 0\}$ is a Cauchy sequence. Since $\hat{K}$ is complete, there is $b \in \hat{K}$ such that $\hat{v}(b - b_\gamma) > \gamma$ for every γ. Then $b \in \hat{I}$. Since $\hat{v}(h(b) - h(b_\gamma)) > \gamma$ by (19), we have $\hat{v}(h(b)) > \gamma$ for every $\gamma \in \Gamma$, i.e., $h(b) = 0$. $\square$

Putting all the things together, we obtain the following characterization of open induction. We note that the fact that the completion of a real-closed field is real-closed was shown by Scott [28].

Lemma 6.7 *Let* D *be a nonstandard DOR such that* $D \vDash \mathit{DIV}$*,* F *its fraction field endowed with its natural valuation, and* $\hat{F}$ *its completion. The following are equivalent.*

(*i*) $D \vDash IOpen$.

(*ii*) $\hat{F}$ *is real-closed.*

(*iii*) F *is almost henselian, its value group is divisible, and its residue field is real-closed.*

Proof: (ii) and (iii) are equivalent by Theorem 6.5 and Lemma 6.6, using the fact that $\hat{F}$ is an immediate extension of F.

(ii) $\to$ (i) follows from Lemma 6.1 as F is dense in $\hat{F}$. Conversely, assume that F is a dense subfield of a RCF R. By Theorem 6.5, R is henselian, its value group is divisible, and its residue field is a RCF. The completion $\hat{R}$ is also henselian by Lemma 6.6, and it has the same Γ and k as R, hence it is a RCF by Theorem 6.5. However, the density of F in $\hat{R}$ implies $\hat{F} \simeq \hat{R}$ by Lemma 6.4, hence $\hat{F}$ is a RCF. □

We remark that we could have used any nontrivial convex subring in place of the natural valuation in Lemma 6.4 (any two such valuations determine the same uniform structure by Lemma 6.3, which means that their completions are the same qua topological fields, and one checks easily that they also carry the same order). Likewise, Lemma 6.7 continues to hold when F is endowed with any nontrivial valuation with a convex valuation ring; this may make a difference for verification of condition (iii). Notice that such valuation rings correspond to proper cuts (in the models-of-arithmetic sense) on D closed under multiplication.

We can now prove the main result of this paper.

Theorem 6.8 *$VTC^0 + IMUL$ proves IOpen on binary integers.*

Proof: Let $M \vDash VTC^0 + IMUL$, and D be its ring of binary integers, we need to show that $D \vDash IOpen$. We may assume without loss of generality that M, and therefore D, is ω-saturated. Since $VTC^0 + IMUL \vdash DIV$, it suffices to check the conditions of Lemma 6.7 (iii).

As we have mentioned above, the residue field k of any ordered field under its natural valuation is a subfield of $\mathbb{R}$. The ω-saturation of D implies that every Dedekind cut on $\mathbb{Q}$ is realized by an element of F, hence in fact $k = \mathbb{R}$, which is a real-closed field.

Every element of the value group Γ is the difference of valuations of two (positive) elements of D. Let thus $a \in D^+$, and $k \in \mathbb{Z}^+$. Put $n = \|a\| - 1$, which is a unary integer of M such that $2^n \le a < 2^{n+1}$. Put $m = \lfloor n/k \rfloor$ and $b = 2^m$. Then $b^k \le a < 2^k b^k$, hence $kv(b) = v(a)$. This shows that Γ is divisible.

Let $\gamma \in \Gamma$, and $h(x) = \sum_{i \le d} a_i x^i \in F[x]$ be such that $v(a_i) \ge 0$, $v(a_0) > 0$, and $a_1 = 1$. Then $a = \max\{1, \sum_{i=2}^{d} |a_i|\}$ is bounded by a standard integer, whereas a_0 is infinitesimal, thus $\alpha = 4a|a_0|$ is also infinitesimal. Let N be a nonstandard unary integer of M such that $v(2^{-N}) > \gamma$, and let x_N be as in Theorem 5.5. Then using a crude estimate,

$$|h(x_N)| \le N^d |a_0| \alpha^N \le 2^N 4^{-N} = 2^{-N},$$

which means that $v(h(x_N)) > \gamma$. Moreover, $|x_N| \le |a_0|/(1 - \alpha)$ is infinitesimal. Thus, F is almost henselian. □

As explained in Section 3, Theorem 6.8 implies that for any constant d, $VTC^0 + IMUL$ can formalize a TC^0 algorithm for approximation of roots of degree d rational polynomials. The reader might find it disappointing that we have shown its existence nonconstructively using the abstract nonsense from this section, so let us give at least a rough idea how this algorithm may actually look like; it is somewhat different from the one in [15].

Clearly, one ingredient is Theorem 5.5, which gives an explicit description of a TC^0 algorithm for approximation of roots of polynomials of a special form (small constant coefficient and large linear coefficient). The remaining part is a reduction of general root approximation to this special case, and this happens essentially in Theorem 6.5. This theorem has a proof with a fairly algorithmic flavour using Newton polygons (cf. [2, §2.6], where a similar argument is given in the special case of real Puiseux series). The Newton polygon of a polynomial $f(x) = \sum_{i=0}^{d} a_i x^i \in K[x]$ is the lower convex hull of the set of points $\{e_i = \langle i, v(a_i)\rangle : i = 0, \dots, d\} \subseteq \mathbb{Q} \times \Gamma$.

The basic idea is as follows. Take an edge of the Newton polygon with endpoints e_{i_0}, e_{i_1}. The slope of the edge is in Γ due to its divisibility, hence we can replace $f(x)$ by a suitable polynomial of the form $af(bx)$ to ensure $v(a_{i_0}) = v(a_{i_1}) = 0$. Then $f \in O[x]$, its image $\overline{f} \in k[x]$ has degree i_1, and the least exponent of its nonzero coefficient is i_0. If we find a nonzero root $\overline{a} \in k^\times$ of $\overline{f}$ of multiplicity m using the real-closedness of k, the Newton polygon of the shifted polynomial $f(x + a)$ will have an edge whose endpoints satisfy $i'_0 < i'_1 \leq m \leq i_1 - i_0$, since m is the least exponent with a nonzero coefficient in $\overline{f}(x+\overline{a})$. This is strictly shorter than the original edge unless $\overline{f}$ is a constant multiple of $x^{i_0}(x-\overline{a})^{i_1-i_0}$, which case has to be handled separately. If we set up the argument properly, we can reduce f by such linear substitutions in at most d steps into a polynomial whose Newton polygon has e_0, e_1 for vertices, and then we can apply the henselian property to find its root in K.

One can imagine that a proper TC^0 algorithm working over $\mathbb{Q}$ instead of a nonarchimedean field can be obtained along similar lines by replacing "infinitesimal" with a suitable notion of "small enough" (e.g., employing an approximation of $-\log|a|$ as a measure of magnitude in place of $v(a)$). However, the details are bound to be quite unsightly due to complications arising from the loss of the ultrametric inequality of v.

7 Application to Buss's theories

While $VTC^0 + IMUL$ does not stand much chance of proving induction for interesting classes of formulas with quantifiers in the language of ordered rings, we will show in this section that we can do better in the richer language $L_B = \langle 0, 1, +, \cdot, \leq, \#, |x|, \lfloor x/2 \rfloor\rangle$ of Buss's one-sorted theories of bounded arithmetic—$VTC^0 + IMUL$ proves the $RSUV$-translation of T^0_2, and even minimization for sharply bounded formulas (Σ^b_0-MIN). The main tool is a description of Σ^b_0-definable sets discovered by Mantzivis [23], whose variants were also given in [4, 20]: in essence, a Σ^b_0-definable subset of $[0, 2^n)$ can be written as a union of $n^{O(1)}$ intervals on each residue class modulo 2^c, where c is a standard constant. As we will see, this property can be formalized in $VTC^0 + IMUL$ using the provability of $IOpen$ for the base case of polynomial inequalities, and as a consequence, our theory proves minimization and induction for Σ^b_0

formulas. (We stress that as in the case of *IOpen*, these are minimization and induction over binary numbers. Despite the same name, the schemata denoted as *IND* and *MIN* in the two-sorted framework only correspond to *LIND* and minimization over lengths in Buss's language, respectively.) We will present the messier part of the argument as a normal form for Σ^b_0 formulas over a weak base theory, in the hope that this will make the result more reusable.

We will assume the reader is familiar with definitions of Buss's theories (see e.g. [5, 21]), in particular, with *BASIC*. Recall that a formula is sharply bounded if all its quantifiers are of the form $\exists x \leq |t|$ or $\forall x \leq |t|$. We reserve Σ^b_0 for the class of sharply bounded formulas of L_B, whereas sharply bounded formulas in an extended language $L_B \cup L'$ will be denoted $\Sigma^b_0(L')$. Let $BASIC^+$ denote the extension of Buss's *BASIC* by the axioms

$$x(yz) = (xy)z, \tag{20}$$

$$y \leq x \to \exists z\,(y + z = x), \tag{21}$$

$$u \leq |x| \to \exists y\,(|y| = u), \tag{22}$$

$$z < x \# y \to |z| \leq |x||y|, \tag{23}$$

$$|x| \leq x. \tag{24}$$

(The quantifiers in (21), (22) could be bounded by x, if desired.) On top of *BASIC*, axioms (20) and (21) imply the theory of nonnegative parts of discretely ordered rings, hence we can imagine the universe is extended with negative numbers in the usual fashion. In particular, we can work with integer polynomials. We introduce two extra functions by

$$\begin{aligned} x \dot{-} y = z \quad &\text{iff} \quad y + z = x \vee (x < y \wedge z = 0),\\ 2^{\min\{u,|x|\}} = z \quad &\text{iff} \quad z \# 1 = 2z \wedge \big((u \leq |x| \wedge |z| = u + 1) \vee (u > |x| \wedge |z| = |x| + 1)\big). \end{aligned}$$

$BASIC^+$ proves that $\dot{-}$ and $2^{\min\{u,|x|\}}$ are well-defined total functions. Notice that $BASIC^+$ is universally axiomatizable in a language with $\dot{-}$ and $2^{\min\{u,|x|\}}$. We will write 2^u for $2^{\min\{u,|x|\}}$ when a self-evident value of x such that $u \leq |x|$ can be inferred from the context (e.g., when u is a sharply bounded quantified variable).

If p is a polynomial with nonnegative integer coefficients, one can construct easily a term t such that $BASIC^+ \vdash p(|x_1|, \dots, |x_k|) \leq |t(\vec{x})|$. Conversely, one can check that $BASIC^+$ proves $|xy| \leq |x| + |y|$; together with other axioms, this implies that for every term t (even using $\dot{-}$ and $2^{\min\{u,|x|\}}$) there is a polynomial p such that $BASIC^+ \vdash |t(\vec{x})| \leq p(|\vec{x}|)$.

Lemma 7.1 *Let $\varphi(x_1, \dots, x_k)$ be a $\Sigma^b_0(\dot{-}, 2^{\min\{u,|x|\}})$ formula. Then $BASIC^+$ proves $\varphi(\vec{x})$ equivalent to a formula of the form*

$$\bigvee_{\sigma_1,\dots,\sigma_k < 2^c} \Big(\bigwedge_{i=1}^{k} (x_i \equiv \sigma_i \pmod{2^c}) \wedge Q_1 u_1 \leq p(|\vec{x}|) \cdots Q_l u_l \leq p(|\vec{x}|)\, f_{\vec{\sigma}}(x_1, \dots, x_k, u_1, \dots, u_l, 2^{u_1}, \dots, 2^{u_l}) \geq 0\Big),$$

where c is a constant, $Q_1, \dots, Q_l \in \{\exists, \forall\}$, p is a nonnegative integer polynomial, $x_i \equiv \sigma_i \pmod{2^c}$ stands for $x_i = \sigma_i + 2^c \lfloor \cdots \lfloor \lfloor x_i / \underbrace{2\rfloor/2\rfloor \cdots /2}_{c} \rfloor$, and $f_{\vec{\sigma}}$ is an integer polynomial.

Proof: Using the remark before the lemma, we can find a nonnegative integer polynomial p such that $p(|\vec{x}|)$ bounds the values of $|t|$ for every subterm $t(\vec{x},\vec{u})$ occurring in φ and all possible values of the quantified variables $\vec{u}$. Then we can rewrite φ in the form

$$Q_1 u_1 \leq p(|\vec{x}|) \cdots Q_l u_l \leq p(|\vec{x}|)\, \psi(\vec{x},\vec{u}),$$

where ψ is open. The next step is elimination of unwanted function symbols. Let $|t|$ be a subterm of ψ, and write $\psi(\vec{x},\vec{u}) = \psi'(\vec{x},\vec{u},|t|)$. Then $\psi(\vec{x},\vec{u})$ is equivalent to

$$\exists u \leq p(|\vec{x}|)\, (|t| = u \wedge \psi'(\vec{x},\vec{u},u)).$$

Using the axioms of *BASIC*$^+$ and the definition of 2^u, this is equivalent to

$$\exists u \leq p(|\vec{x}|)\, (\lfloor 2^u/2 \rfloor \leq t < 2^u \wedge \psi'(\vec{x},\vec{u},u)).$$

Likewise,

$$\psi(\vec{x},\vec{u},t \# s) \leftrightarrow \exists u,v,w \leq p(|\vec{x}|)\, (u = |t| \wedge v = |s| \wedge w = uv \wedge \psi(\vec{x},\vec{u},2^w)),$$
$$\psi(\vec{x},\vec{u},2^{\min\{t,|s|\}}) \leftrightarrow \exists u,v \leq p(|\vec{x}|)\, (u = |s| \wedge v = \min\{t,u\} \wedge \psi(\vec{x},\vec{u},2^v)),$$

where we further eliminate $|t|$ and $|s|$ as above, and $\min\{t,u\}$ in an obvious way. Applying successively these reductions, we can eventually write φ as

$$Q_1 u_1 \leq p(|\vec{x}|) \cdots Q_l u_l \leq p(|\vec{x}|)\, \psi(\vec{x},\vec{u},2^{\vec{u}}), \tag{25}$$

where ψ is an open formula in the language $\langle 0,1,+,\cdot,\dot{-},\lfloor x/2 \rfloor,\leq \rangle$.

Claim 1 *Let $t(\vec{x})$ be a $\langle 0,1,+,\cdot,\dot{-},\lfloor x/2 \rfloor \rangle$-term such that the nesting depth of $\lfloor x/2 \rfloor$ in t is c, and the number of occurrences of $\dot{-}$ is r. For every $\vec{\sigma} < 2^c$, there are integer polynomials $g_1,\dots,g_r$ and $\{f_{\vec{\alpha}} : \alpha_1,\dots,\alpha_r \in \{0,1\}\}$ such that BASIC$^+$ proves*

$$\bigwedge_{i=1}^{r} (g_i(\vec{x}) \geq 0)^{\alpha_i} \to t(2^c\vec{x} + \vec{\sigma}) = f_{\vec{\alpha}}(\vec{x}), \tag{26}$$

where $\varphi^1 = \varphi$, $\varphi^0 = \neg\varphi$.

Proof: By induction on the complexity of t. For example, assume (26) holds for t, and consider the term $\lfloor t/2 \rfloor$. Let $\vec{\tau} < 2$, and assume that $f_{\vec{\alpha}}(\vec{\tau}) \equiv \rho \pmod 2$, $\rho \in \{0,1\}$. Notice that all coefficients of $f_{\vec{\alpha}}(2\vec{x} + \vec{\tau}) - \rho$ are even, so $h_{\vec{\alpha}}(\vec{x}) = \frac{1}{2}(f_{\vec{\alpha}}(2\vec{x}) - \rho)$ is again an integer polynomial, and *BASIC*$^+$ proves

$$\bigwedge_{i=1}^{r} (g_i(2\vec{x} + \vec{\tau}) \geq 0)^{\alpha_i} \to t(2^{c+1}\vec{x} + (2^c\vec{\tau} + \vec{\sigma})) = \left\lfloor \frac{f_{\vec{\alpha}}(2\vec{x})}{2} \right\rfloor = \left\lfloor \frac{2h_{\vec{\alpha}}(\vec{x}) + \rho}{2} \right\rfloor = h_{\vec{\alpha}}(\vec{x}).$$

□ (Claim 1)

Claim 2 *Every open formula $\psi(\vec{x})$ in the language $\langle 0, 1, +, \cdot, \dot{-}, \lfloor x/2 \rfloor, \leq \rangle$ is equivalent to a formula of the form*

$$\bigvee_{\vec{\sigma}<2^c} \Big(\bigwedge_i (x_i \equiv \sigma_i \pmod{2^c}) \wedge \psi_{\vec{\sigma}}(\vec{x}) \Big)$$

over $BASIC^+$, where each $\psi_{\vec{\sigma}}$ is a Boolean combination of integer polynomial inequalities.

Proof: Using Claim 1 and $BASIC^+$-provable uniqueness of the representation $x = 2^c y + \sigma$, $\sigma < 2^c$, we obtain an equivalent of ψ in almost the right form except that $\psi_{\vec{\sigma}}$ is a Boolean combination of inequalities of the form

$$f(2^{-c}(\vec{x} - \vec{\sigma})) \geq 0,$$

where f is an integer polynomial. If $d = \deg(f)$, $g(\vec{x}) = 2^{cd} f(2^{-c}(\vec{x} - \vec{\sigma}))$ is an integer polynomial, and the inequality above is equivalent to $g(\vec{x}) \geq 0$. □ (Claim 2)

Let us apply Claim 2 to the formula $\psi(\vec{x}, \vec{u}, 2^{\vec{u}})$ in (25). Since $BASIC^+$ knows that $2^0 = 1$ and $2^{u+1} = 2 \cdot 2^u$, we can replace $2^{u_i} \equiv \sigma \pmod{2^c}$ with $2^{u_i} = \sigma \vee (u_i \geq c \wedge \sigma = 0)$. Moreover, $u_i \equiv \sigma \pmod{2^c}$ can be written as $\exists v \leq p(|\vec{x}|)\,(u_i = 2^c v + \sigma)$, and $x_i \equiv \sigma \pmod{2^c}$ can be moved outside the quantifier prefix. Thus, $\varphi(\vec{x})$ is equivalent to

$$\bigvee_{\vec{\sigma}<2^c} \Big(\bigwedge_{i=1}^{k} (x_i \equiv \sigma_i \pmod{2^c}) \wedge Q_1 u_1 \leq p(|\vec{x}|) \cdots Q_l u_l \leq p(|\vec{x}|)\, \psi_{\vec{\sigma}}(\vec{x}, \vec{u}, 2^{\vec{u}}) \Big),$$

where $\psi_{\vec{\sigma}}$ is a Boolean combination of integer polynomial inequalities. We can reduce $\psi_{\vec{\sigma}}$ to a single inequality using

$$\neg(f \geq 0) \leftrightarrow -f - 1 \geq 0,$$
$$f \geq 0 \wedge g \geq 0 \leftrightarrow \forall v \leq p(|\vec{x}|)\,(vf + (1-v)^2 g \geq 0),$$

assuming $p(|\vec{x}|) \geq 1$. □

Lemma 7.2 *$VTC^0 + IMUL$ proves the following for every constant d: if $\{f_u : u < n\}$ is a sequence of integer polynomials of degree d (each given by a $(d+1)$-tuple of binary integer coefficients), and $a > d$ is a binary integer, there exists a double sequence $w = \{w_{u,i} : u < n, i \leq d+1\}$ such that $0 = w_{u,0} < w_{u,1} < \cdots < w_{u,d+1} = a$ and $f_u(x)$ has a constant sign on each interval $[w_{u,i}, w_{u,i+1})$, that is,*

$$\forall u < n\, \forall x \bigwedge_{i \leq d} \big(w_{u,i} \leq x < w_{u,i+1} \rightarrow (f_u(x) \geq 0 \leftrightarrow f_u(w_{u,i}) \geq 0)\big). \tag{27}$$

Proof: Using *IOpen*, $\{x < a : f(x) \geq 0\}$ is a union of at most d intervals for every polynomial f of degree at most d, i.e., $VTC^0 + IMUL$ proves

$$\forall f\, \forall a > d\, \exists 0 = x_0 < \cdots < x_{d+1} = a\, \forall x \bigwedge_{i \leq d} \big(x_i \leq x < x_{i+1} \rightarrow (f(x) \geq 0 \leftrightarrow f(x_i) \geq 0)\big).$$

Now we would like to invoke Σ_1^B-AC^R to find a sequence w satisfying (27), but we cannot directly do that as the conclusion is only Π_1^B.

Let $M \vDash VTC^0 + IMUL$, and R be its real closure. Quantifier elimination for RCF furnishes an open formula ϑ in L_{OR} such that $M \vDash \vartheta(x, y, a_0, \dots, a_d)$ iff $f(x) = \sum_{i \le d} a_i x^i$ has no roots in the interval $(x, y]_R$. By replacing f with $2f + 1$ if necessary, we may assume f has no integral roots. Let $\alpha_1 < \cdots < \alpha_c$, $c \le d$, be the list of all roots of f in $(0, a]_R$, and let $x_0, \dots, x_{d+1} \in M$ be the sequence of integers $0, \lceil \alpha_1 \rceil, \dots, \lceil \alpha_c \rceil, a$ (which exist due to *IOpen*) with duplicates removed, and dummy elements added if necessary to make it the proper length. Then f has no roots in the intervals $(x_i, x_{i+1} - 1]_R$. This means we can prove in $VTC^0 + IMUL$ the statement

$$\forall f \, \forall a > d \, \exists 0 = x_0 < x_1 < \cdots < x_{d+1} = a \bigwedge_{i \le d} \vartheta(x_i, x_{i+1} - 1, f),$$

which has the right complexity, hence we can use $\Sigma_1^B\text{-}AC^R$ to derive the existence of a sequence w such that

$$\forall u < n \Big(w_{u,0} = 0 \wedge w_{u,d+1} = a \wedge \bigwedge_{i \le d} \big(w_{u,i} < w_{u,i+1} \wedge \vartheta(w_{u,i}, w_{u,i+1} - 1, f_u) \big) \Big).$$

This implies (27). □

Theorem 7.3 *The RSUV-translation of $BASIC^+ + \Sigma_0^b(\dot{-}, 2^{\min\{u,|x|\}})$-MIN, and a fortiori of T_2^0, is provable in $VTC^0 + IMUL$.*

Proof: Work in $VTC^0 + IMUL$. It is straightforward but tedious to verify the axioms of $BASIC^+$. Let $\varphi(x)$ be (the translation of) a $\Sigma_0^b(\dot{-}, 2^{\min\{u,|x|\}})$ formula (possibly with other parameters), and a a binary number such that $\varphi(a)$, we have to find the least such number. Since it is enough to do this separately on each residue class modulo 2^c, we can assume using Theorem 7.3 that $\varphi(x)$ is equivalent to

$$Q_1 u_1 \le n \cdots Q_l u_l \le n \, f(x, \vec{u}, 2^{\vec{u}}) \ge 0$$

for $x < a$, where n is a unary number, and f is a polynomial with binary integer coefficients. By Lemma 7.2, there is a sequence w such that

$$w_{\vec{u},i} \le x < w_{\vec{u},i+1} \to (f(x, \vec{u}, 2^{\vec{u}}) \ge 0 \leftrightarrow f(w_{\vec{u},i}, \vec{u}, 2^{\vec{u}}) \ge 0)$$

for all $x < a$, $\vec{u} \le n$, and $i \le d$. As VTC^0 proves that every sequence of integers can be sorted, there is an increasing sequence $\{w'_j : j < m\}$ whose elements include every $w_{\vec{u},i}$. Consequently, the truth value of $\varphi(x)$ is constant on each interval $[w'_j, w'_{j+1})$, and the minimal $x < a$ satisfying $\varphi(x)$, if any, is w'_{j_0}, where

$$j_0 = \min\{j < m : \varphi(w'_j)\}.$$

The latter exists by $\Sigma_0^B(L_{\overline{VTC^0 + IMUL}})$-*COMP*. □

We remark that the proof used nothing particularly special about division by 2, except that *BASIC* conveniently includes the $\lfloor x/2 \rfloor$ function symbol and the relevant axioms. We could allow more general instances of division as long as the values of all denominators encountered when evaluating a Σ^b_0 formula on $[0, a]$ have a common multiple which is a length (unary number); in particular, Theorem 7.3 (along with an appropriate version of Lemma 7.1) holds for Σ^b_0 formulas in a language further expanded by function symbols for $\lfloor x/2^{||y||} \rfloor$ and $\lfloor x/\max\{1, ||y||\} \rfloor$.

We formulated Theorem 7.3 for $VTC^0 + IMUL$ as we have been working with this two-sorted theory throughout the main part of the paper, however here it is perhaps more natural to state the result directly in terms of one-sorted arithmetic to avoid needless *RSUV* translation. A theory Δ^b_1-*CR* corresponding to TC^0 was defined by Johannsen and Pollett [19], and shown *RSUV*-isomorphic to VTC^0 by Nguyen and Cook [24]. Recall also Johannsen's theory $C^0_2[div]$ from Section 3.

Corollary 7.4 *The theories Δ^b_1-CR + $IMUL$ and $C^0_2[div]$ prove $\Sigma^b_0(\dot{-}, 2^{\min\{u,|x|\}})$-$MIN$ and therefore T^0_2.* □

To put Theorem 7.3 in context, there has been a series of results to the effect that various subsystems of bounded arithmetic axiomatized by sharply bounded schemata are pathologically weak. Takeuti [30] has shown that $S^0_2 = \Sigma^b_0$-*PIND* does not prove the totality of the predecessor function, and Johannsen [16] extended his method to show that S^0_2 in a language including $\dot{-}$, $\lfloor x/2^y \rfloor$, and bit counting does not prove the totality of division by three (or even of the AC^0 function $\lfloor 2^{|x|}/3 \rfloor$). Boughattas and Kołodziejczyk [4] have shown that $T^0_2 = \Sigma^b_0$-*IND* does not prove that nontrivial divisors of powers of two are even, and by Kołodziejczyk [20], it does not even prove $3 \nmid 2^{|x|}$. These results also apply to certain mild extensions of T^0_2, nevertheless no unconditional independence result is known for Σ^b_0-*MIN*, or its subtheory $T^0_2 + S^0_2$.

What makes such separations possible is a lack of computational power. It is no coincidence that there are no result of this kind for two-sorted Zambella-style theories, where already the base theory V^0 proves the totality of all AC^0-functions: we can show $V^0(p) \nsubseteq V^0(q)$ for primes $p \neq q$ using the known lower bounds for $\mathrm{AC}^0[p]$, but we have no independence results for stronger theories without complexity assumptions such as $\mathrm{AC}^0[6] \neq \mathrm{PH}$. This is directly related to the expressive power of sharply bounded formulas: while Σ^B_0 formulas can define all AC^0 predicates, the ostensibly quite similar Σ^b_0 formulas (that even involve the TC^0-complete multiplication function) have structural properties that preclude this, as witnessed by Mantzivis's result. Indeed, the pathological behaviour of T^0_2 disappears if we slightly extend its language: as proved in [13], $T^0_2(\lfloor x/2^y \rfloor) = PV_1$, and this can be easily extended to show $\Sigma^b_0(\lfloor x/2^y \rfloor)$-$MIN = T^1_2$.

Theorem 7.3 formally implies only conditional separations: in particular, $PV_1 \nsubseteq \Sigma^b_0$-*MIN* unless $\mathrm{P} = \mathrm{TC}^0$, and Σ^b_0-$MIN \subsetneq T^1_2$ unless $\mathrm{PH} = \mathrm{BH} \subseteq \mathrm{TC}^0/\mathrm{poly}$ and $\mathrm{PLS} = \mathrm{FTC}^0$ (provably in Σ^b_0-*MIN*). However, heuristically it gives us more. If Σ^b_0-*MIN* were a "computationally reasonable" theory, we would expect it to coincide with T^1_2 due to its shape, or at the very least to correspond to a class closer to PLS than TC^0. Thus, Theorem 7.3 indicates that it might be a pathologically weak theory in some way, and therefore amenable to unconditional independence results by means of a direct combinatorial construction of models in the spirit of [4, 20].

8 Conclusion

The weakest theory of bounded arithmetic in the setup of [33, 8] that can talk about elementary arithmetic operations on binary integers is VTC^0. We have shown that its strengthening $VTC^0 + IMUL$ proves that these operations are fairly well behaved in that they satisfy open induction. Despite that the theory $VTC^0 + IMUL$ corresponds to the complexity class TC^0 similarly to VTC^0, it is still an interesting problem what properties of integer arithmetic operations are provable in plain VTC^0. In view of Theorem 6.8 and Corollary 3.6, we have:

Corollary 8.1 *VTC^0 proves IOpen if and only if it proves DIV.* □

Question 8.2 *Does VTC^0 prove DIV? In particular, does it prove the soundness of the division algorithm by Hesse et al. [11]?*

While the analysis of the algorithm in [11] generally relies on quite elementary tools, its formalization in VTC^0 suffers from "chicken-and-egg" problems. For instance, the proof of Lemma 6.1, whose goal is to devise an algorithm for finding small powers in groups, assumes there is a well-behaved powering function, and uses its various properties to establish that its value is correctly computed by the algorithm. This is no good if we need the very algorithm to construct the powering function in the first place. Similarly, integer division is employed throughout Section 4. It is not clear whether one can circumvent these circular dependencies in VTC^0. On the other hand, the requisite operations such as division are available in $VTC^0 + IMUL$, which makes it plausible that $VTC^0 + IMUL$ *can* formalize the arguments.

We remark that it is not difficult to do division by *standard* integers in VTC^0. This means VTC^0 knows that binary integers form a $\mathbb{Z}$-*ring*, and in particular, they satisfy all universal consequences of *IOpen* by a result of Wilkie [32]. (*IOpen* itself is a $\forall\exists$-axiomatized theory, and likewise, *DIV* is a $\forall\exists$ sentence.)

As explained in Section 7, our main result implies that $VTC^0 + IMUL$ (or better, the corresponding one-sorted theory Δ^b_1-$CR + IMUL$) proves minimization for Σ^b_0 formulas in Buss's language, which suggests that the theory axiomatized by Σ^b_0-*MIN* is rather weak. Consequently, it might be feasible to unconditionally separate this theory from stronger fragments of S_2, nevertheless our argument gives no clue how to do that.

Problem 8.3 *Prove that Σ^b_0-MIN is strictly weaker than T^1_2 without complexity-theoretic assumptions.*

Acknowledgement

I am indebted to Leszek Kołodziejczyk for useful suggestions on an earlier version of this paper.

References

[1] David A. Mix Barrington, Neil Immerman, and Howard Straubing, *On uniformity within* NC^1, Journal of Computer and System Sciences 41 (1990), no. 3, pp. 274–306.

[2] Saugata Basu, Richard Pollack, and Marie-Françoise Roy, *Algorithms in real algebraic geometry*, Springer, 2006.

[3] Paul W. Beame, Stephen A. Cook, and H. James Hoover, *Log depth circuits for division and related problems*, SIAM Journal on Computing 15 (1986), no. 4, pp. 994–1003.

[4] Sedki Boughattas and Leszek A. Kołodziejczyk, *The strength of sharply bounded induction requires MSP*, Annals of Pure and Applied Logic 161 (2010), no. 4, pp. 504–510.

[5] Samuel R. Buss, *Bounded arithmetic*, Bibliopolis, Naples, 1986, revision of 1985 Princeton University Ph.D. thesis.

[6] Ashok K. Chandra, Larry Stockmeyer, and Uzi Vishkin, *Constant depth reducibility*, SIAM Journal on Computing 13 (1984), no. 2, pp. 423–439.

[7] Andrew Y. Chiu, George I. Davida, and Bruce E. Litow, *Division in logspace-uniform* NC^1, RAIRO – Theoretical Informatics and Applications 35 (2001), no. 3, pp. 259–275.

[8] Stephen A. Cook and Phuong Nguyen, *Logical foundations of proof complexity*, Perspectives in Logic, Cambridge University Press, New York, 2010.

[9] Antonio J. Engler and Alexander Prestel, *Valued fields*, Springer Monographs in Mathematics, Springer, 2005.

[10] András Hajnal, Wolfgang Maass, Pavel Pudlák, Márió Szegedy, and György Turán, *Threshold circuits of bounded depth*, Journal of Computer and System Sciences 46 (1993), no. 2, pp. 129–154.

[11] William Hesse, Eric Allender, and David A. Mix Barrington, *Uniform constant-depth threshold circuits for division and iterated multiplication*, Journal of Computer and System Sciences 65 (2002), no. 4, pp. 695–716.

[12] Neil Immerman, *Expressibility and parallel complexity*, SIAM Journal on Computing 18 (1989), no. 3, pp. 625–638.

[13] Emil Jeřábek, *The strength of sharply bounded induction*, Mathematical Logic Quarterly 52 (2006), no. 6, pp. 613–624.

[14] ———, *On theories of bounded arithmetic for* NC^1, Annals of Pure and Applied Logic 162 (2011), no. 4, pp. 322–340.

[15] ———, *Root finding with threshold circuits*, Theoretical Computer Science 462 (2012), pp. 59–69.

[16] Jan Johannsen, *On the weakness of sharply bounded polynomial induction*, in: Computational Logic and Proof Theory, Proceedings of Kurt Gödel Colloquium '93 (G. Gottlob, A. Leitsch, and D. Mundici, eds.), Lecture Notes in Computer Science vol. 713, Springer, 1993, pp. 223–230.

[17] ———, *Weak bounded arithmetic, the Diffie-Hellman problem, and Constable's class K*, in: Proceedings of the 14th Annual IEEE Symposium on Logic in Computer Science, 1999, pp. 268–274.

[18] Jan Johannsen and Chris Pollett, *On proofs about threshold circuits and counting hierarchies (extended abstract)*, in: Proceedings of the 13th Annual IEEE Symposium on Logic in Computer Science, 1998, pp. 444–452.

[19] ———, *On the Δ^b_1-bit-comprehension rule*, in: Logic Colloquium '98: Proceedings of the 1998 ASL European Summer Meeting held in Prague, Czech Republic (S. R. Buss, P. Hájek, and P. Pudlák, eds.), ASL, 2000, pp. 262–280.

[20] Leszek A. Kołodziejczyk, *Independence results for variants of sharply bounded induction*, Annals of Pure and Applied Logic 162 (2011), no. 12, pp. 981–990.

[21] Jan Krajíček, *Bounded arithmetic, propositional logic, and complexity theory*, Encyclopedia of Mathematics and Its Applications vol. 60, Cambridge University Press, 1995.

[22] Alexis Maciel and Denis Thérien, *Efficient threshold circuits for power series*, Information and Computation 152 (1999), no. 1, pp. 62–73.

[23] Spyro-Giorgio Mantzivis, *Circuits in bounded arithmetic part I*, Annals of Mathematics and Artificial Intelligence 6 (1991), no. 1–3, pp. 127–156.

[24] Phuong Nguyen and Stephen A. Cook, *Theories for TC^0 and other small complexity classes*, Logical Methods in Computer Science 2 (2006), no. 1, paper no. 3.

[25] Ian Parberry and Georg Schnitger, *Parallel computation with threshold functions*, Journal of Computer and System Sciences 36 (1988), no. 3, pp. 278–302.

[26] John H. Reif, *Logarithmic depth circuits for algebraic functions*, SIAM Journal on Computing 15 (1986), no. 1, pp. 231–242.

[27] John H. Reif and Stephen R. Tate, *On threshold circuits and polynomial computation*, SIAM Journal on Computing 21 (1992), no. 5, pp. 896–908.

[28] Dana Scott, *On completing ordered fields*, in: Applications of Model Theory to Algebra, Analysis, and Probability (W. A. J. Luxemburg, ed.), Holt, Rinehart and Winston, New York, 1969, pp. 274–278.

[29] John C. Shepherdson, *A nonstandard model for a free variable fragment of number theory*, Bulletin de l'Académie Polonaise des Sciences, Série des Sciences Mathématiques, Astronomiques et Physiques 12 (1964), no. 2, pp. 79–86.

[30] Gaisi Takeuti, *Sharply bounded arithmetic and the function $a \dot{-} 1$*, in: Logic and Computation, Proceedings of a Workshop held at Carnegie Mellon University, June 30–July 2, 1987 (W. Sieg, ed.), Contemporary Mathematics vol. 106, American Mathematical Society, 1990, pp. 281–288.

[31] Peter Vámos, *Decomposition problems for modules over valuation domains*, Journal of the London Mathematical Society s2-41 (1990), no. 1, pp. 10–26.

[32] Alex J. Wilkie, *Some results and problems on weak systems of arithmetic*, in: Logic Colloquium '77 (A. Macintyre, ed.), North-Holland, 1978, pp. 285–296.

[33] Domenico Zambella, *Notes on polynomially bounded arithmetic*, Journal of Symbolic Logic 61 (1996), no. 3, pp. 942–966.