Iterated multiplication in VTC^0

Emil Jeřábek

Institute of Mathematics, Czech Academy of Sciences

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

September 23, 2021

Abstract

We show that VTC^0, the basic theory of bounded arithmetic corresponding to the complexity class TC^0, proves the $IMUL$ axiom expressing the totality of iterated multiplication satisfying its recursive definition, by formalizing a suitable version of the TC^0 iterated multiplication algorithm by Hesse, Allender, and Barrington. As a consequence, VTC^0 can also prove the integer division axiom, and (by our previous results) the $RSUV$-translation of induction and minimization for sharply bounded formulas. Similar consequences hold for the related theories Δ^b_1-CR and C^0_2.

As a side result, we also prove that there is a well-behaved Δ_0 definition of modular powering in $I\Delta_0 + WPHP(\Delta_0)$.

Keywords: bounded arithmetic, integer division, iterated multiplication, modular powering, threshold circuits

MSC (2020): 03F20, 03F30, 03D15, 03C62

1 Introduction

The underlying theme of this paper is *feasible reasoning* about the elementary integer arithmetic operations $+, \cdot, \leq$: what properties of these operations can be proven using only concepts whose complexity does not exceed that of $+, \cdot, \leq$ themselves? There is a common construction in proof complexity that allows to make such questions formal: given a (sufficiently well-behaved) complexity class C, we can define a theory of arithmetic T that "corresponds" to C. While the notion of correspondence is somewhat vague, what this typically means is that on the one hand, the provably total computable (in a suitable sense) functions of T are exactly the C-functions, and on the other hand, T can reason with C-concepts: it proves induction, comprehension, minimization, or similar schemata for formulas that express predicates computable in C.

In our case, the right complexity class[1] is TC^0: the elementary arithmetic operations are all computable in TC^0, and while $+$ and $\leq$ are already in $\mathrm{AC}^0 \subsetneq \mathrm{TC}^0$, multiplication is TC^0-complete under AC^0 Turing-reductions. The arithmetical theory corresponding to TC^0 that we

[1] Originally, TC^0 was introduced as a nonuniform circuit class by Hajnal et al. [12], but in this paper we always mean the DLOGTIME-uniform version of the class, which gives a robust notion of "fully uniform" TC^0 with several equivalent definitions across various computation models (cf. [4]). Likewise for AC^0.

will work with in this paper is VTC^0, defined by Nguyen and Cook [23] as a two-sorted theory of bounded arithmetic in the style of Zambella [28]. Earlier, Johannsen and Pollett [17, 18] introduced two theories corresponding to TC^0 in the framework of single-sorted theories of Buss [7]: Δ^b_1-CR, which is equivalent to VTC^0 under the $RSUV$ translation, and its extension C^0_2. (Since C^0_2 is conservative over Δ^b_1-CR for a class of formulas that encompasses the statements that we are interested in in this paper, there is no difference between these theories for our purposes.)

While it is easy to show (and not particularly difficult to formalize in VTC^0) that TC^0 includes $+$, $\cdot$, $-$, and iterated addition $\sum_{i<n} X_i$, it is considerably harder to prove that it includes integer *division* and *iterated multiplication* $\prod_{i<n} X_i$. The history of this result starts with Beame, Cook, and Hoover [5], who proved (in present terminology) that division, iterated multiplication, and powering X^n (with n given in unary) are TC^0 Turing-reducible to each other, and that they are all computable in P-*uniform* TC^0. (In fact, [5] predates the definition of TC^0; they referred to NC^1 in the paper. It is easy to observe though that their algorithms can be implemented using threshold circuits.) The basic idea of [5] is to compute iterated multiplication in the *Chinese remainder representation* (*CRR*), i.e., modulo a sequence of small primes $\vec{m}$, and then reconstruct the result in binary from CRR. The main source of nonuniformity (or insufficient uniformity) in [5] is the CRR reconstruction procedure: they require the CRR basis $\vec{m}$ to be fixed in advance (for a given input length), and supplied to the algorithm along with the product $\prod_i m_i$.

The next breakthrough was achieved by Chiu, Davida, and Litow [8], who devised a more efficient CRR reconstruction procedure based on computation of the rank of CRR that did not rely on $\prod_i m_i$, and as a consequence, proved that division and iterated multiplication are in L-uniform TC^0, and in particular, in L itself. (Their paper still refers to NC^1 rather than TC^0.) Subsequently, Hesse, Allender, and Barrington [13] proved the optimal result that division and iterated multiplication are in (fully uniform) TC^0 by first reducing the remaining nonuniformity in CRR reconstruction to the modular powering function $\mathrm{pow}(a, r, m) = a^r \bmod m$ (with all inputs in unary, and m prime), and then showing that pow is in fact computable in $\mathrm{AC}^0 \subseteq \mathrm{TC}^0$.

We mention that once we know that TC^0 includes iterated multiplication, it follows easily that it can do many other arithmetic functions: in particular, the basic operations $+, \cdot, \dots$ (including iterated $\sum$ and $\prod$) are TC^0-computable not just in the integers, but also in $\mathbb{Q}$ and more general number fields, and in rings of polynomials; and we can compute rational approximations of analytic functions given by sufficiently nice power series, such as trigonometric and inverse trigonometric functions, log and exp (for inputs of small magnitude). On the arithmetical side, it was shown in Jeřábek [15] that the theory VTC^0 augmented with an iterated multiplication axiom is fairly powerful: by formalizing TC^0 root approximation algorithms for constant-degree univariate polynomials, it proves binary-number induction for quantifier-free formulas in the language of ordered rings (*IOpen*), and even binary-number induction and minimization for $RSUV$ translations of Σ^b_0 formulas in Buss's language.

In view of these developments, it is natural to ask whether TC^0 integer division and iterated multiplication algorithms can be formalized in the corresponding theory VTC^0. This problem was posed in the concluding section of Nguyen and Cook [23], where it was attributed to A. Atserias; it was then restated in Cook and Nguyen [9, IX.7.6] and Jeřábek [15, Q. 8.2]. Earlier, Atserias [2, 3] asked whether $I\Delta_0$ can formalize a Δ_0 definition of modular exponentiation (whose existence is another consequence of [13]). Johannsen [16] (predating [8, 13]) devised a theory $C^0_2[div]$ extending C^0_2 that corresponds to the TC^0-closure of division; the problem of formalizing division and iterated multiplication in VTC^0 is equivalent to the question if $C^0_2 \equiv C^0_2[div]$ (more precisely, if $C^0_2[div]$ is an extension of C^0_2 by a definition), but this was not explicitly posed as a problem in [16].

To clarify, since all TC^0 functions are provably total in VTC^0, it trivially follows that the theory can define provably total functions that express the division and iterated multiplication algorithms of [13]. However, the theory does not necessarily *prove* anything about such functions, besides the fact that they compute the correct specific outputs for inputs given by standard constants. When we ask for formalization of division in VTC^0, what we actually mean is whether the theory can prove an axiom DIV postulating the existence of $\lfloor Y/X \rfloor$ that satisfies the defining property

$$X \neq 0 \to \lfloor Y/X \rfloor X \leq Y < \big(\lfloor Y/X \rfloor + 1\big)X,$$

and likewise, formalization of iterated multiplication refers to an axiom $IMUL$ stating the existence of iterated products $\prod_{i<n} X_i$ satisfying the defining recurrence

$$\prod_{i<0} X_i = 1,$$
$$\prod_{i<n+1} X_i = X_n \prod_{i<n} X_i.$$

(The exact definitions of $IMUL$ and DIV are given in Section 2.) This requires much more than just totality of the two functions. Note that whether we ask about the provability of $IMUL$ or DIV is just a matter of convenience: it follows from the results of [16, 15] (formalizing the reductions from [5]) that $IMUL$ implies DIV over VTC^0, and that VTC^0 proves DIV if and only if it proves $IMUL$. For the purposes of this paper, it will be more natural to work with $IMUL$.

The reader may wonder what makes the formalization of the iterated multiplication algorithm from [13] so challenging. After all, the algorithm and its analysis are rather elementary, they do not rely on any sophisticated number theory. It is true that the argument in [13] does not really just consist of a single algorithm—it has a complex structure with several interdependent parts:

(i) Show that iterated multiplication is in $\mathrm{TC}^0(\mathrm{pow})$, using CRR reconstruction.

(ii) Show that iterated multiplication with polylogarithmically small input is in AC^0, by scaling down part (i).

(iii) Show that pow is in AC^0 using (ii), and plug it into (i).

However, this is not by itself a fundamental obstacle. What truly makes the formalization difficult is that the analysis of the algorithms suffers from several problems of a "chicken or egg" type: which came first, the chicken or the egg? Specifically:

- The analysis (proof of soundness) of the CRR reconstruction procedure in part (i) heavily relies on iterated products and divisions: e.g., it refers to the product $\prod_i m_i$ of primes from the CRR basis. However, when working in VTC^0, we need the soundness of the CRR reconstruction procedure to define such iterated products in the first place.

- Similarly, the analysis of the modular exponentiation algorithm in part (iii) refers to results of modular exponentiation such as $a^{\lfloor n/d_i \rfloor}$, and in particular, it relies on Fermat's little theorem $a^n = 1$. However, the latter cannot be stated, let alone proved, without having a means to define modular exponentiation in the first place.

- A more subtle, but all the more important, issue is that in part (i), the reduction of iterated modular multiplication $\mathrm{imul}(\vec{a}, m) = \prod_i a_i \bmod m$ (m prime) to pow relies on cyclicity of the multiplicative groups $(\mathbb{Z}/m\mathbb{Z})^\times$, which is notoriously difficult to prove in bounded arithmetic (cf. [14, Q. 4.8]). While this may look more like an instance of "sophisticated number theory" at first sight, what makes it a chicken-or-egg problem as well is that the cyclicity of $(\mathbb{Z}/m\mathbb{Z})^\times$ is in fact provable in $VTC^0 + IMUL$.

The main result of this paper is that *IMUL* is, after all, provable in VTC^0, and specifically, VTC^0 can formalize the soundness of a version of the Hesse, Allender, and Barrington [13] algorithm. Our formalization follows the basic outline of the original argument, adjusted to overcome the above-mentioned difficulties:

- Since we do not know how to prove directly the cyclicity of $(\mathbb{Z}/m\mathbb{Z})^\times$ in VTC^0, we formalize part (i) using imul as a primitive instead of pow: that is, we prove *IMUL* in $VTC^0(\mathrm{imul})$. We get around the chicken-or-egg problems by developing many low-level properties of CRR in $VTC^0(\mathrm{imul})$, in particular the effects of simple CRR operations such as those used in the definition of the CRR reconstruction procedure. This is the most technical part of the paper.

- Part (ii) is easy to formalize in the basic theory V^0 (corresponding to AC^0) by observing that polylogarithmic cuts of models of V^0 are models of *VNL*, which improves a result of Müller [19].

- We avoid the chicken-or-egg problems in part (iii) by modifying the modular powering algorithm so that it does not need the auxiliary values $a^{\lfloor n/d_i \rfloor}$ at all, using more directly the underlying idea from [13] of applying CRR to exponents. Since we need the weak pigeonhole principle to ensure there are enough "good" primes for the CRR, the formalization proceeds in $V^0 + \mathit{WPHP}$ rather than plain V^0. By exploiting the conservativity of V^0 over $I\Delta_0$, we obtain the stand-alone result that there is a Δ_0 definition of pow (even for nonprime moduli) whose defining recurrence is provable in $I\Delta_0 + \mathit{WPHP}(\Delta_0)$, which may be of independent interest.

- The results so far suffice to establish that over VTC^0, *IMUL* is equivalent to the totality of imul, and to the cyclicity of $(\mathbb{Z}/m\mathbb{Z})^\times$ for prime m, which reduces to the statement that for any prime p, all elements of order p modulo m are powers of each other. Paying attention to how large products are needed to prove the last statement for a given m and p, and vice versa, we show how to make progress on each turn around this circle of implications, using a partial formalization of the structure theorem for finite abelian groups. This allows us to set up a proof by induction to finish the derivation of $IMUL$ in VTC^0.

As a consequence of our main theorem, the above-mentioned results of [15] on $VTC^0 + IMUL$ apply to VTC^0: that is, VTC^0 proves the binary-number induction and minimization for $RSUV$ translations of Σ^b_0 formulas. In terms of Johannsen and Pollett's theories, iterated multiplication and Σ^b_0-minimization (in Buss's language) are provable in Δ^b_1-CR and in C^0_2, and the theory $C^0_2[div]$ is an extension of C^0_2 by a definition (and therefore a conservative extension).

The paper is organized as follows. Section 2 consists of preliminaries on VTC^0 and related theories. In Section 3, we prove a suitable lower bound on the number of primes (to be used for CRR) in VTC^0. Section 4 formalizes a proof of division by small primes in VTC^0(pow). The core Section 5 formalizes various properties of CRR in VTC^0(imul), leading to a proof of soundness of the CRR reconstruction procedure, and of $IMUL$. In Section 6, we discuss polylogarithmic cuts and the ensuing results about V^0. In Section 7, we construct modular exponentiation in $V^0 + WPHP$. We finish the proof of $IMUL$ in VTC^0 in Section 8. In Section 9, we improve some of our auxiliary results to a more useful stand-alone form. Section 10 concludes the paper.

2 Preliminaries

We will work with two-sorted (second-order) theories of bounded arithmetic in the style of Zambella [28]. Our main reference for these theories is Cook and Nguyen [9].

The language $L_2 = \langle 0, S, +, \cdot, \le, \in, |\cdot| \rangle$ of two-sorted bounded arithmetic is a first-order language with equality with two sorts of variables, one for natural numbers (called *small* or *unary* numbers), and one for finite sets of small numbers, which can also be interpreted as *large* or *binary* numbers so that X represents $\sum_{u\in X} 2^u$. Usually, variables of the number sort are written with lowercase letters $x, y, z, \dots$, and variables of the set sort with uppercase letters $X, Y, Z, \dots$. The symbols $0, S, +, \cdot, \le$ of L_2 provide the standard language of arithmetic on the unary sort; $x \in X$ is the elementhood predicate, also written as $X(x)$, and the intended meaning of the $|X|$ function is the least strict upper bound on elements of X. We write $x < y$ as an abbreviation for $x \le y \wedge x \ne y$, and $\operatorname{bit}(X, i)$ for the indicator function of $i \in X$.

Bounded quantifiers are introduced by

$$\exists x \le t\, \varphi \Leftrightarrow \exists x\, (x \le t \wedge \varphi),$$
$$\exists X \le t\, \varphi \Leftrightarrow \exists X\, \bigl(|X| \le t \wedge \varphi\bigr),$$

where t is a term of unary sort not containing x or X (resp.), and similarly for universal bounded quantifiers. For any $i \ge 0$, the class Σ^B_i consists of formulas that can be written as i alternating (possibly empty) blocks of bounded quantifiers, the first being existential, followed by a formula with only bounded first-order quantifiers. Purely number-sort Σ^B_0 formulas without set-sort parameters (i.e., bounded formulas in the usual single-sorted language of arithmetic) are called Δ_0. A formula is Σ^1_1 if it consists of a block of (unbounded) existential quantifiers followed by a Σ^B_0 formula.

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

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

and the bounded comprehension schema

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

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 Σ^B_0-induction schema Σ^B_0-*IND* and the Σ^B_0-minimization schema Σ^B_0-*MIN*; in particular, V^0 includes the theory $I\Delta_0$ (the single-sorted theory of arithmetic axiomatized by induction for Δ_0 formulas over a base theory such as Robinson's arithmetic) on the small number sort. In fact, V^0 is a conservative extension of $I\Delta_0$ [9, Thm. V.1.9].

Following [9], a set X can code a sequence (indexed by small numbers) of sets whose uth element is $X^{[u]}=\bigl\{x:\langle u,x\rangle\in X\bigr\}$, where $\langle x,y\rangle=(x+y)(x+y+1)/2+y$. Likewise, we can code sequences of small numbers using $X^{(u)}=|X^{[u]}|$. (See below for a more efficient sequence encoding scheme.) While we stick to the official notation in formal contexts such as when stating axioms, elsewhere we will generally write $\vec{X}=\langle X_i:i<n\rangle$ to indicate that $\vec{X}$ codes a sequence of length n whose ith element is X_i. We denote the length of the sequence as $\mathrm{lh}(\vec{X})=n$. (The official sequence coding system does not directly indicate the length, hence we need to supply it using a separate first-order variable.)

There is a Δ_0-definition of the graph of 2^n such that $I\Delta_0$ proves that it is a partial function whose domain is an initial segment closed under $+$, and that it satisfies the defining recurrence $2^0=1$, $2^{n+1}=2\cdot 2^n$ (see e.g. Hájek and Pudlák [11, §V.3(c)]). Thus, there is also a well-behaved Δ_0-definition of the function $\mathrm{bit}(x,i)=\lfloor x2^{-i}\rfloor \operatorname{rem} 2$, and $|x|=\min\{n:x<2^n\}$. In particular, in V^0 there is a Σ^B_0-definable bijection identifying any small number x with the corresponding large number, represented by the set $\{i<|x|:\mathrm{bit}(x,i)=1\}$. Numbers of the form $n=|x|$, or equivalently, such that 2^n exists as a small number, will be called *logarithmically small.* The axiom Ω_1 is defined as $\forall x\,\exists y\,\bigl(y=2^{|x|^2}\bigr)$, or equivalently, $\forall x\,\exists y\,\bigl(y=x^{|x|}\bigr)$.

VTC^0 is extends V^0 by the axiom

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

asserting that for every set X, there is a sequence Y supplying the counting function $Y^{(i)}=\mathrm{card}(X\cap\{0,\dots,i-1\})$. Thus, in VTC^0, there is a well-behaved Σ^B_1 definition of cardinality of sets $\mathrm{card}(X)$ that provably satisfies

$$\mathrm{card}(\varnothing)=0, \tag{1}$$

$$\mathrm{card}(X\cup\{u\})=\mathrm{card}(X)+1,\quad u\notin X. \tag{2}$$

V^0 can Σ^B_0-define $X + Y$ and $X < Y$, and prove that they make large numbers into a non-negative part of a discrete totally ordered abelian group. Moreover, VTC^0 can Σ^B_1-define iterated addition $\sum_{i<n} X^{[i]}$ satisfying the recurrence

$$\sum_{i<0} X^{[i]} = 0, \tag{3}$$

$$\sum_{i<n+1} X^{[i]} = X^{[n]} + \sum_{i<n} X^{[i]}, \tag{4}$$

and as a special case, it can Σ^B_1-define multiplication $X \cdot Y$, satisfying the axioms of non-negative parts of discretely ordered rings. The embedding of small numbers to large numbers respects the arithmetic operations.

While we normally use set variables $X, \dots$ to represent nonnegative integers, we can also make them represent arbitrary integers by reserving one bit for sign. We can extend $<, +, \cdot$, and $\sum_{i<n} X_i$ to signed integers with no difficulty. We can also use fractions to represent rational numbers, but we have to be careful with their manipulation: in particular, converting a bunch of fractions to a common denominator (such as when summing them) requires the product of the denominators, and taking integer parts requires division with remainder (see below); one case easy to handle is when all denominators are powers of 2. (Note that $2^n = \{n\}$ is easily definable in V^0.) Also, reducing fractions to lowest terms is impossible in general, as integer gcd is not known to be computable in the NC hierarchy. (However, gcd of small integers can be done already in $I\Delta_0$.)

When $Y = Q \cdot X + R$, where $0 \le R < X$ (including the case of negative Y and Q), we will write[2] $Q = \lfloor Y/X \rfloor$ and $R = Y \text{ rem } X$. We will also use the divisibility predicate $X \mid Y$, meaning $Y \text{ rem } X = 0$, and the congruence predicate $Y \equiv Y' \pmod{X}$, meaning $X \mid (Y - Y')$. (If the modulus X is the same throughout an argument, we may write just $Y \equiv Y'$.) Since the provability of the totality of division in VTC^0 is equivalent to the main result of this paper, we will need to make sure that the relevant quotients and remainders exist whenever we employ these notations; in particular, $I\Delta_0$ proves that we can divide small numbers, V^0 can divide large numbers by powers of 2, and we will prove in Section 4 that $VTC^0(\mathrm{pow})$ can divide large numbers by small primes.

Both notations $Y \text{ rem } X$ and $Y \equiv Y' \pmod{X}$ will establish contexts where everything inside Y and Y' is evaluated modulo X (except for nested mod/rem expressions modulo a different X'); in particular, since $I\Delta_0$ proves that x has an inverse modulo m when $\gcd(x, m) = 1$, we may use x^{-1} inside contexts evaluated modulo m. We denote by $(\mathbb{Z}/m\mathbb{Z})^\times$ the group of units modulo m: that is, with domain $\{x < m : \gcd(x, m) = 1\}$ (which is just the interval $[1, m-1]$ for m prime) and the operation of multiplication modulo m.

Following [15], we define the iterated multiplication axiom

$$\forall n, X\, \exists Y\, \forall u \le v < n \left(Y^{[u,u]} = 1 \wedge Y^{[u,v+1]} = Y^{[u,v]} \cdot X^{[v]} \right), \tag{\textit{IMUL}}$$

[2]Conventionally, our $Y \text{ rem } X$ is written as just $Y \bmod X$. Since we will frequently mix this notation with the $Y \equiv Y' \pmod{X}$ congruence notation, we want to distinguish the two more clearly than by relying on the typographical difference between $Z = Y \bmod X$ and $Z \equiv Y \pmod{X}$, considering also that many authors write the latter as $Z \equiv Y \mod X$, or even $Z = Y \mod X$.

the meaning being that for any sequence $\langle X_i : i < n\rangle$, we can find a triangular matrix $\langle Y_{u,v} : u \le v \le n\rangle$ with entries $Y_{u,v} = \prod_{i=u}^{v-1} X_i$.

Let us briefly recall the definitions of AC^0 and TC^0 for context, even though we will not actually need to work with complexity classes in this paper. A language L belongs to AC^0 if it is computable by a DLOGTIME-uniform family of constant-depth polynomial-size circuits using $\neg$ and unbounded-fan-in $\bigwedge$ and $\bigvee$ gates. Equivalently, $L \in \mathrm{AC}^0$ iff it is computable on an alternating Turing machine (with random-access input) in time $O(\log n)$ using $O(1)$ alternations, iff L (represented as a class of finite structures) is $\mathrm{FO}[+,\cdot]$-definable. A function $F(X)$ is in FAC^0 (and is called an AC^0 function) if $|F(X)| \le p\bigl(|X|\bigr)$ for some polynomial p, and the *bit-graph* $\{\langle X, i\rangle : \mathrm{bit}(F(X), i) = 1\}$ is an AC^0 language. A language L is in TC^0 iff it is computable by a DLOGTIME-uniform family of constant-depth polynomial-size circuits using $\neg$ and unbounded-fan-in $\bigwedge$, $\bigvee$, and Majority gates (or more generally, threshold gates), iff L is computable in $O(\log n)$ time on a threshold Turing machine (see [24]) using $O(1)$ thresholds, iff it is definable in FOM (first-order logic with majority quantifiers).

A predicate is Σ^B_0-definable in the standard model of L_2 iff it is in AC^0. The provably total Σ^1_1-definable (= "computable") functions of V^0 are exactly the AC^0 functions, and the provably total Σ^1_1-definable functions of VTC^0 (or of $VTC^0 + IMUL$) are exactly the TC^0 functions. Here, objects of the set sort are represented as bit-strings in the usual way, and objects from the number sort are represented in unary; see [9, §IV,§A] for details.

We will need to work with various theories postulating totality of certain functions. Cook and Nguyen [9, §IX.2] developed a general framework for such theories under the slogan of *theories VC associated with complexity classes C*. We refrain from this terminology as most of our theories will correspond to the *same* complexity class (TC^0, sometimes AC^0), but we will adopt the machinery as such, using the notation of [15].

For notational simplicity, we will formulate the setup for a single function of one variable $F(X)$ whose input and output are binary numbers, but it applies just the same when we have several functions in several variables whose inputs and outputs are a mix of binary and unary numbers. Thus, let $F(X)$ be a function with a Σ^B_0-definable graph $\delta_F(X;Y)$ which is polynomially bounded, i.e., $|F(X)| \le t(X)$ for some term t. We assume that V^0 proves

$$\delta_F(X;Y) \wedge \delta_F(X;Y') \to Y = Y', \tag{5}$$

$$\delta_F(X;Y) \to |Y| \le t(X). \tag{6}$$

The totality of F is expressed by the sentence

$$\forall X\, \exists Y\, \delta_F(X;Y). \tag{Tot_F}$$

The *aggregate function of* F is the function F^* that maps (the code of) a sequence $\langle X_i : i < n\rangle$ to $\langle F(X_i) : i < n\rangle$. The graph of F^* is defined by

$$\delta^*_F(n, X; Y) \Leftrightarrow \forall i < n\, \delta_F\bigl(X^{[i]}; Y^{[i]}\bigr),$$

and its totality is expressed by

$$\forall n\, \forall X\, \exists Y\, \delta^*_F(n, X; Y). \tag{Tot^*_F}$$

(Strictly speaking, δ^*_F does not define the graph of a function, as sequence codes are not completely unique. This is why we write δ^*_F and Tot^*_F rather than δ_{F^*} and Tot_{F^*}.) The *Cook–Nguyen (CN) theory* associated with δ_F is $V^0(F) = V^0 + \mathit{Tot}^*_F$.

The *choice schema* (also called replacement or bounded collection) Σ^B_0-AC consists of the axioms

$$\forall P \left[\forall x < n\, \exists Y \le m\, \varphi(x, Y, P) \to \exists W\, \forall x < n\, \varphi\big(x, W^{[x]}, P\big)\right]$$

for $\varphi \in \Sigma^B_0$; a theory T is closed under the *choice rule* Σ^B_0-AC^R if

$$T \vdash \forall X\, \exists Y\, \varphi(X, Y) \implies T \vdash \forall n\, \forall X\, \exists Y\, \forall i < n\, \varphi\big(X^{[i]}, Y^{[i]}\big)$$

for all $\varphi \in \Sigma^B_0$.

The main properties of CN theories were summarized in [15, Thm. 3.2] (mostly based on [9, §IX.2]), which we repeat here:

Theorem 2.1 *Let $V^0(F)$ be a CN theory.*

(i) The provably total Σ^1_1-definable (or Σ^B_1-definable) functions of $V^0(F)$ are exactly the functions in the AC^0-closure (see [9, §IX.1]) of F.

(ii) $V^0(F)$ has a universal extension $\overline{V^0(F)}$ by definitions (and therefore conservative) in a language $L_{\overline{V^0(F)}}$ consisting of Σ^B_1-definable functions of $V^0(F)$. The theory $\overline{V^0(F)}$ has quantifier elimination for $\Sigma^B_0(F)$-formulas, and it proves $\Sigma^B_0(F)$-COMP, $\Sigma^B_0(F)$-IND, and $\Sigma^B_0(F)$-MIN, where $\Sigma^B_0(F)$ denotes the class of bounded formulas without second-order quantifiers in $L_{\overline{V^0(F)}}$.

(iii) $V^0(F)$ is closed under Σ^B_0-AC^R, and $V^0(F) + \Sigma^B_0$-AC is $\forall\Sigma^1_1$-conservative over $V^0(F)$.

□

A consequence of (iii) is that whenever a CN theory proves Tot_G for some Σ^B_0-defined function G, it also proves Tot^*_G.

As a special case of Theorem 2.1 for a trivial function F, V^0 has a universal extension $\overline{V^0}$ by definitions in a language $L_{\overline{V^0}}$ (called $\mathcal{L}_{\boldsymbol{FAC}^0}$ in [9]) consisting of Σ^B_1-definable functions of V^0. Unlike general CN theories, it has the property that $\Sigma^B_0(L_{\overline{V^0}}) = \Sigma^B_0$ (more precisely, every $\Sigma^B_0(L_{\overline{V^0}})$ formula is equivalent to a Σ^B_0 formula over $\overline{V^0}$) by [9, L. V.6.7]. In particular, we will use the consequence that if $V^0 \vdash \mathit{Tot}_F$, then $\Sigma^B_0(F) = \Sigma^B_0$.

Note that any finite $\forall\Sigma^B_0$-axiomatized extension of V^0 is trivially a CN theory: an axiom of the form $\forall X\, \varphi(X)$ with $\varphi \in \Sigma^B_0$ is equivalent over V^0 to Tot_{F_φ} and to $\mathit{Tot}^*_{F_\varphi}$ where $\delta_{F_\varphi}(X; Y)$ is $\varphi(X) \wedge Y = 0$. We still have that if $T = V^0 + \forall X\, \varphi(X) \vdash \mathit{Tot}_F$, then $\Sigma^B_0(F) = \Sigma^B_0$ over T (by quantifier elimination for $\overline{V^0}$, $\forall X\, \varphi(X)$ is equivalent to a universal formula in $\overline{V^0}$, thus using Herbrand's theorem, F is defined by an $L_{\overline{V^0}}$ function symbol in $\overline{V^0} + T$).

It is easy to show that $VTC^0 \vdash \mathit{Tot}^*_{\mathrm{card}}$ (see [9, L. IX.3.3]), hence $VTC^0 = V^0(\mathrm{card})$ is a CN theory. The $\Sigma^B_0(\mathrm{card})$-definable predicates in the standard model are exactly the TC^0 predicates.

As we already mentioned above, the whole setup may be formulated for several functions $F_0, \dots, F_k$ in place of F, thus we may define $V^0(F_0, \dots, F_k)$; formally, we may easily combine

$F_0,\dots,F_k$ to a single function, hence $V^0(F_0,\dots,F_k)$ is a CN theory. In particular, we will consider various theories of the form $VTC^0(F) = V^0(\mathrm{card}, F)$. More generally, we could iterate the construction to define CN theories over a fixed CN theory (such as VTC^0) as a base theory in place of V^0; that is, we can introduce $VTC^0(F)$ when F is given by a $\Sigma^B_0(\mathrm{card})$ formula δ_F such that (5) and (6) are provable in VTC^0. One can show that the resulting theories are CN theories according to the original definition. In particular, as explained in [15], $VTC^0 + \mathit{IMUL}$ is a CN theory.

Apart from V^0, VTC^0, and $VTC^0 + \mathit{IMUL}$, we will consider the following CN theories (often in conjunction with VTC^0).

- $VTC^0(\mathrm{Div})$: given Y and $X > 0$, there are $\lfloor Y/X \rfloor$ and $Y \operatorname{rem} X$; i.e, $\delta_{\mathrm{Div}}(X,Y;Q,R)$ is

  $$X = Q = R = 0 \lor (R < X \land Y = QX + R).$$

  The $\mathit{Tot}_{\mathrm{Div}}$ axiom is also denoted DIV. As shown in [15] (using results of Johannsen[16]), $VTC^0(\mathrm{Div}) = VTC^0 + \mathit{IMUL}$.

- $V^0(\mathrm{pow})$: given a, r, and prime m, we can compute $a^r \operatorname{rem} m$, or rather, the witnessing sequence $Y = \langle a^i \operatorname{rem} r : i \le r\rangle$. Formally, $\delta_{\mathrm{pow}}(a,r,m;Y)$ is

  $$\bigl(\neg \mathit{Prime}(m) \land Y = 0\bigr) \lor \bigl(\mathit{Prime}(m) \land Y^{(0)} = 1 \operatorname{rem} m \land \forall i < r\, Y^{(i+1)} = aY^{(i)} \operatorname{rem} m\bigr),$$

  where $\mathit{Prime}(m)$ stands for $m > 1 \land \forall x, y\,(xy = m \to x = 1 \lor y = 1)$, and here and below, we ignore issues with non-uniqueness of sequence codes.

- $V^0(\mathrm{imul})$: given a sequence $\langle a_i : i < n\rangle$ and a prime m, we can find (a witnessing sequence for) $\prod_{i<n} a_i \operatorname{rem} m$. Formally, $\delta_{\mathrm{imul}}(A,n,m;Y)$ is

  $$\bigl(\neg \mathit{Prime}(m) \land Y = 0\bigr) \lor \bigl(\mathit{Prime}(m) \land Y^{(0)} = 1 \operatorname{rem} m \land \forall i < n\, Y^{(i+1)} = Y^{(i)}A^{(i)} \operatorname{rem} m\bigr).$$

- $V^0 + \mathit{WPHP}$: WPHP is the $\forall\Sigma^B_0$ axiom $\forall n\,\forall X\,\mathit{PHP}^{2n}_n(X)$, where $\mathit{PHP}^m_n(X)$ is

  $$\forall x < m\,\exists y < n\, X(x,y) \to \exists x < x' < m\,\exists y < n\,\bigl(X(x,y) \land X(x',y)\bigr).$$

  By results of Paris, Wilkie, and Woods [26], $V^0 + \mathit{WPHP} \subseteq V_0 + \Omega_1$. (This was locally improved by Atserias [2, 3], who showed $V^0 \vdash \forall n\,\forall X\,\bigl(\exists r\, r = n^{(\log n)^{1/k}} \to \mathit{PHP}^{2n}_n(X)\bigr)$ for any constant k.) We mention that VTC^0 even proves $\forall n\,\forall X\,\mathit{PHP}^{n+1}_n(X)$ by [9, Thm. IX.3.23].

- $VL = V^0(\mathrm{Iter})$ (see [9, §IX.6.3]): given a function F from $[0,a]$ to itself, we can compute its iterates $F^i(0)$. Formally, $\delta_{\mathrm{Iter}}(a,F,n;Y)$ is

  $$\bigl(\neg \mathit{Func}(F,a) \land Y = 0\bigr) \lor \bigl(\mathit{Func}(F,a) \land Y^{(0)} = 0 \land \forall i < n\, F\bigl(Y^{(i)}, Y^{(i+1)}\bigr)\bigr),$$

  where $\mathit{Func}(F,a)$ is $\forall x \le a\,\exists! y \le a\, F(x,y)$.

- $VNL = V^0(\mathrm{Reach})$ (see [9, §IX.6.1]): given a relation $E \subseteq [0,a] \times [0,a]$ and d, we can define E-reachability (from 0) in $\le n$ steps. Formally, $\delta_{\mathrm{Reach}}(a, E, n; Y)$ is

$$Y \subseteq [0,d] \times [0,a] \wedge \forall x \le a \, \big[\big(Y(0,x) \leftrightarrow x = 0\big) \\ \wedge \forall d < n \, \big(Y(d+1,x) \leftrightarrow \exists y \le a \, \big(Y(d,y) \wedge (x = y \vee E(y,x))\big)\big)\big]$$

We will use the fact that $VNL = V^0 + Tot_{\mathrm{Reach}}$ (see [9, L. IX.6.7]).

For some of our axioms, we will also need formulas expressing that they hold restricted to some bound:

- $IMUL[w]$ states the totality of the aggregate function of iterated multiplication $\prod_{i<n} X_i$ restricted so that $\sum_{i<n} |X_i| \le w$. Using the formulation of $IMUL$ as above, this can be expressed as

$$\forall n, X \, \exists Y \, \Big(\forall u \le n \, Y^{[u,u]} = 1 \wedge \forall u \le v < n \, \Big(\sum_{i=u}^{v} |X_i| \le w \to Y^{[u,v+1]} = Y^{[u,v]} \cdot X^{[v]}\Big)\Big).$$

- $Tot^*_{\mathrm{Div}}[w]$ states the totality of the aggregate function of division restricted to arguments of length w:

$$\forall n, X, Y \, \exists Q, R \, \forall i < n \, \big(0 < |X^{[i]}| \le w \wedge |Y^{[i]}| \le w \to Y^{[i]} = Q^{[i]} X^{[i]} + R^{[i]} \wedge R^{[i]} < X^{[i]}\big).$$

- $Tot^*_{\mathrm{imul}}[w, -]$ states the totality of imul* restricted to $\prod_{i<n} a_i$ rem m where $n \le w$:

$$\forall t, N, A, M \, \exists Y \, \forall u < t \, \big(N^{(u)} \le w \to \delta_{\mathrm{imul}}\big(A^{[u]}, N^{(u)}, M^{(u)}, Y^{[u]}\big)\big).$$

- $Tot^*_{\mathrm{imul}}[-, w]$ states the totality of imul* restricted to $\prod_{i<n} a_i$ rem m where $m \le w$:

$$\forall t, N, A, M \, \exists Y \, \forall u < t \, \big(M^{(u)} \le w \to \delta_{\mathrm{imul}}\big(A^{[u]}, N^{(u)}, M^{(u)}, Y^{[u]}\big)\big).$$

Berarducci and D'Aquino [6] proved that for any Δ_0-definable function $f(i)$, there exist a Δ_0 definition of the graph of the iterated product $\prod_{i<x} f(i) = y$ such that $I\Delta_0$ proves the recurrence $\prod_{i<0} f(i) = 1$ and (if either side exists) $\prod_{i<x+1} f(i) = f(x) \prod_{i<x} f(i)$. The argument relativizes, hence it applies in V^0 to functions defined by second-order objects: that is, we can construct a well-behaved product $\prod_{i<n} x_i$ of a sequence $X = \langle x_i : i < n \rangle$ as long as $\sum_{i<n} |x_i| \le |w|$ for some w (which guarantees that the resulting product, if any, is a small number, and then by induction on n, that it exists). In our notation, this becomes:

Theorem 2.2 (Berarducci, D'Aquino [6]) *V^0 proves $\forall w \, IMUL\big[|w|\big]$.* □

We will improve this result in Corollary 6.5.

Paris and Wilkie [25] showed how to count polylogarithmic-size sets in $I\Delta_0$, and Paris, Wilkie and Woods [26] extended this to polylogarithmic sums. We can reformulate their results in the two-sorted setup as follows.

Theorem 2.3 *For any constant c, V^0 proves:*

(*i*) *For every X and w, either there exists a* (*unique*) *$s < |w|^c$ and a bijection $F\colon X \to [0,s)$, or there exists an injection $F\colon \bigl[0,|w|^c\bigr) \to X$.*

(*ii*) *For every X and w, there exists a sequence $\bigl\langle \sum_{i<n} X^{[i]} : n \le |w|^c \bigr\rangle$ that satisfies* (3) *and* (4) *for $n < |w|^c$.*

Proof: In [25, Thm. 5′], (i) is proved for Δ_0-definable sets in models of $I\Delta_0$; the argument is uniform in X, hence it also applies to arbitrary sets X in models of V^0. Likewise, (ii) is proved for Δ_0-definable sequences of small numbers in [26, Thm. 10], and the argument applies to arbitrary sequences of small numbers in V^0.

In order to generalize it to sums of sequences of large numbers, we split each $X^{[i]}$ into $|w|$-bit blocks: $X^{[i]} = \sum_{j<2m} x_{i,j} 2^{j|w|}$, where $x_{i,j} < 2^{|w|} \le 2w$, and $m \le \max_i |X^{[i]}|/|w|$. Notice that for each $j < 2m$, we have $\sum_{i<|w|^c} x_{i,j} < |w|^c 2^{|w|} \le 2^{2|w|}$ if w is sufficiently large, hence we may construct Y_{even} and Y_{odd} such that

$$Y^{[n]}_{\mathrm{even}} = \sum_{j<m} 2^{2j|w|} \sum_{i<n} x_{i,2j},$$
$$Y^{[n]}_{\mathrm{odd}} = \sum_{j<m} 2^{(2j+1)|w|} \sum_{i<n} x_{i,2j+1}$$

for each $n \le |w|^c$ by just concatenating suitably shifted copies of the small-number sums $\sum_{i<n} x_{i,j}$. If we then define Y such that $Y^{[n]} = Y^{[n]}_{\mathrm{even}} + Y^{[n]}_{\mathrm{odd}}$, it satisfies the required recurrence $Y^{[0]} = 0$, $Y^{[n+1]} = Y^{[n]} + X^{[n]}$ for $n < |w|^c$. □

Some of our arguments will require rather tight bounds on the sizes of the objects involved, and in particular, on sequence codes. Clearly, we need at least $\approx \sum_{i<n} |X_i|$ bits to encode a sequence $\langle X_i : i < n\rangle$, but the encoding scheme from [9] as defined above does not meet this lower bound: it uses $\approx \bigl(n + \max_i |X_i|\bigr)^2$ bits, which may be quadratically larger than the ideal size in unfavourable conditions. We will now introduce a more efficient encoding scheme in VTC^0; it is based on the idea of Nelson [20, §10], but we repurpose it to directly encode sequences rather than just sets.

The encoding works as follows: the code of $\langle X_i : i < n\rangle$ is a set X representing a pair of sets R, B by $X = \{2x : x \in R\} \cup \{2x+1 : x \in B\}$, where B consists of the concatenation of bits of all the X_i's (in order), and R is a "ruler" indicating where each X_i starts in B; that is, $R = \{r_i : i < n\}$ with $0 = r_0 < r_1 < \dots < r_{n-1}$, and X_i is given by the bits $r_i, \dots, r_{i+1} - 1$ of B (taking $\max\bigl\{|B|, r_{n-1} + 1\bigr\}$ for r_n).

Formally, the sequence coded by X has length $\mathrm{lh}(X) = \mathrm{card}\{x : X(2x)\}$, and for $i < \mathrm{lh}(X)$, the ith element of X, denoted X_i, is

$$\bigl\{x : \exists r\, \bigl(X(2r) \wedge \mathrm{card}\{u < r : X(2u)\} = i \wedge X(2(x+r)+1) \wedge \forall i < x\, \neg X(2(r+i+1))\bigr)\bigr\}.$$

Here, all the quantifiers and comprehension variables can be bounded by $|X|$, hence $\mathrm{lh}(X)$ and X_i are $\Sigma^B_0(\mathrm{card})$-definable in VTC^0, and VTC^0 proves that we can convert X to a set $Y = \bigl\{\langle i, x\rangle : i < \mathrm{lh}(X), x \in X_i\bigr\}$ that represents the same sequence using the sequence encoding from [9] (that is, $Y^{[i]} = X_i$ for all $i < \mathrm{lh}(X)$). Conversely, if Y represents a sequence of length n using the encoding from [9], we can Σ^B_0(card)-define $r_i = \sum_{j<i} \max\bigl\{1, |Y^{[i]}|\bigr\}$ and $X = \{2r_i : i < n\} \cup \bigl\{2(r_i + x) + 1 : i < n, Y(i,x)\bigr\}$ in VTC^0. Then X represents under our new scheme the same sequence as Y and n (i.e., $\mathrm{lh}(X) = n$ and $X_i = Y^{[i]}$ for all $i < n$), and moreover,

$$|X| \le 2 \sum_{i<n} \max\bigl\{1, |X_i|\bigr\}, \tag{7}$$

thus the new encoding scheme realizes the optimal size bound up to a multiplicative constant. We can also encode sequences of small numbers $\langle x_i : i < n\rangle$ by sequences of the corresponding sets, i.e., $\langle X_i : i < n\rangle$ where $X_i = \{j < |x_i| : \mathrm{bit}(x_i, j) = 1\}$.

For general sequences, the efficient coding scheme requires[3] VTC^0. However, for sequences of *polylogarithmic* length (i.e., $\langle X_i : i < n\rangle$ where $n \le |w|^c$ for some w and a standard constant c), it works already in V^0: using Theorem 2.3, $\mathrm{lh}(X)$ and X_i are well-defined in V^0 (in fact, Σ^B_0-definable), and V^0 proves that a given sequence has a code obeying (7).

In the special case $c = 1$, a sequence of small numbers $\langle x_i : i < n\rangle$ such that n and $\sum_i |x_i|$ are bounded by $|w|$ has a code of length $O(|w|)$, and as such, it can be represented by a *small number*. Then the encoding scheme does not involve any second-order objects at all, and it is Δ_0-definable in $I\Delta_0$. When passing to $I\Delta_0$, the statement that a given sequence can be encoded to satisfy (7) becomes the theorem that for any Δ_0-definable function $f(i)$ (possibly with parameters), if $n \le |w|$ and $\sum_{i<n} |f(i)| \le |w|$, there exists $x \le w^{O(1)}$ that encodes the sequence $\langle f(i) : i < n\rangle$.

3 Prime supply

Since we will work extensively with the Chinese remainder representation, we will need lots of primes. To begin with, if we want to represent a number X in CRR modulo a sequence of primes $\langle m_i : i < k\rangle$, we must have $\prod_i m_i > X$, thus we need to get hold of sequences of primes such that $\sum_i |m_i|$ exceeds any given small number.

Already in mid 19th century, Chebyshev proved using elementary methods that the number of primes below x is $\Theta(x/\log x)$, or equivalently,

$$\sum_{p\le x} \log p = \Theta(x). \tag{8}$$

(Here and below in this section, sums indexed by p are supposed to run over primes.) See e.g. Apostol [1, Thm. 4.6] for a nowadays-standard simple result of this type, based on considering the contribution of various primes to the prime factorization of binomial coefficients (this form of

[3] We could make $\mathrm{lh}(X)$ and X_i Σ^B_0-definable using a more elaborate definition of R: e.g., indicate the start of X_i in R not just by a single 1-bit, but by $1 + v_2(i)$ 1-bits (followed by at least one 0-bit). We leave it to the reader's amusement to verify that this encoding is Σ^B_0-decodable, and that it can encode $\langle X_i : i < n\rangle$ using $O\bigl(n + \sum_i |X_i|\bigr)$ bits. But crucially, proving the latter *still* requires VTC^0, or at least some form of approximate counting that allows close enough estimation of $\sum_{j<i} |X_j|$. Thus, we do not really accomplish much with this more complicated scheme.

the proof is due to Erdős and Kalmár). As we will see, it is fairly straightforward to formalize a version of Chebyshev's theorem in VTC^0. Similar to [1], we will compute with sums of logarithms rather than with products of primes, factorials, and binomial coefficients. For our purposes, the simple approximation of $\log n$ by $|n|$ is sufficient.

We mention that Woods [27] proved Sylvester's theorem in $I\Delta_0 + WPHP(\Delta_0)$ by formalizing similar elementary arguments; our job is much easier as we can directly use bounded sums in VTC^0, which Woods avoided by applying $WPHP$ to ingeniously constructed functions (he also needed much more elaborate approximations of logarithms).

In fact, Nguyen [22] already proved a version of (8) with fairly good bounds in VTC^0, also using elaborate approximate logarithms. We keep our argument below (which gives much worse bounds) as it is simpler and more elementary than the proof in [22], while making this paper more self-contained.

First, note that using

$$|x| + |y| - 1 \le |xy| \le |x| + |y|, \tag{9}$$

$I\Delta_0$ proves

$$y = \prod_{i<k} x_i \to |y| \le \sum_{i<k} |x_i| \wedge |y| - 1 \ge \sum_{i<k} \big(|x_i| - 1\big). \tag{10}$$

Considering a sequence of maximal length whose product is x (where we use the efficient sequence encoding), it is easy to prove that every positive number is a product of a sequence of primes:

$$I\Delta_0 \vdash \forall x > 0\, \exists s = \langle p_i : i < k\rangle \Big(x = \prod_{i<k} p_i \wedge \forall i < k\, Prime(p_i)\Big).$$

Moreover, the sequence code s is bounded by a polynomial in x.

By double counting, VTC^0 proves

$$\sum_{\substack{n \le x \\ n = \prod_j p_j}} \sum_j |p_j| = \sum_{p \le x} |p| \sum_{i \colon p^i \le x} \left\lfloor \frac{x}{p^i} \right\rfloor, \tag{11}$$

$$\sum_{\substack{n \le x \\ n = \prod_j p_j}} \sum_j \big(|p_j| - 1\big) = \sum_{p \le x} \big(|p| - 1\big) \sum_{i \colon p^i \le x} \left\lfloor \frac{x}{p^i} \right\rfloor. \tag{12}$$

Here and below in this section, sum indices such as n and i are supposed to start at 1.

Our goal is to prove a lower bound on the number of primes (Theorem 3.2), but we first need the following upper bound, which is a formalization of a weak form of Mertens's theorem: $\sum_{p \le x} p^{-1} = O(\log\log x)$. The reason is that when proving our lower bound, the crude approximation to $\log p$ provided by the $|p|$ function will introduce a copious amount of error into the calculations, and the lemma below is needed to bound the error.

Lemma 3.1 *VTC^0 proves*

$$\sum_{p \le x} \sum_{i \colon p^i \le x} \left\lfloor \frac{x}{p^i} \right\rfloor \le 16x||x||.$$

Proof: Let $k = |x|$. For any $l < |k|$, we have

$$\begin{aligned}
\lceil k2^{-(l+1)} \rceil \sum_{p=2^{\lceil k2^{-(l+1)} \rceil}}^{2^{\lceil k2^{-l} \rceil}-1} \left\lceil \frac{2^k}{p} \right\rceil &\leq \sum_{p=2^{\lceil k2^{-(l+1)} \rceil}}^{2^{\lceil k2^{-l} \rceil}-1} \big(|p|-1\big) \left\lceil \frac{2^k}{p} \right\rceil \\
&\leq 2^{k-\lceil k2^{-l} \rceil} \sum_{p=2^{\lceil k2^{-(l+1)} \rceil}}^{2^{\lceil k2^{-l} \rceil}-1} \big(|p|-1\big) \left\lceil \frac{2^{\lceil k2^{-l} \rceil}}{p} \right\rceil \\
&\leq 2^{k+1-\lceil k2^{-l} \rceil} \sum_{p=2^{\lceil k2^{-(l+1)} \rceil}}^{2^{\lceil k2^{-l} \rceil}-1} \big(|p|-1\big) \left\lfloor \frac{2^{\lceil k2^{-l} \rceil}}{p} \right\rfloor \\
&\leq 2^{k+1-\lceil k2^{-l} \rceil} \sum_{\substack{n<2^{\lceil k2^{-l} \rceil} \\ n=\prod_{j<t} p_j}} \sum_{j<t} \big(|p_j|-1\big) \\
&\leq 2^{k+1-\lceil k2^{-l} \rceil} \sum_{n<2^{\lceil k2^{-l} \rceil}} \big(|n|-1\big) \\
&\leq 2^{k+1} \big(\lceil k2^{-l} \rceil - 1\big)
\end{aligned}$$

using (10) and (12), thus

$$\sum_{p=2^{\lceil k2^{-(l+1)} \rceil}}^{2^{\lceil k2^{-l} \rceil}-1} \left\lceil \frac{2^k}{p} \right\rceil \leq \frac{\lceil k2^{-l} \rceil - 1}{\lceil k2^{-(l+1)} \rceil} 2^{k+1} \leq 2^{k+2}.$$

Summing over all $l < |k|$ gives

$$\sum_{p<2^k} \left\lceil \frac{2^k}{p} \right\rceil \leq 2^{k+2}|k|,$$

thus

$$\sum_{p \leq x} \left\lceil \frac{x}{p} \right\rceil \leq 2^{k+2}|k| \leq 8x||x||$$

as $x < 2^k \leq 2x$. Then estimating the geometric series

$$\sum_{i:\, p^i \leq x} \left\lfloor \frac{x}{p^i} \right\rfloor \leq 2 \left\lceil \frac{x}{p} \right\rceil$$

gives the result. $\square$

Theorem 3.2 *There is a standard constant c such that VTC^0 proves*

$$x \geq c \to \sum_{p \leq x|x|^{17}} \big(|p|-1\big) \geq x.$$

Proof: For any $0 < x < y$, we have

$$\begin{aligned}
x(|y|-|x|+1) &\le \sum_{y<n\le x+y} |n| - \sum_{n\le x}\big(|n|-1\big) \\
&\le \sum_{\substack{y<n\le x+y\\ n=\prod_j p_j}} \sum_j |p_j| - \sum_{\substack{n\le x\\ n=\prod_j p_j}} \sum_j \big(|p_j|-1\big) \\
&\le \sum_{p\le x+y} |p| \sum_{i\colon p^i\le x+y} \left(\left\lfloor\frac{x+y}{p^i}\right\rfloor - \left\lfloor\frac{y}{p^i}\right\rfloor\right) - \sum_{p\le x}\big(|p|-1\big) \sum_{i\colon p^i\le x} \left\lfloor\frac{x}{p^i}\right\rfloor \\
&\le \sum_{p\le x+y} |p| \sum_{i\colon p^i\le x+y} \left(\left\lfloor\frac{x+y}{p^i}\right\rfloor - \left\lfloor\frac{x}{p^i}\right\rfloor - \left\lfloor\frac{y}{p^i}\right\rfloor\right) + \sum_{p\le x}\sum_{i\colon p^i\le x} \left\lfloor\frac{x}{p^i}\right\rfloor \\
&\le \sum_{p\le x+y} |p| \sum_{i\colon p^i\le x+y} 1 + 16x||x|| \\
&\le \sum_{p\le x+y} |p| + \sum_{p\le\sqrt{x+y}} |p| \left\lfloor\frac{|x+y|-1}{|p|-1}\right\rfloor + 16x||x|| \\
&\le \sum_{p\le x+y} |p| + 2|x+y|\lfloor\sqrt{x+y}\rfloor + 16x||x||
\end{aligned}$$

using (10)–(12) and Lemma 3.1. Taking $y = x|x|^{17} - x$, we have $|y| \ge |x+y|-1 \ge |x|+17||x||-18$ and $|x+y| \le |x| + 17||x||$ by (10), thus

$$\sum_{p\le x|x|^{17}} |p| \ge \big(17||x|| - 17 - 16||x||\big)x - 2\big(|x| + 17||x||\big)\lfloor\sqrt{x|x|^{17}}\rfloor \ge \big(||x|| - 18\big)x$$

and

$$\sum_{p\le x|x|^{17}} \big(|p|-1\big) \ge \frac{1}{2}\sum_{p\le x|x|^{17}} |p| \ge \frac{||x||-18}{2}\,x \ge x$$

for large enough x. □

4 Division by small primes

We need a one more simple but important preparatory result: VTC^0(pow), and a fortiori VTC^0(imul), can perform division with remainder by *small primes.* This is indispensable when working with the Chinese remainder representation: it is required to define the CRR in the first place, but we will also extensively use it when studying its properties.

Notice that pow directly provides $2^n \operatorname{rem} m$, and as it turns out, the bits of $\lfloor 2^n/m\rfloor$ can be explicitly expressed in terms of $2^i \operatorname{rem} m$ as well. We then obtain $\lfloor X/m\rfloor$ and $X \operatorname{rem} m$ for general X by summing over its bits.

Lemma 4.1 VTC^0(pow) *proves that we can divide by small primes:*

$$\forall X\,\forall m\,\big(Prime(m) \to \exists Q\,\exists r < m\; X = mQ + r\big).$$

Proof: We may assume m is odd. Let us first consider $X = 2^n$. Using pow, define

$$Q_n = \sum_{i<n} 2^i \big((2^{n-i} \text{ rem } m) \text{ rem } 2\big).$$

We will prove

$$2^n = mQ_n + (2^n \text{ rem } m) \tag{13}$$

by induction on n. The statement holds for $n = 0$. For the induction step, we have

$$\begin{aligned} Q_{n+1} &= \sum_{i<n+1} 2^i \big((2^{n+1-i} \text{ rem } m) \text{ rem } 2\big) \\ &= \big((2^{n+1} \text{ rem } m) \text{ rem } 2\big) + \sum_{i<n} 2^{i+1} \big((2^{n-i} \text{ rem } m) \text{ rem } 2\big) \\ &= 2Q_n + \big((2^{n+1} \text{ rem } m) \text{ rem } 2\big), \end{aligned}$$

thus using the induction hypothesis,

$$\begin{aligned} mQ_{n+1} &= 2mQ_n + \big((2^{n+1} \text{ rem } m) \text{ rem } 2\big)m \\ &= 2^{n+1} - 2(2^n \text{ rem } m) + \big((2^{n+1} \text{ rem } m) \text{ rem } 2\big)m. \end{aligned}$$

Now, either $2^n \text{ rem } m < m/2$, in which case

$$2^{n+1} \text{ rem } m = 2(2^n \text{ rem } m) \qquad \text{and} \qquad (2^{n+1} \text{ rem } m) \text{ rem } 2 = 0,$$

or $2^n \text{ rem } m > m/2$, in which case

$$2^{n+1} \text{ rem } m = 2(2^n \text{ rem } m) - m \qquad \text{and} \qquad (2^{n+1} \text{ rem } m) \text{ rem } 2 = 1.$$

Either way,

$$(2^{n+1} \text{ rem } m) + \big((2^{n+1} \text{ rem } m) \text{ rem } 2\big)m = 2(2^n \text{ rem } m),$$

hence $mQ_{n+1} = 2^{n+1} - (2^{n+1} \text{ rem } m)$ as required.

Now, for general X, we have

$$X = \sum_{n \in X} 2^n = m \sum_{n \in X} Q_n + x,$$

where

$$x = \sum_{n \in X} (2^n \text{ rem } m) \leq |X|\, m$$

is small, thus already $I\Delta_0$ can divide x by m, yielding $X = m\big(Q_n + \lfloor x/m \rfloor\big) + (x \text{ rem } m)$. $\square$

5 Chinese remainder representation

We are coming to the core technical part of the paper. First, the basic definition:

Definition 5.1 (In $VTC^0(\mathrm{pow})$.) If $\vec{m} = \langle m_i : i < k \rangle$ is a sequence of distinct primes, the *Chinese remainder representation* (*CRR*) of X modulo $\vec{m}$ is the sequence $X \operatorname{rem} \vec{m} = \langle X \operatorname{rem} m_i : i < k \rangle$, which is well-defined by Lemma 4.1. The sequence $\vec{m}$ is called the *basis* of the CRR.

Our goal in this section is to define in $VTC^0(\mathrm{imul})$ a CRR reconstruction procedure, that is, a function that recovers X from $X \operatorname{rem} \vec{m}$ (under suitable conditions); this will in turn easily imply that $VTC^0(\mathrm{imul})$ proves *IMUL*.

The principal problem we face when trying to formalize the CRR reconstruction procedure from [13] is that the argument involves various numbers constructed by iterated multiplication (and division), which we do not a priori know to exist when working inside $VTC^0(\mathrm{imul})$. Besides many references to the product $\prod_i m_i$, the reconstruction procedure for instance involves computing a CRR representation of a product of the form $X \prod_{u<t} \frac{1}{2}\bigl(1 + \prod_j a_{u,j}\bigr)$ for a certain sequence of primes $a_{u,j}$. We sidestep these problems by developing in $VTC^0(\mathrm{imul})$ low-level operations on CRR. We will systematically exploit the fact that even though we cannot a priori convert a CRR representation to the number X it represents, we *can* compute certain "shadows" of X: approximations to the ratio $X/\prod_i m_i$, and $X \operatorname{rem} a$ for small primes a; we will formally define these quantities shortly in Definition 5.3, but let us first introduce a few notational conventions in order to save repetitive typing.

Definition 5.2 (In $VTC^0(\mathrm{imul})$.) In this section, $\vec{m}$ stands for a sequence of distinct primes, whose length is denoted k: $\vec{m} = \langle m_i : i < k \rangle$. When we need another sequence of primes, we use $\vec{a}$ of length l. We write $\vec{x} < \vec{m}$ for $\vec{x}$ being a sequence of residues modulo $\vec{m}$, i.e., $\vec{x} = \langle x_i : i < k \rangle$ such that $0 \le x_i < m_i$ for each $i < k$.

We put $[\vec{m}] = \prod_{i<k} m_i$ (evaluated using imul modulo some prime specified in the context), and likewise $[\vec{m}]_{\ne i} = \prod_{j \ne i} m_j$. If $\vec{m}$ and $\vec{a}$ are sequences of primes, $\vec{m} \perp \vec{a}$ denotes that each m_i is coprime to (i.e., distinct from) each a_j. We interpret mod / rem notations modulo $\vec{m}$ elementwise, so that, e.g., $X \operatorname{rem} \vec{m}$ means $\langle X \operatorname{rem} m_i : i < k \rangle$ (as already indicated in Definition 5.1), $\vec{y} = \vec{x} \operatorname{rem} \vec{m}$ means $y_i = x_i \operatorname{rem} m_i$ for each $i < k$, and $\vec{x} \equiv \vec{y} \pmod{\vec{m}}$ means $x_i \equiv y_i \pmod{m_i}$ for each $i < k$.

We will write $y = x \pm a$ for $x - a \le y \le x + a$; more generally, $y = x \pm^a_b$ abbreviates $x - b \le y \le x + a$.

In the real world, if $\vec{x}$ is the CRR of X modulo a basis $\vec{m}$, we can reconstruct X by

$$X \equiv \sum_{i<k} x_i h_i [\vec{m}]_{\ne i} \pmod{[\vec{m}]},$$

where $h_i = [\vec{m}]^{-1}_{\ne i} \operatorname{rem} m_i$ (recall that this denotes the multiplicative inverse of $[\vec{m}]_{\ne i}$ modulo m_i). Thus, the right-hand side equals $X + r[\vec{m}]$ for some natural number r, easily seen to satisfy $r < \sum_i m_i$. This integer is called the *rank* of $\vec{x}$, and it obeys

$$\sum_{i<k} \frac{x_i h_i}{m_i} = r + \frac{X}{[\vec{m}]}. \tag{14}$$

This equation holds (with the same r) in any field where the $\vec{m}$ are invertible: in particular, evaluating (14) in $\mathbb{Q}$ can provide TC^0 approximations to $X/[\vec{m}]$, and evaluating it modulo a prime a coprime to $\vec{m}$ yields the value of X modulo a, that is, an extension of $\vec{x}$ to CRR modulo the basis $\langle \vec{m}, a \rangle$ ("basis extension").

We need *IMUL* to make sense of (14) in $\mathbb{Q}$, hence we cannot use it directly in VTC^0(imul). However, we will consider an approximation of rank and related quantities, and we will prove their various properties from first principles, which will ultimately allow us to make CRR reconstruction work.

Definition 5.3 (In VTC^0(imul).) Given $\vec{x} < \vec{m}$ and n, let $h_i = [\vec{m}]_{\neq i}^{-1} \operatorname{rem} m_i$ for $i < k$, and define

$$\begin{aligned} S_n(\vec{m}; \vec{x}) &= \sum_{i<k} \left\lceil \frac{2^n x_i h_i}{m_i} \right\rceil, \\ r_n(\vec{m}; \vec{x}) &= \lfloor 2^{-n} S_n(\vec{m}; \vec{x}) \rfloor, \\ \xi_n(\vec{m}; \vec{x}) &= 2^{-n} \big(S_n(\vec{m}; \vec{x}) \operatorname{rem} 2^n \big), \\ e_n(\vec{m}; \vec{x}; a) &= \Big(\sum_{i<k} x_i h_i [\vec{m}]_{\neq i} - [\vec{m}] r_n(\vec{m}; \vec{x}) \Big) \operatorname{rem} a \end{aligned}$$

for any prime a, using Lemma 4.1 and imul. That is, $r_n \leq \sum_i m_i$ is an estimate of the rank of $\vec{x}$, $\xi_n \in [0,1]$ is a dyadic rational approximation of $X/[\vec{m}]$ per (14), and $e_n < a$ is an estimate of X modulo a. In order to make the notation less heavy, we may omit $\vec{m}$ if it is understood from the context.

Observe that

$$e_n(\vec{m}; \vec{x}; m_i) = x_i. \tag{15}$$

If $\vec{a}$ is a sequence of primes (which may include $\vec{m}$), we let $e_n(\vec{m}; \vec{x}; \vec{a}) = \langle e_n(\vec{m}; \vec{x}; a_j) : j < l \rangle$. This should be thought of as extension of $\vec{x}$ to CRR modulo $\vec{a}$.

Example 5.4 Let $\vec{x} = \vec{1}$ (which is the CRR of $X = 1$). Then for n large enough, $e_n(\vec{m}; \vec{x}; a) = 1$ and $\xi_n(\vec{m}; \vec{x}) \approx 1/[\vec{m}]$. See Lemma 5.8 for a formalization of this.

Note that the rank is a discrete quantity; while $2^{-n} S_n$ is an approximation of $\sum_i x_i h_i / m_i$ that can be expected to converge in a reasonable way to the true value as n gets larger, r_n will make abrupt jumps. If r_n happens to be the true rank, then ξ_n should be a close approximation of $X/[\vec{m}]$, and e_n has the correct value, but if r_n is off by 1, then ξ_n is very far from the right value, and e_n (another discrete quantity) is also off. Thus, one of the annoying problems we need to deal with in VTC^0(imul) is that it is a priori difficult to guess how large n we need so that r_n is "correct".

The remainder of this section is organized into two subsections. In Section 5.1, we will develop computation with CRR in VTC^0(imul), in particular, we will show how various manipulations of CRR affect the related r_n, ξ_n, and e_n values. In Section 5.2, we define and analyze the CRR reconstruction procedure and derive $IMUL$ in VTC^0(imul).

5.1 Auxiliary properties of CRR

Results in this section are nominally proved in the theory VTC^0(imul). In fact, the proofs will only use instances of imul modulo primes listed in the statements ($\vec{m}$, sometimes $\vec{a}$ or $\vec{b}$), which fact will become relevant in Section 8. However, we do not indicate this explicitly in an effort not to make the notation more cluttered than it already is.

We start with two lemmas on basis extension. The first one is a formalization of the observation that if $\vec{x} < \vec{m}$ is the CRR of $X < [\vec{m}]$, and $\vec{a} \perp \vec{m}$, then the CRR of $[\vec{a}]X < [\vec{m}][\vec{a}]$ modulo the extended basis $\langle \vec{m}, \vec{a} \rangle$ is $\langle [\vec{a}]\vec{x}, \vec{0} \rangle$. Here and below, operations on residue sequences $\vec{x} < \vec{m}$ (such as multiplication by $[\vec{a}]$) are assumed to be evaluated modulo $\vec{m}$.

Lemma 5.5 VTC^0(imul) *proves that for any $\vec{x} < \vec{m}$ and $\vec{a}, a \perp \vec{m}$,*

$$r_n(\vec{m}, a; a\,\vec{x}, 0) = r_n(\vec{m}; \vec{x}) + \sum_{i<k} x_i \left\lfloor \frac{a\tilde{h}_i}{m_i} \right\rfloor, \tag{16}$$

$$e_n(\vec{m}, \vec{a}; [\vec{a}]\vec{x}, \vec{0}; \vec{b}) = [\vec{a}] e_n(\vec{m}; \vec{x}; \vec{b}) \text{ rem } \vec{b}, \tag{17}$$

$$\xi_n(\vec{m}, \vec{a}; [\vec{a}]\vec{x}, \vec{0}) = \xi_n(\vec{m}; \vec{x}), \tag{18}$$

where $\tilde{h}_i = (a[\vec{m}]_{\neq i})^{-1} \text{ rem } m_i$.

Proof: Let $h_i = [\vec{m}]_{\neq i}^{-1} \text{ rem } m_i$. We have $a\tilde{h}_i \equiv h_i \pmod{m_i}$, i.e.,

$$a\tilde{h}_i = h_i + m_i \left\lfloor \frac{a\tilde{h}_i}{m_i} \right\rfloor, \tag{19}$$

thus

$$\begin{aligned} S_n(\vec{m}, a; a\,\vec{x}, 0) &= \sum_{i<k} \left\lceil \frac{2^n x_i a\tilde{h}_i}{m_i} \right\rceil = \sum_{i<k} \left\lceil \frac{2^n x_i h_i}{m_i} \right\rceil + 2^n \sum_{i<k} x_i \left\lfloor \frac{a\tilde{h}_i}{m_i} \right\rfloor \\ &= S_n(\vec{m}; \vec{x}) + 2^n \sum_{i<k} x_i \left\lfloor \frac{a\tilde{h}_i}{m_i} \right\rfloor. \end{aligned}$$

This gives (16), and (18) for $l = 1$; the general case of (18) follows by induction[4] on l.

We can again prove (17) by induction on l, hence it is enough to show it for $l = 1$. Obviously,

[4] More precisely: for fixed $\vec{a} = \langle a_i : i < l \rangle$, we prove by induction on $l' \leq l$ that (18) holds for $\langle a_i : i < l' \rangle$, which is a Σ_0^B(imul) property. Most proofs by induction in this section should be interpreted similarly.

we may also assume $\mathrm{lh}(\vec{b}) = 1$. Computing modulo b, we have

$$\begin{aligned}
e_n(\vec{m}, a; a\vec{x}, 0; b) &\equiv \sum_{i<k} a x_i \tilde{h}_i a[\vec{m}]_{\neq i} - a[\vec{m}] r_n(\vec{m}, a; a\,\vec{x}, 0) \\
&\equiv a\Big(\sum_{i<k} x_i a\tilde{h}_i [\vec{m}]_{\neq i} - [\vec{m}] r_n(\vec{m}, a; a\,\vec{x}, 0)\Big) \\
&\equiv a\left(\sum_{i<k} x_i h_i [\vec{m}]_{\neq i} + [\vec{m}] \sum_{i<k} x_i \left\lfloor \frac{a\tilde{h}_i}{m_i} \right\rfloor - [\vec{m}] r_n(\vec{m}, a; a\,\vec{x}, 0)\right) \\
&\equiv a\Big(\sum_{i<k} x_i h_i [\vec{m}]_{\neq i} - [\vec{m}] r_n(\vec{m}; \vec{x})\Big) \\
&\equiv a\, e_n(\vec{m}; \vec{x}; b)
\end{aligned}$$

using (19) and (16). □

The second lemma formalizes the idea that $e_n(\vec{m}; \vec{x}; \vec{m}, \vec{a}) = \langle \vec{x}, e_n(\vec{m}; \vec{x}; \vec{a})\rangle$ is the extension of $\vec{x}$ to the basis $\langle \vec{m}, \vec{a}\rangle$ (representing the same number). Since the effect of basis extension on the ξ_n approximation is essentially division by $[\vec{a}]$, which we cannot do directly, we first formulate the result for a single prime a, and then we obtain a version for arbitrary $\vec{a}$ using a crude approximation of $[\vec{a}]$.

Lemma 5.6 *VTC^0(imul) proves that for any $\vec{x} < \vec{m}$ and $a \perp \vec{m}$, if $n \geq |k|$, then*

$$a\, r_n\big(\vec{m}, a; e_n(\vec{m}; \vec{x}; \vec{m}, a)\big) = r_n(\vec{m}; \vec{x}) + e_n(\vec{m}; \vec{x}; a)\tilde{h} + \sum_{i<k} x_i \left\lfloor \frac{a\tilde{h}_i}{m_i} \right\rfloor, \tag{20}$$

$$e_n\big(\vec{m}, a; e_n(\vec{m}; \vec{x}; \vec{m}, a); \vec{b}\big) = e_n(\vec{m}; \vec{x}; \vec{b}), \tag{21}$$

$$\xi_n\big(\vec{m}, a; e_n(\vec{m}; \vec{x}; \vec{m}, a)\big) = \tfrac{1}{a}\xi_n(\vec{m}; \vec{x}) \pm_0^{2^{-n}(k+1)(1-a^{-1})}, \tag{22}$$

where $\tilde{h} = [\vec{m}]^{-1}$ rem a, $\tilde{h}_i = (a[\vec{m}]_{\neq i})^{-1}$ rem m_i.

Proof: Put $h_i = [\vec{m}]_{\neq i}^{-1}$ rem m_i and $y = e_n(\vec{m}; \vec{x}; a)$ so that $e_n(\vec{m}; \vec{x}; \vec{m}, a) = \langle \vec{x}, y\rangle$, and let ϱ denote the right-hand side of (20). First, using (19), we have

$$\begin{aligned}
[\vec{m}]\varrho &\equiv [\vec{m}] r_n(\vec{x}) + y + \sum_{i<k} x_i m_i \left\lfloor \frac{a\tilde{h}_i}{m_i} \right\rfloor [\vec{m}]_{\neq i} \\
&\equiv \sum_{i<k} x_i h_i [\vec{m}]_{\neq i} + \sum_{i<k} x_i m_i \left\lfloor \frac{a\tilde{h}_i}{m_i} \right\rfloor [\vec{m}]_{\neq i} \equiv \sum_{i<k} x_i a\tilde{h}_i [\vec{m}]_{\neq i} \equiv 0 \pmod{a},
\end{aligned}$$

that is, ϱ/a is an integer. Observe that for any rational ω, $a\lceil\omega\rceil < a(\omega+1) = a\omega + a \leq \lceil a\omega\rceil + a$, hence

$$\lceil a\omega\rceil \leq a\lceil\omega\rceil \leq \lceil a\omega\rceil + (a-1).$$

Using this, we obtain

$$\begin{aligned}
2^n\big(\varrho+\xi_n(\vec m;\vec x)\big)&=S_n(\vec m;\vec x)+2^n\left(y\tilde h+\sum_{i<k}x_i\left\lfloor\frac{a\tilde h_i}{m_i}\right\rfloor\right)\\
&=\sum_{i<k}\left\lceil\frac{2^nx_ih_i}{m_i}\right\rceil+\sum_{i<k}\frac{2^nx_im_i\lfloor a\tilde h_i/m_i\rfloor}{m_i}+2^ny\tilde h\\
&=\sum_{i<k}\left\lceil\frac{2^nax_i\tilde h_i}{m_i}\right\rceil+2^ny\tilde h\\
&=a\sum_{i<k}\left\lceil\frac{2^nx_i\tilde h_i}{m_i}\right\rceil+a\left\lceil\frac{2^ny\tilde h}{a}\right\rceil\pm^{0}_{(k+1)(a-1)}\\
&=aS_n(\vec m,a;\vec x,y)\pm^{0}_{(k+1)(a-1)}.
\end{aligned}$$

On the one hand, this gives $\varrho/a\le 2^{-n}S_n(\vec m,a;\vec x,y)<\big(r_n(\vec m,a;\vec x,y)+1\big)$, thus $\varrho/a\le r_n(\vec m,a;\vec x,y)$. On the other hand,

$$a\,r_n(\vec m,a;\vec x,y)\le 2^{-n}a\,S_n(\vec m,a;\vec x,y)<\varrho+1+2^{-n}(k+1)(a-1)\le\varrho+a$$

as long as $2^n\ge k+1$, thus $r_n(\vec m,a;\vec x,y)<\varrho/a+1$, i.e., $r_n(\vec m,a;\vec x,y)\le\varrho/a$. This proves (20), whence also (22):

$$a\,\xi_n(\vec m,a;\vec x,y)=2^{-n}a\,S_n(\vec m,a;\vec x,y)-\varrho=\xi_n(\vec m;\vec x)\pm^{2^{-n}(k+1)(a-1)}_{0}.$$

To prove (21), we may assume $\mathrm{lh}(\vec b)=1$; working modulo b,

$$\begin{aligned}
e_n(\vec m,a;\vec x,y;b)&\equiv\sum_{i<k}x_i\tilde h_ia[\vec m]_{\ne i}+y\tilde h[\vec m]-[\vec m]a\,r_n(\vec m,a;\vec x,y)\\
&\equiv\sum_{i<k}x_ih_i[\vec m]_{\ne i}+[\vec m]\left(\sum_{i<k}x_i\left\lfloor\frac{a\tilde h_i}{m_i}\right\rfloor+y\tilde h-a\,r_n(\vec m,a;\vec x,y)\right)\\
&\equiv\sum_{i<k}x_ih_i[\vec m]_{\ne i}-r_n(\vec m;\vec x)\\
&\equiv e_n(\vec m;\vec x;b)
\end{aligned}$$

using (19) and (20). □

Corollary 5.7 *VTC^0(imul) proves that for any $\vec x<\vec m$ and $\vec a\perp\vec m$, if $n\ge|k+l|$, then*

$$e_n\big(\vec m,\vec a;e_n(\vec m;\vec x;\vec m,\vec a);\vec b\big)=e_n(\vec m;\vec x;\vec b),\tag{23}$$

$$2^{-\sum_j|a_j|}\xi_n(\vec m;\vec x)\le\xi_n\big(\vec m,\vec a;e_n(\vec m;\vec x;\vec m,\vec a)\big)\le 2^{-\sum_j(|a_j|-1)}\xi_n(\vec m;\vec x)+2^{-n}(k+l).\tag{24}$$

Proof: By induction in l, using (21), (22), and $2^{-|a|}<\frac1a\le 2^{-(|a|-1)}$. □

The CRR of 1, which is just the sequence $\vec 1$, will feature prominently in many calculations, as $\xi_n(\vec m;\vec 1)$ is our proxy for $1/[\vec m]$. The next lemma summarizes its most basic properties.

Lemma 5.8 *VTC^0(imul) proves: if $n \ge |k| \ge 1$, then*

$$2^{-\sum_i |m_i|} < \xi_n(\vec{m}; \vec{1}) < 2^{-\sum_i(|m_i|-1)} + 2^{-n}(k+1), \tag{25}$$

$$e_n(\vec{m}; \vec{1}; \vec{a}) = \vec{1}. \tag{26}$$

Proof: Since $m_0 \ge 2$ and $2^n \ge 2$, we have $r_n(m_0; 1) = \lfloor 2^{-n} \lceil 2^n/m_0 \rceil \rfloor = 0$, thus

$$e_n(m_0; 1; a) = 1 \cdot 1 \cdot 1 - 0 = 1$$

for any a, i.e., $e_n(m_0; 1; \vec{a}) = \vec{1}$. In particular, $e_n(m_0; 1; \vec{m}) = \vec{1}$, hence

$$e_n(\vec{m}; \vec{1}; \vec{a}) = e_n\big(\vec{m}; e_n(m_0; 1; \vec{m}); \vec{a}\big) = e_n(m_0; 1; \vec{a}) = \vec{1}$$

by (23). Moreover,

$$2^{-|m_0|} < \frac{1}{m_0} \le 2^{-n} \left\lceil \frac{2^n}{m_0} \right\rceil = \xi_n(m_0; 1) < \frac{1}{m_0} + 2^{-n} \le 2^{-(|m_0|-1)} + 2^{-n},$$

thus

$$\begin{aligned} \xi_n(\vec{m}; \vec{1}) = \xi_n\big(\vec{m}; e_n(m_0; 1; \vec{m})\big) &\le 2^{-\sum_{i>0}(|m_i|-1)} \xi_n(m_0; 1) + 2^{-n}k \\ &< 2^{-\sum_i(|m_i|-1)} + 2^{-n}(k+1) \end{aligned}$$

using (24). The other inequality is similar. $\square$

The next lemma expresses the fact that if $\vec{x}$ and $\vec{y}$ are respectively the CRR of $X, Y < [\vec{m}]$, then $\vec{x} + \vec{y}$ (modulo $\vec{m}$) is the CRR of $(X+Y) \bmod [\vec{m}]$, which is $X + Y - c[\vec{m}]$ for $c \in \{0, 1\}$. The first version we prove here also allows $c = -1$ (which is impossible in the real world); we will fix this discrepancy in Corollary 5.11 below, under a stronger requirement on n.

Lemma 5.9 *VTC^0(imul) proves: if $\vec{x}, \vec{y} < \vec{m}$, $\vec{z} = (\vec{x} + \vec{y}) \operatorname{rem} \vec{m}$, and $n \ge |k|$, then there exists $c \in \{-1, 0, 1\}$ such that*

$$r_n(\vec{m}; \vec{z}) = r_n(\vec{m}; \vec{x}) + r_n(\vec{m}; \vec{y}) + c - \sum_{x_i + y_i \ge m_i} h_i, \tag{27}$$

$$e_n(\vec{m}; \vec{z}; a) \equiv e_n(\vec{m}; \vec{x}; a) + e_n(\vec{m}; \vec{y}; a) - c[\vec{m}] \pmod{a}, \tag{28}$$

$$\xi_n(\vec{m}; \vec{z}) = \xi_n(\vec{m}; \vec{x}) + \xi_n(\vec{m}; \vec{y}) - c \pm^{0}_{2^{-n}k}, \tag{29}$$

where $h_i = [\vec{m}]^{-1}_{\ne i} \operatorname{rem} m_i$.

Proof: Let $I = \{i < k : x_i + y_i \ge m_i\}$, so that $z_i = x_i + y_i$ for $i \notin I$, and $z_i = x_i + y_i - m_i$ for $i \in I$. Then

$$\begin{aligned} 2^{-n} S_n(\vec{m}; \vec{z}) &= 2^{-n} \sum_{i<k} \left\lceil \frac{2^n (x_i + y_i) h_i}{m_i} \right\rceil - \sum_{i \in I} h_i \\ &= 2^{-n} S_n(\vec{m}; \vec{x}) + 2^{-n} S_n(\vec{y}; \vec{m}) - \sum_{i \in I} h_i \pm^{0}_{2^{-n}k} \\ &= r_n(\vec{m}; \vec{x}) + r_n(\vec{y}; \vec{m}) - \sum_{i \in I} h_i + \xi_n(\vec{m}; \vec{x}) + \xi_n(\vec{y}; \vec{m}) \pm^{0}_{2^{-n}k}. \end{aligned}$$

Since $k \le 2^n$ and $0 \le \xi_n(\vec m;\vec x) + \xi_n(\vec y;\vec m) < 2$, this readily implies (27) and (29). Moreover,

$$\begin{aligned} e_n(\vec m;\vec z;a) &\equiv \sum_{i<k} x_i h_i[\vec m]_{\ne i} + \sum_{i<k} y_i h_i[\vec m]_{\ne i} - \sum_{i\in I} h_i[\vec m] \\ &\qquad - \Big(r_n(\vec m;\vec x) + r_n(\vec m;\vec y) + c - \sum_{i\in I} h_i\Big)[\vec m] \\ &\equiv e_n(\vec m;\vec x;a) + e_n(\vec m;\vec y;a) - c[\vec m] \end{aligned}$$

modulo a. □

The following lemma can be read as stating that $0 < X < [\vec m] \implies 1 \le X \le [\vec m]-1$. While this sounds like a triviality, it is in fact an important result implying that (for large enough n) ξ_n cannot take arbitrary values in $[0,1]$, but it is a discrete quantity coming in steps of $1/[\vec m]$ (i.e., $\xi_n(\vec m;\vec 1)$). Among other consequences, this will eventually allows us to prove a bound on n above which r_n and e_n stabilize.

Lemma 5.10 *VTC^0*(imul) *proves that for any $\vec 0 \ne \vec x < \vec m$,*

$$\min\big\{\xi_n(\vec m;\vec x), 1-\xi_n(\vec m;\vec x)\big\} \ge \xi_n(\vec m;\vec 1) - 2^{-n}(3k). \tag{30}$$

Proof: The statement is vacuous for $k = 0$, and it also holds trivially unless $2^n > 3k$ and $\xi_n(\vec m;\vec 1) > 2^{-n}(3k)$. We claim that this condition implies

$$2^n \ge \max_{i<k} m_i. \tag{31}$$

If $k \ge 2$, then $\xi_n(\vec m;\vec 1) > 2^{-n}(3k)$ gives

$$2^{-n}(3k) < 2^{-\sum_i(|m_i|-1)} + 2^{-n}(k+1)$$

by (25), hence

$$\max_{i<k} m_i \le 2^{1+\sum_i(|m_i|-1)} \le (2k-1)2^{\sum_i(|m_i|-1)} < 2^n.$$

If $k = 1$, then $m_0 \ge 2$ and $n \ge 1$ ensure $\lceil 2^n/m_0\rceil \le 2^{n-1} < 2^n$, thus $\xi_n(m_0;1) = 2^{-n}\lceil 2^n/m_0\rceil$. If $2^n\xi_n(m_0;1) > 3k = 3$, we obtain $2^n/m_0 > 3$, and a fortiori $2^n \ge m_0$.

Now, let us prove (30) by induction on k. For $k = 1$, we have $\xi_n(m_0;1) = 2^{-n}\lceil 2^n/m_0\rceil$, and (31) ensures $\lceil 2^n(m_0-1)/m_0\rceil < 2^n$, thus $\xi_n(m_0;x) = 2^{-n}\lceil 2^n x/m_0\rceil$, and we obtain

$$\xi_n(m_0;1) \le \xi_n(m_0;x) \le 1 - \xi_n(m_0;1) + 2^{-n}.$$

Assume (30) holds for $k \ge 1$, we will prove it for $k+1$. Let $\langle \vec 0, 0\rangle \ne \langle \vec x, y\rangle < \langle \vec m, m_k\rangle$. As above, we assume $\xi_n(\vec m, m_k;\vec 1, 1) > 3(k+1)2^{-n}$, thus $2^n \ge m_k$ by (31), which ensures $\lceil 2^n(m_k-1)/m_k\rceil < 2^n$.

We have

$$\xi_n(\vec m, m_k;\vec 1, 1) \le \frac{1}{m_k}\xi_n(\vec m;\vec 1) + 2^{-n}(k+1)(1-m_k^{-1}) \tag{32}$$

by (22). We distinguish two cases. If $\vec{x} = \vec{0}$, let $\tilde{y} = y[\vec{m}]^{-1}$ rem m_k; then $1 \le \tilde{y} \le m_k - 1$, and

$$\xi_n(\vec{m}, m_k; \vec{x}, y) = 2^{-n} \left\lceil \frac{2^n \tilde{y}}{m_k} \right\rceil = \frac{\tilde{y}}{m_k} \pm {}^{2^{-n}}_{0},$$

hence

$$\min\bigl\{\xi_n(\vec{m}, m_k; \vec{x}, y), 1 - \xi_n(\vec{m}, m_k; \vec{x}, y)\bigr\} \ge \frac{1}{m_k} - 2^{-n} \ge \xi_n(\vec{m}, m_k; \vec{1}, 1) - 2^{-n}(k+2)$$

using (32).

If $\vec{x} \ne \vec{0}$, let $y' = \bigl(y - e_n(\vec{m}; \vec{x}; m_k)\bigr)$ rem m_k, and $\tilde{y} = y'[\vec{m}]^{-1}$ rem m_k. Then

$$\begin{aligned}
\xi_n(\vec{m}, m_k; \vec{x}, y) &= \xi_n\bigl(\vec{m}, m_k; e_n(\vec{m}; \vec{x}; \vec{m}, m_k)\bigr) + \xi_n(\vec{m}, m_k; \vec{0}, y') - c \pm {}^{0}_{2^{-n}(k+1)} \\
&= \frac{1}{m_k} \xi_n(\vec{m}; \vec{x}) + 2^{-n} \left\lceil \frac{2^n \tilde{y}}{m_k} \right\rceil - c \pm 2^{-n}(k+1) \\
&= \frac{1}{m_k} \bigl(\xi_n(\vec{m}; \vec{x}) + \tilde{y}\bigr) - c \pm 2^{-n}(k+2)
\end{aligned}$$

for some $c \in \{-1, 0, 1\}$ using (29) and (22). Since $0 \le \tilde{y} \le m_k - 1$, we have

$$\min\bigl\{\tfrac{1}{m_k}\bigl(\xi_n(\vec{m}; \vec{x}) + \tilde{y}\bigr), 1 - \tfrac{1}{m_k}\bigl(\xi_n(\vec{m}; \vec{x}) + \tilde{y}\bigr)\bigr\} \ge \frac{1}{m_k}\bigl(\xi_n(\vec{m}; \vec{1}) - 2^{-n}(3k)\bigr)$$

by the induction hypothesis, thus

$$\begin{aligned}
\min\bigl\{&\xi_n(\vec{m}, m_k; \vec{x}, y) + c, 1 - \bigl(\xi_n(\vec{m}, m_k; \vec{x}, y) + c\bigr)\bigr\} \\
&\ge \xi_n(\vec{m}, m_k; \vec{1}, 1) - 2^{-n}\bigl(3k m_k^{-1} + (k+1)(1 - m_k^{-1}) + k + 2\bigr) \\
&\ge \xi_n(\vec{m}, m_k; \vec{1}, 1) - 2^{-n}\bigl(k m_k^{-1} + k + 1 + (k+1)(2 - m_k^{-1})\bigr) \\
&\ge \xi_n(\vec{m}, m_k; \vec{1}, 1) - 2^{-n}\bigl(3(k+1)\bigr) > 0
\end{aligned}$$

using (32) and $m_k \ge 2$, which implies $c = 0$ and the result. □

Corollary 5.11 *VTC^0(imul) proves that if $n \ge |k| + 2 + \sum_{i<k} |m_i|$, then Lemma 5.9 holds with $c \in \{0, 1\}$.*

Proof: If, say, $\vec{x} = 0$, then $\vec{z} = \vec{y}$, and the statement holds with $c = 0$. Thus, we may assume $\vec{x} \ne \vec{0} \ne \vec{y}$. If $c = -1$, then

$$1 > \xi_n(\vec{m}; \vec{z}) = \xi_n(\vec{m}; \vec{x}) + \xi_n(\vec{m}; \vec{y}) + 1 \pm {}^{0}_{2^{-n}k}$$

implies

$$2^{-n}k > \xi_n(\vec{m}; \vec{x}) + \xi_n(\vec{m}; \vec{y}) \ge 2\xi_n(\vec{m}; \vec{1}) - 2^{-n}(6k) > 2^{1 - \sum_i |m_i|} - 2^{-n}(6k)$$

using Lemmas 5.10 and 5.8, thus

$$2^{1 - \sum_i |m_i|} < 2^{-n}(7k) < 2^{|k| + 3 - n}.$$

This is a contradiction if $n \ge |k| + 2 + \sum_{i<k} |m_i|$. □

The next crucial lemma states how large n needs to be so that $r_n(\vec{m};\vec{x})$ is the true rank, and $e_n(\vec{m};\vec{x};\vec{a})$ the correct basis extension of $\vec{x}$; it also gives the rate of convergence of $\xi_n(\vec{m};\vec{x})$. This will considerably simplify our subsequent arguments, as we can fix the rank and basis extension functions independently of any extraneous parameters, and it will make calculations with ξ_n self-correcting, preventing accumulation of errors (we may temporarily switch to $\xi_{n'}$ with $n' \ge n$ as large as we want to make any given argument work with sufficient accuracy, and get back to ξ_n using (35)).

Lemma 5.12 *VTC^0(imul) proves: if $n' \ge n \ge |k| + 2 + \sum_{i<k}|m_i|$, then for all $\vec{x} < \vec{m}$ and $\vec{a}$,*

$$r_n(\vec{m};\vec{x}) = r_{n'}(\vec{m};\vec{x}), \tag{33}$$

$$e_n(\vec{m};\vec{x};\vec{a}) = e_{n'}(\vec{m};\vec{x};\vec{a}), \tag{34}$$

$$\xi_n(\vec{m};\vec{x}) = \xi_{n'}(\vec{m};\vec{x}) \pm_0^{2^{-n}k}. \tag{35}$$

Proof: If $\vec{x} = \vec{0}$, all quantities in (33)–(35) are 0, thus we may assume $\vec{x} \ne \vec{0}$ (whence $k \ge 1$). Put $h_i = [\vec{m}]_{\ne i}^{-1} \text{ rem } m_i$. Since

$$2^{n'-n}\left\lfloor \frac{2^n x_i h_i}{m_i} \right\rfloor \le \left\lfloor \frac{2^{n'} x_i h_i}{m_i} \right\rfloor, \qquad 2^{n'-n}\left\lceil \frac{2^n x_i h_i}{m_i} \right\rceil \ge \left\lceil \frac{2^{n'} x_i h_i}{m_i} \right\rceil,$$

we have

$$2^{-n'} S_{n'}(\vec{x}) = 2^{-n'} \sum_{i<k} \left\lceil \frac{2^{n'} x_i h_i}{m_i} \right\rceil \le 2^{-n'} \sum_{i<k} 2^{n'-n} \left\lceil \frac{2^n x_i h_i}{m_i} \right\rceil = 2^{-n} S_n(\vec{x}) \tag{36}$$

and

$$\begin{aligned} 2^{-n} S_n(\vec{x}) &\le 2^{-n} \sum_{i<k} \left\lfloor \frac{2^n x_i h_i}{m_i} \right\rfloor + 2^{-n}k = 2^{-n'} \sum_{i<k} 2^{n'-n} \left\lfloor \frac{2^n x_i h_i}{m_i} \right\rfloor + 2^{-n}k \\ &\le 2^{-n'} \sum_{i<k} \left\lfloor \frac{2^{n'} x_i h_i}{m_i} \right\rfloor + 2^{-n}k \le 2^{-n'} S_{n'}(\vec{x}) + 2^{-n}k. \end{aligned} \tag{37}$$

Thus, using (30) and Lemma 5.8,

$$r_n(\vec{x}) + 1 > 2^{-n'} S_{n'}(\vec{x}) \ge r_n(\vec{x}) + \xi_n(\vec{x}) - 2^{-n}k \ge r_n(\vec{x}) + 2^{-\sum_i |m_i|} - 2^{-n}(4k) \ge r_n(\vec{x})$$

as long as $n \ge \sum_i |m_i| + |k| + 2$. Then $r_{n'}(\vec{x}) = r_n(\vec{x})$; (34) follows as the only dependence of e_n on n is through r_n, and (35) follows from (36) and (37). □

Definition 5.13 For $\vec{x} < \vec{m}$, we define $r(\vec{m};\vec{x}) = r_n(\vec{m};\vec{x})$ and $e(\vec{m};\vec{x};\vec{a}) = e_n(\vec{m};\vec{x};\vec{a})$, where $n = |k| + 2 + \sum_{i<k}|m_i|$.

The meaning of the next lemma is that if $\vec{m}$ is odd, the CRR of $(1 + [\vec{m}])/2$ is $2^{-1} \text{ rem } \vec{m}$ (i.e., the sequence of inverses of 2 modulo each m_i). The CRR reconstruction procedure will involve such factors.

Lemma 5.14 *VTC^0(imul) proves: if $\vec{x} < \vec{m} \perp 2$, $\vec{a} \perp 2$, $k > 0$, and $n \geq |k+1| + 4 + \sum_i |m_i|$, then*

$$e(\vec{m}; 2^{-1} \operatorname{rem} \vec{m}; \vec{a}) \equiv 2^{-1}(1 + [\vec{m}]) \pmod{\vec{a}}, \tag{38}$$

$$\xi_n(\vec{m}; 2^{-1} \operatorname{rem} \vec{m}) = \frac{1}{2} + \xi_n(\vec{m}, 2; \vec{1}, 1). \tag{39}$$

Proof: We may assume $\operatorname{lh}(\vec{a}) = 1$. Working modulo a, we have

$$\begin{aligned} 2e(\vec{m}; 2^{-1} \operatorname{rem} \vec{m}; a) &= e(\vec{m}, 2; \vec{1}, 0; a) \\ &\equiv e(\vec{m}, 2; \vec{1}, 1; a) - [\vec{m}] + \big(r(\vec{m}, 2; \vec{1}, 1) - r(\vec{m}, 2; \vec{1}, 0)\big) 2[\vec{m}] \\ &\equiv 1 - [\vec{m}] + \big(r(\vec{m}, 2; \vec{1}, 1) - r(\vec{m}, 2; \vec{1}, 0)\big) 2[\vec{m}] \end{aligned}$$

by (17), the definition of e_n, and (26). Now, the definition of S_n gives

$$S_n(\vec{m}, 2; \vec{1}, 1) - S_n(\vec{m}, 2; \vec{1}, 0) = \left\lceil \frac{2^n}{2} \right\rceil = 2^{n-1}, \tag{40}$$

thus

$$r(\vec{m}, 2; \vec{1}, 1) - r(\vec{m}, 2; \vec{1}, 0) = \begin{cases} 1, & \text{if } \xi_n(\vec{m}, 2; \vec{1}, 1) < \frac{1}{2}, \\ 0, & \text{otherwise} \end{cases}$$

for any $n \geq |k+1| + 4 \sum_i |m_i|$. However, (25) ensures $\xi_n(\vec{m}, 2; \vec{1}, 1) < \frac{1}{2}$ as long as $k \geq 1$ and $2^n \geq 4(k+2)$, hence

$$2e(\vec{m}; 2^{-1} \operatorname{rem} \vec{m}; a) \equiv 1 + [\vec{m}] \pmod{a}$$

as required. Also, (40) ensures

$$\xi_n(\vec{m}; 2^{-1} \operatorname{rem} \vec{m}) = \xi_n(\vec{m}, 2; \vec{1}, 0) = \frac{1}{2} + \xi_n(\vec{m}, 2; \vec{1}, 1)$$

using Lemma 5.5. □

The following lemma shows that if X (which is not too big w.r.t. $\vec{m}$) has CRR $\vec{x}$, then $e(\vec{x}; \vec{a})$ is $X \operatorname{rem} \vec{a}$ as expected, and $\xi_n(\vec{x}) \approx X/[\vec{m}]$ (formulated with $\xi_n(\vec{1})$).

As a corollary, we obtain that X (which is not too big) is uniquely determined by its CRR.

Lemma 5.15 *VTC^0(imul) proves: if $|X| \leq \sum_{i<k} \big(|m_i| - 1\big)$, $\vec{x} = X \operatorname{rem} \vec{m}$, and $n \geq |k| + 2 + \sum_{i<k} |m_i|$, then*

$$e(\vec{m}; \vec{x}; \vec{a}) = X \operatorname{rem} \vec{a}, \tag{41}$$

$$X\big(\xi_n(\vec{m}; \vec{1}) - 2^{1-n} k\big) \leq \xi_n(\vec{m}; \vec{x}) \leq X \xi_n(\vec{m}; \vec{1}). \tag{42}$$

Proof: We may assume $\operatorname{lh}(\vec{a}) = 1$. If we fix X, we can prove the statement for $\lfloor 2^{-t} X \rfloor$, $t \leq |X|$, by reverse induction on t; that is, it suffices to show that it holds for $X = 0$ (trivial) and $X = 1$ (Lemma 5.8), and that it holds for $X \geq 2$ assuming it holds for $\lfloor X/2 \rfloor$. To facilitate the induction argument, we strengthen the lower bound for $X \geq 1$ to

$$X \xi_n(\vec{1}) - (2X - 1) 2^{-n} k \leq \xi_n(\vec{x}) \leq X \xi_n(\vec{1}). \tag{43}$$

Assume that (41) and (43) hold for $Y = \lfloor X/2 \rfloor$, and put $\vec{y} = \lfloor X/2 \rfloor \operatorname{rem} \vec{m}$. Using Corollary 5.11, there is a constant $c \in \{0,1\}$ such that

$$\begin{aligned} e(2\vec{y};a) &\equiv 2e(\vec{y};a) - c[\vec{m}] \pmod{a}, \\ \xi_n(2\vec{y}) &= 2\xi_n(\vec{y}) - c \pm^{0}_{2^{-n}k}. \end{aligned}$$

However, since

$$2\xi_n(\vec{y}) \le 2Y\xi_n(\vec{1}) \le X2^{-\sum_i(|m_i|-1)} \le X2^{-|X|} < 1$$

by the induction hypothesis and Lemma 5.8, we must have $c = 0$, thus

$$e(2\vec{y};a) \equiv 2e(\vec{y};a) \equiv 2Y \pmod{a},$$

and

$$2Y\xi_n(\vec{1}) - \big(4Y - 2 + 1\big)2^{-n}k \le \xi_n(2\vec{y}) \le 2Y\xi_n(\vec{1})$$

using the induction hypothesis. If $X = 2Y$, then $\vec{x} = 2\vec{y}$ and we are done. If $X = 2Y + 1$ and $\vec{x} = 2\vec{y} + \vec{1}$, we apply Corollary 5.11 once again: there is $c' \in \{0,1\}$ such that

$$\begin{aligned} e(\vec{x};a) &\equiv e(2\vec{y};a) + 1 - c'[\vec{m}] \pmod{a}, \\ \xi_n(\vec{x}) &= \xi_n(2\vec{y}) + \xi_n(\vec{1}) - c' \pm^{0}_{2^{-n}k} \end{aligned}$$

using (26). As above,

$$\xi_n(2\vec{y}) + \xi_n(\vec{1}) \le (2Y+1)\xi_n(\vec{1}) \le X2^{-\sum_i(|m_i|-1)} \le X2^{-|X|} < 1,$$

thus $c' = 0$, and

$$\begin{aligned} e(\vec{x};a) \equiv e(2\vec{y};a) + 1 \equiv 2Y + 1 \equiv X \pmod{a}, \\ X\xi_n(\vec{1}) - (2X-1)2^{-n}k \le X\xi_n(\vec{1}) - (4Y)2^{-n}k \le \xi_n(\vec{x}) \le X\xi_n(\vec{1}) \end{aligned}$$

as required. $\square$

Corollary 5.16 *VTC^0(imul) proves: if $|X|, |Y| \le \sum_{i<k}\big(|m_i| - 1\big)$ and $X \equiv Y \pmod{\vec{m}}$, then $X = Y$.*

Proof: Put $\vec{x} = X \operatorname{rem} \vec{m}$ and $\vec{y} = Y \operatorname{rem} \vec{m}$. If, say $X < Y$, then

$$\xi_n(\vec{x}) \le (Y-1)\xi_n(\vec{1}) < Y\big(\xi_n(\vec{1}) - 2^{1-n}k\big) \le \xi_n(\vec{y})$$

by Lemma 5.15 as long as $n \ge |k| + 2 + \sum_{i<k}|m_i|$ and $Y2^{1-n}k < \xi_n(\vec{1})$. (Since $Y < 2^{\sum_i(|m_i|-1)}$ and $\xi_n(\vec{1}) > 2^{-\sum_i|m_i|}$ by (25), this holds if we take $n \ge |k| + 2 + 2\sum_i|m_i|$.) Then it follows that $\vec{x} \ne \vec{y}$. $\square$

The final, and most complicated, technical result in this subsection expresses that given the CRR of $X < [\vec{m}]$ in basis $\vec{m}$, and the CRR of $Y < [\vec{a}]$ in basis $\vec{a}$ (where $\vec{m} \perp \vec{a}$), we obtain the CRR of $XY < [\vec{m}][\vec{a}]$ in the basis $\langle \vec{m}, \vec{a} \rangle$ by extending both original CRRs to the combined basis, and multiplying them elementwise (modulo each prime).

We first need a simple "reciprocity lemma" relating inverses of two primes modulo each other.

Lemma 5.17 *$I\Delta_0$ proves that if m and a are distinct primes, then*

$$m\bigl(m^{-1} \text{ rem } a\bigr) - a\bigl((-a^{-1}) \text{ rem } m\bigr) = 1. \tag{44}$$

Proof: We have $m(m^{-1} \text{ rem } a) \equiv 1 \pmod{a}$, i.e., $m(m^{-1} \text{ rem } a) = 1 + au$ for some u. Since $0 < m(m^{-1} \text{ rem } a) < am$, we have $0 \leq u < m$, and $-au \equiv 1 \pmod{m}$, thus $u = (-a^{-1}) \text{ rem } m$. $\square$

Definition 5.18 If $\vec{x}, \vec{y} < \vec{m}$, then $\vec{x} \times \vec{y}$ denotes the elementwise product $\langle x_i y_i \text{ rem } m_i : i < k \rangle$. More generally, we will write $\prod_{u<t} \vec{x}_u$ for the elementwise product of terms $\langle x_{u,i} : i < k \rangle = \vec{x}_u < \vec{m}$, $u < t$.

Lemma 5.19 *VTC^0(imul) proves: let $\vec{m} \perp \vec{a}$, $\vec{x} < \vec{m}$, $\vec{y} < \vec{a}$, and $n \geq |k+l| + 2 + \sum_{i<k} |m_i| + \sum_{j<l} |a_j|$. Then*

$$e\bigl(\vec{m}, \vec{a}; e(\vec{m}; \vec{x}; \vec{m}, \vec{a}) \times e(\vec{a}; \vec{y}; \vec{m}, \vec{a}); \vec{b}\bigr) = e(\vec{m}; \vec{x}; \vec{b}) \times e(\vec{a}; \vec{y}; \vec{b}), \tag{45}$$

$$\xi_n\bigl(\vec{m}, \vec{a}; e(\vec{m}; \vec{x}; \vec{m}, \vec{a}) \times e(\vec{a}; \vec{y}; \vec{m}, \vec{a})\bigr) = \xi_n(\vec{m}; \vec{x})\, \xi_n(\vec{a}; \vec{y}) \pm 2^{-n}(k+l). \tag{46}$$

Proof: If, say, $\vec{x} = \vec{0}$, then both sides of (45) and (46) are 0, thus we may assume $\vec{x} \neq \vec{0} \neq \vec{y}$. Put $\vec{u} = e(\vec{a}; \vec{y}; \vec{m})$ and $\vec{v} = e(\vec{m}; \vec{x}; \vec{a})$, so that

$$e(\vec{m}; \vec{x}; \vec{m}, \vec{a}) \times e(\vec{a}; \vec{y}; \vec{m}, \vec{a}) = \langle \vec{x} \times \vec{u}, \vec{y} \times \vec{v} \rangle.$$

Let

$$h_i = [\vec{m}]_{\neq i}^{-1} \text{ rem } m_i, \qquad \tilde{h}_i = [\vec{a}]^{-1} h_i \text{ rem } m_i,$$
$$h'_j = [\vec{a}]_{\neq j}^{-1} \text{ rem } a_j, \qquad \tilde{h}'_j = [\vec{m}]^{-1} h'_j \text{ rem } a_j.$$

For any $i < k$ and $j < l$, Lemma 5.17 gives

$$\begin{aligned}
\left\lceil \frac{2^n x_i h_i}{m_i} \right\rceil \left\lceil \frac{2^n y_j h'_j}{a_j} \right\rceil &= 2^{2n} \frac{x_i h_i y_j h'_j}{m_i a_j} \pm_0^{2^n(m_i + a_j)} \\
&= 2^n x_i h_i \bigl(m_i^{-1} \text{ rem } a_j\bigr) \frac{2^n y_j h'_j}{a_j} \\
&\qquad - 2^n y_j h'_j \bigl((-a_j^{-1}) \text{ rem } m_i\bigr) \frac{2^n x_i h_i}{m_i} \pm_0^{2^n(m_i + a_j)} \\
&= 2^n x_i h_i \bigl(m_i^{-1} \text{ rem } a_j\bigr) \left\lceil \frac{2^n y_j h'_j}{a_j} \right\rceil \\
&\qquad - 2^n y_j h'_j \bigl((-a_j^{-1}) \text{ rem } m_i\bigr) \left\lceil \frac{2^n x_i h_i}{m_i} \right\rceil \pm_{2^n m_i^2 a_j}^{2^n(m_i + a_j + m_i a_j^2)}
\end{aligned}$$

Then, expanding the definition,

$$\begin{aligned}
\xi_n(\vec{x})\,\xi_n(\vec{y}) &= \bigl(2^{-n}S_n(\vec{x})-r(\vec{x})\bigr)\bigl(2^{-n}S_n(\vec{y})-r(\vec{y})\bigr)\\
&= 2^{-2n}\sum_{\substack{i<k\\ j<l}}\left\lceil\frac{2^n x_i h_i}{m_i}\right\rceil\left\lceil\frac{2^n y_j h'_j}{a_j}\right\rceil\\
&\qquad -2^{-n}r(\vec{y})\sum_{i<k}\left\lceil\frac{2^n x_i h_i}{m_i}\right\rceil-2^{-n}r(\vec{x})\sum_{j<l}\left\lceil\frac{2^n y_j h'_j}{a_j}\right\rceil+r(\vec{x})\,r(\vec{y})\\
&= 2^{-n}\sum_{i<k}\left\lceil\frac{2^n x_i h_i}{m_i}\right\rceil\Bigl(-\sum_{j<l}y_j h'_j\bigl((-a_j^{-1})\ \mathrm{rem}\ m_i\bigr)-r(\vec{y})\Bigr)\\
&\qquad +2^{-n}\sum_{j<l}\left\lceil\frac{2^n y_j h'_j}{a_j}\right\rceil\Bigl(\sum_{i<k}x_i h_i\bigl(m_i^{-1}\ \mathrm{rem}\ a_j\bigr)-r(\vec{x})\Bigr)\\
&\qquad +r(\vec{x})\,r(\vec{y})\pm^{2^{-n}\left(\sum_i m_i+\sum_j a_j+\sum_i m_i\sum_j a_j^2\right)}_{2^{-n}\sum_i m_i^2\sum_j a_j}.
\end{aligned}$$

For any $i<k$,

$$h_i\Bigl(-\sum_{j<l}y_j h'_j\bigl((-a_j^{-1})\ \mathrm{rem}\ m_i\bigr)-r(\vec{y})\Bigr)\equiv h_i[\vec{a}]^{-1}e(\vec{a};\vec{y};m_i)\equiv\tilde{h}_i u_i\pmod{m_i},$$

thus

$$s_i=\frac{\tilde{h}_i u_i+h_i\Bigl(\sum_{j<l}y_j h'_j\bigl((-a_j^{-1})\ \mathrm{rem}\ m_i\bigr)+r(\vec{y})\Bigr)}{m_i}$$

is a (small) integer, and we have

$$\begin{aligned}
&\left\lceil\frac{2^n x_i h_i}{m_i}\right\rceil\Bigl(-\sum_{j<l}y_j h'_j\bigl((-a_j^{-1})\ \mathrm{rem}\ m_i\bigr)-r(\vec{y})\Bigr)\\
&\qquad=\frac{2^n x_i h_i}{m_i}\Bigl(-\sum_{j<l}y_j h'_j\bigl((-a_j^{-1})\ \mathrm{rem}\ m_i\bigr)-r(\vec{y})\Bigr)\pm^{0}_{m_i\sum_j a_j^2}\\
&\qquad=\frac{2^n x_i\tilde{h}_i u_i}{m_i}-2^n x_i s_i\pm^{0}_{m_i\sum_j a_j^2}\\
&\qquad=\left\lceil\frac{2^n x_i u_i\tilde{h}_i}{m_i}\right\rceil-2^n x_i s_i\pm^{0}_{m_i\sum_j a_j^2+1}.
\end{aligned}$$

Likewise,

$$\left\lceil\frac{2^n y_j h'_j}{a_j}\right\rceil\Bigl(\sum_{i<k}x_i h_i\bigl(m_i^{-1}\ \mathrm{rem}\ a_j\bigr)-r(\vec{x})\Bigr)=\left\lceil\frac{2^n y_j v_j\tilde{h}'_j}{a_j}\right\rceil-2^n y_j t_j\pm^{a_j\sum_i m_i^2}_{\sum_i m_i},$$

where

$$t_j=\frac{\tilde{h}'_j v_j-h'_j\Bigl(\sum_{i<k}x_i h_i\bigl(m_i^{-1}\ \mathrm{rem}\ a_j\bigr)-r(\vec{x})\Bigr)}{a_j}$$

is an integer. Thus, continuing the computation above,

$$\begin{aligned}
\xi_n(\vec{x})\,\xi_n(\vec{y}) &= 2^{-n}\left\lceil \frac{2^n x_i u_i \tilde{h}_i}{m_i} \right\rceil + 2^{-n}\left\lceil \frac{2^n y_j v_j \tilde{h}'_j}{a_j} \right\rceil \\
&\qquad - \sum_{i<k} x_i s_i - \sum_{j<l} y_j t_j + r(\vec{x})\,r(\vec{y}) \pm^{2^{-n}\left(\sum_i m_i + \sum_j a_j + \sum_i m_i \sum_j a_j^2 + \sum_i m_i^2 \sum_j a_j\right)}_{2^{-n}\left(\sum_i m_i^2 \sum_j a_j + \sum_i m_i \sum_j a_j^2 + k + l \sum_i m_i\right)} \\
&= S_n(\vec{x}\times\vec{u}, \vec{y}\times\vec{v}) - \sum_{i<k} x_i s_i - \sum_{j<l} y_j t_j + r(\vec{x})\,r(\vec{y}) \\
&\qquad \pm 2^{-n}\Bigl(\sum_i m_i \sum_j a_j^2 + \sum_i m_i^2 \sum_j a_j + \sum_i m_i \sum_j a_j\Bigr) \\
&= S_n(\vec{x}\times\vec{u}, \vec{y}\times\vec{v}) - \sum_{i<k} x_i s_i - \sum_{j<l} y_j t_j + r(\vec{x})\,r(\vec{y}) \pm 2^{-n} \sum_i m_i^2 \sum_j a_j^2
\end{aligned}$$

(using $(m_i - 1)(a_j - 1) \geq 2$, which implies $m_i a_j^2 + m_i^2 a_j + m_i a_j \leq m_i^2 a_j^2$). By Lemmas 5.8 and 5.10, there is n_0 such that

$$\min\bigl\{\xi_n(\vec{x})\,\xi_n(\vec{y}), 1 - \xi_n(\vec{x})\,\xi_n(\vec{y})\bigr\} > 2^{-n} \sum_i m_i^2 \sum_j a_j^2$$

for all $n \geq n_0$. It follows that

$$r(\vec{x}\times\vec{u}, \vec{y}\times\vec{v}) = \sum_{i<k} x_i s_i + \sum_{j<l} y_j t_j - r(\vec{x})\,r(\vec{y}), \tag{47}$$

and

$$n \geq n_0 \implies \xi_n(\vec{x}\times\vec{u}, \vec{y}\times\vec{v}) = \xi_n(\vec{x})\,\xi_n(\vec{y}) \pm 2^{-n} \sum_i m_i^2 \sum_j a_j^2.$$

In order to prove (46) for all $n \geq |k+l| + 2 + \sum_i |m_i| + \sum_j |a_j|$, we pick $n' \geq \max\{n, n_0\}$ such that $2^{n'} > 2^{2n+1} \sum_i m_i^2 \sum_j a_j^2$, and we apply Lemma 5.12:

$$\begin{aligned}
\xi_n(\vec{x}\times\vec{u}, \vec{y}\times\vec{v}) &= \xi_{n'}(\vec{x}\times\vec{u}, \vec{y}\times\vec{v}) \pm^{2^{-n}(k+l)}_{0} \\
&= \xi_{n'}(\vec{x})\,\xi_{n'}(\vec{y}) \pm^{2^{-n}(k+l)}_{0} \pm 2^{-n'} \sum_i m_i^2 \sum_j a_j^2 \\
&= \bigl(\xi_n(\vec{x}) \pm^{0}_{2^{-n}k}\bigr)\bigl(\xi_n(\vec{y}) \pm^{0}_{2^{-n}l}\bigr) \pm^{2^{-n}(k+l)}_{0} \pm 2^{-n'} \sum_i m_i^2 \sum_j a_j^2 \\
&= \xi_n(\vec{x})\,\xi_n(\vec{y}) \pm \bigl(2^{-n}(k+l) + 2^{-n'} \sum_i m_i^2 \sum_j a_j^2\bigr) \\
&= \xi_n(\vec{x})\,\xi_n(\vec{y}) \pm \bigl(2^{-n}(k+l) + 2^{-2n-1}\bigr).
\end{aligned}$$

Since the terms on both sides are integer multiples of 2^{-2n}, this implies

$$\xi_n(\vec{x}\times\vec{u}, \vec{y}\times\vec{v}) = \xi_n(\vec{x})\,\xi_n(\vec{y}) \pm 2^{-n}(k+l).$$

It remains to prove (45). We may assume $\operatorname{lh}(\vec{b}) = 1$, i.e., $\vec{b} = \langle b \rangle$. The result is easy to check if $b = m_i$ or $b = a_j$, hence we may assume $b \perp \vec{m}, \vec{a}$. Using Lemma 5.17 again, we compute modulo b:

$$
\begin{aligned}
[\vec m]^{-1}[\vec a]^{-1}e(\vec x;b)\,e(\vec y;b) &\equiv \Bigl(\sum_{i<k} x_i h_i m_i^{-1} - r(\vec x)\Bigr)\Bigl(\sum_{j<l} y_j h'_j a_j^{-1} - r(\vec y)\Bigr)\\
&\equiv \sum_{\substack{i<k\\ j<l}} x_i h_i y_j h'_j m_i^{-1} a_j^{-1}\\
&\qquad - r(\vec y)\sum_{i<k} x_i h_i m_i^{-1} - r(\vec x)\sum_{j<l} y_j h'_j a_j^{-1} + r(\vec x)\,r(\vec y)\\
&\equiv \sum_{\substack{i<k\\ j<l}} x_i h_i y_j h'_j \bigl(a_j^{-1}(m_i^{-1} \text{ rem } a_j) - m_i^{-1}((-a_j^{-1}) \text{ rem } m_i)\bigr)\\
&\qquad - r(\vec y)\sum_{i<k} x_i h_i m_i^{-1} - r(\vec x)\sum_{j<l} y_j h'_j a_j^{-1} + r(\vec x)\,r(\vec y)\\
&\equiv \sum_{i<k} x_i h_i m_i^{-1}\Bigl(-\sum_{j<l} y_j h'_j\bigl((-a_j^{-1}) \text{ rem } m_i\bigr) - r(\vec y)\Bigr)\\
&\qquad + \sum_{j<l} y_j h'_j a_j^{-1}\Bigl(\sum_{i<k} x_i h_i\bigl(m_i^{-1} \text{ rem } a_j\bigr) - r(\vec x)\Bigr) + r(\vec x)\,r(\vec y)\\
&\equiv \sum_{i<k} x_i m_i^{-1}(\tilde h_i u_i - m_i s_i) + \sum_{j<l} y_j a_j^{-1}(\tilde h'_j v_j - a_j t_j) + r(\vec x)\,r(\vec y)\\
&\equiv \sum_{i<k} x_i u_i \tilde h_i m_i^{-1} + \sum_{j<l} y_j v_j \tilde h'_j a_j^{-1}\\
&\qquad - \Bigl(\sum_{i<k} x_i s_i + \sum_{j<l} y_j t_j - r(\vec x)\,r(\vec y)\Bigr)\\
&\equiv \sum_{i<k} x_i u_i \tilde h_i m_i^{-1} + \sum_{j<l} y_j v_j \tilde h'_j a_j^{-1} - r(\vec x\times\vec u, \vec y\times\vec v)\\
&\equiv [\vec m]^{-1}[\vec a]^{-1}e(\vec x\times\vec u, \vec y\times\vec v; b)
\end{aligned}
$$

by (47). □

5.2 Chinese remainder reconstruction and iterated products

We now introduce the CRR reconstruction procedure. The definition mostly follows the proof of [13, Thm. 4.1], inlining the construction from [13, L. 4.5]. (The latter lemma shows how to compute the CRR of $\lfloor X/[\vec a]\rfloor$ from the CRR of X; since we cannot yet define what $[\vec a]$ is in the first place, we do not know how to formulate the lemma in a stand-alone way.)

Definition 5.20 (In VTC^0(imul).) If $\vec x < \vec m$ and $\vec a$ is a subsequence of $\vec m$, let $\vec x \restriction \vec a$ denote the corresponding subsequence of $\vec x$. (Thus, in fact, $\vec x \restriction \vec a = e(\vec m; \vec x; \vec a)$.)

Let $\mathrm{Rec}(\vec m; \vec x)$ denote the $\Sigma^B_0(\text{card}, \text{imul})$-definable function formalizing the following algorithm. Given a nonempty $\vec m \perp 2$ and $\vec x < \vec m$, let $s = 2 + \sum_{i<k}|m_i|$, and using Theorem 3.2, let $\vec a = \langle a_{u,j} : u < s, j < l\rangle$ be a sequence of distinct odd primes such that $\vec a \perp \vec m$ and

$$\sum_{j<l}\bigl(|a_{u,j}| - 1\bigr) > 2s \tag{48}$$

for all $u < s$. We write $\vec{a}_u = \langle a_{u,j} : j < l \rangle$ and $\vec{a}_{<t} = \langle a_{u,j} : u < t, j < l \rangle$. For each $t \le s$, we define residue sequences $\vec{w}_t < \langle \vec{m}, \vec{a}_{<t} \rangle$ and $\vec{y}_t < \vec{m}$ by

$$\vec{w}_t = \Bigl(2^{-t} \prod_{u<t} \bigl(1 + [\vec{a}_u]\bigr)\Bigr) e(\vec{m}; \vec{x}; \vec{m}, \vec{a}_{<t}) \text{ rem } \langle \vec{m}, \vec{a}_{<t} \rangle,$$
$$\vec{y}_t = [\vec{a}_{<t}]^{-1} \bigl(\vec{w}_t \restriction \vec{m} - e(\vec{a}_{<t}; \vec{w}_t \restriction \vec{a}_{<t}; \vec{m})\bigr) \text{ rem } \vec{m},$$

and for $t < s$, we define a residue sequence $\vec{z}_t < \vec{m}$ and a (possibly negative) number b_t by

$$\vec{z}_t = (\vec{y}_t - 2\vec{y}_{t+1}) \text{ rem } \vec{m},$$
$$b_t = \begin{cases} -1, & \text{if } \vec{z}_t \equiv -\vec{1} \pmod{\vec{m}}, \\ z_{t,0} & \text{otherwise.} \end{cases}$$

(Here, $z_{t,0} < m_0$ is the 0th component of $\vec{z}_t = \langle z_{t,i} : i < k \rangle$.) Finally, we define

$$\mathrm{Rec}(\vec{m}; \vec{x}) = \sum_{t<s} 2^t b_t.$$

To get the basic intuition: in the real world, if $\vec{x}$ is the CRR of X in basis $\vec{m}$, then $\vec{w}_t$ is the CRR of $X \prod_{u<t} \bigl(1+[\vec{a}_u]\bigr)/2$ in basis $\langle \vec{m}, \vec{a}_{<t} \rangle$, and $\vec{y}_t$ is the CRR of $\bigl\lfloor X \prod_{u<t} \bigl(1 + [\vec{a}_u]\bigr) / \bigl(2[\vec{a}_u]\bigr) \bigr\rfloor = \lfloor X 2^{-t} \rfloor$ in basis $\vec{m}$ (using the fact that $[\vec{a}_u]$ is large enough so that $\bigl(1 + [\vec{a}_u]\bigr)/\bigl(2[\vec{a}_u]\bigr)$ exceeds $1/2$ only by a negligible amount). Thus, $\vec{z}_t$ is the CRR of $\mathrm{bit}(X, t) = b_t$, and $\mathrm{Rec}(\vec{m}; \vec{x}) = X$.

In particular, in reality $b_t \in \{0, 1\}$, whereas our argument in $VTC^0(\mathrm{imul})$ will only establish that $\vec{z}_t$ is the CRR of one of -1, 0, 1, 2, which is extracted as b_t (see Lemma 5.23); a priori, $\mathrm{Rec}(\vec{m}; \vec{x})$ may be negative.

Since we cannot refer in $VTC^0(\mathrm{imul})$ to the product $X \prod_{u<t} \bigl(1 + [\vec{a}_u]\bigr)/2$ that we do not know to exist, we base our analysis instead on ξ_n estimation: in particular, we aim to show $\xi_n(\vec{y}_t) \approx \xi_n(\vec{w}_t) \approx 2^{-t} \xi_n(\vec{x})$. To this end, we first need to rewrite the definition of $\vec{w}_t$ as a recurrence:

Lemma 5.21 $VTC^0(\mathrm{imul})$ *proves: using the notation from Definition 5.20,*

$$e(\vec{m}, \vec{a}_{<t}; \vec{w}_t; \vec{m}, \vec{a}) = e(\vec{m}; \vec{x}; \vec{m}, \vec{a}) \times \prod_{u<t} e(\vec{a}_u; 2^{-1} \text{ rem } \vec{a}_u; \vec{m}, \vec{a}), \tag{49}$$

$$\vec{w}_{t+1} = e(\vec{m}, \vec{a}_{<t}; \vec{w}_t; \vec{m}, \vec{a}_{\le t}) \times e(\vec{a}_t; 2^{-1} \text{ rem } \vec{a}_t; \vec{m}, \vec{a}_{\le t}), \tag{50}$$

for all $t < s$.

Proof: By Lemma 5.14, the definition of $\vec{w}_t$ amounts to

$$\vec{w}_t = e(\vec{m}; \vec{x}; \vec{m}, \vec{a}_{<t}) \times \prod_{u<t} e(\vec{a}_u; 2^{-1} \text{ rem } \vec{a}_u; \vec{m}, \vec{a}_{<t}). \tag{51}$$

In light of this, for any given t, (49) implies (50): we have

$$\begin{aligned}
&e(\vec{m}, \vec{a}_{<t}; \vec{w}_t; \vec{m}, \vec{a}_{\le t}) \times e(\vec{a}_t; 2^{-1} \text{ rem } \vec{a}_t; \vec{m}, \vec{a}_{\le t}) \\
&\qquad = e(\vec{m}; \vec{x}; \vec{m}, \vec{a}_{\le t}) \times \prod_{u<t} e(\vec{a}_u; 2^{-1} \text{ rem } \vec{a}_u; \vec{m}, \vec{a}_{\le t}) \times e(\vec{a}_t; 2^{-1} \text{ rem } \vec{a}_t; \vec{m}, \vec{a}_{\le t}) \\
&\qquad = e(\vec{m}; \vec{x}; \vec{m}, \vec{a}_{\le t}) \times \prod_{u\le t} e(\vec{a}_u; 2^{-1} \text{ rem } \vec{a}_u; \vec{m}, \vec{a}_{\le t}) \\
&\qquad = \vec{w}_{t+1}.
\end{aligned}$$

Thus, it suffices to prove (49) by induction on t. For $t = 0$, the statement follows from $\vec{w}_0 = \vec{x}$. Assuming (49) holds for t, we also have (50), therefore

$$\begin{aligned}
e(\vec{m}, \vec{a}_{\le t}; \vec{w}_{t+1}; \vec{m}, \vec{a}) &= e\big(\vec{m}, \vec{a}_{\le t}; e(\vec{m}, \vec{a}_{<t}; \vec{w}_t; \vec{m}, \vec{a}_{\le t}) \times e(\vec{a}_t; 2^{-1} \text{ rem } \vec{a}_t; \vec{m}, \vec{a}_{\le t}); \vec{m}, \vec{a}\big) \\
&= e(\vec{m}, \vec{a}_{<t}; \vec{w}_t; \vec{m}, \vec{a}) \times e(\vec{a}_t; 2^{-1} \text{ rem } \vec{a}_t; \vec{m}, \vec{a}) \\
&= e(\vec{m}; \vec{x}; \vec{m}, \vec{a}) \times \prod_{u<t} e(\vec{a}_u; 2^{-1} \text{ rem } \vec{a}_u; \vec{m}, \vec{a}) \times e(\vec{a}_t; 2^{-1} \text{ rem } \vec{a}_t; \vec{m}, \vec{a}) \\
&= e(\vec{m}; \vec{x}; \vec{m}, \vec{a}) \times \prod_{u\le t} e(\vec{a}_u; 2^{-1} \text{ rem } \vec{a}_u; \vec{m}, \vec{a})
\end{aligned}$$

by Lemma 5.19. □

Now we can estimate $\xi_n(\vec{w}_t)$ and $\xi_n(\vec{y}_t)$ using the properties developed in Section 5.1.

Lemma 5.22 *VTC^0(imul) proves: using the notation from Definition 5.20, let $n \ge |k| + 2 + \sum_i |m_i|$. Then for all $t \le s$,*

$$\xi_n(\vec{m}; \vec{y}_t) = 2^{-t}\xi_n(\vec{m}; \vec{x}) \pm^{2^{-n}k+2^{-2s}}_{2^{-n}k+\xi_n(\vec{m};\vec{1})}. \tag{52}$$

Proof: Let us first assume that n is sufficiently large. We start with a bound on $\xi_n(\vec{w}_t)$. We have

$$\xi_n(\vec{m}; \vec{w}_0) = \xi_n(\vec{m}; \vec{x}).$$

By Lemmas 5.21, 5.19, 5.14, and 5.8, we have

$$\begin{aligned}
\xi_n(\vec{m}, \vec{a}_{\le t}; \vec{w}_{t+1}) &= \xi_n(\vec{m}, \vec{a}_{<t}; \vec{w}_t) \left(\tfrac{1}{2} + \xi_n(\vec{a}_t, 2; \vec{1})\right) \pm 2^{-n}\big(k + s(t+1)\big) \\
&= \xi_n(\vec{m}, \vec{a}_{<t}; \vec{w}_t) \left(\tfrac{1}{2} \pm^{2^{-\sum_j (|a_{t,j}|-1)}}_{0}\right) \pm 2^{-n}\big(k + s(t+1)\big) \\
&= \xi_n(\vec{m}, \vec{a}_{<t}; \vec{w}_t) \left(\tfrac{1}{2} \pm^{2^{-2s-1}}_{0}\right) \pm 2^{-n}\big(k + s(t+1)\big),
\end{aligned}$$

thus by induction on $t \le s$, we obtain

$$\xi_n(\vec{m}, \vec{a}_{<t}; \vec{w}_t) = 2^{-t}\xi_n(\vec{m}; \vec{x}) \pm^{2^{1-n}(k+ts)+2^{-2s}}_{2^{1-n}(k+ts)}.$$

Notice that

$$\vec{w}_t - e(\vec{a}_{<t}; \vec{w}_t \restriction \vec{a}_{<t}; \vec{m}, \vec{a}_{<t}) = \langle [\vec{a}_{<t}]\vec{y}_t, \vec{0}\rangle,$$

thus by Lemma 5.5 and Corollary 5.11, there is $c_t \in \{0,1\}$ such that

$$\begin{aligned}\xi_n(\vec{m};\vec{y}_t) &= \xi_n(\vec{m},\vec{a}_{<t};[\vec{a}_{<t}],\vec{0})\\ &= \xi_n(\vec{m},\vec{a}_{<t};\vec{w}_t) - \xi_n\big(\vec{m},\vec{a}_{<t};e(\vec{a}_{<t};\vec{w}_t\restriction\vec{a}_{<t};\vec{m},\vec{a}_{<t})\big) + c_t \pm_0^{2^{-n}(k+ts)}\end{aligned}$$

(for n large enough, c_t is independent of n due to Lemma 5.12). Now, since

$$e(\vec{a}_{<t};\vec{w}_t\restriction\vec{a}_{<t};\vec{m},\vec{a}_{<t}) = e(\vec{m};\vec{1};\vec{m},\vec{a}_{<t}) \times e(\vec{a}_{<t};\vec{w}_t\restriction\vec{a}_{<t};\vec{m},\vec{a}_{<t}),$$

we have

$$\begin{aligned}e(\vec{a}_{<t};\vec{w}_t\restriction\vec{a}_{<t};\vec{m},\vec{a}_{<t}) &\le \xi_n(\vec{m};\vec{1})\,\xi_n(\vec{a}_{<t};\vec{w}_t\restriction a_{<t}) + 2^{-n}(k+ts)\\ &\le \big(1-2^{-\sum_{u,j}|a_{u,j}|}+2^{-n}(3ts)\big)\xi_n(\vec{m};\vec{1}) + 2^{-n}(k+ts)\\ &\le \xi_n(\vec{m};\vec{1}) - 2^{-\tilde{s}} + 2^{-n}(k+4ts)\end{aligned}$$

by Lemmas 5.19, 5.10, and 5.8, where $\tilde{s} = s + \sum_{u,j}|a_{u,j}|$. It follows that

$$1-\xi_n(\vec{m};\vec{1}) + 2^{-n}(3k) \ge \xi_n(\vec{m};\vec{y}_t) \ge c_t - \xi_n(\vec{m};\vec{1}) + 2^{-\tilde{s}} - 2^{-n}(k+4ts),$$

which implies $c_t = 0$ by considering n large enough so that $2^{-\tilde{s}} > 2^{-n}(4k+4ts)$. Thus,

$$\begin{aligned}\xi_n(\vec{m};\vec{y}_t) &= \xi_n(\vec{m},\vec{a}_{<t};\vec{w}_t) \pm_{\xi_n(\vec{m};\vec{1})+2^{-n}(k+4ts)}^{2^{-n}(k+ts)}\\ &= 2^{-t}\xi_n(\vec{m};\vec{x}) \pm_{\xi_n(\vec{m};\vec{1})+2^{-n}(3k+6ts)}^{2^{-2s}+2^{-n}(3k+3ts)}.\end{aligned}$$

In order to obtain the bound as stated in the lemma, we use Lemma 5.12 as in the proof of Lemma 5.19: for sufficiently sufficiently large n',

$$\begin{aligned}\xi_n(\vec{m};\vec{y}_t) &= \xi_{n'}(\vec{m};\vec{y}_t) \pm_0^{2^{-n}k}\\ &= 2^{-t}\xi_{n'}(\vec{m};\vec{x}) \pm_{\xi_{n'}(\vec{m};\vec{1})+2^{-n'}(3k+6ts)}^{2^{-2s}+2^{-n}k+2^{-n'}(3k+3ts)}\\ &= 2^{-t}\xi_n(\vec{m};\vec{x}) \pm_{\xi_n(\vec{m};\vec{1})+2^{-n}k+2^{-n'}(3k+6ts)}^{2^{-2s}+2^{-n}k+2^{-n'}(3k+3ts)}.\end{aligned}$$

For large enough n', we may drop the $2^{-n'}(3k+6ts)$ terms, as all the remaining terms are integer multiples of 2^{-z} for $z = \max\{n+t, 2s\}$. □

The next task is to make sense of $\vec{z}_t$ and b_t: the basic idea is to derive $\xi_n(\vec{z}_t) = O\big(\xi_n(\vec{1})\big)$ from the bounds on $\xi_n(\vec{y}_t)$, and then use discreteness of the ξ_n values (Lemma 5.10) to infer that $\vec{z}_t$ is the CRR of an $O(1)$ integer, which is b_t.

Lemma 5.23 *VTC^0(imul) proves: using the notation from Definition 5.20, $\vec{y}_0 = \vec{x}$, $\vec{y}_s = \vec{0}$, and for each $t < s$, we have $b_t \in \{-1,0,1,2\}$ and $\vec{z}_t = b_t \operatorname{rem} \vec{m}$. Moreover,*

$$\xi_n(\vec{m};\vec{y}_t) = 2\xi_n(\vec{m};\vec{y}_{t+1}) + b_t\xi_n(\vec{m};\vec{1}) \pm_{2^{-n}(3k)}^{2^{-n}k} \tag{53}$$

for $n \ge |k| + 2 + \sum_i |m_i|$.

Proof: The first identity follows immediately from the definition. By Lemmas 5.22 and 5.8,

$$\xi_n(\vec{y}_s) \le 2^{-s} + 2^{-2s} + 2^{-n}k < 2^{2-s} - 2^{-n}(3k) < \xi_n(\vec{1}) - 2^{-n}(3k)$$

for large enough n, which implies $\vec{y}_s = \vec{0}$ by Lemma 5.10.

Let $t < s$. By Corollary 5.11 and Lemma 5.22, we have

$$\xi_n(2\vec{y}_{t+1}) = 2\xi_n(\vec{y}_{t+1}) \pm^{0}_{2^{-n}k} = 2^{-t}\xi_n(\vec{x}) \pm^{2^{1-2s}+2^{1-n}k}_{2\xi_n(\vec{1})+2^{-n}(3k)}$$

(the right-hand side is < 1 for n large enough, hence the constant c from Lemma 5.9 cannot be 1). Using Corollary 5.11 again, there is $c_t \in \{0,1\}$ (independent of n if n is large enough) such that

$$\xi_n(\vec{z}_t) = \xi_n(\vec{y}_t) - \xi_n(2\vec{y}_{t+1}) + c_t \pm^{2^{-n}k}_{0} = c_t \pm^{2\xi_n(\vec{1})+2^{-2s}+2^{-n}(5k)}_{\xi_n(\vec{1})+2^{1-2s}+2^{-n}(3k)},$$

thus for large enough n, we have

$$\Big(c_t = 0 \quad \text{and} \quad \xi_n(\vec{z}_t) \le \frac{5}{2}\xi_n(\vec{1})\Big) \qquad \text{or} \qquad \Big(c_t = 1 \quad \text{and} \quad \xi_n(\vec{z}_t) \ge 1 - \frac{3}{2}\xi_n(\vec{1})\Big).$$

We claim that this implies

$$\vec{z}_t = -\vec{1} \text{ rem } \vec{m} \qquad \text{or} \qquad \vec{z}_t = \vec{0} \qquad \text{or} \qquad \vec{z}_t = \vec{1} \qquad \text{or} \qquad \vec{z}_t = \vec{2}. \tag{54}$$

Assume first $\xi_n(\vec{z}_t) \le \frac{5}{2}\xi_n(\vec{1})$. Either $\vec{z}_t = \vec{0}$ and we are done, or

$$\xi_n(\vec{z}_t) \ge \xi_n(\vec{1}) - 2^{-n}(3k)$$

by Lemma 5.10, and $\vec{z}_t' = \vec{z}_t - \vec{1}$ satisfies

$$\xi_n(\vec{z}_t') = \xi_n(\vec{z}_t) - \xi_n(\vec{1}) + c \pm^{2^{-n}k}_{0} \ge c - 2^{-n}(3k)$$

for some $c \in \{0,1\}$ by Corollary 5.11. For n large enough, $c = 1$ is ruled out by Lemma 5.10, hence $c = 0$, and

$$\xi_n(\vec{z}_t') \le \frac{3}{2}\xi_n(\vec{1}) + 2^{-n}k.$$

Repeating the same argument, either $\vec{z}_t' = \vec{0}$ and $\vec{z}_t = \vec{1}$, or $\vec{z}_t'' = \vec{z}_t' - \vec{1}$ satisfies

$$\xi_n(\vec{z}_t'') \le \frac{1}{2}\xi_n(\vec{1}) + 2^{1-n}k,$$

in which case we must have $\vec{z}_t'' = \vec{0}$ by Lemma 5.10, hence $\vec{z}_t = \vec{2}$.

If $\xi_n(\vec{z}_t) \ge 1 - \frac{3}{2}\xi_n(\vec{1})$, a similar argument yields $\vec{z}_t \equiv -\vec{1} \pmod{\vec{m}}$.

Now, (54) immediately gives $b_t \in \{-1,0,1,2\}$ and $\vec{z}_t \equiv b_t\vec{1} \pmod{\vec{m}}$. Moreover, Lemma 5.9 gives

$$\xi_n(\vec{2}) = 2\xi_n(\vec{1}) \pm^{0}_{2^{-n}k},$$
$$\xi_n(-\vec{1}) = 1 - \xi_n(\vec{1}) \pm^{2^{-n}k}_{0},$$

and then

$$\begin{aligned}\xi_n(\vec{y}_t) &= \xi_n(2\vec{y}_{t+1}) + \xi_n(b_t\vec{1}) - c_t \pm^{0}_{2^{-n}k} \\ &= 2\xi_n(\vec{y}_{t+1}) + \xi_n(b_t\vec{1}) - c_t \pm^{0}_{2^{-n}(2k)} \\ &= 2\xi_n(\vec{y}_{t+1}) + b_t\xi_n(\vec{1}) \pm^{2^{-n}k}_{2^{-n}(3k)}\end{aligned}$$

follows.[5] We did not pay attention to how large n need to be, but we can make sure it holds for $n \geq |k| + 2 + \sum_i |m_i|$ using Lemma 5.12 as above. $\square$

We are ready to prove that CRR reconstruction works.

Theorem 5.24 *VTC^0(imul) proves: if $\vec{m}$ is a nonempty sequence of distinct odd primes, and $\vec{x} < \vec{m}$, then $X = \operatorname{Rec}(\vec{m}; \vec{x})$ satisfies $0 \leq X < 2^{\sum_i |m_i|}$ and $\vec{x} = X \operatorname{rem} \vec{m}$.*

Proof: Using the notation from Definition 5.20, we define

$$Y_t = \sum_{u<s-t} 2^u b_{t+u}$$

for all $t \leq s$, where $b_t \in \{-1, 0, 1, 2\}$ by Lemma 5.23. Clearly, $Y_s = 0$, and we see that

$$Y_t = 2Y_{t+1} + b_t \tag{55}$$

for $t < s$. By the definition of $\vec{z}_t$ and Lemma 5.23, we have $\vec{y}_s = \vec{0}$ and

$$\vec{y}_t \equiv 2\vec{y}_{t+1} + b_t\vec{1} \pmod{\vec{m}}$$

for $t < s$, hence by reverse induction on t, we obtain

$$\vec{y}_t = Y_t \operatorname{rem} \vec{m}.$$

In particular, $Y_0 = X$ satisfies $\vec{x} = X \operatorname{rem} \vec{m}$.

At this point, X may be negative; we only know $-2^s < X < 2^{s+1}$. However, combining (55) with (53), we obtain for large enough n

$$\xi_n(\vec{y}_t) = Y_t\xi_n(\vec{1}) \pm 2^{s-t-n}(3k)$$

by reverse induction on t, hence in particular

$$\xi_n(\vec{x}) = X\xi_n(\vec{1}) \pm 2^{s-n}(3k).$$

This ensures $X \geq 0$, and in view of Lemma 5.8, also $X < 2^{\sum_i |m_i|}$. $\square$

[5] A subtle point here is that we rely on $-\vec{1} \not\equiv \vec{2} \pmod{\vec{m}}$: otherwise, if $c_t = 0$ and $\vec{z}_t = \vec{2}$, then Definition 5.20 makes $b_t = -1$ rather than $b_t = 2$, in which case $b_t\xi_n(\vec{1})$ is off by 1 from $\xi_n(b_t\vec{1}) - c_t$ in the argument above. That is, the given proof only works unless $k = 1$ and $m_0 = 3$. However, in the latter case, all the numbers involved are standard, and one can check that in actual reality, always $b_t \in \{0, 1\}$, hence the bad case does not arise.

Corollary 5.25 *VTC^0(imul) proves: if $\vec{m}$ is a nonempty sequence of distinct odd primes, and $\vec{x} = X$ rem $\vec{m}$, where $|X| < \sum_{i<k}\big(|m_i| - 1\big)$, then* $\mathrm{Rec}(\vec{m};\vec{x}) = X$.

Proof: Let $h = |X|$. For large enough n, we have

$$\xi_n(\vec{y}_h) \le (1 - 2^{-h})\xi_n(\vec{1}) + 2^{-2s} + 2^{-n}k < \xi_n(\vec{1}) - 2^{-n}(3k)$$

by Lemmas 5.22 and 5.15, thus $\vec{y}_h = \vec{0}$ by Lemma 5.10. Likewise, $\vec{y}_t = \vec{0}$ for all $t \ge h$, thus $b_t = 0$ for $t \ge h$. It follows that $\mathrm{Rec}(\vec{m},\vec{x}) < 2^{h+1}$, hence $X \equiv \mathrm{Rec}(\vec{m};\vec{x}) \pmod{\vec{m}}$ implies $X = \mathrm{Rec}(\vec{m};\vec{x})$ by Corollary 5.16. □

It is now straightforward to infer *IMUL*: we can compute $\prod_{i<n} X_i$ by performing the iterated product in CRR and applying Rec; the soundness of the reconstruction procedure easily implies that the result satisfies the required recurrence.

Theorem 5.26 *VTC^0(imul) proves IMUL.*

Proof: Given a sequence $\langle X_i : i < n\rangle$, let us fix a sequence of distinct odd primes $\vec{m}$ such that

$$\sum_{i<k}\big(|m_i| - 1\big) > \sum_{i<n}|X_i| \tag{56}$$

using Theorem 3.2. For each $i < n$, let $\vec{x}_i = X_i$ rem $\vec{m}$, and for each $u \le v \le n$, we define

$$\begin{aligned} \vec{y}_{u,v} &= \prod_{i=u}^{v-1} \vec{x}_i \text{ rem } \vec{m}, \\ Y_{u,v} &= \mathrm{Rec}(\vec{m};\vec{y}_{u,v}) \end{aligned}$$

(this is elementwise modular product). Clearly, $\vec{y}_{u,u} = \vec{1}$, hence $Y_{u,u} = 1$ by Corollary 5.25. For any fixed $u \le n$, we prove

$$|Y_{u,v+1}| \le \sum_{i=u}^{v}|X_i| \qquad \text{and} \qquad Y_{u,v+1} = Y_{u,v}\cdot X_v \tag{57}$$

by induction on $v = u,\dots,n-1$: for $v = u$, we have $\vec{y}_{u,u+1} = \vec{x}_u$, hence $Y_{u,u+1} = X_u$ by Corollary 5.25. Assuming (57) holds for $v - 1$, we have

$$|Y_{u,v}X_v| \le |Y_{u,v}| + |X_v| \le \sum_{i=u}^{v}|X_i| < \sum_{i<k}\big(|m_i| - 1\big),$$

and

$$\vec{y}_{u,v+1} = \vec{y}_{u,v} \times \vec{x}_v \equiv Y_{u,v}X_v \pmod{\vec{m}}$$

by Theorem 5.24, hence

$$Y_{u,v}X_v = \mathrm{Rec}(\vec{m};\vec{y}_{u,v+1}) = Y_{u,v+1}$$

by Corollary 5.25, which gives (57) for v.

Thus, $\langle Y_{u,v} : u \le v \le n\rangle$ witnesses that *IMUL* holds. □

For purposes of the next section, it will be convenient to observe that Theorem 5.26 also gives a proof of *IMUL* in the basic theory corresponding to logspace:

Corollary 5.27 *VL proves IMUL.*

Proof: Since *VL* is a CN theory and includes VTC^0, it suffices to show $VL \vdash Tot_{\mathrm{imul}}$. Now, Tot_{Iter} clearly implies its variant where we start the iteration at a different element than 0, and then we can construct the sequence witnessing the computation of $\prod_{i<n} a_i \text{ rem } m$ by iterating the function $F(\langle i, x\rangle) = \langle i+1, xa_i \text{ rem } m\rangle$ starting from $\langle 0, 1\rangle$. □

6 The polylogarithmic cut

After putting iterated multiplication in $\mathrm{TC}^0(\mathrm{pow})$, Hesse, Allender, and Barrington [13] go on to show that iterated multiplication restricted to *polylogarithmically small inputs* is in AC^0, essentially by proving that AC^0 includes the polylogarithmically scaled-down version of $\mathrm{TC}^0(\mathrm{pow})$. In fact, although they do not state it that way, this is a consequence of Nepomnjaščij's theorem [21], which implies more generally that AC^0 includes the polylogarithmically scaled-down version of L, and even NL (which is essentially $\mathrm{NSPACE}(\log\log n)$, as $\log\bigl((\log n)^{O(1)}\bigr) = O(\log\log n)$).

The counterpart of such scaling-down arguments in arithmetic is the following model-theoretic construction:

Definition 6.1 If $\mathcal{M} = \langle M_1, M_2, \in, |\cdot|, 0, 1, +, \cdot, <\rangle$ is a model of V^0, the *polylogarithmic cut* $\mathcal{M}_{\mathrm{pl}}$ *of* $\mathcal{M}$ is the substructure of $\mathcal{M}$ with first-order and second-order domains

$$M_{\mathrm{pl},1} = \{x \in M_1 : \exists c \in \omega\, \mathcal{M} \vDash \exists z\, x \leq |z|^c\},$$
$$M_{\mathrm{pl},2} = \{X \in M_2 : |X| \in M_{\mathrm{pl},1}\} = \{X \in M_2 : X \subseteq M_{\mathrm{pl},1}\}.$$

By formalizing Nepomnjaščij's construction, Müller [19] proved that polylogarithmic cuts of models of V^0 are models of VNC^1 (see [9] for a definition):

Theorem 6.2 (Müller [19]) *If* $\mathcal{M} \vDash V^0$*, then* $\mathcal{M}_{\mathrm{pl}} \models VNC^1$. □

In fact, earlier Zambella [29] effectively proved that polylogarithmic cuts are even models of the stronger theory *VL*, though the result was presented in a different way. For definiteness, we include a self-contained proof while strengthening the theory further to *VNL*, again following the idea of Nepomnjaščij [21]. A similar formalization of Nepomnjaščij's theorem in $I\Delta_0(\alpha)$ was given by Atserias [2, 3].

Theorem 6.3 *If* $\mathcal{M} \vDash V^0$*, then* $\mathcal{M}_{\mathrm{pl}} \models$ *VNL.*

Proof: Work in V^0. Let $0 < a \leq |z|^c$ and $E \subseteq [0, a] \times [0, a]$. For $l = 0, \dots, 2c$, We define Σ^B_0 formulas $\varphi_l(d, s, t)$ with parameter E that express E-reachability in $\leq d \leq w^l$ steps, where

$w = \lceil |z|^{1/2} \rceil$:

$$\varphi_0(d,s,t) \Leftrightarrow d \le 1 \wedge s \le a \wedge t \le a \wedge \big(s = t \vee (d = 1 \wedge E(s,t))\big),$$
$$\varphi_{l+1}(d,s,t) \Leftrightarrow \exists \langle x_i : i \le k\rangle \ \big(k < w \wedge kw^l \le d \wedge \forall i \le k\, x_i \le a \wedge x_0 = s \wedge \forall i < k\, \varphi_l(w^l, x_i, x_{i+1}) \wedge \varphi_l(d - kw^l, x_k, t)\big).$$

Notice that (using our efficient sequence encoding) the sequence quantified in the definition of φ_{l+1} has bit-length $O\big(k + \sum_{i\le k}|x_i|\big) = O(w|a|) = O(|z|^{1/2}||z||) = O(|z|)$, hence it can be encoded by a small number bounded by a polynomial in z, thus the formulas φ_l are indeed Σ^B_0.

By (meta)induction on l, we claim that V^0 proves

$$\varphi_l(d,s,t) \to d \le w^l \wedge s \le a \wedge t \le a, \tag{58}$$
$$\forall s,t \le a\ \big(\varphi_l(0,s,t) \leftrightarrow s = t\big), \tag{59}$$
$$\forall d < w^l\ \forall s,t \le a\ \big(\varphi_l(d+1,s,t) \leftrightarrow \exists u \le a\ \big[\varphi_l(d,s,u) \wedge \big(u = t \vee E(u,t)\big)\big]\big). \tag{60}$$

The properties (58) and (59) are straightforward. We have (60) for $l = 0$ from the definition of φ_0. Assuming (60) holds for l, we prove it for $l+1$.

Left to right: if $\varphi_{l+1}(d+1,s,t)$, let $\vec{x} = \langle x_i : i \le k\rangle$ be the sequence that witnesses the definition. By (58), we have $kw^l \le d+1 \le (k+1)w^l$; if $d+1 = kw^l$, we may drop the last element $x_k = t$ from $\vec{x}$ and the definition will still be satisfied, hence we may assume $kw^l \le d < (k+1)w^l$. By (60) for l, $\varphi_l(d+1-kw^l, x_k, t)$ implies $\varphi_l(d - kw^l, x_k, u)$ for some $u \le a$ such that $u = t$ or $E(u,t)$. Then $\vec{x}$ witnesses that $\varphi_{l+1}(d, x_k, u)$ holds.

For the right-to-left implication, we reverse the process: if $\vec{x}$ witnesses $\varphi_{l+1}(d,s,u)$, where $u = t$ or $E(u,t)$, we can ensure $kw^l \le d < (k+1)w^l$ by extending $\vec{x}$ with u if necessary; then $\varphi_l(d-kw^l, x_k, u)$ implies $\varphi_l(d+1-kw^l, x_k, t)$ by (60) for l, whence $\vec{x}$ witnesses $\varphi_{l+1}(d+1,s,t)$.

It follows that

$$Y = \big\{\langle d,u\rangle : d,u \le a \wedge \varphi_{2c}(d,0,u)\big\},$$

which exists by Σ^B_0-*COMP*, witnesses the truth of Tot_{Reach} (the defining axiom of *VNL*) in the polylogarithmic cut. □

Corollary 6.4 *If VNL proves $\forall X\, \varphi(X)$, where $\varphi \in \Sigma^1_1$, then*

$$V^0 \vdash \forall z\, \forall X\ \big(|X| \le |z|^c \to \varphi(X)\big)$$

for every constant c.

Proof: Σ^1_1 formulas are preserved upwards from cuts. □

Corollary 6.5 V^0 *proves* $\forall w\, IMUL\big[|w|^c\big]$, $\forall w\, Tot^*_{\mathrm{Div}}\big[|w|^c\big]$, *and* $\forall w\, Tot^*_{\mathrm{imul}}\big[|w|^c, -\big]$ *(even modulo arbitrary $m > 0$, not just primes) for every constant c.*

Proof: $VL \subseteq VNL$ proves *IMUL*, hence *DIV*, by Corollary 5.27, hence V^0 proves $IMUL\big[|w|^c\big]$ and $Tot^*_{\mathrm{Div}}\big[|w|^c\big]$ by Corollary 6.4. Then $Tot^*_{\mathrm{imul}}\big[|w|^c, -\big]$ also follows: given m and $\langle x_i : i < n\rangle$ where $n \le |w|^c$ and $w \ge \max_i x_i$, we can compute $Y = \prod_{i<n} x_i$ using $IMUL\big[|w|^{c+1}\big]$, and $Y \operatorname{rem} m$ using $Tot^*_{\mathrm{Div}}\big[|w|^{c+1}\big]$. □

Remark 6.6 Using the arguments in Corollary 5.27 and Theorem 6.3, it is easy to prove in V^0 directly Tot^*_{imul} restricted to products $\prod_{i<n} a_i$ rem m where $n \le |w|^c$ and $|m| \le |w|^{1-\varepsilon}$ for some constant $\varepsilon > 0$. However, a nontrivial result like Theorem 5.26 seems to be required to get to larger m.

As a consequence of Corollary 6.5, $\prod_{i<\min\{n,|w|^c\}} a_i$ rem m is in $\overline{V^0}$ definable by an $L_{\overline{V^0}}$ function $f_c(A, n, m, w)$ (where A encodes $\langle a_i : i < n\rangle$), and consequently, $\Sigma^B_0(f_c) = \Sigma^B_0$ over $\overline{V^0}$. In other words, we may, and will, use modular products of polylogarithmic length freely in Σ^B_0 formulas.

7 Modular exponentiation

While [13] show modular powering a^r rem m of small integers to be in AC^0, we do not know how to prove the corresponding result in V^0; instead, we will work in the theory $V^0 + \mathit{WPHP} \subseteq \mathit{VTC}^0$.

The argument in [13] involves computation with $a^{\lfloor n/d\rfloor}$, where $n = m - 1$ is the size of the group, and d a logarithmically small prime. This means it suffers from chicken-vs-egg problems as the analysis of the modular powering algorithm needs powering with non-polylogarithmic exponents, which is only defined after the modular powering algorithm is proved to work. Moreover, the expression of $a^{\lfloor n/d\rfloor}$ in terms of $(a^{-n \text{ rem } d})^{1/d}$ relies on Fermat's little theorem, which again cannot be stated, let alone proved, without having a means to express a^n in the group. (Actually, Fermat's little theorem is not even known to be provable in the theory $V_0 + \Omega_1 \supseteq V_0 + \mathit{WPHP}$, which *can* define modular exponentiation with no difficulty; it appears that the strong pigeonhole principle is required to prove it. See [14, §4].)

It turns out we can avoid both problems by using a modified (and arguably simpler) algorithm that exploits the basic idea of [13], viz. Chinese remaindering of exponents, more directly. We formulate the results for prime moduli here, but this is only to simplify the bounds; the construction as such works for any finite abelian group.

First, we need to make sure there are enough polylogarithmically small primes d such that $x \mapsto x^d$ is a bijection on $(\mathbb{Z}/m\mathbb{Z})^\times$. (In the real world, these are exactly the primes not dividing $m - 1$.) We obtain this with two applications of *WPHP*: one ensures that $x \mapsto x^d$ is surjective whenever it is injective, and the other shows that the number of primes d for which it is not injective (i.e., such that $(\mathbb{Z}/m\mathbb{Z})^\times$ contains an element of order d) is quite limited, essentially because $(\mathbb{Z}/m\mathbb{Z})^\times$ contains a subgroup whose order is the product of all such "bad" primes.

Lemma 7.1 *For any constant c, $V^0 + \mathit{WPHP}$ proves: if m and $d \le |w|^c$ are primes such that $x^d \not\equiv 1 \pmod m$ for all $1 < x < m$, then for all y coprime to m, there exists a unique $x < m$ such that $x^d \equiv y \pmod m$. We will write $x = y^{1/d}$.*

Proof: Since $x \mapsto x^d$ is a group homomorphism, the fact that it has trivial kernel implies it is injective. Assume for contradiction that it is not surjective, and fix y outside its image. Since m is prime, the residues coprime to m comprise the interval $[1, m - 1]$. Thus, we can define an injective function $F\colon \{0, 1\} \times [1, m - 1] \to [1, m - 1]$ by $F(u, x) = y^u x^d$ rem m, contradicting $\mathit{PHP}^{2(m-1)}_{m-1}$. □

Lemma 7.2 *For any constant c, V^0 + WPHP proves: if m is a prime, and $\langle d_i : i < k\rangle$ a sequence of distinct primes $d_i \le |w|^c$ such that for each i, $x \mapsto x^{d_i} \operatorname{rem} m$ is not a bijection on $(\mathbb{Z}/m\mathbb{Z})^\times$, then $\sum_{i<k}\bigl(|d_i| - 1\bigr) \le |m|$.*

Proof: Using Lemma 7.1, for each i, let x_i be the least number in $[2, m-1]$ such that $x_i^{d_i} \equiv 1 \pmod m$. (This is Σ^B_0 definable, hence $\langle x_i : i < k\rangle$ exists.)

Notice that using $x_i^{d_i} \equiv 1$ and $Tot^*_{\mathrm{imul}}\bigl[|w|^c, -\bigr]$, we can define $x_i^u \operatorname{rem} m$ for arbitrary u as $x_i^{u \operatorname{rem} d_i} \operatorname{rem} m$; this will satisfy $x_i^{u+v} \equiv x_i^u x_i^v \pmod m$ by induction on v. Since d_i is prime and $x_i \not\equiv 1$, we have $x_i^u \equiv 1$ only if $d_i \mid u$.

Assume first that $\sum_{i<k}|d_i| \le 2|m| + c||w||$, thus $d = \prod_{i<k} d_i$ exists, and $d \le 2^{c+2}m^2|w|^c$ is a small number. Using $Tot^*_{\mathrm{imul}}\bigl[k|w|^c, -\bigr]$, we can define a function $F\colon [0, d) \to [1, m-1]$ by $F(u) = \prod_i x_i^{u_i} \operatorname{rem} m$, where $u_i = \lfloor u / \prod_{j<i} d_j\rfloor \operatorname{rem} d_i$ (that is, we use $[0, d)$ to encode $\prod_i [0, d_i)$). We claim that F is injective, hence $d < 2m$ by PHP^{2m}_m, which implies

$$\sum_{i<k}\bigl(|d_i| - 1\bigr) \le |2m| - 1 = |m| \tag{61}$$

by (10). Since F is a group homomorphism w.r.t. the elementwise sum of sequences modulo $\vec d$, it suffices to show that it has trivial kernel. Thus, let $\vec u < \vec d$ be such that $\prod_i x_i^{u_i} \equiv 1$. By induction on v, we can prove

$$\prod_{i<k} x_i^{u_i v} \equiv 1$$

for all v. In particular, for any $j < k$, taking $v_j = \prod_{i \ne j} d_i$ gives

$$1 \equiv \prod_{i<k} x_i^{u_i v_j} \equiv x_j^{u_j v_j},$$

thus $d_j \mid u_j v_j$. Since v_j is coprime to d_j, this shows $d_j \mid u_j$, i.e., $u_j = 0$; thus, $\vec u = \vec 0$, as j was arbitrary.

If $\sum_i |d_i| > 2|m| + c||w||$, let $k' < k$ be maximal such that $\sum_{i<k'}|d_i| \le 2|m| + c||w||$. By the proof above, we have $\sum_{i<k'}\bigl(|d_i| - 1\bigr) \le |m|$, thus

$$\sum_{i<k'+1} |d_i| \le 2\sum_{i<k}\bigl(|d_i| - 1\bigr) + |d_{k'}| \le 2|m| + c||w||,$$

contradicting the choice of k'. □

We now get to the construction of modular exponentiation $a^r \operatorname{rem} m$. As we already mentioned, the basic idea (following [13]) is to express exponents in CRR modulo a list $\vec d$ of polylogarithmic primes such that $x \mapsto x^{1/d_i}$ is well-defined. Unlike [13], the way we employ this idea here is to define $a^{x/d}$ for $x = O(d)$, where $d = \prod_i d_i$, using a form of (14). We then extend it to all x by periodicity, allowing us to define a^r as $a^{(rd)/d}$.

Theorem 7.3 *V^0 + WPHP proves Tot^*_{pow}.*

Proof: Since $V^0 + \mathit{WPHP}$ is a CN theory, it suffices to prove $\mathit{Tot}_{\rm pow}$. Given a prime m, let $\langle d_i : i < k' \rangle$ be the list[6] of all primes

$$d_i \le 2|m|\big(||m||+1\big)^{17} \tag{62}$$

such that $x^{d_i} \not\equiv 1 \pmod m$ for all $x \not\equiv 1 \pmod m$. We have

$$\sum_{d \le 2|m|(||m||+1)^{17}} \big(|d|-1\big) \ge 2|m|$$

by Theorems 3.2 and 6.3, hence

$$\sum_{i<k'} \big(|d_i|-1\big) \ge 2|m| - |m| = |m|$$

by Lemma 7.2. Let $k \le k'$ be smallest such that

$$\sum_{i<k} \big(|d_i|-1\big) \ge |m|.$$

Then

$$\sum_{i<k} \big(|d_i|-1\big) \le |m| - 1 + |d_{k-1}| \le |m| + ||m|| + 17\big|||m||+1\big| = O(|m|),$$

hence $d = \prod_{i<k} d_i$ exists as a small number, while

$$d \ge 2^{\sum_i (|d_i|-1)} \ge 2^{|m|} > m.$$

By Lemma 7.1, $x \mapsto x^{d_i} \operatorname{rem} m$ is a bijection on $(\mathbb{Z}/m\mathbb{Z})^\times$ for each $i < k$. Put $\tilde d_i = \prod_{j \ne i} d_j = d/d_i$.

Let $0 < a < m$ be given. For every $r \le 2d$, we define

$$a^{r/d} = a^{u(r)} \prod_{i<k} (a^{1/d_i})^{u_i(r)} \operatorname{rem} m \tag{63}$$

using the notation of Lemma 7.1, where

$$\begin{aligned} u_i(r) &= r \tilde d_i^{-1} \operatorname{rem} d_i, \\ u(r) &= \frac{1}{d}\Big(r - \sum_{i<k} u_i(r) \tilde d_i\Big). \end{aligned}$$

Here,

$$\sum_{i<k} u_i(r)\tilde d_i \equiv u_j(r)\tilde d_j \equiv r \pmod{d_j}$$

for each $j < k$, hence $\sum_{i<k} u_i(r)\tilde d_i \equiv r \pmod d$, i.e., $u(r)$ is an integer, and $-k \le u(r) \le 2$, where $k \le |m|$. Thus, $a^{r/d}$ can be evaluated using $\mathit{Tot}^*_{\rm imul}\big[|m|^{O(1)}, -\big]$.

[6] It may not be immediately apparent why we can construct a *sequence* consisting of all these primes. Note that the ith element of the sequence is Δ_0-definable using Theorem 2.3 as the unique prime d satisfying (62) and $\forall x < m\, (x > 1 \to x^d \not\equiv 1 \pmod m)$ such that there are exactly i smaller primes with this property.

We claim that

$$a^{(r+s)/d} \equiv a^{r/d} a^{s/d} \pmod{m} \tag{64}$$

for all r, s such that $r + s \leq 2d$. Indeed, we have $u_i(r+s) = u_i(r) + u_i(s) - c_i d_i$ with $c_i \in \{0, 1\}$, hence $u(r+s) = u(r) + u(s) + \sum_{i<k} c_i$, and

$$\begin{aligned}
a^{(r+s)/d} &\equiv a^{u(r)+u(s)+\sum_i c_i} \prod_{i<k} (a^{1/d_i})^{u_i(r)+u_i(s)-c_i d_i} \\
&\equiv a^{u(r)} a^{u(s)} a^{\sum_i c_i} \prod_{i<k} (a^{1/d_i})^{u_i(r)} (a^{1/d_i})^{u_i(s)} a^{-c_i} \\
&\equiv a^{r/d} a^{s/d}.
\end{aligned}$$

Using *WPHP*, there exist $r < s \leq 2m \leq 2d$ such that $a^{r/d} = a^{s/d}$. Putting $t = s - r$, we have $0 < t \leq 2m$ and $a^{t/d} = 1$ by (64) (which implies $a^{(rt)/d} = 1$ for all r such that $rt \leq 2d$ by induction on r). We then extend the definition of $a^{r/d}$ to arbitrary small r by putting

$$a^{r/d} = a^{(r \text{ rem } t)/d}.$$

This agrees with the original definition for $r \leq 2d$ using (64), and the new definition also satisfies (64). Finally, we define

$$a^r = a^{(rd)/d}.$$

Direct computation shows that $u_i(0) = u_i(d) = 0$, $u(0) = 0$, and $u(d) = 1$, hence $a^{0/d} = 1$ and $a^{d/d} = a$. Thus, we obtain the defining recurrence for pow:

$$\begin{aligned}
a^0 &= 1, \\
a^{r+1} &= a^r a \text{ rem } m.
\end{aligned}$$

We only defined it for $0 < a < m$, but we can simply put

$$0^r = \begin{cases} 1, & r = 0, \\ 0, & r > 0 \end{cases}$$

for $a = 0$. □

As in Remark 6.6, it follows that we can use pow freely in Σ_0^B formulas (as long as we stick to extensions of $V^0 + \mathit{WPHP}$):

Corollary 7.4 $\Sigma_0^B(\text{pow}) = \Sigma_0^B$ *over* $\overline{V^0} + \mathit{WPHP}$. □

Once we have exponentiation, let us show for further reference that any element of $(\mathbb{Z}/m\mathbb{Z})^\times$ has a well-defined order, and that orders have the expected basic properties.

Lemma 7.5 $V^0 + \mathit{WPHP}$ *proves: if m is a prime, then every $0 < a < m$ has a unique* order *$0 < o_m(a) < 2m$ which satisfies*

$$a^r \equiv 1 \pmod{m} \iff o_m(a) \mid r$$

for all r.

Proof: Using *WPHP*, there are $r < r' < 2m$ such that $a^r \equiv a^{r'} \equiv a^r a^{r'-r} \pmod{m}$, thus $r' - r > 0$ and $a^{r'-r} \equiv 1 \pmod{m}$ as a^r is invertible. Let $o_m(a) = t$ be the least $t > 0$ such that $a^t \equiv 1 \pmod{m}$. On the one hand, this implies $a^{tr} \equiv 1 \pmod{m}$ for all r. On the other hand, if $a^r \equiv 1 \pmod{m}$, we have

$$1 \equiv a^r \equiv a^{(r \text{ rem } t)+t\lfloor r/t \rfloor} \equiv a^{r \text{ rem } t}(a^t)^{\lfloor r/t \rfloor} \equiv a^{r \text{ rem } t} \pmod{m},$$

hence $r \equiv 0 \pmod{t}$ by the minimality of t. □

We note that $o_m(a)$ is Σ^B_0-definable (using Corollary 7.4) as the least $t > 0$ such that $a^t \equiv 1 \pmod{m}$.

Lemma 7.6 *V^0 + WPHP proves that for any prime m and $0 < a, a' < m$:*

(i) For any r, $o_m(a^r) = o_m(a)/\gcd\{o_m(a), r\}$. Thus, if $r \mid o_m(a)$, then $o_m(a^r) = o_m(a)/r$.

(ii) There exists $0 < b < m$ such that $o_m(b) = \operatorname{lcm}\{o_m(a), o_m(a')\}$.

Proof: (i): Let $t = o_m(a)$ and $d = \gcd\{t, r\}$. Then for any s, $a^{rs} \equiv 1$ iff $t \mid rs$ iff $\frac{t}{d} \mid \frac{r}{d}s$ iff $\frac{t}{d} \mid s$ as $\frac{t}{d}$ and $\frac{r}{d}$ are coprime.

(ii): Put $t = o_m(a)$ and $t' = o_m(a')$. First, we claim that if $\gcd\{t, t'\} = 1$, then $o_m(aa') = tt'$: on the one hand, $(aa')^{tt'} \equiv (a^t)^{t'}(a'^{t'})^t \equiv 1$. On the other hand, if $(aa')^r \equiv 1$, then $1 \equiv (aa')^{rt'} \equiv a^{rt'}$, hence $t \mid rt'$, which implies $t \mid r$ as t and t' are coprime. A symmetric argument gives $t' \mid r$, hence $tt' = \operatorname{lcm}\{t, t'\} \mid r$.

We prove the general case by induction on t. If $t = 1$, we may take $b = a'$. Otherwise, t is divisible by a prime p; write $t = sp^e$ and $t' = s'p^{e'}$, where $p \nmid s, s'$. Since $o_m(a^{p^e}) = s < t$ and $o_m(a'^{p^{e'}}) = s'$ by (i), there exists b such that $o_m(b) = \operatorname{lcm}\{s, s'\}$ by the induction hypothesis. Moreover, one of a^s and $a'^{s'}$ has order $p^{\max\{e,e'\}}$, hence ba^s or $ba'^{s'}$ has order $\operatorname{lcm}\{s, s'\}p^{\max\{e,e'\}} = \operatorname{lcm}\{t, t'\}$ by the coprime case. □

8 Generators of multiplicative groups

We could finish the proof of the main result at this point if we could show that VTC^0 (possibly using, say, Tot^*_{pow} and $Tot^*_{\text{imul}}\big[|w|^c, -\big]$) proves Tot_{imul}. In the real world, iterated multiplication modulo a prime m reduces easily to powering modulo m as $(\mathbb{Z}/m\mathbb{Z})^\times$ is cyclic, and we can do iterated sums of the corresponding discrete logarithms in TC^0. Thus, it would suffice to prove in VTC^0 that multiplicative groups of prime fields are cyclic.

Unfortunately, we do not know how to do that directly. However, as a starting point to further investigation, let us at least establish that *IMUL* is *equivalent* to the cyclicity of multiplicative groups of prime fields over VTC^0.

Proposition 8.1 *The following are equivalent over VTC^0.*

(i) IMUL.

(*ii*) *For all primes m, the groups $(\mathbb{Z}/m\mathbb{Z})^\times$ are cyclic:*

$$\exists g < m\, \forall a < m\, \bigl(a \neq 0 \to \exists r < m\; g^r \equiv a \pmod{m}\bigr).$$

(*iii*) *For all primes m and p, if $a, b < m$ are such that $a \neq 1$ and $a^p \equiv b^p \equiv 1 \pmod{m}$, then $b \equiv a^r \pmod{m}$ for some $r < m$.*

Proof:

(ii) $\to$ (i): In view of Theorem 5.26, it suffices to prove Tot^*_{imul}. Given a prime m and $\langle a_i : i < n\rangle$, where w.l.o.g. $0 < a_i < m$ for each $i < n$, we define g to be the least generator of $(\mathbb{Z}/m\mathbb{Z})^\times$, a sequence $\langle r_i : i < n\rangle$ such that $r_i < m$ is least such that $g^{r_i} \equiv a_i \pmod{m}$, and a sequence $\langle b_i : i \leq n\rangle$ by

$$b_i = g^{\sum_{j<i} r_j} \operatorname{rem} m.$$

Then $b_0 = 1$ and $b_{i+1} = b_i a_i \operatorname{rem} m$, hence $\vec{b}$ witnesses that Tot_{imul} holds. Now, we need to apply this argument in parallel several times to get the aggregate function, but this is not a problem.

(iii) $\to$ (ii): Let g be an element of $(\mathbb{Z}/m\mathbb{Z})^\times$ of maximal order, and put $t = o_m(g)$. (While Lemma 7.5 only claims $t < 2m$, we have in fact $t < m$, as VTC^0 implies PHP^m_{m-1}.) Assume for contradiction that g is not a generator of $(\mathbb{Z}/m\mathbb{Z})^\times$, and fix $0 < a < m$ such that $a \not\equiv g^r$ for all $r < t$. Let $s \leq o_m(a)$ be minimal such that $a^s \equiv g^r$ for some $r < t$. Since $s > 1$, there is a prime $p \mid s$; replacing a with $a^{s/p}$ if necessary, we may assume $s = p$. This implies $p \mid o_m(a)$: otherwise $a \equiv (a^p)^{p^{-1} \operatorname{rem} o_m(a)} \equiv g^r$ for some r, a contradiction.

By Lemma 7.6 (ii), the maximality of t implies $p \mid o_m(a) \mid t$, thus $b = g^{t/p}$ has order p. But then $a \equiv b^r \equiv g^{rt/p}$ for some r by (iii), a contradiction.

(i) $\to$ (iii): Let $o_m(a) = p$ and $b^p \equiv 1 \pmod{m}$. The basic idea is to use $IMUL$ to construct the polynomials $f_i(x) = \prod_{j<i}(x - a^j) \pmod{m}$ for $i \leq p$, aiming to show $f_p(x) \equiv x^p - 1$, which yields $\prod_{j<p}(b - a^j) \equiv 0$.

Fix $n \geq p|m|$, put $\alpha_j = (-a^j) \operatorname{rem} m$ for $j < p$, and write

$$\prod_{j<i}(2^n + \alpha_j) = \sum_{j\leq i} C_{i,j} 2^{jn}, \qquad 0 \leq C_{i,j} < 2^n.$$

By induction on $i \leq p$, we claim that

$$\sum_{j\leq i} C_{i,j} \leq m^i, \tag{65}$$

$$C_{i,j} = \begin{cases} 1, & j = i, \\ C_{i-1,j-1} + \alpha_{i-1} C_{i-1,j}, & 0 < j < i, \\ \alpha_{i-1} C_{i-1,0}, & 0 = j < i. \end{cases} \tag{66}$$

For $i = 0$, (65) and (66) are obvious. Assuming the statements hold for i, we have

$$\begin{aligned} \sum_{j\leq i+1} C_{i+1,j} 2^{nj} &= (2^n + \alpha_i) \sum_{j\leq i} C_{i,j} 2^{jn} \\ &= C_{i,i} 2^{(i+1)n} + \sum_{j=1}^{i} (C_{i,j-1} + \alpha_i C_{i,j}) 2^{jn} + \alpha_i C_{i,0}. \end{aligned} \tag{67}$$

Here,

$$C_{i,i} + \sum_{j=1}^{i} (C_{i,j-1} + \alpha_i C_{i,j}) + \alpha_i C_{i,0} = (1+\alpha_i) \sum_{j \le i} C_{i,j} \le m \cdot m^i = m^{i+1}$$

by the induction hypothesis, hence also the individual terms in this sum are bounded by $m^{i+1} \le m^p < 2^n$. Thus, matching up the terms in (67) gives (66) for $i+1$, hence also (65).

If we also define $C_{i,j} = 0$ for $j < 0$ or $j > i$ for notational convenience, (66) gives the recurrence

$$\begin{aligned} C_{0,0} &= 1, \\ C_{i+1,j} &\equiv C_{i,j-1} - a^i C_{i,j} \pmod{m} \end{aligned}$$

for all j and $0 \le i < p$, which amounts to saying that $\sum_j C_{i,j} x^j$ is the polynomial $\prod_{j<i} (x - a^j)$; formally, for any $u < m$, we can prove

$$\prod_{j<i} (u - a^j) \equiv \sum_{j \le i} C_{i,j} u^j \pmod{m} \tag{68}$$

by induction on $i \le p$.

We now wish to formalize the symmetry property $f_p(x) \equiv f_p(ax)$ (or equivalently, $f_p(x) \equiv f_p(a^{-1}x)$), which will imply that most coefficients of f_p vanish. To this end, we claim that $C_{i,j}$ satisfies the recurrence

$$C_{i+1,j} \equiv a^{i-j+1} C_{i,j-1} - a^{i-j} C_{i,j} \tag{69}$$

for all j and $0 \le i < p$, which expresses the identity of polynomials

$$\prod_{j \le i} (x - a^j) \equiv a^i (x-1) \prod_{j<i} (a^{-1}x - a^j) \pmod{m}.$$

Since (69) holds trivially for $j < 0$ or $j > i+1$, and the cases $j = 0$ and $j = i+1$ amount to the identities $C_{i+1,0} \equiv -a^i C_{i,0}$ and $C_{i+1,i+1} \equiv 1 \equiv C_{i,i}$, it suffices to prove by induction on i that (69) holds for all $0 < j \le i$. For $i = 0$, this statement is vacuous. Assuming it holds for i, we prove it for $i+1$ as follows:

$$\begin{aligned} C_{i+2,j} &\equiv C_{i+1,j-1} - a^{i+1} C_{i+1,j} \\ &\equiv (a^{i-j+2} C_{i,j-2} - a^{i-j+1} C_{i,j-1}) - a^{i+1} (a^{i-j+1} C_{i,j-1} - a^{i-j} C_{i,j}) \\ &\equiv a^{i-j+2} C_{i,j-2} - (a^{i-j+1} + a^{2i-j+2}) C_{i,j-1} + a^{2i-j+1} C_{i,j} \\ &\equiv a^{i-j+2} (C_{i,j-2} - a^i C_{i,j-1}) - a^{i-j+1} (C_{i,j-1} - a^i C_{i,j}) \\ &\equiv a^{i-j+2} C_{i+1,j-1} - a^{i-j+1} C_{i+1,j}. \end{aligned}$$

Applying (69) with $i = p-1$, we obtain

$$\begin{aligned} C_{p,j} &\equiv a^{p-j} C_{p-1,j-1} - a^{p-j-1} C_{p-1,j} \\ &\equiv a^{-j} (C_{p-1,j-1} - a^{p-1} C_{p-1,j}) \\ &\equiv a^{-j} C_{p,j}, \end{aligned}$$

which implies

$$C_{p,j} \equiv 0$$

for all $0 < j < p$. We also have $C_{p,p} = 1$, and then (68) for $i = p$ and $u = 1$ gives

$$0 \equiv \sum_{j \le p} C_{p,j} \equiv 1 + C_{p,0},$$

thus $C_{p,0} \equiv -1$; that is, $f_p(x) \equiv x^p - 1$. Then, assuming $b^p \equiv 1$, (68) for $u = b$ gives

$$\prod_{j<p} (b - a^j) \equiv b^p - 1 \equiv 0,$$

whence $b \equiv a^j$ for some $j < p$. $\square$

The proof of (ii) $\to$ (i) in Proposition 8.1 does not quite require the cyclicity of $(\mathbb{Z}/m\mathbb{Z})^\times$. Recalling that (apart from pow) we have $Tot^*_{\mathrm{imul}}\bigl[O\bigl(|m|\bigr), -\bigr]$, it would be enough to find a (Σ^B_0(card)-definable) set $X \subseteq [1, m-1]$ of cardinality $O\bigl(|m|\bigr)$ such that every element of $(\mathbb{Z}/m\mathbb{Z})^\times$ can be written as $\prod_{y\in Y} y \bmod m$ for some $Y \subseteq X$; in particular, such an X can be constructed if we can find a set G of generators of $(\mathbb{Z}/m\mathbb{Z})^\times$ such that $\sum_{a\in G} |o_m(a)| = O\bigl(|m|\bigr)$.

Ignoring issues of definability, the *structure theorem for finite abelian groups* (stating that any such group is the product of cyclic groups of prime power orders) ensures that such a generating set exists in the real world for *every* finite abelian group, obviating the need for a condition like (iii). The structure theorem for finite abelian groups was proved in [14] in the theory $S^1_2 + WPHP(\Sigma^b_1)$, which, in our present setup, is a fragment of $V^0 + \Omega_1$; unfortunately, the Ω_1 is needed in the argument not just to prove *WPHP* (which we have in VTC^0 anyway), but also to quantify over subsets of $(\mathbb{Z}/m\mathbb{Z})^\times$ of cardinality $O\bigl(|m|\bigr)$, and thus of bit-size $O\bigl(|m|^2\bigr)$. As such, we do not know how to make the proof work in VTC^0.

However, a key insight is that we can smoothly combine this approach with a (iii)-like condition. Namely, assume that for a given m, we know (iii) to hold for $p < x$. Then the argument in (iii) $\to$ (ii) ensures that $(\mathbb{Z}/m\mathbb{Z})^\times$ has a cyclic subgroup that includes the p-torsion components of $(\mathbb{Z}/m\mathbb{Z})^\times$ for all $p < x$, thus, when looking for other generators as in the structure theorem, we may assume their orders are powers of primes $p \ge x$. In particular, this restricts the number of generators to about $|m|/|x|$, reducing the bit-size of the generating set to $O\bigl(|m|^2/|x|\bigr)$.

We will show below (Lemma 8.5) how to make this idea formal, and use it to break the circular argument in Proposition 8.1: by paying attention to how large numbers are needed in each step, we will see that if we assume (iii) to hold up to x, and go around the circle, we end up with (iii) holding up to something larger than x, setting the stage for a *coup de grâce* by induction.

Definition 8.2 Let $Cyc[z, x]$ denote condition (iii) in Proposition 8.1 restricted to $m \le z$ and $p < x$. Notice that Cyc is a Σ^B_0 formula.

Lemma 8.3 *VTC^0 proves $IMUL\big[x^2|z|\big] \to Cyc[z,x]$.*

Proof: The main instance of *IMUL* used in the proof of (i) $\to$ (iii) in Proposition 8.1 was $\prod_{j<p}(2^n+\alpha_j)$, where $n = p|m|$, thus $\sum_{j<p}|2^n+\alpha_j| = p(n+1) \le (p+1)^2|m| \le x^2|z|$. Moreover, we need products of length p modulo m in (68), simulated with *IMUL* followed by division by m (using pow); these instances have size $p|m| \le x|z|$. $\square$

Lemma 8.4 *VTC^0 proves $Tot^*_{\mathrm{imul}}[-,x^3] \to IMUL[x]$.*

Proof: We need to examine the usage of imul in Section 5. For Subsection 5.1, the reader can easily verify that as we already announced at the beginning of 5.1, the proof of each result in Section 5.1 uses only instances of imul modulo primes that actually appear in the statement of the result (generally $\vec{m}$, as well as the various $\vec{a}$ and $\vec{b}$); the only place where we introduce a new auxiliary prime p to work modulo p is in Lemma 5.14, where $p = 2$, and we can do products modulo 2 already in V^0.

As for Subsection 5.2, all the results up to Corollary 5.25 need only instances of imul modulo $\vec{m}$ as given in the statements, and modulo the primes $\vec{a}$ introduced in Definition 5.20. Finally, the proof of Theorem 5.26 that we are actually interested in uses imul modulo $\vec{m}$ as introduced in the proof, and modulo the corresponding primes $\vec{a}$ from Definition 5.20 in order to apply the preceding results.

In order to estimate $\vec{m}$ and $\vec{a}$, let $\sum_{i<n}|X_i| \le x$. The only requirement on $\vec{m}$ was that $\vec{m} \perp 2$ and (56). Now, in view of $|2| = 2$, Theorem 3.2 ensures that it suffices to take for $\vec{m}$ all odd primes up to $(x+2)|x+2|^{17} = O\big(x\,|x|^{17}\big)$ as long as x is larger than a suitable standard constant (which we may assume w.l.o.g. as $IMUL[x]$ is trivially provable for each standard x). Going back to Definition 5.20, we have $s = O(x)$; we claim that in order to find $\vec{a}$ satisfying the requirements, it suffices to take the list of all primes below $t = O\big(s^2|s|^{17}\big)$, omit 2 and $\vec{m}$, and split it into sublists $\vec{a}_u$, $u < s$, of minimal length that satisfy (48). Since the individual primes on the list have length $O\big(|s|\big)$, this will make

$$\sum_{j<l}\big(|a_{u,j}|-1\big) \le 2s + O\big(|s|\big)$$

for each $u < s$, while

$$|2| - 1 + \sum_{i<k}\big(|m_i|-1\big) \le s,$$

thus there will be enough primes available as long as

$$\sum_{p\le t}\big(|p|-1\big) \ge 2s^2 + O\big(s\,|s|\big),$$

and Theorem 3.2 guarantees that a suitable $t = O\big(s^2|s|^{17}\big) = O\big(x^2|x|^{17}\big)$ will satisfy this. This makes $t < x^3$ for x larger than a suitable standard constant. $\square$

Lemma 8.5 *For any polynomial p, VTC^0 proves $Cyc[z,x] \to Tot^*_{\mathrm{imul}}\big[-,\min\big\{z,p(x,|z|)\big\}\big]$.*

Proof: Consider a prime $m \leq z$ such that $|m| = O\bigl(|x| + ||z||\bigr)$. As in the proof of (iii) → (ii) in Proposition 8.1, let g be an element of $(\mathbb{Z}/m\mathbb{Z})^\times$ of maximal order $t = o_m(g) < m$. By Lemma 7.6, $o_m(a) \mid t$ for all $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. We will expand $\{g\}$ to a not-too-large generating set by mimicking the proof of [14, Thm. 3.12].

Let us say that $\langle g_i : i < k\rangle$ is a *good independent sequence with exponents* $\langle t_i : i < k\rangle$ if $\sum_{i<k}|t_i| \leq 2|m|$, each t_i is a prime power $p_i^{e_i}$ where $p_i \geq x$, $g_i^{t_i} \equiv 1 \pmod m$, and

(70) $$\forall r < t\, \forall \vec{r} < \vec{t}\, \Bigl(g^r \prod_{i<k} g_i^{r_i} \equiv 1 \pmod m \implies \langle r, \vec{r}\rangle = \vec{0}\Bigr).$$

Here, the product modulo m can be evaluated using Tot^*_{pow} and $Tot^*_{\mathrm{imul}}\bigl[|m|, -\bigr]$, and the conditions on $\vec{t}$ ensure that $\vec{r}$ can be encoded by a bounded first-order quantifier (using the efficient sequence encoding scheme), hence the definition of good independent sequences is Σ^B_0.

If $\vec{g}$ is a good independent sequence with exponents $\vec{t}$, then $t_i = o_m(g_i) < m$ for each $i < k$, and the mapping
$$\varphi_{\vec{g}}(r, \vec{r}) = g^r \prod_{i<k} g_i^{t_i} \text{ rem } m \qquad (r < t, \vec{r} < \vec{t})$$
is a group homomorphism $C_t \times \prod_{i<k} C_{t_i} \to (\mathbb{Z}/m\mathbb{Z})^\times$ with a trivial kernel; as such, it is injective. Moreover, $\varphi_{\vec{g}}$ is Σ^B_0-definable, hence it exists as a set. Since $t_i \geq x$, we have $k \leq 2|m|/|x|$; it follows that the sequence $\vec{g}$ can be encoded using $O\bigl(k\,|m|\bigr) = O\bigl(|m|^2/|x|\bigr) = O\bigl(|z|\bigr)$ bits, that is, by a bounded first-order variable. Consequently, we can use bounded Σ^B_0-maximization to find a good independent sequence $\vec{g}$ such that $\sum_{i<k}|t_i|$ is maximal possible.

We claim that $\varphi_{\vec{g}}$ is surjective. Assume for contradiction that $b \notin \mathrm{im}(\varphi_{\vec{g}})$. Since $\mathrm{im}(\varphi_{\vec{g}})$ is Σ^B_0-definable, there exists a least $r > 0$ such that $b^r \in \mathrm{im}(\varphi_{\vec{g}})$. We have $r > 1$, thus r has a prime divisor p. By replacing b with $b^{r/p}$ if necessary, we may assume $r = p$. Thus, we can write
$$b^p = g^s \prod_{i<k} g_i^{s_i}$$
for some $s < t$ and $\vec{s} < \vec{t}$. We define $s' < t$, $\vec{s}' < \vec{t}$, and $b' = g^{s'} \prod_i g_i^{s'_i}$ as follows:

- Since $p \mid o_m(b) \mid t$, we have $g^{\frac{t}{p}s} \prod_i g_i^{\frac{t}{p}s_i} \equiv 1$, thus $t \mid \frac{t}{p}s$ by independence, that is, $p \mid s$. We put $s' = s/p$ so that $g^{s'p} = g^s$.
- For any $i < k$ such that $p_i \neq p$, let $s'_i = s_i p^{-1}$ rem t_i, so that $g_i^{s'_i p} \equiv g_i^{s_i}$.
- For any $i < k$ such that $p_i = p$ and $p \mid s_i$, we put $s'_i = s_i/p$ so that $g_i^{s'_i p} = g_i^{s_i}$.
- Otherwise, $s'_i = 0$.

Since $b' = \varphi_{\vec{g}}(s', \vec{s}')$, bb'^{-1} rem m is still outside $\mathrm{im}(\varphi_{\vec{g}})$, while $(bb'^{-1})^p$ is inside. Thus, we may replace b with bb'^{-1}; this ensures $s = 0$, and

(71) $$s_i \neq 0 \implies p = p_i \wedge p \nmid s_i$$

for each $i < k$. We distinguish two cases.

If $\vec{s} = \vec{0}$, then $b^p \equiv 1$. We claim that $\langle \vec{g}, b \rangle$ is a good independent sequence with exponents $\langle \vec{t}, p \rangle$, contradicting the maximality of $\sum_i |t_i|$. Since $p \mid t$, the elements b and $a = g^{t/p}$ have both order p, while b cannot be a power of a as it is outside $\mathrm{im}(\varphi_{\vec{g}})$; thus, $Cyc[z, x]$ implies $p \geq x$. The independence of $\vec{g}$ together with $b^i \notin \mathrm{im}(\varphi_{\vec{g}})$ for $0 < i < p$ implies that $\langle \vec{g}, b \rangle$ satisfies (70). This means that $\varphi_{\vec{g},b}$ is injective, hence $pt \prod_i t_i$ (which exists by Theorem 2.2) is less than m by *PHP*; in particular,

$$|p| + \sum_{i<k} |t_i| \leq 2\Big(|p| - 1 + \sum_{i<k} \big(|t_i| - 1\big)\Big) < 2|m|,$$

as required by the definition of a good independent sequence.

If $\vec{s} \neq \vec{0}$, let $i_0 < k$ be such that $s_{i_0} \neq 0$ (thus $p_{i_0} = p$ and $p \nmid s_{i_0}$ by (71)), and such that e_{i_0} is maximal possible among these. Without loss of generality, assume $i_0 = 0$. We claim that $\langle b, g_1, \dots, g_{k-1} \rangle$ is a good independent sequence with exponents $\langle pt_0, t_1, \dots, t_{k-1} \rangle$, again contradicting the maximality of $\vec{g}$. The maximality of e_0 along with (71) implies $b^{pt_0} \equiv 1$. What remains to show is that the sequence satisfies (70); the bound $|pt_0| + \sum_{i \geq 1} |t_i| \leq 2|m|$ then follows from *PHP* as above. So, assume that

$$g^r b^{r'_0} \prod_{i=1}^{k-1} g_i^{r_i} \equiv 1, \tag{72}$$

where $r < t$, $r'_0 < pt_0$, and $r_i < t_i$ for $0 < i < k$. By taking the pth power, this implies

$$g^{pr} g_0^{r'_0 s_0} \prod_{i=1}^{k-1} g_i^{pr_i + r'_0 s_i} \equiv 1,$$

hence in particular $p \mid t_0 \mid r'_0$ by the independence of $\vec{g}$, as $p \nmid s_0$. Thus, writing $r_0 = r'_0/p$, (72) can be written as

$$g^r g_0^{r_0 s_0} \prod_{i=1}^{k-1} g_i^{r_i + r_0 s_i} \equiv 1.$$

Then the independence of $\vec{g}$ gives $r = 0$, $r_0 = 0$ (using $p \nmid s_0$ and $r_0 < t_0$), and then $r_i = 0$ for all $0 < i < k$, as required.

This finishes the proof that $\varphi_{\vec{g}}$ is a bijection, thus $\{g\} \cup \{g_i : i < k\}$ generates $(\mathbb{Z}/m\mathbb{Z})^\times$. In order to save us from the trouble of dealing with exponents, let

$$X = \big\{ g^{2^j} : j < |t| \big\} \cup \big\{ g_i^{2^j} : i < k, j < |t_i| \big\};$$

then $X \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$ has size $\mathrm{card}(X) = |t| + \sum_i |t_i| = O\big(|m|\big)$, and every $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ can be written as $a = \prod Y \mathbin{\mathrm{rem}} m$ for some $Y \subseteq X$. Notice that having fixed X, we can represent Y by $\mathrm{card}(X)$ bits, and therefore by a single small number; in particular, we can Σ^B_0-define the Y_a with the least code such that $a \equiv \prod Y_a$. Then we can compute iterated products modulo m using $Tot^*_{\mathrm{imul}}\big[O\big(|m|\big), -\big]$ and Tot^*_{pow} by

$$\prod_{i<n} a_i \equiv \begin{cases} 0, & \text{if } a_i \equiv 0 \text{ for some } i < n, \\ \displaystyle\prod_{x \in X} x^{\mathrm{card}\{i<n : x \in Y_{a_i}\}}, & \text{otherwise.} \end{cases}$$

This definition provably satisfies the recurrence

$$\prod_{i<0} a_i \equiv 1,$$
$$\prod_{i<n+1} a_i \equiv a_n \prod_{i<n} a_i.$$

We have proved $Tot_{\mathrm{imul}}[-,w]$ for $w = \min\{z, p(x,|z|)\}$. In order to show $Tot^*_{\mathrm{imul}}[-,w]$, we have to deal with a sequence of iterated products modulo different $m \le w$ in parallel. As usual, it suffices to show that given m, we can Σ^B_0-define a suitable set X as above. Now, we have already seen that a good independent sequence $\vec{g}$ for m can be encoded using $O(|z|)$ bits; the corresponding exponents $\vec{t}$ are Σ^B_0-definable from $\vec{g}$ as $t_i = o_m(g_i)$, thus we can Σ^B_0-define the maximum of $\sum_i |t_i|$ among such sequences, and then Σ^B_0-define a good independent sequence with least code that achieves the maximum. Then we can define X from $\vec{g}$. □

We note that the argument in Lemma 8.5 actually shows $Cyc[z,x] \to Tot^*_{\mathrm{imul}}[-,w]$ whenever $w \le z$ and $|w|^2 \le |x|\,|y|$ for some y. However, we will only need the formulation given in Lemma 8.5 to proceed, while in the end, we will obtain full Tot^*_{imul} anyway.

We are now ready to finish the proof of the main result of this paper.

Theorem 8.6 *VTC^0 proves IMUL.*

Proof: For any fixed z, we can prove

$$x^6|z|^3 \le z \to Cyc[z,x] \tag{73}$$

by induction on x: $Cyc[z,0]$ holds vacuously, and VTC^0 proves

$$\begin{aligned} Cyc[z,x] \wedge (x+1)^6|z|^3 \le z &\to Tot^*_{\mathrm{imul}}\big[-,(x+1)^6|z|^3\big] \\ &\to IMUL\big[(x+1)^2|z|\big] \\ &\to Cyc[z,x+1] \end{aligned}$$

by Lemmas 8.3, 8.4, and 8.5.

This implies $IMUL[x]$ for all x: taking z such that $z \ge x^6|z|^3$, we have $Cyc[z,x]$ by (73), thus $Tot^*_{\mathrm{imul}}[x^3]$ by Lemma 8.5, and $IMUL[x]$ by Lemma 8.4. □

Corollary 8.7 *VTC^0 proves that $(\mathbb{Z}/m\mathbb{Z})^\times$ is cyclic for all primes m.* □

Corollary 8.8 *VTC^0 proves DIV: for every $X > 0$ and Y, there are Q and $R < X$ such that $Y = QX + R$.* □

By results of Jeřábek [15], we obtain the following consequence of Theorem 8.6 relating VTC^0 to Buss's single-sorted theories of arithmetic (see [15] for background):

Corollary 8.9 *VTC^0 proves the RSUV translations of Σ^b_0-IND and Σ^b_0-MIN.* □

Using the $RSUV$-isomorphism of VTC^0 to Δ^b_1-CR, we can formulate the results in terms of the theories of Johannsen and Pollett:

Corollary 8.10 *Δ^b_1-CR and C^0_2 prove Σ^b_0-IND, Σ^b_0-MIN, and (a suitable single-sorted formulation of) IMUL. Moreover, $C^0_2[div]$ is an extension of C^0_2 by a definition, and therefore a conservative extension.* □

We stress that in Corollary 8.10, Σ^b_0 refers to sharply bounded formulas in Buss's original language, not in the expanded language employed in [17, 18]. (In the latter language, Σ^b_0-*IND* is equivalent to PV_1, and Σ^b_0-*MIN* to T^1_2, which is strictly stronger than C^0_2 unless the polynomial hierarchy collapses to TC^0, provably in the theory.)

9 Tying up loose ends

Our arguments leading to the proof of Theorem 8.6 involved a few side results that might be interesting in their own right, but we only proved them in a minimal form sufficient to carry out the main argument. In this section, we polish them to more useful general results.

9.1 Chinese remainder reconstruction

The first side-result concerns the CRR reconstruction procedure. The statement of Theorem 5.24 gives only a loose bound on $\mathrm{Rec}(\vec{m};\vec{x})$, and involves unnecessary constraints on $\vec{m}$. These restrictions carry over to Corollary 5.25, whose statement also imposes an unnecessary bound on X.

Once we prove *IMUL* and *DIV* in VTC^0, it is not particularly difficult to improve the bounds in Theorem 5.24 and Corollary 5.25 to $X < \prod_{i<k} m_i$, and to generalize $\mathrm{Rec}(\vec{m};\vec{x})$ so that it also applies to $m_i = 2$. Alternatively, we may abandon Definition 5.20 altogether in favour of a more obvious algorithm (note that we do not require $\vec{m}$ to consist of primes):

Definition 9.1 (In VTC^0.) Given a sequence $\vec{m}$ of pairwise coprime nonzero numbers, and $\vec{x} < \vec{m}$, let

$$\mathrm{Rec}^+(\vec{m};\vec{x}) = \Big(\sum_{i<k} x_i h_i \prod_{j\neq i} m_j\Big) \operatorname{rem} \prod_{i<k} m_i,$$

where

$$h_i = \prod_{j\neq i} m_j^{-1} \operatorname{rem} m_i.$$

Theorem 9.2 *VTC^0 proves the following for any pairwise coprime sequence $\vec{m}$.*

(*i*) *For every $\vec{x} < \vec{m}$, $\mathrm{Rec}^+(\vec{m};\vec{x})$ is the unique $X < \prod_i m_i$ such that $\vec{x} = X \operatorname{rem} \vec{m}$.*

(*ii*) *For every X, $\mathrm{Rec}^+(\vec{m}; X \operatorname{rem} \vec{m}) = X \operatorname{rem} \prod_i m_i$.*

Proof:

(i): Put $M = \prod_{i<k} m_i$. It is easy to show by induction on k that if X is divisible by m_i for each $i < k$, then it is divisible by M. Thus, also $X \equiv X' \pmod{\vec{m}}$ implies $X \equiv X' \pmod{M}$.

This shows uniqueness. We have $\mathrm{Rec}^+(\vec{m};\vec{x}) < M$ by definition, and

$$h_i \prod_{j\neq i} m_j \equiv \begin{Bmatrix} 1, & i' = i \\ 0, & i' \neq i \end{Bmatrix} \pmod{m_{i'}}$$

implies $\mathrm{Rec}^+(\vec{m};\vec{x}) \equiv x_i \pmod{m_i}$.

(ii): By definition, $X' = X \text{ rem } M$ satisfies $X' < M$ and $X \equiv X' \pmod{\vec{m}}$, thus $X' = \mathrm{Rec}^+(\vec{m}; X \text{ rem } \vec{m})$ by (i). □

Remark 9.3 It is possible to generalize CRR reconstruction further to *arbitrary* sequences $\vec{m}$. First, VTC^0 can define $M = \mathrm{lcm}(\vec{m})$ as $\prod_{j<l} p_j^{e_j}$, where $\vec{p}$ is a list collecting all prime factors of $\vec{m}$, and $e_j = \max_i v_{p_j}(m_i)$. Then, VTC^0 can prove that for any $\vec{x} < \vec{m}$ which satisfies $x_i \equiv x_{i'} \pmod{\gcd(m_i, m_{i'})}$ for all $i < i' < k$, there exists a unique $X < M$ such that $\vec{x} = X \text{ rem } \vec{m}$ by applying Theorem 9.2 modulo $\langle p_j^{e_j} : j < l\rangle$. We leave the details to the reader.

9.2 Modular powering

In Theorem 7.3, we proved that $V^0 + \mathit{WPHP}$ can do powering modulo (small) primes. We will generalize it in two ways: first, we can formalize powering modulo arbitrary small nonzero numbers, and second, we will indicate how to formulate the result purely in the single-sorted theory $I\Delta_0 + \mathit{WPHP}(\Delta_0)$.

Theorem 9.4 *$V^0 + \mathit{WPHP}$ proves that for every m, $a < m$, and r, there exists an elementwise unique sequence $\langle a_i : i \leq r\rangle$ such that $a_i < m$, $a_0 \equiv 1 \pmod{m}$, and $a_{i+1} \equiv a a_i \pmod{m}$ for each i.*

Proof: Uniqueness follows by induction on i.

For existence, assume first that $m = p^e$ is a prime power. Then we can define powering in $(\mathbb{Z}/m\mathbb{Z})^\times$ in the same way as in Section 7: as already noted there, the basic method applies to arbitrary abelian groups (provided we can do products of logarithmic length, which we can here as the proof of $\mathit{Tot}^*_{\mathrm{imul}}\big[|w|, -\big]$ in Corollary 6.5 works modulo arbitrary m); we only need to be a bit more careful with applications of WPHP, as $(\mathbb{Z}/m\mathbb{Z})^\times$ no longer consists of the entire interval $[1, m-1]$. However, we may construct (as a set) a bijection between $(\mathbb{Z}/m\mathbb{Z})^\times$ and $\big[0, \varphi(m)\big)$, where $\varphi(m) = (p-1)p^{e-1}$: e.g., we can map $x < \varphi(m)$ to $p\lfloor x/(p-1)\rfloor + \big(x \text{ rem } (p-1)\big) + 1 \in (\mathbb{Z}/m\mathbb{Z})^\times$. With this in mind, we can prove Lemma 7.1 (for x coprime to m) using an instance of $\mathit{PHP}^{2\varphi(m)}_{\varphi(m)}$. The proof of Lemma 7.2 then works unchanged (making sure the x_i are coprime to m), and so does the proof of Theorem 7.3 as long as a is coprime to m. For general a, we write $a \equiv p^u \tilde{a}$ with $u \leq e$ and $\tilde{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$, and we define

$$a^i \equiv \begin{cases} 0, & ui \geq e, \\ p^{ui}\tilde{a}^i, & \text{otherwise.} \end{cases}$$

If m is not a prime power, we find its prime factorization $m = \prod_{j<k} p_j^{e_j}$. We apply the construction above in parallel to define $\langle a_{i,j} : i \leq r, j < k\rangle$ where $a_{i,j} = a^i \text{ rem } p_j^{e_j}$, and then we define $a^i \text{ rem } m$ as the unique $a_i < m$ such that $a_i \equiv a_{i,j} \pmod{p_j^{e_j}}$ for each $j < k$. (This form of the Chinese remainder theorem is provable already in V^0, cf. D'Aquino [10].) □

In order to get the result already in $I\Delta_0 + WPHP(\Delta_0)$, one way would be to chase the proofs in Sections 6 and 7 as well as of Theorem 9.4, and make sure that we can formulate everything without explicit usage of second-order objects, using only Δ_0-definable "classes". However, it is perhaps less work to infer it directly from Theorem 9.4 using the witnessing theorem for V^0 and the conservativity of V^0 over $I\Delta_0$:

Proposition 9.5 *If $V^0 \vdash \forall x\, \exists X\, \varphi(x, X)$, where $\varphi \in \Sigma_0^B$, there exists a polynomial p and a Δ_0 formula $\theta(x, u)$ such that*

$$I\Delta_0 \vdash \forall x\, \varphi\big(x, \{u < p(x) : \theta(x, u)\}\big). \tag{74}$$

Here, $\varphi\big(x, \{u < p(x) : \theta(x, u)\}\big)$ denotes the Δ_0 formula obtained from $\varphi(x, X)$ by replacing all atomic subformulas $t \in X$ with $t < p(x) \wedge \theta(x, t)$, and atomic subformulas $\alpha\big(|X|, \dots\big)$ with $\exists z \le p(x)\, \big(\alpha(z, \dots) \wedge \forall w \le p(x)\, \big(z \le w \leftrightarrow \forall u < p(x)\, (\theta(x, u) \to u < w)\big)\big)$.

The same holds for $V^0 + WPHP$ and $I\Delta_0 + WPHP(\Delta_0)$ in place of V^0 and $I\Delta_0$, respectively.

Proof: By [9, Thm. V.5.1] (which is basically Herbrand's theorem for $\overline{V^0}$), there is an $L_{\overline{V^0}}$ function symbol F such that $\overline{V^0} \vdash \forall x\, \varphi(F(x))$, and F is Σ_0^B bit-definable by the Claim in the proof of [9, V.6.5], i.e., $\overline{V^0} \vdash F(x) = \{u < p(x) : \theta(x, u)\}$ for some term p and $\theta \in \Sigma_0^B$. Thus, (74) by the conservativity of $\overline{V^0}$ over V^0 and over $I\Delta_0$.

In the presence of $WPHP$, we have $V^0 \vdash \forall x\, \exists X\, \exists n\, \big(\varphi(x, X) \vee \neg PHP_n^{2n}(X)\big)$, thus there is an $L_{\overline{V^0}}$ function $F(x) = \{u < p(x) : \theta(x, u)\}$ such that $\overline{V^0} \vdash \forall x\, \exists n\, \big(\varphi(x, F(x)) \vee \neg PHP_n^{2n}(F(x))\big)$ as above. Then $I\Delta_0 \vdash \forall x\, \exists n\, \big(\varphi(x, \{u < p(x) : \theta(x, u)\}) \vee \neg PHP_n^{2n}(\{u < p(x) : \theta(x, u)\})\big)$ by conservativity, hence $I\Delta_0 + WPHP(\Delta_0)$ proves $\forall x\, \varphi\big(x, \{u < p(x) : \theta(x, u)\}\big)$. □

Alternatively, Proposition 9.5 has an easy direct model-theoretic proof as in [9, L. V.1.10].

Corollary 9.6 *There exists a Δ_0 formula $\pi(a, r, m, b)$ such that $I\Delta_0 + WPHP(\Delta_0)$ proves*

$$\begin{gathered}
\pi(a, r, m, b) \to b < m, \\
m \neq 0 \to \exists! b\, \pi(a, r, m, b), \\
m \neq 0 \to \pi(a, 0, m, 1 \text{ rem } m), \\
\pi(a, r, m, b) \to \pi(a, r + 1, m, ab \text{ rem } m).
\end{gathered}$$

Proof: By applying Proposition 9.5 to Theorem 9.4, we obtain a Δ_0 formula $\pi'(a, r, m, i)$ that, provably in $I\Delta_0 + WPHP(\Delta_0)$, defines the bit-graph of a function $\langle a, r, m\rangle \mapsto a_r + 2^{|m|} A$, where A is a code of a sequence $\langle a_i : i \le r\rangle$ satisfying $a_0 = 1 \text{ rem } m$ and $a_{i+1} = a a_i \text{ rem } m$. We can then define $\pi(a, r, m, b)$ as $b < m \wedge \forall i < |m|\, \big(\mathrm{bit}(b, i) = 1 \leftrightarrow \pi'(a, r, m, i)\big)$. □

Remark 9.7 Using Δ_0-induction, it is easy to show in $I\Delta_0 + WPHP(\Delta_0)$ that the formula π in Corollary 9.6 is unique up to provable equivalence, and that it satisfies the Tarski high-school identities $a^{r+s} \equiv a^r a^s$, $(ab)^r \equiv a^r b^r$, and $a^{rs} \equiv (a^r)^s$ modulo m.

Since the statements in Corollary 6.5 are $\forall\Sigma_1^1$, they can be translated to $I\Delta_0$ in a similar way. Not all of these translations are genuinely interesting, though. In particular, functions with non-small integers as inputs or outputs are rather awkward to formulate, using Δ_0 formulas describing individual bits of the numbers, etc. On the other hand, when restricted to *small* numbers, the translation of $\mathit{IMUL}\big[|w|^c\big]$ (actually, the result is small only if $c = 1$, barring uninteresting products with lots of 1s) to $I\Delta_0$ is already known from [6]. Likewise, division of small numbers is trivial. Concerning imul, if $\langle a_i : i < n\rangle$ is given in $I\Delta_0$ explicitly by a sequence, we can again do $\prod_{i<n} a_i \text{ rem } m$ by the results of [6] as we can just compute $\prod_{i<n} a_i$ and reduce it modulo m, but the result is new in the more general case that $\langle a_i : i < n\rangle$ is only given by a Δ_0-definable function:

Corollary 9.8 *For every Δ_0 formula $\varphi(\vec{z}, n, a)$ and every constant c, there is a Δ_0 formula $\pi(\vec{z}, n, m, w, y)$ such that $I\Delta_0$ proves: for all $m > 0$, w, and $\vec{z}$, if $\forall n < |w|^c\, \exists! a\, \varphi(\vec{z}, n, a)$, then $\forall n \le |w|^c\, \exists! y\, \pi(\vec{z}, n, m, w, y)$, and for all $n < |w|^c$ and all y, a,*

$$\pi(\vec{z}, 0, m, w, 1 \text{ rem } m),$$
$$\pi(\vec{z}, n, m, w, y) \wedge \varphi(\vec{z}, n, a) \to \pi(\vec{z}, n+1, m, w, ya \text{ rem } m).$$

(That is, if φ with parameters $\vec{z}$ defines a function $f(n)$, then π defines a function $g(n, m)$ satisfying $g(0, m) \equiv 1 \pmod{m}$ and $g(n+1, m) \equiv g(n, m) f(n, m) \pmod{m}$ for all $n < |w|^c$.)

□

10 Conclusion

We proved that VTC^0 can formalize the Hesse, Allender, and Barrington TC^0 algorithms for integer division and iterated multiplication. While this result is hopefully interesting in its own right, on a broader note it contributes to our understanding of VTC^0 as a robust and surprisingly powerful theory, capable of adequate formalization of common TC^0-computable predicates and functions and their fundamental properties. In particular, it makes a strong case that VTC^0 is indeed the right theory corresponding to TC^0; previous results of [15] suggested that $VTC^0 + \mathit{IMUL}$ might be another viable choice, perhaps more suitable than VTC^0 itself, but results of the present paper render this distinction moot.

A possible area for further development of VTC^0 is to try and see what it can prove about approximations of analytic functions such as exp, log, trigonometric and inverse trigonometric functions. In view of bounds on primes in Section 3 and in Nguyen [22], another intriguing question is if VTC^0 can prove the prime number theorem.

On a different note, our result on formalization of a Δ_0-definition of modular exponentiation essentially relied on several instances of the weak pigeonhole principle, but it is not clear to what extent is this really necessary. We leave it as an open problem if we can we construct a well-behaved modular exponentiation function in a substantially weaker theory than $I\Delta_0 + \mathit{WPHP}(\Delta_0)$, or even in $I\Delta_0$ itself. The latter problem was first posed by Atserias [2, 3].

Acknowledgements

I am grateful to the anonymous referee for helpful comments, in particular drawing my attention to [2, 3]. The research was supported by grant 19-05497S of GA ČR. The Institute of Mathematics of the Czech Academy of Sciences is supported by RVO: 67985840.

References

[1] Tom M. Apostol, *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, Springer, 1976.

[2] Albert Atserias, *Improved bounds on the Weak Pigeonhole Principle and infinitely many primes from weaker axioms*, in: Mathematical Foundations of Computer Science 2001 (J. Sgall, A. Pultr, and P. Kolman, eds.), Lecture Notes in Computer Science vol. 2136, Springer, 2001, pp. 148–158.

[3] ———, *Improved bounds on the Weak Pigeonhole Principle and infinitely many primes from weaker axioms*, Theoretical Computer Science 295 (2003), pp. 27–39.

[4] 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.

[5] 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.

[6] Alessandro Berarducci and Paola D'Aquino, Δ_0*-complexity of the relation* $y = \prod_{i \le n} F(i)$, Annals of Pure and Applied Logic 75 (1995), no. 1–2, pp. 49–56.

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

[8] 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.

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

[10] Paola D'Aquino, *Local behaviour of the Chebyshev theorem in models of* $I\Delta_0$, Journal of Symbolic Logic 57 (1992), no. 1, pp. 12–27.

[11] Petr Hájek and Pavel Pudlák, *Metamathematics of first-order arithmetic*, Perspectives in Mathematical Logic, Springer, 1993, second edition 1998.

[12] 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.

[13] 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.

[14] Emil Jeřábek, *Abelian groups and quadratic residues in weak arithmetic*, Mathematical Logic Quarterly 56 (2010), no. 3, pp. 262–278.

[15] ———, *Open induction in a bounded arithmetic for* TC^0, Archive for Mathematical Logic 54 (2015), no. 3–4, pp. 359–394.

[16] Jan Johannsen, *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.

[17] 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.

[18] ———, *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.

[19] Sebastian Müller, *Polylogarithmic cuts in models of* $\mathbf{V}^0$, Logical Methods in Computer Science 9 (2013), no. 1, article no. 16, 16 pp.

[20] Edward Nelson, *Predicative arithmetic*, Mathematical Notes vol. 32, Princeton University Press, Princeton, 1986.

[21] V. A. Nepomnjaščij, *Rudimentary predicates and Turing calculations*, Doklady Akademii Nauk SSSR 195 (1970), no. 2, pp. 282–284 (in Russian), English translation in: Soviet Mathematics – Doklady 11 (1970), no. 6, pp. 1462–1465.

[22] Phuong Nguyen, *Bounded reverse mathematics*, Ph.D. thesis, University of Toronto, 2008.

[23] Phuong Nguyen and Stephen A. Cook, *Theories for TC^0 and other small complexity classes*, Logical Methods in Computer Science 2 (2006), no. 1, article no. 3, 39 pp.

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

[25] Jeff B. Paris and Alex J. Wilkie, *Counting Δ_0 sets*, Fundamenta Mathematicae 127 (1987), no. 1, pp. 67–76.

[26] Jeff B. Paris, Alex J. Wilkie, and Alan R. Woods, *Provability of the pigeonhole principle and the existence of infinitely many primes*, Journal of Symbolic Logic 53 (1988), no. 4, pp. 1235–1244.

[27] Alan R. Woods, *Some problems in logic and number theory, and their connections*, Ph.D. thesis, University of Manchester, 1981.

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

[29] ———, *End extensions of models of linearly bounded arithmetic*, Annals of Pure and Applied Logic 88 (1997), no. 2–3, pp. 263–277.