Collapsing modular counting in bounded arithmetic and constant depth propositional proofs

Samuel R. Buss*
Department of Mathematics
University of California, San Diego
La Jolla, CA 92093-0112, USA
sbuss@math.ucsd.edu

Leszek Aleksander Kołodziejczyk*
Institute of Mathematics
University of Warsaw
Banacha 2, 02-097 Warszawa, Poland
lak@mimuw.edu.pl

Konrad Zdanowski *
Faculty of Mathematics and Natural Sciences
Cardinal Stefan Wyszyński University
Wóycickiego 1/3, 01-938 Warszawa, Poland
k.zdanowski@uksw.edu.pl

June 19, 2013

Abstract

Jeřábek introduced fragments of bounded arithmetic which are axiomatized with weak surjective pigeonhole principles and support a robust notion of approximate counting. We extend these fragments to accommodate modular counting quantifiers. These theories can formalize and prove the relativized versions of Toda's theorem on the collapse of the polynomial hierarchy with modular counting. We introduce a version of the Paris-Wilkie translation for converting formulas and proofs of bounded arithmetic with modular counting quantifiers into constant depth propositional logic with modular counting gates. We also define Paris-Wilkie translations to Nullstellensatz and polynomial calculus refutations. As an application, we prove that constant

*The first author was supported in part by NSF grant DMS-1101228. In the preliminary stages of this work, the second and third authors were supported by grant no. N N201 382234 of the Polish Ministry of Science and Higher Education. Most of this work was carried out while the second author was visiting the University of California, San Diego, supported by Polish Ministry of Science and Higher Education programme "Mobilność Plus" with additional support from a grant from the Simons Foundation (#208717 to Sam Buss).

depth propositional proofs that use connectives AND, OR, and mod p gates, for p a prime, can be translated, with quasipolynomial increase in size, into propositional proofs containing only propositional formulas of depth three in which the top level is Boolean, the middle level consists of mod p gates, and the bottom level subformulas are small conjunctions. These results are improved to depth two by using refutations from the weak surjective pigeonhole principles.

1 Introduction

A major open problem on the frontier of research in propositional proof complexity is to prove lower bounds on the size of constant depth proofs in the language with the usual connectives $\bigwedge, \bigvee, \neg$, and a modulo p counting connective, where p is a prime. These are often called $\mathrm{AC}^0[p]$-Frege proofs; however, the present paper calls them constant depth $\mathrm{PK}_{\oplus_p}$ proofs. Constant depth proof systems can be seen as nonuniform versions of (relativized) bounded arithmetic theories, so the problem also has an arithmetic variant: to prove an interesting combinatorial independence result for the theory $T_2(\oplus_p, \alpha)$, relativized bounded arithmetic in the language with a mod p counting quantifier.

It has been suggested that this problem, in both of its variants, could be within reach of current methods. As the techniques used to obtain lower bounds for AC^0 circuits [1, 22, 23] were eventually refined to obtain lower bounds for constant depth proofs [2, 6], it should be possible — so the reasoning goes — to discover lower bounds for constant depth proofs with mod p gates by refining the known lower bound arguments for $\mathrm{AC}^0[p]$ circuits [37, 40]. However, the idea at the heart of those arguments, "approximating" small $\mathrm{AC}^0[p]$ circuits by low degree polynomials over $\mathbb{F}_p$, does not seem to mesh well with logic; in particular, the approximation operation does not commute with inference rules. For this reason and others, answers to basic questions about the strength of constant depth proof systems with mod p gates remain unknown after years of study, and it increasingly seems that these systems are just not very well understood.

Our aim in this paper is to contribute to this understanding by pointing out an important structural feature of constant depth proofs with mod p connectives: they do not form a strict hierarchy with respect to depth. A (sufficiently simple) formula with a constant depth proof involving mod p connectives has a quasipolynomially larger proof in which all formulas have depth at most 3, with $\bigwedge$ as the topmost connective and mod p connectives applied to "small" conjunctions of literals below that. At the cost of intro-

ducing additional axioms, the proof can be simplified even further, almost to the point of being formalizable in polylog degree Polynomial Calculus.

Results on the possibility of depth reduction in this context are neither totally unexpected nor altogether new. It is known that $\mathrm{AC}^0[p]$ *circuits* can be simulated by $\mathrm{AC}^0[p]$ circuits of fixed constant depth and quasipolynomial size [3]; this follows from the relativized version of Toda's theorem [43]. Moreover, Maciel and Pitassi [31] showed that every constant depth *proof* with mod p gates translates into a quasipolynomially larger "flat" proof of depth 3. However, formulas in the flat proofs of [31] involve an exact counting (threshold) connective, so in general they cannot even be expressed, let alone proved, in constant depth with counting modulo p. Maciel and Pitassi's results also apply to proof systems with mod p^k gates. Yao [45] and Beigel-Tarui [11] showed that, for any $m > 2$, circuits with mod m gates can be collapsed to depth two circuits with exact counting gates at the top level. However, Maciel and Pitassi's results are not known to hold for constant depth proofs with mod m gates for m not a prime power.

To avoid the use of exact counting connectives in propositional proof systems, we employ the machinery of "approximate counting in bounded arithmetic", developed by Jeřábek. The papers [26, 27] introduced two fragments of bounded arithmetic and showed that they support reasonably well-behaved notions of approximate cardinality. The weaker of the two fragments is the theory PV_1+sWPHP(PV_1), also called APC_1 by [17]. Here, sWPHP is the "surjective weak pigeonhole principle", and PV_1 denotes both a class of function symbols representing polytime functions and a theory in which these functions are well-behaved. APC_1 is able to determine the size of any polynomial time subset X of 2^n to within an error $\epsilon 2^n$ for any $\epsilon > 0$ polynomially related to $1/n$. The second theory is $T^1_2 + \mathrm{sWPHP}(\mathrm{PV}_2)$, also called APC_2. Since this is essentially APC_1 relativized to Σ^b_1 (that is, NP) properties, whatever APC_1 can do with polytime, APC_2 can do with P^{NP}. More significantly, APC_2 is also more-or-less able to define the approximate size of polytime $X \subseteq 2^n$ to within an error of $\epsilon|X|$, rather than $\epsilon 2^n$.

Jeřábek's theories can be smoothly relativized to $\oplus_p\mathrm{P}$ properties, yielding the theories $\mathrm{APC}_1^{\oplus_p\mathrm{P}}$ and $\mathrm{APC}_2^{\oplus_p\mathrm{P}}$. We show that $\mathrm{APC}_2^{\oplus_p\mathrm{P}}$ is actually equal in strength to all of $T_2(\oplus_p)$. Essentially, the reason for this is that $\mathrm{APC}_2^{\oplus_p\mathrm{P}}$ proves Toda's theorem, in the form that the polynomial hierarchy with a mod p quantifier collapses to $\mathrm{BP} \cdot \oplus_p\mathrm{P}$.

This collapse result in arithmetic is reflected at the level of propositional logic because of the well-known Paris-Wilkie translation [33], which maps proofs in arithmetic into uniform families of quasipolynomial size con-

stant depth propositional proofs. It is a folklore observation that the Paris-Wilkie translation can also be used with modular counting quantifiers added to the language of arithmetic, and modular counting gates allowed in the propositional fomulas. To make this observation precise, we define theories $\mathrm{PV}_1^{\oplus_p\mathrm{P}}, T_2^{1,\oplus_p\mathrm{P}}, T_2^{2,\oplus_p\mathrm{P}}, \ldots$, which are relativizations of the more usual $\mathrm{PV}_1, T_2^1, T_2^2, \ldots$ to $\oplus_p\mathrm{P}$ predicates, and then define propositional systems corresponding to them in the Paris-Wilkie translation. A side effect of our treatment is that for some variants of the translation, we obtain correspondences which seem to be slightly stronger than the ones known from the literature, even in the setting without modular counting.

$\mathrm{APC}_2^{\oplus_p\mathrm{P}}$ is a subtheory of $T_2^{3,\oplus_p\mathrm{P}}$. Therefore, the collapse of $T_2(\oplus_p)$ down to $\mathrm{APC}_2^{\oplus_p\mathrm{P}}$ translates into the collapse of constant depth propositional proof systems with mod p connectives down to the system corresponding to $T_2^{3,\oplus_p\mathrm{P}}$, namely to the depth 3 system described above. Working directly with $\mathrm{APC}_2^{\oplus_p\mathrm{P}}$ rather than $T_2^{3,\oplus_p\mathrm{P}}$ lets us push the collapse down even further, but this requires allowing additional propositional axioms corresponding to sWPHP.

The implications of our results are unclear. On one hand, they can be viewed as a potential step on the way to lower bounds for constant depth proofs with mod p gates. On the other hand, perhaps the right interpretation is more pessimistic: since we know that the search for those lower bounds involves serious difficulties, the new results show that the difficulties appear already at a seemingly very low level, "just above" systems for which lower bounds have been known for long time.

The outline of the paper is as follows. Section 2 has a preliminary character and splits into two parts. The first part, Section 2.1, discusses propositional proof systems, defining both the general constant depth systems $\mathrm{PK}_{\oplus_p}$ with unbounded fanin boolean and modular counting connectives, and the systems PCK_p^i where modular counting connectives may be applied only to sets of small conjunctions. It also defines propositional proof systems that use polynomials over $\mathbb{F}_p$. Section 2.2 reviews the background concepts needed from bounded arithmetic, and defines arithmetic theories that incorporate modular counting quantifiers C_p^k. Section 3 concerns the Paris-Wilkie translation between arithmetic and propositional proofs, modified so as to take into account the availability of counting modulo p. It includes some sharpened Paris-Wilkie translations that improve slightly on what was known even for systems without modular counting quantifiers. Section 4.1 contains a discussion of Jeřábek's framework for approximate counting, along with some useful reformulations. Section 4.2 formalizes the

Valiant-Vazirani theorem in the approximate counting theory $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$; then Section 4.3 formalizes Toda's theorem in the same theory, and thus proves the collapse of $T_2(\oplus_p)$ to $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$. Section 5 establishes one of the main results, namely the above-discussed collapse of the constant depth propositional systems with mod p connectives. Finally, Section 6 discusses what remains of the hierarchy of constant depth arithmetic systems (and proof systems) with mod p gates: we discuss the best lower bounds known for these systems. This includes an independence result for the pigeonhole principle PHP_a^{a+1} which is proved using lower bounds for Nullstellensatz proofs combined with Paris-Wilkie translations. We conclude with some speculations on the difficulty of finding further independence results for stronger fragments of arithmetic.

Historical note: The first results for this paper were obtained by the second and third authors, who proved the core results of sections 4.2 and 4.3 about formalizability of the Valiant-Vazirani and Toda theorems. The remaining research was subsequently carried out by the first and second authors during 2011-2012 in San Diego.

We are indebted to the referee for extensive insightful comments and suggestions which helped us make significant improvements to the paper.

2 Preliminaries

2.1 Propositional proof systems

We work with a number of different constant depth propositional proof systems that incorporate unbounded fanin modular counting gates $\oplus_p$. This subsection first defines Boolean versions of these proof systems, and establishes that valid cedents containing decision trees have simple proofs in these systems. We then review the Nullstellensatz and Polynomial Calculus systems that use polynomials over $\mathbb{F}_p$, and finally define proof systems that combine (low-degree) $\mathbb{F}_p$ polynomials with unbounded fanin AND's and OR's.

Let p be a fixed prime. We will define the propositional proof systems $\mathrm{PK}_{\oplus_p}$ and PCK_p^i. Propositional formulas are formed from literals x and $\overline{x}$, combined with unbounded fanin $\bigwedge$'s and $\bigvee$'s, and unbounded fanin $\oplus_p$ connectives. The propositional variables x range over the values *True* and *False*. The negation of a literal x is $\overline{x}$, and negation is involutive so $\overline{\overline{x}}$ is x. The input to an unbounded fanin connective is a multiset of formulas. We allow $\bigwedge$ and $\bigvee$ to have the empty set of inputs, in which case they denote the constant $\top$ or $\bot$ for *True* or *False*, respectively.

Our proof systems are Tait-style systems; namely, the lines in a proof are *cedents*. Our convention is that a cedent is a set of formulas (not a multiset or a sequence). The intended meaning of a cedent is that at least one member of the cedent has value *True*. The logical initial cedents for literals are the cedents $x, \overline{x}$, where x is a propositional variable. The rules of inference are:

$$\frac{\Gamma}{\Gamma, \Delta}\ \text{Weakening} \qquad \frac{\Gamma, \varphi \qquad \Gamma, \overline{\varphi}}{\Gamma}\ \text{Cut}$$

$$\frac{\Gamma, \varphi_{i_0}}{\Gamma, \bigvee_{i\in I}\varphi_i}\ \bigvee \qquad \frac{\Gamma, \varphi_i \qquad \text{for all } i \in I}{\Gamma, \bigwedge_{i\in I}\varphi_i}\ \bigwedge$$

where $i_0 \in I$.

To simplify the handling of negation, we add $2p$ many $\oplus_p$ connectives: First, for $k \in [p] := \{0, 1, \ldots, p-1\}$, there is a connective $\oplus_p^k$ with the intended meaning that the number of inputs with value *True* is congruent to k mod p. The input to $\oplus_p^k$ is a non-empty finite multiset of formulas, written as $\oplus_p^k\{\varphi_1, \ldots, \varphi_\ell\}$. Second, for each $k \in [p]$, there is a connective $\bar{\oplus}_p^k$ which represents the complement (the negation) of $\oplus_p^k$. (We shall discuss below how the connectives $\bar{\oplus}_p^k$ can be removed using Fermat's little theorem. Of course, one could simply replace $\bar{\oplus}_p^k$ by $\bigvee_{\ell\neq k} \oplus_p^\ell$, but that has the undesirable effect of increasing depth.) The complement of $\oplus_p^k\Phi$ is denoted $\overline{\oplus_p^k\Phi}$, and is the formula $\bar{\oplus}_p^k\Phi$. Complementation is involutive, so the complement of $\bar{\oplus}_p^k\Phi$ is $\oplus_p^k\Phi$. We sometimes write $\oplus_p^k$ or $\bar{\oplus}_p^k$ when k might be $\geq p$. In this case, we mean $\oplus_p^{k \bmod p}$ or $\bar{\oplus}_p^{k \bmod p}$.

There are five types of initial cedents that apply to the $\oplus_p$ connectives:

$$\varphi, \oplus_p^0\{\varphi\} \qquad \overline{\varphi}, \oplus_p^1\{\varphi\}$$

$$\oplus_p^k\Phi, \bar{\oplus}_p^k\Phi \qquad \bar{\oplus}_p^k\Phi, \bar{\oplus}_p^\ell\Phi, \text{ for } k \neq \ell$$

$$\bar{\oplus}_p^k\Phi, \bar{\oplus}_p^\ell\Psi, \oplus_p^{k+\ell}(\Phi \cup \Psi)$$

Definition The propositional proof system $\mathrm{PK}_{\oplus_p}$ has formulas formed from variables and negated variables and the connectives $\bigwedge$, $\bigvee$, $\oplus_p^k$, and $\bar{\oplus}_p^k$. Its initial sequents are the logical initial sequents for literals and the five $\oplus_p$ axioms. Its rules of inference are weakening, cut, and the $\bigwedge$ and $\bigvee$ rules.

We are interested in two different kinds of constant depth subsystems of $\mathrm{PK}_{\oplus_p}$. The *depth* of a $\mathrm{PK}_{\oplus_p}$ formula is the number of alternations of

$\bigwedge$'s, $\bigvee$'s, and $\oplus_p$ connectives along any branch in the formula (viewing the formula as a tree). *Constant depth* $\mathrm{PK}_{\oplus_p}$ *proofs* have an $O(1)$ bound on the depth of formulas.

The second kind of constant depth $\mathrm{PK}_{\oplus_p}$ proofs, denoted PCK_p^i, allows $\oplus_p$ connectives to be applied only to conjunctions of literals. This restriction will be useful for the Paris-Wilkie translations of the systems $T_2^{i,\oplus_p\mathrm{P}}$ defined in the next subsection.

An $\oplus_p^-$ formula is defined to be a formula of the form $\oplus_p^k\Phi$ or $\bar{\oplus}_p^k\Phi$, where every member of Φ is a conjunction of literals. The $\Sigma_i(\oplus_p^-)$ and $\Pi_i(\oplus_p^-)$ formulas are defined inductively. $\Sigma_0(\oplus_p^-)$ and $\Pi_0(\oplus_p^-)$ formulas are defined to be $\oplus_p^-$ formulas. A $\Pi_{i+1}(\oplus_p^-)$ formula is either a $\Sigma_i(\oplus_p^-)$ formula or a formula $\bigwedge\Phi$ where Φ is a multiset of $\Sigma_i(\oplus_p^-)$ formulas. The $\Sigma_{i+1}(\oplus_p^-)$ formulas are defined dually.

Note that this means a $\Sigma_0(\oplus_p^-)$ and $\Pi_0(\oplus_p^-)$ formula contains exactly one occurrence of a $\oplus_p^k$ or $\bar{\oplus}_p^k$ connective: for instance, to express a literal x as a $\Sigma_0(\oplus_p^-)$ formula, we write it as $\oplus_p^1\bigwedge\{x\}$, with the $\oplus_p^1$ having a single argument, which is a conjunction of size 1.

Definition Let $p \geq 2$ and $i \geq 0$. The propositional proof system PCK_p^i is the subsystem of $\mathrm{PK}_{\oplus_p}$ restricted to use cedents in which all formulas are literals, conjunctions or disjunctions of literals, or $\Pi_i(\oplus_p^-)$ or $\Sigma_i(\oplus_p^-)$ formulas.

Definition The *size* of a proof is the number of symbols in the proof. The *height* of a proof is the maximum number of inferences along any path in the proof from the final line to an initial line.

The size, but not the height, of a proof can depend on whether the proof is dag-like or tree-like. Following Krajíček [28], the Paris-Wilkie translations use a notion of "Σ-size" for the systems PCK_p^i which restricts both the size of a proof and the sizes of inputs to $\oplus_p$ gates.

Definition A formula φ has Σ-size S provided that φ has size $\leq S$ and that any conjunction or disjunction of literals which appears as a subformula of φ contains $\leq \log S$ many literals. In particular, this means that if $\oplus_p^k\Phi$ or $\bar{\oplus}_p^k\Phi$ is a is a subformula of φ, then the set Φ contains conjunctions of $\leq \log S$ many literals. A PCK_p^i proof P has Σ-*size* S provided that P has size $\leq S$ and every formula in P has Σ-size S.

The next lemma establishes some simple properties about provability with $\oplus_p$ connectives.

Definition If φ is a conjunction of the form $\bigwedge\Theta$ then Θ is the (multi)set of *conjuncts* of φ and is denoted $cnjct(\varphi)$. Let Φ and Ψ be multisets of conjunctions. Then $\Phi\times\Psi$ is the multiset $\{\bigwedge(cnjct(\varphi)\cup cnjct(\psi)) : \varphi\in\Phi, \psi\in\Psi\}$. We write Φ^j for $\Phi\times\Phi\times\cdots\times\Phi$ with j occurrences of Φ.

Lemma 1 *Let Φ and Ψ be multisets of conjunctions of literals and have Σ-size S. The following cedents have tree-like PCK_p^0 proofs which have Σ-size $S^{O(1)}$, height $(\log S)^{O(1)}$, and $O(1)$ many formulas in each cedent.*

(a) $\oplus_p^0\Phi, \oplus_p^1\Phi, \ldots, \oplus_p^{p-1}\Phi$.

(b) $\bar{\oplus}_p^k\Phi, \bar{\oplus}_p^\ell\Psi, \oplus_p^{k\cdot\ell}\Phi\times\Psi$.

(c) $\bar{\oplus}_p^0\Phi, \oplus_p^0\Phi^{p-1}$.

(d) $\bar{\oplus}_p^k\Phi, \oplus_p^1\Phi^{p-1}$, *for* $k\neq 0$.

(e) $\oplus_p^0\Phi^{p-1}, \oplus_p^1\Phi^{p-1}$.

(f) $\bar{\oplus}_p^0\Phi^{p-1}, \oplus_p^0\Phi$.

Proof (Sketch.) The proof of a cedent (a) is constructed inductively on the cardinality M of Φ. If Φ is a singleton, it follows from the first two $\oplus_p$ axioms, along with a cut and a weakening. Otherwise $M>1$, and let Φ_1 be some $\lfloor M/2\rfloor$ element subset of Φ, and Φ_2 be $\Phi\setminus\Phi_1$. Using the cedents of the form (a) for Φ_1 and Φ_2 in place of Φ, and cuts against instances of the fifth $\oplus_p$ axiom, we obtain cedent (a) for Φ.

Now consider a cedent (b). If both Φ and Ψ are singletons, then (b) follows from the first four $\oplus_p$ axioms. Otherwise, suppose w.l.o.g. that Φ has cardinality >1. Define Φ_1 and Φ_2 as before. By (a) and the fourth $\oplus_p$ axiom, there are unique values k, k_1, and k_2 such that $\oplus_p^k\Phi$, $\oplus_p^{k_1}\Phi_1$, and $\oplus_p^{k_2}\Phi_2$ hold. By the fourth and fifth $\oplus_p$ axioms, we also have $k_i+k_2=k \pmod p$. Arguing inductively, the two cedents (b) hold: $\bar{\oplus}_p^{k_j}\Phi_j, \bar{\oplus}_p^\ell\Psi, \oplus_p^{k_j\cdot\ell}\Phi_j\times\Psi$ for $j=0,1$. Finally, since $\Phi\times\Psi=(\Phi_1\times\Psi)\cup(\Phi_2\times\Psi)$, another use of the fifth $\oplus_p$ axiom gives the desired cedent (b).

Cedent (c) is an immediate consequence of (b). Cedent (d) is a form of Fermat's little theorem. It follows by $p-2$ uses of (b) and the truth of Fermat's little theorem. Cedent (e) now follows easily from (a), (c), and (d). Cedent (f) likewise follows easily. □

Note that parts (c), (e), and (f) of the lemma show that $\bar{\oplus}_p^0\Phi$ is equivalent to $\oplus_p^1\Phi^{p-1}$. Since $\bar{\oplus}_p^k\Phi$ can be expressed as $\bar{\oplus}_p^0\Phi'$ where Φ' is Φ plus $p-k$

copies of $\top$, this means that the connectives $\bar{\oplus}_p^k$ can be eliminated in favor of uses of $\oplus_p^0$ without significantly affecting the complexity of formulas.

The next lemma lets us express a conjunction $\bigwedge_{j=1}^k \oplus_p^1 \Phi_j$ with a single $\oplus_p^1$ connective. It is an immediate consequence of Lemma 1.

Lemma 2 *Let each Φ_j be a multiset of conjunctions of literals. The following cedents are PCK_p^0-provable.*

(a) $\bar{\oplus}_p^1(\Phi_1^{p-1} \times \cdots \times \Phi_k^{p-1}), \oplus_p^1 \Phi_j^{p-1}$.

(b) $\bar{\oplus}_p^1 \Phi_1^{p-1}, \ldots, \bar{\oplus}_p^1 \Phi_k^{p-1}, \oplus_p^1(\Phi_1^{p-1} \times \cdots \times \Phi_k^{p-1})$.

If each Φ_i has Σ-size S and $k = (\log S)^{O(1)}$, then the PCK_p^0 proofs have Σ-size quasipolynomial in S, have polylogarithmic height, and have $\leq k + O(1)$ many formulas in each cedent.

To understand Lemma 2, note that (a) states that $\oplus_p^1(\Phi_1^{p-1} \times \cdots \times \Phi_k^{p-1})$ implies each of $\oplus_p^1 \Phi_j^{p-1}$; and (b) states that conversely the k many latter formulas jointly imply the former formula. A similar construction allows a single $\oplus_p^1$ formula to express the disjunction of k many $\oplus_p^1$ formulas.

To help the Paris-Wilkie translation go smoothly, we need some results about Boolean decision trees.

Definition A *Boolean decision tree* T is a labeled binary tree. Each internal node is labeled with a literal x, and has one outgoing edge labeled with x and the other outgoing edge labeled with $\overline{x}$. The leaves of the tree are labeled with *True* or *False*. The decision tree T defines a Boolean function in the obvious way. The negation of T is denoted $\overline{T}$ and is obtained by interchanging the labels *True* and *False*.

A path in T is associated with the conjunction of the literals on the edges of the path. The *dt-cedent* expressing T is denoted $\mathsf{cd}(T)$ and is the set containing exactly these conjunctions associated with paths in T that end with the label *True*.

Definition A formula of the form $\oplus_p^k \mathsf{cd}(T)$ or $\bar{\oplus}_p^k \mathsf{cd}(T)$, where T is a decision tree, is called an *$\oplus$-dt formula*.

Lemma 3 *Let Γ be a cedent containing as formulas (only) literals and $\oplus$-dt formulas. Suppose Γ is valid for all truth assignments. Also suppose Γ has ℓ formulas with $\ell \leq S$, and each formula has Σ-size S. Then Γ has a tree-like PCK_p^0 proof P of Σ-size $2^{O(\ell^2 \log S)} = S^{O(\ell^2)}$ in which all formulas are either literals or $\oplus_p^-$ formulas. The height of P is polynomial in ℓ and $\log S$. In addition, the cedents in the proof P contain only $\ell + O(1)$ many formulas.*

Proof This is obvious if there are no $\oplus$-dt formulas in Γ. Otherwise, we use induction on the number of literals in Γ plus the sum of the heights of the Boolean decision trees for the $\oplus$-dt formulas in Γ.

First, suppose there is a literal $\overline{x}$ appearing as a formula in Γ. If Γ also contains the formula x, then we are done. And, if x does not appear anywhere else in Γ, then we can just omit $\overline{x}$ from Γ without affecting its validity. (In other words, the literal $\overline{x}$ is to be introduced by a weakening inference.) So suppose, x appears in some $\oplus$-dt formula $\oplus_p^k\Psi$ in Γ; namely, Γ has the form $\Gamma', \overline{x}, \oplus_p^k\Psi$. (The case of $\bar{\oplus}_p^k\Psi$ is similar.) Ψ is a set of paths from a Boolean decision tree T. We partition these paths according to whether they query x and, if so, whether they include x positively or negatively, in order to express the set Ψ as $(\{x\} \times \Psi_x) \cup (\{\overline{x}\} \times \Psi_{\overline{x}}) \cup \Psi'$ where the literal x does not appear in Ψ_x, $\Psi_{\overline{x}}$ or Ψ'. Strictly speaking, $\{x\}$ actually means the multiset containing the singleton conjunction $\wedge\{x\}$, and similarly for $\{\overline{x}\}$. The multisets Ψ_x, $\Psi_{\overline{x}}$ and Ψ' are still dt-cedents from decision trees: this allows possibly being the empty multiset (denoting the Boolean value *False*), or the singleton multiset containing the empty conjunction (i.e., the constant $\top$). Lemma 1 and the first, second and fifth $\oplus_p$ axioms give a proof of $\overline{x}, \bar{\oplus}_p^k(\Psi_x \cup \Psi'), \oplus_p^k\Psi$. With this, a cut inference allows Γ to be inferred from $\Gamma', \overline{x}, \oplus_p^k(\Psi_x \cup \Psi')$. Note that $\oplus_p^k(\Psi_x \cup \Psi')$ is still a $\oplus$-dt formula. Repeat this construction for each $\oplus$-dt formula $\oplus_p^k\Psi$ in Γ that contains x or $\overline{x}$. The result is a cedent in which x occurs only once in the cedent, namely as the formula $\overline{x}$. As discussed above, the formula $\overline{x}$ can be now removed without affecting the validity of the cedent.

Now, suppose that no literal appears as a formula in Γ, and let $\oplus_p^k\mathsf{cd}(T)$ be a formula in Γ. (The case $\bar{\oplus}_p^k\mathsf{cd}(T)$ is similar.) Let x be the variable labeling the root of the decision tree associated with T. We have that $\mathsf{cd}(T)$ is equal to $(\{x\} \times \Phi_x) \cup (\{\overline{x}\} \times \Phi_{\overline{x}})$, where the multisets Φ_x and $\Phi_{\overline{x}}$ are, as before, dt-cedents from a decision tree. By Lemma 1(a,b) and using the first, second and fifth $\oplus_p$ axioms, we can derive Γ immediately from the pair of cedents

$$\Gamma', \overline{x}, \oplus_p^k\Phi_x \qquad\qquad \Gamma', x, \oplus_p^k\Phi_{\overline{x}}$$

with $\Gamma' = \Gamma \setminus \{\oplus_p^k\mathsf{cd}(T)\}$. These two cedents are valid since Γ is. This has reduced the sums of the heights of the decision trees by at least one, and the literals x and $\overline{x}$ can be handled by the construction of the previous paragraph.

The desired bounds on the size of the proof P follow from the constructions. □

As an immediate consequence of Lemma 3, we obtain proofs of the cedent $\oplus_p^0\mathsf{cd}(T), \oplus_p^1\mathsf{cd}(T)$. Another corollary is that we can infer Γ from the two cedents $\Gamma, \oplus_p^1\mathsf{cd}(T)$ and $\Gamma, \oplus_p^1\mathsf{cd}(\overline{T})$. To prove this, note that $\bar{\oplus}_p^1\mathsf{cd}(T), \bar{\oplus}_p^1\mathsf{cd}(\overline{T})$ is valid, and use Lemma 3 and two cuts.

We next define algebraic proof systems for propositional logic. Algebraic proof sytems use polynomials over $\mathbb{F}_p$ for p a fixed prime, with variables x that have value 0 or 1. A polynomial f over $\mathbb{F}_p$ is identified with the assertion that f has value 0. Since $x^2 = x$ holds for 0/1-valued x, we shall replace every polynomial with its multilinearization; namely, any occurrence of x^i with $i > 1$ is replaced with just x. For the sake of definiteness, we assume that a multilinear polynomial is syntactically represented by the list of its non-zero monomials, where a monomial is given by the set of variables appearing in it together with a coefficient.

The Nullstellensatz system and the Polynomial Calculus (PC) are refutation systems that work with polynomials over $\mathbb{F}_p$, see [5, 19, 16]. Let $\mathcal{F} = \{f_k : k \in [m]\}$ be a set of multilinear polynomials, called *initial polynomials*, in variables x_j. A Nullstellensatz refutation of $\mathcal{F}$ consists of polynomials g_k such that

$$g_0 f_0 + g_1 f_1 + \cdots + g_{m-1} f_{m-1} \;=\; 1$$

where the left hand of the side denotes (as always) the multilinearization of the indicated polynomial, and the equals sign denotes equality as polynomials. This refutation shows that $\{f_k\}_k$ is *unsatisfiable*; namely, that it is impossible to set the variables x_j to 0/1 values so that the polynomials f_k all evaluate to 0 over $\mathbb{F}_p$. The *degree* of the refutation is the maximum of the degrees of $g_k f_k$; its *size* is the total number of occurrences of variables in g_k and f_k.

The Polynomial Calculus system gives a more general kind of refutation. The lines of a Polynomial Calculus refutation are multilinear polynomials over $\mathbb{F}_p$. The initial polynomials must be members of $\mathcal{F}$. The two rules of inference for the Polynomial Calculus are:

$$\frac{f}{fg}\ \text{Product}\ (\cdot) \qquad \frac{f \qquad g}{f+g}\ \text{Sum}\ (+)$$

As a reminder, fg denotes the multilinearization of fg.

The final line in a Polynomial Calculus refutation contains the constant polynomial 1; this serves as a refutation of $\mathcal{F}$. The *degree* of a refutation is equal to the maximum degree of any line in the refutation; the *size* of a refutation is the number of symbols in it.

We next define the Tait-style system $\mathrm{PCK}_{\mathbb{F}_p}$, and its subsystems $\mathrm{PCK}^i_{\mathbb{F}_p}$, in which formulas can combine multilinear $\mathbb{F}_p$ polynomials with unbounded fanin Boolean connectives $\bigwedge$ and $\bigvee$. The lines of a $\mathrm{PCK}_{\mathbb{F}_p}$ proof are cedents whose members are multilinear polynomials or Boolean combinations of multilinear polynomials. For instance, the intended interpretation of the cedent

$$f_1, f_2 \wedge f_3$$

is that either $f_1 = 0$ or $f_2 = f_3 = 0$. The only Boolean connectives are unbounded fanin $\bigwedge$ and $\bigvee$.

There is no connective for negation in $\mathrm{PCK}_{\mathbb{F}_p}$. The negation $\overline{f}$ of a polynomial f is defined by letting $\overline{f}$ equal the multilinearization of the polynomial $\prod_{k=1}^{p-1}(f-k)$. Since we are working over $\mathbb{F}_p$, the polynomial $\overline{f}$ has value 0 or 1 depending on whether f has non-zero value or value 0, respectively.[1] The negation of a formula $\bigvee_k \varphi_k$ or $\bigwedge_k \varphi_k$ is denoted $\overline{\bigvee_k \varphi_k}$ or $\overline{\bigwedge_k \varphi_k}$, and is defined to equal $\bigwedge_k \overline{\varphi_k}$ or $\bigvee_k \overline{\varphi_k}$, respectively.

The initial cedents for a $\mathrm{PCK}_{\mathbb{F}_p}$ or $\mathrm{PCK}^i_{\mathbb{F}_p}$ proof are the *axiom mod p* polynomials:

$$f, f{+}1, f{+}2, \cdots, f{+}(p{-}1).$$

The rules of inference are the product and sum rules above, plus the four rules cut, weakening, $\bigwedge$, and $\bigvee$.

Definition Let p be a prime. The *propositional Polynomial Calculus proof system*, $\mathrm{PCK}_{\mathbb{F}_p}$, is a Tait-style proof system with formulas formed from multilinear polynomials over $\mathbb{F}_p$ using conjunctions and disjunctions. The initial axioms are the axioms mod p, and the rules of inference are all six rules product, sum, cut, weakening, $\bigwedge$, and $\bigvee$ (with the product and sum rules modified in the obvious way to allow side formulas).

Note that $\mathrm{PCK}_{\mathbb{F}_p}$ is a proof system, not a refutation system. The "PC" in the name can stand for either "Polynomial Calculus", or even more relevantly, for "propositional counting" (for counting mod p). The "K" comes from Gentzen's notation "LK", with "K" standing for "Kalkül".

The Paris-Wilkie translations for subtheories of bounded arithmetic with modular counting quantifiers C^k_p will yield subsystems of $\mathrm{PCK}_{\mathbb{F}_p}$ with bounded alternations of $\bigwedge$ and $\bigvee$ connectives. For this, we inductively define the $\Pi_i(\mathbb{F}_p)$ and $\Sigma_i(\mathbb{F}_p)$ formulas as follows: A $\Pi_0(\mathbb{F}_p)$ formula or $\Sigma_0(\mathbb{F}_p)$ formula

[1] It is perhaps disconcerting that complementation is not involutive, that is, that $\overline{\overline{f}}$ is not generally the same as f. Nonetheless, this does not substantially affect the power of the propositional proof systems.

is an $\mathbb{F}_p$ polynomial. A $\Pi_{i+1}(\mathbb{F}_p)$ formula is either a $\Sigma_i(\mathbb{F}_p)$ formula or a formula $\bigwedge\Phi$ where Φ is a multiset of $\Sigma_i(\mathbb{F}_p)$ formulas. The $\Sigma_{i+1}(\mathbb{F}_p)$ formulas are defined dually.

Definition Let $i \geq 0$. A $\mathrm{PCK}^i_{\mathbb{F}_p}$ proof is a $\mathrm{PCK}_{\mathbb{F}_p}$ proof in which every formula is a $\Sigma_i(\mathbb{F}_p)$ or $\Pi_i(\mathbb{F}_p)$ formula.

Although the systems $\mathrm{PCK}^i_{\mathbb{F}_p}$ use $\mathbb{F}_p$ polynomials, they are effectively equivalent for our purposes to the PCK^i_p systems. Consider a $\oplus^-_p$ Boolean formula φ of the form $\oplus^k_p\Phi$ where Φ is a multiset of conjunctions of literals. As is well-known, this can be transformed into an $\mathbb{F}_p$ polynomial f which has value 0 exactly when φ is true. That is, if variables are given 0/1 values, with 0 corresponding to the Boolean value *False* and 1 to *True*, then then condition $f = 0$ is equivalent to φ having value *True*. The polynomial f is formed by rewriting the conjunctions of literals in Φ as products of literals, taking the sums of these products and subtracting k, replacing negatively occurring literals x with $(1 - x)$, and using the distributive law to express the result as a sum of monomials. The negated formula $\bar{\oplus}^k_p\Phi$ then translates to $(1 - f^{p-1})$, which also can be written a sum of monomials by applying the distributive law. Clearly, the degree of f is bounded by the maximum size of the conjunctions in Φ. (The number of monomials in f can be exponentially larger.) With this construction, any $\Pi_i(\oplus^-_p)$ formula φ is equivalent to a $\Pi_i(\mathbb{F}_p)$ formula, denoted $\varphi^{\mathbb{F}_p}$. (A converse equivalence holds as well.)

The Paris-Wilkie translations in Theorem 11 will yield $\mathrm{PCK}^i_{\mathbb{F}_p}$ proofs with quasipolynomial size and polylogarithmic degree; these quantities are measured with Σ-size:

Definition A $\mathrm{PCK}^i_{\mathbb{F}_p}$ proof has Σ-*size* S provided it has size $\leq S$ and every polynomial in the proof has degree less than $\log S$.

We next prove an analogue of Lemma 3 for $\mathrm{PCK}^i_{\mathbb{F}_p}$ proofs. The situation is simpler for polynomials than for Boolean decision trees.

Definition Let $f_1, \ldots, f_k, g$ be multilinear $\mathbb{F}_p$ polynomials. Then $f_1, \ldots, f_k \vDash g$ means that, for any assignment of 0/1 values to variables, if every f_j evaluates to zero, then also g evaluates to zero.

Lemma 4 *Suppose $f_1, \ldots, f_k \vDash g$. Then there are multilinear polynomials $h_1, \ldots, h_k$ such that g is equal to the multilinearization of $h_1f_1 + h_2f_2 + \cdots + h_kf_k$. Furthermore, if d bounds the degrees of g and the f_j's, then each h_j has degree $\leq (p-1)kd$.*

Proof By $f_1, \ldots, f_k \vDash g$, the polynomial $g(1-f_1^{p-1})(1-f_2^{p-1})\cdots(1-f_k^{p-1})$ always evaluates to zero for 0/1 inputs, and hence its multilinearization is the zero polynomial. Thus, setting $h_\ell = g f_\ell^{p-2}(1-f_{\ell+1}^{p-1})\cdots(1-f_k^{p-1})$ satisfies the conditions of the lemma. Note that the degree of h_ℓ is bounded by $(p-1)kd$. □

2.2 Theories of modular counting and approximate counting

We describe below how to extend the theories S_2^i and T_2^i of bounded arithmetic to incorporate new bounded quantifiers C_p^k for counting modulo p. We also augment the theories APC_1 and APC_2 to include counting modulo p. In later sections, we will give Paris-Wilkie translations for these theories, and prove that the hierarchy of theories collapses. We presume the reader is familiar with bounded arithmetic, including the formula classes Σ_i^b and Π_i^b and the theories S_2^i and T_2^i; for these, consult [12, 15, 29]. We will usually use *strict* Σ_i^b and Π_i^b formulas, denoted $\hat{\Sigma}_i^b$ and $\hat{\Pi}_i^b$ for short. $\hat{\Sigma}_i^b$ and $\hat{\Pi}_i^b$ formulas must be in prenex form, and can have up to i alternating universal and existential blocks of quantifiers in front of a sharply bounded subformula. (Unlike some definitions of "strict", we allow the sharply bounded subformula to not be in prenex form and to contain multiple sharply bounded quantifiers.) It is known that Σ_i^b and Π_i^b formulas are equivalent to $\hat{\Sigma}_i^b$ and $\hat{\Pi}_i^b$ formulas (resp.) and that induction may be restricted to strict formulas without affecting the strength of the theories S_2^i and T_2^i [25, 36].

The usual bounded quantifiers for bounded arithmetic have the form $(\exists x \le t)$ and $(\forall x \le t)$. For a fixed prime $p \ge 2$, we augment the language of bounded arithmetic to include mod p counting quantifiers C_p^k with $k \in [p]$. The intended meaning of $(\mathsf{C}_p^k x \le t)A(x)$ is that the number of values $x \le t$ for which A is true is congruent to k mod p. Note there may be variables other than x which appear free in $A(x)$. These new quantifiers have the following axioms. To avoid cluttering superscripts with extra "mod p"s, we adopt the convention that C_p^k means $\mathsf{C}_p^{k \bmod p}$.

$$A(0) \to (\mathsf{C}_p^1 x \le 0)A(x) \qquad \neg A(0) \to (\mathsf{C}_p^0 x \le 0)A(x)$$
$$A(t+1) \wedge (\mathsf{C}_p^k x \le t)A(x) \to (\mathsf{C}_p^{k+1} x \le t{+}1)A(x)$$
$$\neg A(t+1) \wedge (\mathsf{C}_p^k x \le t)A(x) \to (\mathsf{C}_p^k x \le t{+}1)A(x)$$
$$\neg[(\mathsf{C}_p^k x \le t)A(x) \wedge (\mathsf{C}_p^\ell x \le t)A(x)] \qquad \text{for } k \not\equiv \ell \pmod p \ .$$

The final axiom states that the number of true $A(x)$'s, $x \le t$, cannot be equal to both k and ℓ mod p. Our theories will admit induction (IND) for all permitted bounded formulas with a C_p^k quantifier as outermost symbol,

and can prove that $\bigvee_{k=0}^{p-1}(\mathsf{C}_p^k x \le t)A(x)$ holds. In addition, induction allows basic facts about the C_p^k quantifiers to be proved such as

$$(\forall x \le s)(A(x+t+1) \leftrightarrow B(x)) \wedge (\mathsf{C}_p^k x \le t)A(x) \wedge (\mathsf{C}_p^\ell x \le s)B(x) \qquad (1)$$
$$\rightarrow (\mathsf{C}_p^{k+\ell} x \le t+s+1)A(x).$$

By convention, the first-order language contains the usual set of PV_1 function and predicate symbols, used to denote polynomial time functions and relations. (This set of symbols is more commonly called simply PV, but we use "PV_1" to distinguish it from "PV_2"). When there is a second-order predicate (an oracle), denoted α, the language includes all $\mathrm{PV}_1(\alpha)$ functions and predicates; namely all polynomial time functions and predicates that have oracle access to α.

A *bounded formula* is a formula in which all quantifiers are bounded. Note that C_p^k quantifiers are considered to be bounded. For languages that contain the C_p^k quantifiers, the notation $\Sigma_\infty^b(\oplus_p)$ denotes the set of bounded formulas.

Definition The theory $T_2(\oplus_p)$, also denoted $S_2(\oplus_p)$, is the theory axiomatized by the defining axioms for PV_1 symbols and the axioms for C_p^k quantifiers appearing in front of $\Sigma_\infty^b(\oplus_p)$ formulas, and with induction for all $\Sigma_\infty^b(\oplus_p)$ formulas. The theory $T_2(\oplus_p, \alpha)$ is defined similarly with $\mathrm{PV}_1(\alpha)$ instead of PV_1.

The next definition gives theories where the modular counting quantifiers are restricted to counting polynomial time sets.

Definition A $\oplus_p\mathrm{P}$ formula is a formula which is either atomic, or of the form $(\mathsf{C}_p^k x \le t)A(x)$ where A is Σ_0^b. Since the language includes all PV_1 symbols, A can represent any PV_1 predicate. We define $\Sigma_0^{b,\oplus_p\mathrm{P}} = \Pi_0^{b,\oplus_p\mathrm{P}}$ to be the class of formulas obtained as the closure of $\oplus_p\mathrm{P}$ formulas under Boolean connectives $\wedge$, $\vee$ and $\neg$ and under sharply bounded existential and universal quantifiers. For $i \ge 1$, the strict formula classes $\hat{\Sigma}_i^{b,\oplus_p\mathrm{P}}$ and $\hat{\Pi}_i^{b,\oplus_p\mathrm{P}}$ are defined in the usual way by counting alternations of bounded (universal and existential) quantifiers.

The classes $\oplus_p\mathrm{P}(\alpha)$ and $\hat{\Sigma}_i^{b,\oplus_p\mathrm{P}}(\alpha)$ and $\hat{\Pi}_i^{b,\oplus_p\mathrm{P}}(\alpha)$ are defined similarly, but over the language $\mathrm{PV}_1(\alpha)$ instead of PV_1.

The theory $T_2^{i,\oplus_p\mathrm{P}}$ is the theory of bounded arithmetic axiomatized by the axioms for PV_1 symbols, the C_p^k axioms for Σ_0^b formulas $A(x)$, and $\Sigma_i^{b,\oplus_p\mathrm{P}}$-IND. The theory $S_2^{i,\oplus_p\mathrm{P}}$ is defined similarly, but with $\hat{\Sigma}_i^{b,\oplus_p\mathrm{P}}$-PIND

in place of $\hat{\Sigma}_i^{b,\oplus_p \mathrm{P}}$-IND. The theories $T_2^{i,\oplus_p \mathrm{P}}(\alpha)$ and $S_2^{i,\oplus_p \mathrm{P}}(\alpha)$ are defined analogously with the $\mathrm{PV}_1(\alpha)$ axioms, the C_p^k axioms for $\Sigma_0^b(\alpha)$ formulas $A(x)$ formulas, and induction for $\hat{\Sigma}_i^{b,\oplus_p \mathrm{P}}(\alpha)$ formulas.

The following lemma, which is never invoked explicitly, lists some typical examples of simple modular counting arguments that can be carried out at the lowest level of the $T_2^{i,\oplus_p \mathrm{P}}$ hierarchy. Such arguments are often tacitly used in Section 4.

Lemma 5 *Let $A(x)$ and $B(x)$ be Σ_0^b formulas. $T_2^{0,\oplus_p \mathrm{P}}$ proves the formula* (1)*, as well as*

$$(\forall x{\leq}z)[\neg(A(x) \wedge B(x))] \rightarrow \qquad (2)$$
$$[(\mathsf{C}_p^k x \leq z)(A(x) \vee B(x)) \leftrightarrow \bigvee_{\ell+\ell'=k} ((\mathsf{C}_p^\ell x{\leq}z)A(x) \wedge (\mathsf{C}_p^{\ell'} x{\leq}z)B(x))].$$

For f a PV_1 function, $T_2^{0,\oplus_p \mathrm{P}}$ proves that if f is a bijection between $\{x \leq z : A(x)\}$ and $\{y \leq w : B(y)\}$, then

$$(\mathsf{C}_p^k x{\leq}z)A(x) \leftrightarrow (\mathsf{C}_p^k y{\leq}w)B(y). \qquad (3)$$

The proof of (2) is by induction on z. Note that (1) is a special case of (2); they both concern counting disjoint unions. To prove (3), argue by induction on $v \leq w$ that the sets $\{y \leq v : B(y)\}$ and $\{x \leq z : A(x) \wedge f(x) \leq v\}$ have the same number of elements modulo p. The inductive step makes use of (2).

For p a prime, Theorem 22 will show that $T_2^{3,\oplus_p \mathrm{P}}$, and even $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$, has the same logical strength as all of $T_2(\oplus_p)$. That is to say, we have a collapse of the hierarchy of theories in this setting. Thus, we will work extensively with $T_2^{3,\oplus_p \mathrm{P}}$, and its subtheory $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$.

In many cases, it is important to know that standard witnessing, provability, and conservativity results in bounded arithmetic also hold after relativization to $\oplus_p \mathrm{P}$. To see why this is true, it is convenient to think in terms of a special "modular counting oracle", σ_p, instead of the mod p counting quantifiers.

As usual, let $p \geq 2$ be fixed. The intended meaning of σ_p is that $\sigma_p(k, \ulcorner C \urcorner, z)$ is true precisely when $\ulcorner C \urcorner$ is the Gödel number of a Boolean circuit C that has n binary inputs and the number of inputs $x \in \{0,1\}^n$ such that $x \leq z$ and $C(x)$ is true is congruent to k mod p. By the (proof of the) P-completeness of the circuit value problem, the oracle σ_p can be

used to compute the truth value of any $\oplus_p$P formula. The axioms for the modular counting oracle σ_p are obtained in the obvious way from the five initial sequents for the C_p^k quantifers.

The oracle σ_p can also be used in the presence of other oracle predicates α. In this situation, the circuit C is an "oracle circuit" that has access to the oracle α in the form of unbounded fanin "α-gates". This allows σ_p to compute the truth value of an arbitrary $\oplus_p\mathrm{P}(\alpha)$ formula. Note, however, that C does not have oracle access to σ_p.

Definition The theory T_2^{i,σ_p} is defined by extending T_2^i to include a relation symbol for the oracle σ_p that counts the number of satisfying assignments of Boolean circuits modulo p. In addition, the language of T_2^{i,σ_p} includes the language $\mathrm{PV}_1(\sigma_p)$, namely it includes symbols for all function and predicate symbols which are polynomial time relative to σ_p. T_2^{i,σ_p} is axiomatized with axioms for σ_p, with the defining equations for all $\mathrm{PV}_1(\sigma_p)$ functions and relations, and with induction for $\Sigma_i^b(\sigma_p)$ formulas.

The theory $T_2^{i,\sigma_p}(\alpha)$ is defined similarly, except that σ_p counts the number of satisfying assignments for Boolean circuits that include α-gates. $T_2^{i,\sigma_p}(\alpha)$ uses the language $\mathrm{PV}_1(\sigma_p,\alpha)$ and has induction for $\Sigma_i^b(\sigma_p,\alpha)$ formulas.

We claim that T_2^{i,σ_p} has the same logical and expressive strength as $T_2^{i,\oplus_p\mathrm{P}}$. This claim is proved in two stages. First, since $T_2^{i,\oplus_p\mathrm{P}}$ allows the C_p^k quantifiers only on polynomial time predicates and since any polynomial time property can be equivalently expressed by a polynomial size circuit, C_p^k quantifiers can be replaced by uses of the σ_p predicate. Conversely, every σ_p predicate can be expressed in terms of a C_p^k quantifier. Thus, $T_2^{i,\oplus_p\mathrm{P}}$ is essentially a notational variant of a theory defined like T_2^{i,σ_p} except that its language contains only PV_1 symbols as opposed to $\mathrm{PV}_1(\sigma_p)$ symbols. We temporarily call this theory $T_2^{i,\sigma_p\mathrm{P}}$.

Second, we claim that $T_2^{i,\sigma_p\mathrm{P}}$ is strong enough to Σ_1^b-define all functions in $\mathrm{PV}_1(\sigma_p)$. For $i \geq 1$, this holds by [13] which showed T_2^1 can Σ_1^b-define all polynomial time computable functions. For $i = 0$, Jeřábek [25] showed that, if the language contains the MSP function, then T_2^0 can Σ_1^b-define all polynomial time computable functions, and use them freely in induction axioms. This construction also works relative to oracles, and thus $T_2^{i,\sigma_p\mathrm{P}}$ can Σ_1^b-define all $\mathrm{PV}_1(\sigma_p)$ functions, and use them in induction axioms. Therefore, adding all $\mathrm{PV}_1(\sigma_p)$ functions and relations to the language yields a conservative extension, which happens to be T_2^{i,σ_p}.

The definition of T_2^{i,σ_p} also works relative to an oracle α, and therefore $T_2^{i,\sigma_p}(\alpha)$ is similarly conservative over $T_2^{i,\oplus_p\mathrm{P}}(\alpha)$.

Standard witnessing, provability, and conservativity results concerning the theories T_2^i are known to relativize to an uninterpreted oracle predicate. It is straightforward to deduce that they also relativize to the modular counting oracle σ_p. (The precise argument involves Parikh's Theorem and the fact that negations of the defining axioms for σ_p are $\exists\Sigma_0^b(\sigma_p)$.) The correspondence between $T_2^{i,\oplus_p\mathrm{P}}$ and T_2^{i,σ_p} means that all these results can also be relativized to $\oplus_p\mathrm{P}$ and $\oplus_p\mathrm{P}(\alpha)$ formulas. Below, this observation will be sometimes invoked, and at other times tacitly used.

The theories as defined above do not allow nesting of modular counting operations. Namely, $S_2^{i,\oplus_p\mathrm{P}}$ and $T_2^{i,\oplus_p\mathrm{P}}$ do not allow nesting of C_p^k quantifiers. And, in S_2^{i,σ_p} and T_2^{i,σ_p}, the modular counting oracle σ_p cannot be applied to circuits that have σ_p gates. The next theorem shows that these restrictions cause no loss of expressive power. We write $\mathrm{P}^{\oplus_p\mathrm{P}}$ to denote the predicates which are computable in polynomial time with access to an oracle for $\oplus_p\mathrm{P}$ predicates (or, equivalently, to the oracle σ_p). Then $\oplus_p\mathrm{P}^{\oplus_p\mathrm{P}}$ denotes the set of predicates defined by

$$R(y) \iff (\mathsf{C}_p^k u \le y)A(y,u), \tag{4}$$

where $A(y,u)$ is a $\mathrm{P}^{\oplus_p\mathrm{P}}$ predicate. (There may be extra parameter variables in addition to u and y.)

Theorem 6 *Suppose p is a prime. $\oplus_p\mathrm{P}^{\oplus_p\mathrm{P}}$ is contained in $\oplus_p\mathrm{P}$.*

Proof We first prove the theorem for the simpler case of $p = 2$. Let R be defined as in (4). Let $n = |y|$. The polynomial time algorithm for $A(y,u)$ can be assumed to make exactly $p(n)$ queries to σ_p for some polynomial p, and w.l.o.g. each query has the form $\sigma_p(0, \ulcorner C \urcorner, z(y))$, where $z = z(y)$ depends only on y, is polynomially bounded, and is an even number. Since z is even, there are an odd number of $x \le z$ which make C true and an even number that make C false, or vice-versa.

We form a polynomial time predicate $B(v)$ and a term $t(y)$ so that

$$R(y) \iff (\mathsf{C}_p^k v \le t(y))B(y,v). \tag{5}$$

The predicate B is computed by the following algorithm. It first checks whether $v = \langle u, z_1, \ldots, z_{p(n)}\rangle$ with $u \le y$ and each $z_j \le z$. (The term $t(y)$ is chosen large enough to upper bound all such values v.) If v is not of this

form, $B(v, y)$ rejects. Otherwise, B simulates the polynomial time algorithm for $A(y, u)$. When the simulation reaches the j-th query made by A, namely a query to $\sigma_p(0, \ulcorner C_j \urcorner, z(y))$, then B evaluates the circuit $C_j(z_j)$. If $C_j(z_j)$ evaluates to true, then B continues simulating A as if the σ_p query returned *False*. Otherwise, $C_j(z_j)$ evaluates to false, and B continues simulating A as if the σ_p query returned *True*.

It is not hard to check that the definition of B makes the equivalence (5) hold. Specifically, for the j-th query there are an odd number of values z_j that correspond to B simulating the correct execution of A, and an even number that correspond to B simulating an incorrect execution of A. This means that, for each value of u, there are an odd number of values for v for which B simulates the correct execution of A, but each possible incorrect execution of A is simulated for an even number of values for v.

That completes the $p = 2$ case of the proof. A similar proof works for primes $p > 2$, using the construction of Fermat's little theorem. Namely, we can assume without loss of generality that any query made by A has the form $\sigma_p(0, \ulcorner C \urcorner, z)$ with $z \equiv 0 \bmod p$, and that the number of $x \leq z$ such that $C(x)$ is true is equal to either 0 or 1 mod p. This can be done as follows: Inputs to σ_p are restricted to have the form $z = (z_0 + 1)^{p-1} - 1$ where z_0 is a multiple of p. The circuit C encodes the value of z_0 and a circuit C_0, and an input x to C is interpreted as $x = \langle x_1, \ldots, x_{p-1} \rangle$. Then C accepts x iff each $x_j \leq z_0$ and is accepted by the circuit C_0. We leave the details to the reader. □

Corollary 7 *Suppose p is a prime. Any formula formed from sharply bounded universal and existential quantifiers, C_p^k quantifiers, Boolean connectives, and* PV_1 *functions and predicates can be expressed as a $\oplus_p\mathrm{P}$ predicate. The same holds relative to a second-order oracle α.*

Since our language for bounded arithmetic includes all polynomial time functions and predicates, the first-order theory T_2^0 is the same as the theory often denoted PV_1, a well-known conservative extension of Cook's equational theory PV [20] to first-order logic.

We let $\mathrm{PV}_1^{\oplus_p\mathrm{P}}$ and $\mathrm{PV}_1^{\oplus_p\mathrm{P}}(\alpha)$ denote the theories T_2^{0,σ_p} and $T_2^{0,\sigma_p}(\alpha)$. That is, the languages of these theories include symbols for all functions and relations in $\mathrm{P}^{\oplus_p\mathrm{P}}$ or $\mathrm{P}^{\oplus_p\mathrm{P}}(\alpha)$, respectively. It is straightforward to show that the proofs of Theorem 6 and Corollary 7 can be formalized in $\mathrm{PV}_1^{\oplus_p\mathrm{P}}$. It follows that the strengths of the theories $T_2^{i,\oplus_p\mathrm{P}}$, T_2^{i,σ_p}, $T_2^{i,\oplus_p\mathrm{P}}(\alpha)$ and $T_2^{i,\sigma_p}(\alpha)$ would be essentially unchanged if they allowed C_p^k quantifiers to be nested, or σ_p to apply to circuits with σ_p gates.

Theories for approximate counting and modular counting Jeřábek [26, 27] defined two fragments of T_2^3 based on the surjective weak pigeonhole principle, and showed they can define coherent notions of *approximate* counting. These two theories were named APC_1 and APC_2 in [17], and defined as

$$\mathrm{APC}_1 \ := \ \mathrm{PV}_1 + \mathrm{sWPHP}(\mathrm{PV}_1)$$

and

$$\mathrm{APC}_2 \ := \ T_2^1 + \mathrm{sWPHP}(\mathrm{PV}_2),$$

where in this definition, PV_1 denotes both the set of PV_1 functions and the theory axiomatized by the defining axioms for PV_1 functions and relations, and where PV_2 denotes the set of functions which are computable in polynomial time relative to an NP oracle. The axiom scheme $\mathrm{sWPHP}(\mathcal{F})$ means the set of axioms expressing the surjective weak pigeonhole principle

$$(\forall x)(\forall y)[x > 0 \to (\exists v \leq x(|y|+1))(\forall u \leq x|y|)(f(u) \neq v)]$$

for any $f \in \mathcal{F}$.

We will work with extended versions of these two theories,

$$\mathrm{APC}_1^{\oplus_p\mathrm{P}} \ := \ \mathrm{PV}_1^{\oplus_p\mathrm{P}} + \mathrm{sWPHP}(\mathrm{PV}_1^{\oplus_p\mathrm{P}})$$

and

$$\mathrm{APC}_2^{\oplus_p\mathrm{P}} \ := \ T_2^{1,\oplus_p\mathrm{P}} + \mathrm{sWPHP}(\mathrm{PV}_2^{\oplus_p\mathrm{P}}),$$

where $\mathrm{PV}_2^{\oplus_p\mathrm{P}}$ means functions that can be computed in polynomial time relative to $\mathrm{NP}^{\oplus_p\mathrm{P}}$.

These theories can be relativized with the addition of an oracle α. The relativized theory $\mathrm{APC}_1^{\oplus_p\mathrm{P}}(\alpha)$ is defined as $\mathrm{PV}_1^{\oplus_p\mathrm{P}}(\alpha)+\mathrm{sWPHP}(\mathrm{PV}_1^{\oplus_p\mathrm{P}}(\alpha))$. The theory $\mathrm{APC}_1^{\oplus_p\mathrm{P}}(\alpha)$ is $T_2^{1,\oplus_p\mathrm{P}}(\alpha) + \mathrm{sWPHP}(\mathrm{PV}_2^{\oplus_p\mathrm{P}}(\alpha))$.

3 Paris-Wilkie translations

The Paris-Wilkie translation is a method for converting proofs in bounded arithmetic into constant depth propositional proofs. Theorem 8 states several versions of this for the systems $T_2^{i,\oplus_p\mathrm{P}}(\alpha)$, translating into quasipolynomial Σ-size $\mathrm{PCK}_p^{i'}$ proofs, where i' will equal $i-2$, $i-1$, or i. Theorems 11 and 12 give translations to the systems $\mathrm{PCK}_{\mathbb{F}_p}^{i'}$, as well as translations from $T_2^{0,\oplus_p\mathrm{P}}(\alpha) = \mathrm{PV}_1^{\oplus_p\mathrm{P}}(\alpha)$ and from $T_2^{1,\oplus_p\mathrm{P}}(\alpha)$ into Nullstellensatz and Polynomial Calculus proofs, respectively.

The core constructions for the Paris-Wilkie translation are well known (see [34, 29, 14]), but we restate them below for completeness. One novelty is that we work with mod p quantifiers and $\oplus_p^k$ gates. In addition, parts (d) and (e) of Theorem 8 are new; and analogous theorems hold also for the usual theories of bounded arithmetic with no modular counting quantifiers. Our inspiration for parts (d), (e), and especially (f) came from ideas we first heard from Neil Thapen [personal communication] about converting PLS algorithms for $\Sigma_1^b(\alpha)$ consequences of $T_2^1(\alpha)$ into dag-like narrow resolution proofs.

For $\psi(x_1, \ldots, x_\ell)$ a (strict) bounded formula, and for integers $n_1, \ldots, n_\ell$, the Paris-Wilkie propositional translation $[\![\psi]\!]_{n_1,\ldots,n_\ell}$ is defined inductively on the complexity of ψ. The propositional variables of $[\![\psi]\!]_{\vec{n}}$ are variables x_j for $j \in \mathbb{N}$ and are intended to denote the truth value of $\alpha(j)$.

For $\psi \in \hat{\Sigma}_0^{b,\oplus_p \mathrm{P}}(\alpha)$, namely with all Boolean quantifiers sharply bounded, $[\![\psi]\!]_{\vec{n}}$ will be a $\oplus$-dt formula. This $\oplus$-dt formula $[\![\psi]\!]_{\vec{n}}$ is formed by using the algorithm implicit in Corollary 7. That corollary states that φ is equivalent to a $\oplus_p \mathrm{P}$ predicate, namely, to a formula of the form $(\mathsf{C}_p^0 u \leq r(\vec{x}))\delta(\vec{x}, u)$ where δ is polynomial time computable. Given fixed values $\vec{n}, m$ for $\vec{x}, y$, the truth value of $\delta(\vec{n}, m)$ can be expressed as a decision tree $[\![\delta(\vec{x}, u)]\!]_{\vec{n},m}$ that queries values of $\alpha(j)$. The C_p^0 quantifier is then replaced by the $\oplus_p^0$ connective which has as inputs the set Φ of conjunctions of literals which correspond to the accepting paths of the decision trees $[\![\delta(\vec{x}, u)]\!]_{\vec{n},m}$ for $0 \leq m \leq r(\vec{n})$. Let $n = \max\{n_1, \ldots, n_\ell\}$. The predicate δ has runtime polynomially bounded in terms of $|n| \approx \log n$, so the size of each conjunction in Φ is $(\log n)^{O(1)}$. Likewise, the total size of the set Φ is quasipolynomially bounded in terms of n.

The Paris-Wilkie translation extends to $\hat{\Sigma}_i^{b,\oplus_p \mathrm{P}}(\alpha)$ formulas ψ for $i > 0$ by translating (non-sharply) bounded quantifiers to unbounded fanin $\bigvee$'s or $\bigwedge$'s. If ψ has the form $(\exists u \leq r(\vec{x}))\delta(\vec{x}, u)$, then $[\![\psi]\!]_{\vec{n}}$ is defined to equal $\bigvee_{m=0}^{r(\vec{n})} [\![\delta]\!]_{\vec{n},m}$. Bounded universal quantifiers are handled similarly with a $\bigwedge$.

Theorem 8 fixes $i \geq 0$ and $j \geq 1$, and assumes that $T_2^{i,\oplus_p \mathrm{P}}(\alpha)$ proves a strict $\Sigma_j^{b,\oplus_p \mathrm{P}}(\alpha)$ formula

$$\varphi(x) \ := \ (\exists y \leq t(x))\eta(x, y).$$

We will further assume w.l.o.g. that every quantifier in φ, both sharply bounded and non-sharply bounded, has the form $(Qx \leq r(x))$ for $r(x)$ a PV_1 term which has x as its only variable. Note especially that the terms $r(x)$ do not depend on α. When $j > 1$, $\eta(x, y)$ has the form $(\forall z \leq s(x))\xi(x, y, z)$,

so

$$\varphi(x) \ := \ (\exists y \leq t(x))(\forall z \leq s(x))\xi(x, y, z).$$

Thus, η is a $\hat{\Pi}^{b,\oplus_p \mathrm{P}}_{j-1}(\alpha)$ formula, and, when defined, ξ is a $\hat{\Sigma}^{b,\oplus_p \mathrm{P}}_{j-2}(\alpha)$ formula.

Theorem 8 uses three different types of Paris-Wilkie translations of $\varphi(x)$:

(1) The most direct version of the Paris-Wilkie translation gives PCK^i_p proofs of $[\![\varphi]\!]_n$.

(2) For the second type of Paris-Wilkie translation, let H_n be the set of formulas $\overline{[\![\eta]\!]_{n,m}}$, for $0 \leq m \leq t(n)$. In this case, the Paris-Wilkie translation gives a $\mathrm{PCK}^{i'}_p$ refutation of H_n. Here, i' will equal either $i-1$ or i.

(3) For the third type of translation, let Ξ_n be the set of the $t(n)+1$ many cedents of the form

$$\overline{[\![\xi]\!]_{n,m,0}}, \ \overline{[\![\xi]\!]_{n,m,1}}, \ \ldots, \ \overline{[\![\xi]\!]_{n,m,s(n)}} \tag{6}$$

where $0 \leq m \leq t(n)$. Note each cedent (6) contains $s(n)+1$ formulas. In this case, the Paris-Wilkie translation gives a $\mathrm{PCK}^{i'}_p$ refutation of Ξ_n, where i' equals either $i-2$ or $i-1$.

Theorem 8 *Let $i \geq 0$ and $j \geq 1$. Suppose $\varphi(x) \in \hat{\Sigma}^{b,\oplus_p \mathrm{P}}_j(\alpha)$ and $T^{i,\oplus_p \mathrm{P}}_2(\alpha) \vdash (\forall x)\varphi(x)$. Let η, ξ, H_n and Ξ_n be as above.*

(a) *Suppose $j = i \geq 1$. For $n \geq 0$, the formula $[\![\varphi]\!]_n$ has a tree-like PCK^i_p proof P with Σ-size quasipolynomial in n and height polylogarithmic in n such that each cedent in P contains $O(1)$ formulas.*

(b) *Suppose $j = i \geq 1$. For $n \geq 0$, the set of cedents H_n has a tree-like PCK^{i-1}_p refutation P such that the Σ-size of P is quasipolynomial in n.*

(c) *Suppose $j = i \geq 2$. For $n \geq 0$, the set of cedents Ξ_n has a dag-like PCK^{i-2}_p refutation P such that the Σ-size of P is quasipolynomial in n.*

(d) *Suppose $j = i+1 \geq 1$. For $n \geq 0$, the set of cedents H_n has a tree-like PCK^i_p refutation P such that the Σ-size of P is quasipolynomial in n, the height of P is polylogarithmic in n, and each cedent in P has polylogarithmically many formulas.*

(e) *Suppose $j = i + 1 \geq 2$. For $n \geq 0$, the set of cedents Ξ_n has a tree-like* PCK_p^{i-1} *refutation P such that the Σ-size of P is quasipolynomial in n.*

(f) *Suppose $j = i \geq 1$. For $n \geq 0$, the set of cedents H_n has a dag-like* PCK_p^{i-1} *refutation P such that the Σ-size of P is quasipolynomial in n and such that each cedent in P contains polylogarithmically many formulas.*

Proof The proof of (a) is the standard kind of argument used for a Paris-Wilkie translation. We nonetheless present a proof sketch to illustrate what is unique to our setting. Let Q be a $T_2^{i,\oplus_p\mathrm{P}}(\alpha)$ proof of $\varphi(c)$ where c is the only free variable in $\varphi(c)$. By free-cut elimination, cf. [9], we may assume that Q contains only $\hat{\Sigma}_j^{b,\oplus_p\mathrm{P}}(\alpha)$ and $\hat{\Pi}_j^{b,\oplus_p\mathrm{P}}(\alpha)$ formulas. Without loss of generality, Q is in free-variable normal form, every free variable a in Q is bounded explicitly by a term $t_a(c)$ with the formula $a > t_a(c)$ present in every cedent in which a appears, and every quantifier $(Qx \leq r(c))$ in Q has bound $r(c)$ which is a PV_1 term that has c as its only variable (see [12]).

We shall prove that, for any cedent Γ in Q with free variables $c, a_1, \ldots, a_\ell$, and every choice of values $n \geq 0$ and $m_i \leq t_{a_i}(n)$, there is a tree-like PCK_p^i proof of the cedent $[\![\Gamma]\!]_{n,\vec{m}}$ of Σ-size quasipolynomial in n and height polylogarithmic in n, with $O(1)$ many formulas per cedent. The proof is by induction on the number of cedents in Q, and splits into cases based on the last inference of Q. The initial cedents of Q contain $O(1)$ many $\Sigma_0^{b,\oplus_p\mathrm{P}}(\alpha)$ formulas. The Paris-Wilkie translation of an initial cedent is valid and contains $O(1)$ many $\oplus$-dt formulas; thus, by Lemma 3, it has a tree-like PCK_p^0 proof of quasipolynomial Σ-size, polylogarithmic height, and $O(1)$ many formulas in each cedent.

The cases of $\wedge$, $\vee$, and sharply bounded quantifier inferences are essentially trivial, because these inferences have a $\Sigma_0^{b,\oplus_p\mathrm{P}}(\alpha)$ formula as their principal formula. For example, consider a $\wedge$ inference in Q:

$$\frac{\Gamma, A \qquad \Gamma, B}{\Gamma, A \wedge B}$$

Taking the translation of these formulas under the Paris-Wilkie translation gives an "inference" of the form

$$\frac{[\![\Gamma]\!]_{n,\vec{m}}, [\![A]\!]_{n,\vec{m}} \qquad [\![\Gamma]\!]_{n,\vec{m}}, [\![B]\!]_{n,\vec{m}}}{[\![\Gamma]\!]_{n,\vec{m}}, [\![A \wedge B]\!]_{n,\vec{m}}}$$

By Lemma 3, since $[\![A]\!]_{n,\vec{m}}$, $[\![B]\!]_{n,\vec{m}}$ and $[\![A \wedge B]\!]_{n,\vec{m}}$ are $\oplus$-dt formulas, the cedent

$$\overline{[\![A]\!]_{n,\vec{m}}},\ \overline{[\![B]\!]_{n,\vec{m}}},\ [\![A \wedge B]\!]_{n,\vec{m}}$$

has a quasipolynomial Σ-size, tree-like, polylogarithmic height proof with $O(1)$ many formulas in each cedent. Using two cuts allows the displayed inference to be inferred.

The cases of an $\vee$ inference, C^k_p axioms, axioms for $\mathrm{PV}_1(\alpha)$ functions and relations, or sharply bounded $\exists$ inferences are handled similarly. The argument for a sharply bounded $\forall$ inference is a little more complicated. Suppose that Q ends with the inference

$$\frac{\Gamma, a_0 > |r(c)|, A(a_0)}{\Gamma, (\forall v \leq |r(c)|)A(v)}$$

where the eigenvariable a_0 appears only as indicated. Note that the formulas $[\![a_0 > |r(c)|]\!]_{n,m_0,\vec{m}}$ are just the constant $\bot$ for all $m_0 \leq |r(n)|$. Thus, we wish to derive the propositional inference

$$\frac{[\![\Gamma]\!]_{n,\vec{m}}, [\![A(b)]\!]_{n,0,\vec{m}} \quad \cdots \quad [\![\Gamma]\!]_{n,\vec{m}}, [\![A(b)]\!]_{n,|r(n)|,\vec{m}}}{[\![\Gamma]\!]_{n,\vec{m}}, [\![(\forall v \leq |r(c)|)A(v)]\!]_{n,\vec{m}}} \tag{7}$$

Note there are $|r(n)| + 1$ many hypotheses in this inference.

To derive (7), we use Lemma 3 to give proofs of the cedents

$$\overline{[\![A(b)]\!]_{n,0,\vec{m}}},\ [\![(\forall v \leq b)A(v)]\!]_{n,0,\vec{m}}$$

and

$$\overline{[\![(\forall v \leq b)A(v)]\!]_{n,\ell,\vec{m}}},\ \overline{[\![A(b)]\!]_{n,\ell+1,\vec{m}}},\ [\![(\forall v \leq b)A(v)]\!]_{n,\ell+1,\vec{m}}$$

for $\ell < |r(n)|$. (To apply Lemma 3 in this way, we are effectively treating the quantifier $(\forall v \leq b)$ as being sharply bounded; this is OK since $\ell < |r(n)|$.) These sequents combine with cuts to derive (7).

Suppose that Q ends with an induction inference

$$\frac{\Gamma, \overline{A(d)}, A(d+1)}{\Gamma, \overline{A(0)}, A(s)}$$

Arguing similarly as on pages 80-81 of [12], we may assume w.l.o.g. that the term $s = s(c, \vec{a})$ is a pure PV_1 term and does not involve the oracle α. Let $m_0 = s(n, \vec{m})$. The induction hypothesis gives propositional proofs of the m_0 many cedents $[\![\Gamma]\!]_{n,\vec{m}}, \overline{[\![A(d)]\!]_{n,\ell,\vec{m}}}, [\![A(d)]\!]_{n,\ell+1,\vec{m}}$, for $0 \leq \ell < m_0$. Combining these with balanced cuts gives the desired Paris-Wilkie translation of $[\![\Gamma]\!]_{n,\vec{m}}, \overline{[\![A(0)]\!]_{n,\vec{m}}}, [\![A(s)]\!]_{n,\vec{m}}$.

Now suppose that Q ends with a bounded $\forall$ inference

$$\frac{a_0 > r(c), \Gamma, A(a_0)}{\Gamma, (\forall x \leq r(c))A(x)}$$

The induction hypothesis gives proofs of the cedents

$$[\![\Gamma]\!]_n,\ [\![A(a_0)]\!]_{n,m_0,\vec{m}}$$

for all $m_0 \leq r(n)$. From these, a single $\bigwedge$ inference gives the desired cedent $[\![\Gamma]\!]_n, [\![(\forall x \leq r(c))A(x)]\!]_{n,\vec{m}}$.

Finally, suppose that Q ends with a bounded $\exists$ inference

$$\frac{\Gamma, A(s)}{s > r(c), \Gamma, (\exists x \leq r(c))A(x)}$$

Here $s = s(c, \vec{a})$ is an arbitrary term and may contain $\mathrm{PV}_1(\alpha)$ functions. The next lemma will help handle this case. For $\ell \in \mathbb{N}$, we let $\underline{\ell}$ be a closed term with value ℓ such that $\underline{\ell}$ has $O(|\ell|)$ symbols.

Lemma 9 (i) *Suppose $0 \leq \ell \leq r(n)$, the values $\vec{m}$ are quasipolynomially bounded by n, $B(d)$ is a $\hat{\Sigma}_i^{b,\oplus_p \mathrm{P}}(\alpha)$ formula, and s is a $\mathrm{PV}_1(\alpha)$ term appearing in Q. Then the cedent*

$$\overline{[\![s = \underline{\ell}]\!]_{n,\vec{m}}},\ \overline{[\![B(s)]\!]_{n,\vec{m}}}, [\![B(\underline{\ell})]\!]_{n,\vec{m}} \tag{8}$$

has a tree-like PCK_p^i proof of Σ-size quasipolynomial in n and height polylogarithmic in n with $O(1)$ many formulas in each cedent of the proof.

(ii) *Let $0 \leq \ell_1 < \ell_2 \leq r(n)$ and s be a term in the proof Q. Then the cedent*

$$[\![s < \underline{\ell_1}]\!]_{n,\vec{m}},\ \bigvee_{\ell=\ell_1}^{\ell_2} [\![s = \underline{\ell}]\!]_{n,\vec{m}},\ [\![s > \underline{\ell_2}]\!]_{n,\vec{m}} \tag{9}$$

has a tree-like PCK_p^1 proof of Σ-size quasipolynomial in n and height $O(\log(\ell_2 - \ell_1 + 1))$, and with $O(1)$ many formulas in each cedent of the proof.

Proof (Sketch) Part (i) of the lemma is proved by induction on the complexity of B. For $B \in \Sigma_0^{b,\oplus_p \mathrm{P}}(\alpha)$, it follows immediately from Lemma 3. For B having outermost quantifier a (non-sharply) bounded $\exists$ or $\forall$, it follows straightforwardly from the induction hypothesis using a $\bigvee$ and $\bigwedge$ inference.

The proof of (ii) is by induction on $\ell_2 - \ell_1$ using binary divide-and-conquer. Lemma 3 again provides the necessary inferences at each step. □

We can now prove the bounded $\exists$ case of Theorem 8(a). The induction hypothesis gives a proof of $[\![\Gamma]\!]_{n,\vec{m}}, [\![A(s)]\!]_{n,\vec{m}}$. From (9) with $\ell_1 = 0$ and $\ell_2 = r(n)$, we obtain the cedent $\bigvee_{\ell=0}^{r(n)} [\![s = \underline{\ell}]\!]_{n,\vec{m}}, [\![s > r(c)]\!]_{n,\vec{m}}$. Taking B to be A and using the $r(n)+1$ many cedents (8) and a $\bigwedge$ and a $\bigvee$ inference, we obtain

$$\bigwedge_{\ell=0}^{r(n)} \overline{[\![s = \underline{\ell}]\!]_{n,\vec{m}}}, \overline{[\![A(s)]\!]_{n,\vec{m}}}, \bigvee_{\ell=0}^{r(n)} [\![A(\underline{\ell})]\!]_{n,\vec{m}}.$$

The last formula in this cedent is the same as $[\![(\exists x \leq r(c))A(x)]\!]_{n,\vec{m}}$; thus combining the three cedents with cuts gives the cedent

$$[\![s > r(c)]\!]_{n,\vec{m}}, [\![\Gamma]\!]_{n,\vec{m}}, [\![(\exists x \leq r(c))A(x)]\!]_{n,\vec{m}}$$

as desired. This completes the proof of part (a) of Theorem 8.

Parts (b) and (c) follow from (a) via proof constructions in [8] due originally to Razborov [38] and Krajíček [30]. The proofs P_n of $[\![\varphi]\!]_n$ given by (a) can be converted into tree-like refutations P'_n of H_n of quasipolynomial Σ-size and polylogarithmic depth with $O(1)$ formulas per cedent, by replacing the $\vee$ inferences in P_n that introduce the formula $[\![\varphi]\!]_n$ with cuts against cedents $\overline{[\![\eta]\!]_{n,m}}$. Given these refutations P'_n, (b) follows by the construction from the proof of Lemma 5 of [8] adapted to our setting of PCK^i_p.[2] The refutations of H_n of (b) can be converted to tree-like, quasipolynomial Σ-size refutations P''_n of Ξ_n by using $\vee$ inferences to derive the cedents $\overline{[\![\eta]\!]_{n,m}}$ in H_n from the cedents in Ξ_n. The refutations P''_n and Lemma 6 of [8] give the refutations needed for part (c).

We now prove (d). By the "quantifier-oracle" correspondence discussed in Section 2.2, the witnessing theorem for S^{i+1}_2 and the $\forall\Sigma^b_{i+1}$-conservativity of S^{i+1}_2 over T^i_2 [12, 13] apply also to the theories $S^{i+1,\oplus_p\mathrm{P}}_2(\alpha)$ and $T^{i,\oplus_p\mathrm{P}}_2(\alpha)$. Thus there is an algorithm $A(x)$ which computes a witness $y \leq t(x)$ for the truth of the $\hat{\Sigma}^{b,\oplus_p\mathrm{P}}_{i+1}(\alpha)$ formula $\varphi(x)$ which runs in polynomial time $|x|^{O(1)}$ and makes oracle queries to $\hat{\Sigma}^{b,\oplus_p\mathrm{P}}_i(\alpha)$ properties. For any fixed value $x = n$, we convert this algorithm into a refutation P_n of H_n.

The oracle queries of $A(n)$ are made to a single (universal) $\hat{\Sigma}^{b,\oplus_p\mathrm{P}}_i(\alpha)$ predicate $B(\cdots)$, and we can assume that $A(n)$ is constrained to always make exactly $p(|n|)$ many oracle queries before producing a witness y for $\varphi(n)$. We shall use partial computations of $A(n)$ to build cedents $\Gamma_{q,w,n}$ in P_n so that each $\Gamma_{q,w,n}$ corresponds to a possible set of answers for the first

[2] As the referee noted, the proof of Lemma 5 of [8] erroneously states that the proof construction yields a tree-like proof. This is not correct (a corrected proof is in preparation), but since the proofs P'_n are of polylogarithmic depth, that construction still converts the proofs P'_n into tree-like refutations of quasipolynomial Σ-size.

q oracle queries of $A(n)$. There are many potential computations based on whether the oracle answers "Yes" or "No", and different sequences of Yes/No answers will correspond to different paths in the tree-like refutation. Each cedent $\Gamma_{q,w,n}$ will contain the negations of the oracle answers received so far. Formally, a value $w \geq 0$ codes the oracle query answers by letting $Bit(q,w) = \lfloor w/2^q \rfloor \bmod 2$ equal zero or one depending on whether the $(q+1)$-st oracle answer is yes or no. There is a deterministic polynomial time function $f(q,w,n)$ such that, if the first q answers to oracle queries of $A(n)$ are given by the bits of w, then $B(f(q,w,n))$ is the $(q+1)$-st query made by $A(n)$. We write $\overline{B}$ for the prenex form of $\neg B$, and let $B^*_{q,w,n}$ denote the formula $B(f(q,w,n))$ if the answer to this oracle query as coded by w is "No" and denote $\overline{B(f(q,w,n))}$ if the answer as coded by w is "Yes". For $q \leq p(|n|)$, and any w such that $|w| \leq q$, let the cedent $\Gamma_{q,w,n}$ be the cedent

$$[\![B^*_{0,w,n}]\!],\ [\![B^*_{1,w,n}]\!],\ \ldots,\ [\![B^*_{q-1,w,n}]\!].$$

That is to say, the cedent $\Gamma_{q,w,n}$ contains the Paris-Wilkie translations of the *negations* of the assertions made by the first q oracle answers.

$\Gamma_{0,w,n}$ is the empty cedent, and is the final line of the refutation P_n. For $q < p(|n|)$, $\Gamma_{q,w,n}$ is derived from $\Gamma_{q+1,w,n}$ and $\Gamma_{q+1,w+2^q,n}$ by a cut on $[\![B(f(q,w,n))]\!]$. For $q = p(|n|)$, let $g(w,n)$ be the deterministic polynomial time function that computes the value output by the algorithm $A(n)$ after receiving the $p(|n|)$ oracle answers coded by w. The cedent $\Gamma_{p(|n|),w,n}$ is derived by a cut inference from the cedent $\overline{[\![\eta]\!]_{n,g(w,n)}} \in \mathrm{H}_n$ and the cedent

$$[\![B^*_{0,w,n}]\!],\ \ldots,\ [\![B^*_{p(|n|)-1,w,x}]\!],\ [\![\eta]\!]_{n,g(w,n)}. \tag{10}$$

To complete the description of the refutation P_n we must show that (10) has a tree-like PCK^i_p proof with quasipolynomial Σ-size, polylogarithmic height, and polylogarithmically many formulas in each cedent. We claim that this follows from the fact that, since it proves the correctness of the algorithm A, $T_2^{i,\oplus_p \mathrm{P}}(\alpha)$ proves

$$\begin{aligned}(\forall x, w)(\exists q < p(|x|))[(Bit(q,w){=}0 \wedge \overline{B(f(q,w,x))}) \\ \vee (Bit(q,w){=}1 \wedge B(f(q,w,x))) \vee \eta(x, g(x,w))].\end{aligned} \tag{11}$$

In fact, for $i \geq 1$, part (a) of Theorem 8 comes close to saying that the provability of (11) implies the existence of the desired PCK^i_p proofs of (10). This is not quite true however, as the formula (11) is a $\Sigma^b_0(\hat{\Sigma}^{b,\oplus_p \mathrm{P}}_i(\alpha))$ formula instead of just a $\hat{\Sigma}^{b,\oplus_p \mathrm{P}}_i(\alpha)$ formula. The next lemma extends (a) to handle this situation.

Lemma 10 *Let $i \geq 0$. For $n \geq 0$ and $|w_0| \leq p(|n|)$, the sequents* (10) *with $w := w_0$ have tree-like* PCK_p^i *proofs of* Σ*-size quasipolynomial in n and height polylogarithmic in n, and in which all cedents have polylogarithmically many formulas.*

Lemma 10 is proved essentially by the same method as (a) of Theorem 8. (The $i = 0$ case follows from Lemma 3.) Consider a free-cut free $T_2^{i,\oplus_p \mathrm{P}}(\alpha)$ proof Q of the formula (11), with the $(\forall x, w)$ quantifiers removed and the formulas $(Bit(q,w){=}0 \wedge \overline{B(f(q,w,x))})$ and $(Bit(q,w){=}1 \wedge B(f(q,w,x)))$ rewritten as a $\hat{\Pi}_i^{b,\oplus_p \mathrm{P}}(\alpha)$ formula $B_0(q,w,x)$ and a $\hat{\Sigma}_i^{b,\oplus_p \mathrm{P}}(\alpha)$ formula $B_1(q,w,x)$, respectively. The only formulas in Q which are not $\hat{\Sigma}_i^{b,\oplus_p \mathrm{P}}(\alpha)$ or $\hat{\Pi}_i^{b,\oplus_p \mathrm{P}}(\alpha)$ formulas are ancestors of subformulas of this modified version of (11), with some terms s possibly substituted for the variable q. We extend the Paris-Wilkie translation $[\![\cdots]\!]$ to these additional formulas, translating the outermost sharply bounded existential quantifier and disjunctions of (11) by means of the cedent comma as opposed to $\bigvee$. In more detail, the translation of $B_0(s,w,x) \vee B_1(s,w,x)$ is

$$[\![B_0(s,w,x)]\!]_{w_0,n,\vec{m}}, [\![B_1(s,w,x)]\!]_{w_0,n,\vec{m}},$$

where $\vec{m}$ are values for the additional free variables of the term s. The formula $B_0(s,w,x) \vee B_1(s,w,x) \vee \eta(x, g(x,w))$ translates to

$$[\![B_0(s,w,x)]\!]_{w_0,n,\vec{m}}, [\![B_1(s,w,x)]\!]_{w_0,n,\vec{m}}, [\![\eta]\!]_{n,g(w_0,n)}.$$

Finally, the translation of the subformula in the endcedent of Q is

$$\begin{aligned}&[\![B_0(q,w,x)]\!]_{0,w_0,n}, [\![B_1(q,w,x)]\!]_{0,w_0,n}, \ldots,\\ &\quad [\![B_0(q,w,x)]\!]_{p(|n|)-1,w_0,n}, [\![B_1(q,w,x)]\!]_{p(|n|)-1,w_0,n}, [\![\eta]\!]_{n,g(w_0,n)}. \quad (12)\end{aligned}$$

The proof method for part (a) of Theorem 8, with slight modifications in the $\exists$ and $\vee$ cases to take care of the unusual translation, gives proofs of the Paris-Wilkie translations of each cedent in Q: by inspection, these proofs are tree-like PCK_p^i, have Σ-size quasipolynomial in n and height polylogarithmic in n. Moreover, each cedent contains only $O(1)$ many formulas in addition to ancestors of those in the endcedent (12), so in particular it contains only polylogarithmically many formulas.

It remains to derive (10) from (12) by means of a tree-like PCK_p^i proof obeying the requisite bounds. Consider a specific $q_0 \in \{0, \ldots, p(|n|) - 1\}$. If $Bit(q_0, w_0) = 0$, there are very simple tree-like PCK_p^i derivations of $\overline{[\![B_0(q,w,x)]\!]_{q_0,w_0,n}}, [\![B^*_{q_0,w_0,n}]\!]$ and of $\overline{[\![B_1(q,w,x)]\!]_{q_0,w_0,n}}$; otherwise, there are

very simple tree-like PCK_p^i derivations of $\overline{[\![B_1(q,w,x)]\!]_{q_0,w_0,n}}, [\![B^*_{q_0,w_0,n}]\!]$ and of $\overline{[\![B_0(q,w,x)]\!]_{q_0,w_0,n}}$. We can use cuts against these cedents to derive (12) with $[\![B_0(q,w,x)]\!]_{q_0,w_0,n}, [\![B_1(q,w,x)]\!]_{q_0,w_0,n}$ replaced by $[\![B^*_{q_0,w_0,n}]\!]$. Doing this for all the (polylogarithmically many) values of q_0 derives (10).

That proves Lemma 10, and thereby also part (d) of Theorem 8.

Part (e) of the theorem follows from (d) by the same arguments as used to prove parts (b) and (c) from (a).

We now prove part (f). By the relativization of the polynomial local search (PLS) construction [18] to $\oplus_p\mathrm{P}$ and to values of $i > 1$, there is a PLS problem (N, c), and a term $r(x)$, such that the functions N and c are computable in polynomial time while making queries to a $\hat{\Sigma}_{i-1}^{b,\oplus_p\mathrm{P}}(\alpha)$ oracle, and such that if $s \leq r(x)$ then $N(x,s) \leq r(x)$ and if also $c(x,s) \leq c(x,N(x,s))$ then $s \leq t(x)$ and $\eta(x,s)$. Furthermore, $T_2^{i-1,\oplus_p\mathrm{P}}(\alpha)$ proves all these facts.[3]

The PLS problem (N, c) gives rise to the following strategy for witnessing $\varphi(n)$. Starting with $s_0 = 0$, calculate successively $c(n, s_\ell)$, $s_{\ell+1} = N(n, s_\ell)$, and $c(n, s_{\ell+1})$, making $\mathrm{poly}(|n|)$ many queries to a $\hat{\Sigma}_{i-1}^{b,\oplus_p\mathrm{P}}(\alpha)$ oracle for each ℓ. We will use this strategy to form a PCK_p^{i-1} refutation P_n of H_n. W.l.o.g., the polynomial time algorithms computing $c(n,s)$ and $N(n,s)$ always make exactly $p(|n|)$ queries to a $\Sigma_{i-1}^{b,\oplus_p\mathrm{P}}(\alpha)$ oracle B. The Yes/No answers to these queries are encoded by values w and v with the convention that $\mathit{Bit}(q,w)$, resp. $\mathit{Bit}(q,v)$, specifies whether the $(q+1)$-st oracle query in the computation of $c(n,s)$, resp. $N(n,s)$, is answered yes or no.

The PCK_p^{i-1} refutation P_n of H_n ends with the empty cedent and has initial cedents from H_n. The internal portions of P_n are constructed in a manner similar to the P_n constructed for the proof of (d). For $q \leq p(|n|)-1$, let $f(q,w,s,n)$ be the deterministic polynomial-time function such that if the bits of w encode the first q queries made in the computation of $c(n,s)$, then the $(q+1)$-st query is $B(f(q,w,s,n))$. Let $B^*_{q,w,s,n}$ denote the formula $B(f(q,w,s,n))$ or $\overline{B(f(q,w,s,n))}$ depending on whether the answer to the query, as coded by w, is "No" or "Yes", respectively. Similarly, let $g(q,v,s,n)$ be the deterministic polynomial-time function such that if the bits of v encode the first q queries made in the computation of $N(n,s)$, then the $(q+1)$-st query is $B(g(q,v,s,n))$. Let $B'_{q,v,s,n}$ denote the formula $B(g(q,v,s,n))$ or $\overline{B(g(q,v,s,n))}$ depending on whether the answer to the query, as coded by v, is "No" or "Yes", respectively. Let $C(w,s,n)$ give

[3] In fact, it is possible to prove suitable "new-style" witnessing theorems in the style of [10, 42] that show that $T_2^{0,\oplus_p\mathrm{P}}(\alpha)$ proves these facts about N, c and r.

the cost value output by the computation of $c(n,s)$ if the bits of w encode the answers to the $p(|n|)$ oracle queries of $c(n,s)$. Likewise, let $S(v,s,n)$ be the value of $N(n,s)$ when v encodes the oracle answers received during the computation. Note that C and S are deterministic polynomial time.

The refutation P_n is built around "key" cedents $\Gamma_{w,s}$

$$[\![B^*_{0,w,s,n}]\!],\ [\![B^*_{1,w,s,n}]\!],\ \ldots,\ [\![B^*_{p(|n|)-1,w,s,n}]\!]$$

for $s = 0,\ldots,r(x)$ and $|w| \leq p(|n|)$. (Unneeded cedents may be discarded once the refutation has been constructed.) Note there are $2^{p(|n|)}$ such cedents for any fixed s. Also note that each $\Gamma_{w,s}$ implicitly specifies a cost value for s, namely $C(w,s,n)$. The final empty cedent of P is derived from the cedents $\Gamma_{w,0}$ where $s = 0$, by using a balanced tree of cuts.

An arbitrary fixed cedent $\Gamma_{w,s}$ is derived in P_n by the following. Let v and w' be values with $|v|, |w'| \leq p(|n|)$. Let $s' = S(v,s,n)$, namely the neighbor of s as computed with oracle answers specified by v. Then $\Gamma_{w,s,v,w'}$ is defined to be the cedent containing the formulas of $\Gamma_{w,s}$ plus the formulas $[\![B'_{q,v,s,n}]\!]$ for $q < p(|n|)$ and the formulas of $\Gamma_{w',s'}$. For a fixed w, there are $2^{2p(|n|)}$ cedents $\Gamma_{w,s,v,w'}$, and the cedent $\Gamma_{w,s}$ is derived from these by a balanced tree of cuts, where the order in which cuts are performed respects the order of the oracle queries in the computations of $c(n,s)$ and $N(n,s)$. (This is similar to the way that, in the proof of part (d), the cedent $\Gamma_{0,w,n}$ was inferred from the cedents $\Gamma_{p(|n|),w,n}$.)

The cedents $\Gamma_{w,s,v,w'}$ are derived in P_n in one of two possible ways. First, if $C(w,s,n) > C(w',s',n)$, then $\Gamma_{w,s,v,w'}$ is derived by a weakening from $\Gamma_{w',s'}$. Otherwise, $C(w,s,n) \leq C(w',s',n)$. In this case, let $m = s$ and derive $\Gamma_{w,s,v,w'}$ from the cedent

$$\Gamma_{w,s,v,w'},\ [\![\eta]\!]_{n,m} \tag{13}$$

using a cut against the cedent $\overline{[\![\eta]\!]_{n,m}}$ in H_n.

To give the derivations of the cedent (13), note that $T_2^{i-1,\oplus_p \mathrm{P}}(\alpha)$ proves

$$\begin{aligned}
&(\forall x,s,s',w,v,w')(\exists q \leq p(|x|))\\
&\quad[(Bit(q,w) = 0 \wedge \neg B(f(q,w,s,x))) \vee (Bit(q,w) = 1 \wedge B(f(q,w,s,x)))\\
&\quad\ \vee (Bit(q,v) = 0 \wedge \neg B(g(q,v,s,x))) \vee (Bit(q,w) = 1 \wedge B(g(q,v,s,x)))\\
&\quad\ \vee (Bit(q,w') = 0 \wedge \neg B(f(q,w',s',x))) \vee (Bit(q,w') = 1 \wedge B(f(q,w',s',x)))\\
&\quad\ \vee s' \neq S(v,s,x) \vee C(w,s,x) > C(w',s',x) \vee \eta(n,m)].
\end{aligned}$$

For values of w,v,w',s,s' being considered, the Paris-Wilkie translations of the formulas $s' \neq S(v,s,x)$ and $C(w,s,x) > C(w',s',x)$ are just the

constants *False*. Therefore, by the same argument used for Lemma 10 at the end of part (d) above, there are PCK_p^{i-1} derivations of the cedents (13) of quasipolynomial Σ-size and polylogarithmically many formulas per cedent. This completes the proof of part (f).

It is perhaps interesting to note that an alternative proof of (c) can be given using (f) and the comment after Lemma 5 in [8] about translating depth i dag-like proofs with small numbers of formulas per cedent into depth $i-1$ dag-like proofs. Q.E.D. Theorem 8.

We next consider Paris-Wilkie translations into the propositional systems $\mathrm{PCK}^i_{\mathbb{F}_p}$ based on polynomials. We redefine the Paris-Wilkie translation of a strict bounded formula ψ, now denoting it $[\![\psi]\!]^{\mathbb{F}_p}_{\vec{n}}$. For $\psi \in \Sigma_0^{b,\oplus_p \mathrm{P}}(\alpha)$, $[\![\psi]\!]^{\mathbb{F}_p}_{\vec{n}}$ will be a multilinear $\mathbb{F}_p$ polynomial g which equals zero under a given truth assignment if and only if ψ is true. The variables x_k of g are intended to be 0/1 valued and represent the truth value of $\alpha(k)$. This polynomial g can be formed from the $\oplus$-dt formula $[\![\psi]\!]^{\mathbb{F}_p}_{\vec{n}}$ via the construction mentioned near the end of Section 2.1. Note that the degree of g is polynomially bounded in terms of $|\vec{n}|$.

For ψ a $\hat{\Sigma}_i^{b,\oplus_p \mathrm{P}}(\alpha)$ formula, the Paris-Wilkie translation $[\![\psi]\!]^{\mathbb{F}_p}_{\vec{n}}$ is defined by the same method as the definition of $[\![\psi]\!]_{\vec{n}}$, namely by expanding disjunctions of conjunctions into sums of monomials using the distributive law, and translating quantifiers and outermost Boolean connectives to $\bigwedge$'s and $\bigvee$'s.

Theorem 11 *All six parts of Theorem 8 still hold for* $\mathrm{PCK}^{i'}_{\mathbb{F}_p}$, $[\![\varphi]\!]^{\mathbb{F}_p}_n$, $\mathrm{H}^{\mathbb{F}_p}_n$ *and* $\Xi^{\mathbb{F}_p}_n$ *in place of* $\mathrm{PCK}^{i'}_p$, $[\![\varphi]\!]_n$, H_n *and* Ξ_n.

Theorem 11 can be proved by translating the $\mathrm{PCK}^{i'}_p$ proofs of Theorem 8 into $\mathrm{PCK}^{i'}_{\mathbb{F}_p}$ by the method discussed near the end of Section 2.1. This translation preserves the property of being quasipolynomial size, because in the $\mathrm{PCK}^{i'}_p$ proofs, the inputs to the $\oplus^k_p$ connectives are all polylogarithmic size conjunctions, so the application of the distributive law to convert formulas of the form $\oplus^k_p\Phi$ to sums of monomials causes only a quasipolynomial increase in size. Alternatively, a direct proof of Theorem 11 could be given by the method of proof of Theorem 8, but handling the cases of axioms and inferences involving sharply bounded formulas with Lemma 4 instead of Lemma 3. □

The $j = 1$ cases (d) and (f) of Theorems 8 and 11, which gave $\mathrm{PCK}^0_{\mathbb{F}_p}$ proofs with only polylogarithmically many formulas per cedent, can be further improved to give pure Nullstellensatz and Polynomial Calculus proofs.

Theorem 12 *Fix a prime p. Let $\varphi(x)$ be a $\hat{\Sigma}_1^{b,\oplus_p\mathrm{P}}(\alpha)$ formula.*

(d′) *Suppose $\mathrm{PV}_1^{\oplus_p\mathrm{P}}(\alpha) \vdash \varphi(x)$. Then there is a Nullstellensatz refutation over $\mathbb{F}_p$ of $\mathrm{H}_n^{\mathbb{F}_p}$ of polylogarithmic degree (and thus quasipolynomial size).*

(f′) *Suppose $T_2^{1,\oplus_p\mathrm{P}}(\alpha) \vdash \varphi(x)$. Then there is a Polynomial Calculus refutation over $\mathbb{F}_p$ of $\mathrm{H}_n^{\mathbb{F}_p}$ of polylogarithmic degree and quasipolynomial size.*

Proof If the hypothesis of (f′) holds, then by part (f) of Theorems 8 and 11 with $j = i = 1$, there is a dag-like $\mathrm{PCK}^0_{\mathbb{F}_p}$ refutation P_n of H_n with quasipolynomial Σ-size and with polylogarithmically many formulas in each cedent. By definition, this means that each line in the refutation P_n is a cedent containing $(\log n)^{O(1)}$ $\mathbb{F}_p$ polynomials, each of degree $(\log n)^{O(1)}$.

Consider a cedent Γ in P_n; it is of the form $f_1, \ldots, f_k$, which has the intuitive meaning that at least one f_ℓ evaluates to zero under any 0/1-assignment of values to the variables. Define Γ_n^* to be the cedent containing the single polynomial $f_1 f_2 \cdots f_k$. Form a new refutation P_n^*, by replacing each cedent Γ in P_n with Γ^*. By examining the rules of inference for the Polynomial Calculus (and noting that the $\bigwedge$ and $\bigvee$ rules do not apply since the cedents all contain only polynomials), it is clear that if Γ is inferred from Γ_1 and Γ_2 in P_n, then $\Gamma_1^*, \Gamma_2^* \vDash \Gamma^*$. By Lemma 4 there is an easy derivation of Γ^* from Γ_1^* and Γ_2^*, namely, $\Gamma^* = h_1\Gamma_1^* + h_2\Gamma_2^*$ for some multilinear polynomials h_1 and h_2. Therefore, P_n^* can be made to be a valid Polynomial Calculus refutation of $\mathrm{H}_n^{\mathbb{F}_p}$. By construction, P_n^* has quasipolynomially many lines, and the degree of P_n^* is polylogarithmic in n. Hence, the size of P_n^* is quasipolynomial in n.

The same argument works for case (d′) to prove the existence of a *tree-like* Polynomial Calculus refutation P_n^* of $\mathrm{H}_n^{\mathbb{F}_p}$ of quasipolynomially many lines and polylogarithmic degree. By Theorem 5.4 of [16], this implies the existence of a Nullstellensatz refutation of $\mathrm{H}_n^{\mathbb{F}_p}$ of polylogarithmic degree. □

4 A collapse of modular counting

4.1 Approximate counting in APC_1 and APC_2

Jeřábek [26] showed that APC_1 can define a notion of "approximate" cardinality for PV_1 definable sets. Working inside APC_1, suppose $X, Y \subseteq 2^n$ are

defined by Boolean circuits with n inputs, and $\epsilon \leq 1$ is a rational. Then, APC_1 can define a relation $X \preceq_\epsilon Y$ expressing

> "there exists a non-zero $v \in \mathrm{Log}$ and a circuit G such that G computes a surjection $v \times (Y \sqcup \epsilon 2^n) \twoheadrightarrow v \times X$."

Here the notation $\twoheadrightarrow$ indicates a surjective map, and $\sqcup$ means disjoint union. Usually, although not always, $1/\epsilon \in \mathrm{Log}$, where Log is the set of integers which are lengths. For $1/\epsilon \in \mathrm{Log}$, Jeřábek [26] showed that APC_1 can prove that $\preceq_\epsilon$ satisfies many basic properties expected of an "approximately smaller than" relation, including properties about subsets and certain types of unions and intersections. In addition, APC_1 can prove that, for any X, n, and ϵ as above, there is an $a \geq 0$ such that $X \approx_\epsilon a$, where we are now using Jeřábek's convention of $a = [0, a)$ and where $\approx_\epsilon$ is the intersection of $\preceq_\epsilon$ and $\succeq_\epsilon$.

The definition of $X \preceq_\epsilon Y$ is an $\exists\Pi^b_2$ formula. To reduce the quantifier complexity, [26] introduced a conservative extension of APC_1 called $\mathrm{HARD}^{\mathrm{A}}$. The language of $\mathrm{HARD}^{\mathrm{A}}$ contains an additional oracle function γ plus an axiom stating that $\gamma(x)$ defines the truth-table of a Boolean function in $||x||$ variables which is "hard on average" in the sense that any Boolean circuit that computes $\gamma(x)$ for substantially more than one half the values of x must be large. (See [26] for the exact definition.) $\mathrm{HARD}^{\mathrm{A}}$ proves there is a $\mathrm{PV}_1(\gamma)$ function $\mathit{Size}(C, 2^n, e)$ such that, for $\epsilon \in 1/\mathrm{Log}$, the set $X \subseteq 2^n$ defined by the circuit C satisfies $X \approx_\epsilon \mathit{Size}(C, 2^n, 2^{\epsilon^{-1}})$.

As a further simplification, we introduce another conservative extension of APC_1. APC^+_1 is a theory in the language with an additional binary function symbol Sz. The axioms of APC^+_1 include those of $\mathrm{APC}_1(Sz)$, namely the theory $\mathrm{PV}_1(Sz) + \mathrm{sWPHP}(\mathrm{PV}_1(Sz))$. In addition, there is an axiom stating that for any circuit C with n variables that defines a set $X \subseteq 2^n$ and any $\epsilon \in 1/\mathrm{Log}$, there exists a circuit witnessing that $X \approx_\epsilon Sz(C, 2^n)$. Note that the function Sz does not have an argument corresponding to ϵ; instead, it produces an approximate cardinality that is accurate to within ϵ fraction of 2^n for every $\epsilon \in \mathrm{Log}$.

Proposition 13 APC^+_1 *is a* $\forall\Sigma^b_\infty$*-conservative extension of* APC_1.

Proof Let $\mathcal{A} \vDash \mathrm{HARD}^{\mathrm{A}} + \varphi$, where φ is an $\exists\Sigma^b_\infty$ sentence. Proposition 13 will be proved by giving a model $\mathcal{B}$ of $\mathrm{APC}^+_1 + \varphi$. First take an elementary extension $\tilde{\mathcal{B}}$ of $\mathcal{A}$ which is not cofinal with $\mathcal{A}$. Take some δ such that δ^{-1} is in $\mathrm{Log}(\tilde{\mathcal{B}})$ but above $\mathrm{Log}(\mathcal{A})$. The model $\mathcal{B}$ for $\mathrm{APC}^+_1 + \varphi$ is defined by letting

$\mathcal{B}$ be the initial segment of $\tilde{\mathcal{B}}$ determined by $\mathcal{A}$ and interpreting $Sz(C, 2^n)$ as $Size(C, 2^n, 2^{\delta^{-1}})$.

The axioms of $\mathrm{APC}_1(Sz)$ are $\forall\Sigma^b_\infty(Sz)$ formulas, so they automatically hold in the initial segment $\mathcal{B}$ of $\tilde{\mathcal{B}}$. We also must show that, for $\epsilon \in 1/\mathrm{Log}(\mathcal{B})$ and X a set defined by an n-variable circuit C from $\mathcal{B}$, circuits witnessing $X \approx_\epsilon Sz(C, 2^n)$ exist in $\mathcal{B}$. (The circuits witnessing $X \approx_\delta Sz(C, 2^n)$ may be outside of $\mathcal{B}$.) We argue the $\preceq_\epsilon$ direction, as the other is similar. Since $\mathcal{B} \models \mathrm{APC}_1(Sz)$, $\mathcal{B}$ contains a $v \neq 0$ and a circuit mapping $v \times (Size(C, 2^n, 2^{(\epsilon/3)^{-1}}) \sqcup (\epsilon/3)2^n)$ surjectively onto $v \times X$. We claim that $Sz(C, 2^n) + \epsilon 2^n \geq Size(C, 2^n, 2^{(\epsilon/3)^{-1}}) + (\epsilon/3)2^n$, which, if true, is enough to complete the proof.

Assume that $Sz(C, 2^n) < Size(C, 2^n, 2^{(\epsilon/3)^{-1}}) - (2/3)\epsilon 2^n$. For some nonzero $w \in \tilde{\mathcal{B}}$, the following surjections are witnessed by circuits in $\tilde{\mathcal{B}}$:

$$w \times (Sz(C, 2^n) + (\epsilon/3 + \delta)2^n) \twoheadrightarrow w \times (X \sqcup (\epsilon/3)2^n) \twoheadrightarrow w \times Size(C, 2^n, 2^{(\epsilon/3)^{-1}}).$$

Thus, $\tilde{\mathcal{B}}$ also contains a surjection from $w \times (Size(C, 2^n, 2^{(\epsilon/3)^{-1}}) - (\epsilon/3 - \delta)2^n)$ onto $w \times Size(C, 2^n, 2^{(\epsilon/3)^{-1}})$. Since $\epsilon/3 \gg \delta$, this contradicts $\mathrm{HARD}^{\mathrm{A}}$ in $\tilde{\mathcal{B}}$. □

Below, we use the Sz function freely when proving results about bounded formulas in APC_1. In the spirit of [26], we typically abuse notation and write $Sz(X)$ for $Sz(C, 2^n)$, where X is the subset of 2^n defined by the n-variable circuit C.

To save space in some arguments involving Sz, we introduce the notation $x \trianglelefteq_a y$ to stand for "for every $\epsilon \in 1/\mathrm{Log}$, $x \leq y + \epsilon a$" and $\bowtie$ to stand for the intersection of $\trianglelefteq$ and $\trianglerighteq$. Note that $\trianglelefteq$ and $\bowtie$ are not definable by bounded formulas, so we cannot use induction for formulas involving them. Note also that for each model $\mathcal{A} \models \mathrm{BASIC}$ and each $a \in \mathcal{A}$, $\trianglelefteq_a$ is a quasiorder, the associated equivalence relation $\bowtie_a$ is a congruence with respect to $+$, and $(\mathcal{A} \cup -\mathcal{A}, +)/\bowtie_a$ is an ordered group.

The following proposition lists a few simple basic properties of the approximate counting mechanism from [26], formulated in terms of Sz and $\trianglelefteq$.

Proposition 14 (in APC^+_1) *Let $X, Y \subseteq 2^n$ be definable by n-variable circuits, and let $a < 2^n$ be a number, treated as the subset $[0, a)$ of 2^n.*

(a) $Sz(a) \bowtie_{2^n} a$,

(b) If $X \preceq_0 Y$, *then* $Sz(X) \trianglelefteq_{2^n} Sz(Y)$,

(c) If $X \cap Y = \emptyset$, *then* $Sz(X \cup Y) \bowtie_{2^n} Sz(X) + Sz(Y)$.

Item (c) is from Lemma 2.11(v) of [26]. Note that item (a) also implies $Sz(a) \bowtie_a a$ for a sufficiently large, say $a \geq 2^n/n^{O(1)}$. We will use the properties listed in Proposition 14 without explicit mention. More advanced properties of approximate counting will be invoked as needed.

The major limitation of the approximate counting available in APC_1 is that the size of $X \subseteq 2^n$ is approximated only up to an ϵ-fraction of 2^n rather than an ϵ-fraction of the "actual size" of X. Thus, the size of sparse sets is not measured well. To remedy this, Jeřábek [27] developed a more precise version of approximate counting, which involves PV_2 functions and thus requires APC_2. The only result of [27] that we use is the following:

Theorem 15 [27, Thm 3.21] (in APC_2) *If X is a bounded Σ^b_1 definable set and $\epsilon \in 1/\mathrm{Log}$, then there exist PV_2 functions with parameters (i.e. circuits with access to a Σ^b_1 oracle) f, g such that for some number m,*

$$m(1+\epsilon) \overset{f}{\twoheadrightarrow} X \overset{g}{\twoheadrightarrow} m.$$

An inspection of the proof shows that the above theorem also holds in a parametrized version: if X is a bounded Σ^b_1 set and X_y denotes $\{x : \langle x, y\rangle \in X\}$, then there are two-variable PV_2 functions with parameters f and g such that for each y, the functions $f(y,\cdot)$ and $g(y,\cdot)$ witness

$$m_y(1+\epsilon) \twoheadrightarrow_{\mathrm{PV}_2} X_y \twoheadrightarrow_{\mathrm{PV}_2} m_y$$

for some m_y. The notation $\twoheadrightarrow_{\mathrm{PV}_2}$ indicates the existence of a PV_2 surjection. The value m_y is computable as a function of y by a PV_2 function with parameters.

For $X \subseteq 2^n$, $\epsilon, p \in [0,1]$, and a an integer such that $|a| = n$, [26] uses the notation $\Pr_{x<a}(x \in X) \preceq_\epsilon p$ to mean $X \cap a \preceq_\epsilon pa$. We will additionally let $\Pr_{x<a}(x \in X)$ denote the fractional number $Sz(X)/a$. Thus, we write things such as $\Pr_{x<a}(x \in X) \leq p$ to mean $Sz(X \cap a) \leq pa$. There is no confusion between the two uses of Pr, as the first appears only in the context of $\preceq_\epsilon$, while the second appears in the context of $\leq$ or $\trianglelefteq$.

When it is understood that $X \subseteq a$, we write just $\Pr(X)$ instead of $\Pr_{x<a}(x \in X)$. Note that $\Pr(X) \trianglelefteq_1 p$ thus means the same as $Sz(X) \trianglelefteq_a pa$.

The methods of approximate counting from [26] and [27] relativize without difficulty. By the correspondence between the C^k_p quantifiers and a modular counting oracle, this includes relativization to $\oplus_p\mathrm{P}$.

Below, we work mostly in $\mathrm{APC}_2^{\oplus_p\mathrm{P}}$, that is, with APC_2 relativized to an $\mathrm{NP}^{\oplus_p\mathrm{P}}$-complete oracle (sometimes this is also relativized to a new uninterpreted predicate α). This theory is able to count $\mathrm{PV}_2^{\oplus\mathrm{P}}$ sets in the

style of [26]. To do this, all references to circuits or PV_1 functions in the definitions of $\preceq$, Sz, etc. need to be replaced by references to circuits with $\mathrm{NP}^{\oplus_p \mathrm{P}}$ oracles, resp. $\mathrm{PV}_2^{\oplus_p \mathrm{P}}$ functions. Formally, this should be reflected in a change of notation to something like $\preceq^{1,\oplus_p \mathrm{P}}$ etc. However, "moderation in all things" certainly applies to superscripts as well; we thus keep the basic notation for notions related to counting also in the relativized case.

We next give two simple technical lemmas which will be useful later on. The first corresponds to a special case of the inclusion-exclusion principle, while the second is a version of the union bound. Both hold also for the typically tricky case of families whose size is not in Log.

Lemma 16 (in T_2^1) *Let A, I, X be PV_1 sets with $A \subseteq I \times X$. For $i \in I$, let A_i stand for $\{x \in X : \langle i, x\rangle \in A\}$. There exists a PV_2 surjection from $\bigcup_{i\in I} A_i \sqcup \{\langle i, j, x\rangle : i < j, x \in A_i \cap A_j\}$ onto $\{\langle i, x\rangle : x \in A_i\}$.*

The intuition for Lemma 16 is the inclusion-exclusion principle that

$$|\textstyle\bigcup_i A_i| \;\geq\; \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j|\,.$$

The lemma witnesses this with a surjective PV_2 mapping

$$(\textstyle\bigcup_i A_i) \cup \bigsqcup_{i<j} (A_i \cap A_j) \twoheadrightarrow \bigsqcup_i A_i.$$

Note that the inclusion-exclusion principle of Proposition 2.19 of [26] applies only to families for which the size of the index set I is in Log.

Proof On input $x \in \bigcup_{i\in I} A_i$, the function finds the smallest value i_0 for which $x \in A_{i_0}$, and maps x to $\langle i_0, x\rangle$. This involves a binary search procedure which asks Σ_1^b queries. On input $\langle i, j, x\rangle$, where $i < j$ and $x \in A_i \cap A_j$, the function simply outputs $\langle j, x\rangle$.

To verify surjectivity, consider $\langle i, x\rangle$ such that $x \in A_i$. If there exists $i_0 < i$ such that $x \in A_{i_0}$, then $\langle i_0, i, x\rangle$ is mapped to $\langle i, x\rangle$. Otherwise, x itself is. □

Lemma 17 (in APC_2) *Let m, k, n be numbers. Let Y be a PV_2 set such that $m \twoheadrightarrow_{\mathrm{PV}_2} Y$. Let X be a Σ_1^b set such that for each $y \in Y$, the set $X_y := \{x : \langle x, y\rangle \in X\}$ is contained in 2^n and $X_y \preceq_0 k$. Then for every $\epsilon \in 1/\mathrm{Log}$,*

$$mk(1+\epsilon) \twoheadrightarrow_{\mathrm{PV}_2} \{\langle x, y\rangle \in X : y \in Y\}$$

and

$$mk(1+\epsilon) \twoheadrightarrow_{\mathrm{PV}_2} \{x : \exists y \in Y\, (x \in X_y)\}.$$

The lemma is quite close to [27, Theorem 3.19], but it does not seem to follow immediately from that result. [26, Proposition 2.16] is less relevant, as the error it introduces may be much too large if Y or the X_y's are sparse.

Proof Fix ϵ. By the remark after Theorem 15 there is a two-variable PV_2 function f such that for every $y \in Y$, $f(y,\cdot) : k_y(1+\epsilon/3) \twoheadrightarrow X_y$ and $X_y \twoheadrightarrow_{\mathrm{PV}_2} k_y$ for some k_y. By sWPHP(PV_2), k_y has to be smaller than $k(1+\epsilon/3)$, so $f(y,\cdot)$ is also a surjection from $k(1+\epsilon)$ onto X_y.

If g is the PV_2 surjection from m onto Y, then h defined by

$$h(w,z) = \langle f(g(w),z), g(w)\rangle$$

is a surjection from $mk(1+\epsilon)$ onto $\{\langle x,y\rangle \in X : y \in Y\}$. Composing h with a projection yields the required surjection from $mk(1+\epsilon)$ onto the set $\{x : \exists y \in Y\,(x \in X_y)\}$. □

4.2 The Valiant-Vazirani Theorem

We next formalize and prove the Valiant-Vazirani Theorem [44] in APC_2. It turns out that the usual proof, see e.g. the textbook [4], can be formalized directly in APC_2. The only difference is that the constants are slightly worse since APC_2 can only do approximate counting. We write "$\exists^1 x,\, A(x)$" to mean there is exactly one value x such that $A(x)$. We similarly write "$\exists^{\geq 2} x,\, A(x)$" to mean there are at least two values x such that $A(x)$.

Lemma 18 (Valiant-Vazirani Theorem) (in APC_2) *There exists a* PV_1 *function which takes as inputs a propositional CNF formula φ with n propositional variables $\vec{q} = \langle q_1,\ldots,q_n\rangle$ and a (randomly chosen) value r of length $(n+3)n+|n|$, and outputs a CNF formula φ_r with the same variables $\vec{q}$ such that*

$$\varphi \in \textsc{Sat} \implies \Pr_r[\neg\exists^1 b, b \models \varphi_r] \preceq_0 1 - \frac{1}{2^{|n|}\cdot 65}, \tag{14}$$

$$\varphi \notin \textsc{Sat} \implies \varphi_r \notin \textsc{Sat}. \tag{15}$$

The notation $b \models \varphi_r$ means that b encodes a string of n bits that specifies a satisfying assignment for φ_r. Note that b is implicitly bounded by 2^n.

Proof We argue informally in APC_2. W.l.o.g. the all zero assignment $b = 0$ does not satisfy φ (otherwise it is easy to construct φ_r even ignoring r). The function interprets its random input r as a pair $\langle j, v\rangle$, where j is a number from $[1, 2^{|n|}]$ and $v = \langle v_1,\ldots,v_{n+3}\rangle$ is an $(n+3)$-tuple of n-bit vectors. If

$j > n$, the formula $\varphi_{\langle j,v\rangle}$ is 0. Otherwise, $\varphi_{\langle j,v\rangle}$ is the conjunction $\varphi \wedge \varphi^{\perp}_{j,v}$ for $\varphi^{\perp}_{j,v}$ equal to

$$\bigwedge_{i=1}^{j+3} \vec{q} \perp v_i,$$

where $\vec{q} \perp v_i$ is a propositional formula stating that the inner product of $\vec{q}$ and v_i as bit vectors is equal to 1. Property (15) is clearly true, so we only need to show $\varphi_{\langle j,v\rangle}$ satisfies (14). Assume that φ is satisfiable. Let S be the set $\{b \in \{0,1\}^n : b \models \varphi\}$.

By Theorem 15, there are numbers m, k such that $k \in [1, n]$ and m approximates the size of S in the following sense:

$$2^{k-2} \leq m \twoheadleftarrow_{PV_2} S \twoheadleftarrow_{PV_2} \frac{3}{2}m \leq 2^k. \tag{16}$$

Informally, this says $2^{k-2} \leq |S| \leq 2^k$.

We now fix this value of k (or the smaller value if there are two such values) and consider only pairs $r = \langle k, v\rangle$ for this specific k. We henceforth write φ_v and $\varphi^{\perp}_v$ for $\varphi_{\langle k,v\rangle}$ and $\varphi^{\perp}_{k,v}$, respectively.

To prove (14), it is enough to show that $\Pr_v[\exists^1 b, b \models \varphi_v] \trianglerighteq_1 1/64$. We have

$$\Pr_v[\exists^1 b, b \models \varphi_v] \bowtie_1 \Pr_v[\exists b, b \models \varphi_v] - \Pr_v[\exists^{\geq 2} b, b \models \varphi_v]. \tag{17}$$

Accordingly, we need a lower bound for $\Pr_v[\exists b, b \models \varphi_v]$ and an upper bound for $\Pr_v[\exists^{\geq 2} b, b \models \varphi_v]$.

For a fixed value b, it is easy to compute a bijection between $2^{-k-3}2^{(n+3)n}$ and the set $\{v : b \models \varphi^{\perp}_v\}$. (Namely, for each of the first $k+3$ entries in the tuple v, toggle the bit corresponding to the first non-zero bit of b.) By the "left half" of (16), this gives a surjection

$$\{\langle b, v\rangle : b \models \varphi_v\} \twoheadrightarrow_{\mathrm{PV}_2} 2^{k-2}2^{-k-3}2^{(n+3)n} = 2^{-5}2^{(n+3)n} \tag{18}$$

Similarly, for fixed $b < b'$, there is a simple bijection between $2^{-2k-6}2^{(n+3)n}$ and the set $\{v : b, b' \models \varphi^{\perp}_v\}$. By the "right half" of (16), this gives a surjection

$$\{\langle b, b', v\rangle : b < b' \text{ and } b, b' \models \varphi_v\} \twoheadleftarrow_{\mathrm{PV}_2} \binom{2^k}{2} 2^{-2k-6}2^{(n+3)n} \leq 2^{-7}2^{(n+3)n}. \tag{19}$$

It follows that

$$\Pr_v[\exists^{\geq 2} b, b \models \varphi_v] \trianglelefteq_1 2^{-7}, \tag{20}$$

and this gives our desired upper bound on $\Pr_v[\exists^{\geq 2} b, b \models \varphi_v]$. To get a lower bound on $\Pr_v[\exists b, b \models \varphi_v]$, we make use of Lemma 16, according to which:

$$\{v : \exists b, b \models \varphi_v\} \sqcup \{\langle b, b', v\rangle : b < b', b, b' \models \varphi_v\} \twoheadrightarrow_{\mathrm{PV}_2} \{\langle b, v\rangle : b \models \varphi_v\}.$$

Combining this with (18) and (19) gives

$$\Pr_v[\exists b, b \models \varphi_v] \trianglerighteq_1 2^{-5} - 2^{-7}.$$

This, plus (17) and (20), gives

$$\Pr_v[\exists^1 b, b \models \varphi_v] \trianglerighteq_1 2^{-5} - 2 \cdot 2^{-7} = 2^{-6},$$

and completes the proof of the Valiant-Vazirani Theorem. □

Lemma 18 gives a reduction of SAT to UNIQUE-SAT that works with a one-sided error, and probability of success $1/(65 \cdot 2^{|n|})$. This success probability is too small for us work with usefully, and it is an open problem whether it can be improved substantially. Reductions with a higher probability of success can be obtained by working with "PARITY-SAT", or more generally, "mod p SAT". The next two definitions are intended to be formulated in $\mathrm{APC}_1^{\oplus_p \mathrm{P}}$.

Definition Let p be prime and $0 \leq k < p$. Then $\oplus_p^k$SAT is the set of propositional formulas φ such that the number of satisfying assignments of φ is congruent to k mod p.

Definition A language L is in $\mathrm{BP} \cdot \oplus_p \mathrm{P}$ if there exist PV_1 functions f and u such that for all x,

$$x \in L \iff \Pr_{r<u(x)}[f(x,r) \notin \oplus_p^1 \mathrm{SAT}] \preceq_0 1/4, \tag{21}$$

$$x \notin L \iff \Pr_{r<u(x)}[f(x,r) \notin \oplus_p^0 \mathrm{SAT}] \preceq_0 1/4. \tag{22}$$

See Lemma 20 for an even stronger condition equivalent to the definition of being $\mathrm{BP} \cdot \oplus_p \mathrm{P}$.

Since the definition of $\mathrm{BP} \cdot \oplus_p \mathrm{P}$ is formulated in $\mathrm{APC}_1^{\oplus_p \mathrm{P}}$, the functions witnessing the $\preceq_0$ relation in the definition must be $\mathrm{PV}_1^{\oplus_p \mathrm{P}}$ functions. When the definitions are formulated in $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$ instead, the decision whether to keep the functions as $\mathrm{PV}_1^{\oplus_p \mathrm{P}}$ or allow them to be $\mathrm{PV}_2^{\oplus_p \mathrm{P}}$ no longer matters. This is because the "$\preceq_0 1/4$" relation defined in terms of $\mathrm{PV}_2^{\oplus_p \mathrm{P}}$ functions

can be amplified to, say, "$\preceq_0 1/5$" (see also Lemma 20 below), and then the probabilities of the corresponding $\mathrm{PV}_1^{\oplus_p \mathrm{P}}$ events can be approximated in terms of $\mathrm{PV}_1^{\oplus_p \mathrm{P}}$ functions. By sWPHP($\mathrm{PV}_2^{\oplus_p \mathrm{P}}$), for a good enough approximation this will give $\mathrm{PV}_1^{\oplus_p \mathrm{P}}$ functions witnessing the "$\preceq_0 1/4$" conditions. Therefore, in practice, when working in $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$, we adhere to our usual convention regarding $\preceq$ and allow the probability witnessing functions to be $\mathrm{PV}_2^{\oplus_p \mathrm{P}}$.

Lemma 19 (in $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$) *Every Σ_1^b property is in $\mathrm{BP} \cdot \oplus_p \mathrm{P}$.*

Proof Of course, it is enough to show that SAT is in $\mathrm{BP} \cdot \oplus_p \mathrm{P}$. Since already $\mathrm{PV}_1^{\oplus_p \mathrm{P}}$ knows that a formula with exactly one satisfying assignment is in $\oplus_p^1$SAT and an unsatisfiable formula is in $\oplus_p^0$SAT, Lemma 18 gives us a PV_1 function which takes input φ and a random input r, and outputs φ_r such that

$$\begin{aligned} \varphi \in \textsc{Sat} &\implies \Pr_r[\varphi_r \notin \oplus_p^1 \textsc{Sat}] \preceq_0 1 - \frac{1}{2^{|n|} \cdot 65}, \\ \varphi \notin \textsc{Sat} &\implies \varphi_r \in \oplus_p^0 \textsc{Sat}. \end{aligned}$$

As in the usual proof of $\mathrm{NP} \subseteq \mathrm{BP} \cdot \oplus_p \mathrm{P}$, upgrading this to the result that $\textsc{Sat} \in \mathrm{BP} \cdot \oplus_p \mathrm{P}$ requires two observations. The first is that for a large enough term t, given φ and a randomly chosen sequence $\langle r_0, \ldots, r_{|t(\varphi)|-1} \rangle$ we have:

$$\begin{aligned} \varphi \in \textsc{Sat} &\implies \Pr_{\vec{r}}[\forall i{<}|t|\, \varphi_{r_i} \notin \oplus_p^1 \textsc{Sat}] \preceq_0 \frac{1}{4}, \\ \varphi \notin \textsc{Sat} &\implies \forall i{<}|t|\, \varphi_{r_i} \in \oplus_p^0 \textsc{Sat}. \end{aligned}$$

This follows easily from Chernoff's bound, which is provable in $\mathrm{APC}_1^{\oplus_p \mathrm{P}}$ by Proposition 2.18 of [26].

The second observation is that there exists a PV_1 function g which, given a sequence of formulas $\langle \varphi_0, \ldots, \varphi_{l-1} \rangle$, finds a single formula which is in $\oplus_p^1$SAT iff at least one of the φ_i is not in $\oplus_p^0$SAT. The definition of g involves two basic constructions, whose correctness is straightforward to verify in $\mathrm{PV}_1^{\oplus_p \mathrm{P}}$. Firstly, let $\psi(q_1, \ldots, q_n)$ be a formula, and for $0 < k < p$, let $\chi_k(q_1, \ldots, q_n)$ have exactly k satisfying assignments. (W.l.o.g., $n \geq p$). Let q_0 be a new variable; then the formula

$$(\psi \wedge q_0) \vee (\chi_k \wedge \neg q_0)$$

has exactly k many more satisfying assignments than ψ. Secondly, for any $\langle \psi_0, \ldots, \psi_{l-1} \rangle$ with disjoint sets of variables, if each $\psi_m \in \oplus_p^{k_m} \textsc{Sat}$, then the conjunction of the ψ_k's is in $\oplus_p^{k'} \textsc{Sat}$, for k' equal to the product mod p of the k_m's. A particular application of this is based on Fermat's Little Theorem: a conjunction of $p-1$ copies of a formula in disjoint sets of variables is in $\oplus_p^0 \textsc{Sat}$ if the original formula was, and in $\oplus_p^1 \textsc{Sat}$ otherwise.

A formula φ which has $k \bmod p$ satisfying assignments with k equal to either 0 or 1 can be converted by a "negation transformation" into a formula with $(1-k) \bmod p$ many satisfying assignments. This negation transformation first adds $p-1$ satisfying assignments, then squares the number of satisfying assignments.

The function g now can be defined first applying the "Fermat's Little Theorem" construction followed by the negation transformation to each of the φ_ℓ's separately, then taking their conjunction in distinct variables, and finally applying the negation transformation again. □

A slightly different amplification argument gives:

Lemma 20 (in $\mathrm{APC}_1^{\oplus_p \mathrm{P}}$) *For a language L in $\mathrm{BP}\cdot\oplus_p\mathrm{P}$ and a term $t(x) > 0$, there exist PV_1 functions f, u such that for all x,*

$$x \in L \implies \Pr_{r<u(x)}[f(x,r) \notin \oplus_p^1 \textsc{Sat}] \preceq_0 1/t(x),$$
$$x \notin L \implies \Pr_{r<u(x)}[f(x,r) \notin \oplus_p^0 \textsc{Sat}] \preceq_0 1/t(x).$$

Proof Let L be a language in $\mathrm{BP}\cdot\oplus_p\mathrm{P}$, as witnessed by some PV_1 functions f, u satisfying (21) and (22). By Chernoff's bound, if we take a large enough term s and on input x apply f not to one randomly chosen r but to independently chosen $r_0, \ldots, r_{|s(x)|-1}$, then for $x \in L$ with high probability a majority of the $f(x, r_i)$'s are in $\oplus_p^1 \textsc{Sat}$ (the opposite event happens with probability $\preceq_0 1/t(x)$) and for $x \notin L$ with high probability a majority of the $f(x, r_i)$'s are in $\oplus_p^0 \textsc{Sat}$.

It remains to verify that there is a PV_1 function g which on input $\langle \varphi_0, \ldots, \varphi_\ell \rangle$ produces a formula φ which is in $\oplus_p^1 \textsc{Sat}$ if a majority of the φ_i's are in $\oplus_p^1 \textsc{Sat}$, and is in $\oplus_p^0 \textsc{Sat}$ otherwise. The property "a majority of of the φ_i's are in $\oplus_p^1 \textsc{Sat}$" is polynomial-time computable with $\oplus_p^1 \textsc{Sat}$ as an oracle. We claim that, provably in $\mathrm{APC}_1^{\oplus_p \mathrm{P}}$, all such properties are polynomial-time many-one reducible to $\oplus_p^1 \textsc{Sat}$. This is proved via a rather routine formalization in $\mathrm{APC}_1^{\oplus_p \mathrm{P}}$ of the construction from the proof of Theorem 6. In fact, for proving Lemma 20 we need only the special case of Theorem 6 which

states that $\mathrm{P}^{\oplus_p \mathrm{P}}$ is contained in $\oplus_p \mathrm{P}$. We leave the details of the argument to the reader. □

We conclude this subsection with a strengthening of Lemma 19 which will be needed in the proof of Theorem 22 below.

Definition $\exists \cdot \oplus_p \mathrm{P}$ is the class of formulas of the form

$$\exists y < t \, (f(x, y) \in \oplus_p^k \mathrm{SAT})$$

for $f \in \mathrm{PV}_1$.

Lemma 21 (in $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$) *Every* $\exists \cdot \oplus_p \mathrm{P}$ *property is in* $\mathrm{BP} \cdot \oplus_p \mathrm{P}$.

Proof We first note that it is enough to prove that $\mathrm{BP} \cdot \oplus_p \mathrm{P}$ contains the set

$$\{\varphi(\vec{q}, \vec{r}) : \exists b \in \{0,1\}^n \varphi(b, \vec{r}) \in \oplus_p^1 \mathrm{SAT}\}, \tag{23}$$

where n is the number of variables in $\overline{q}$. This set is many-one complete for $\exists \cdot \oplus_p \mathrm{P}$ provably in $\mathrm{PV}_1^{\oplus_p \mathrm{P}}$. Moreover, by the usual Fermat's Little Theorem "$p-1$ copies" trick, we may consider only the case of φ for which $\varphi(b, \vec{r})$ is always either in $\oplus_p^1 \mathrm{SAT}$ or in $\oplus_p^0 \mathrm{SAT}$.

The argument showing that (23) is in $\mathrm{BP} \cdot \oplus_p \mathrm{P}$ mirrors the one for SAT. One first proves an analogue of Lemma 18: SAT is replaced by the set (23) in the statement, while "$b \models \varphi$" is replaced by "$\varphi(b, \vec{r}) \notin \oplus_p^0 \mathrm{SAT}$" and the PV_2 functions used for approximate counting are replaced by $\mathrm{PV}_2^{\oplus_p \mathrm{P}}$ functions.

We then make the appropriate modifications to the proof of Lemma 19 from Lemma 18. The amplification part of the argument remains essentially unchanged, so the only thing that requires replacing is the observation that a formula with exactly one satisfying assignment is in $\oplus_p^1 \mathrm{SAT}$ and an unsatisfiable formula is in $\oplus_p^0 \mathrm{SAT}$. Its place is taken by the observation, also provable in $\mathrm{PV}_1^{\oplus_p \mathrm{P}}$, that for any formula $\psi(\vec{q}, \vec{r})$, if $\psi(b, \vec{r}) \in \oplus_p^1 \mathrm{SAT}$ for exactly one assignment b to the $\vec{q}$ variables and $\psi(b, \vec{r}) \in \oplus_p^0 \mathrm{SAT}$ for all other b's, then $\psi \in \oplus_p^1 \mathrm{SAT}$; on the other hand, if $\psi(b, \vec{r}) \in \oplus_p^0 \mathrm{SAT}$ for all b's, then $\psi \in \oplus_p^0 \mathrm{SAT}$. □

4.3 Toda's Theorem, formalized

The next theorem states that $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$ can formalize the proof of Toda's Theorem [43] about the collapse of the modular counting polynomial time hierarchy. Recall that the notation $\Sigma_\infty^b(\oplus_p)$ describes formulas formed from

bounded existential, universal, and C_p^k quantifiers. The language of $T_2(\oplus_p)$ includes all $\Sigma^b_\infty(\oplus_p)$ formulas; whereas the languages of $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$ and the theories $T_2^{i,\oplus_p \mathrm{P}}$ restrict the counting quantifiers C_p^k to apply to sharply bounded formulas, and thus have only $\Sigma^{b,\oplus_p \mathrm{P}}_\infty$ formulas as bounded formulas.

Theorem 22 *$T_2(\oplus_p)$ is conservative over $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$. Furthermore, $T_2(\oplus_p)$ proves that any $\Sigma^b_\infty(\oplus_p)$ formula defines a property in $\mathrm{BP} \cdot \oplus_p \mathrm{P}$.*

Since $\mathrm{APC}_2^{\oplus_p \mathrm{P}} \subseteq T_2^{3,\oplus_p \mathrm{P}} \subseteq T_2(\oplus_p)$, this gives as an immediate corollary:

Corollary 23 *$T_2(\oplus_p)$ is conservative over $T_2^{3,\oplus_p \mathrm{P}}$.*

And, since the theories $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$ and $T_2^{k,\oplus_p \mathrm{P}}$ have the same languages:

Corollary 24 *The theories $T_2^{k,\oplus_p \mathrm{P}}$ for $k \geq 3$ are all equal to $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$.*

Theorem 22 and the corollaries relativize, so $T_2(\oplus_p, \alpha)$ is conservative over $\mathrm{APC}_2^{\oplus_p \mathrm{P}}(\alpha)$. Likewise, $\mathrm{APC}_2^{\oplus_p \mathrm{P}}(\alpha)$ equals $T_2^{k,\oplus_p \mathrm{P}}(\alpha)$ for $k \geq 3$.

Proof (of Theorem 22.) We will inductively assign to each $\Sigma^b_\infty(\oplus_p)$ formula φ a "$\mathrm{BP} \cdot \oplus_p \mathrm{P}$ translation" given by a pair $\langle f_\varphi, u_\varphi \rangle$, where f_φ is a PV_1 function and u_φ is a term. It will be verifiable in $T_2(\oplus_p)$ that f_φ, u_φ represent a $\mathrm{BP} \cdot \oplus_p \mathrm{P}$ property according to conditions (21) and (22), and that this $\mathrm{BP} \cdot \oplus_p \mathrm{P}$ property is equivalent to φ.

It will also be possible to verify in the subtheory $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$ that f_φ, u_φ represent a $\mathrm{BP} \cdot \oplus_p \mathrm{P}$ property, and that the translation is correct in the sense of commuting with connectives and quantifiers up to provable equivalence. In the case of the C_p^k quantifier, this means that the axioms governing its use are satisfied.

Conservativity of $T_2(\oplus_p)$ over $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$ can then be shown as follows. Take a proof in $T_2(\oplus_p)$, with $\Sigma^b_\infty(\oplus_p)$ induction formalized as a rule. Apply the $\mathrm{BP} \cdot \oplus_p \mathrm{P}$ translation to each formula in each cedent of the proof; strictly speaking, this means that the $\mathrm{BP} \cdot \oplus_p \mathrm{P}$ translation is applied to any maximal $\Sigma^b_\infty(\oplus_p)$ subformula appearing in the proof, while unbounded quantifiers and operators which have an unbounded quantifier in their scope are left unchanged. The translation makes all axioms and inferences provably sound in $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$ (this is argued in some detail below, after the translation is defined). Thus, in particular, the translation of the endcedent of the $T_2(\oplus_p)$ proof is provable in $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$. However, by the correctness of the translation,

a formula in the language of $\mathrm{APC}_2^{\oplus_p\mathrm{P}}$ is equivalent to its translation provably in $\mathrm{APC}_2^{\oplus_p\mathrm{P}}$. Therefore, if the endcedent of the $T_2(\oplus_p)$ proof consists of a single formula in the language of $\mathrm{APC}_2^{\oplus_p\mathrm{P}}$, then that formula is provable in $\mathrm{APC}_2^{\oplus_p\mathrm{P}}$.

We now proceed to the definition of the translation.

Atomic formulas. An atomic formula $\varphi(\vec{x})$ in the language of $T_2(\oplus_p)$ represents a PV_1 relation, and thus can be reduced to $\oplus_p^1\textsc{Sat}$ by a function $f_\varphi(\vec{x})$ which outputs a single propositional variable if $\varphi(\vec{x})$ holds, and $\bot$ otherwise. Since f does not use a random input, the choice of u_φ is irrelevant.

Negation. If φ is $\neg\psi$ then, given a translation f_ψ, u_ψ for ψ, the translation for φ differs only in that f_φ outputs the formula obtained by applying the "negation transformation" described in the proof of Lemma 19 to f_ψ. Thus $f_\varphi(\vec{x})$ is in $\oplus_p^1\textsc{Sat}$ if $f_\psi(\vec{x})$ is in $\oplus_p^0\textsc{Sat}$, and in $\oplus_p^0\textsc{Sat}$ if $f_\psi(\vec{x})$ is in $\oplus_p^1\textsc{Sat}$.

Disjunction and the existential quantifier. We describe only the harder case of the existential quantifier. If $\varphi(\vec{x})$ is $\exists y{<}t(\vec{x})\psi(\vec{x},y)$, let f_ψ, u_ψ represent the $\mathrm{BP}\cdot\oplus_p\mathrm{P}$ translation of ψ. By Lemma 20, the $\mathrm{BP}\cdot\oplus_p\mathrm{P}$ property represented by f_ψ, u_ψ can also be represented by some $\tilde{f}_\psi, \tilde{u}_\psi$, where $\tilde{u}_\psi$ can easily be made independent of y as long as $y < t(\vec{x})$, such that:

$$\begin{aligned}
\psi(\vec{x},y) &\implies \Pr_{r<\tilde{u}_\psi(\vec{x})}[\tilde{f}_\psi(\vec{x},y,r) \notin \oplus_p^1\textsc{Sat}] \preceq_0 1/(11t(\vec{x})),\\
\neg\psi(\vec{x},y) &\implies \Pr_{r<\tilde{u}_\psi(\vec{x})}[\tilde{f}_\psi(\vec{x},y,r) \notin \oplus_p^0\textsc{Sat}] \preceq_0 1/(11t(\vec{x})).
\end{aligned}$$

We will abuse notation slightly and write f_ψ, u_ψ for $\tilde{f}_\psi, \tilde{u}_\psi$. We have

$$\varphi(\vec{x}) \implies \Pr_{r<u_\psi(\vec{x})}[\forall y{<}t(\vec{x})(f_\psi(\vec{x},y,r) \notin \oplus_p^1\textsc{Sat})] < 1/10,$$

and by Lemma 17,

$$\neg\varphi(\vec{x}) \implies \Pr_{r<u_\psi(\vec{x})}[\exists y{<}t(\vec{x})(f_\psi(\vec{x},y,r) \notin \oplus_p^0\textsc{Sat})] < 1/10.$$

By Lemmas 21 and 20, there is a PV_2 function g and a term v such that

$$\begin{aligned}
\exists y{<}t(\vec{x})(f_\psi(\vec{x},y,r) \in \oplus_p^1\textsc{Sat}) &\implies \Pr_{s<v(\vec{x},r)}[g(\vec{x},r,s) \notin \oplus_p^1\textsc{Sat}] < 1/10,\\
\forall y{<}t(\vec{x})(f_\psi(\vec{x},y,r) \notin \oplus_p^1\textsc{Sat}) &\implies \Pr_{s<v(\vec{x},r)}[g(\vec{x},r,s) \notin \oplus_p^0\textsc{Sat}] < 1/10.
\end{aligned}$$

Thus, writing $A(\vec{x},r)$ for $\exists y{<}t(\vec{x})(f_\psi(\vec{x},y,r) \in \oplus_p^1\textsc{Sat})$, and $B(\vec{x},r,s)$ for $g(\vec{x},r,s) \in \oplus_p^1\textsc{Sat}$, and suppressing the bounds on r and s, we have:

$$\begin{aligned}
\varphi(\vec{x}) &\implies \Pr_r[\neg A(\vec{x},r)] < 1/10,\\
A(\vec{x},r) &\implies \Pr_s[\neg B(\vec{x},r,s)] < 1/10.
\end{aligned}$$

We also have:

$$1 \trianglelefteq_1 \Pr_{r,s}[\neg A(\vec{x}, r)] + \Pr_{r,s}[A(\vec{x}, r) \wedge \neg B(\vec{x}, r, s)] + \Pr_{r,s}[B(\vec{x}, r, s)].$$

If $\varphi(\vec{x})$, then $\Pr_{r,s}[\neg A(\vec{x}, r)] \trianglelefteq_1 1/9$. Moreover, a simple argument using Lemma 17 shows that $\Pr_{r,s}[A(\vec{x}, r) \wedge \neg B(\vec{x}, r, s)] \trianglelefteq_1 1/9$ always holds. Hence $\varphi(\vec{x})$ implies $\Pr_{r,s}[B(\vec{x}, r, s)] \trianglerighteq_1 7/9$. Therefore, by the definition of B,

$$\varphi(\vec{x}) \implies \Pr_{r,s}[g(\vec{x}, r, s) \notin \oplus_p^1 \textsc{Sat}] \trianglelefteq_0 1/4.$$

An analogous argument gives

$$\neg\varphi(\vec{x}) \implies \Pr_{r,s}[g(\vec{x}, r, s) \notin \oplus_p^0 \textsc{Sat}] \trianglelefteq_0 1/4.$$

This shows that g and w are a $\mathrm{BP} \cdot \oplus_p \mathrm{P}$ representation for φ, where $w(\vec{x})$ is a suitable bound on pairs $\langle r, s\rangle$ such that $r < u_\psi(\vec{x})$ and $s < v(\vec{x}, r)$.

The counting quantifiers. Let $\varphi(\vec{x})$ be $\mathsf{C}_p^k y{<}t(\vec{x})\psi(\vec{x}, y)$, where ψ has $\mathrm{BP} \cdot \oplus_p \mathrm{P}$ representation f_ψ, u_ψ. As before, using Lemma 20, we may reduce the error in the representation of ψ and assume that for $y < t(\vec{x})$, the set of random inputs depends only on $\vec{x}$ and not on y. So, again abusing notation by writing f_ψ, u_ψ instead of $\tilde{f}_\psi, \tilde{u}_\psi$, we have:

$$\psi(\vec{x}, y) \implies \Pr_{r<u_\psi(\vec{x})}[f_\psi(\vec{x}, y, r) \notin \oplus_p^1 \textsc{Sat}] \trianglelefteq_0 1/(5t(\vec{x})), \tag{24}$$

$$\neg\psi(\vec{x}, y) \implies \Pr_{r<u_\psi(\vec{x})}[f_\psi(\vec{x}, y, r) \notin \oplus_p^0 \textsc{Sat}] \trianglelefteq_0 1/(5t(\vec{x})). \tag{25}$$

For the $\mathrm{BP} \cdot \oplus_p \mathrm{P}$ translation of φ, let $u_\varphi(\vec{x})$ be $u_\psi(\vec{x})$, and define $f_\varphi(\vec{x}, r)$ as follows. For particular values of $\vec{x}$ and the random input $r < u_\psi(\vec{x})$, let $f_\varphi^-(\vec{x}, r)$ be the Cook-Levin style propositional translation of the formula $y < t(\vec{x}) \wedge z = f_\psi(\vec{x}, y, r) \wedge (v \models z)$. The formula $f_\varphi^-(\vec{x}, r)$ has propositional variables $\vec{p}_y, \vec{p}_z, \vec{p}_v$ corresponding to the bits of y, z, v respectively. In addition it contains auxiliary variables $\vec{q}$ for a Cook-Levin encoding of intermediate values in the polynomial time computations of $f_\psi(\vec{x}, y, r)$ and $v \models z$. The values of $\vec{p}_z$ and $\vec{q}$ are uniquely determined by the values of $\vec{p}_y, \vec{p}_v$, so, provably in $\mathrm{PV}_1^{\oplus_p \mathrm{P}}$, we may take only $\vec{p}_y$ and $\vec{p}_v$ into account when counting the number of satisfying assignments.

The intent is that, with high probability over r, the Boolean formula $f_\varphi^-(\vec{x}, r)$ has $k \bmod p$ many satisfying assignments precisely when $\varphi(\vec{x})$ is true. Accordingly, we let $f_\varphi(\vec{x}, r)$ be a Boolean formula which has $1 \bmod p$ many satisfying assignments when $f_\varphi^-(\vec{x}, r)$ has $k \bmod p$ many, and has

$0 \bmod p$ many satisfying assignments otherwise. This is done using the techniques of Lemma 20: namely, form $f_\varphi(\vec{x}, r)$ by modifying the formula $f_\varphi^-(\vec{x}, r)$ in four steps: first adding $p - k$ many satisfying assignments, then conjoining $p - 1$ copies with disjoint variables to raise the number of satisfying assignments to the power $p - 1$, then adding $p - 1$ more satisfying assignments, and finally using conjunction again to square the number of satisfying assignments. This works provably, even in $\mathrm{PV}_1^{\oplus_p \mathrm{P}}$, so that we have the equivalences

$$\begin{aligned} f_\varphi^-(\vec{x}, r) \in \oplus_p^k \textsc{Sat} \quad &\iff \quad f_\varphi(\vec{x}, r) \in \oplus_p^1 \textsc{Sat}, \\ f_\varphi^-(\vec{x}, r) \notin \oplus_p^k \textsc{Sat} \quad &\iff \quad f_\varphi(\vec{x}, r) \in \oplus_p^0 \textsc{Sat}. \end{aligned}$$

Below, we will write $\langle b_y, b_v \rangle \models f_\varphi(\vec{x}, r)$ for the statement that the valuation which substitutes the bits of y for $\vec{p}_y$ and the bits of v for $\vec{p}_v$ satisfies $f_\varphi(\vec{x}, r)$, and similarly for $f_\varphi^-(\vec{x}, r)$.

The $\mathrm{BP} \cdot \oplus_p \mathrm{P}$ translation of $\varphi(\vec{x})$ is by definition

$$\Pr_{r < u_\varphi(\vec{x})}[f_\varphi(\vec{x}, r) \notin \oplus_p^1 \textsc{Sat}] \preceq_0 1/4. \tag{26}$$

We must show this definition for the $\mathrm{BP} \cdot \oplus_p \mathrm{P}$ translation is faithful in the sense that the axioms for the C_p^k quantifiers are satisfied for the translations. The $\mathrm{BP} \cdot \oplus_p \mathrm{P}$ translation (26) is equivalent to the formula $C_k^{\varphi,t}$ defined as

$$\Pr_{r < u_\varphi(\vec{x})}[f_\varphi^-(\vec{x}, r) \notin \oplus_p^k \textsc{Sat}] \preceq_0 1/4.$$

Arguing in $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$, we first prove that

$$C_0^{\varphi,t}(\vec{x}) \vee C_1^{\varphi,t}(\vec{x}) \vee \cdots \vee C_{p-1}^{\varphi,t}(\vec{x}) \tag{27}$$

holds. From this it will follow that

$$\Pr_{r < u_\varphi(\vec{x})}[f_\varphi(\vec{x}, r) \notin \oplus_p^1 \textsc{Sat}] \preceq_0 1/4 \vee \Pr_{r < u_\varphi(\vec{x})}[f_\varphi(\vec{x}, r) \notin \oplus_p^0 \textsc{Sat}] \preceq_0 1/4.$$

To prove (27), fix $\vec{x}$ and, for $y < t(\vec{x})$ and $r < u_\varphi(\vec{x})$, define $A(y, r)$ as

$$(f_\psi(\vec{x}, y, r) \notin \oplus_p^1 \textsc{Sat} \wedge \psi(\vec{x}, y)) \vee (f_\psi(\vec{x}, y, r) \notin \oplus_p^0 \textsc{Sat} \wedge \neg\psi(\vec{x}, y)).$$

The occurrences of $\psi(\vec{x}, y)$ are expressed using a $\mathrm{PV}_1^{\oplus_p \mathrm{P}}$ formula equivalent to the $\mathrm{BP} \cdot \oplus_p \mathrm{P}$ representation of ψ on an appropriately large bounded interval; thus $A(y, r)$ is itself a $\mathrm{PV}_1^{\oplus_p \mathrm{P}}$ formula. The intended meaning of

$A(y,r)$ is that the random value r gives the wrong result for evaluating the truth of $\psi(\vec{x},y)$ using the BP$\cdot\oplus_p$P translation of ψ. In other words, that r disagrees with the majority of the r's in determining the truth value of $\psi(\vec{x},y)$.

We have $\Pr_r[A(y,r)] \preceq_0 1/5t(\vec{x})$ for each y, and hence $\Pr_r[\exists y\, A(y,r)] \preceq_0 1/4$ by Lemma 17. Now consider r, r' such that $\forall y\,(\neg A(y,r) \wedge \neg A(y,r'))$. Using the fact that for each y and each $\ell \in \{0,1\}$, $f_\psi(\vec{x},y,r) \in \oplus_p^\ell$SAT $\iff$ $f_\psi(\vec{x},y,r') \in \oplus_p^\ell$SAT, it can be proved, by $\mathrm{PV}_1^{\oplus_p \mathrm{P}}$-induction on $w \le t(\vec{x})$, that

$$\bigwedge_{\ell=0}^{p-1} \Big[\mathsf{C}_p^\ell\langle y,v\rangle(y<w \wedge \langle b_y,b_v\rangle \models f_\varphi^-(\vec{x},r)) \\ \leftrightarrow \quad \mathsf{C}_p^\ell\langle y,v\rangle(y<w \wedge \langle b_y,b_v\rangle \models f_\varphi^-(\vec{x},r'))\Big].$$

It follows that $f_\varphi^-(\vec{x},r) \in \oplus_p^\ell$SAT iff $f_\varphi^-(\vec{x},r') \in \oplus_p^\ell$SAT for each $\ell = 0,\ldots,p-1$. So (27) holds.

To verify that the translations $C_k^{\varphi,t}$ satisfy the axioms for the C_p^k quantifiers, we first make the following observation. Assume that $\tilde{f}_\psi, \tilde{u}_\psi$ also represent the BP$\cdot\oplus_p$P property given by f_ψ, u_ψ and satisfy the bounds (24) and (25) and the independence of y condition on $\tilde{u}_\psi$. Let $\tilde{f}_\varphi^-$ and $\tilde{u}_\varphi$ be constructed from $\tilde{f}_\psi$ and $\tilde{u}_\psi$ exactly as f_φ^-, u_φ were constructed from f_ψ, u_ψ. Then

$$\Pr_{r<u_\varphi(\vec{x})}[f_\varphi^-(\vec{x},r) \notin \oplus_p^k\mathrm{SAT}] \preceq_0 1/4 \iff \Pr_{\tilde{r}<\tilde{u}_\varphi(\vec{x})}[\tilde{f}_\varphi^-(\vec{x},\tilde{r}) \notin \oplus_p^k\mathrm{SAT}] \preceq_0 1/4.$$

This argument for this is similar to the one justifying (27): "most" values r and $\tilde{r}$ will agree with the majority choice over r's, resp. $\tilde{r}$'s, for every $y < t(\vec{x})$, and for each given y the majority choice over r's has to agree with the majority choice over $\tilde{r}$'s, since they both agree with $\psi(\vec{x},y)$. So, given "typical" r and $\tilde{r}$, it can be proved by induction that $f_\varphi^-(\vec{x},r) \in \oplus_p^k$SAT iff $\tilde{f}_\varphi^-(\vec{x},\tilde{r}) \in \oplus_p^k$SAT.

We now argue that the axiom

$$\mathsf{C}_p^k y{<}t(\vec{x})\psi(\vec{x},y) \wedge \psi(\vec{x},t(\vec{x})) \to \mathsf{C}_p^{k+1} y{<}(t(\vec{x}){+}1)\psi(\vec{x},y)$$

is satisfied after the BP$\cdot\oplus_p$P translation. (The other C_p axioms are handled similarly.) Write φ for $\mathsf{C}_p^k y{<}t(\vec{x})\psi(\vec{x},y)$ and $\tilde{\varphi}$ for $\mathsf{C}_p^{k+1} y{<}(t(\vec{x}){+}1)\psi(\vec{x},y)$. Let f_ψ, u_ψ be the translation of ψ used for constructing a translation of φ, and let $\tilde{f}_\psi, \tilde{u}_\psi$ be the translation of ψ used for translating $\tilde{\varphi}$. (We cannot assume that $\tilde{f}_\psi, \tilde{u}_\psi$ are the same as f_ψ, u_ψ, since the former have to satisfy (24)

and (25) with $t(\vec{x})+1$ instead of $t(\vec{x})$.) Assume that the translation $C_k^{\varphi,t}(\vec{x})$ of $\varphi(\vec{x})$ holds. Then for all but at most a $1/4$ fraction of the r's below $u_\psi(\vec{x})$, $f_\varphi^-(\vec{x},r) \in \oplus_p^k\textsc{Sat}$. Since $\tilde{f}_\psi, \tilde{u}_\psi$ satisfy all the bounds and uniformity conditions required of f_ψ, u_ψ, the observation above implies that for all but at most a $1/4$ fraction of all $\tilde{r}$'s below $\tilde{u}_\psi(\vec{x})$,

$$\mathsf{C}_p^k\langle y,v\rangle\,(y < t(\vec{x}) \wedge \langle b_y, b_v\rangle \models \tilde{f}_{\tilde{\varphi}}^-(\vec{x},\tilde{r})).$$

Assume that (the translation of) $\psi(\vec{x},t(\vec{x}))$ also holds. Then for all but at most a $1/(5t(\vec{x})+5)$ fraction of the $\tilde{r}$'s,

$$\mathsf{C}_p^1 v\,(\langle b_{t(\vec{x})}, b_v\rangle \models \tilde{f}_{\tilde{\varphi}}^-(\vec{x},\tilde{r})).$$

$\mathrm{PV}_1^{\oplus_p\mathrm{P}}$ induction then shows that for most $\tilde{r}$'s,

$$\mathsf{C}_p^{k+1}\langle y,v\rangle\,(y < t(\vec{x})+1 \wedge \langle b_y, b_v\rangle \models \tilde{f}_{\tilde{\varphi}}^-(\vec{x},\tilde{r})).$$

But $f_{\tilde{\varphi}}^-(\vec{x},\tilde{r})$ does not have satisfying assignments $\langle b_y, b_v\rangle$ for $y \geq t(\vec{x})+1$. Hence, for most $\tilde{r}$'s,

$$f_{\tilde{\varphi}}^-(\vec{x},\tilde{r}) \in \oplus_p^{k+1}\textsc{Sat}.$$

In other words, the translation $C_{k+1}^{\tilde{\varphi},t+1}(\vec{x})$ of $\tilde{\varphi}(\vec{x})$ does hold, so the translation of $\mathsf{C}_p^k v$ is correct. This completes the definition of the $\mathrm{BP}\cdot\oplus_p\mathrm{P}$ translation.

To complete the proof of conservativity of $T_2(\oplus_p)$ over $\mathrm{APC}_2^{\oplus_p\mathrm{P}}$, it remains to verify that the translations of all axioms and inferences in a $T_2(\oplus_p)$ proof are provably sound in $\mathrm{APC}_2^{\oplus_p\mathrm{P}}$.

For the modular counting axioms, this has been done above. The other axioms are valid already in first-order logic with equality, and they contain only quantifier-free formulas, which are equivalent to their translations even in $\mathrm{PV}_1^{\oplus_p\mathrm{P}}$ (as the translations do not actually involve the random input).

The $\mathrm{BP}\cdot\oplus_p\mathrm{P}$ translation of a weakening inference is a weakening inference, which is obviously sound. The translations of cuts and propositional inferences are sound by the correctness of the translation for $\neg$ and $\vee$. The translations of $\forall$-introduction inferences (both bounded and unbounded) are also unproblematic.

The case of $\exists$-introduction is more subtle. Consider for instance

$$\frac{\Gamma, \varphi(t)}{\Gamma, \exists y\,\varphi(y)}$$

(the bounded $\exists$ case is quite similar once the correctness of the translation for bounded $\exists$ is known). The problem is that on the syntactic level, the $\mathrm{BP} \cdot \oplus_p \mathrm{P}$ translation does not respect term substitution, so the translation of $\varphi(t)$ is not identical to the formula obtained from the translation of $\varphi(y)$ by substituting t for y.

To deal with this issue, it is enough to show that $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$ proves that (for y a fresh variable) if $y = t(\vec{x})$, then the translation of $\varphi(\vec{x}, y)$ is equivalent to the translation of $\varphi(\vec{x}, t(\vec{x}))$. This is shown by induction on the complexity of φ. The base case is immediate, and the steps for propositional connectives and (bounded or unbounded) $\exists$ and $\forall$ follow easily from the correctness of the translation for $\neg, \vee, \exists$. The most delicate case is the one for the counting quantifiers, in which we have to show that if if $y = t(\vec{x})$, then the translations of $\mathsf{C}_p^k z{<}y\psi(\vec{x}, y, z)$ and $\mathsf{C}_p^k z{<}t(\vec{x})\psi(\vec{x}, t(\vec{x}), z)$ are equivalent (with the equivalence between the translations of $\psi(\vec{x}, y, z)$ and $\psi(\vec{x}, t(\vec{x}), z)$ as the inductive assumption). This is proved in much the same way as the correctness of the translation for C_p^k. We leave the details to the reader.

The last type of inference to consider is a $\Sigma_\infty^b(\oplus_p)$ induction inference:

$$\frac{\Gamma, \neg\varphi(x), \varphi(x+1)}{\Gamma, \neg\varphi(0), \varphi(t)}$$

The soundness of this inference follows essentially from the fact that induction for $\mathrm{BP} \cdot \oplus_p \mathrm{P}$ properties holds already in $\mathrm{APC}_1^{\oplus_p \mathrm{P}}$, as on bounded intervals they are definable by $\mathrm{PV}_1^{\oplus_p \mathrm{P}}$ formulas (by the relativization to $\oplus_p \mathrm{P}$ of the well-known fact that $\mathrm{BPP} \subseteq \mathrm{P/poly}$, as formalized in $\mathrm{APC}_1^{\oplus_p \mathrm{P}}$ by [26, Lemma 3.10]). We also need to make sure that the translations of $\varphi(x+1), \neg\varphi(0), \varphi(t)$ are provably equivalent to the translation of $\varphi(x)$ with $x+1, 0, t$ substituted for x. This is similar to the proof of soundness for $\exists$ inferences described above. $\square$

5 The propositional collapse

We now use Theorems 8 and 22 to prove a collapse result for constant depth proof systems with mod p gates. Recall that $\mathrm{PK}_{\oplus_p}$ is the propositional proof system that allows arbitrary use of unbounded fanin $\bigwedge$, $\bigvee$, and $\oplus_p^k$ and $\bar{\oplus}_p^k$ connectives; whereas PCK_p^i is the system that allows sequents to contain only formulas with i alternating levels of $\wedge$'s and $\vee$'s in which mod p gates ($\oplus_p^k$ and $\bar{\oplus}_p^k$) apply only to (multi)sets of of logarithmic size conjunctions. The next theorem states that constant depth $\mathrm{PK}_{\oplus_p}$ proofs of $\Sigma_j(\oplus_p^-)$ formulas are quasipolynomially simulated by PCK_p^j proofs.

Theorem 25 *Let p be prime. Let $j > 0$ and let φ be a $\Sigma_j(\oplus_p^-)$ formula of Σ-size $\leq S$. Suppose there is a depth d $\mathrm{PK}_{\oplus_p}$ proof of φ of size $\leq S$. Then φ has a PCK_p^j proof of Σ-size $S^{\log^e S}$, where $e \in \mathbb{N}$ is a constant depending only on d.*

For $j \geq 3$, the proof of Theorem 25 uses a reflection principle and the Paris-Wilkie translation of part (a) of Theorem 8, so there is a uniform construction of the PCK_p^j proof from the $\mathrm{PK}_{\oplus_p}$ proof. Thus, this gives a uniform quasipolynomial simulation of $\mathrm{PK}_{\oplus_p}$ by PCK_p^j.

The simulation can be sharpened, in a way which also gives the missing cases $j = 1, 2$, by using part (c) of Theorem 8 instead of part (a). For $j = 3$ and thus for PCK_p^1 this gives:

Theorem 26 *Let p be a prime. Let φ be a $\Sigma_3(\oplus_p^-)$ formula of the form $\bigvee_{k<K} \bigwedge_{\ell<L_k} \psi_{k,\ell}$, where the $\psi_{k,\ell}$ are $\Sigma_1(\oplus_p^-)$. Assume that φ has Σ-size $\leq S$ and there is a depth d $\mathrm{PK}_{\oplus_p}$ proof of φ of size $\leq S$. Then the set of cedents $\{\overline{\psi_{k,0}}, \ldots, \overline{\psi_{k,L_k-1}}\}_{k<K}$ has a PCK_p^1 refutation of Σ-size $S^{\log^e S}$, where $e \in \mathbb{N}$ is a constant depending only on d.*

Similarly, the set $\{\overline{\psi_{k,0}}^{\mathbb{F}_p}, \ldots, \overline{\psi_{k,L_k-1}}^{\mathbb{F}_p}\}_{k<K}$ has a $\mathrm{PCK}_{\mathbb{F}_p}^1$ refutation of Σ-size $S^{\log^e S}$.

The proof of Theorems 25 and 26 is a standard argument invoking reflection principles for constant depth $\mathrm{PK}_{\oplus_p}$. Let α, β, and γ be second-order predicates. We define j-Ref(d-$\mathrm{PK}_{\oplus_p}$) to be a $\forall\Sigma_j^{b,\oplus_p\mathrm{P}}(\alpha, \beta, \gamma)$ sentence expressing the fact that for every a and b, if $\beta\restriction_{[0,b)}$ encodes a $\Sigma_j(\oplus_p^-)$ propositional formula φ, and $\alpha\restriction_{[0,a)}$ encodes a depth d $\mathrm{PK}_{\oplus_p}$ proof of φ, then φ is satisfied by the truth assignment encoded by γ.

The predicate β encodes the formula φ as follows. Propositional variables $p_0, p_1, \ldots$, and their negations $\overline{p}_0, \overline{p}_1, \ldots$ can be represented by letting $2 \cdot i$ and $2 \cdot i + 1$ respectively represent p_i and $\overline{p}_i$. Polylogarithmic size sets of literals are represented by first-order objects w. Without loss of generality, the outermost connective of each $\oplus_p^-$ subformula of φ is $\oplus_p^0$. (Since, in any event, φ can be proved equivalent to such a formula by a polynomial size PCK_p^j proof.) The top j levels of the syntactic tree of the $\Sigma_j(\oplus_p^-)$ formula are alternating $\bigvee$'s and $\bigwedge$'s, and are encoded by letting $\beta(k, y, z)$, for $k < j$, hold if the z-th connective at level $k + 1$ of the formula is an input to the y-th connective at level k. (By convention, the output gate is connective number 0 at level 0.) At the bottom level, $\beta(j, y, \langle w, u\rangle)$ means that the conjunction of the set of literals w is the u-th input to the y-th modular counting connective. The additional index u is needed because the inputs to

a counting connective form a multiset, so there may be multiple occurrences of the conjunction w as an input to the y-th counting connective. The notation $\beta\restriction_{[0,b)}$ means that arguments of $\beta(k,\cdot,\cdot)$ above b are ignored, so that the formula encoded by $\beta\restriction_{[0,b)}$ has size at most polynomial in b, but the size of the bottom level conjunctions is at most logarithmic.

A truth assignment is coded in the obvious way, by letting $\gamma(y)$ stand for the value of p_y. It is possible to write down a $\Sigma_j^{b,\oplus_p\mathrm{P}}(\beta,\gamma)$ formula stating "the $\Sigma_j(\oplus_p^-)$ formula encoded by $\beta\restriction_{[0,b)}$ is true under the assignment given by γ", with an $\exists/\forall$ quantifier corresponding to each of the top j levels of $\bigvee/\bigwedge$'s, and a $\Sigma_0^{b,\oplus_p\mathrm{P}}(\beta,\gamma)$ formula describing what happens at the level of the counting quantifiers and below.

The oracle α encodes the structure of a depth d proof, including information about what formula appears in a given line and which rules and premises are used for each inference, in some straightforward fashion. This permits $T_2(\oplus_p,\alpha,\gamma)$ to use bounded formulas to express properties of the proof encoded by α and to express the truth of formulas in the depth d proof under a truth assignment γ. Thus, $T_2(\oplus_p,\alpha,\gamma)$ can use induction on x to establish that "the first x lines of the proof coded by α are true under γ". The details of the encoding used by α are less important than in the case of β, as we do not care about the exact quantifier complexity of the statement "the depth d formula appearing in line x of the proof coded by $\alpha\restriction_{[0,a)}$ is true under γ", as long as it is bounded.

Formulas in the d-$\mathrm{PK}_{\oplus_p}$ proof encoded by α which happen to be $\Sigma_j(\oplus_p^-)$ formulas have two truth definitions: one based on α and one based on β. It is clearly possible to arrange that these two truth definitions are $T_2(\oplus_p)$-provably equivalent. This shows:

Proposition 27 *For each $j,d\in\mathbb{N}$, $T_2(\oplus_p,\alpha,\beta,\gamma)\vdash j\text{-Ref}(d\text{-}\mathrm{PK}_{\oplus_p})$.*

We now turn to the proof of Theorem 26. A separate proof of Theorem 25 is not needed, since the case $j=1$ follows from Theorem 26, whereas the case for general j follows from a generalized version of Theorem 26 in which $\Sigma_3(\oplus_p^-)$ is replaced by $\Sigma_{j+2}(\oplus_p^-)$ and PCK_p^1 is replaced by PCK_p^j. The proof of the generalization to $j>1$ involves no additional ideas, so we omit it.

Proof (Of Theorem 26.) Let Π be the size S depth d $\mathrm{PK}_{\oplus_p}$ proof of φ. Let n,m be such that Π and φ can be encoded by oracles $\alpha\restriction_{[0,n)}$ and $\beta\restriction_{[0,m)}$, respectively. Since S bounds both the size of Π and the Σ-size of φ, the numbers n and m are at most quasipolynomial in S.

By the relativization of Theorem 22 and Proposition 27, $\mathrm{APC}_2^{\oplus_p \mathrm{P}}(\alpha, \beta, \gamma)$, and hence also $T_2^{3,\oplus_p \mathrm{P}}(\alpha, \beta, \gamma)$, proves 3-Ref($d$-$\mathrm{PK}_{\oplus_p}$). By part (c) of Theorem 8, this implies that the set of cedents $\Xi_{n,m}$ obtained from the formula $[\![\neg 3\text{-Ref}(d\text{-}\mathrm{PK}_{\oplus_p})]\!]_{n,m}$ in the way described before Theorem 8 has a PCK_p^1 refutation P of Σ-size quasipolynomial in n and m, and thus in S. We substitute into the refutation P the bits of Π for the variables corresponding to α and the bits of φ for variables corresponding to β, leaving the bits corresponding to γ untouched. This yields a new proof P'; we claim that after simplifying by removing constants $\top$ and $\bot$, P' is readily converted into the desired refutation of $\{\overline{\psi_{k,0}}, \ldots, \overline{\psi_{k,L_k-1}}\}_{k<K}$.

For this, we must examine the clauses in $[\![\neg 3\text{-Ref}(d\text{-}\mathrm{PK}_{\oplus_p})]\!]_{n,m}$. The formula 3-Ref($d$-$\mathrm{PK}_{\oplus_p}$) is formulated as (the prenex form of) a disjunction $\neg Pf(\alpha, \beta, a, b) \vee Tr(\beta, \gamma, b)$, where $Pf(\alpha, \beta, a, b)$ states that $\beta\restriction_{[0,b)}$ codes a well-formed $\Sigma_3(\oplus_p^-)$ formula and that $\alpha\restriction_{[0,a)}$ encodes a valid proof of that formula, and where $Tr(\beta, \gamma, b)$ states that γ gives a satisfying assignment for the formula coded by $\beta\restriction_{[0,b)}$. The formula $Pf(\alpha, \beta, a, b)$ does not involve γ, and after substitution of constants for the bits of α and β, the Paris-Wilkie translation becomes just the constant $\top$ (or, strictly speaking, a variable-free $\oplus$-dt formula that evaluates to $\top$). The second disjunct $Tr(\beta, \gamma, b)$ has the form

$$(\exists y_1)(\forall y_2)(\exists y_3)[\beta(0,0,y_1) \wedge [\beta(1,y_1,y_2) \rightarrow [\beta(2,y_2,y_3) \wedge (\mathsf{C}_p^0\langle u,w\rangle)(\beta(3,y_3,\langle u,w\rangle) \wedge (\forall \ell \in w)(\gamma(\lfloor \ell/2 \rfloor) \leftrightarrow \ell \bmod 2 = 0))]]].$$

For notational simplicity, we have omitted all bounds on the quantified variables y_1, y_2, y_3, u, w, but these bounds are readily computed by polynomial time functions. The test "$\ell \bmod 2 = 0$" checks whether ℓ is negated or unnegated. The quantifier "$(\forall \ell \in w)$" is a shorthand notation for a sharply bounded quantifier.

Applying the Paris-Wilkie translation to the formula $Tr(\beta, \gamma, b)$, with constants $\top$ and $\bot$ substituted for variables that represent values of β, allows us to form cedents $\Xi_{n,m}$ of the type defined for Theorem 8. These cedents $\Xi_{n,m}$ are essentially the cedents $\{\overline{\psi_{k,0}}, \ldots, \overline{\psi_{k,L_k-1}}\}_{k<K}$ except with extra occurrences of $\bot$'s and $\top$'s. Thus the cedents $\Xi_{n,m}$ can be easily derived, by tree-like PCK_p^1 proofs, from the cedents $\{\overline{\psi_{k,0}}, \ldots, \overline{\psi_{k,L_k-1}}\}_{k<K}$. Part (c) of Theorem 8 now gives the desired PCK_p^1 refutation.

The proof for the case of $\mathrm{PCK}_{\mathbb{F}_p}^1$ is carried out in much the same way, with all the obvious changes involved in moving from the boolean to the polynomial setting. We leave the details to the reader. □

By exploiting the fact that $T_2(\oplus_p)$ is actually conservative over $\mathrm{APC}_2^{\oplus_p\mathrm{P}}$ rather than just $T_3^{\oplus_p\mathrm{P}}$, we can bring the collapse down to an even weaker proof system at the cost of introducing additional axioms related to weak pigeonhole principles.

Theorem 28 *Let φ be a $\Sigma_2(\oplus_p^-)$ formula of the form $\bigvee_{k<K}\bigwedge_{\ell<L_k}\psi_{k,\ell}$, where the $\psi_{k,\ell}$ are $\oplus_p^-$ formulas. Assume φ has Σ-size S and is provable by a depth d $\mathrm{PK}_{\oplus_p}$ proof of size S.*

Then, for some constant $e \in \mathbb{N}$ dependent only on d, there is a term $t = O(S^{\log^e S})$ and a Σ-size $S^{\log^e S}$ tree-like PCK_p^0 refutation of the set of cedents

$$\{\{\overline{\psi_{0,0}},\ldots,\overline{\psi_{0,L_0-1}}\},\ldots,\{\overline{\psi_{K-1,0}},\ldots,\overline{\psi_{K-1,L_{K-1}-1}}\}\}\cup\{f(u)\neq c\}_{u<t},$$

where f is a $\mathrm{PV}_2^{\oplus_p\mathrm{P}}$ function (depending on d, φ and the depth d $\mathrm{PK}_{\oplus_p}$ proof of φ) with oracle access to the variables of φ, c is an element below t^2 represented by $2\log t$ new variables standing for its bits, and $f(u)\neq c$ is a set of cedents expressing in a natural way that $f(u)$ does not evaluate to c.

An analogous result holds with $\overline{\psi_{k,\ell}}$ replaced by $\overline{\psi_{k,\ell}}^{\mathbb{F}_p}$ and tree-like PCK_p^0 replaced by tree-like $\mathrm{PCK}_{\mathbb{F}_p}^0$.

Proof $\mathrm{APC}_2^{\oplus_p\mathrm{P}}(\alpha,\beta,\gamma)$ proves 2-Ref(d-$\mathrm{PK}_{\oplus_p}$). Since $S_2^{2,\oplus\mathrm{P}}$ proves the equivalence of the $a\twoheadrightarrow a(1+1/|a|)$ version of sWPHP($\mathrm{PV}_2^{\oplus_p\mathrm{P}}$) with parameters and the $a\twoheadrightarrow a^2$ version without parameters [41, 24], we have

$$S_2^{2,\oplus\mathrm{P}}(\alpha,\beta,\gamma)\vdash[\forall v{<}t^2\,\exists u{<}t\,f(u)=v]\vee 2\text{-Ref}(d\text{-}\mathrm{PK}_{\oplus_p}),$$

where f is a fixed $\mathrm{PV}_2^{\oplus_p\mathrm{P}}(\alpha,\beta,\gamma)$ function depending on d, and t is a term involving the free variables a,b of 2-Ref(d-$\mathrm{PK}_{\oplus_p}$). By the $\forall\Sigma_2^{b,\oplus_p\mathrm{P}}$-conservativity of $S_2^{2,\oplus\mathrm{P}}$ over $T_2^{1,\oplus\mathrm{P}}$, the same formula is provable in $T_2^{1,\oplus\mathrm{P}}(\alpha,\beta,\gamma)$.

Arguing as in the proof of Theorem 26 with part (c) of Theorem 8 replaced by part (e), we obtain a quasipolynomial Σ-size tree-like PCK_p^0 refutation of

$$\{\{\overline{\psi_{0,0}},\ldots,\overline{\psi_{0,L_0-1}}\},\ldots,\{\overline{\psi_{K-1,0}},\ldots,\overline{\psi_{K-1,L_{K-1}-1}}\}\}\cup\{f(u)\neq m\}_{u<t},$$

for each concrete value of $m<t^2$. Such a refutation can be transformed into a proof of the cedent $c\neq m$ from

$$\{\{\overline{\psi_{0,0}},\ldots,\overline{\psi_{0,L_0-1}}\},\ldots,\{\overline{\psi_{K-1,0}},\ldots,\overline{\psi_{K-1,L_{K-1}-1}}\}\}\cup\{f(u)\neq c\}_{u<t}.$$

However, the cedent

$$c = 0, \ldots, c = t^2 - 1$$

has a quasipolynomial Σ-size tree-like PCK^0_p proof. Combining this proof with those of the $c \neq m$ cedents gives the desired refutation.

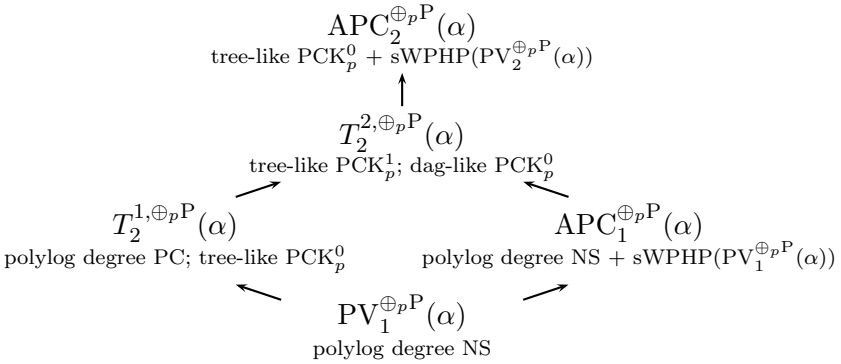
As before, the polynomial case is similar to the boolean case. □

The reason why Theorem 28 is stated in terms of tree-like PCK^0_p and $\mathrm{PCK}^0_{\mathbb{F}_p}$ rather than polylog degree Polynomial Calculus is that the negated sWPHP(PV_2) principle, even without parameters, is a $\forall\Sigma^b_2$- rather than $\forall\Sigma^b_1$ statement. However, over T^1_2, full sWPHP(PV_2) is actually conservative over the so-called retraction weak pigeonhole principle rWPHP(PV_2), which states that for PV_2 functions $f : t^2 \to t$ and $g : t \to t^2$, $g \circ f$ cannot be the identity. Negating the parameter-free version of rWPHP(PV_2) does give a $\forall\Sigma^b_1$ statement. Therefore, negations of $\Sigma_1(\oplus^-_p)$ formulas provable in constant depth $\mathrm{PK}_{\oplus_p}$ do have quasipolynomially longer refutations in the Polynomial Calculus with additional axioms corresponding to rWPHP($\mathrm{PV}_2^{\oplus_p \mathrm{P}}$).

Unfortunately, these axioms seem less natural than those corresponding to sWPHP($\mathrm{PV}_2^{\oplus_p \mathrm{P}}$), mainly because in the $\forall\Sigma^{b,\oplus_p \mathrm{P}}_1$ statement of negated rWPHP($\mathrm{PV}_2^{\oplus_p \mathrm{P}}$), the initial universal block has to contain a quantifier over claimed witnesses to Yes answers of the Σ^b_1 oracle in the computation of f and g. For this reason, we chose to formulate Theorem 28 only in the sWPHP version, leaving the rWPHP variant to the interested reader.

6 Lower bounds and speculation

The picture below presents part of the hierarchy of subtheories of $T_2(\oplus_p, \alpha)$ which remains intact in the wake of Theorem 22 and its corollaries. The proof systems corresponding to these theories are what remains of the hierarchy of subsytems of bounded depth Frege with mod p gates, at least if one is content with quasipolynomial simulations and considers only low complexity tautologies.



The sWPHP($\mathrm{PV}_2^{\oplus_p\mathrm{P}}(\alpha)$) axioms in the proof system corresponding to $\mathrm{APC}_2^{\oplus_p\mathrm{P}}(\alpha)$ are formulated as in Theorem 28. The system NS + sWPHP($\mathrm{PV}_1^{\oplus_p\mathrm{P}}(\alpha)$) is defined in a similar way; note that the statement that an element c is not in the range of a relativized $\mathrm{PV}_1^{\oplus_p\mathrm{P}}$ function on a given bounded domain can be expressed as a system of polynomials. The correspondence between $\mathrm{APC}_1^{\oplus_p\mathrm{P}}(\alpha)$ and polylog degree proofs in NS + sWPHP($\mathrm{PV}_1^{\oplus_p\mathrm{P}}(\alpha)$) follows from Theorem 12 part (d′) by an argument similar to the proof of Theorem 28.

The obvious question is how much of the picture consists of systems/theories for which we have lower bounds/relevant independence results. In terms of bounded arithmetic theories with C_p^k quantifiers, the best results we are aware of are as follows.

Theorem 29 *The pigeonhole principle* $\mathrm{PHP}_a^{a+1}(\alpha)$ *is independent from:*

(a) $T_2^{1,\oplus_p\mathrm{P}}(\alpha)$,

(b) $\mathrm{PV}_1^{\oplus_p\mathrm{P}}(\alpha) + \mathrm{sWPHP}(\mathrm{PV}_1(\alpha))$.

Note that the theory in part (b), unlike $\mathrm{APC}_1^{\oplus_p\mathrm{P}}(\alpha)$, contains the sWPHP only for polynomial time functions that do not make parity queries. Here $\mathrm{PHP}_a^{a+1}(\alpha)$ is the principle:

$$(\exists x{<}a{+}1)\neg(\mathsf{C}_p^1 y{<}a)\alpha(x,y)$$
$$\vee\,[\exists x_1{<}x_2{<}a{+}1\;\exists y{<}a(\alpha(x_1,y)\wedge\alpha(x_2,y))]$$
$$\vee\,[\exists x{<}a{+}1\;\exists y_1{<}y_2{<}a(\alpha(x,y_1)\wedge\alpha(x,y_2))].$$

The idea for the proof of Theorem 29 is to use the correspondence of Theorem 12 together with already known lower bounds for the polynomial calculus and the Nullstellensatz. For part (a) this is immediate. Part (b) requires some additional proof.

Proof Part (a) follows immediately from Theorem 12 and the linear degree lower bounds on refutations of ¬PHP in the Polynomial Calculus [39].

We sketch the argument for (b) assuming some some familiarity with switching lemma-based methods of proving lower bounds for PHP, as presented in [7], which also contains the Nullstellensatz degree lower bound that we use. If $\mathrm{PV}_1^{\oplus_p \mathrm{P}}(\alpha) + \mathrm{sWPHP}(\mathrm{PV}_1(\alpha))$ proves $\mathrm{PHP}_a^{a+1}(\alpha)$, then arguing as in the proof of Theorem 28, we obtain

$$\mathrm{PV}_1^{\oplus_p \mathrm{P}}(\alpha) \vdash \forall a\,[(\forall v{<}t^2\,\exists u{<}t\, f(u) = v) \vee \mathrm{PHP}_a^{a+1}(\alpha)],$$

where $t(a)$ is a term and f is a $\mathrm{PV}_1(\alpha)$ function. By Theorem 12, this means that for every $n \in \mathbb{N}$ there is a polylogarithmic degree Nullstellensatz refutation of

$$\{[\![c \neq f(u)]\!]\}_{u<t(n)} \cup \neg\mathrm{PHP}_n^{n+1},$$

where PHP_n^{n+1} is the Paris-Wilkie translation of $\mathrm{PHP}_a^{a+1}(\alpha)$, and c is represented by $2\log t(n)$ variables standing for its bits. The refutation remains valid if we substitute bits of a concrete $m < t^2(n)$ for the variables of c. However, we prove that given a term t, a $\mathrm{PV}_1(\alpha)$ function f, and a suitably chosen $\ell = \epsilon \log n$, for sufficiently large n there exists $m < t^2(n)$ such that Nullstellensatz refutations of

$$\{[\![m \neq f(u)]\!]\}_{u<t(n)} \cup \neg\text{onto-PHP}_n^{n+p^\ell} \tag{28}$$

require degree $n^{\Omega(1)}$. Here $\text{onto-PHP}_n^{n+p^\ell}$ is the propositional translation of the first-order statement which rules out that α maps $n + p^\ell$ pigeons bijectively onto n holes:

$$\begin{aligned}(\exists x < n{+}p^\ell)\neg(\mathsf{C}_p^1 y < n)\alpha(x,y) \vee (\exists y < n)\neg(\mathsf{C}_p^1 x < n{+}p^\ell)\alpha(x,y)\\ \vee[\exists x_1{<}x_2{<}n{+}p^\ell\,\exists y{<}n(\alpha(x_1,y) \wedge \alpha(x_2,y))]\\ \vee[\exists x{<}n{+}p^\ell\,\exists y_1{<}y_2{<}n(\alpha(x,y_1) \wedge \alpha(x,y_2))].\end{aligned}$$

Note this is weaker than $\mathrm{PHP}_{n+p^\ell-1}^{n+p^\ell}$.

Assume that for each m there is a refutation of (28) of degree d. We wish to prove that $d = n^{\Omega(1)}$. For a string w representing oracle answers in a possible computation of f, let C_w be the polylogarithmic width clause which is true exactly if w is *not* the string of oracle answers actually obtained. Abusing notation, we also write C_w for the multilinear polynomial which is 0 exactly if the clause is true. For each m and u, $[\![m \neq f(u)]\!]$ is the sum of C_w over all w which lead a computation of $f(u)$ to output m. Modify the

Nullstellensatz refutation by replacing this sum by the individual terms C_w; this can be done without increasing the degree.

Consider the set $\widetilde{C_w}$ which contains a monomial/clause corresponding to each minimal partial matching from $n + p^\ell$ to n that matches the pigeons and holes appearing in w and would cause w to be given as the set of oracle answers during a computation of f. (For instance, if w is the string of length two containing $\alpha(1,1)$ and $\neg\alpha(2,3)$, and the variable $x_{i,j}$ is used to represent $\alpha(i,j)$, then C_w in its polynomial form is $x_{1,1}(1 - x_{2,3})$, while $\widetilde{C_w}$ contains each monomial of the form $x_{1,1}x_{2,k}$ for $k \in \{0, \ldots, n-1\} \setminus \{1,3\}$.) Each C_w can be obtained from $\widetilde{C_w} \cup \neg\text{onto-PHP}_n^{n+p^\ell}$ by a polylog(n) degree Nullstellensatz refutation. It follows that $\neg\text{onto-PHP}_n^{n+p^\ell}$ together with $\widetilde{C_w}$ for every w yielding $f(u) = m$ for some u has a $d + \text{polylog}(n)$ degree refutation R_m.

The formula

$$\bigvee_{v<t^2(n)} \bigwedge_{u<t(n)} f(u) \neq v \tag{29}$$

has a quasipolynomial size constant depth Frege proof P [35, 32]. Let ρ be a partial restriction (partial matching) which leaves n^δ holes free and assigns to each subformula of a formula in P a matching decision tree of height n^γ, $\gamma < \delta$, in a way consistent with Definition 4.1 of [7]. Since (29) is provable, all branches of its tree must be labeled "True". This means that we can choose some partial matching π of size $\leq n^\gamma$ such that for some concrete m, $\rho\pi$ selects a specific "True" branch in the tree assigned to

$$\bigwedge_{u<t(n)} f(u) \neq m.$$

Consider the effect of $\rho\pi$ on the refutation R_m. For every $u < t(n)$ and every w leading $f(u)$ to output m, each monomial in $\widetilde{C_w}$ becomes 0 under $\rho\pi$. On the other hand, $\neg\text{onto-PHP}_n^{n+p^\ell} \restriction_{\rho\pi}$ is essentially $\neg\text{onto-PHP}_{n^\delta - n^\gamma}^{n^\delta - n^\gamma + p^\ell}$. Thus, $\neg\text{onto-PHP}_{n^\delta - n^\gamma}^{n^\delta - n^\gamma + p^\ell}$ has a refutation of degree $d + \text{polylog}(n)$. However, by Theorem 8.1 of [7], for a well chosen $\ell = \epsilon \log n$ any refutation of $\neg\text{onto-PHP}_{n^\delta - n^\gamma}^{n^\delta - n^\gamma + p^\ell}$ must have degree $n^{\Omega(1)}$. Thus, $d = n^{\Omega(1)}$. □

It seems conceivable that part (b) could be extended by similar methods to the unprovability of $\text{PHP}_a^{a+1}(\alpha)$ in $T_2^{1,\oplus_p\text{P}}(\alpha) + \text{sWPHP}(\text{PV}_2(\alpha))$. The part that appears to be missing is a degree lower bound on Polynomial Calculus proofs of the onto version of $\text{PHP}_n^{n+p^\ell}$, as opposed to the general PHP.

On the other hand, it is less clear how to obtain nontrivial independence results for fragments of $\mathrm{APC}_2^{\oplus_p \mathrm{P}}(\alpha)$, or even $\mathrm{APC}_1^{\oplus_p \mathrm{P}}(\alpha)$, which contain the sWPHP for functions involving the parity quantifier. We expand on this for the case of $\mathrm{APC}_1^{\oplus_p \mathrm{P}}(\alpha)$. On the propositional level, this corresponds to polylog degree Nullstellensatz with axioms for $\mathrm{sWPHP}(\mathrm{PV}_1^{\oplus_p \mathrm{P}})$.

Given some tautology τ of size $\mathrm{poly}(n)$ whose negation is expressible by a set of $\mathrm{polylog}(n)$ degree polynomials, consider potential approaches to showing that there is no polylog degree Nullstellensatz refutation of

$$\{[\![c \neq f(u)]\!]\}_{u<t(n)} \cup \neg\tau,$$

where t is a term, c is represented by $2\log t(n)$ variables standing for its bits, and f is now a function from $\mathrm{PV}_1^{\oplus_p \mathrm{P}}(\alpha)$, as opposed to $\mathrm{PV}_1(\alpha)$. Since the translations of $c \neq f(u)$ now involve the $\oplus_p$ connective, we cannot apply switching lemma arguments to them. The usefulness of standard, "design"-based lower bound methods for Nullstellensatz in dealing with the $[\![c \neq f(u)]\!]$ polynomials is not evident.

One remarkable feature of the $[\![c \neq f(u)]\!]$ axioms is their probabilistic properties. These axioms involve polylogarithmically many new variables (the bits of c) in addition to the variables of τ, and for each assignment to the old variables, almost all assignments to the new variables (a $1 - 1/t(n)$ fraction) make all the $[\![c \neq f(u)]\!]$ true. Thus, it might be tempting to search for some τ hard for "randomized Nullstellensatz", a "proof system" allowed to use additional axioms which involve polylogarithmically many new variables and are "almost always true" under any assignment to the old variables.

In fact, [17] proposes to study a similarly randomized version of low width resolution, in the hope of obtaining separations for some interesting fragments of (non-modular counting) $\mathrm{APC}_2(\alpha)$. Dershowitz and Tzameret [21] study promise proof systems which are another approach to randomized proof systems.

Unfortunately, the next proposition shows that "randomized Nullstellensatz" has low degree proofs of all tautologies, thus depriving us of the one potentially promising line of attack on Nullstellensatz with the $[\![c \neq f(u)]\!]$ axioms.

Proposition 30 *Let $\{p_i : i < n\}$ be an unsatisfiable sequence of polynomials over $\mathbb{F}_p$, each of degree at most d. Let $t = t(n, 2^d)$ be quasipolynomial in n and 2^d. There exists an $\mathbb{F}_p$ polynomial q such that:*

(a) q has $\mathrm{poly}(\log n, d)$ new variables in addition to those of the p_i's,

(b) $\deg(q) \leq \mathrm{poly}(\log n, d)$,

(c) for any assignment to the variables of the p_i's, q equals 0 for all but a $1/t$ fraction of the assignments to the new variables,

(d) $\{p_i : i < n\} \cup \{q\}$ has a Nullstellensatz refutation over $\mathbb{F}_p$ of degree $\mathrm{poly}(\log n, d)$.

Proof The construction of the additional axiom q essentially mimics the Valiant-Vazirani construction and the proof that $\exists \cdot \oplus \mathrm{P} \subset \mathrm{BP} \cdot \oplus_p \mathrm{P}$ described in Section 4.2. For simplicity, we only sketch the construction for $p = 2$. The case of general p involves additional uses of the "$p-1$ copies" and negation transformations as described in the proof of Lemma 19.

First, for $\log^2 n + O(\log n)$ new variables $\vec{r}$, to be interpreted as a number $j \leq \log n$ and $3 + \log n$ many $\log n$-bit vectors $v_1, \ldots, v_{3+\log n}$, and for $i < n$, let $q_{\vec{r},i}$ be the (multilinearized) polynomial which is equal to 1 exactly if p_i equals 1 and each of $v_1, \ldots, v_{j+3}$ is orthogonal to i, interpreted as a $\log n$-bit vector. The degree of $q_{\vec{r},i}$ is at most $d + O(\log n)$.

Let $q_{\vec{r}}$ be $1 + \sum_{i<n} q_{\vec{r},i}$. By the proof of Lemma 18 and the unsatisfiability of $\{p_i : i < n\}$, for any given assignment to the variables of the p_i, at least a $1/O(\log n)$ fraction of assignments to the new variables makes q_r equal 0. To amplify this probability to $1 - 1/t$, take a sufficiently large (but polynomial in $\log n$ and d) number of disjoint tuples of variables $\vec{r}$ and let q be $\prod_{\vec{r}} q_{\vec{r}}$.

We leave the simple verification that q also satisfies property (d) to the reader. The key point is that each $q_{\vec{r},i}$ is a multiple of p_i; hence, the $q_{\vec{r},i}$'s are readily derivable from the p_i's. □

References

[1] M. Ajtai, Σ^1_1*-formulae on finite structures*, Annals of Pure and Applied Logic, 24 (1983), pp. 1–48.

[2] ——, *The complexity of the pigeonhole principle*, in Proceedings of the 29-th Annual IEEE Symposium on Foundations of Computer Science, 1988, pp. 346–355.

[3] E. Allender and U. Hertrampf, *Depth reduction for circuits of unbounded fan-in*, Information and Computation, 112 (1994), pp. 217–238.

[4] S. Arora and B. Barak, *Computational Complexity: A Modern Approach*, Cambridge University Press, 2009.

[5] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák, *Lower bounds on Hilbert's Nullstellensatz and propositional proofs*, Proceedings of the London Mathematical Society, 73 (1996), pp. 1–26.

[6] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, P. Pudlák, and A. Woods, *Exponential lower bounds for the pigeonhole principle*, in Proceedings of the 24-th Annual ACM Symposium on Theory of Computing, 1992, pp. 200–220.

[7] P. Beame and S. Riis, *More on the relative strength of counting principles*, in Proof Complexity and Feasible Arithmetics, P. Beame and S. Buss, eds., American Mathematical Society, 1997, pp. 13–36.

[8] A. Beckmann and S. R. Buss, *Separation results for the size of constant-depth propositional proofs*, Annals of Pure and Applied Logic, 136 (2005), pp. 30–55.

[9] ——, *Corrected upper bounds for free-cut elimination*, Theoretical Computer Science, 412 (2011), pp. 5433–5445.

[10] ——, *Improved witnessing and local improvement principles for second-order bounded arithmetic*. To appear in ACM Transactions on Computational Logic, 2014.

[11] R. Beigel and J. Tarui, *On ACC*, Computational Complexity, 4 (1994), pp. 350–366.

[12] S. R. Buss, *Bounded Arithmetic*, Bibliopolis, 1986. Revision of 1985 Princeton University Ph.D. thesis.

[13] ——, *Axiomatizations and conservation results for fragments of bounded arithmetic*, in Logic and Computation, proceedings of a Workshop held Carnegie-Mellon University, 1987, vol. 106 of Contemporary Mathematics, American Mathematical Society, 1990, pp. 57–84.

[14] ——, *Bounded arithmetic and propositional proof complexity*, in Logic of Computation, H. Schwichtenberg, ed., Springer-Verlag, Berlin, 1997, pp. 67–121.

[15] ——, *First-order proof theory of arithmetic*, in Handbook of Proof Theory, S. R. Buss, ed., North-Holland, 1998, pp. 79–147.

[16] S. R. Buss, R. Impagliazzo, J. Krajíček, P. Pudlák, A. A. Razborov, and J. Sgall, *Proof complexity in algebraic systems and bounded depth Frege systems with modular counting*, Computational Complexity, 6 (1996/1997), pp. 256–298.

[17] S. R. Buss, L. A. Kołodziejczyk, and N. Thapen, *Fragments of approximate counting.* Submitted for publication, 2012.

[18] S. R. Buss and J. Krajíček, *An application of Boolean complexity to separation problems in bounded arithmetic*, Proc. London Math. Society, 69 (1994), pp. 1–21.

[19] M. Clegg, J. Edmonds, and R. Impagliazzo, *Using the Groebner basis algorithm to find proofs of unsatisfiability*, in Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing, 1996, pp. 174–183.

[20] S. A. Cook, *Feasibly constructive proofs and the propositional calculus*, in Proceedings of the Seventh Annual ACM Symposium on Theory of Computing, 1975, pp. 83–97.

[21] N. Dershowitz and I. Tzameret, *Complexity of propositional proofs under a promise*, ACM Transactions on Computational Logic, 11 (2010), pp. 1–29.

[22] M. Furst, J. B. Saxe, and M. Sipser, *Parity, circuits and the polynomial-time hierarchy*, Math. Systems Theory, 17 (1984), pp. 13–27.

[23] J. Håstad, *Almost Optimal Lower Bounds for Small Depth Circuits*, vol. 5 of Advances in Computing Research, JAI Press, 1989, pp. 143–170.

[24] E. Jeřábek, *Dual weak pigeonhole principle, boolean complexity, and derandomization*, Annals of Pure and Applied Logic, 124 (2004), pp. 1–37.

[25] ——, *The strength of sharply bounded induction*, Mathematical Logic Quarterly, 6 (2006), pp. 613–624.

[26] ——, *Approximate counting in bounded arithmetic*, Journal of Symbolic Logic, 72 (2007), pp. 959–993.

[27] ——, *Approximate counting by hashing in bounded arithmetic*, Journal of Symbolic Logic, 74 (2009), pp. 829–860.

[28] J. Krajíček, *Lower bounds to the size of constant-depth propositional proofs*, Journal of Symbolic Logic, 59 (1994), pp. 73–86.

[29] ——, *Bounded Arithmetic, Propositional Calculus and Complexity Theory*, Cambridge University Press, Heidelberg, 1995.

[30] ——, *Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic*, Journal of Symbolic Logic, 62 (1997), pp. 457–486.

[31] A. Maciel and T. Pitassi, *Towards lower bounds for bounded-depth Frege proofs with modular connectives*, in Proof Complexity and Feasible Arithmetics, P. W. Beame and S. R. Buss, eds., American Mathematical Society, 1998, pp. 195–227.

[32] A. Maciel, T. Pitassi, and A. R. Woods, *A new proof of the weak pigeonhole principle*, Journal of Computer and System Sciences, 64 (2002), pp. 843–872.

[33] J. B. Paris and A. J. Wilkie, Δ_0 *sets and induction*, in Open Days in Model Theory and Set Theory, W. Guzicki, W. Marek, A. Pelc, and C. Rauszer, eds., 1981, pp. 237–248.

[34] ——, *Counting problems in bounded arithmetic*, in Methods in Mathematical Logic, Lecture Notes in Mathematics #1130, Springer-Verlag, 1985, pp. 317–340.

[35] J. B. Paris, A. J. Wilkie, and A. R. Woods, *Provability of the pigeonhole principle and the existence of infinitely many primes*, Journal of Symbolic Logic, 53 (1988), pp. 1235–1244.

[36] C. Pollett, *Structure and definability in general bounded arithmetic theories*, Annals of Pure and Applied Logic, 100 (1999), pp. 189–245.

[37] A. A. Razborov, *Lower bounds on the size of bounded depth networks over a complete basis with logical addition*, Matematicheskie Zametki, 41 (1987), pp. 598–607. English translation in *Mathematical Notes of the Academy of Sciences of the USSR* 41 (1987) 333-338.

[38] ——, *On provably disjoint NP-pairs*, Tech. Report RS-94-36, Basic Research in Computer Science Center, Aarhus, Denmark, November 1994. http://www.brics.dk/index.html.

[39] ——, *Lower bounds for the polynomial calculus*, Computational Complexity, 7 (1998), pp. 291–324.

[40] R. Smolensky, *Algebraic methods in the theory of lower bounds for Boolean circuit complexity*, in Proceedings of the Nineteenth Annual ACM Symposium on the Theory of Computing, ACM Press, 1987, pp. 77–82.

[41] N. Thapen, *A model-theoretic characterization of the weak pigeonhole principle*, Annals of Pure and Applied Logic, 118 (2002), pp. 175–195.

[42] ——, *Higher complexity search problems for bounded arithmetic and a formalized no-gap theorem*, Archive for Mathematical Logic, 50 (2011), pp. 665–680.

[43] S. Toda, *PP is as hard as the polynomial-time hierarchy*, SIAM Journal on Computing, 20 (1991), pp. 865–877.

[44] L. G. Valiant and V. V. Vazirani, *NP is a easy as detecting unique solutions*, Theoretical Computer Science, 47 (1986), pp. 85–93.

[45] A. C.-C. Yao, *On ACC and threshold circuits*, in Proc. 31st IEEE Symp. on Foundations of Computer Science (FOCS), 1990, pp. 619–627.