Collapsing Modular Counting in Bounded Arithmetic and Constant Depth Propositional Proofs

Sam Buss

joint work with L. Kołodziejczyk and K. Zdanowski

Limits of Theorem Proving
Rome, Italy
September 2012

$\mathrm{AC}^0[p]$ circuits and proofs

Fix an integer $m \geq 2$.

Definition. $\mathbf{AC^0[m]}$ **circuits** are *constant depth* circuits for computing boolean functions.

- Literals and constants: x, $\overline{x}$, $\top$ (*True*), $\bot$ (*False*).
- Unbounded fanin connectives: $\wedge$, $\vee$, $\oplus_m$.

- $\oplus_m(\vec{x}) =$ *True* iff the number of true arguments is $\equiv 0 \bmod m$.

Definition. An $\mathbf{AC^0[m]}$ **proof** is a propositional proof in which each line is an $\mathrm{AC}^0[m]$-circuit (equivalently: is an $\mathrm{AC}^0[m]$-formula).

We are mostly interested in the case where m is equal to a prime p. We call $\mathrm{AC}^0[p]$ proofs **constant depth** $\mathrm{PK}_{\oplus_p}$ **proofs**.

Theorem [Beigel-Tarui'94, see also Allender-Hertrampf'94, Toda'91, Yao, ...]. Let $m \geq 2$. An $\mathrm{AC}^0[m]$ circuit of size S can be converted into a quasipolynomial-size depth three formula consisting of a symmetric gate applied to $\oplus_m$-gates applied to polylogarithmic size conjunctions of literals.

This expressive power of quasipolynomial size, depth three formulas, carries over to the power of propositional proofs:

Theorem [Maciel-Pitassi'98] Let $m = p^k$, a prime power. $\mathrm{AC}^0[p^k]$ proofs can be quasipolynomially simulated by proofs in which every line is a depth three formula formed from a threshold gate applied to $\oplus_m$ gates of polylogarithmic size conjunctions.

Recall: The "quasipolynomial simulation" means there is a $2^{\log^{O(1)} n}$-time procedure to thusly convert $\mathrm{AC}^0[p^k]$ proofs.

Open: Does this hold for composite m as well?

Collapsing $\mathrm{AC}^0[p]$ without threshold gates

Theorem. [Allender-Hertrampf'94] Let p be prime. An $\mathrm{AC}^0[p]$ circuit of size S can be converted into a quasipolynomial-size depth 4 circuit formed as disjunctions ($\vee$'s) of conjunctions ($\wedge$'s) of $\oplus_p$-gates of polylogarithmic conjunctions of literals.

Theorem A. [BKZ - this talk]
Let p be prime. Constant depth $\mathrm{PK}_{\oplus_p}$ proofs ($\mathrm{AC}^0[p]$ proofs) can be quasipolynomially simulated by Tait-style propositional proofs in which each formula is a (subformula of a) depth three formula formed as a conjunction applied to $\oplus_p$ gates of polylogarithmic size conjunctions.

Remainder of the talk will outline the proof.

- Constant-depth proof systems with $\oplus_p$ connectives.
- Fragments of bounded arithmetic with approximate counting.
- Valiant-Vazirani and Toda theorems.
- A collapse of bounded arithmetic with modular counting.
- Paris-Wilkie translations.
- Reflection principles.
- Precise statement of simulation results.
- Concluding questions.

Tait-style systems $\mathrm{PK}_{\oplus_p}$

The lines of a Tait-calculus proof are **cedents**, sets of formulas which are interpreted as their disjunction. The system, PK, with connectives $\wedge$ and $\vee$ has the rules of inference:

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

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

where $i_0 \in I$.
- $\overline{\varphi}$ is the De-Morgan negation of ϕ.

For counting mod p, we use $2p$ many connectives $\oplus_p^k$ and $\bar{\oplus}_p^k$ which are true (resp.) false when the number of true inputs is $\equiv k \bmod p$.

The system has the same rules of inference as PK, plus the initial cedents:

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

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

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

By convention, “$\oplus_p^{k+\ell}$” means “$\oplus_p^{(k+\ell) \bmod p}$”.

Constant depth $\mathrm{PK}_{\oplus_p}$ and PCK^i_p

Constant depth $\mathbf{PK}_{\oplus_\mathbf{p}}$ proofs allow $\wedge$'s, $\vee$'s, and $\oplus_p$ gates to appear at any level. **$\mathbf{PCK}^\mathbf{i}_\mathbf{p}$ proofs** are depth $i+1\frac{1}{2}$ proofs in which the inputs to $\oplus_p$ gates are restricted to be conjunctions of literals:

Definition. For $i \geq 0$, a **$\mathbf{PCK}^\mathbf{i}_\mathbf{p}$ proof** contains literals, conjunctions of literals, disjunctions of literals, and formulas that have $\leq i$ alternating levels of conjunctions and disjunctions above $\oplus^j_p$ and $\bar{\oplus}^j_p$ gates, which are applied only to "small" conjunctions of literals.

Remark: It is also possible to work over finite fields of characteristic p, and replace the $\oplus_p$ gates with low-degree polynomials. The resulting system corresponding to PCK^i_p is denoted $\mathrm{PCK}^i_{\mathbb{F}_p}$. Similar results hold for $\mathrm{PCK}^i_{\mathbb{F}_p}$ as for PCK^i_p; this talk discusses only the propositional systems PCK^i_p however.

Recall that Theorem A gives a translation from constant depth $\mathrm{PK}_{\oplus_p}$ proofs into PCK_p^1 proofs.

For this, the size of PCK_p^i proofs is measured in terms of "Σ-size".

Definition. The **Σ-size** of a PCK_p^i proof P is $\le S$ provided there are $\le S$ formulas in P, each of size $\le S$ symbols, and every conjunction or disjunction of literals in P has size $\le \log S$.

Bounded arithmetic: subtheories of Peano arithmetic.

Bounded arithmetic theories have close connections with low-level complexity classes, but more relevantly for this talk, proofs in bounded arithmetic can be viewed as **uniform versions of constant depth proofs** via the Paris-Wilkie translation.

Function symbols: all polynomial time functions and relations.
Bounded quantifiers: $(\forall x{\le}t)$ and $(\exists x{\le}t)$.
Sharply bounded quantifiers: $(\forall x{\le}|t|)$ and $(\exists x{\le}|t|)$

Classes $\boldsymbol{\Sigma^b_i}$ and $\boldsymbol{\Pi^b_i}$ are the formulas containing $\le i$ alternating blocks of bounded quantifiers, ignoring sharply bounded quantifiers.

The **strict** classes, $\boldsymbol{\hat\Sigma^b_i}$ and $\boldsymbol{\hat\Pi^b_i}$, require prenex form, and disallow sharply bounded quantifiers outside of bounded quantifiers.

$\mathbf{T^i_2}$ is axiomatized with induction for all Σ^b_i- and Π^b_i-formulas.

Modular counting quantifiers

Fix a prime p. The syntax of bounded arithmetic is now augmented with **modular counting quantifiers** $\mathrm{C}_{\mathbf{p}}^{\mathbf{k}}$, for $0 \le k < p$. The meaning of

$$(\mathrm{C}_p^k x{\le}t)A(x)$$

is that the number of $x \le t$ such that $A(x)$ is $\equiv k \bmod p$.
The axioms for the C_p^k quantifiers are:

$$A(0) \rightarrow (\mathrm{C}_p^1 x \le 0)A(x) \qquad \neg A(0) \rightarrow (\mathrm{C}_p^0 x \le 0)A(x)$$

$$A(t+1) \wedge (\mathrm{C}_p^k x \le t)A(x) \rightarrow (\mathrm{C}_p^{k+1} x \le t{+}1)A(x)$$

$$\neg A(t+1) \wedge (\mathrm{C}_p^k x \le t)A(x) \rightarrow (\mathrm{C}_p^k x \le t{+}1)A(x)$$

$$\neg[(\mathrm{C}_p^k x \le t)A(x) \wedge (\mathrm{C}_p^\ell x \le t)A(x)] \qquad \text{for } k \ne \ell \pmod{p} \ .$$

The $(\mathrm{C}_p^k{\le}\cdots)$ quantifiers above are considered bounded and may appear in bounded formulas. Notation: $\Sigma_\infty^{b,\oplus_p\mathrm{P}}(\oplus_p)$.

Definition. The theory $\mathbf{T_2(\oplus_p)}$, equivalent to $\mathbf{S_2(\oplus_p)}$, has induction for *all* bounded formulas; i.e., allowing quantifiers $(\mathsf{C}_p^k x{\le}t)$ to appear in front of arbitrary bounded formulas.

Definition. A $\oplus_\mathbf{p}\mathrm{P}$**-formula** is atomic, or of the form $(\mathsf{C}_p^k x \le t)A(x)$ where A is a sharply bounded (so A polynomial time computable).
The $\boldsymbol{\hat{\Sigma}_i^{b,\oplus_p\mathrm{P}}}$ **and** $\boldsymbol{\hat{\Pi}_i^{b,\oplus_p\mathrm{P}}}$ **formulas** are defined by counting alternations of bounded $\exists/\forall$ quantifiers acting on $\oplus_p\mathrm{P}$ formulas, ignoring sharply bounded quantifiers.

Definition. The theory $\mathbf{T_2^{i,\oplus_p\mathrm{P}}}$ is axiomatized with the C_p^k axioms for $\oplus_p\mathrm{P}$ formulas and with induction for $\Sigma_i^{b,\oplus_p\mathrm{P}}$ formulas.
The C_p^k quantifiers can be syntactically restricted to appear only in $\oplus_p\mathrm{P}$ formulas.

In essence, C_p^k quantifiers appear only in $\oplus_p\mathrm{P}$ formulas for $T_2^{i,\oplus_p\mathrm{P}}$.

This condition can be relaxed somewhat:

Theorem. We have

$$\oplus_p\mathrm{P}^{\oplus_p\mathrm{P}} = \oplus_p\mathrm{P}.$$

In fact, any formula composed of sharply bounded quantifiers, bounded C_p^k quantifiers, boolean operations, and polynomial time predicates is equivalent to a $\oplus_p\mathrm{P}$ predicate.

Thus, the theories $T_2^{i,\oplus_p\mathrm{P}}$ are robustly defined.

Theorem B.

A lot more than that is true, however: The hierarchy of modular counting theories of bounded arithmetic collapses to the third level:

Theorem B. $T_2(\oplus_p)$ is conservative over $T_2^{3,\oplus_p\mathrm{P}}$. In fact, any $\Sigma^b_\infty(\oplus_p)$ formula (i.e., any bounded formula) is provably equivalent to a $\Sigma_2^{b,\oplus_p\mathrm{P}}$ formula.

Theorem B is one of the main ingredients for the proof of Theorem A. For its proof we introduce Jeřábek's bounded arithmetic theories for approximate counting.

Jeřábek's theories for approximate counting were axiomatized with the following, surjective, weak pigeonhole principle, **sWPHP(f)**:

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

Then, define (in the notation of [BKT]),

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

and

$$\mathrm{APC}_2 \;:=\; T^1_2 + \mathrm{sWPHP}(\mathrm{PV}_2).$$

PV_1 is the set of polynomial time functions.
PV_2 is the set of functions polynomial time relative to NP.

"APC" = "**AP**proximate **C**ounting"

We work with versions of APC_1 and APC_2 extended to include $\oplus_p\mathrm{P}$ predicates and functions:

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

and

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

$\mathrm{PV}_1^{\oplus_p\mathrm{P}}$: functions polynomial time relative to $\oplus_p\mathrm{P}$.
$\mathrm{PV}_2^{\oplus_p\mathrm{P}}$: functions that are polynomial time relative to $\mathrm{NP}^{\oplus_p\mathrm{P}}$.

Jeřábek showed that APC_1 can count the size of polynomial time sets to within a constant fraction ϵ.

Namely, let $X, Y \subseteq 2^n$ be defined by Boolean circuits. Roughly speaking the "size of X" can be defined to within an error tolerance of $\epsilon 2^n$.
Specifically, the relation $\mathbf{X} \preceq_\epsilon \mathbf{Y}$ can be defined expressing

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

where $\sqcup$ is disjoint union, where Log is the set of lengths, and where $\epsilon = 0$ or $\epsilon \in \mathrm{Log}$.

For APC_2, Jeřábek showed that the size of X can be approximated to within an error tolerance of $\epsilon|X|$.

Furthermore, APC_1 and APC_2 can prove many properties about approximate counting, including facts about union, intersection, some versions of exclusion/inclusion, Chebyshev inequalities, randomized computation, BPP, AM, MA, and so forth.

These constructions all relativize to $\mathrm{APC}_1^{\oplus_p \mathrm{P}}$ and $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$.

Formalized Valiant-Vazirani theorem

Theorem C. (in APC_2) There is a PV_1 function which, given a CNF formula φ over the propositional variables $\vec{q} = \langle q_1, \dots, q_n \rangle$ and a (randomly chosen) value r of length $(n+3)n + |n|$, outputs a CNF formula φ_r with the same variables $\vec{q}$ such that

$$\begin{aligned} \varphi \in \textsc{Sat} \quad &\Longrightarrow \quad \Pr_r[\neg\exists^1 b, b \models \varphi_r] \preceq_0 1 - \frac{1}{2^{|n|} \cdot 65}, \\ \varphi \notin \textsc{Sat} \quad &\Longrightarrow \quad \varphi_r \notin \textsc{Sat}. \end{aligned}$$

"$\mathbf{\exists^1 b}$" means there exists a **unique** b.
"$\mathbf{b \models \varphi_r}$" means that b codes a satisfying assignment for φ_r as a string of n bits.

The constant $1/65$ is not as good as in VV'86 due to the need to formalize the result in APC_2.

Definition. (in $\mathrm{APC}_1^{\oplus_p \mathrm{P}}$ or $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$). $\oplus_{\mathbf{p}}^{\mathbf{k}}\textsc{Sat}$ is the set of propositional formulas φ such that the number of satisfying assignments of φ is congruent to k mod p.

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

$$\begin{aligned} x \in L &\iff \Pr_{r<u(x)}[f(x,r) \notin \oplus_p^1\textsc{Sat}] \preceq_0 1/4, \\ x \notin L &\iff \Pr_{r<u(x)}[f(x,r) \notin \oplus_p^0\textsc{Sat}] \preceq_0 1/4. \end{aligned}$$

Amplification allows the constant $1/4$ to be improved to 2^{-n^c}.

Formalized Toda theorem in $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$

Theorem D. $T_2(\oplus_p)$ proves that any $\Sigma^b_\infty(\oplus_p)$ formula defines a property in $\mathrm{BP} \cdot \oplus_p \mathrm{P}$. Furthermore, these equivalences can be essentially expressed and proved in $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$.

Proof idea: The necessary probabilistic arguments can be carried out (with difficulty) in $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$*.*

Corollary. $T_2(\oplus_p)$, and in essence $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$, can prove the uniform analogue of the Allender-Hertrampf theorem about the collapse of $\mathrm{AC}^0[p]$.

Corollary E. $T_2(\oplus_p)$ is conservative over $\mathrm{APC}_2^{\oplus_p \mathrm{P}}$.

Since $T_2^{3,\oplus_p \mathrm{P}} \vDash \mathrm{APC}_2^{\oplus_p \mathrm{P}}$, we also get

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

Paris-Wilkie translation

Let $\varphi(\vec{x})$ be a bounded formula involving an oracle α.

The Paris-Wilkie translation of $\varphi(\vec{x})$ gives an infinite family of constant depth propositional formulas $[\![\varphi]\!]_{\vec{n}}$.

The propositional variables of $[\![\varphi]\!]_{\vec{n}}$ are x_i's indicating that $\alpha(i)$ is true.

The integer values $\vec{n}$ assign values to free variables $\vec{x}$ of φ.

Sharply bounded subformulas of φ become small depth (depth polylogarithmic in $\vec{n}$) decision trees in $[\![\varphi]\!]_{\vec{n}}$; expressed as a disjunction of small conjunctions.

$\oplus_p\mathrm{P}$ subformulas of φ become a $\oplus_p$ gate applied to small conjunctions.

Bounded quantifiers $(\exists x{\le}t)$ and $(\forall x{\le}t)$ in φ become big (quasipolynomial size in n) disjunctions or conjunctions $[\![\varphi]\!]_{\vec{n}}$.

Paris-Wilkie Theorem: (one of several forms)
Let $\varphi(x) \in \hat{\Sigma}_i^{b,\oplus_p\mathrm{P}}(\alpha)$ be a formula of the form

$$\varphi(x) \;:=\; (\exists y{\le}t(x))\,(\forall z{\le}s(x))\,\xi(x,y,z).$$

so $\xi(x,y,z) \in \hat{\Sigma}_{i-2}^{b,\oplus_p\mathrm{P}}(\alpha)$.

Express $\neg\varphi(x)$ as the set Ξ_n of $t(n)+1$ many cedents

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

where $0 \le m \le t(n)$. Each cedent in Ξ_n has $s(n)+1$ formulas.

Suppose $T_2^{i,\oplus_p\mathrm{P}}(\alpha) \vdash (\forall x)\varphi(x)$, $i \ge 2$. Then

> *The set of cedents Ξ_n has a dag-like PCK_p^{i-2} refutation P such that the Σ-size of P is quasipolynomial in n.*

A reflection theorem

The Reflection Principle, j-$\mathbf{Ref}$(d-$\mathrm{PK}_{\oplus_p}$)(α,β,γ):

> *If β codes a $\Sigma_j(\oplus_p^-)$ propositional formula φ, and α codes a depth d $\mathrm{PK}_{\oplus_p}$ proof of φ, then the truth assignment coded by γ satisfies φ.*

Note that α,β,γ are second-order, hence code exponentially large objects.
j-$\mathrm{Ref}(d$-$\mathrm{PK}_{\oplus_p})$ is a $\forall\Sigma_j^{b,\oplus_p\mathrm{P}}(\alpha,\beta,\gamma)$ formula.

Reflection Theorem: $T_2(\oplus_p)(\alpha,\beta,\gamma) \vdash j\text{-}\mathrm{Ref}(d\text{-}\mathrm{PK}_{\oplus_p})$.

Corollary: $T_2^{3,\oplus_p\mathrm{P}}(\alpha,\beta,\gamma) \vdash j\text{-}\mathrm{Ref}(d\text{-}\mathrm{PK}_{\oplus_p})$.

Proof idea: $T_2(\oplus_p)(\alpha,\beta,\gamma)$ can give a truth definition for the depth d formulas in the proof coded by α.

Theorem A'. Let φ be $\bigvee_{k<K} \bigwedge_{\ell<L_k} \psi_{k,\ell}$, where the $\psi_{k,\ell}$'s are $\Sigma_1(\oplus_p^-)$ (that is, PCK_p^1-formulas). Suppose φ has a depth d $\mathrm{PK}_{\oplus_p}$ proof of size $\le S$. 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.

Proof idea. Form the Paris-Wilkie translation of the reflection principle as provable in $T_2^{3,\oplus_p\mathrm{P}}(\alpha, \beta, \gamma)$.
This gives a PCK_p^1-proof Q.
In Q, substitute for the propositional variables describing values of α and β, the actual description of the proof P and the formula ψ.
Using the fact that β really codes a valid proof P of ψ, the resulting restriction simplifies the proof Q into the desired refutation of the above cedents. QED

Remark. It is possible to work with $\mathrm{APC}_2^{\oplus_p \mathrm{P}}(\alpha, \beta, \gamma)$ instead $T_2^{3, \oplus_p \mathrm{P}}(\alpha, \beta, \gamma)$.

This allows replacing the PCK_p^1 proof of Theorem A' with a PCK_p^0 proof, but at the cost of adding additional initial cedents that express the surjective weak pigeonhole principle.

Some questions

1. What does the collapse of $\mathrm{PK}_{\oplus_p}$ proofs imply about the possibility of proving superpolynomial lower bounds on the size of $\mathrm{PK}_{\oplus_p}$-proof (that is, $\mathrm{AC}^0[p]$-proofs)?
2. The theories $\mathrm{APC}_1^{\oplus_p\mathrm{P}}$ and $\mathrm{APC}_2^{\oplus_p\mathrm{P}}$, as well as APC_1 and APC_2, deserve more study. For instance, is $\mathrm{APC}_2 \subseteq T_2^2$?

Thank you!