Bounded Arithmetic

and

Propositional Proofs

Part II:
Propositional Proofs and Two Translations from Bounded Arithmetic

Samuel R. Buss
Department of Mathematics
University of California, San Diego
La Jolla, CA 92093-0112, USA

Lengths of Propositional Proofs

Def'n: *Propositional Formulas* are formed with logical connectives $\wedge$, $\vee$, $\neg$ and $\supset$, variables $p_1, p_2, \ldots$, and parentheses.

Cook's Thm: $P = NP$ iff there is a polynomial time algorithm for determining if a propositional formula is valid.

Def'n: A *Frege* ($\mathcal{F}$) proof system is a usual proof system for propositional logic with a finite set of axiom schemes and with only the modus ponens rule. $\mathcal{F}$ is sound and complete.

Open: Does every tautology have a polynomial size $\mathcal{F}$-proof? If so, then NP=co-NP.

Pf: The set of tautologies is co-NP complete and having a polynomial size $\mathcal{F}$-proof is an NP property.

Def'n: The extended Frege ($e\mathcal{F}$) proof system is a Frege proof system plus the *extension rule*:

Extension Rule: whenever q is a variable which has not been used in the proof so far and does not appear in the final line of the proof or in φ then we may infer

$$q \leftrightarrow \varphi.$$

This allows us to use q as abbreviation for φ. By iterating uses of extension rule the extension rule can apparently make proofs logarithmically smaller by reducing the formula size.

(Tseĭtin, 1968) first used the extension rule, for resolution proofs. Also, (Statman, 1977) and (Cook, Reckhow, 1979).

Thm: (Reckhow, 1976) The choice of axiom schemas or of logical language does not affect the lengths of $\mathcal{F}$- or $e\mathcal{F}$-proofs by more than a polynomial amount.

Def'n: A *propositional proof system* is a polynomial time function f with range equal to the set of all valid formulas.

An (extended) Frege proof system can be viewed as a propositional proof system by letting $f(w)$ equal the last line of w if w is a valid (e)$\mathcal{F}$-proof. Similarly, any theory (e.g. set theory) can be viewed as a propositional proof system.

Thm: (Cook, 1975)
NP = coNP iff there is a proof system f for which tautologies have polynomial size proofs.

Such a proof system f, if it exists, is called *super*.

Def'n: Let S and T be proof systems (with the same propositional language). S *simulates* T iff there is a polynomial p so that for any T-proof of size n there is an S-proof of the same formula of size $\leq p(n)$. S *p-simulates* T iff the S-proof is obtainable as an FP function of the T-proof.

Open: Does $\mathcal{F}$ simulate $e\mathcal{F}$?

This is related to the question of whether Boolean circuits have equivalent polynomial size formulas. By (Ladner, 1975) and (Buss, 1987) this is a non-uniform version of

"Does P=ALOGTIME?"

Open: Is there a *maximal* proof system which simulates all other propositional proof systems?

(Krajíček, Pudlák, 1989): If NEXP=co-NEXP then "Yes".

Def'n: The propositional pigeon hole principle PHP_n is the formula

$$\bigwedge_{0\leq i\leq n}\bigvee_{0\leq j<n} p_{i,j} \supset \bigvee_{0\leq i<m\leq n}\bigvee_{0\leq j<n}(p_{i,j}\wedge p_{m,j})$$

states that $n+1$ pigeons can't fit singly into n holes. $p_{i,j}$ means "pigeon i is in hole j".

Thm: (Cook-Reckhow, 1979) There are polynomial size $e\mathcal{F}$-proofs of PHP_n.

Thm: (Buss, 1987) There are polynomial size $\mathcal{F}$-proofs of PHP_n.

Thm: (Haken, 1985) The shortest resolution proofs of PHP_n are of exponential size.

Cook and Reckhow had proposed PHP_n as an example for showing that $\mathcal{F}$ could not simulate $e\mathcal{F}$.

Problem: Find a combinatorial principle that might separate $\mathcal{F}$ from $e\mathcal{F}$.

Proof that PHP_n has polysize $e\mathcal{F}$-proofs

Conceptual Version: (by contradiction)

Given $f\colon [n] \overset{1-1}{\longmapsto} [n-1]$

define $f_k\colon [k] \overset{1-1}{\longmapsto} [k-1]$

as $f_n(i) = f(i)$,

$$f_k(i) = \begin{cases} f_{k+1}(i) & \text{if } f_{k+1}(i) < k \\ f_{k+1}(k+1) & \text{otherwise.} \end{cases}$$

For $k = 1$, $f_1 : [1] \overset{1-1}{\longmapsto} [0]$ — contradiction.

$e\mathcal{F}$-proof: Uses $q^k_{i,j}$ for "$f_k(i) = j$".

$$q^n_{i,j} \leftrightarrow p_{i,j}$$
$$q^k_{i,j} \leftrightarrow q^{k+1}_{i,j} \vee (q^{k+1}_{i,k} \wedge q^{k+1}_{k+1,j})$$

Then prove for $k = n, n-1, \ldots, 1$ that $q^k_{i,j}$'s code a one-to-one function from $[k]$ to $[k-1]$. For $k = 1$, we have "f_1 is total and one-to-one":

$$q^1_{0,0} \wedge q^1_{1,0} \wedge \neg(q^1_{0,0} \wedge q^1_{1,0})$$

which is impossible. □

The First Translation

S^1_2 and Polysize $e\mathcal{F}$ Proofs

Part of Cook's motivation for the introduction of the feasibly constructive proof system PV was that there is an intimate translation between PV-proofs and polynomial size $e\mathcal{F}$-proofs.

(Cook, 1975) showed that if $A(x)$ is a polynomial time equation provable in PV, then there is a family of tautologies $[\![A]\!]^n$ such that

(1) $[\![A]\!]^n$ is a polynomial size propositional formula,

(2) $[\![A]\!]^n$ says that $A(x)$ is true whenever $|x| \leq n$,

(3) $[\![A]\!]^n$ has polynomial size $e\mathcal{F}$-proofs.

Generalizations have been proved by (Dowd, 1985) and (Krajíček, Pudlak, 1988).

We shall prove the version of Cook's theorem for S^1_2 and Π^b_2-formulas A. (see Buss, 1988).

Def'n: Let $t(\vec{a})$ be a term. The *bounding polynomial* of t is a polynomial $q_t(\vec{n})$ such that

$$(\forall \vec{x})(|t(\vec{x})| \leq q_t(\max\{|\vec{x}|\})).$$

The inductive definition is:

$$\begin{aligned}
q_0(n) &= 1 \\
q_a(n) &= n \quad \text{for } a \text{ a variable} \\
q_{S(t)}(n) &= q_t(n) + 1 \\
q_{s+t}(n) &= q_s(n) + q_t(n) \\
q_{s \cdot t}(n) &= q_s(n) + q_t(n) \\
q_{s \# t}(n) &= q_s(n) \cdot q_t(n) + 1 \\
q_{|t|}(n) &= q_{\lfloor \frac{1}{2} t \rfloor}(n) = q_t(n)
\end{aligned}$$

Def'n: Let $A(\vec{a})$ be a bounded formula. The *bounding polynomial* of A is a polynomial $q_A(\vec{a})$ so that if $|a_i| \leq n$ for all a_i in $\vec{a}$, then $A(\vec{a})$ refers only to numbers of length $\leq q_A(n)$.

q_A is inductively defined by:

(1) $q_{s \leq t} = q_{s=t} = q_s + q_t$

(2) $q_{\neg A} = q_A$

(3) $q_{A \wedge B} = q_{A \vee B} = q_{A \supset B} = q_A + q_B$

(4) $q_{(Qx \leq t)A} = q_t(n) + q_A(n + q_t(n))$

Next we define $[\![t]\!]_m$ to be a vector of polynomial size formulas that define (compute) the term t for values of length $\leq m$. For this it is useful to think of formulas as being circuits of fanout 1.

Let $[\![+]\!]_m$ be a polynomial size, fanout 1 circuit which accepts $2m$ binary inputs and outputs m binary signals; $[\![+]\!]_m$ computes the bitwise sum of two m-bit integers (and discards any overflow). Likewise define $[\![\cdot]\!]_m$, $[\![\#]\!]_m$, $[\![\lfloor \frac{1}{2} x \rfloor]\!]_m$, etc.

Def'n: Let $t(\vec{a})$ be a term and $m \geq q_t(n)$. $[\![t]\!]^n_m$ is a vector of m propositional formulas defining the lower m bits of the value of $t(\vec{a})$ when $|a_i| \leq n$.

For b a free variable in t, a propositional variable v^b_i represents the i-th bit of b's value.

(1) $[\![0]\!]^n_m$ is a sequence of m false formulas (for example $p \wedge \neg p$).

(2) For b a variable, $[\![b]\!]^n_m$ is a sequence of $m - n$ false formulas followed by $v^b_{n-1}, \ldots, v^b_0$.

(3) $[\![s + t]\!]^n_m$ is $[\![+]\!]_m([\![s]\!]^n_m, [\![t]\!]^n_m)$ (the formulas corresponding to the circuit for addition applied to the outputs of $[\![s]\!]^n_m$ and $[\![t]\!]^n_m$).

(4) And similarly for other cases.

Note that $[\![t]\!]^n_m$ is a polynomial size formula (in m and n).

Next: for $A \in \Pi_2^b$ define a propositional formula $[\![A]\!]_m^n$ for $m \geq q_A(n)$.

If B is formula, we assign new 'existential' variables ϵ_i^B and new 'universal' variables μ_i^B to B ($i \geq 0$). Different occurences of B will generally get assigned different such variables.

Def'n: EQ_m is a circuit for equality:

$$EQ_m(\vec{p}, \vec{q}) \text{ is } \bigwedge_{k=0}^{m-1} (p_k \leftrightarrow q_k)$$

$LE_m(\vec{p}, \vec{q})$ is a circuit for $\leq$:

$$EQ_m(\vec{p}, \vec{q}) \vee \bigvee_{0 \leq i < m} \Big(q_i \wedge \neg p_i \wedge \bigwedge_{i < j < m} (q_i \leftrightarrow p_i) \Big)$$

Def'n: A is in negation-implication normal form (NINF) iff all negation signs are applied to atomic subformulas and there are no implications in A.

Def'n: Assume $A \in \Pi^b_2$ and A is in NINF and $m \geq q_A(n)$. Define $[\![A]\!]^n_m$ inductively by:

(1) $[\![s = t]\!]^n_m$ is $EQ_m([\![s]\!]^n_m, [\![t]\!]^n_m)$

(2) $[\![s \leq t]\!]^n_m$ is $LE_m([\![s]\!]^n_m, [\![t]\!]^n_m)$

(3) $[\![\neg A]\!]^n_m$ is $\neg[\![A]\!]^n_m$ for A atomic.

(4) $[\![A \wedge B]\!]^n_m$ is $[\![A]\!]^n_m \wedge [\![B]\!]^n_m$

(5) $[\![A \vee B]\!]^n_m$ is $[\![A]\!]^n_m \vee [\![B]\!]^n_m$

(6) $[\![(\exists x \leq t)A(x)]\!]^n_m$ is $[\![x \leq t \wedge A(x)]\!]^n_m(\{\varepsilon^A_i / v^x_i\}^{n-1}_{i=0})$

(7) $[\![(\forall x \leq t)A(x)]\!]^n_m$ is $[\![\neg x \leq t \vee A(x)]\!]^n_m(\{\mu^A_i / v^x_i\}^{n-1}_{i=0})$

(8) $[\![(\forall x \leq |t|)A(x)]\!]^n_m$ is $\bigwedge_{k=0}^{m-1} [\![\neg \underline{k} \leq |t| \vee A(\underline{k})]\!]^n_m$

Note that $|t| \leq m$ (by our assumption on m).

(9) $[\![(\exists x \leq |t|)A(x)]\!]^n_m$ is $\bigvee_{k=0}^{m-1} [\![\underline{k} \leq |t| \wedge A(\underline{k})]\!]^n_m$

Prop: The formula $[\![A]\!]^n_m$ is equivalent to A in that $A(\vec{a})$ is true ($|a_i| \leq n$) iff for all truth assignments to the universal variables in $[\![A]\!]^n_m$ there is an assignment to the existential variables which satisfies $[\![A]\!]^n_m$. $\Box$

We can extend the definition of $[\![A]\!]$ in the obvious way to formulas not in NINF.

Def'n: An $e\mathcal{F}$-proof of $[\![A]\!]^n_m$ is defined like an ordinary $e\mathcal{F}$-proof except now we additionally allow the existential variables (but not the other variables) in $[\![A]\!]^n_m$ to be defined by the extension rule (each existential variable may be defined only once).

Theorem: (essentially Cook, 1975).
If $A \in \Pi^b_2$ and $S^1_2 \vdash (\forall \vec{x})A(\vec{x})$ then there are polynomial size (in n) $e\mathcal{F}$-proofs of $[\![A]\!]^n_{q_A(n)}$. These $e\mathcal{F}$-proofs are obtainable in polynomial time.

Proof: of Cook's theorem. If $\Gamma \longrightarrow \Delta$ is provable in S^1_2, we prove the theorem for

$$[\![\neg\Gamma \vee \Delta]\!].$$

By free-cut elimination it will suffice to do it for $\Gamma \subset \Sigma^b_1$ and $\Delta \subset \Pi^b_2$. We proceed by induction on the number of inferences in a free-cut free proof.

Case (1): A logical axiom $B \longrightarrow B$. Obviously

$$[\![\neg B \vee B]\!] \;=\; \neg[\![B]\!] \vee [\![B]\!]$$

has a polynomial size $e\mathcal{F}$-proof.

Case (2): A BASIC axiom. For example,

$$[\![(x+y)+z = x+(y+z)]\!]^n_{3n}$$

has straightforward polynomial size $\mathcal{F}$-proofs using techniques of (Buss, 1987).

Case (3) The proof ends with a contraction:

$$\frac{\Gamma \longrightarrow \Delta, B, B}{\Gamma \longrightarrow \Delta, B}$$

Recall that all three B's are assigned different existential and universal variables. The induction hypothesis says there are polynomial size $e\mathcal{F}$-proofs of

$$[\![\neg\Gamma \vee \Delta \vee B \vee B]\!].$$

Modify these proofs by (1) identifying the universal variables for different B's; (2) at the end of the proof use extension to define

$$\epsilon''_j \leftrightarrow ([\![B]\!](\vec{\epsilon}) \wedge \epsilon_j) \vee (\neg[\![B]\!](\vec{\epsilon}) \wedge \epsilon'_j)$$

where $\vec{\epsilon}''$ are the existential variables for the lower B and the others are the existential variables for the upper B's; and (3) then extend to a proof of

$$[\![\neg\Gamma]\!] \vee [\![\Delta]\!] \vee [\![B]\!](\vec{\epsilon}'').$$

Case (4) The proof ends with a Cut:

$$\frac{\Gamma \longrightarrow \Delta, B \qquad B, \Pi \longrightarrow \Lambda}{\Gamma, \Pi \longrightarrow \Delta, \Lambda}$$

By free cut elimination, $B \in \Sigma_1^b$; so B has existential variables $\vec{\epsilon}$ and $\neg B$ has universal variables $\vec{\mu}$. By induction hypothesis, there are polynomial size eF-proofs of

$$[\![\neg\Gamma]\!] \vee [\![\Delta]\!] \vee [\![B]\!](\vec{\epsilon})$$

and

$$[\![\neg\Pi]\!] \vee [\![\Lambda]\!] \vee [\![\neg B]\!](\vec{\mu})$$

The polynomial size eF-proof of

$$[\![\neg\Gamma \vee \neg\Pi \vee \Delta \vee \Lambda]\!]$$

consists of the first proof above followed by the second proof except with the $\vec{\mu}$'s changed to $\vec{\epsilon}$'s followed by a (simulated) cut.

Case (5) For Σ_1^b-PIND inferences, iterate the construction for Cut and contractions.

Case (6) If the proof ends with:

$$\frac{\Gamma \longrightarrow \Delta, A(t)}{t \leq s, \Gamma \longrightarrow \Delta, (\exists x \leq s) A(x)}$$

Let $\vec{\epsilon}$ be the existential variables for $(\exists x \leq s)A$. The desired $e\mathcal{F}$-proof contains:

(a) Extension: $\vec{\epsilon} \leftrightarrow [\![t]\!]$.

(b) The proof from the induction hypothesis of

$$[\![\neg\Gamma \vee \Delta \vee A(t)]\!]$$

(c) A further derivation of

$$[\![\neg t \leq s \vee \neg\Gamma \vee \Delta \vee (t \leq s \wedge A(t))]\!]$$

(d) A derivation of

$$[\![\neg t \leq s \vee \neg\Gamma \vee \Delta \vee (\exists x \leq s) A(x)]\!]$$

by changing some $[\![t]\!]$'s to ϵ's. □

Corollaries to Cook's Theorem

Thm's A-C are due to (Cook, 1975)—for PV

Thm A: Let $G \supseteq \mathcal{F}$ be a propositional proof system. If $S^1_2 \vdash Con(G)$ then $e\mathcal{F}$ p-simulates G.

Thm B: If $S^1_2 \vdash$ NP = coNP then $e\mathcal{F}$ is super.

Thm C: $e\mathcal{F}$ has polynomial size proofs of the propositional formulas $Con_{e\mathcal{F}}(n)$ which assert that there is no $e\mathcal{F}$-proof of $p \wedge \neg p$ of length $\leq n$.

Thm D: (Buss, 1989) $\mathcal{F}$ has polynomial size proofs of the self-consistency formulas $Con_{\mathcal{F}}(n)$.

Pf of Thm A from Thm C: (Idea) Suppose there is a G proof P of a tautology φ. A polynomial size $e\mathcal{F}$ proof of φ is constructed as follows: Let $\vec{p}$ be the free variables in $\varphi(\vec{p})$. Reason inside $e\mathcal{F}$. First show that if $\neg\varphi$ then there is an $\mathcal{F}$-proof P_1 of $\neg\varphi(\underline{\vec{p}})$ where $\underline{\vec{p}}$ denotes a vector of $\top$'s and $\bot$'s: the truth values of $\vec{p}$. By substituting $\underline{\vec{p}}$ for $\vec{p}$ in P and combining this with P_1, we construct a G-proof P_2 of a contradiction. This proof has size polynomial in $|P|$ since P_1 has size polynomial in $|\varphi| \leq |P|$.

By Thm C there is a polynomial size $e\mathcal{F}$-proof of $Con_G(|P_2|)$ so the assumption that $\neg\varphi$ is impossible; i.e., φ is true. □

Pf of Thm C: $S^1_2 \vdash Con(e\mathcal{F})$. □

Pf of Thm D: The $\mathcal{F}$-self-consistency proof is a "brute-force" proof that truth is preserved by axioms and modus ponens using the fact that the Boolean formula value problem is in ALOGTIME. □

Def'n: A *substitution Frege* $s\mathcal{F}$ proof system is a Frege proof system plus the substitution rule:

$$\frac{\psi(p)}{\psi(\varphi)}$$

for ψ, φ arbitrary formulas, all occurences of p substituted for.

Thm: (Cook, Reckhow, 1979), (Dowd, 1985), (Krajíček, Pudlák, 1989)
$s\mathcal{F}$ and $e\mathcal{F}$ p-simulate each other.

Pf: $s\mathcal{F}$ p-simulates $e\mathcal{F}$ is not hard to show directly. $e\mathcal{F}$ p-simulates $s\mathcal{F}$ since $S^1_2 \vdash Con(s\mathcal{F})$. □

Constant Depth Frege Proofs

Let propositional formulas use connectives $\wedge$ and $\vee$ with negations only on variables. The *depth* of a formula is the maximum number of blocks (alternations) of $\wedge$'s and $\vee$'s on any branch of the formula, viewed as a tree.

The *depth* of a Frege proof is the maximum depth of formulas occuring in the proof.

Completeness Thm: Constant-depth Frege systems are complete (for constant depth tautologies.

Proof: By the cut-elimination theorem. □

The Second Translation
$I\Delta_0 / S_2$ and constant depth $\mathcal{F}$

(Paris-Wilkie'85) developed the following translation between provability in $I\Delta_0$ (or $I\Delta_0 + \Omega_1$) and the lengths of constant depth Frege proofs.

First, we shall work with $I\Delta_0(\alpha, f)$ or $S_2(\alpha, f)$ where α and/or f are allowed to be new predicate or function symbols (resp.) which may be used in induction axioms. We translate closed (=variable-free) arithmetic formulas A into propositional formulas A^{PW}: this is defined inductively as follows.

(1) $(\alpha(t))^{PW}$ is q_i, where i is the numeric value of the variable-free term t.

(2) $(f(t) = s)^{PW}$ is $p_{i,j}$, where i and j are the numeric values of t and s. Wlog, f occurs only in this context.

(3) For other atomic formulas,

$P(\vec{t})^{PW}$ is defined to be either the constant $\top$ or the constant $\bot$.

(4) Boolean connectives are translated without any change. E.g., $(A \wedge B)^{PW}$ is $A^{PW} \wedge B^{PW}$.

(5) $[(\forall x \leq t)A(x)]^{PW}$ is $\bigwedge_{i=0}^{value(t)} [A(\underline{i})]^{PW}$.

(6) $[(\exists x \leq t)A(x)]^{PW}$ is $\bigvee_{i=0}^{value(t)} [A(\underline{i})]^{PW}$.

Thm: (essentially Paris-Wilkie'85)
Suppose $I\Delta_0(\alpha, f)$ proves $(\forall x)A(x)$. Then the formulas $\{A(n)^{PW} : n \geq 0\}$ are tautologies and have polynomial size, constant-depth Frege proofs.

Pf-idea: Given a $I\Delta_0(\alpha, f)$ proof $P(x)$ of $A(x)$ and given $n \geq 0$, replace x everywhere with $\underline{n}$, to get a proof $P(n)$ of $A(\underline{n})$. W.l.o.g., $P(x)$ is free-cut free, so has only bounded formulas. Replace every formula B in $P(n)$ with its translation B^{PW}. Thus every sequent $\Gamma \longrightarrow \Delta$ in $P(n)$ becomes a propositional sequent $\Gamma^{PW} \longrightarrow \Delta^{PW}$.

(a) *Size of new formulas*. A simple size analysis gives that there is a constant c such that for every formula $A \in P(n)$, the formula A^{PW} as at most n^c many symbols. This is since every term $t(n)$ is bounded by n^c and there are finitely many formulas A in $P(n)$.

(b) *Size of propositional proofs* of $\Gamma^{PW} \longrightarrow \Delta^{PW}$ is likewise bounded by n^d for some constant d. To prove this, consider how the propositional proof is obtained from the proof $P(n)$: the general idea is to work from the bottom of the proof upwards, always considering sequents in $P(n)$ with values assigned to all the free variables.

(b.i) A $\exists \leq$:right inference in $P(n)$:

$$\frac{\Gamma \longrightarrow \Delta, B(s)}{s \leq t, \Gamma \longrightarrow \Delta, (\exists x \leq t) B(x)} .$$

If $s \leq t$, the propositional translation of this is:

$$\cfrac{\cfrac{\Gamma^{PW} \longrightarrow \Delta^{PW}, B(s)^{PW}}{\Gamma^{PW} \longrightarrow \Delta^{PW}, \bigvee_{i=0}^{t} B(i)^{PW}} \vee\text{:right's}}{\top, \Gamma^{PW} \longrightarrow \Delta^{PW}, \bigvee_{i=0}^{t} B(i)^{PW}}$$

(b.ii) A $\forall \leq$:right inference in $P(n)$:

$$\frac{a \leq t, \Gamma \longrightarrow \Delta, B(a)}{\Gamma \longrightarrow \Delta, (\forall x \leq t) B(x)}$$

has propositional translation:

$$\frac{\{\top, \Gamma^{PW} \longrightarrow \Delta^{PW}, B(i)^{PW}\}_{i=0}^{t}}{\Gamma^{PW} \longrightarrow \Delta^{PW}, \bigwedge_{i=0}^{t} B(i)^{PW}} \wedge\text{:right's}$$

(b.iii) A induction inference in $P(n)$

$$\frac{\Gamma, B(a) \longrightarrow B(a+1), \Delta}{\Gamma, B(0) \longrightarrow B(t), \Delta}$$

has propositional translation

$$\frac{\{\Gamma^{PW}, B(i)^{PW} \longrightarrow B(i+1)^{PW}, \Delta^{PW}\}_{i=0}^{t-1}}{\Gamma^{PW}, B(0)^{PW} \longrightarrow B(t)^{PW}, \Delta^{PW}} \text{Cuts}$$

Other inferences are handled similarly. Since the proof $P(n)$ has constant size, and since the values of terms are $\leq n^{\alpha}$, for some constant α, the size bound is proved. $\square$

When Ω_1 is used the function $x \mapsto x^{\log x}$ is total, the growth rate is a little larger:

Thm: (essentially Paris-Wilkie'85)
Suppose $I\Delta_0(\alpha, f)+\Omega_1$ proves $(\forall x)A(x)$. Then the formulas $\{A(n)^{PW} : n \geq 0\}$ are tautologies and have quasi-polynomial size, constant-depth Frege proofs.

Pf: Very similar argument works.

For S_2^i and T_2^i we get the following improvement:

First, at the cost of adding a finite set polynomial time functions such as the Gödel β function, we may assume that every formula in $\Sigma_i^b(\alpha, f)$ or $\Pi_i^b(\alpha, f)$ consists of exactly i bounded quantifiers, then a sharply bounded quantifer and then a Boolean combination of atomic formulas of the form $\alpha(t)$ or $f(t) = s$ or which do not use α or f. [Basically, because of the quantifier exchange property and by contracting like quantifiers.]

With this convention, then if $A \in \Sigma_i^b$ or $A \in \Pi_i^b$ then the translation A^{PW} is a depth $i+1$ propositional formula where the bottom depth has polylogarithmic fanin.

Thm: Suppose $T_2^i \vdash \Gamma \longrightarrow \Delta$, sequent of $\Sigma_i^b \cup \Pi_i^b$ formulas. Then the sequents $\Gamma^{PW} \longrightarrow \Delta^{PW}$ have polynomial size propositional sequent calculus proofs of depth $i+1$ in which every formula has polylogarithmic fanin at the bottom level.

Furthermore, there is a constant c such that every sequent in the propositional proof has at most c formulas.

If every formula in the T_2^i-proof is in Π_i^b, then every formula in the propositional proofs starts with a (topmost) block of $\bigwedge$'s.

Proof: As above. □