Bounded Arithmetic

and

Propositional Proofs

Part I: Bounded Arithmetic

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

Feasibly Constructive Proof Systems

A **constructive** proof system is one in which proofs of existence contain, or imply the existence of, algorithms for finding the object which is proved to exist. For a feasibly constructive system, the algorithm will be feasible, not merely effective.

I.e., if $\forall x \exists y A(x, y)$ is provable then there should be an algorithm to find y as a function of x.

Effective versus **Feasible**:

"Effective" means "recursive" - Church's thesis.

"Feasible" means "Computable with a reasonable amount of time or space resources".

The usual mathematical model for *feasible* is "polynomial-time computable".

PRELIMINARIES: COMPUTATIONAL COMPLEXITY

Def'n: P is the set of polynomial time recognizable functions. FP is the set of polynomial time computable *functions*.
Functions and predicates are *arithmetic*: polynomial time means in terms of the length $|x|$ of the input x. (Instead of having functions and predicates operate on strings of characters.)

$|x| = \lceil \log_2(x+1) \rceil$ = the length of the binary representation of x

$|\vec{x}| = |x_1|, |x_2|, \ldots, |x_k|$

Cobham (1964) defined FP as the closure of some base functions under compostion and *limited iteration on notation*.

Base Functions: 0, S (successor), $\lfloor\frac{1}{2}x\rfloor$, $2 \cdot x$,

$$x \leq y = \begin{cases} 1 & \text{if } x \leq y \\ 0 & \text{otherwise} \end{cases}$$

$$Choice(x,y,z) = \begin{cases} y & \text{if } x > 0 \\ z & \text{otherwise} \end{cases}$$

Def'n: Let q be a polynomial. f is defined from g and h by **limited iteration on notation** with space bound q iff

$$\begin{array}{rcl} f(\vec{x},0) & = & g(\vec{x}) \\ f(\vec{x},y) & = & h(\vec{x},y,f(\vec{x},\lfloor\frac{1}{2}y\rfloor)) \end{array}$$

provided $|f(\vec{x},y)| \leq q(|\vec{x}|,|y|)$ for all $\vec{x},y$.

Def'n: NP is the set of non-deterministic polynomial time computable predicates. *Co-NP* is the set of complements of NP predicates.

Def'n: If Ψ is a set of predicates, *PB*$\exists(\Psi)$ is the set of predicates A expressible as

$$\vec{x} \in A \Leftrightarrow (\exists y \leq 2^{p(|\vec{x}|)}) B(\vec{x}, y)$$

for some polynomial p and some $B \in \Psi$.
PB$\forall(\Psi)$ is defined similarly with universal polynomially bounded quantification.

Now, $NP =$ *PB*$\exists(P)$ and *co-NP* $=$ *PB*$\forall(P)$.

Def'n: If Ψ is a set of predicates, P^{Ψ} (resp., FP^{Ψ})is the set of predicates (resp., functions) polynomial time recognizable with oracles for a finite number of predicates in Ψ.

Polynomial Time “Hierarchy”:

$$\begin{aligned}
\square_1^p &= FP \\
\Delta_1^p &= P \\
\Sigma_k^p &= PB\exists(\Delta_k^p) \\
\Pi_k^p &= PB\forall(\Delta_k^p) \\
\Delta_{k+1}^p &= P^{\Sigma_k^p} = P^{\Pi_k^p} \\
\square_{k+1}^p &= FP^{\Sigma_k^p} = FP^{\Pi_k^p}
\end{aligned}$$

$$\vdots \qquad\qquad\qquad \vdots$$

$$\Delta_3^p \qquad\qquad\qquad \square_3^p$$

$$\Pi_2^p \qquad\qquad \Sigma_2^p$$

$$\Delta_2^p \qquad\qquad\qquad \square_2^p$$

$$co\text{-}NP = \Pi_1^p \qquad\qquad \Sigma_1^p = NP$$

$$P = \Delta_1^p \qquad\qquad\qquad \square_1^p = FP$$

Open Question: Is this hierarchy proper?

The Equational Theory PV

(Cook, 1975) PV - “Polynomially Verifiable”

- an equational theory analogous to PRA except for polynomial time computability.
- based on dyadic representation of integers as strings of 0’s and 1’s.
- base functions include $\leq$, $Cond$, concatenation and iterated concatenation and two successor functions s_1 and s_2:

$$s_{i+1}(x) = 2x + i$$

- additional function symbols definable by limited iteration; this gives all FP functions.

- a length induction rule (for equations A):

$$\frac{A(0) \quad A(1) \quad (\forall x)(A(x) \supset A(s_1(x)) \wedge A(s_2(x)))}{(\forall x)A(x)}$$

- Statman showed that the full induction (for equations) holds:

$$A(0) \wedge A(1) \wedge (\forall x)(A(x) \supset A(x+1)) \\ \supset (\forall x)A(x)$$

- Bounded Arithmetic will present more appropriate induction axioms for polynomial time/hierarchy complexity

- PV can define precisely the polynomial time functions; equations express precisely the polynomial time predicates.

- Connections between PV and polynomial size extended Frege proofs

Language of Bounded Arithmetic

First-order language for $\mathbf{N}$ with function symbols 0, S, $+$, $\cdot$, $\lfloor \frac{1}{2} x \rfloor$, $|x|$, # and relation symbol $\leq$, where

$$x \# y = 2^{|x| \cdot |y|}$$

The # (pronounced "smash") function allows us to express $2^{q(|\vec{a}|)}$ for q any polynomial with positive integer coefficients.

Def'n: A *bounded quantifier* is a quantifier of the form $(Qx \leq t)$ with t a term. A *sharply bounded quantifier* is one of the form $(Qx \leq |t|)$. $(\forall x)$ and $(\exists x)$ are unbounded quantifiers. A *bounded* formula is one with no unbounded quantifiers.

A hierarchy of classes Σ_k^b, Π_k^b of bounded formulas is defined by counting alternations of bounded quantifiers, ignoring sharply bounded quantifiers. (Analogous to defining the arithmetic hierarchy by counting unbounded quantifiers, ignoring bounded quantifiers.)

$\Sigma_0^b = \Pi_0^b$ is the set of formulas with only sharply bounded quantifiers.
If $A \in \Sigma_k^b$ then $(\forall x \le |t|)A$ and $(\exists x \le t)A$ are in Σ_k^b and $(\forall x \le t)A$ is in Π_{k+1}^b.
Dually, if $A \in \Pi_k^b$ then $(\exists x \le |t|)A$ and $(\forall x \le t)A$ are in Π_k^b and $(\exists x \le t)A$ is in Σ_{k+1}^b.
Connectives $\land$, $\lor$, $\neg$, $\supset$ are treated in the usual manner.

Thm: Fix $k \ge 1$. A predicate Q is in Σ_k^p iff there is a Σ_k^b formula which defines it.

Pf: (Stockmeyer-Wrathall, 1976),
(Kent-Hodgson, 1982)

Reasons the # function and sharply bounded quantifiers are natural choices:

- # has the right growth rate for polynomial time computation.
- the above theorem defines the Σ, Π classes of the polynomial hierarchy syntactically (without use of computation),
- Quantifier Exchange Principle:

$$\begin{aligned}&(\forall x \le |a|)(\exists y \le b)A(x,y) \leftrightarrow \\ &\quad \leftrightarrow (\exists y \le (2a+1)\#(4(2b+1)^2))(\forall x \le |a|) \\ &\qquad [A(x,\beta(x+1,y)) \wedge \beta(x+1,y) \le b]\end{aligned}$$

- Ed Nelson introduced # for defining substitution syntactically. Wilkie-Paris have used Ω_1 ("$x^{\log x}$ is total") similarly.

Induction Axioms for Bounded Arithmetic

The *IND* axioms are the usual induction axioms. The *PIND* and *LIND* axioms are "polynomial" and "length" induction axioms that are intended to be feasibly effective forms of induction.

Σ^b_k-**IND**: For $A \in \Sigma^b_k$,

$$A(0) \land (\forall x)(A(x) \supset A(x+1)) \supset (\forall x)A(x)$$

Σ^b_k-**PIND**: For $A \in \Sigma^b_k$,

$$A(0) \land (\forall x)(A(\lfloor \tfrac{1}{2}x \rfloor) \supset A(x)) \supset (\forall x)A(x)$$

Σ^b_k-**LIND**: For $A \in \Sigma^b_k$,

$$A(0) \land (\forall x)(A(x) \supset A(x+1)) \supset (\forall x)A(|x|)$$

Σ^b_k-LIND and Σ^b_k-PIND typically are equivalent and are (strictly?) weaker than Σ^b_k-IND. Exponentiation is not provably total in Bounded Arithmetic.

Theories of Bounded Arithmetic

Def'n: T_2^i is the first-order theory with language 0, S, $+$, $\cdot$, $\lfloor \frac{1}{2}x \rfloor$, $|x|$, $\#$ and $\leq$ and axioms:

(1) A finite set, BASIC, of (universal closures of) open axioms defining simple properties of the function and relation symbols. BASIC properly contains Robinson's Q since it has to be used with weaker induction axioms.

(2) The Σ_i^b-IND axioms.

T_2^{-1} has no induction axioms.
T_2 is the union of the T_2^i's.

T_2 is equivalent to $I\Delta_0 + \Omega_1$ (Parikh, Wilkie-Paris) except for differences in the nonlogical language.

Def'n: S_2^i is the first-order theory with language 0, S, $+$, $\cdot$, $\lfloor \frac{1}{2}x \rfloor$, $|x|$, $\#$ and $\leq$ and axioms:

(1) The BASIC axioms, and

(2) The Σ_i^b-PIND axioms.

$S_2^{-1} = T_2^{-1}$ has no induction axioms.
S_2 is the union of the S_2^i's.

Thm: (Buss, 1985). Let $i \geq 1$.

$$T_2^i \vdash S_2^i$$

and

$$S_2^i \vdash T_2^{i-1}.$$

So $S_2 \equiv T_2$.

Open: Are the inclusions proper?

$$S_2^1 \subseteq T_2^1 \subseteq S_2^2 \subseteq T_2^2 \subseteq \cdots$$

Def'n: Let $f\colon \mathbf{N}^k \mapsto \mathbf{N}$. f is Σ_i^b-*definable* by a theory R iff there is a formula $A(\vec{x}, y) \in \Sigma_i^b$ and a term t so that

(1) For all $\vec{n} \in \mathbf{N}^k$, $A(\vec{n}, f(\vec{n}))$ is true.

(2) $R \vdash (\forall \vec{x})(\exists y \leq t) A(\vec{x}, y)$

(3) $R \vdash (\forall \vec{x}, y, z)(A(\vec{x}, y) \wedge A(\vec{x}, z) \supset y = z)$

Def'n: Let $Q \subseteq \mathbf{N}$. Q is Δ_i^b-definable by a theory R iff there is a Σ_i^b-formula A and Π_i^b-formula B that define Q so that A and B are provably equivalent in R. A formula is Δ_i^b w.r.t R iff it is provably equivalent to a Σ_i^b- and to a Π_i^b-formula.

Bootstrapping Thm: Every polynomial time function is Σ_1^b-definable by S_2^1 and every polynomial time predicate is Δ_1^b-definable by S_2^1.

Thm: Any Σ_1^b-definable function or Δ_1^b-definable predicate of S_2^i may be introduced into the non-logical language and used freely in induction axioms.

Pf: If f is Σ_1^b-defined by R:

$$R \vdash (\forall x)(\exists! y \le r(\vec{x}))A_f(\vec{x}, y).$$

An atomic formula $\varphi(f(\vec{s}))$ is equivalent to both

$$(\exists y \le r(\vec{s}))(A_f(\vec{s}, y) \land \varphi(y))$$

and

$$(\forall y \le r(\vec{s}))(A_f(\vec{s}, y) \supset \varphi(y))$$

Thus any Σ_i^b-formula involving f is equivalent to one not involving f by tranforming atomic subformulas as above (and by removing f from the quantifier bounds). □

Main Theorems for S^i_2

Theorem: (Buss, 1985) Let $i \geq 1$. Let A be a Σ^b_i-formula. Suppose $S^i_2 \vdash (\forall\vec{x})(\exists y)A(\vec{x}, y)$. Then there is a Σ^b_i-formula B and a function $f \in \square^p_i$ and a term t so that

(1) $S^i_2 \vdash (\forall\vec{x}, y)(B(\vec{x}, y) \supset A(\vec{x}, y))$.

(2) $S^i_2 \vdash (\forall\vec{x})(\exists! y)B(\vec{x}, y)$.

(3) $S^i_2 \vdash (\forall\vec{x})(\exists y \leq t)B(\vec{x}, y)$. [Parikh]

(4) For all $\vec{n}$, $\mathbf{N} \models B(\vec{n}, f(\vec{n}))$.

Conversely: If $f \in \square^p_i$ then there is a formula $B \in \Sigma^b_i$ and a term t so that (2), (3) and (4) hold.

Corollary: $(i \geq 1)$ The Σ_i^b-definable functions of S_2^i are precisely the functions in $\Box_i^p$.

To restate in terms of predicates:

Theorem: $(i \geq 1)$. Suppose $A(\vec{x}) \in \Sigma_i^b$ and $B(\vec{x}) \in \Pi_i^b$ and $S_2^i \vdash A \leftrightarrow B$. Then there is a predicate $Q \in \Delta_i^p$ so that, for all $\vec{n}$,

$$Q(\vec{n}) \Leftrightarrow \mathbf{N} \models A(\vec{n}) \Leftrightarrow \mathbf{N} \models B(\vec{n})$$

Conversely, if $Q \in \Delta_i^p$ then there are A and B so that the above holds.

So, the Δ_i^b-definable predicates of S_2^i are precisely the Δ_i^p-predicates.

Special case when $i = 1$: If A is a formula which is S_2^1-provably in *NP*$\cap$*co-NP* then A defines a polynomial time predicate (provably in S_2^1). Being provably in *NP* $\cap$ *co-NP* means provably equivalent to a Σ_1^b- and to a Π_1^b-formula.

The Sequent Calculus

To prove the Main Theorem, we shall formalize S^i_2 in Gentzen's sequent calculus.

$\land$, $\lor$, $\neg$, $\supset$, $\forall$, $\exists$ are the logical symbols.

$\longrightarrow$ is the sequent connective.

Def'n: A *sequent* is of the form

$$A_1, A_2, \ldots, A_n \longrightarrow B_1, B_2, \ldots, B_k$$

where the A_i's and B_i's are formulas. Its intended meaning is

$$(A_1 \land A_2 \land \cdots \land A_n) \supset (B_1 \lor \cdots \lor B_k)$$

Greek letters $\Gamma, \Delta, \ldots$ are used to denote finite sequences of formulas separated by commas ("cedents").

An *LK-proof* is a tree of sequents: the leaves or *initial sequents* must be of the form $A \longrightarrow A$; the root, or *endsequent*, is what is proved; and the valid inferences are:

$$\frac{\Gamma \longrightarrow \Delta, A}{\neg A, \Gamma \longrightarrow \Delta} \qquad \frac{A, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, \neg A}$$

$$\frac{\Gamma \longrightarrow \Delta, A \qquad \Gamma \longrightarrow \Delta, B}{\Gamma \longrightarrow \Delta, A \land B}$$

$$\frac{A, \Gamma \longrightarrow \Delta}{A \land B, \Gamma \longrightarrow \Delta} \qquad \frac{B, \Gamma \longrightarrow \Delta}{A \land B, \Gamma \longrightarrow \Delta}$$

$$\frac{A, \Gamma \longrightarrow \Delta \qquad B, \Gamma \longrightarrow \Delta}{A \lor B, \Gamma \longrightarrow \Delta}$$

$$\frac{\Gamma \longrightarrow \Delta, A}{\Gamma \longrightarrow \Delta, A \lor B} \qquad \frac{\Gamma \longrightarrow \Delta, B}{\Gamma \longrightarrow \Delta, A \lor B}$$

$$\frac{\Gamma \longrightarrow \Delta, A \qquad B, \Gamma \longrightarrow \Delta}{A \supset B, \Gamma \longrightarrow \Delta}$$

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

$$\frac{A(b), \Gamma \longrightarrow \Delta}{(\exists x)A(x), \Gamma \longrightarrow \Delta} \qquad \frac{\Gamma \longrightarrow \Delta, A(t)}{\Gamma \longrightarrow \Delta, (\exists x)A(x)}$$

$$\frac{A(t), \Gamma \longrightarrow \Delta}{(\forall x)A(x), \Gamma \longrightarrow \Delta} \qquad \frac{\Gamma \longrightarrow \Delta, A(b)}{\Gamma \longrightarrow \Delta, (\forall x)A(x)}$$

In the quantifier inferences the free variable b is called the *eigenvariable* and must not appear in the lower sequent.

$$\frac{\Gamma \longrightarrow \Delta}{A, \Gamma \longrightarrow \Delta} \qquad \frac{\Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, A}$$

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

$$\frac{A, A, \Gamma \longrightarrow \Delta}{A, \Gamma \longrightarrow \Delta} \qquad \frac{\Gamma \longrightarrow \Delta, A, A}{\Gamma \longrightarrow \Delta, A}$$

Cut: $$\frac{\Gamma \longrightarrow \Delta, A \qquad A, \Pi \longrightarrow \Lambda}{\Gamma, \Pi \longrightarrow \Delta, \Lambda}$$

Theorem: (Gentzen)

- LK is complete.
- LK without the Cut inference is complete.

So if P is an LK-proof of $\Gamma \longrightarrow \Delta$ then there is a cut-free proof P^* of $\Gamma \longrightarrow \Delta$. There is an effective (but not feasible) procedure to obtain P^* from P.

Because there are no cuts in P^*, every formula appearing in P^* will be a subformula (in a wide sense) of a formula in $\Gamma \longrightarrow \Delta$. This gives a bound on the logical complexity of formulas needed to prove $\Gamma \longrightarrow \Delta$.

To formulate sequent calculus systems of Bounded Arithmetic, we enlarge LK as follows:

(1) Allow equality axioms and BASIC axioms as initial sequents. An initial sequent will contain only atomic formulas.

(2) Add inferences for bounded quantifiers (the variable b occurs only as indicated):

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

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

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

$$\frac{b \leq s, \Gamma \longrightarrow \Delta, A(b)}{\Gamma \longrightarrow \Delta, (\forall x \leq s)A(x)}$$

(3) Allow induction inferences: (for $A \in \Sigma_i^b$)

$$\Sigma_i^b\text{-IND} \quad \frac{A(b), \Gamma \longrightarrow \Delta, A(b+1)}{A(0), \Gamma \longrightarrow \Delta, A(t)}$$

$$\Sigma_i^b\text{-PIND} \quad \frac{A(\lfloor \frac{1}{2} b \rfloor), \Gamma \longrightarrow \Delta, A(b)}{A(0), \Gamma \longrightarrow \Delta, A(t)}$$

S_2^i and T_2^i may be formulated as sequent calculus systems with BASIC axioms as initial sequents and with Σ_i^b-PIND and Σ_i^b-IND inference rules, respectively. With side formulas, the induction inferences are equivalent to the induction axioms.

Def'n: A cut inference

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

is *free* unless A is the direct descendant either of a formula in an initial sequent or of a principal formula of an induction inference.

Free-Cut Elimination Theorem

(essentially due to Gentzen and Takeuti):

If P is an S_2^i-proof (or T_2^i-proof) then there is a proof P^* in the same theory with the same end-sequent which contains no free cuts.

In a free-cut free proof, every formula will be a subformula (in a wide sense) of an induction formula, of a formula in an axiom or of a formula in the conclusion. (The wide sense allows terms to change.)

In S_2^i and T_2^i, cut formulas may be restricted to be Σ_i^b-formulas.

To prove the Main Theorem

Step 1: Start with an S^i_2-proof P of

$$\longrightarrow(\exists y)A(\vec{c}, y).$$

By free-cut elimination, there is an S^i_2 proof P^* of $\longrightarrow(\exists y \le t)A(\vec{c}, y)$ such that every formula in P^* is a Σ^b_i-formula.

Step 2: Given the proof P^* we will extract an algorithm to compute a function $f(\vec{c})$ such that $A(\vec{n}, f(\vec{n}))$ is true for all n. The function f will be in $\square^p_i$ and will be Σ^b_i-defined by S^i_2. Furthermore, S^i_2 will prove $(\forall\vec{x})A(\vec{x}, f(\vec{x}))$.

P^* can be thought of as a program plus a proof that it is correct.

Proof of Step 2 follows...

The Witness Predicate

Def'n: Let $B(\vec{a})$ be a Σ_i^b-formula with all free variables indicated. Then $\mathit{Witness}_B^{i,\vec{a}}(w,a)$ is a formula defined inductively:

(1) If $B \in \Sigma_{i-1}^b \cup \Pi_{i-1}^b$ then

$$\mathit{Witness}_B^{i,\vec{a}}(w,\vec{a}) \Leftrightarrow B(\vec{a})$$

(2) If $B = C \vee D$ then

$$\mathit{Witness}_B^{i,\vec{a}}(w,\vec{a}) \Leftrightarrow \mathit{Witness}_C^{i,\vec{a}}(\beta(1,w),\vec{a}) \\ \vee \mathit{Witness}_D^{i,\vec{a}}(\beta(2,w),\vec{a})$$

(3) If $B = C \wedge D$ then

$$\mathit{Witness}_B^{i,\vec{a}}(w,\vec{a}) \Leftrightarrow \mathit{Witness}_C^{i,\vec{a}}(\beta(1,w),\vec{a}) \\ \wedge \mathit{Witness}_D^{i,\vec{a}}(\beta(2,w),\vec{a})$$

(4) If $B = (\exists x \leq t)C(\vec{a},x)$ then

$$\mathit{Witness}_B^{i,\vec{a}}(w,\vec{a}) \Leftrightarrow \beta(1,w) \leq t \\ \wedge \mathit{Witness}_{C(\vec{a},b)}^{i,\vec{a},b}(\beta(2,w),\vec{a},\beta(1,w))$$

(5) If $B = (\forall x \leq |t|)C(\vec{a}, x)$ then

$$\mathit{Witness}_B^{i,\vec{a}}(w, \vec{a}) \Leftrightarrow$$
$$(\forall x \leq |t|)\mathit{Witness}_{C(\vec{a},b)}^{i,\vec{a},b}(\beta(x+1, w), \vec{a}, x)$$

(6) If $B = \neg C$ use prenex operations to push the negation sign inside.

Lemma: Let $B \in \Sigma_i^b$.

(1) For some term t_B, S_2^i proves

$$B(\vec{a}) \leftrightarrow (\exists w \leq t_B)\mathit{Witness}_B^{i,\vec{a}}(w, \vec{a})$$

(2) $\mathit{Witness}_B^{i,\vec{a}} \in \Delta_i^p$ $(= P$ if $i = 1)$

(3) $\mathit{Witness}_B^{i,\vec{a}}$ is Δ_i^b with respect to S_2^i.

Pf: Induction on complexity of B.

The Main Lemma

Lemma: Suppose $S^i_2 \vdash \Gamma \longrightarrow \Delta$ where Γ and Δ contain only Σ^b_i-formulas. Let $\vec{c}$ be the free variables in Γ and Δ. Then, there is a function f such that

(1) f is Σ^b_i-defined by S^i_2

(2) S^i_2 proves

$$\mathit{Witness}^{i,\vec{c}}_{\bigwedge\!\!\!\bigwedge \Gamma}(w,\vec{c}) \supset \mathit{Witness}^{i,\vec{c}}_{\bigvee\!\!\!\bigvee \Delta}(f(w,\vec{c}),\vec{c})$$

(3) $f \in \Box^p_i$ $(= FP$ if $i = 1)$

Proof is by induction on the number of inferences in a free-cut free S^i_2-proof of $\Gamma \longrightarrow \Delta$.

As an example of one case of the proof of the main lemma, suppose that P is a free-cut free proof and ends with the inference

$$\frac{B(\lfloor \frac{1}{2}a \rfloor) \longrightarrow B(a)}{B(0) \longrightarrow B(t)}$$

By the induction hypothesis, there is a function g so that

(1) g is Σ_i^b-defined by S_2^i

(2) g is in $\Box_i^p$ $(= FP$ if $i = 1)$

(3) $S_2^i \vdash \mathit{Witness}^{i,a,\vec{c}}_{B(\lfloor \frac{1}{2}a \rfloor)}(w, a, \vec{c}) \supset$

$$\supset \mathit{Witness}^{i,a,\vec{c}}_{B(a)}(g(w,a,\vec{c}), a, \vec{c}).$$

(4) $S_2^i \vdash (\forall a, \vec{c})[g(w, a, \vec{c}) \leq t_B(a, \vec{c})]$

Now define f by limited iteration as

$$\begin{aligned} f(w,0,\vec{c}) &= g(w,0,\vec{c}) \\ f(w,a,\vec{c}) &= g(f(w,\lfloor\tfrac{1}{2}a\rfloor,\vec{c}),a,\vec{c}) \end{aligned}$$

so $f(w,a,\vec{c}) \le t_B(a,\vec{c})$ and the following hold:

(1) $f \in \Box_i^p$ $(= FP$ if $i = 1)$

Pf: Since f is defined by limited iteration from g

(2) S_2^i can Σ_i^b-define f and prove that f satisfies the above conditions

(3) $S_2^i \vdash \mathit{Witness}_{B(0,\vec{c})}^{i,a,\vec{c}}(w,a,\vec{c}) \supset$

$$\supset \mathit{Witness}_{B(a,\vec{c})}^{i,a,\vec{c}}(f(w,a,\vec{c}),a,\vec{c}).$$

Pf: Since $\mathit{Witness}_{B(a,\vec{c})}^{i,b,\vec{c}}$ is a Σ_i^b-formula, S_2^i can prove this by Σ_i^b-PIND directly from the induction hypothesis.

Q.E.D. Main Lemma

Proof of Main Theorem from Main Lemma

Suppose $S_2^i \vdash (\forall\vec{x})(\exists y)A(\vec{x},y)$. By a theorem of Parikh, there is a term t so that S_2^i proves $\longrightarrow(\exists y \leq t)A(\vec{c},y)$. By the Main Lemma,

$$S_2^i \vdash \mathit{Witness}^{i,\vec{c}}_{(\exists y \leq t)A}(g(\vec{c}),\vec{c})$$

for some Σ_i^b-defined function g. Define

$$B(\vec{c},y) \text{ to be } y = \beta(1,g(\vec{c}))$$

Since g is Σ_i^b-defined by S_2^i, B is a Σ_i^b-formula and by the properties of *Witness*,

$$S_2^i \vdash (\forall\vec{x},y)(B(\vec{x},y) \supset A(\vec{x},y))$$

Finally, define $f(\vec{c}) = \beta(1,g(\vec{c}))$.
Q.E.D. Main Theorem

Other Axioms for Bounded Arithmetic

Let Ψ be a set of formulas. The axioms below are schemes where $A \in \Psi$:

Ψ-**MIN**: (Minimization)

$$(\exists x)A(x) \supset (\exists x)[A(x) \wedge (\forall y < x)(\neg A(y))]$$

Ψ-**LMIN**: (Length minimization)

$$(\exists x)A(x) \supset A(0) \vee (\exists x)[A(x) \wedge (\forall y \le \lfloor \tfrac{1}{2}x \rfloor)(\neg A(y))]$$

Ψ-**replacement**:

$$\begin{aligned}&(\forall x \le |t|)(\exists y \le s)A(x,y) \leftrightarrow \\ &\qquad \leftrightarrow (\exists w \le SqBd(t,s))(\forall x \le |t|) \\ &\qquad\qquad (A(x, \beta(Sx,w)) \wedge \beta(Sx,w) \le s)\end{aligned}$$

strong Ψ-**replacement**:

$$\begin{aligned}&(\exists w \le SqBd(t,s))(\forall x \le |t|) \\ &\qquad [(\exists y \le s)A(x,y) \leftrightarrow \\ &\qquad\qquad \leftrightarrow A(x, \beta(Sx,w) \wedge \beta(Sx,w) \le s]\end{aligned}$$

For $i \geq 1$, relative to S^1_2:

$$\begin{tikzcd}
\Sigma^b_i\text{-IND} \arrow[r, Leftrightarrow] \arrow[d, Rightarrow] & \Pi^b_i\text{-IND} \arrow[r, Leftrightarrow] & \Sigma^b_i\text{-MIN} \arrow[r, Leftrightarrow] & \Delta^b_{i+1}\text{-IND} \\
\Sigma^b_i\text{-PIND} \arrow[r, Leftrightarrow] \arrow[d, Leftrightarrow] & \Pi^b_i\text{-PIND} \arrow[r, Leftrightarrow] & \Sigma^b_i\text{-LIND} \arrow[r, Leftrightarrow] & \Pi^b_i\text{-LIND} \\
\Sigma^b_i\text{-LMIN} \arrow[r, Leftrightarrow] \arrow[d, Rightarrow] & \text{strong } \Sigma^b_i\text{-replacement} \arrow[d, Leftrightarrow] & & \\
\Sigma^b_{i-1}\text{-IND} & (\Sigma^b_{i+1} \cap \Pi^b_{i+1})\text{-PIND} & &
\end{tikzcd}$$

$$\Sigma^b_{i+1}\text{-MIN} \Leftrightarrow \Pi^b_i\text{-MIN}$$

$$\Sigma^b_{i+1}\text{-replacement} \Rightarrow \Sigma^b_i\text{-PIND} \Rightarrow \Sigma^b_i\text{-replacement}$$

$$S^{i+1}_2 \underset{\Sigma^b_{i+1}}{\succ} T^i_2$$

$$S^{i+1}_2 \underset{\mathcal{B}(\Sigma^b_{i+1})}{\succ} T^i_2 + \Sigma^b_{i+1}\text{-replacement}$$

Thm: (Buss, 1985)

$S^1_2 + \Sigma^b_i$-$PIND \vdash \Delta^b_i$-IND.
Hence $S^i_2 \supset T^{i-1}_2$.

Pf: Suppose A is Δ^b_i w.r.t. S^i_2. Assume $(\forall x)(A(x) \supset A(x+1))$ and argue inside S^i_2.
Let $B(x,z)$ be the formula

$$(\forall w \le x)(\forall y \le z+1)(A(w \dot{-} y) \supset A(w)).$$

So B is equivalent to a Π^b_i-formula. Now by definition of B, $(\forall x, z)(B(x, \lfloor \frac{1}{2} z \rfloor) \supset B(x,z))$ and hence by Π^b_i-PIND on $B(x,z)$ w.r.t z,

$$(\forall x)(B(x,0) \supset B(x,x)).$$

By the assumption, $(\forall x)B(x,0)$; hence $(\forall x)B(x,x)$, from whence

$$(\forall x)(A(0) \supset A(x))$$

□

Conservation Results

Thm: (Buss, 1987) Let $i \geq 1$.

S_2^{i+1} is conservative over T_2^i with respect to $\boldsymbol{\Sigma}_{i+1}^b$-formulas, and hence with respect to $\forall\exists\boldsymbol{\Sigma}_{i+1}^b$-sentences.

Pf: (Idea). Fix $i \geq 1$ and let Z be PV or T_2^{i-1} as appropriate. First show that every $\square_i^p$-function is definable in Z in an appropriate sense. For $i = 1$, there is a function symbol for every polynomial time function; for $i \geq 1$, we show that every $\square_i^p$-function can be "Q_i-defined" — this is stronger than "$\boldsymbol{\Sigma}_i^b$-defined". Second, prove a stronger version of the Main Lemma above; in essence, we partially formalize the Main Lemma in Z and prove that the witnessing function f is defined appropriately in Z. Namely, we prove:

Lemma: If $S_2^i \vdash A$ with $A \in \boldsymbol{\Sigma}_i^b$ then $Z \vdash A$.

Witnessing Theorem for T^1_2

Defn: [Papadimitriou] A *Polynomial Local Search (PLS)*, problem is specified by polynomial time functions F, N, c:

(1) $c(s,x)$ is a *cost function*,

(2) $N(s,x)$ is a neighborhood function, such that for all s s.t. $F(x,s)$

$$c(N(s,x),x) \leq c(s,x)$$

(3) $\{s : F(s,x)\}$ is the solution space for input x, and $F(0,x)$ always holds, and such that, if $F(s,x)$, then $|s| < p(|x|)$ for p a polynomial.

A solution to the PLS problem is a (multivalued) function f, s.t., for all x,

$$c(N(f(x),s),s) = c(f(x),x).$$

Thm [Buss-Krajíček'94] Suppose T^1_2 proves $(\forall x)(\exists y)A(x,y)$ where $A \in \Sigma^b_1$. Then there is a PLS function $f(x) = y$ and a polynomial time function π such that

$$T^1_2 \vdash (\forall x)A(x, \pi \circ f(x)).$$

Furthermore, every PLS function (and every function $\pi \circ f$) is Σ^b_1-definable by T^1_2.

Corollary The same holds for S^2_2 by conservativity of S^2_2 over T^1_2.

Proof-idea: A free-cut free T^1_2-proof can be transformed into a PLS problem. □

The KPT Witnessing Theorem

Thm [Krajíček-Pudlák-Takeuti,91]
Suppose $A \in \Sigma^b_{i+2}$ and $T^i_2 \vdash (\forall x)(\exists y)(\forall z)A(x,y,z)$. Then there $k > 0$ and functions $f_i(x, z_1, ..., z_{i-1})$ so that

(1) Each f_i is Σ^b_{i+1}-defined by T^i_2.

(2) T^i_2 proves

$$
\begin{aligned}
&(\forall x)[(\forall z_1)[A(x, f_1(x), z_1) \vee \\
&\quad (\forall z_2)[A(x, f_2(x, z_1), z_2) \vee \\
&\quad (\forall z_3)[A(x, f_3(x, z_1, z_2), z_3) \vee \cdots \\
&\quad (\forall z_k)[A(x, f_k(x, z_1, \ldots, z_{k-1}), z_k)] \cdots]]].
\end{aligned}
$$

This is called a "nocounterexample interpretation"; and is a special form of a generalized Herbrand's theorem (see [Buss'95]).

Thm [KPT'91; Buss'9?,Zambella'9?] If $T_2^i = S_2^{i+1}$, then the polynomial time hierarchy collapses, provably in T_2^i. In fact, in this case, T_2^i proves that every Σ_3^p predicate is (a) equivalent to a Boolean combination of Σ_2^p-predicates and (b) is in $\Sigma_1^p/poly$.

Proof-idea For simplicity, assume $i = 0$. Suppose $T_2^0(PV) = S_2^1$. Let $\overline{\varphi}$ represent a vector of Boolean formula $\overline{\varphi} = \langle\varphi_1, \ldots, \varphi_n\rangle$. Then $T_2^0(PV)$ proves

$$\begin{aligned}&\forall\overline{\varphi}(\exists\ell \leq n)(\exists\langle w_1, \ldots, w_\ell\rangle)\\ &\qquad[(\forall j \leq \ell)(w_j \text{ satisfies } \varphi_j)\\ &\qquad\wedge \text{“}\ell = n \text{ or } \varphi_{\ell+1} \text{ is unsatisfiable”}]\end{aligned}$$

The formula in $[\cdots]$ is in Π_1^b, so the KPT witnessing theorem can be applied to get $k > 0$ and polynomial time functions $f_1, \ldots, f_k$ so that $T_2^0(PV)$ proves (setting $n = k$) that given $\varphi_1, \ldots, \varphi_k$ satisfied by $w_1, \ldots w_k$, that one of $f_j(\overline{\varphi}, w_1, \ldots, w_{j-1})$ produces a witness to φ_j. [Note that f_j has all φ_i's as input.]

Let $PreAdvice(a, \langle \varphi_{\ell+1}, \ldots, \varphi_k \rangle)$ mean that for all $\varphi_1, \ldots, \varphi_\ell < a$ (not nec. satisfiable), that $f_j(\overline{\varphi}, w_1, \ldots, w_{j-1})$ satisfies φ_j for some $j \leq \ell$.

Let $Advice(a, \langle \varphi_{\ell+1}, \ldots, \varphi_k \rangle)$ mean that $PreAdvice$ holds, and that ℓ is the minimum possible value for which there is such *PreAdvice*.

Claim: $T^0_2(PV)$ proves, that if $\varphi_\ell < a$ and if $Advice(a, \langle \varphi_{\ell+1}, \ldots, \varphi_k \rangle)$, then φ_ℓ is satisfiable if and only if for all $\varphi_1, \ldots, \varphi_{\ell-1}$, satisfied by $w_1, \ldots, w_{\ell-1}$, there is $j \leq \ell$ such that $f_j(\overline{\varphi}, w_1, \ldots, w_{j-1})$ satisfies φ_j.

Pf: If the latter condition is true, then the only way for $\langle \varphi_\ell, \ldots, \varphi_k \rangle$ to not be "preadvice", (which it isn't, by def'n of "advice") is for φ_ℓ to be satisfied by $f_\ell(\overline{\varphi}, \vec{w})$ for some $\varphi_1, \ldots, \varphi_{\ell-1}$, $w_1, \ldots, w_{\ell-1}$. □

Note that this means that the NP complete property of satisfiability is in coNP relative to the polynomial size advice, $\langle \varphi_{\ell-1}, \ldots, \varphi_k \rangle$.

The above shows that $T^0_2(PV)$ would prove $NP \subseteq coNP/poly$. From this, Karp-Lipton style methods can show that $T^0_2(PV)$ proves the polynomial time hierarchy collapses.

In fact it can be shown that $T^0_2(PV)$ proves that every polynomial time hierarchy predicate is equivalent to Boolean combination of Σ^p_2 predicates. The proof idea is that the property $PreAdvice$ is in $coNP$ and therefore, property

$$\mathit{PAlen}(\ell) \equiv \exists \langle \varphi_{\ell+1}, \ldots, \varphi_k \rangle PreAdvice(a, \langle \vec{\varphi} \rangle)$$

is a Σ^p_2-property. Q.E.D.

Similar methods work for $i \geq 1$.

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

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

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 "$f_k(i) = j$".

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

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 (Krajı̃ček, 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

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

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 $|a_i| \le n$ for all a_i in $\vec{a}$, then $A(\vec{a})$ refers only to numbers of length $\le q_A(n)$.

q_A is inductively defined by:

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

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

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

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

Next we define $[\![t]\!]_m$ to be a vector of polynomial size formulas that define (compute) the term t for values of length $\le m$. 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 $\llbracket A \rrbracket_m^n$ is equivalent to A in that $A(\vec{a})$ is true ($|a_i| \le n$) iff for all truth assignments to the universal variables in $\llbracket A \rrbracket_m^n$ there is an assignment to the existential variables which satisfies $\llbracket A \rrbracket_m^n$. □

We can extend the definition of $\llbracket A \rrbracket$ in the obvious way to formulas not in NINF.

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

Theorem: (essentially Cook, 1975).
If $A \in \Pi_2^b$ and $S_2^1 \vdash (\forall \vec{x})A(\vec{x})$ then there are polynomial size (in n) $e\mathcal{F}$-proofs of $\llbracket A \rrbracket_{q_A(n)}^n$. 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 $e\mathcal{F}$-proofs of

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

and

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

The polynomial size $e\mathcal{F}$-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), (Krajĩček, 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 $\displaystyle\bigwedge_{i=0}^{value(t)} [A(\underline{i})]^{PW}$.

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

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 $\exists \le$:right inference in $P(n)$:

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

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

$$\begin{array}{c}
\Gamma^{PW} \longrightarrow \Delta^{PW}, B(s)^{PW} \\
\hline\hline
\Gamma^{PW} \longrightarrow \Delta^{PW}, \bigvee_{i=0}^{t} B(i)^{PW} \\
\hline
\top, \Gamma^{PW} \longrightarrow \Delta^{PW}, \bigvee_{i=0}^{t} B(i)^{PW}
\end{array}
\quad \lor\text{:right's}$$

(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. $\Box$

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 $T^i_2 \vdash \Gamma \longrightarrow \Delta$, sequent of $\Sigma^b_i \cup \Pi^b_i$ 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^i_2-proof is in Π^b_i, then every formula in the propositional proofs starts with a (topmost) block of $\bigwedge$'s.

Proof: As above. □

Bounded Arithmetic

and

Propositional Proofs

Part III: Natural Proofs and Interpolation Theorems

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

Interpolation Thm for Propositional Logic

(Craig,1957) gave stronger version for first logic.

Thm: Let $A(\vec{p},\vec{q})$ and $B(\vec{p},\vec{r})$ be propositional formulas involving only the indicated variables. Suppose

$$A(\vec{p},\vec{q}) \supset B(\vec{p},\vec{r})$$

is a tautology. Then there is a propositional formula $C(\vec{p})$ using only the common variables, so that

$$A \supset C \qquad \text{and} \qquad C \supset B$$

are tautologies.

Pf: Since $A(\vec{p},\vec{q}) \models B(\vec{p},\vec{r})$; if we have already assigned truth values to $\vec{p} = p_1,\ldots,p_k$, then it is not possible to extend this to a truth assignment on $\vec{p},\vec{q},\vec{r}$ such that both $A(\vec{p},\vec{q})$ and $\neg B(\vec{p},\vec{r})$ hold.......

Let $\tau_1, \ldots, \tau_n$ be the truth assignments to $p_1, \ldots, p_k$ for which it is possible to make $A(\vec{p}, \vec{q})$ true by further assignment of truth values to $\vec{q}$.

Let $C(\vec{p})$ say that one of $\tau_1, \ldots, \tau_n$ holds for $\vec{p}$, i.e.,

$$C = \bigvee_{i=1}^{n} \left(p_1^{(i)} \wedge p_2^{(i)} \wedge \ldots \wedge p_k^{(i)} \right)$$

where

$$p_j^{(i)} = \begin{cases} p_j & \text{if } \tau_i(p_j) = \textit{True} \\ \neg p_j & \text{otherwise} \end{cases}$$

Then clearly, $A(\vec{p}, \vec{q}) \models C(\vec{p})$.
Also, by the comment from the previous slide, $C(\vec{p}) \models B(\vec{p}, \vec{r})$. $\Box$

Note that $C(\vec{p})$ may be exponentially larger than $A(\vec{p}, \vec{q})$ and $B(\vec{p}, \vec{r})$.

Example: Let $p_1, \ldots, p_k$ code the binary representation of a k-bit integer P.

Let $A(\vec{p}, \vec{q})$ be a formula which is satisfiable iff P is composite (e.g. q codes two integers > 1 with product P).

Let $B(\vec{p}, \vec{r})$ be a formula which is satisfiable iff P is prime (i.e., $\vec{r}$ codes a Pratt-primality witness).

$$\begin{aligned} P \text{ is prime} \quad &\Leftrightarrow \quad \exists \vec{r} B(\vec{p}, \vec{r}) \\ &\Leftrightarrow \quad \neg \exists \vec{q} A(\vec{p}, \vec{q}). \end{aligned}$$

and $A(\vec{p}, \vec{q}) \supset \neg B(\vec{p}, \vec{r})$ is a tautology.

An interpolant $C(\vec{p})$ must express "$\vec{p}$ codes a composite".

Open: Is primality expressible by a polynomial size formula?

Generalizing this example gives:

Thm: (Mundici'83-84) If there is a polyonomial upper bound on the circuit size of interpolants in propositional logic, then

$$NP/poly \cap coNP/poly = P/poly$$

Pf: Let $\exists \vec{q} A(\vec{p}, \vec{q})$ express an $NP/poly$ property $R(\vec{p})$ and $\forall \vec{r} B(\vec{p}, \vec{r})$ express $R(\vec{p})$ in $coNP/poly$ form. Then

$$\exists \vec{q} A(\vec{p}, \vec{q}) \models \forall \vec{r} B(\vec{p}, \vec{r}),$$

which is equivalent to

$$A(\vec{p}, \vec{q}) \supset B(\vec{p}, \vec{r})$$

being a tautology. Let $C(\vec{p})$ be a polynomial size interpolant s.t.,

$$A(\vec{p}, \vec{q}) \supset C(\vec{p}) \quad \text{and} \quad C(\vec{p}) \supset B(\vec{p}, \vec{r})$$

are tautologies. Thus

$$\exists \vec{q} A(\vec{p}, \vec{q}) \models C(\vec{p}) \models \forall \vec{r} B(\vec{p}, \vec{r}),$$

I.e., $R(\vec{p}) \Leftrightarrow C(\vec{p})$ and $R(\vec{p})$ has a polynomial size circuit, so $R(\vec{p})$ is in $P/poly$. $\Box$

Defn: Let PK be the propositional fragment of the Gentzen sequent calculus. Size of a proof $|P|$ is the number of steps in P. $|P|_{dag}$ is used for non-treelike proofs. $V(A)$ denotes the set of free variables in A. For C a formula, $|C|$ is the number of $\land$'s and $\lor$'s in C.

Thm: Let P be a <u>cut-free</u> PK proof of $A \longrightarrow B$, where $V(A) \subseteq \{\vec{p}, \vec{q}\}$ and $V(B) \subseteq \{\vec{p}, \vec{q}\}$. Then there is an interpolant C such that

(1) $A \supset C$ and $C \supset B$ are valid,

(2) $V(C) \subseteq \{\vec{p}\}$,

(3) $|C| \leq |P|$ and $|C|_{dag} \leq |P|_{dag}$.

I.e., tree-like cut-free proofs have interpolants of polynomial formula size, and general cut-free proofs have interpolants of polynomial circuit size.

Remark: The theorem also holds for proofs which have cuts only on formulas D such that $V(D) \subseteq \{\vec{p}, \vec{r}\}$ or $V(D) \subseteq \{\vec{p}, \vec{r}\}$

Pf: We prove by induction on the number of inferences in P a slightly more general statement:

Claim: If P is a proof of $\Gamma_1, \Gamma_2 \longrightarrow \Delta_1, \Delta_2$ and if $V(\Gamma_1, \Delta_1) \subseteq \{\vec{p}, \vec{q}\}$ and $V(\Gamma_2, \Delta_2) \subseteq \{\vec{p}, \vec{r}\}$, then there is an interpolant C so that

(1) $\Gamma_1 \longrightarrow \Delta_1, C$ and $C, \Gamma_2 \longrightarrow \Delta_2$ are valid,

(2) $V(C) \subseteq \{\vec{p}\}$, and

(3) The polynomial size bounds hold too.

<u>Base Case:</u> Initial sequent.

If the initial sequent if $q_i \longrightarrow q_i$, take C to be $\perp$ since

$$q_i \longrightarrow q_i, \perp \quad \text{and} \quad \perp \longrightarrow$$

are valid.

For initial sequent $r_i \longrightarrow r_i$, take C to be $\top$.

For an initial sequent $p_i \longrightarrow p_i$, C will be either $\top$, $\perp$, p_i or $(\neg p_i)$ depending on how the p_i's are split into $\Gamma_1, \Gamma_2, \Delta_1, \Delta_2$.

Induction Step: There are a number of cases, depending on the type of the last inference in the proof.

(1) For last inference an $\lor right$

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

the interpolant for the upper sequent still works for the lower sequent, i.e., use C such that

(a) $\Gamma_1 \longrightarrow \Delta_1, A, B, C$ and $C, \Gamma_2 \longrightarrow \Delta_2$,

or

(b) $\Gamma_1 \longrightarrow \Delta_1, C$ and $C, \Gamma_2 \longrightarrow \Delta_2, A, B$,

depending on if $A \lor B$ is in Δ_1 or Δ_2 (respectively).

(2) For last inference an $\wedge$:right:

$$\frac{\Gamma \longrightarrow \Delta, A \quad \Gamma \longrightarrow \Delta, B}{\Gamma \longrightarrow \Delta, A \wedge B}$$

(2.a) If $A \wedge B$ is in Δ_1, apply the induction hypothesis twice to have interpolants C_A and C_B so that

$$\Gamma_1 \longrightarrow \Delta_1^-, A, C_A \qquad\qquad C_A, \Gamma_2 \longrightarrow \Delta_2$$

$$\Gamma_1 \longrightarrow \Delta_1^-, B, C_B \qquad\qquad C_B, \Gamma_2 \longrightarrow \Delta_2$$

are valid. Now the derivations

$$\frac{\dfrac{\Gamma_1 \longrightarrow \Delta_1^-, A, C_A}{\Gamma_1 \longrightarrow \Delta_1^-, A, C_A \vee C_B} \quad \dfrac{\Gamma_1 \longrightarrow \Delta_1^-, B, C_B}{\Gamma_1 \longrightarrow \Delta_1^-, B, C_A \vee C_B}}{\Gamma_1 \longrightarrow \Delta_1^-, A \wedge B, C_A \vee C_B}$$

and

$$\frac{C_A, \Gamma_2 \longrightarrow \Delta_2 \quad C_B, \Gamma_2 \longrightarrow \Delta_2}{C_A \vee C_B, \Gamma_2 \longrightarrow \Delta_2}$$

show $(C_A \vee C_B)$ is an interpolant.

(2b)If $A \wedge B$ is in Δ_2 applying the induction hypothesis twice gives C_A and C_B so that

$$\Gamma_1 \longrightarrow \Delta_1, C_A \qquad\qquad C_A, \Gamma_2 \longrightarrow \Delta_2^-, A$$

$$\Gamma_1 \longrightarrow \Delta_1, C_B \qquad\qquad C_B, \Gamma_2 \longrightarrow \Delta_2^-, B$$

are valid. Now the following derivations show $(C_A \wedge C_B)$ is an interpolant:

$$\dfrac{\dfrac{C_A, \Gamma_2 \longrightarrow \Delta_2^-, A}{C_A \wedge C_B, \Gamma_2 \longrightarrow \Delta_2^-, A} \quad \dfrac{C_B, \Gamma_2 \longrightarrow \Delta_2^-, B}{C_A \wedge C_B, \Gamma_2 \longrightarrow \Delta_2^-, B}}{C_A \wedge C_B, \Gamma_2 \longrightarrow \Delta_2^-, A \wedge B}$$

$$\dfrac{\Gamma_1 \longrightarrow \Delta_1, C_A \quad \Gamma_1 \longrightarrow \Delta_1, C_B}{\Gamma_1 \longrightarrow \Delta_1, C_A \wedge C_B}$$

The other cases are similar and the size bounds on C are immediate. □

Interpolation Theorems for Resolution

Defns: A *literal* is a propositional variable p or a negated variable $\neg p$.

$\overline{p}$ is $\neg p$, and $\overline{(\neg p)}$ is p.

A *clause* is a set of literals; its intended meaning is the disjunction of its members.

A *set of clauses* represents the conjunction of its members. Thus a set of clauses "is" a formula in conjunctive normal form.

Resolution Inference: $\dfrac{C \cup \{p\} \qquad D \cup \{\overline{p}\}}{C \cup D}$

We assume w.l.o.g. $p, \overline{p} \notin C$ and $p, \overline{p} \notin D$.

A *resolution refutation* of a set Γ of clauses is a derivation of the empty clause $\emptyset$ from Γ by resolution inferences.

Thm: Resolution is refutation-complete (and sound).

Interpolation Theorem Let $\{A_1(\vec{p},\vec{q}),\ldots,A_k(\vec{p},\vec{q})\}$ and $\{B_1(\vec{p},\vec{r}),\ldots,B_\ell(\vec{p},\vec{r})\}$ be a sets of clauses, so that their union Γ is inconsistent. Then there is a formula $C(\vec{p})$ such that for any truth assignment τ, $domain(\tau)\supseteq\{\vec{p},\vec{q},\vec{r}\}$,

(1) If $\tau(C(\vec{p}))=$ *False*, then

$$\tau(A_i(\vec{p},\vec{q}))= \textit{False}, \text{ for some } i.$$

(2) If $\tau(C(\vec{p}))=$ *True*, then

$$\tau(B_j(\vec{p},\vec{q}))= \textit{False}, \text{ for some } j.$$

Pf: From Γ unsatisfiable, we have

$$A_1(\vec{p},\vec{q}),\ldots,A_k(\vec{p},\vec{q})\longrightarrow\neg B_1(\vec{p},\vec{r}),\ldots,\neg B_\ell(\vec{p},\vec{r})$$

is valid. Thus there is an interpolant $C(\vec{p})$ such that

$$A_1(\vec{p},\vec{q}),\ldots,A_k(\vec{p},\vec{q})\longrightarrow C(\vec{p})$$

and

$$C(\vec{p})\longrightarrow\neg B_1(\vec{p},\vec{r}),\ldots,\neg B_\ell(\vec{p},\vec{r})$$

are valid. □

Thm (Krajíček'9?) Let $\{A_i(\vec{p},\vec{q})\}_i \cup \left\{B_j(\vec{p},\vec{r})\right\}_j$ have a refutation R of n resolution inferences. Then an interpolant, $C(\vec{p})$, can be chosed with $O(n)$ symbols in dag representation.

If R is tree-like, then $C(\vec{p})$ is a formula with $O(n)$ symbols.

Pf: [Pudlák] We view R as a dag or as a tree, each node corresponding to an inference and labeled with the clause inferred at that inference. For each clause E in R, define $C_E(\vec{p})$ as follows:

(1) For $E = A_i(\vec{p},\vec{q})$, a hypothesis,

set $C_E = \bot$ (*False*).

(2) For $E = B_j(\vec{p},\vec{q})$, a hypothesis,

set $C_E = \top$ (*True*).

(3) For an inference $\dfrac{F \cup \{q_i\} \quad G \cup \{\overline{q}_i\}}{F \cup G}$

set $C_{F\cup G} = C_{F\cup\{q_i\}} \vee C_{G\cup\{\overline{q}_i\}}$.

(4) For an inference $\dfrac{F \cup \{r_i\} \quad G \cup \{\overline{r}_i\}}{F \cup G}$

set $C_{F\cup G} = C_{F\cup\{r_i\}} \wedge C_{G\cup\{\overline{r}_i\}}$.

(5) For an inference $\dfrac{F \cup \{p_i\} \quad G \cup \{\overline{p}_i\}}{F \cup G}$

set $C_{F\cup G} = (\overline{p}_i \wedge C_{F\cup\{p_i\}}) \vee (p_i \wedge C_{G\cup\{\overline{p}_i\}})$.

Lemma For all clauses $F \in R$, $C_F(\vec{p})$ satisfies the following condition:

If τ is a truth assignment and $\tau(F) = $ *False*, then

(a) if $\tau(C_F) = $ *False*, then

$\tau(A_i(\vec{p}, \vec{q})) = $ *False* for some i

(b) if $\tau(C_F) = $ *True*, then

$\tau(B_j(\vec{p}, \vec{r})) = $ *False* for some j

Pf of lemma is by induction on the def'n of C_F.

Q.E.D. Lemma and Theorem.

Resolution with limited extension

“Extension’ $=$ introduction of variables that represent complex propositional formulas. When A is a formula, σ_A is the extension variable for A:
For p a variable, σ_p is just p.
For other A, σ_A is a new variable.

Defn: When A is a formula, $LE(A)$ is a set of clauses which define the meanings of the extensions variables for all subformulas of A; to wit:

(1) $LE(p) = \emptyset$

(2) $LE(\neg A) = LE(A) \cup \{ \underbrace{\{\sigma_{\neg A}, \sigma_A\}}_{\neg\sigma_A \supset \sigma_{\neg A}}, \underbrace{\{\overline{\sigma_{\neg A}}, \overline{\sigma_A}\}}_{\sigma_{\neg A} \supset \neg\sigma_A} \}$

(3) $LE(A \wedge B) = LE(A) \cup LE(B)$

$$\cup\{ \underbrace{\{\overline{\sigma_{A\wedge B}}, \sigma_A\}}_{\sigma_{A\wedge B}\supset\sigma_A}, \underbrace{\{\overline{\sigma_{A\wedge B}}, \sigma_B\}}_{\sigma_{A\wedge B}\supset\sigma_B}, \underbrace{\{\sigma_{A\wedge B}, \overline{\sigma_A}, \overline{\sigma_B}\}}_{\sigma_A\wedge\sigma_B\supset\sigma_{A\wedge B}} \}$$

(4) $LE(A \vee B) = LE(A) \cup LE(B)$

$$\cup\{ \underbrace{\{\overline{\sigma_A}, \sigma_{A\vee B}\}}_{\sigma_A\supset\sigma_{A\vee B}}, \underbrace{\{\overline{\sigma_B}, \sigma_{A\vee B}\}}_{\sigma_B\supset\sigma_{A\vee B}}, \underbrace{\{\sigma_A, \sigma_B, \overline{\sigma_{A\vee B}}\}}_{\sigma_{A\vee B}\supset\sigma_A\vee\sigma_B} \}$$

Defn: Let $\mathcal{A}$ be a set of formulas. Then $LE(\mathcal{A})$ is $\cup_{A\in\mathcal{A}}\{LE(A)\}$.
$LE(\vec{p},\vec{q}) = \cup\{LE(A) : V(A) \subseteq \{\vec{p},\vec{q}\}\}$.
$LE(\vec{p},\vec{r}) = \cup\{LE(A) : V(A) \subseteq \{\vec{p},\vec{r}\}\}$.

Thm: Let Γ be the set of clauses

$$\{A_i(\vec{p},\vec{q})\}_i \cup \{B_j(\vec{p},\vec{r})\}_j \cup LE(\vec{p},\vec{q}) \cup LE(\vec{p},\vec{r})$$

and suppose Γ has a refutation R of n resolution inferences.
Then there is an interpolant $C(\vec{p})$ for the sets $\{A_i(\vec{p},\vec{q})\}_i$ and $\{B_j(\vec{p},\vec{r})\}_j$ of circuit size $O(n)$.

Pf: Let $C(\vec{p})$ be the interpolant for

$$\{A_i(\vec{p},\vec{q})\}_i \cup LE(\vec{p},\vec{q})$$

and

$$\{B_j(\vec{p},\vec{r})\}_j \cup LE(\vec{p},\vec{r})$$

given by the earlier interpolation theorem.

Claim: $C(\vec{p})$ is the desired interpolant.

Pf: Any truth assignment τ with domain $\{\vec{p}, \vec{q}\}$ can be uniquely extended to satisfy $LE(\vec{p}, \vec{q})$.

Suppose $\tau(C(\vec{p})) = $ *False*. Extend τ so as to satisfy $LE(\vec{p}, \vec{q})$. By choice of $C(\vec{p})$, τ makes a clause from $\{A_i(\vec{p}, \vec{q})\}_i \cup LE(\vec{p}, \vec{q})$ false, hence makes one of the A_i's false.

A similar argument shows that if $\tau(C(\vec{p})) =$ *True*, then τ falsifies some $B_j(\vec{p}, \vec{r})$.

Q.E.D. Claim and Theorem. □

Natural Proofs (Razborov-Rudich'94)

Defn: Represent a Boolean function $f_n(x_1, \ldots, x_n)$ by its truth table (this has size $N = 2^n$).

$\mathcal{C} = \{C_n\}_n$ is **quasipolynomial-time natural against** $P/poly$ iff each C_n is a set of truth tables of n-ary Boolean functions, and the following hold:

Constructivity: "$f_n \in C_n$?" is decidable in $TIME(2^{(\log N)^{O(1)}})/poly$, and

Largeness: $|C_n| \geq 2^{-cn} \cdot 2^{2^n}$ for some $c > 0$, and

Usefulness: If $f_n \in C_n$ for all n, then the family $\{f_n\}_n$ is not in $P/poly$ (i.e., does not have polynomial size circuits).

Motivation 'Constructive' proofs that $NP \not\subset P/poly$ ought to give (quasi)polynomial time property which is natural against $P/poly$.

Remark: Note that 'quasipolynomial time', is measured as a function of the size of the truth table of f_n.

The Strong Pseudo-Random Number Generator (SPRNG) Conjecture

Defn: Let $G_n : \{0,1\}^n \to \{0,1\}^{2n}$ be a pseudo-random number generator. The *hardness*, $H(G_n)$, of G_n is the least $S > 0$ such that, for some circuit C of size S,

$$\left| \underset{\overline{x} \in \{0,1\}^n}{Prob}[C(G_n(\overline{x}))=1] - \underset{\overline{y} \in \{0,1\}^{2n}}{Prob}[C(\overline{y})=1] \right| \geq \frac{1}{S}$$

SPRNG Conjecture There are pseudorandom number generators G_n, computed by polynomial size circuits, with hardness $H(G_n) \geq 2^{n^\epsilon}$, for some $\epsilon > 0$.

Thm: (Razborov-Rudich) If the SPRNG conjecture is true, then there are no properties which are quasipolynomial time/poly natural against $P/poly$.

Pf: omitted.

Split Bounded Arithmetic Theories

Let α and β be new unary predicate symbols.

$S_2^i(\alpha,\beta)$ and $T_2^i(\alpha,\beta)$ are defined as usual, allowing induction on $\Sigma_i^b(\alpha,\beta)$-formulas.

Let $\Sigma_\infty^b(\alpha)$ denote all bounded formulas in the language of S_2 plus α. Define:

$$\mathcal{S}\Sigma_i^b = \Sigma_i^b(\Sigma_\infty^b(\alpha), \Sigma_\infty^b(\beta))$$

where $\Sigma_1^b(X)$ indicates the closure of X under $\wedge$, $\vee$, sharply bounded quantification and existential bounded quantification, where $\Pi_1^b(X)$ is defined similarly and

$$\Sigma_{i+1}^b(X) = \Sigma_1^b(\Pi_i^b(X))$$

and $\Pi_{i+1}^b(X)$ is similarly defined.

Defn: Split versions of S_2^i and T_2^i:

$$\begin{aligned}\mathcal{S}S_2^i &= BASIC + \mathcal{S}\Sigma_i^b\text{-PIND}\\ \mathcal{S}T_2^i &= BASIC + \mathcal{S}\Sigma_i^b\text{-IND}\end{aligned}$$

Suppose superpolynomial lower bounds are provable in $S^2_2(\alpha)$ as follows.

Let $N \geq 0$ and $n = |N| \approx \log N$. $(n = |x|)$.

Also suppose $t(n) = n^{\omega(1)}$ (a superpolynomial lower bound), and that $S(N, x)$ is a Σ^b_∞-formula.

Let $LB(t, S, \alpha)$ be the statement

$$\neg[\alpha \text{ codes a circuit of size} \leq t(n) \text{ s.t. } (\forall x \in \{0,1\}^n)(\alpha(x) = 1 \leftrightarrow S(N, x))]$$

(1) The free variables of $LB(t, S, \alpha)$ are N and α.

(2) By "α encodes a ciruit" we mean that α encodes gate types and gate connections in some straightforward manner, plus, α may encode the full truth table description of the functions computed by every gate in the circuit!

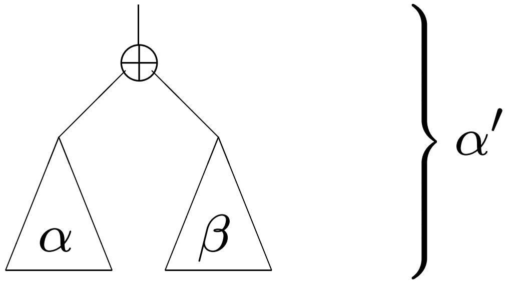
Thm: If $S^2_2(\alpha) \vdash LB(t, S, \alpha)$, then

$$\mathcal{S}S^2_2 \vdash SLB(t, S, \alpha, \beta)$$

where $SLB(t, S, \alpha, \beta)$ is

$\neg[\alpha$ codes a circuit of size $\leq t(n)/2 - 1$ and
β codes a circuit of size $\leq t(n)/2 - 1$ s.t.
$\forall x \in \{0,1\}^n((\alpha \oplus \beta)(x) = 1 \leftrightarrow S(N, x))]$

Pf: If $\neg SLB(t, S, \alpha, \beta)$, then the circuit α'



satisfies $\neg LB(t, S, \alpha)$. □

By rephrasing $SLB(t, S, \alpha, \beta)$, we let γ be a new predicate symbol and we have that if

$$\mathcal{S}S_2^2 \vdash SLB(t, S, \alpha, \beta),$$

then

$$\mathcal{S}S_2^2 \vdash \neg CC(t/2-1, \gamma, \alpha) \vee \neg CC(t/2-1, S \oplus \gamma, \beta)$$

where $CC(t, T(x), \alpha)$ states:

$$[\alpha \text{ codes a circuit of size} \leq t(n) \text{ s.t.} \\ \forall x \in \{0,1\}^n (\alpha(x) = 1 \leftrightarrow T(x))]$$

or, in sequent form, $\mathcal{S}S_2^2(\alpha)$ proves

$$CC(t/2-1, \gamma, \alpha), CC(t/2-1, S \oplus \gamma, \beta) \longrightarrow$$

Since CC is a Σ_1^b formula, this sequent is also provable in $\mathcal{S}T_2^1$ by $\forall\Sigma_2^b$-conservativity. (By the same proof that shows S_2^2 is conservative over T_2^1.)

Thm: (Razborov'95) If $\mathcal{S}S^2_2 \vdash SLB(t,S,\alpha,\beta)$ for some $t = n^{\omega(1)}$ and $S \in \Sigma^b_\infty$, then the SPRNG conjecture is false.

Corollary: If the SPRNG conjecture holds, then S^2_2 does not prove superpolynomial lower bounds on circuit size for any bounded formula (i.e., for any polynomial time hierarchy predicate).

Pf: (rest of slides) We shall prove that, if

$$\mathcal{S}T^1_2 \vdash CC(t,\gamma,\alpha), CC(t, S\oplus\gamma,\beta) \longrightarrow ,$$

then there are quasipolynomial size circuits which are natural against $P/poly$.

First Step: Convert the $\mathcal{S}T^1_2$ proof and the sequent into a constant-depth propositional proof.

To convert to propositional logic

Use variables $\vec{q}$ for the values of α, i.e,

$$q_i \text{ denotes } \alpha_i$$

Likewise use variables $\vec{r}$ for the values of $\beta(x)$ and variables $\vec{p}$ for the values of $\gamma(x)$.

By expanding the language to include the β function and using $\mathcal{S}\Pi_1^b$-IND and applying free cut-elimination, we may assume that every formula in the $\mathcal{S}T_2^1$ proof is of the form

$$(\forall y \le r)(\exists z \le |r'|)(\cdots)$$

where $(\cdots)$ is a Boolean combination of $\Sigma_\infty^b(\alpha)$ formulas and $\Pi_\infty^b(\beta)$ formulas and of formulas $\gamma(\cdots)$.

When translated into propositional logic by the Paris-Wilkie translation, this becomes

$$\bigwedge_{i=0}^{2^{n^{O(1)}}} \bigvee_{j=0}^{n^{O(1)}} E_{i,j}$$

where each $E_{i,j}$ is (1) $\pm p_i$ or (2) involves only $\vec{p}, \vec{q}$ or (3) involves only $\vec{p}, \vec{r}$.

Fixing N and $f(x) = S(N,\alpha)$, we obtain a propositional sequent calculus proof of:

$$\bigwedge_i A_i(\vec{p},\vec{q}), \bigwedge_j B_j(\vec{p},\vec{r}) \longrightarrow$$

where:

(1) $\{A_i(\vec{p},\vec{q})\}_i$ is a set of clauses stating that $\vec{q}$ codes a circuit of size t computing the function γ with graph given by $\vec{p}$.

(2) $\{B_j(\vec{p},\vec{q})\}_j$ is a set of clauses stating that $\vec{r}$ codes a circuit of size t computing the function $\gamma \oplus f$.

(3) f does not have a circuit of size $2t + 1$

(4) Each formula in the proof is a conjunction of disjunctions of formulas involving just $\vec{p}, \vec{q}$ or just $\vec{p}, \vec{r}$ (as on last slide).

(5) Each sequent has only c many formulas, c a constant independent of N.

(6) The proof has only $2^{n^{O(1)}}$ many symbols.

Second Step: Remove the $\bigwedge$'s from the proof as follows.

(a) Given a sequent

$$\bigwedge_{i=1}^{p_1} E_{1,i}, \ldots, \bigwedge_{i=1}^{p_{c'}} E_{c',i} \longrightarrow \bigwedge_{i=1}^{q_1} F_{1,i}, \ldots, \bigwedge_{i=1}^{q_{c''}} F_{c'',i}$$

replace it with the $q_1 \cdot q_2 \cdot \cdots \cdot q_{c''}$ sequents

$$\begin{aligned} E_{1,1}, E_{1,2}, \ldots, E_{1,p_1}, E_{2,1}, \ldots, E_{c',p_{c'}} &\longrightarrow \\ \longrightarrow F_{1,i_1}, F_{1,i_2}, \ldots, F_{c'',i_{c''}} \end{aligned}$$

Since each $q_i = 2^{n^{O(1)}}$ and $c'' = O(1)$, this still only $2^{n^{O(1))}}$ many sequents.

(b) Build a new proof of *all* these sequents. The hardest case of making this a valid new proof, is the case of a cut on $\bigwedge_{i=1}^{p} F_i$. For this, an inference

$$\frac{\Gamma \longrightarrow \Delta, \bigwedge_{i=1}^{p} F_i \qquad \bigwedge_{i=1}^{p} F_i, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta}$$

is replaced by p cuts; i.e., by

$$\dfrac{\dfrac{\Gamma^*\longrightarrow\Delta^*, F_3 \qquad \dfrac{\Gamma^*\longrightarrow\Delta^*, F_2 \qquad \dfrac{\Gamma^*\longrightarrow\Delta^*, F_1 \qquad F_1, F_2, \ldots, F_p, \Gamma^*\longrightarrow\Delta^*}{F_2, F_3, \ldots, F_p, \Gamma^*\longrightarrow\Delta^*}}{F_3, \ldots, F_p, \Gamma^*\longrightarrow\Delta^*}}{\vdots}}{\Gamma^*\longrightarrow\Delta^*}$$

At the end of the second step, we have a treelike sequent calculus proof of

$$A_1(\vec{p},\vec{q}), \ldots, A_k(\vec{p},\vec{q}), B_1(\vec{p},\vec{r}), \ldots B_\ell(\vec{p},\vec{r}) \longrightarrow$$

such that every formula in in the proof is a disjunction of formulas which either involve just $\vec{p}$ and $\vec{q}$ or involve just $\vec{p}$ and $\vec{r}$.

Third Step: Convert to a resolution with limited extension refutation.

Each sequent in the proof obtained in the second step has the form

$$\bigvee_{i=1}^{p_1} E_{1,i}, \ldots, \bigvee_{i=1}^{p_u} E_{u,i}, \longrightarrow \bigvee_{i=1}^{q_1} F_{1,i}, \ldots, \bigvee_{i=1}^{q_v} F_{v,i} \quad \text{(A)}$$

where each $E_{a,i}$, $F_{a,i}$ involves only $\{\vec{p}, \vec{q}\}$ or $\{\vec{p}, \vec{r}\}$.

Associate with sequent (A), the following set (B) of clauses:

$$\Big\{\{E_{1,i}\}_{i=1}^{p_1}, \ldots, \{E_{u,i}\}_{i=1}^{p_u}, \qquad \text{(B)}$$
$$\{\neg F_{1,1},\}, \{\neg F_{1,2},\}, \ldots, \{\neg F_{v,q_v},\}\Big\}$$

Now (B) is not really a proper set of clauses, since clauses are supposed to contain literals (not formulas).

So instead of using (B), we introduce extension variables to form the following set (C) of clauses:

$$\Big\{\{\sigma_{E_{1,i}}\}_{i=1}^{p_1},\ldots,\{\sigma_{E_{u,i}}\}_{i=1}^{p_u}, \qquad \text{(C)}$$
$$\{\sigma_{\neg F_{1,1}},\},\{\sigma_{\neg F_{1,2}},\},\ldots,\{\sigma_{\neg F_{v,q_v}},\}\Big\}$$

If sequent (A) is $\Gamma \longrightarrow \Delta$, then the set (C) of clauses is denoted $(\Gamma \longrightarrow \Delta)^{LE}$. It is important that all the extension variables used in (C) are from $LE(\vec{p},\vec{q})$ and $LE(\vec{p},\vec{r})$.

Lemma: If $\Gamma \longrightarrow \Delta$ is derived in m lines of the sequent calculus proof constructed in Step (2) above, then

$$(\Gamma \longrightarrow \Delta)^{LE} \cup LE(\vec{p},\vec{q}) \cup LE(\vec{p},\vec{r})$$

has a resolution refutation (not necessarily tree-like) of $O(m^2)$ resolution inferences.

Proof: by induction on m. — splits into cases depending on the last inference of the proof.

Case (1) $\Gamma \longrightarrow \Delta$ is $A \longrightarrow A$.

If $A = \bigvee A_i$, then

$$\Big\{\{\sigma_{A_1}, \ldots, \sigma_{A_u}\}, \{\sigma_{\neg A_1}\}, \ldots, \{\sigma_{\neg A_u}\}\Big\} \cup LE(A)$$

has a resolution refutation of $O(u)$ inferences.

Case (2): Suppose $A = \bigvee\limits_i A_i$ involves only $\vec{p}, \vec{q}$. Then $\{\sigma_A\}$ and $\{\sigma_{A_1}, \ldots, \sigma_{A_u}\}$ can be derived from each other (in the presence of $LE(A)$). Therefore it is not important how we express formulas as disjunctions when there is a choice.

Case (3): $\wedge$:left and $\vee$:right inferences involve only fomulas that use just $\vec{p}, \vec{q}$ or just $\vec{p}, \vec{r}$; these are therefore straightforward (the $\wedge$:right is a little harder than the $\vee$:left case).

Case (4): An $\vee$:left inference can be:

$$\frac{\bigvee\limits_i E_i, \Gamma \longrightarrow \Delta \qquad \bigvee\limits_j F_j, \Gamma \longrightarrow \Delta}{\vee\{E_i, F_j\}_{i,j}, \Gamma \longrightarrow \Delta}$$

Case (4) cont'd: The induction hypotheses give refutations R_1 and R_2:

$$\left.\begin{array}{l}(\Gamma\longrightarrow\Delta)^{LE}\\ \{\sigma_{E_i}\}_i\\ LE(\vec{p},\vec{q})\\ LE(\vec{p},\vec{r})\end{array}\right\}\quad\overset{R_1}{\Longrightarrow}\quad\emptyset$$

and

$$\left.\begin{array}{l}(\Gamma\longrightarrow\Delta)^{LE}\\ \{\sigma_{F_j}\}_j\\ LE(\vec{p},\vec{q})\\ LE(\vec{p},\vec{r})\end{array}\right\}\quad\overset{R_2}{\Longrightarrow}\quad\emptyset$$

Combine these as:

$$\left.\begin{array}{l}(\Gamma\longrightarrow\Delta)^{LE}\\ \{\sigma_{E_i}\}_i\cup\{\sigma_{F_j}\}_j\\ LE(\vec{p},\vec{q})\\ LE(\vec{p},\vec{r})\end{array}\right\}\overset{R_1'}{\Longrightarrow}\quad\left.\begin{array}{l}\{\sigma_{F_j}\}_j\\ (\Gamma\longrightarrow\Delta)^{LE}\\ LE(\vec{p},\vec{q})\\ LE(\vec{p},\vec{r})\end{array}\right\}\overset{R_2}{\Longrightarrow}\emptyset$$

where R_1' is like R_1 but uses $\{\sigma_{E_i}\}_i\cup\{\sigma_{F_j}\}_j$ in place of $\{\sigma_{E_i}\}_i$.

Remark: Note the refutation is not tree-like since $\{\sigma_{F_j}\}_j$ may be used multiple times in R_2.

Case 5: Last inference is cut:

$$\frac{\Gamma \longrightarrow \Delta, \bigvee_i A_i \qquad \bigvee_i A_i, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta}$$

The induction hypotheses give refutations R_1 and R_2:

$$\left.\begin{array}{l} (\Gamma \longrightarrow \Delta)^{LE} \\ \{\sigma_{\neg A_1}\}, \ldots, \{\sigma_{\neg A_u}\} \\ LE(\vec{p}, \vec{q}) \\ LE(\vec{p}, \vec{r}) \end{array}\right\} \overset{R_1}{\Longrightarrow} \quad \emptyset$$

and

$$\left.\begin{array}{l} (\Gamma \longrightarrow \Delta)^{LE} \\ \{\sigma_{A_1}, \ldots, \sigma_{A_u}\} \\ LE(\vec{p}, \vec{q}) \\ LE(\vec{p}, \vec{r}) \end{array}\right\} \overset{R_2}{\Longrightarrow} \quad \emptyset$$

Combine these as below, with R_1' equal to R_1 minus any uses of $\{\sigma_{\neg A_i}\}$'s:

$$\left.\begin{array}{l} (\Gamma \longrightarrow \Delta)^{LE} \\ LE(\vec{p}, \vec{q}) \\ LE(\vec{p}, \vec{r}) \end{array}\right\} \overset{R_1'}{\Longrightarrow} \left.\begin{array}{l} \{\sigma_{A_1}, \ldots, \sigma_{A_u}\} \\ (\Gamma \longrightarrow \Delta)^{LE} \\ LE(\vec{p}, \vec{q}) \\ LE(\vec{p}, \vec{r}) \end{array}\right\} \overset{R_2}{\Longrightarrow} \emptyset$$

Q.E.D. Lemma.

From the Lemma & Interpolation Thm:

There is a circuit $C(\vec{p})$ of size $2^{n^{O(1)}}$ such that

(1) If $C(\vec{p}) = 0$, then $\{A_i(\vec{p}, \vec{q})\}_i$ is unsatisfiable

(2) If $C(\vec{p}) = 1$, then $\{B_j(\vec{p}, \vec{q})\}_j$ is unsatisfiable

Note the size of $C(\vec{p})$ is $2^{(\log N)^{O(1)}}$ which is quasipolynomial in $N = 2^n$.

In case (1), when $C(\vec{p}) = 0$, the function $\gamma(x)$ does not have a circuit of size $t = n^{\omega(1)}$.

In case (2), when $C(\vec{p}) = 1$, the function $(\gamma \oplus f)(x)$ does not have a circuit of size $t = n^{\omega(1)}$.

(Recall $f(x)$ does not have a circuit of size $2t + 1$.)

Defn: Let

$$C^*(\vec{p}) \overset{df}{=} (\neg C(\vec{p})) \vee C(\vec{p} \oplus f),$$

where $\vec{p} \oplus f$ is $p_0 \oplus f(0), \ldots p_{N-1} \oplus f(\underline{N-1})$. (Each $f(i)$ is 0 or 1, of course.)

Claim: Under the above assumptions, $C^*(\vec{p})$ is a quasipolynomial time property against $P/poly$.

Pf: There are three things to show:

(1) "Constructivity"

C^* has circuits of size $2^{(\log N)^{O(1)}}$ since C does.

(2) "Largeness" For all γ,
either $C^*(\gamma)$ or $C^*(\gamma \oplus f)$ holds (since either $\neg C(\gamma)$ holds, or $C((\gamma \oplus f) \oplus f)$ holds). Therefore, $C^*(\gamma)$ holds for at least half of the γ's.

(3) "Usefulness" We must show that if $C^*(\gamma)$ holds, then γ does not have a polynomial size circuit.

(3.a) If $\neg C(\vec{p})$, i.e., $C(\vec{p}) = 0$, then $\gamma = \vec{p}$ does not have a circuit of size t, by choice of C.

(3.b) If $C(\vec{p} \oplus f)$, i.e., $C(\vec{p} \oplus f) = 1$, then $(\vec{p} \oplus f) \oplus f = \vec{p}\ (= \gamma)$ likewise does not have a circuit of size t.

Q.E.D. Razborov's Theorem !!

The proof presented above is essentially a simplification of Razborov's proof, due to Krajíček.