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 a stronger version for first logic.

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

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

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

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

are tautologies.

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

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

where

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

Then clearly, $A(\vec{p}, \vec{q}) \models C(\vec{p})$.

Also, by the comment from the previous slide, $C(\vec{p}) \models B(\vec{p}, \vec{r})$. $\square$

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

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

\[
P \text{ is prime} \iff \exists \bar{r} B(\bar{p}, \bar{r}) \\
\iff \neg \exists \bar{q} A(\bar{p}, \bar{q}).
\]

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

An interpolant \( C(\bar{p}) \) **must** express “\( \bar{p} \) codes a composite”.

**Open:** Is primality expressible by a polynomial size formula?
Generalizing this example gives:

**Thm:** (Mundici’83-84) If there is a polynomial 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 \( P/poly \). \( \square \)
**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 cut-free $PK$ proof of $A \rightarrow B$, where $V(A) \subseteq \{\bar{p}, \bar{q}\}$ and $V(B) \subseteq \{\bar{p}, \bar{q}\}$. Then there is an interpolant $C$ such that

1. $A \supset C$ and $C \supset B$ are valid,
2. $V(C) \subseteq \{\bar{p}\}$,
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 $V(D) \subseteq \{\bar{p}, \bar{r}\}$ or $V(D) \subseteq \{\bar{p}, \bar{r}\}$
**Pf:** We prove by induction on the number of inferences in $P$ a slightly more general statement:

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

1. $\Gamma_1 \rightarrow \Delta_1, C$ and $C, \Gamma_2 \rightarrow \Delta_2$ are valid,
2. $V(C) \subseteq \{\bar{p}\}$, and
3. The polynomial size bounds hold too.

**Base Case:** Initial sequent.

If the initial sequent if $q_i \rightarrow q_i$, take $C$ to be $\bot$ since

$q_i \rightarrow q_i, \bot$ and $\bot \rightarrow$

are valid.

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

For an initial sequent $p_i \rightarrow p_i$, $C$ will be either $\top$, $\bot$, $p_i$ 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

\[
\Gamma \rightarrow \Delta, A, B \\
\Gamma \rightarrow \Delta, A \lor B
\]

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

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

or

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

depending on if \( A \lor B \) is in \( \Delta_1 \) or \( \Delta_2 \) (respectively).
(2) For last inference an \(\land\): right:

\[
\frac{\Gamma \rightarrow \Delta, A}{\Gamma \rightarrow \Delta, A \land B} \quad \frac{\Gamma \rightarrow \Delta, B}{\Gamma \rightarrow \Delta, A \land B}
\]

(2.a) If \(A \land B\) is in \(\Delta_1\), apply the induction hypothesis twice to have interpolants \(C_A\) and \(C_B\) so that

\[
\Gamma_1 \rightarrow \Delta_1^-, A, C_A \quad \Gamma_1 \rightarrow \Delta_1^-, B, C_B
\]

are valid. Now the derivations

\[
\Gamma_1 \rightarrow \Delta_1^-, A, C_A \quad \Gamma_1 \rightarrow \Delta_1^-, B, C_B
\]

\[
\Gamma_1 \rightarrow \Delta_1^-, A \land B, C_A \land C_B
\]

and

\[
\Gamma_1 \rightarrow \Delta_1^-, A \land B, C_A \land C_B
\]

\[
\Gamma_1 \rightarrow \Delta_1^-, A \land B, C_A \land C_B
\]

show \((C_A \lor C_B)\) is an interpolant.
(2b) If $A \land B$ is in $\Delta_2$ applying the induction hypothesis twice gives $C_A$ and $C_B$ so that

$$\Gamma_1 \rightarrow \Delta_1, C_A \quad \Gamma_1 \rightarrow \Delta_1, C_B$$

$$C_A, \Gamma_2 \rightarrow \Delta_2^-, A \quad C_B, \Gamma_2 \rightarrow \Delta_2^-, B$$

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

$$\Gamma_1 \rightarrow \Delta_1, C_A \quad \Gamma_1 \rightarrow \Delta_1, C_B$$

$$C_A, \Gamma_2 \rightarrow \Delta_2^-, A \quad C_B, \Gamma_2 \rightarrow \Delta_2^-, B$$

$$C_A \land C_B, \Gamma_2 \rightarrow \Delta_2^-, A \land B$$

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 $(\neg p)$ 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:**

\[
\frac{C \cup \{p\} \quad D \cup \{\overline{p}\}}{C \cup D}
\]

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

A *resolution refutation* of a set $\Gamma$ of clauses is a derivation of the empty clause $\emptyset$ from $\Gamma$ 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 \( \Gamma \) is inconsistent. Then there is a formula \( C(\vec{p}) \) such that for any truth assignment \( \tau \), \( \text{domain}(\tau) \supseteq \{\vec{p}, \vec{q}, \vec{r}\} \),

1. If \( \tau(C(\vec{p})) = \text{False} \), then
   \[
   \tau(A_i(\vec{p}, \vec{q})) = \text{False}, \text{ for some } i.
   \]
2. If \( \tau(C(\vec{p})) = \text{True} \), then
   \[
   \tau(B_j(\vec{p}, \vec{q})) = \text{False}, \text{ for some } j.
   \]

**Pf:** From \( \Gamma \) unsatisfiable, we have

\[
A_1(\vec{p}, \vec{q}), \ldots, A_k(\vec{p}, \vec{q}) \rightarrow \neg B_1(\vec{p}, \vec{r}), \ldots, \neg B_\ell(\vec{p}, \vec{r})
\]

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

\[
A_1(\vec{p}, \vec{q}), \ldots, A_k(\vec{p}, \vec{q}) \rightarrow C(\vec{p})
\]

and

\[
C(\vec{p}) \rightarrow \neg B_1(\vec{p}, \vec{r}), \ldots, \neg B_\ell(\vec{p}, \vec{r})
\]

are valid. \( \square \)
**Thm** (Krajíček’9?) Let \( \{A_i(\bar{p}, \bar{q})\}_i \cup \{B_j(\bar{p}, \bar{r})\}_j \) have a refutation \( R \) of \( n \) resolution inferences. Then an interpolant, \( C(\bar{p}) \), can be chosen with \( O(n) \) symbols in dag representation.

If \( R \) is tree-like, then \( C(\bar{p}) \) 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 \( C_E(\bar{p}) \) as follows:

1. For \( E = A_i(\bar{p}, \bar{q}) \), a hypothesis,
   set \( C_E = \bot (False) \).
2. For \( E = B_j(\bar{p}, \bar{q}) \), a hypothesis,
   set \( C_E = \top (True) \).
3. For an inference
   \[
   \frac{F \cup \{q_i\}}{F \cup G \cup \{\overline{q_i}\}}
   \]
   set \( C_{F \cup G} = C_{F \cup \{q_i\}} \lor C_{G \cup \{\overline{q_i}\}} \).
(4) For an inference \[
\frac{F \cup \{r_i\} \quad G \cup \{\overline{r}_i\}}{F \cup G}
\]
set \(C_{F \cup G} = C_{F \cup \{r_i\}} \land C_{G \cup \{\overline{r}_i\}}\).

(5) For an inference \[
\frac{F \cup \{p_i\} \quad G \cup \{\overline{p}_i\}}{F \cup G}
\]
set \(C_{F \cup G} = (\overline{p}_i \land C_{F \cup \{p_i\}}) \lor (p_i \land C_{G \cup \{\overline{p}_i\}})\).

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

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

(a) if \(\tau(C_F) = False\), then
\[
\tau(A_i(\overline{p}, \overline{q})) = False \text{ for some } i
\]

(b) if \(\tau(C_F) = True\), then
\[
\tau(B_j(\overline{p}, \overline{r})) = False \text{ for some } j
\]

**Proof 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, $\sigma_A$ is the extension variable for $A$:

For $p$ a variable, $\sigma_p$ is just $p$.

For other $A$, $\sigma_A$ 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. $LE(\neg A) = LE(A) \cup \{\{\neg \sigma_A, \sigma_A\}, \{\sigma_A, \sigma_A\}\}$
3. $LE(A \land B) = LE(A) \cup LE(B)$
   $$\cup \{\{\sigma_A \land \neg B, \sigma_A\}, \{\sigma_A \land B, \sigma_B\}, \{\sigma_A \land B, \sigma_A, \sigma_B\}\}$$
4. $LE(A \lor B) = LE(A) \cup LE(B)$
   $$\cup \{\{\neg \sigma_A, \sigma_A \lor B\}, \{\neg \sigma_B, \sigma_A \lor B\}, \{\sigma_A, \sigma_B, \sigma_A \lor B\}\}$$
**Defn:** Let \( A \) be a set of formulas. Then \( LE(A) \) is \( \bigcup_{A \in A} \{LE(A)\} \).

\[ LE(\bar{p}, \bar{q}) = \bigcup \{LE(A) : V(A) \subseteq \{\bar{p}, \bar{q}\}\} \]

\[ LE(\bar{p}, \bar{r}) = \bigcup \{LE(A) : V(A) \subseteq \{\bar{p}, \bar{r}\}\} \]

**Thm:** Let \( \Gamma \) be the set of clauses

\[ \{A_i(\bar{p}, \bar{q})\}_i \cup \{B_j(\bar{p}, \bar{r})\}_j \cup LE(\bar{p}, \bar{q}) \cup LE(\bar{p}, \bar{r}) \]

and suppose \( \Gamma \) has a refutation \( R \) of \( n \) resolution inferences.

Then there is an interpolant \( C(\bar{p}) \) for the sets \( \{A_i(\bar{p}, \bar{q})\}_i \) and \( \{B_j(\bar{p}, \bar{r})\}_j \) of circuit size \( O(n) \).

**Pf:** Let \( C(\bar{p}) \) be the interpolant for

\[ \{A_i(\bar{p}, \bar{q})\}_i \cup LE(\bar{p}, \bar{q}) \]

and

\[ \{B_j(\bar{p}, \bar{r})\}_j \cup LE(\bar{p}, \bar{r}) \]

given by the earlier interpolation theorem.
**Claim:** $C(\bar{p})$ is the desired interpolant.

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

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

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

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 $NP \not\subseteq P/poly$ 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 $G_n : \{0,1\}^n \rightarrow \{0,1\}^{2n}$ 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 $S$,

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

**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 $\alpha$ and $\beta$ 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 $\alpha$. Define:

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

where $\Sigma_1^b(X)$ indicates the closure of $X$ under $\land, \lor$, 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 $T_2^i$:

$$SS_2^i = BASIC + S\Sigma_i^b-PIND$$

$$ST_2^i = BASIC + S\Sigma_i^b-IND$$
Suppose superpolynomial lower bounds are provable in $S_2^2(\alpha)$ as follows.

Let $N \geq 0$ and $n = |N| \approx \log N$. \hspace{1cm} (\(n = |x|\)).

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

(2) By “$\alpha$ encodes a circuit” we mean that $\alpha$ encodes gate types and gate connections in some straightforward manner, plus, $\alpha$ 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

$$SS_2^2 \vdash SLB(t, S, \alpha, \beta)$$

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

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

**Pf:** If $\neg SLB(t, S, \alpha, \beta)$, then the circuit $\alpha' \left\{ \begin{array}{c} \alpha \\ \beta \end{array} \right\}$

satisfies $\neg LB(t, S, \alpha)$. □
By rephrasing $SLB(t, S, \alpha, \beta)$, we let $\gamma$ be a new predicate symbol and we have that if

\[ SS_2^2 \vdash SLB(t, S, \alpha, \beta), \]

then

\[ SS_2^2 \vdash \neg CC(t/2 - 1, \gamma, \alpha) \lor \neg CC(t/2 - 1, S \oplus \gamma, \beta) \]

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, $SS_2^2(\alpha)$ proves

\[ CC(t/2 - 1, \gamma, \alpha), CC(t/2 - 1, S \oplus \gamma, \beta) \rightarrow \]

Since $CC$ is a $\Sigma^b_1$ formula, this sequent is also provable in $ST^1_2$ by $\forall \Sigma^b_2$-conservativity. (By the same proof that shows $S_2^2$ is conservative over $T^1_2$.)
**Thm:** (Razborov’95) If $SS_2^2 \vdash SLB(t, S, \alpha, \beta)$ 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

$$ST_2^1 \vdash CC(t, \gamma, \alpha), CC(t, S \oplus \gamma, \beta) \rightarrow,$$

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

**First Step:** Convert the $ST_2^1$ proof and the sequent into a constant-depth propositional proof.
To convert to propositional logic

Use variables $q_i$ for the values of $\alpha$, i.e.,

$q_i$ denotes $\alpha_i$

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

By expanding the language to include the $\beta$ 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

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

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

$$2^{n^{O(1)}} n^{O(1)}$$

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

where each $E_{i,j}$ is (1) $\pm p_i$ or (2) involves only $p'$, $q'$ or (3) involves only $p'$, $r'$.
Fixing $N$ and $f(x) = S(N, \alpha)$, we obtain a propositional sequent calculus proof of:

$$\prod_{i} A_{i}(\bar{p}, \bar{q}), \prod_{j} B_{j}(\bar{p}, \bar{r}) \rightarrow$$

where:

(1) $\{A_{i}(\bar{p}, \bar{q})\}_{i}$ is a set of clauses stating that $\bar{q}$ codes a circuit of size $t$ computing the function $\gamma$ with graph given by $\bar{p}$.

(2) $\{B_{j}(\bar{p}, \bar{q})\}_{j}$ is a set of clauses stating that $\bar{r}$ 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 $\bar{p}, \bar{q}$ or just $\bar{p}, \bar{r}$ (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

\[
\bigwedge_{i=1}^{p_1} E_{1,i}, \ldots, \bigwedge_{i=1}^{p_{c'}} E_{c',i} \rightarrow \bigwedge_{i=1}^{q_1} F_{1,i}, \ldots, \bigwedge_{i=1}^{q_{c''}} F_{c'',i}
\]

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

\[
\bigwedge_{1}^{E_{1,1}}, \bigwedge_{1}^{E_{1,2}}, \ldots, \bigwedge_{1}^{E_{1,p_1}}, \bigwedge_{1}^{E_{2,1}}, \ldots, \bigwedge_{1}^{E_{c',p_{c'}}} \rightarrow \bigwedge_{i=1}^{F_1,i_1}, \bigwedge_{i=1}^{F_1,i_2}, \ldots, \bigwedge_{i=1}^{F_{c'',i_{c''}}}
\]

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

\[
\Gamma \rightarrow \Delta, \bigwedge_{i=1}^{p} F_i, \bigwedge_{i=1}^{p} F_i, \Gamma \rightarrow \Delta 
\]

\[
\Gamma \rightarrow \Delta
\]
is replaced by \( p \) cuts; i.e., by

\[
\Gamma^* \rightarrow \Delta^*, \ F_1, \ F_1, \ F_2, \ldots, \ F_p, \ \Gamma^* \rightarrow \Delta^*
\]

\[
\Gamma^* \rightarrow \Delta^*, \ F_2, \ F_2, \ F_3, \ldots, \ F_p, \ \Gamma^* \rightarrow \Delta^*
\]

\[
\Gamma^* \rightarrow \Delta^*, \ F_3, \ F_3, \ldots, \ F_p, \ \Gamma^* \rightarrow \Delta^*
\]

\[
\vdots
\]

\[
\Gamma^* \rightarrow \Delta^*
\]

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

\[
A_1(p, q), \ldots, A_k(p, q), B_1(p, r), \ldots, B_\ell(p, r) \rightarrow
\]

such that every formula in the proof is a disjunction of formulas which either involve just \( p \) and \( q \) or involve just \( p \) and \( r \).
**Third Step:** Convert to a resolution with limited extension refutation.

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

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

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

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

$$\begin{align*}
\{ \{E_{1,i}\}_{i=1}^{p_1}, \ldots, \{E_{u,i}\}_{i=1}^{p_u} & , \ \{\neg F_{1,1}, \}, \{\neg F_{1,2}, \}, \ldots, \{\neg F_{v,q_v}, \} \} \quad (B)
\end{align*}$$

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:

\[
\begin{align*}
\{ \{ \sigma_{E_1,i} \} &_{i=1}^{p_1}, \ldots, \{ \sigma_{E_u,i} \} &_{i=1}^{p_u} , \\
\{ \sigma_{\neg F_1,1}, \} & , \{ \sigma_{\neg F_1,2}, \} , \ldots, \{ \sigma_{\neg F_v,q_v}, \} \}
\end{align*}
\]  

(C)

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

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

\[
(\Gamma \rightarrow \Delta)^{LE} \cup LE(\bar{p}, \bar{q}) \cup LE(\bar{p}, \bar{r})
\]

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) $\Gamma \rightarrow \Delta$ is $A \rightarrow A$.

If $A = \bigvee A_i$, then

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

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

Case (2): Suppose $A = \bigvee A_i$ involves only $\bar{p}, \bar{q}$. 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 formulas that use just $\bar{p}, \bar{q}$ or just $\bar{p}, \bar{r}$; these are therefore straightforward (the $\wedge$:right is a little harder than the $\vee$:left case).

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

$$\begin{align*}
\bigvee_i E_i, \Gamma &\rightarrow \Delta \\
\bigvee_j F_j, \Gamma &\rightarrow \Delta \\
\bigvee \{E_i, F_j\}_{i,j}, \Gamma &\rightarrow \Delta
\end{align*}$$
Case (4) cont’d: The induction hypotheses give refutations $R_1$ and $R_2$:

$$(\Gamma \rightarrow \Delta)^{LE}$$

$\{\sigma_{E_i}\}_i$

$LE(\vec{p}, \vec{q})$

$LE(\vec{p}, \vec{r})$

$\overset{R_1}{\Rightarrow} \emptyset$

and

$$(\Gamma \rightarrow \Delta)^{LE}$$

$\{\sigma_{F_j}\}_j$

$LE(\vec{p}, \vec{q})$

$LE(\vec{p}, \vec{r})$

$\overset{R_2}{\Rightarrow} \emptyset$

Combine these as:

$$(\Gamma \rightarrow \Delta)^{LE}$$

$\{\sigma_{E_i}\}_i \cup \{\sigma_{F_j}\}_j$

$LE(\vec{p}, \vec{q})$

$LE(\vec{p}, \vec{r})$

$\overset{R_1'}{\Rightarrow} \{\sigma_{F_j}\}_j$

$$(\Gamma \rightarrow \Delta)^{LE}$$

$\overset{R_2}{\Rightarrow} \emptyset$

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 $R_2$. 

32
Case 5: Last inference is cut:

\[
\frac{\Gamma \rightarrow \Delta, \bigvee_i A_i \quad \bigvee_i A_i, \Gamma \rightarrow \Delta}{\Gamma \rightarrow \Delta}
\]

The induction hypotheses give refutations \( R_1 \) and \( R_2 \):

\[
(\Gamma \rightarrow \Delta)^{LE} \quad \left\{ \{\sigma_{-A_1}\}, \ldots, \{\sigma_{-A_u}\}\right\} \quad \left\{ \begin{array}{c} LE(\vec{p}, \vec{q}) \\ LE(\vec{p}, \vec{r}) \end{array} \right\} \quad \overset{R_1}{\Rightarrow} \quad \emptyset
\]

and

\[
(\Gamma \rightarrow \Delta)^{LE} \quad \left\{ \{\sigma_{A_1}, \ldots, \sigma_{A_u}\}\right\} \quad \left\{ \begin{array}{c} LE(\vec{p}, \vec{q}) \\ LE(\vec{p}, \vec{r}) \end{array} \right\} \quad \overset{R_2}{\Rightarrow} \quad \emptyset
\]

Combine these as below, with \( R' \) equal to \( R_1 \) minus any uses of \( \{\sigma_{-A_i}\} \)'s:

\[
(\Gamma \rightarrow \Delta)^{LE} \quad \left\{ \begin{array}{c} LE(\vec{p}, \vec{q}) \\ LE(\vec{p}, \vec{r}) \end{array} \right\} \quad \overset{R'}{\Rightarrow} \quad \left\{ \{\sigma_{A_1}, \ldots, \sigma_{A_u}\}\right\} \quad \left\{ \begin{array}{c} (\Gamma \rightarrow \Delta)^{LE} \\ LE(\vec{p}, \vec{q}) \\ LE(\vec{p}, \vec{r}) \end{array} \right\} \quad \overset{R_2}{\Rightarrow} \quad \emptyset
\]

Q.E.D. Lemma.
From the Lemma & Interpolation Thm:
There is a circuit $C(\bar{p})$ of size $2^{n^{O(1)}}$ such that
(1) If $C(\bar{p}) = 0$, then $\{A_i(\bar{p}, \bar{q})\}_i$ is unsatisfiable
(2) If $C(\bar{p}) = 1$, then $\{B_j(\bar{p}, \bar{q})\}_j$ is unsatisfiable
Note the size of $C(\bar{p})$ is $2^{(\log N)^{O(1)}}$ which is quasipolynomial in $N = 2^n$.
In case (1), when $C(\bar{p}) = 0$, the function $\gamma(x)$ does not have a circuit of size $t = n^{\omega(1)}$.
In case (2), when $C(\bar{p}) = 1$, 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
$$C^*(\bar{p}) \overset{df}{=} (-C(\bar{p})) \lor C(\bar{p} \oplus f),$$
where $\bar{p} \oplus f$ is $p_0 \oplus f(0), \ldots p_{N-1} \oplus f(N-1)$.
(Each $f(i)$ is 0 or 1, of course.)
Claim: Under the above assumptions, $C^*(\bar{p})$ 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 $\gamma$, 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 $\gamma$'s.

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

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

3.b) If $C(\bar{p} \oplus f)$, i.e., $C(\bar{p} \oplus f) = 1$, then $(\bar{p} \oplus f) \oplus f = \bar{p} (= \gamma)$ 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.