Bounded Arithmetic

and

<u>Propositional Proofs</u>

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

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

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 $A(\vec{p}, \vec{q})$ 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 $\wedge$'s and $\vee$'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 $\bot$ since

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

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 $\top$, $\bot$, 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 $\vee right$

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

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 $A \vee B$ 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

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

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

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. $\square$

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. $\Box$

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:

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

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

<u>Usefulness</u>: 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!

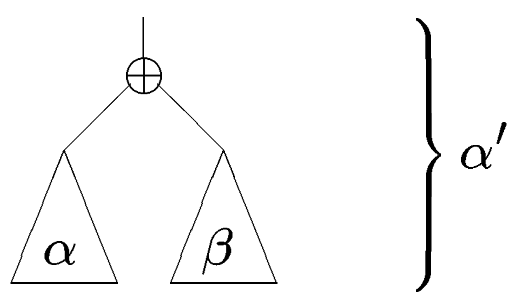
Thm: If $S^2_2(\alpha) \vdash LB(t, S, \alpha)$, then

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

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

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

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



satisfies $\neg LB(t, S, \alpha)$. $\square$

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:

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

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 $\bigwedge\!\!\!\bigwedge$'s from the proof as follows.

(a) Given a sequent

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

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 $\bigwedge\!\!\!\bigwedge_{i=1}^{p} F_i$. For this, an inference

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

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:

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

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 $A = \bigvee_i A_i$ 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:

$$\frac{\bigvee_i E_i, \Gamma \longrightarrow \Delta \qquad \bigvee_j F_j, \Gamma \longrightarrow \Delta}{\vee\{E_i, F_j\}_{i,j}, \Gamma \longrightarrow \Delta}$$

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

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

and

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

Combine these as:

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

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.

<u>Case 5</u>: 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:

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

and

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

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

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

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

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

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 Krajı̌ček.