Today:

Feasible Interpolation & Automatizability

Cutting Planes

LBs for CPs via Feasible Interpolation

Reminder: email me about course presentations

Automatizability : Meta-algorithmic question

Searching for P-proofs of f

- # of proofs of size $s \approx 2^s$
- there is always a proof of size 2^n and easy to find

Q: Can we find a P-proof in time poly(size of smallest P-proof)?

Defn [Bonet-P-Raz]

P is **automatizable** in time $f(s)$ if $\exists$ algorithm A that given an UNSAT F, outputs a P-refutation of F in time $f(s)$, where s = size of shortest P-refutation of F

Automatizability: motivation

1. Fundamental algorithmic question behind automated theorem proving / SAT solvers

2. Has lead to amazing new algorithms for unsupervised learning problems, as well as approximation algorithms (SOS)

   (P automatizable + efficient P-proof of sample complexity upper Bounds $\Rightarrow$ efficient learning alg)

3. (Nearly) Equivalent to Feasible interpolation

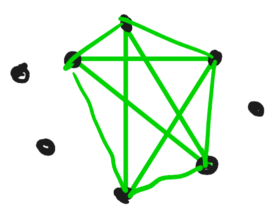
4. Connections to PAC Learning

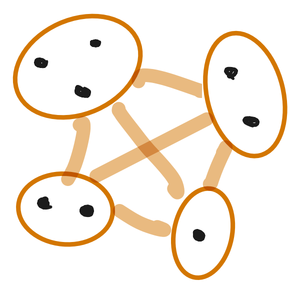
Feasible Interpolation [Krajicek]

Interpolant formula: $A(\vec{x}, \vec{z}) \wedge B(\vec{y}, \vec{z})$

Interpolant function $f_{A,B}(\alpha) = \begin{cases} 1 \text{ if } A(\vec{x}, \alpha) \text{ is SAT} \\ 0 \text{ if } B(\vec{y}, \alpha) \text{ is SAT} \\ * \text{ otherwise} \end{cases}$

Example 1: $\mathrm{Clique}_k(\vec{x}, \vec{z}) \wedge \mathrm{Color}_{k-1}(\vec{y}, \vec{z})$





$K=5$

Feasible Interpolation [Krajicek]

Interpolant formula: $A(\vec{x}, \vec{z}) \wedge B(\vec{y}, \vec{z})$

Interpolant function

$$f_{A,B}(\alpha) = \begin{cases} 1 \text{ if } A(\vec{x}, \alpha) \text{ is SAT} \\ 0 \text{ if } B(\vec{y}, \alpha) \text{ is SAT} \\ * \text{ otherwise} \end{cases}$$

Example 1: $\mathrm{Clique}_k(\vec{x}, \vec{z}) \wedge \mathrm{Color}_{k-1}(\vec{y}, \vec{z})$

Example 2: $\underbrace{\mathrm{Ref}_P(\vec{x}, \vec{z})}_{\vec{x} \text{ is a } P \text{ refutation of } \vec{z}} \wedge \underbrace{\mathrm{SAT}(\vec{y}, \vec{z})}_{\vec{y} \text{ is a satisfying assignment of } \vec{z}}$

Disjoint NP Pairs

Feasible Interpolation [Krajicek]

Interpolant formula: $A(\vec{x},\vec{z}) \wedge B(\vec{y},\vec{z})$

Interpolant function $f_{A,B}(\alpha) = \begin{cases} 1 & \text{if } A(\vec{x},\alpha) \text{ is SAT} \\ 0 & \text{if } B(\vec{y},\alpha) \text{ is SAT} \\ * & \text{otherwise} \end{cases}$

Extracts computational content from proof

Defn [Krajicek]

P has feasible interpolation if there is a circuit $C(\alpha)$ that computes $f_{A,B}$ for every UNSAT interpolant formula $A \wedge B$, and size(C) is poly in size of P-refutation of $f_{A,B}$

Feasible Interpolation [Krajicek]

Interpolant formula: $A(\vec{x}, \vec{z}) \wedge B(\vec{y}, \vec{z})$

Interpolant function $f_{A,B}(\alpha) = \begin{cases} 1 \text{ if } A(\vec{x}, \alpha) \text{ is SAT} \\ 0 \text{ if } B(\vec{y}, \alpha) \text{ is SAT} \\ * \text{ otherwise} \end{cases}$

Defn [Krajicek]

P has monotone feasible interpolation if whenever the $\vec{z}$-variables occur only negatively in B and positively in A, C is a monotone circuit (of size polynomial in the size of P-refutation of $f_{A,B}$

Automatizability + Feasible Interpolation

Interpolant formula: $A(\vec{x},\vec{z}) \wedge B(\vec{y},\vec{z})$

Interpolant function $f_{A,B}(\alpha) = \begin{cases} 1 \text{ if } A(\vec{x},\alpha) \text{ is SAT} \\ 0 \text{ if } B(\vec{y},\alpha) \text{ is SAT} \\ * \text{ otherwise} \end{cases}$

Theorem [BPR]

1. Automatizability $\Rightarrow$ feasible interpolation

2. for suff strong P (that can efficiently prove their reflection principle)

   feasible interp $\Rightarrow$ automatizability

BPR: "On interpolation and automatization for Frege systems"

Bonet-Pitassi-Raz

Automatizability + Feasible Interpolation

Interpolant formula: $A(\vec{x},\vec{z}) \wedge B(\vec{y},\vec{z})$

Interpolant function $f_{A,B}(\alpha) = \begin{cases} 1 & \text{if } A(\vec{x},\alpha) \text{ is SAT} \\ 0 & \text{if } B(\vec{y},\alpha) \text{ is SAT} \\ * & \text{otherwise} \end{cases}$

Theorem [BPR]

1. Automatizability $\Rightarrow$ feasible interpolation
2. for suff strong P (that can efficiently prove their reflection principle)

   feasible interp $\Rightarrow$ automatizability

$\therefore$ automatizability of P $\approx$ proofs in P are "simple"

$\approx$ superpoly LBs for P (via feas. interp)

① Automizable $\rightarrow$ Feasible Interp. [Impagliazzo, BPR]

Let $A(\vec{x},\vec{z}) \wedge B(\vec{y},\vec{z})$ have a P-refutation Π

Algorithm to solve $f_{A,B}$:

on input α, run autom alg for $|\Pi|$ steps
on $A(\vec{x},\alpha)$. If it outputs a refutation output "A unsat"
else output "B unsat"

Key point: If $B(\vec{y},\alpha)$ satisfiable, let β be satisfying assignment. Then $A(\vec{x},\alpha) \wedge B(\beta,\alpha) = A(\vec{x},\alpha) \wedge 1$

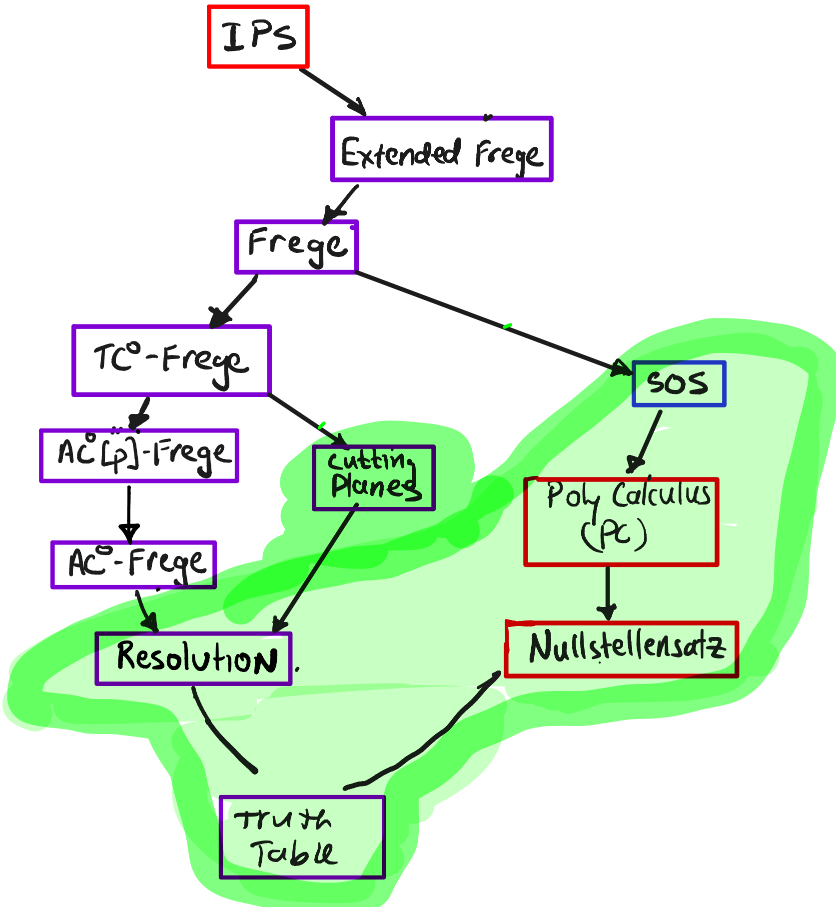
So $\Pi|_{\vec{z}=\alpha,\ \vec{y}=\beta}$ is a refutation of $A(\vec{x},\alpha)$

2. If P can prove its own soundness

then Feasible Interp for P $\rightarrow$ automizability of P

See Pudlak "On reducibility and symmetry of Disjoint NP pairs"

Feasible Interpolation - UPPER BOUNDS



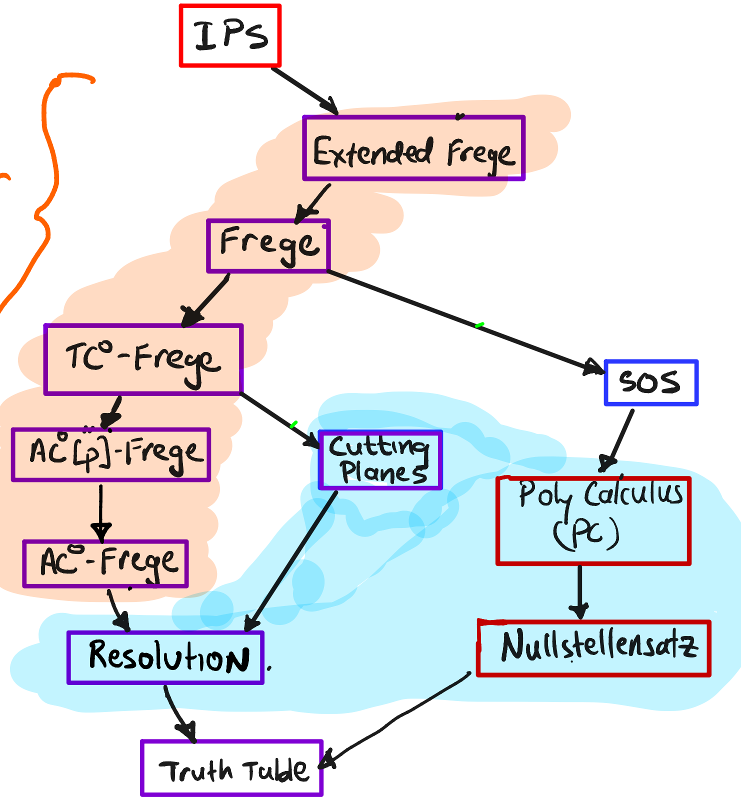
Automatizability - LOWER BOUNDS

NON-automatizable in polytime under crypto assumptions

EF: RSA

Rest: Diffie-Hellman

[KP'98, BPR'97, BDGMP'99]



non-automatizable in polytime unless W[P] = FPT [AR'01]

NP-hard to automate [AM'19]

[dRGNPRS'21, GKMP'20]

Cutting Planes

Refutation system for proving unsolvability of a system of linear inequalities where vars $x_1 \dots x_n \in \mathbb{Z}$

Defn (Cutting Planes Refutations)

Let $Ax \geq b$ be a system of integer linear inequalities

$$\{a^1 \cdot x \geq b^1,\ a^2 \cdot x \geq b^2,\ \dots,\ a^m \cdot x \geq b^m\} \qquad A \in \mathbb{Z}^{m \times n}, \quad b \in \mathbb{Z}^m$$

$$\overset{A}{\boxed{}} \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} \geq \bar{b}$$

A cutting planes (CP) refutation of $Ax \geq b$ is a sequence of inequalities such that each line (inequality) is either one of original ones or follows from previously derived inequalities by one of the following rules:

Division Rule

$$\frac{a \cdot x \geq c}{\frac{a}{d} \cdot x \geq \lceil \frac{c}{d} \rceil}$$

where d divides every a_i

Non-Neg Linear Combination

$$\frac{a \cdot x \geq c \qquad b \cdot x \geq d}{(\alpha a + \beta b) x \geq \alpha c + \beta d}$$

where $\alpha, \beta \geq 0$

Cutting Planes

Division Rule

$$\frac{a \cdot x \geq c}{\frac{a}{d} \cdot x \geq \lceil \frac{c}{d} \rceil}$$

where d divides every a_i

Non-Neg Linear Combination

$$\frac{a \cdot x \geq c \qquad b \cdot x \geq d}{(\alpha a + \beta b) x \geq \alpha c + \beta d}$$

where $\alpha, \beta \geq 0$

Observations:

① To refute a CNF $F = C_1 \wedge \dots \wedge C_m$: convert each clause to linear inequality

$$x_1 \vee \bar{x}_2 \vee x_3 \rightsquigarrow x_1 + (1 - x_2) + x_3 \geq 1$$

and add $2n$ additional inequalities $\{x_i \geq 0,\ x_i \leq 0 \mid i \in [n]\}$

② Linear comb'n rule is sound even over $\mathbb{R}$; Division rule preserves only integer solutions

③ For refuting CNFs, can assume wlog all coefficients have magnitude $\leq 2^{n^2}$. Therefore size(π) can be measured by # of lines (linear ineq's) in the CP refutation

④ CPs is SOUND + COMPLETE

Cutting Planes Complexity

① CP p-simulates Resolution

② Res does not p-simulate CPs.

In particular, 1-1, onto PHP^n_{n-1} has polysize CP refutations

but we showed PHP^n_{n-1} requires exponential-size Res refutations

③ There are UNSAT CNFs $\{F_n\}_{n>0}$ requiring exponential-size CPs refutations

Cutting Planes Complexity

① CP p-simulates Resolution

$$\frac{(x_1 \vee x_2 \vee x_3) \quad (\bar{x}_1 \vee x_4)}{x_2 \vee x_3 \vee x_4}$$

$x_1 + x_2 + x_3 \geq 1 \qquad 1 - x_1 + x_4 \geq 1$

addition rule

$x_1 + x_2 + x_3 + (1 - x_1) + x_4 \geq 2$

$= x_2 + x_3 + x_4 \geq 1$

$$\frac{(x_1 \vee x_2 \vee x_3) \quad (\bar{x}_1 \vee x_2 \vee x_4)}{x_2 \vee x_3 \vee x_4}$$

$x_1 + x_2 + x_3 \geq 1 \qquad 1 - x_1 + x_2 + x_4 \geq 1$

addition

$2x_2 + x_3 + x_4 \geq 1 \qquad x_3 \geq 0 \qquad x_4 \geq 0$

addition

$2x_2 + 2x_3 + 2x_4 \geq 1$

division w/ rounding

$x_2 + x_3 + x_4 \geq 1$

Cutting Planes Complexity

(2) 1-1 onto PHP^n_{n-1} has short CPs refutations

(a) $\forall i \in [n] \quad P_{i1} + P_{i2} + \dots + P_{i\,n-1} \geq 1$

(b) $\forall i \neq i' \in [n], \; j \in [n-1] \quad P_{ij} + P_{i'j} \leq 1$

$\Big\}$ Initial equations for PHP^n_{n-1}

* (1) Derive : $\forall j \in [n-1] \quad P_{1j} + P_{2j} + \dots + P_{n,j} \leq 1$ } Hole inequalities

(2) Add up all eqns from (1) to derive $\sum_{\substack{i \in [n] \\ j \in [n-1]}} P_{ij} \leq n-1$

(3) Add up all eqns from (a) to derive $\sum_{\substack{i \in [n] \\ j \in [n-1]}} P_{ij} \geq n$

(4) Add (2) + (3) to derive $0 \geq 1$

It is left to derive hole inequalities: $\forall j \in [n-1]$: $P_{1j} + P_{2j} + \dots + P_{nj} \le 1$

(1.) $P_{1j} + P_{2j} \le 1$ is an original inequality from (6)

(2) Say we've derived (*) $P_{1j} + P_{2j} + \dots + P_{n'j} \le 1$, $n' < n$

To derive $P_{1j} + P_{2j} + \dots + P_{n'+1,j} \le 1$:

(i) sum up: $P_{ij} + P_{n'+1,j} \le 1$ for all $i = 1 \dots n'$ to get

$$\sum_{i=1}^{n'} P_{ij} + n' \cdot P_{n'+1,j} \le n'$$

(ii) Multiply (*) by $n'-1$ to get $(n'-1) \sum_{i=1}^{n'} P_{ij} \le n'-1$

(iii) Add (i), (ii) : $n' \sum_{i=1}^{n'+1} P_{ij} \le 2n'-1$

(iv) Divide (iii) by n' (with rounding): $\sum_{i=1}^{n'+1} P_{ij} \le 1$

$\blacksquare$

Exponential LBs for CPs - Feasible Interpolation

Defn A CNF $F(\vec{x}, \vec{y}, \vec{z})$ is in split-form if $F = A(\vec{x}, \vec{z}) \wedge B(\vec{y}, \vec{z})$ where A, B are CNFs.

Defn [Interpolant (partial) function associated with a split CNF]
Let $F = A(\vec{x}, \vec{z}) \wedge B(\vec{y}, \vec{z})$. Then define

$$f_F(\vec{z}) = \begin{cases} 1 & \text{if } A(\vec{x}, \vec{z}) \text{ is satisfiable} \\ 0 & \text{if } B(\vec{x}, \vec{z}) \text{ is satisfiable} \\ * & \text{otherwise} \end{cases}$$

Exponential LBs for CPs - Feasible Interpolation

Defn A CNF $F(\vec{x},\vec{y},\vec{z})$ is in split-form if $F = A(\vec{x},\vec{z}) \wedge B(\vec{y},\vec{z})$ where A, B are CNFs.

Defn [Interpolant (partial) function associated with a split CNF]
Let $F = A(\vec{x},\vec{z}) \wedge B(\vec{y},\vec{z})$. Then define
$$f_F(\vec{z}) = \begin{cases} 1 & \text{if } A(\vec{x},\vec{z}) \text{ is satisfiable} \\ 0 & \text{if } B(\vec{x},\vec{z}) \text{ is satisfiable} \\ * & \text{otherwise} \end{cases}$$

Example (Clique-Coclique formula)

$$F = \mathrm{Clique}_k(\vec{x},\vec{z}) \wedge \mathrm{Color}_{k-1}(\vec{y},\vec{z})$$

$\vec{z}$ variables: $n \times n$ matrix representing an undirected graph $g = (V,E)$, $|V| = n$

$\vec{x}$ variables: $k \times n$ matrix that represents a clique of size k (a subset $S \subseteq V$, $|V| = k$)

$\vec{y}$ variables: $(k-1) \times n$ matrix that represents a $(k-1)$-coloring of V

Example (Clique-Coclique formula)

$$F = \text{Clique}_k(\vec{x}, \vec{z}) \wedge \text{Color}_{k-1}(\vec{y}, \vec{z})$$

$\vec{z}$ variables: $n \times n$ matrix representing an undirected graph $G = (V, E)$, $|V| = n$

$\vec{x}$ variables: $k \times n$ matrix that represents a clique of size k (a subset $S \subseteq V$, $|V| = k$)

$\vec{y}$ variables: $(k-1) \times n$ matrix that represents a $(k-1)$-coloring of V

$\text{Clique}_k(\vec{x}, \vec{z})$:

(i) $\forall i \in [k] \quad \bigvee_{v=1}^{n} x_{i,v}$

(ii) $\forall i \neq j \in [k], v \in [n] \quad \bar{x}_{i,v} \vee \bar{x}_{j,v}$

$\vec{x}$ defines a subset $S \subseteq [n]$ of size $\geq k$

(iii) $\forall u \neq v \in [n], i \neq j \in [k] \quad \bar{x}_{i,u} \vee \bar{x}_{j,v} \rightarrow z_{u,v}$

all edges between clique vertices are in G

$\text{Color}_k(\vec{y}, \vec{z})$:

(1.) $\forall u \in [n] \quad \bigvee_{i=1}^{k-1} y_{i,u}$

(2) $\forall u \in [n], \forall i \neq j \in [k-1] \quad \bar{y}_{i,u} \vee \bar{y}_{j,u}$

$\vec{y}$ defines legal coloring of $[n]$

(3) $\forall u \neq v \in [n], \forall i \in [k-1] \quad \bar{y}_{i,u} \vee \bar{y}_{i,v} \vee \bar{z}_{u,v}$

There is no edge in G between vertices of different colors

Example (Clique-Coclique formula) $F = \text{Clique}_k(\vec{x}, \vec{z}) \wedge \text{Color}_{k-1}(\vec{y}, \vec{z})$

Interpolant function for Clique-coclique:

$$f(\vec{z}) = \begin{cases} 1 & \text{if graph encoded by } \vec{z} \text{ contains a } k\text{-clique} \\ 0 & \text{if graph '' '' } \vec{z} \text{ has a } (k-1)\text{-coloring} \\ * & \text{otherwise} \end{cases}$$

$\boxed{\text{Feasible Interpolation Theorem for CP}}$

There exists a polysized circuit $C(F, \Pi, \alpha)$ that outputs $f_F(\alpha)$.

split formula over $\vec{x}, \vec{y}, \vec{z}$ — CP refutation of F — assignment to $\vec{z}$ variables

Furthermore

(a) if $A(\vec{x}, \vec{z})$ is monotone in $\vec{z}$ (only contains positive z-literals) then Circuit C is a monotone real circuit.

(b) and if all coefficients in Π have magnitude $\leq \text{poly}(n)$ then C is a monotone Boolean circuit

Defn Fix k. A <u>minterm</u> (for clique-coclique formula) is a graph containing a k-clique and no other edges

A <u>maxterm</u> is a maximal graph that is $(k-1)$-colorable (its vertices partitioned into $k-1$ groups such that $e_{ij} = 1$ iff vertices i and j belong to different groups)

$k=5$

Theorem [Razborov, "Lower Bounds on the monotone complexity of some Boolean functions"]

Let $k = \sqrt{n}$. Then any monotone circuit C that accepts all minterms and rejects all maxterms has size $2^{\Omega(n^{\varepsilon})}$ for some $\varepsilon > 0$

Feasible Interpolation for CP

Lemma There is a polytime alg $A(F, \Pi, \alpha)$ that outputs $f_F(\alpha)$.

Proof Fix F, Π, and assignment α to $\vec{z}$.

We will show: for each line $f(\vec{x}) + g(\vec{y}) + h(\vec{z}) \geq D$ in Π, $\exists D_0, D_1$, $D_0 + D_1 \geq D - h(\alpha)$

such that we can derive in CPs: $f(\vec{x}) \geq D_0$ from $A(\vec{x}, \alpha)$

$g(\vec{y}) \geq D_0$ from $B(\vec{y}, \alpha)$

Thus we obtain CP derivations of $0 \geq D_0$ from $A(\vec{x}, \alpha)$ and $0 \geq D_1$ from $B(\vec{y}, \alpha)$.

Since either $D_0 \geq 1$ or $D_1 \geq 1$ we have a refutation of $0 \geq 1$ from either $A(\vec{x}, \alpha)$ or from $B(\vec{x}, \alpha)$.

So $A(F, \Pi, \alpha)$ computes D_0 + D_1 + outputs 1 if $D_1 \geq 1$ and 0 if $D_0 \geq 0$.

Feasible Interpolation for CP

Lemma There is a polytime alg $A(F, \Pi, \alpha)$ that outputs $f_F(\alpha)$.

Proof Fix F, Π, and assignment α to $\vec{z}$.

We will show: for each line $f(\vec{x}) + g(\vec{y}) + h(\vec{z}) \geq D$ in Π, $\exists D_0, D_1$, $D_0 + D_1 \geq D - h(\alpha)$

such that we can derive in CPs: $f(\vec{x}) \geq D_0$ from $A(\vec{x}, \alpha)$

$g(\vec{y}) \geq D_0$ from $B(\vec{y}, \alpha)$

- BASE CASE: True for initial clauses
- Linear combination (assume addition) $\quad f_1(\vec{x}) + g_1(\vec{y}) + h_1(\vec{z}) \geq C \quad f_2(\vec{x}) + g_2(\vec{y}) + h_2(\vec{z}) \geq D$

$f_1(\vec{x}) \geq C_0 \quad g_1(\vec{y}) \geq C_1 \qquad f_2(\vec{x}) \geq D_0 \quad g_2(\vec{y}) \geq D_1 \qquad$ By induction

$C_0 + C_1 \geq C - h_1(\alpha) \qquad D_0 + D_1 \geq D - h_2(\alpha)$

$f_1(\vec{x}) + f_2(\vec{x}) \geq C_0 + D_0 \qquad g_1(\vec{y}) + g_2(\vec{y}) \geq C_1 + D_1 \qquad$ Addition

Feasible Interpolation for CP

Lemma There is a polytime alg $A(F, \Pi, \alpha)$ that outputs $f_F(\alpha)$.

Proof Fix F, Π, and assignment α to $\vec{z}$.

We will show: for each line $f(\vec{x}) + g(\vec{y}) + h(\vec{z}) \geq D$ in Π, $\exists D_0, D_1$, $D_0 + D_1 \geq D - h(\alpha)$

such that we can derive in CPs: $f(\vec{x}) \geq D_0$ from $A(\vec{x}, \alpha)$

$g(\vec{y}) \geq D_0$ from $B(\vec{y}, \alpha)$

- BASE CASE: True for initial clauses
- Division w/ rounding: $f(x) + g(y) + h(z) \geq D \longrightarrow \frac{1}{d}(f(x) + g(y) + h(z)) \geq \lceil D/d \rceil$

$f(x) \geq D_0 \quad g(y) \geq D_1, \quad D_0 + D_1 \geq D - h(\alpha)$ By induction

$\frac{1}{d} f(x) \geq \left\lceil \frac{D_0}{d} \right\rceil \quad \frac{1}{d} g(y) \geq \left\lceil \frac{D_1}{d} \right\rceil$ Division

where: $\lceil D_0/d \rceil + \lceil D_1/d \rceil \geq \lceil (D_0 + D_1)/d \rceil \geq \lceil (D - h(\alpha))/d \rceil = \lceil D \rceil - h(\alpha)/d$

since d divides $h(\alpha)$

$\boxed{\text{Feasible Interpolation Theorem for CP}}$

There exists a polysized circuit $C(F, \Pi, \alpha)$ that outputs $f_F(\alpha)$.

split formula over $\vec{x}, \vec{y}, \vec{z}$ — CP refutation of F — assignment to $\vec{z}$ variables

Furthermore

(a) if $A(\vec{x}, \vec{z})$ is monotone in $\vec{z}$ (only contains positive z-literals) then C is a monotone real circuit then Circuit C is a monotone real circuit.

(b) and if all coefficients in Π have magnitude $\leq poly(n)$ then C is a Boolean monotone circuit

Defn A monotone real circuit for $f: \{0,1\}^n \to \{0,1\}$ is a sequence of functions $g_1, \ldots, g_s$ where $g_s = f$ and $\forall i < s$ g_i satisfies one of these conditions:

- $g_i = x_i$
- There is a monotone real function $\phi: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, and $j, k < i$ such that $g_i = \phi(g_j, g_k)$

Proof of Feasible Interpolation for CP follows from previous Lemma by inspection (show for every line in split proof, there is a monotone real ckt that computes $-D_0$). Axioms: $-D_0 = h(\alpha) - D$ which is monotone function of α since z only occurs positively in $A(x, z)$

Intermediate Lines: use additions, multipl. by nonneg constants, division which are all monotone real functions

Cutting Planes Lower Bounds

Theorem (Clique-Coclique formula) $F = \text{Clique}_k(\vec{x}, \vec{z}) \wedge \text{Color}_{k-1}(\vec{y}, \vec{z})$

Any CP refutation of Clique-Coclique formula requires exponential size

Pf

1. By monotone Feasible Interpolation for CPs, a size S CP refutation implies $\text{poly}(S)$ size monotone real circuits for separating k-cliques from $k-1$-colorable graphs, $\forall k$

2. By [Razborov] (for low coefficient case) and [Cook-Haken] (for general case), monotone real circuits for clique-coclique require size $\exp(n^\varepsilon)$

   $\therefore$ for $k = \delta n$; this implies $2^{\Omega(n^\varepsilon)}$ CP Lower bounds.

Other Results and Open problems

1. For a long time the only LBs for CP were via feasible interpolation, and therefore they only held for "split" formulas.
   Recently [Fleming-Pankratov-P.-Robere] and [Hrubes-Pudlak] managed to prove exponential LBs for random kCNFs, $k = O(\log n)$ by generalizing the feasible interp. method to arbitrary formulas.

   Open: Improve the CP LBs for random kCNFs for $k = O(1)$.

2. For Resolution, we have exponential LBs for random k-CNFs for all $k \geq 3$.
   Proof uses random restrictions, or a slick argument [Beame-Karp-Saks-P]
   We may do this later.