# Proof Complexity
# Part D: Pseudo-Boolean and Algebraic Proof Systems, and Automatizability

Sam Buss

Satisfiability Boot Camp
Simons Institute, Berkeley, California
January–May 2021

Part D. discusses:

- Cutting Planes
- Clique-Coloring Principle
- Interpolation
- Nullstellensatz
- Polynomial Calculus
- Automatizability

# Cutting planes proofs

**Cutting planes** is a propositional proof system based on integer programming [Gomory'63; Chvátal'73; Cook-Coullard-Turán'87]

**Variables** $x_1, x_2, \ldots$ are **0/1 valued** (0="False", 1="True").

Lines in a cutting planes proof are **linear inequalities with integer coefficients**:

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \geq a_0.$$

Clauses become inequalities: for example

$x \vee y \vee z$ becomes $x + y + z \geq 1$, and

$x \vee \overline{y} \vee z$ becomes $x - y + z \geq 0$.

Note that $\overline{y}$ is replaced with $1 - y$.

# Cutting planes refutations

Cutting planes is a *refutation system*:
Initial lines are logical axioms,
or encode hypotheses (often obtained from clauses).

**Logical axioms:** $x_i \geq 0$ and $-x_i \geq -1$.

Valid inferences are *Addition* and *Division*.

**Addition rule:**

$$\frac{\sum a_i x_i \geq a_0 \qquad \sum b_i x_i \geq b_0}{\sum (a_i + b_i) x_i \geq a_0 + b_0}$$

**Division rule:** If $c > 0$ and $c | a_i$ for all $i > 0$,

$$\frac{\sum a_i x_i \geq a_0}{\sum (a_i / c) x_i \geq \lceil a_0 / c \rceil}$$

The final line of a refutation must be $0 \geq 1$.

**Example:** Let $\Gamma$ contain the clauses

$$\overline{x} \vee \overline{y} \quad \text{and} \quad \overline{x} \vee \overline{z} \quad \text{and} \quad \overline{y} \vee \overline{z}.$$

This expresses "No two of $x$, $y$, $z$ are true".

Cutting planes expresses these clauses as three inequalities:

$$-x - y \geq -1 \quad \text{and} \quad -x - z \geq -1 \quad \text{and} \quad -y - z \geq -1.$$

**Addition** gives: $-2x - 2y - 2z \geq -3$.

**Division** by $c = 2$ gives: $-x - y - z \geq -1$.

I.e., $x + y + z \leq 1$. This is a more succinct way of expressing that no two of $x$, $y$, $z$ are true.

**Theorem:** Cutting planes has polynomial size refutations of the $\mathrm{PHP}_n^{n+1}$ principle.

**Proof idea:** Use the totality axioms to derive $\sum_{i,j} x_{i,j} \geq n+1$.

Use the injectivity axioms to prove $\sum_{i,j} x_{i,j} \leq n$, similar to the argument in the example.

Conclude $0 \geq 1$. □

**Hence:** Resolution does not p-simulate cutting planes.

**Also:** Constant-depth Frege does not p-simulate cutting planes.

# Two simulations

**Theorem:** Cutting planes p-simulates resolution.

**Proof idea:** It is straightforward to simulate a single resolution step with addition and division by two.

**Thm:** [Goerdt'92] Cutting planes is p-simulated by Frege systems.

**Proof idea:** Use carry-save-addition iterated integer division formulas to express the lines in a cutting planes refutation.

# Two simulations

**Theorem:** Cutting planes p-simulates resolution.

**Proof idea:** It is straightforward to simulate a single resolution step with addition and division by two.

**Thm:** [Goerdt'92] Cutting planes is p-simulated by Frege systems.

**Proof idea:** Use carry-save-addition iterated integer division formulas to express the lines in a cutting planes refutation.

**Thm:** [Pudlák'97] Cutting planes requires exponential size proofs (refutations) for the Clique-Coloring clauses.

Clique-Coloring is defined on the next slide....

# Clique Coloring clauses

The following (unsatisfiable!) set of clauses state that a graph on $n$ nodes has both a clique of size $m$ and a coloring of $m-1$.

**Variables:** $a \in [m]$, $c \in [m-1]$, and $i < j \in [n]$.

- $p_{a,i}$ - node $i$ is the $a$-th member of a clique.
- $q_{i,c}$ - node $i$ has color $c$.
- $r_{i,j}$ - there is a edge joining vertices $i$ and $j$.

**$A(\vec{p}, \vec{r})$ clauses:** (Clique of size $m$)

- $\bigvee_i p_{a,i}$ - for each $a \in [m]$
- $\overline{p_{a,i}} \vee \overline{p_{a',i}}$ - for $a < a' \in [m]$, $i \in [n]$.
- $\overline{p_{a,i}} \vee \overline{p_{a',j}} \vee r_{i,j}$ - for distinct $a, a' \in [m]$, distinct $i, j \in [n]$.

**$B(\vec{q}, \vec{r})$ clauses:** (Coloring of size $m-1$)

- $\bigvee_c q_{i,c}$ - for $i \in [n]$.
- $\overline{q_{i,c}} \vee \overline{q_{i,c'}}$ - for $c < c' \in [m-1]$, $i \in [n]$.
- $\overline{q_{i,c}} \vee \overline{q_{j,c}} \vee \overline{r_{i,j}}$ - for $c \in [m-1]$, distinct $i < j \in [n]$.

**Theorem (Krajíček'97)**

*Any resolution refutation of the clique-coloring tautology for $m = n^{1/2}$ requires exponential size $2^{\omega(n^{3/4})}$.*

**Theorem (Pudlák'97)**

*Cutting planes requires exponential size proofs (refutations) for the Clique-Coloring clauses.*

Both proofs use a Craig interpolation and the known exponential lower bounds on the size of monotone Boolean circuits that distinguish between graphs with large cliques and graphs with large colorings. [Razborov'85, Alon Boppana'87]

Interpolation for resolution is described next ...

# Craig Interpolation

[Bonet-Pitassi-Raz'95, Razborov'95, Krajíček'97, Pudlák'97]

**Defn:** Suppose $A(\vec{p},\vec{r}) \wedge B(\vec{q},\vec{r})$ is unsatisfiable, where $A$ and $B$ depend only on the variables indicated.
A **Craig interpolant** for this formula is a predicate $C(\vec{r})$ such that

- If $\neg C(\vec{r})$, then $A(\vec{p},\vec{r})$ is unsatisfiable.
- If $C(\vec{r})$, then $B(\vec{q},\vec{r})$ is unsatisfiable.
- Equivalently, $A(\vec{p},\vec{r}) \rightarrow C(\vec{r})$ and $C(\vec{r}) \rightarrow \neg B(\vec{q},\vec{r})$ are both tautologies.

**Thm:** A Craig interpolant always exists when $A(\vec{p},\vec{r}) \wedge B(\vec{q},\vec{r})$ is unsatisfiable.

**Pf:** Take $C(r)$ to be either

$$(\exists \vec{p})A(\vec{p},\vec{r}) \qquad \text{or} \qquad (\forall \vec{q})\neg B(\vec{q},\vec{r}).$$

However, the Craig interpolant may not be a feasible predicate of $\vec{r}$.

**Theorem (Krajíček'97)**

*Suppose a set of clauses $A(\vec{p},\vec{r}), B(\vec{q},\vec{r})$ has a resolution refutation of size $m$, and that variables $\vec{r}$ all appear only positively in the clauses in $A(\vec{p},\vec{r})$ or only negatively in the clauses in $B(\vec{q},\vec{r})$. Then, there is a Craig interpolant which is computed by a* monotone *Boolean circuit of size $O(m)$.*

A **monotone** circuit is constructed from literals $r_i$, and $\wedge$ and $\vee$. If the refutation is tree-like, the interpolant is a monotone Boolean *formula*.

Application: The clique-coloring principles require exponential size resolution refutations.

**Proof of the Craig interpolation property:**
A resolution refutation $R$ transforms directly to a monotone circuit.

Each clause $C$ in $R$ corresponds to a gate $g_C$.

| | |
|---|---|
| $C$ is an $A(\vec{p},\vec{r})$ clause | $g_C := \bot$ |
| $C$ is a $B(\vec{q},\vec{r})$ clause | $g_C := \top$ |
| $C, p_i \quad D, \overline{p_i} \;/\; C, D$ | $g_{CD} := g_{Cp_i} \vee g_{D\overline{p_i}}$ |
| $C, q_i \quad D, \overline{q_i} \;/\; C, D$ | $g_{CD} := g_{Cq_i} \wedge g_{D\overline{q_i}}$ |
| $C, r_i \quad D, \overline{r_i} \;/\; C, D$ | $g_{CD} := (r_i \vee g_{Cr_i}) \wedge g_{D\overline{r_i}}$, or<br>$g_{CD} := g_{Cr_i} \vee (r_i \wedge g_{D\overline{r_i}})$,<br>depending on whether $\vec{r}$ is monotone in $A$ or in $B$. |

Invariant: $g_C$ computes an interpolant that is correct for any assignment falsifying $C$.
I.e., $g_C$ is false (true) implies some clause of $A$ (resp. $B$) is false. $\square$

**Theorem** [Krajíček'97] Any resolution refutation of the clique-coloring tautology for $m = n^{1/2}$ requires size $2^{\omega(n^{3/4})}$.

**Proof:** Apply the Craig Interpolation Theorem for resolution.

- The variables $\vec{r}$ encode a graph $G$.
- $C(\vec{r})$ is false means: $A(\vec{p}, \vec{r})$ is unsatisfiable, i.e., $G$ does not have a clique of size $m$.
- $C(\vec{r})$ is true means: $B(\vec{q}, \vec{r})$ is unsatisfiable, i.e., $G$ does not have an $m-1$ coloring.

If the resolution refutation has size $S$, then there is a Craig interpolation of size $s$; namely, a monotone Boolean circuit in the variables $\vec{r}$ of size $s$ separating graphs with a clique of size $m$ from those with a coloring of size $m-1$.
This contradicts the known exponential lower bounds on the size of monotone Boolean circuits that distinguish between graphs with large cliques and graphs with large colorings.
[Razborov'85, Alon Boppana'87] □

# A cutting planes bound for Clique-Coloring

**Thm:** [Pudlák'97] Suppose a set of clauses $A(\vec{p}, \vec{r}), B(\vec{q}, \vec{r})$ has a cutting planes refutation of $m$ steps, and that the variables $\vec{r}$ appear only positively in the clauses in $A(\vec{p}, \vec{r})$ or only negatively in the clauses in $B(\vec{q}, \vec{r})$. Then, there is Craig interpolant which is computed by a monotone real circuit of size $m^{O(1)}$.

**Defn:** A **real monotone circuit** is a circuit with unary and binary gates computing monotone real functions.
We use a threshhold gate as the output gate.

**Corollary:** (Using a modification of [Razborov'85;Alon-Boppana'87].) Cutting Planes does not have polynomial size refutations of the Clique-Coloring clauses expressing that a graph both is $k$-colorable and has a $k+1$ clique.

**Open:** Find methods other Craig interpolation for giving lower bounds to cutting planes proofs.

# The Nullstellensatz proof system

[Beame-Impagliazzo-Krajíček-Pitassi-Pudlák'97]
Work over a finite field, characteristic $p$.

Variables $x_1, x_2, \ldots$ are $0/1$ valued.

A polynomial $f$ is identified with the assertion $f = 0$.

A set of *initial* polynomials $\{f_j\}_j$ is **refuted** in the **Nullstellensatz system** by polynomials $g_j$, $h_i$ such that

$$\sum f_j \cdot g_j + \sum (x_i^2 - x_i) \cdot h_i = 1,$$

where equality indicates equality as polynomials.

Note the equality cannot hold if all $f_j(\vec{x})$ equal zero for some (Boolean) inputs $\vec{x}$.
Hence a Nullstellsatz refutation indeed serves as a refutation.

Nullstellensatz is known not to simulate resolution. Conversely, resolution and even constant depth Frege systems do not simulate Nullstellensatz.

It is traditional to work with the degree of Nullstellensatz proofs, rather than their size. It is also common to work over fields of finite characteristic $p$.

Sample lower bounds on Nullstellensatz include:

- Super-constant degree lower bounds for Nullstellensatz refutations of "counting mod $q$", for $q$ not a power of $p$. [BIKPP'97]
- $\Omega(n)$ degree lower bounds for $\mathrm{PHP}_n^{n+1}$. [Beame-Cook-Edmonds-Impagliazzo-Pitassi'98, Razborov'98]

Applications of Nullstellensatz lower bounds include:

- Separation results for constant depth Frege proofs.
- Separations for subclasses of TFNP.
- Lower bounds for monotone span programs.
- Lower bounds for cutting planes refutations via lifting theorems.

# The Polynomial Calculus proof system

A **Polynomial Calculus** refutation uses the inferences of addition and multiplication:

$$\frac{f \quad g}{f+g} \qquad\qquad \frac{f}{f \cdot g}$$

A **Polynomial Calculus Refutation** of a set of polynomials $\{f_j\}_j$ is a derivation of 1 from the $f_j$'s and the polynomials $(x_i^2 - x_i)$.

The polynomial calculus and the nullstellensatz systems can refute the same sets of polynomials; but a polynomial calculus can be substantially shorter due to cancellation of monomials in intermediate steps.

One sample result:

**Thm:** [Razborov'98] Any polynomial calculus proof of $PHP_n^{n+1}$ must have degree $\Omega(n)$.

# Automatizability

**Defn:** A proof system $T$ is **automatizable** (in polynomial time) if there is a procedure, which given a formula $\varphi$, produces a $T$-proof of $\varphi$ in time bounded by a polynomial of the size of the shortest $T$-proof of $\varphi$ (if any).

**Defn:** A proof system $T$ has **feasible interpolation** if there is polynomial time procedure $C(-,-)$ so that if $P$ is a $T$-proof of $\neg(A(\vec{p},\vec{r}) \wedge B(\vec{q},\vec{r}))$, then $C(\vec{p},\vec{r})$ is a Craig interpolant for $A(\vec{p},\vec{r}) \wedge B(\vec{q},\vec{r})$.

**Thm:** [Bonet-Pitassi-Raz'00] If $T$ is automatizable, then $T$ has feasible interpolation.

**Thm:** [Krajíček-Pudlák'95, also B'97] The extended Frege system $e\mathcal{F}$ does not have feasible interpolation and thus is not automatizable, unless the RSA encryption function, the discrete logarithm encryption function, and the Rabin encryption function can be inverted in polynomial time.

**Thm:** [Bonet-Pitassi-Raz'00] The Frege system $\mathcal{F}$ does not have feasible interpolation and thus is not automatizable, unless Blum integers can be factored in polynomial time.

**Defn: Blum integers** are products of two primes, each congruent to 3 mod 4.

A related theorem holds for bounded depth Frege systems under a stronger hardness assumption about Blum integers. [BDGMP'03].

**Theorem**

*Suppose* $\mathrm{P} \neq \mathrm{NP}$. *Then*

- *Resolution is not automatizable. [Atserias-Müller'20]*
- *Cutting Planes in not automatizable. [Göös-Koroth-Mertz-Pitassi'20]*
- *The Nullstellensatz and Polynomial Calculus proof systems are not automatizable.*

  *[de Rezende-Göös-Nordström-Pitassi-Robere-Sokolov'20]*

On the other hand:

**Theorem (Beame-Pitassi'96; building on CEI'96)**

*Tree-like resolution is automatizable in time* $n^{\log S}$ *where* $n$ *is the number of variables, and* $S$ *is the size of the shortest tree-like resolution refutation. (This is quasipolynomial time.)*

*Resolution is automatizable in time* $n^{\sqrt{n \log S}}$.

End of part D!