RESOLUTION

- Start with clauses of unsatisfiable CNF formula F
- Derive new clauses by RESOLUTION RULE $\dfrac{C \vee x \quad D \vee \bar{x}}{C \vee D}$
- Refutation ends when empty clause $\perp$ (containing no literals) derived

PIGEONHOLE PRINCIPLE FORMULA (PHP_n^{n+1})

$$x_{i,1} \vee x_{i,2} \vee \cdots \vee x_{i,n} \qquad i \in [n+1]$$

$$\bar{x}_{i,j} \vee \bar{x}_{i',j} \qquad i, i' \in [n+1], i < i', j \in [n]$$

THM [Haken '85]

Any resolution refutation of PHP_n^{n+1} requires length (= # clauses) $\exp(\Omega(n))$.

CUTTING PLANES (CP)

Geometric reasoning with linear inequalities over $\mathbb{R}$ with integer coefficients.

Translate clause $C = \bigvee_{x \in P} x \vee \bigvee_{y \in N} \bar{y}$

to $\sum_{x \in P} x + \sum_{y \in N} (1-y) \geq 1$

or $\boxed{\sum_{x \in P} x - \sum_{y \in N} y \geq 1 - |N|}$ Normalize variables on left side constant term on right side

Ex $x \vee y \vee \bar{z} \rightsquigarrow x + y + (1-z) \geq 1$

$\boxed{x + y - z \geq 0}$

Derivation rules

Variable axioms $\dfrac{}{0 \leq x \leq 1}$ $\left(\dfrac{}{x \geq 0} \quad \dfrac{}{-x \geq -1}\right)$

Addition $\dfrac{\sum a_i x_i \geq A \quad \sum b_i x_i \geq B}{\sum (a_i + b_i) x_i \geq A + B}$

Multiplication $\dfrac{\sum a_i x_i \geq A}{\sum c a_i x_i \geq cA}$ $c \in \mathbb{N}^+$

Division (Gomory-Chvátal/CWA) $\dfrac{\sum c a_i x_i \geq A}{\sum a_i x_i \geq \lceil A/c \rceil}$

Note the rounding! very powerful

Prove CNF formula unsatisfiable by deriving $0 \geq 1$ from linear inequalities encoding clauses

LENGTH Total # lines / inequalities in refutation

OBSERVATION (CP efficiently simulates resolution)
If F can be refuted in resolution in length L, then there is a CP refutation in length at most $O(L^2)$

Proof sketch CP can simulate the resolution rule easily. Left as an exercise to fill in the details.

THEOREM CP is exponentially stronger than resolution.

Proof sketch Never worse than resolution by observation above.

Pigeonhole principle formulas are very easy for CP (just count to see that # pigeons > # holes and immediately deduce contradiction). Also good exercise.

Let us look at another example.

EVEN COLOURING FORMULA $EC(G)$ [Merkeström] IV

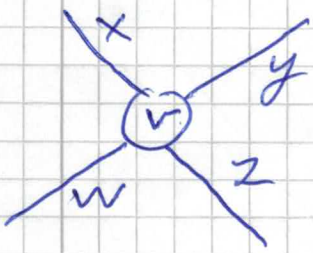
Undirected graph G; all vertices even degree $O(1)$
Variables = edges (also assumed to be connected)

For every vertex v, have CNF constraints

"# true edges incident to v = # false edges incident to v"

Ex

$$(x \vee y) \wedge (\bar{x} \vee \bar{y})$$



$$(xvyvz)\wedge(xvyvw)\wedge(xvzvw)\wedge(yvzvw)$$
$$\wedge(\bar{x}v\bar{y}v\bar{z})\wedge(\bar{x}v\bar{y}v\bar{w})\wedge(\bar{x}v\bar{z}v\bar{w})\wedge(\bar{y}v\bar{z}v\bar{w})$$

OBSERVATION

$EC(G)$ unsatisfiable $\iff$ $|E(G)|$ odd

FACT

If G is a well-connected enough (of even degree) graph with $|E(G)|$ odd, then $EC(G)$ is exponentially hard to refute in resolution.

For instance, take G to be random 6-regular graph with odd # vertices

Lower bound not written down anywhere that I know of, but can be shown with standard proof cplx machinery [at least so it seems]

LEMMA If G is a graph with $|E(G)|$ odd and all vertices having even degree, then cutting planes can refute $\mathrm{EC}(G)$ efficiently

Proof Exercise.

Gives another example than PHP that CP exponentially stronger than resolution.

Intriguing fact

There are so-called pseudo-Boolean solvers using cutting planes reasoning.

Although $\mathrm{EC}(G)$ is easy in theory, PB solvers don't seem able to figure this out.

Would like to understand why (and what to do about it).

Cutting planes very poorly understood proof system.

Essentially only one superpolynomial lower bound [Pudlák '97] for formula talking about cliques and colourings in graphs

CLIQUE - COCLIQUE FORMULA

(a) $q_{k,1} \vee q_{k,2} \vee \cdots \vee q_{k,n}$ $\quad k \in [m]$

(some vertex kth member of clique)

(b) $\bar{q}_{k,i} \vee \bar{q}_{k,j}$ $\quad i,j \in [n],\ i \neq j,\ k \in [m]$

(kth clique member uniquely defined)

(c) $p_{i,j} \vee \bar{q}_{k,i} \vee \bar{q}_{k',j}$ $\quad i,j \in [n],\ i \neq j,\ k,k' \in [m],\ k \neq k'$

(clique members connected by edge)

(d) $r_{i,1} \vee r_{i,2} \vee \cdots \vee r_{i,m-1}$ $\quad i \in [n]$

(every vertex has a colour)

(e) $\bar{p}_{i,j} \vee \bar{r}_{i,\ell} \vee \bar{r}_{j,\ell}$ $\quad i,j \in [n],\ i \neq j,\ \ell \in [m-1]$

$p_{i,j}$ = "there is an edge (i,j)"

$q_{k,i}$ = "vertex i is kth member of clique"

$r_{i,\ell}$ = "vertex i has colour ℓ"

CNF formula consisting of all clauses (a)-(e) claims that there exists a graph that has an m-clique and is also $(m-1)$ colourable

Observation: Clique-coclique formula splits into two parts connected only by variables $p_{i,j}$ encoding (edges in) graph

Can be written $A(\vec{p},\vec{q}) \wedge B(\vec{p},\vec{r})$ for

$A(\vec{p},\vec{q})$ = { clauses (a)-(c) }

$B(\vec{p},\vec{r})$ = { clauses (d)-(e) }

Suppose that we have an unsatisfiable CNF formula that can be written

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

($\vec{p}, \vec{q}, \vec{r}$ all disjoint)

where A CNF over variables $\vec{p}, \vec{q}$
" B CNF " $\vec{p}, \vec{r}$

Given assignment $\vec{\alpha}$ to $\vec{p}$, either $A(\vec{\alpha}, \vec{q})$ or $B(\vec{\alpha}, \vec{r})$ is unsatisfiable (or both)

We say that $I(\vec{p})$ | Boolean formula | is an INTERPOLANT if

$$I(\vec{\alpha}) = 0 \implies A(\vec{\alpha}, \vec{q}) \text{ unsat}$$
$$I(\vec{\alpha}) = 1 \implies B(\vec{\alpha}, \vec{r}) \text{ unsat}$$

Such an interpolant always exists (easy to see), but can be exponentially large

We are interested in when interpolant can be written as small Boolean circuit.

This is possible if $A(\vec{p}, \vec{q}) \wedge B(\vec{p}, \vec{r})$ has a short resolution refutation!

Can be used to obtain proof complexity lower bounds from circuit complexity lower bounds

- Start with formula $A(\vec{p}, \vec{q}) \wedge B(\vec{p}, \vec{r})$
- Assume exists short resolution refutation
- Deduce existence of small interpolating circuit
- Appeal to (previously shown) circuit complexity lower bound saying no such small circuits exist
- Hence there cannot exist short resolution refutations either

Say that resolution has FEASIBLE INTERPOLATION

One of many possible ways of showing resolution lower bounds

Also turns out to work for cutting planes

Only known size lower bound technique for CP

Can be used to show clique-coclique formulas hard for CP

Proof gets a bit too complicated for us to be able to do it, but we will illustrate how it works for resolution, which is much easier

MONOTONE CIRCUIT

Circuit with $\wedge$-(AND) and $\vee$-(OR) gates, but no $\neg$-(NOT) gates

THEOREM [Razborov '85; Thm 14.7 in Arora-Barak]
Let an undirected graph G be represented by $\binom{n}{2}$ bits encoding its edges and non-edges
Then for $m \leq \sqrt[4]{n}$ there is no monotone circuit of size $2^{\Omega(\sqrt{m})}$ that can distinguish these two cases

(1) G has an m-clique
(2) G is $(m-1)$-colourable

But this is exactly what an interpolant $I(\vec{p})$ for clique-colligue formula does!

Remark Monotonicity VERY important.
We don't have lower bounds for non-monotone circuits.

But we will be a bit sloppy with this in the proofs (with details needed provided at the very end).

Let

$$sel(b,x,y) = \begin{cases} x & \text{if } b=0 \\ y & \text{if } b=1 \end{cases}$$

Will build circuits with gates $(\wedge, \vee, sel)$
[sel is not monotone function and needs to be removed in the end]

THEOREM [Pudlák; based on Krajíček]
Suppose $\exists$ resolution refutation $\Pi: A(\vec{p},\vec{q}) \wedge B(\vec{p},\vec{r}) \vdash \bot$ in length L. Then:

(1) $\exists$ circuit $C(\vec{p})$ over $(\wedge, \vee, sel)$ such that
$C(\vec{\alpha}) = 0 \Rightarrow A(\vec{\alpha},\vec{q})$ unsat
$C(\vec{\alpha}) = 1 \Rightarrow B(\vec{\alpha},\vec{r})$ unsat

(2) Can construct from Π resolution refutation
$\left.\begin{array}{l} \Pi_A: A(\vec{\alpha},\vec{q}) \vdash \bot \text{ if } C(\vec{\alpha})=0 \\ \Pi_B: B(\vec{\alpha},\vec{r}) \vdash \bot \text{ if } C(\vec{\alpha})=1 \end{array}\right\}$ in length $\leq L$

(3) If $\vec{p}$-variables occur only positively in $A(\vec{p},\vec{q})$ or only negatively in $B(\vec{p},\vec{r})$ then sel-gates can be replaced by $\wedge$- and $\vee$-gates, yielding monotone circuit.

PROOF PLAN
- Take $\Pi: A(\vec{p},\vec{q}) \wedge B(\vec{p},\vec{r}) \vdash \bot$
- Fixing $\vec{p}$ to $\vec{\alpha}$, split Π into two derivations Π_A from $A(\vec{\alpha},\vec{q})$ and Π_B from $B(\vec{\alpha},\vec{r})$
- One of Π_A and Π_B is a refutation — build circuit that figures out which

q-clause clause in $A(\vec{p},\vec{q})\restriction\vec{\alpha}$ or derived only from $A(\vec{p},\vec{q})\restriction\vec{\alpha}$

r-clause clause in $B(\vec{p},\vec{r})\restriction\vec{\alpha}$ or derived only from $B(\vec{p},\vec{r})\restriction\vec{\alpha}$

q-clauses don't contain variables $\vec{r}$
r-clauses don't contain variables $\vec{q}$

Go over $\pi = (C_1, C_2, \ldots, C_L)$ inductively
Replace each C_i by $\tilde{C}_i$ such that

(a) $\tilde{C}_i \subseteq C_i\restriction\vec{\alpha}$ [and $\tilde{C}_i \neq 1$ if $C_i\restriction\vec{\alpha} \neq 1$]

(b) $\tilde{C}_i$ either q-clause or r-clause

Base case Axioms are either q-clauses or r-clauses — set $\tilde{C}_i = C_i\restriction\vec{\alpha}$

Induction step Resolution rule $\dfrac{C \vee x \quad D \vee \bar{x}}{C \vee D}$

$\tilde{C} \subseteq C \vee x\restriction\vec{\alpha}$ and $\tilde{D} \subseteq D \vee \bar{x}\restriction\vec{\alpha}$
already constructed as q-clauses or r-clauses
Case analysis over variable resolved over

Case 1 $\dfrac{C \vee p_k \quad D \vee \bar{p}_k}{C \vee D}$

$\alpha(p_k) = 0 \Rightarrow$ replace $C \vee D$ by $\tilde{C}$
$\alpha(p_k) = 1 \Rightarrow$ replace $C \vee D$ by $\tilde{D}$

Conditions (a) & (b) hold

Case 2 $\dfrac{C \vee q_k \quad D \vee \bar{q}_k}{C \vee D}$

If $\tilde{C}$ or $\tilde{D}$ r-clause, let such clause replace $C \vee D$ [doesn't contain q_k] (let us say $\tilde{C}$ if possible, else $\tilde{D}$)

If $\tilde{C}$ or $\tilde{D}$ q-clause not containing q_k, let such clause replace $C \vee D$ (let us say $\tilde{C}$ if possible, else $\tilde{D}$)

Otherwise $\tilde{C} = \tilde{C}' \vee q_k$ $\tilde{D} = \tilde{D}' \vee \bar{q}_k$ and both are q-clauses.

Resolve to get $\tilde{C}' \vee \tilde{D}'$ and replace with this clause

Case 3 $\dfrac{C \vee r_k \quad D \vee \bar{r}_k}{C \vee D}$

Dual of case 2. Dealt with in exactly analogous way

$C_\alpha = \bot$ and $\tilde{C}_\alpha \leq C_\alpha | \vec{\alpha} = \bot$

Hence $\tilde{C}_\alpha = \bot$

If $\tilde{C}_\alpha$ q-clause; derived from $A(\vec{p}, \vec{q}) \restriction \vec{\alpha}$

$= A(\vec{\alpha}, \vec{q})$ by resolution

If $\tilde{C}_\alpha$ r-clause, derived from $B(\vec{\alpha}, \vec{q})$ by resolution.

Proves part (2) of thm

To prove part (1), build circuit over $\{\wedge, \vee, \mathrm{sel}\}$ from π

Note that every line C_i in proof has been classified as g-clause or r-clause by inductive process.

For axiom clauses in $A(\vec{p}, \vec{q})$, put constant 0.
" " $B(\vec{p}, \vec{r})$, " " 1

Case 1 $C \vee p_k$ gets value x
$D \vee \bar{p}_k$ gets value y
Then let $C \vee D$ get value $z = sel(p_k, x, y)$
(because construction simply substituted one of these clauses)

Case 2 If one of $C \vee q_k$ (value x) $D \vee \bar{q}_k$ (value y) has been replaced by an r-clause, then we keep that r-clause, otherwise get g-clause

$$z = x \vee y$$

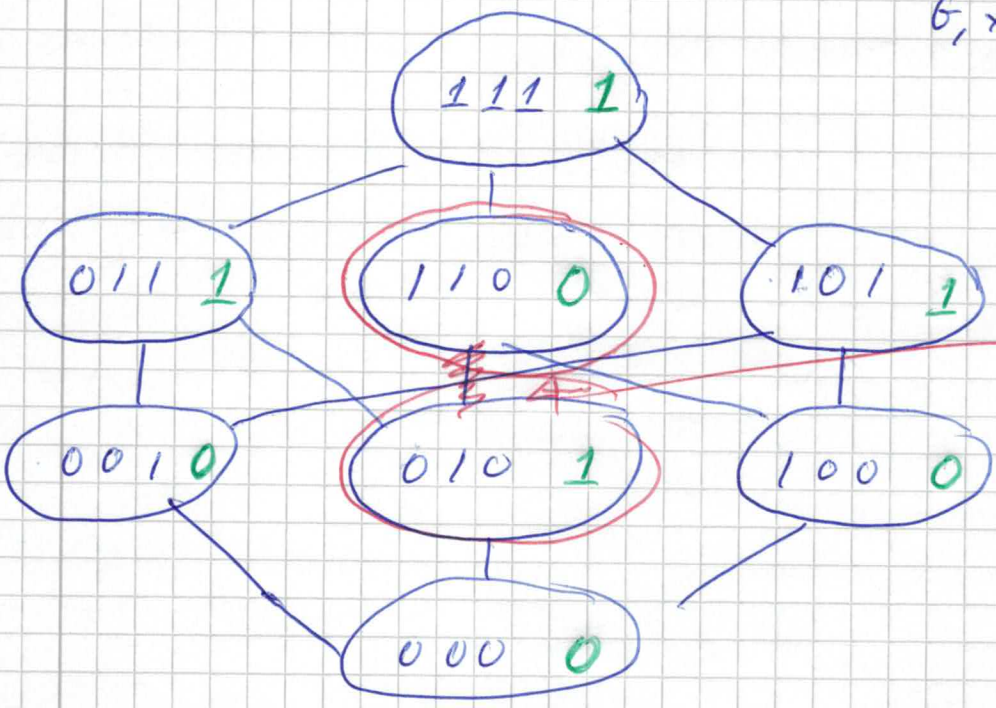
Case 3 $C \vee r_k$ (val x) $D \vee \bar{r}_k$ (val y)

If both clauses r-clauses then we get an r-clause, else a g-clause

$$z = x \wedge y$$

Now output gate corresponding to $C_L = 1$ outputs 0 if $C_L = 1$ g-clause derived from $A(\vec{x}, \vec{q})$ and 1 if 1 derived from $B(\vec{x}, \vec{q})$ so it is an interpolating circuit.

But the circuit is not monotone, because $sel(b,x,y)$ is not monotone



Suppose w.l.o.g. $\vec{p}$ only appears positively in $A(\vec{p},\vec{q})$
(Other case analogous.)
Replace $sel(b,x,y)$ by $(b \vee x) \wedge y$

Only difference for $b=0, x=1, y=0$ ↦ 0

$\alpha(p_k) = 0$ so we should have picked type from $\tilde{C}$, which was an r-clause, but instead we are picking q-clause $\tilde{D}$

WRONG if $\tilde{D}$ contains $\bar{p}_k$, because then $\tilde{D}$ partial but $C \vee D\restriction_{\vec{\alpha}}$ not, and condition $\tilde{D} \leq C \vee D\restriction_{\vec{\alpha}}$ is violated.

But $\tilde{D}$ cannot contain negative literal $\bar{p}_k$ since it is derived from $A(\vec{p},\vec{q})$. So this replacement is OK

This takes care of part (3) ✓

Plugging this into monotone circuit cplx lower bound we obtain that clique-coclique formulas for $m \approx \sqrt[4]{n}$ require resolution length $\exp(n^{\delta})$ for $\delta \approx 1/8$ or so.

SUMMARY

Cutting planes – use linear inequalities to refute unsat CNFs

Cutting planes exponentially stronger than resolution

Only one lower bound technique

Formulas with very particular structure
⇒ **interpolation** yields monotone circuits
⇒ proof cplx lower bounds from circuit cplx lower bounds

Clique-coclique formulas

BIG OPEN PROBLEM to develop other lower bound techniques for cutting planes