Razborov's theorem, interpolation method, and lower bounds for Resolution and Cutting Planes

Author: Alisa Knizel

Plan

- Proof of Razborov's theorem.
- Lower bounds for the resolution proof system.
- Lower bounds for the cutting planes.

Monotone circuits

Definition Boolean circuit :

- directed acyclic graph
- nodes (gates) labelled by: inputs, AND, OR, NOT
- computes a function of its n input bit in the natural way

Conjecture: **NP**-complete problems have no polynomial circuits.

- the best lower bounds we are able to prove are kn (for small constants k)
- let's prove in a weaker circuit model
- the most natural model is the monotone circuits (that is, ones without NOT gates)

Monotone circuits

- Monotone circuits can only compute monotone functions($x \leq y \Rightarrow f(x) \leq f(y)$), and $\forall$ monotone function can be computed by monotone circuit.
- There are monotone NP-complete problems ($CLIQUE_{n,k}$)

CLIQUE

Definition: $CLIQUE_{n,k}$ is the Boolean function. CLIQUE(G(V, E))=1 if G has a clique of size k.

- $CLIQUE_{n,k}$ is a monotone function.
- $CLIQUE_{n,k}$ is **NP**-complete

Monotone circuit for $CLIQUE_{n,k}$

- input gate $g_{[i,j]}$ is set to true $\Leftrightarrow [i,j] \in E$
- $\forall S \subseteq V$ with $|S| = k$ test with AND gates whether S forms a clique
- repeat $\forall S \subseteq V$ with $|S| = k$ and take a big OR of the outcomes

Definition: Crude circuit is a circuit testing whether a family of subsets of V form a clique and returning true $\Leftrightarrow$ one of the sets does. The above circuit is denoted $CC(S_1, ..S_{\binom{n}{k}})$

Razborov's Theorem:

Razborov's Theorem: There is a constant **c** such that for large enough n all monotone circuits for $CLIQUE_{n,k}$ with $k = \sqrt[4]{n}$ have size at least $2^{c\sqrt[8]{n}}$

Plan

- approximate any monotone circuit for $CLIQUE_{n,k}$ by a restricted kind of crude circuit.
- show that each step introduces rather few errors
- show that the resulting crude circuit has exponentially many errors.
- Thus the approximation takes exponentially many steps $\Rightarrow$ the original monotone circuit has exponentially many gates.

The Erdös-Rado Lemma

Defenition: A *sunflower* is a family of p sets $\{P_1, ..., P_p\}$, called *petals*, each of cardinality at most ℓ, such that all pairs of sets in the family have the same intersection (called *the core* of sunflower).

The Erdös-Rado Lemma: Let **Z** be a family of more than $M = (p-1)^{\ell}\ell!$ nonempty sets, each of cardinality ℓ or less. Then **Z** must contain a sunflower.

Proof:

Induction on ℓ.

- $\ell = 1 \Leftrightarrow$ different singletons form a sunflower. **D** is a maximal subset of **Z** of disjoint sets.
- $|D| \geq p$ sets, then it constitutes a sunflower with empty core.
- $\mathbf{F} = \bigcup H_i, H_i \in \mathbf{D}$. We know: $|\mathbf{F}| \leq (p-1)\ell$ and that **D** intersects every set in **Z**.
- There is an element $d \in \mathbf{D}$ which intersects more than $\frac{M}{(p-1)\ell} = (p-1)^{\ell}(\ell-1)!$ sets.

- $\mathbf{G} = \{\mathbf{S} - d : \mathbf{S} \in \mathbf{Z} \text{ and } d \in \mathbf{Z}\}$
- $\mathbf{G}$ has more than $(p-1)^{\ell}(\ell-1)!$ sets $\Rightarrow$ by induction it contains a sunflower $P_1, ..., P_p$. Then $\{P_1 \cup \{d\}, ..., P_p \cup \{d\}\}$ is a sunflower in $\mathbf{Z}$. $\square$

- **Definition:** Plucking a sunflower entails replacing the sets in the sunflower by its core.

$$Z_1, .., Z_p \longrightarrow Z$$

- **Remark:** If there are >M sets in a family, we can reduce their number by repeatedly finding a sunflower and plucking it.

Approximation

- do it inductively (any monotone circuit is considered as the OR or AND of two subcircuits).
- there are two circuits CC(**X**), CC(**Y**), **X**,**Y** are families of $\leq$ M sets of nodes. ($M = (p-1)^{\ell}\ell!$ (p is about $\sqrt[8]{n}$)).
- each set with $\leq \ell$ ($= \sqrt[8]{n}$) nodes.

Approximation steps

- $\mathrm{A}[CC(\mathbf{X}) \vee CC(\mathbf{Y})] = \mathrm{CC}(\mathrm{pluck}(\mathbf{X} \cup \mathbf{Y}))$
- $\mathrm{A}[CC(\mathbf{X}) \wedge CC(\mathbf{Y})] = \mathrm{CC}(\mathrm{pluck}\ (\{U_i \cup V_j : U_i \in \mathbf{X},\ V_i \in \mathbf{Y}$, and $|U_i \cup V_j| \leq \ell\}))$

Positive and negative examples

- **Definition:** A positive example is simply a graph with $\binom{k}{2}$ edges connecting k nodes in all possible ways. There are $\binom{n}{k}$ such graphs, and they all should elicit the "true".
- The negative examples are outcomes of following experiment: color the nodes with $k-1$ different colors. Then join by an edge any two nodes that are colored differently. Such a graph has no k-clique. There are $(k-1)^n$ negative examples overall.

False negatives and false positives

- E is a positive example. $CC_1(E) = true$, $CC = A[CC_1 \vee CC_2]$ and $CC(E) = false \Rightarrow$ the approximation step has introduced a **false negative**.
- N is a negative example.
  $CC_1(N) = false$, $CC_2(N) = false$, $CC = A[CC_1 \vee CC_2]$ and $CC(N) = true \Rightarrow$ the approximation step has introduced a **false positive**.
- E is a positive example.
  $CC_1(E) = true$, $CC_2(N) = true$, $CC = A[CC_1 \wedge CC_2]$ and $CC(E) = false \Rightarrow$ the approximation step has introduced a **false negative**.
- N is a negative example. $CC_1(N) = false$, $CC = (AND)A[CC_1 \wedge CC_2]$ and $CC(N) = true \Rightarrow$ the approximation step has introduced a **false positive**.

Lemma 1 (about false positives)

Lemma: Each approximation step introduces $\leq M^2 2^{-p}(k-1)^n$ false positives.

Proof: First for an OR.
A false positive introduced by plucking (the replacement of sunflower $\{Z_1, ..., Z_p\}$ by its core **Z**) is a coloring such that there is a pair of identically colored nodes in each petal, but at least one node from each petal was plucked away. Let's count such colorings.

Proof (OR):

R(X) is the probability of the event that there are repeated colors in set X. We have:

$$\textbf{prob}[R(Z_1) \wedge ... \wedge R(Z_p) \wedge \neg R(Z)] \leq \textbf{prob}[R(Z_1) \wedge ... \wedge R(Z_p) | \neg R(Z)] =$$

$$= \prod_{i=1}^{p} \textbf{prob}[R(Z_i) | \neg R(Z)] \leq \prod_{i=1}^{p} \textbf{prob}[R(Z_i)]$$

Proof (OR):

R(X) is the probability of the event that there are repeated colors in set X. We have:

$$\mathbf{prob}[R(Z_1) \wedge ... \wedge R(Z_p) \wedge \neg R(Z)] \leq \mathbf{prob}[R(Z_1) \wedge ... \wedge R(Z_p) | \neg R(Z)] =$$

$$= \prod_{i=1}^{p} \mathbf{prob}[R(Z_i) | \neg R(Z)] \leq \prod_{i=1}^{p} \mathbf{prob}[R(Z_i)]$$

Proof (OR):

R(X) is the probability of the event that there are repeated colors in set X. We have:

$$\mathbf{prob}[R(Z_1) \wedge ... \wedge R(Z_p) \wedge \neg R(Z)] \leq \mathbf{prob}[R(Z_1) \wedge ... \wedge R(Z_p) | \neg R(Z)] =$$

$$= \prod_{i=1}^{p} \mathbf{prob}[R(Z_i) | \neg R(Z)] \leq \prod_{i=1}^{p} \mathbf{prob}[R(Z_i)]$$

Proof(OR):

- Consider two nodes in Z_i, **prob**[they have the same color]$=\frac{1}{k-1}$. Then

$$\textbf{prob}[R(Z_i)] \leq \frac{\binom{|Z_i|}{2}}{k-1} \leq \frac{\binom{\ell}{2}}{k-1} \leq \frac{1}{2}$$

- Thus the probability that a randomly chosen coloring is a new false negative is at most 2^{-p}
- There are $(k-1)^n$ different coloring $\Rightarrow$ each plucking introduces $\leq 2^{-p}(k-1)^n$ false positives. The approximation step entails up to $\frac{2M}{p-1}$ pluckings, the lemma holds for the OR approximation step.

Proof (AND):

Consider now an AND approximation step. It can be broken down in 3 phases:

- we form $CC(\{U \cup V : U \in \mathbf{X}, V \in \mathbf{Y}\}) \rightarrow$ no false positives.
- the second phase omits from the approximator circuit several sets $\rightarrow$ no false positives.
- the third phase entails a sequence $< M^2$ pluckings, during each of which $\leq 2^{-p}(k-1)^n$ false positives are introduced. $\square$

Lemma 2(about false negatives)

- **Lemma:** Each approximation step introduce $\leq M^2\binom{n-\ell-1}{k-\ell-1}$ false negatives.
- **Proof:**
- plucking can introduce no false negatives
- $\Rightarrow$ the approximation of an OR introduces no false negatives.
- Consider now an AND approximation step.
- when we form $CC(\{U \cup V : U \in \mathbf{X}, V \in \mathbf{Y}\})$ no f. n. can be introduced.

Proof:

- each deletion of a set W which is larger than ℓ can introduce several false negatives, namely the cliques that contain $W \Rightarrow$ at most $\binom{n-\ell-1}{k-\ell-1}$ f. n. can be introduced by each deletion.

- there are at most M^2 sets to be deleted. $\square$

Conclusion

Lemma 1 and 2 show that each approximation step introduces "few"false positives and false negatives. We'll next show that the resulting crude circuit must have "a lot".

Lemma 3 (number of errors)

Lemma 3: Every crude circuit is not identically **false**(and thus is wrong on all positive examples), or outputs **true** on at least half of the negative examples.

- If the crude circuit is not identically **false**, then it accepts at least those graphs that have a clique on some set X of nodes, with $|X| \leq \ell$.
- But from Lemma 1 at least half of the colorings assign different colors to the nodes of X $\Rightarrow$ half of the negative examples have a clique at X and are accepted. $\square$

The last step of the proof of Razborov's theorem:

- $p = \sqrt[8]{n}\log n$, $\ell = \sqrt[8]{n} \Rightarrow$

$$M = (p-1)^{\ell}\ell! < n^{\frac{1}{3}\sqrt[8]{n}}$$

for large enough n.

- If the final crude circuit is identically **false**$\Rightarrow$ all possitive examples were introduced as false negatives at some step
- $\Rightarrow$ the original monotone circuit for $CLIQUE_{n,k}$ had $\leq$ (Lemma 2)

$$\frac{\binom{n}{k}}{M^2\binom{n-\ell-1}{k-\ell-1}}$$

$$\geq \frac{1}{M^2(\frac{n-\ell}{k})^{\ell}} \geq n^{c\sqrt[8]{n}},$$

with $c = \frac{1}{12}$

The proof of Razborov's theorem:

- Lemma 3 states that there are $\geq \frac{1}{2}(k-1)^n$ false positives, each approximation step introduces $\leq M^2 2^{-p}(k-1)^n$ (Lemma 1) of them.
- $\Rightarrow$ the original monotone circuit had at least $2^{p-1}M^{-2} > n^{c\sqrt[8]{n}}$, with $c = \frac{1}{3}$.

Resolution

Definition The propositional resolution proof system is the one which uses elementary disjunctions i. e., disjunctions of literals, as formulas, and the cut rule as the only one rule

$$\frac{\Gamma \vee p, \Delta \vee \neg p}{\Gamma \vee \Delta}$$

Where Γ, Δ are elementary disjunctions.

Effective interpolation for Resolution

The ternary connective *sel* (selector) is defined by $sel(0, x, y) = x$ and $sel(1, x, y) = y$

- **Theorem 1:** Let P be a resolution proof of the empty clause from clauses $A_i(\bar{p}, \bar{q}), i \in I, B_j(\bar{p}, \bar{r}), j \in J$ where $\bar{p}, \bar{q}, \bar{r}$ are disjoint sets of propositional variables. Then there exists a circuit $C(\bar{p})$ such that for every $0 - 1$ assignment $\bar{a}$ for $\bar{p}$

$$C(\bar{a}) = 0 \Rightarrow A_i(\bar{p}, \bar{q}), i \in I$$

are unsatisfiable, and

$$C(\bar{a}) = 1 \Rightarrow B_j(\bar{p}, \bar{r}), j \in J$$

are unsatisfiable;
the circuit C is in basis $\{0, 1, \vee, \wedge\}$ and its underlying graph is the graph of the proof P.

Theorem 1

Moreover, we can construct in polynomial time a resolution proof of the empty clause from clauses $A_i(\bar{p}, \bar{q}), i \in I$ if $C(\bar{a}) = 0$, respectively $B_j(\bar{p}, \bar{r}), j \in J$ if $C(\bar{a}) = 1$; the length of this proof is less than or equal to the length of P.

Proof:

The transformation of the proof for a given assignment $\bar{p} \rightarrow \bar{a}$

- 1. We replace each clause of P by a subclause so that each clause in the proof is either q-clause or r-clause. We start with initial clause, which are left unchanged and continue along the derivation P.
- Case 1.

$$\frac{\Gamma \vee p_k, \Delta \vee \neg p_k}{\Gamma \vee \Delta}$$

and we have replaced $\Gamma \vee p_k$ by Γ' and $\Delta \vee \neg p_k$ by Δ'. Then we replace $\Gamma \vee \Delta$ by Γ' if $p_k \rightarrow 0$ and by Δ' if $p_k \rightarrow 1$

Proof:

- Case 2.
$$\frac{\Gamma \vee q_k, \Delta \vee \neg q_k}{\Gamma \vee \Delta}$$
and we have replaced $\Gamma \vee q_k$ by Γ' and $\Delta \vee \neg q_k$ by Δ'. If one of Γ', Δ' is an r-clause $\rightarrow$ replace $\Gamma \vee \Delta$ by this clause. If both Γ' and Δ' are q-clauses $\rightarrow$ resolve along q_k, or take one without q_k.
- Case 3.
$$\frac{\Gamma \vee r_k, \Delta \vee \neg r_k}{\Gamma \vee \Delta}$$
This is the dual case to case 2.
- 2.Delete the clauses which contain a $\bar{p}$ literal with value 1, and remove all $\bar{p}$ literals from the remaining clauses.
- We got a valid derivation of the final empty clause from the reduced initial clauses. If this final clause is a q-clause, the proof contains a subproof using only the reduced clauses $A_i, i \in I$; if an r-clause $\Rightarrow$ $B_j, j \in J$

Proof:

- Construction of C:
- The value computed at a gate corresponding to a clause Γ will determine if it is transformed into a q(r)-clause. We assign 0 to q-clauses and 1 to r-clauses.
- Put constant 0 gates on clauses $A_i, i \in I$ and constant 1 gates on clauses $B_j, j \in J$.

Proof:

- Now consider 3 cases as above.
- Case 1. If the gate on $\Gamma \vee p_k$ gets value x and the gate on $\Delta \vee \neg p_k$ gets value y, then the gate on $\Gamma \vee \Delta$ should get the value $z = sel(p_k, x, y)$. We place the *sel* gate on $\Gamma \vee \Delta$.
- Case 2. If the gate on $\Gamma \vee q_k$ gets value x and the gate on $\Delta \vee \neg q_k$ gets value y, then the gate on $\Gamma \vee \Delta$ should get the value $z = x \vee y$). We place the $\vee$ gate on $\Gamma \vee \Delta$.
- Case 3. This is dual to case 2.

□

Theorem 2

Theorem 2:

Suppose moreover that either all variables $\bar{p}$ occur in $A_i(\bar{p}, \bar{q}), i \in I$ only positively or all variables $\bar{p}$ occur in $\bar{p}$ occur in $B_j(\bar{p}, \bar{r}), j \in J$ only negatively, then one can replace the selector connective sel by a monotone ternary connective.

Proof:

- W. l. o. g. assume that all $\bar{p}$'s are positive in clauses $A_i, i \in I$.
- Hence in case 1, if Δ' is a q-clause, it cannot contain $\neg p_k$, hence we can take it for $\Gamma \vee \Delta$, even if $p_k \to 0$.
- Thus we can replace $sel(p_k, x, y)$ by $(p_k \vee x) \wedge y$ which is monotone and differs from selector exactly on one input $(p_k = 0, x = 1, y = 0)$ which corresponds to the above situation.

$\square$

Cutting planes:

- We use propositional variables $\bar{p}$ with the interpretation $0 = \mathit{false}, 1 = \mathit{true}$.
- A proof line is an inequality

$$\sum_k c_k p_k \geq C$$

- Axiom: $0 \leq p_k \leq 1$

The rules

- Addition: $\sum_k c_k p_k \geq C$ and $\sum_k d_k p_k \geq D$
  $\longrightarrow \sum_k (c_k + d_k) p_k \geq C + D$
- Division: $d > 0, d \in \mathbb{Z}, d | c_k$ and $\sum_k c_k p_k \geq C \longrightarrow \sum_k \frac{c_k}{d} p_k \geq \lceil \frac{C}{d} \rceil$
- Multiplication: $d > 0, d \in \mathbb{Z}$ and $\sum_k c_k p_k \geq C \longrightarrow \sum_k d c_k p_k \geq dC$

Theorem 3

- **Theorem 3:** Let P be a cutting plane proof of the contradiction $0 \geq 1$ from inequalities $\sum_k c_{i,k} p_k + \sum_l b_{i,l} q_l \geq A_i, i \in I$, $\sum_k c'_{j,k} p_k + \sum_m d_{j,m} q_m \geq B_j, j \in J$ where $\bar{p}, \bar{q}, \bar{r}$ are disjoint sets of propositional variables. Then there exists a circuit $C(\bar{p})$ such that for every $0-1$ assignment $\bar{a}$ for $\bar{p}$
$C(\bar{a}) = 0 \Rightarrow \sum_k c_{i,k} p_k + \sum_l b_{i,l} q_l \geq A_i, i \in I$ are unsatisfiable, and
$C(\bar{a}) = 1 \Rightarrow \sum_k c'_{j,k} p_k + \sum_m d_{j,m} q_m \geq B_j, j \in J$ are unsatisfiable.
The size of the circuit is polynomial in the binary length of the numbers $A_i, i \in I, B_j, j \in J$ and the number of inequalities in P.

Theorem 3

Moreover, we can construct in polynomial time a cutting plane proof of the contradiction $0 \geq 1$ from inequalities $\sum_k c_{i,k} p_k + \sum_l b_{i,l} q_l \geq A_i, i \in I$ if $C(\bar{a}) = 0$, respectively $\sum_k c'_{j,k} p_k + \sum_m d_{j,m} q_m \geq B_j, j \in J$ if $C(\bar{a}) = 1$; the length of this proof is less than or equal to the length of P.

Proof:

Let P and assignment $\bar{p} \longrightarrow \bar{a}$ be given.

- Replace
  $\sum_k e_k p_k + \sum_l f_l q_l + \sum_l f_l q_l \geq D \longrightarrow \sum_l f_l q_l \geq D_0, \sum_m g_m r_m \geq D_1$
- The pair is at least as strong as the original one
  $D_0 + D_1 \geq D - \sum_k e_k p_k$
- $\sum_k c_{i,k} p_k + \sum_l b_{i,l} q_l \geq A_i \longrightarrow$ the pair
  $\sum_l b_{i,l} q_l \geq A_i - \sum_k c_{i,k} p_k, 0 \geq 0$
- $\sum_k c'_{j,k} p_k + \sum_m d_{j,m} r_m \geq B_j \longrightarrow$ the pair
  $\sum_m d_{j,m} r_m \geq B_j - \sum_k c'_{j,k} p_k, 0 \geq 0$
- The rules are performed in parallel on the 2 inequalities in the pair.

Proof:

- The pair corresponding to the last inequality $0 \geq 1$ is $0 \geq D_0$, $0 \geq D_1$ where $D_0 + D_1 \geq 1$
- $\Rightarrow$D$_0 \geq 1 \vee D_1 \geq 1$
- $\Rightarrow$ We have a proof of contradiction either from $\sum_k c_{i,k} p_k + \sum_l b_{i,l} q_l \geq A_i, i \in I$ or from $\sum_k c'_{j,k} p_k + \sum_m d_{j,m} q_m \geq B_j, j \in J$.
- Each proof P can be transformed in proof P' wich is at most polynomially longer and all the coefficients have polynomially bounded binary length (Clote and Buss).
- All D_i have polynomially bounded binary length $\Rightarrow$ the above procedure can be done in polynomial time in the binary length of $A_i, i \in I, B_j, j \in J$ and the number of inequalities.
- We use the transformation of polynomial time algorithms into sequences of polynomial size circuits.

The End.