Superpolynomial lower bound for CP

Antti Hyvärinen

November 19, 2007

References

The presentation covers only the proof for superpolynomial lower bound for CP

- Proof is based on three papers
  - P. Pudlák: *Lower bounds for resolution and cutting plane proofs and monotone computations*. Journal of Symbolic Logic 52(3). 1997
  - A. Haken: *Counting Bottlenecks to show monotone $P \neq NP$*. Proceedings of the 36th Annual Symposium on Foundations of Computer Science (FOCS'95)
  - A. Haken, and S. A. Cook: *An exponential Lower Bound for the Size of Monotone Real Circuits*. Journal of Computer and System Sciences 58(2). 1999

Overview

- Interpolants
- Monotone circuits
- How to convert CP proofs to a monotone real circuit
- Broken Mosquito Screen Problem
- Shortly go through the proof for superpolynomial lower bound

Interpolants

Let $\mathbf{p}, \mathbf{q}, \mathbf{r}$ be pairwise distinct sets of propositional variables and $\Phi(\mathbf{p}, \mathbf{q}), \Psi(\mathbf{p}, \mathbf{r})$ formulas over variables $\mathbf{p}, \mathbf{q}$ resp. $\mathbf{p}, \mathbf{r}$.

- Remember from Jori's presentation that if $\Phi(\mathbf{p}, \mathbf{q}) \rightarrow \Psi(\mathbf{p}, \mathbf{r})$ is a tautology, then
  - There exists $I(\mathbf{p})$ such that $\Phi(\mathbf{p}, \mathbf{q}) \rightarrow I(\mathbf{p})$ and $I(\mathbf{p}) \rightarrow \Psi(\mathbf{p}, \mathbf{r})$
- Given a truth assignment $\mathbf{a}$ for the variables, we have the following:
  - if $I(a)$ is false, we know that $\Phi(\mathbf{p}, \mathbf{q})$ is false
  - if $I(a)$ is true, we know that $\Psi(\mathbf{p}, \mathbf{r})$ is true

The idea of the CP proof

- We will present a way of transforming every CP proof of a certain tautology of form $\Phi(\mathbf{p}, \mathbf{q}) \rightarrow \Psi(\mathbf{q}, \mathbf{r})$ to an interpolant
- We will see that the interpolant can be presented as a *monotone boolean function* computing over real numbers
- We will show that the interpolant has to be large, so that the proof length will be of order $2^{N^{\frac{1}{8}}}$ where N is the size of the input.

Interpolants with disjunctive tauotology

- We may write the formula $\Phi(\mathbf{p}, \mathbf{q}) \to \Psi(\mathbf{p}, \mathbf{r})$ in disjunction form $\neg\Phi(\mathbf{p}, \mathbf{q}) \vee \Psi(\mathbf{p}, \mathbf{r})$
- It will be more natural to refute two conjuncts $A(\mathbf{p}, \mathbf{q}), B(\mathbf{p}, \mathbf{r})$ so that
  - if $I(\mathbf{p})$ is false, then $A(\mathbf{p}, \mathbf{q})$ is true and
  - if $I(\mathbf{p})$ is true, then $B(\mathbf{p}, \mathbf{r})$ is true
- This is motivated by the set of equations used for CP refutations

Monotone real circuits

- Inputs are at the bottom of the circuit and output is at the top
- Logic can compute any real numbers, but inputs are 0 and 1
- Also the output is assumed to be 0 or 1
- Gates are unary or binary
- A gate is allowed to compute any monotone nondecrasing function of the inputs
  - if output is γ for inputs α, β, and output is γ' for inputs α', β', then
    $$(\alpha \leq \alpha') \wedge (\beta \leq \beta') \Rightarrow (\gamma \leq \gamma')$$
- Inputs are considered to be gates

From CP to an Interpolant

We will study the CP proof of the contradiction $0 \geq 1$ from inequalities

$$\sum_k c_{i,k} p_k + \sum_l b_{i,l} q_l \geq A_i, i \in I$$

$$\sum_k c'_{j,k} p_k + \sum_m d_{j,m} r_m \geq B_j, j \in J$$

with $\mathbf{p}, \mathbf{q}, \mathbf{r}$ disjoint variables. There is a circuit $C(\mathbf{p})$ such that for each truth assignment $\mathbf{a}$,

$$C(\mathbf{a}) = 0 \Rightarrow \sum_k c_{i,k} a_k + \sum_l b_{i,l} q_l \geq A_i, i \in I \text{ are unsatisfiable}$$

$$C(\mathbf{a}) = 1 \Rightarrow \sum_k c'_{j,k} a_k + \sum_l d_{j,m} r_m \geq B_j, j \in J \text{ are unsatisfiable}$$

Notes to the proof

- If all the coefficients $c_{i,k}$ are nonnegative or all the coefficients $c'_{i,k}$ are nonpositive, the proof gives a monotone real boolean function
- We need
  1. Addition of an integer constant,
  2. multiplication by an integer constant
  3. addition
  4. division by a positive integer constant with rounding
  5. a threshold gate as the output gate ($t(x) = 1$ if $x \geq 1$ and $t(x) = 0$ otherwise)
- All but (2) (with negative constant) are monotonic. The proof does not need to multiply with negative numbers (home excercise)

Broken Mosquito Screen Problem (BMS)

- Graph of $m^2 - 2$ vertices, represented as a string of bits with 1 if there is an edge between i, j and 0 otherwise.
- Graph is *good* if there is a partition of vertices into $m - 1$ m-cliques and one $m - 2$-clique
- Graph is *bad* if there is a partition of vertices into $m - 1$ m-anticliques and one $m - 2$-anticlique.
- No instance is both good and bad.
- If an edge is added to a good graph, it remains good
- If an edge is removed from a bad graph, it remains bad
- There are graphs which are neither good or bad

Sounds good for monotone proofs

Idea of the proof

- We define a mapping μ from the set of graphs A to the gates E of the circuit
- We prove that the "graph density" of a gate, $||\mu^{-1}(E)||$ must be small
- We conclude that the number of gates, $\frac{||A||}{||\mu^{-1}(E)||}$ must be large

The set of graphs we are considering is a subset of the set $G_0 \cup B_0$, where

- G_0 is the set of maximal good graphs
- B_0 is the set of maximal bad graphs

These are the most difficult graphs

Iterating the circuit

- μ will map a subset of $G_0 \cup B_0$ to edges, so that
  - a suitable graph is selected from the set $G_i \cup B_i$, and
  - a new iteration is started with the element removed from either G_0 or B_0 depending on whether the graph is good or bad, yielding in a new set $G_1 \cup B_1$.
  - The process is continued until no more suitable graphs exist in the set $G_j \cup B_j$
  - The set A will then be $(G_0 \cup B_0) \setminus (G_j \cup B_j)$

Fences

- A good graph $g \in G_i$ flows through a gate E if $E(g_i) = 1$.
- A fence around g at gate E is a conjunction $C = x_1 \wedge \cdots \wedge x_q$, where x_i are inputs such that $C(g) = 1$ and $(\forall b' \in B_i)[(E(b') = 0) \Rightarrow (C(b') = 0)]$
- A similar definition holds for $b \in B_i$ and disjunction $D = x_1 \vee \cdots \vee x_q$
- A minimal fence is the fence with fewest variables

Fences might get other graphs wrong, they are only concerned with the particular selected graph

Selecting the graphs to the domain

- A fence is long if the number of variables in it is greater than $m/2$
- Let E_0 be the lowest and leftmost graph in the circuit such that there is a graph $d_0 \in G_0 \cup B_0$ that flows through E_0 and requires a long fence.
- Map the graph d_0 to E_0, and remove it from $G_0 \cup B_0$ to yield $G_1 \cup B_1$
- Continue until no more long fences exist
- The size of the domain of μ will be at least

$$||G_0|| = \frac{(m^2-2)!}{(m!)^{m-1}(m-2)!(m-1)!}$$

The lower bound proof

- The overapproximation of $||\mu^{-1}(E)||$, number of graphs mapped at a single gate, given below, follows from a rather long combinatorial argumentation

$$\frac{(km)^{r/2}(m^2-m)^{r/2}(m^2-2-r)!}{(m!)^{m-1}(m-2)!(m-1)!}$$

- k is $m/2$
- r is the greatest even number $\leq \sqrt{m}$
- The number of circuits will then be

$$\frac{(m^2-2)!}{(km)^{r/2}(m^2-m)^{r/2}(m^2-2-r)!}$$

Finally

- By careful approximation, we can deduce that the previous formula is greater than

$$(m^2 - 1 - r/2)^{r/2}/(km)^{r/2}$$

- When $m > 4$, this is greater $1.8^{r/2}$ yielding $1.8^{\sqrt{m}/2}$ and when taking into account the size of the input w.r.t m (not presented), we have for the size of the circuit the lower bound $2^{m^{1/8}}$
- The reference [Pud97] gives a tighter lower bound, but the proof is more complicated. However the set of graphs used in the proof are simpler

Conclusions

- We gave a method how to convert CP proofs of formulas of certain types to monotone real circuits
- We presented the Broken Mosquito Screen problem as a candidate for an exponential lower bound for CP
- We did not give the formulation of BMS problem as a CP formula
  - A polynomial formulation is given in the book
  - The formulation satisfies the non-negativity conditions on the factors of $\mathbf{p}$ required in the monotone circuit proof