Lecture 10

Oct 6

Last time: Cutting Planes stronger than resolution!

(Short proofs of PHP_n^{n+1} — polynomial size and $O(n)$ depth $\hookrightarrow O(\log n)$)

Thm Cutting Planes can efficiently simulate Resolution.

Pf. sketch **Reminder:** $x_1 \vee \overline{x_2} \vee x_3 \overset{\text{encoded}}{\leadsto} x_1 + (1-x_2) + x_3 \geq 1$

Let F be an unsat. CNF formula. Show how to simulate resolution rule with CP rules.

$$\frac{x_1 \vee \overline{x_2} \qquad x_3 \vee x_2}{x_1 \vee x_3} \leadsto \frac{x_1 + (1-x_2) \geq 1 \qquad x_3 + x_2 \geq 1}{x_1 + x_3 \geq 1} \checkmark$$

$$\frac{x_1 \vee \overline{x_2} \qquad x_2 \vee x_1}{x_1} \leadsto \frac{x_1 + (1-x_2) \geq 1 \qquad x_2 + x_1 \geq 1}{2x_1 \geq 1}$$

$$x_1 \geq \left\lceil \frac{1}{2} \right\rceil = 1 \checkmark$$

$$\frac{x_1 \vee \overline{x_2} \qquad x_2 \vee x_3 \vee x_1}{x_1 \vee x_3} \leadsto \frac{x_1 + (1-x_2) \geq 1 \qquad x_1 + x_2 + x_3 \geq 1}{\dfrac{x_i \geq 0 \qquad 2x_1 + x_3 \geq 1}{2x_1 + 2x_3 \geq 1}}$$

$$x_1 + x_3 \geq 1$$

In CP assume $0 \leq x_i \leq 1$ are present for every i.

$\square$

- CP can simulate resolution w/ $O(n)$ overhead

- CP is exp. stronger for some formulas. <u>Oct 6</u>

<u>Next</u> Lower bounds for Cutting Planes

Unlike Resolution — there is no known "combinatorial parameter" (like width in resolution) that controls the complexity of CP proofs.

(Vague) Open Problem: Find one? ("Natural generalization of width is not good")

Despite this, we have one proof technique for lower bounds.

Feasible Interpolation

Basic idea: reduce proving lower bounds on proofs to proving lower bounds on computations.

<u>ex</u> Let F be an unsatisfiable CNF of a particular form:

$F = A(x,y) \wedge B(x,z)$ on three disjoint sets of vars x, y, z.

e.g. Let $x \in \{0,1\}^{\binom{n}{2}}$ encodes edges in some n-vertex graph.

$A(x,y) = 1$ iff y encodes a k-clique in x.

$B(x,z) = 1$ iff z encodes a proper $(k-1)$ colouring of the vertices of x.

$A \wedge B$ is unsat!

(If two vertices u,v have $x_{uv} = 1$ then colours of u and v are different.)

There is a boolean function f_F on x-vars here:

$$f_F(x) := \begin{cases} 1 & A(x,y) \text{ is satisfiable} \\ 0 & \text{o/w} \end{cases}$$

Feasible Interpolation

Complexity of refuting $F = A(x,y) \wedge B(x,z)$ $\sim$ Complexity of computing f_F

Name comes from

Craig Interpolation Theorem [Craig 53]

If $\varphi \to \psi$ is true (φ, ψ are prop. formulas) then there is another formula ρ s.t.

$$\varphi \to \rho \to \psi$$

and further $\text{vars}(\rho) \subseteq \text{vars}(\varphi) \cap \text{vars}(\psi)$.

f_F is just a "ρ"!

$A \wedge B$ unsat $\Longleftrightarrow$ $A \vee \overline{B}$ is a tautology

$\Rightarrow B \Rightarrow A$ $\therefore$ ρ s.t. $B \Rightarrow \rho \Rightarrow A$

[Krajíček 94] Observed that the proof of Craigs Interpolation gives an efficient alg. for ρ.

Goal:

Thm [Pudlák 97] The Clique-Colouring tautologies require exponential length Cutting Planes refutations.

Pf Overview

(1) Given a Cutting Planes proof of $F = A(x,y) \wedge B(x,z)$, extract a real monotone boolean circuit computing the interpolant function f_F. ✓

(2) Prove real monotone circuit lower bounds for f_F.
(will not see)

First prove a "baby version":

Thm Let $F = A(x,y) \wedge B(x,z)$ be an unsatisfiable CNF formula then show the size of the smallest boolean formula computes f_F is at most $O(\text{poly}(S^T_{Res}(F)))$.

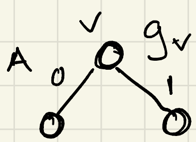
Pf. Uses communication complexity.

Defn Let $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. We consider computing f by the following 2-player game.

2 Players: Alice and Bob — Alice get $x \in \{0,1\}^n$, Bob $y \in \{0,1\}^n$. Their goal is to compute $f(x,y)$.

They do this by means of a communication protocol.

Formally, a protocol π is a tree T, where each internal node is labelled with A or B, and a function $g_v: \{0,1\}^n \to \{0,1\}$. Each outgoing edge is labelled with 0 or 1.



The leaves of the tree will be labelled with bits : $\{0,1\}$.

Given input (x,y), the players trace a path down the tree in the natural way: when they reach a node w/ A, Alice sends a bit to Bob and they go to the child. (Same for Bob if node labelled B).

Protocol computes f if the leaf they arrive at is labelled with $f(x,y)$.

Defn The **Karchmer–Wigderson game** for a boolean function $h:\{0,1\}^n \to \{0,1\}$ is the following 2-player communication problem:

- Alice get $x \in h^{-1}(1)$ – (i.e. $h(x)=1$)
- Bob get $y \in h^{-1}(0)$ – (i.e. $h(y)=0$)

Their goal is to find $i \in [n]$ s.t. $x_i \neq y_i$.

The (depth) **communication complexity** of the KW game to be the number of bits that must be communicated in any protocol solving the game.

The **communication size complexity** of the KW game is the minimum size of any protocol tree solving the game.

Punchline communication depth complexity of $KW(h)$

$$\|\|$$

depth of the shallowest circuit computing h

Communication size complexity of KW(h)

$\equiv$

size of the smallest boolean formula computing h

Search(F)

Communication protocol $\longleftrightarrow$ Prover-Delayer game

$\equiv$ $\qquad\qquad$ $\equiv$

boolean formula $\longleftrightarrow$ Resolution Proof