LECTURE 4

So far in the course: RESOLUTION

Lower bounds for: Pigeonhole principle formulas
Tseitin formula

Several techniques for proving lower bounds:
- Prover-Defendant game
- Random restrictions (partial assignments)
  [WILL SEE LATER IN COURSE]
- Width lower bounds
  [MIGHT BE ON PSET 2]

TODAY

Move on to CUTTING PLANES
Much less well understood
Essentially only one technique for proving size lower bounds: INTERPOLATION

Makes connection to CIRCUIT COMPLEXITY

Agenda
(1) Talk about circuits
(2) Talk about cutting planes
(3) Talk about interpolation (using concrete example)
(4) Illustrate proof technique, but for resolution
Next two lectures will then extend this to cutting planes

CIRCUIT

Directed acyclic graph (DAG)
n sources = labelled by variable inputs
Non-sources labelled by one of fixed set of Boolean functions
Typically require fan-in ≤ 2

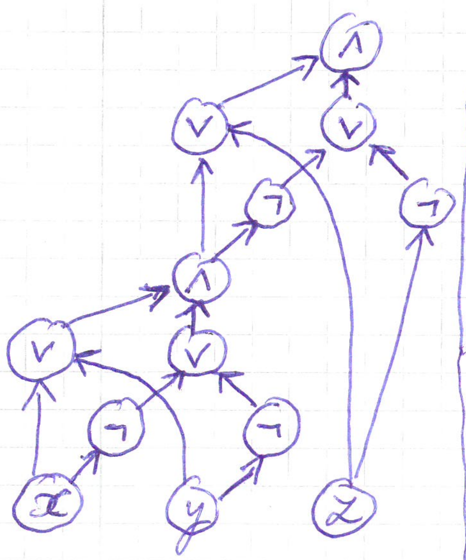
Standard gates

$\wedge$ AND	fan-in	2
$\vee$ OR	fan-in	2
$\neg$ NOT	fan-in	1

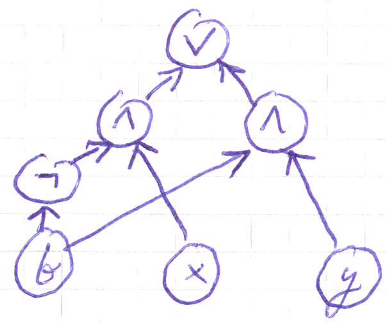
Every non-source vertex computes Boolean function on incoming edges
Single, unique sink = output of circuit

EXAMPLES

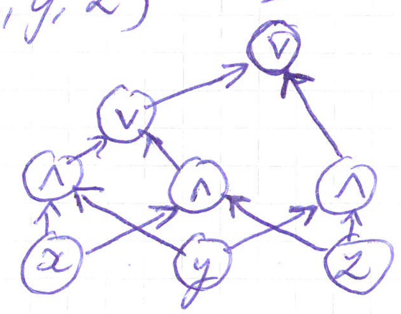
PARITY(x, y, z) [a.k.a. XOR(x,y,z)]



IF – THEN – ELSE
sel(b, x, y) = if b then y else x



MAJ(x, y, z) = majority among bit values x, y, z



For $x, y \in \{0,1\}^n$ write
$x \le y$ if for all $i \in [n]$ $x_i \le y_i$

$f : \{0,1\}^n \to \{0,1\}$ is a MONOTONE FUNCTION
if $x \le y \Rightarrow f(x) \le f(y)$

"Flipping an input bit from 0 to 1 can never flip f from 1 to 0"

PARITY and IF-THEN-ELSE are not monotone
MAJ is monotone

MONOTONE CIRCUIT: AND- and OR-gates but no NOT-gates

FACT A function $f : \{0,1\}^n \to \{0,1\}^n$ can be computed by a monotone circuit iff it is monotone.

Size of circuit: # vertices in DAG
For family of functions $\{f_n : \{0,1\}^n \to \{0,1\}\}_{n=1}^{\infty}$ can study sizes of smallest circuits computing these functions

CIRCUIT COMPLEXITY: Another approach for proving $P \neq NP$ (by showing something stronger)
Also not very successful.

But we can prove lower bounds for subclasses of circuits, e.g., monotone circuits.
We will use this today.

CUTTING PLANES (CP)

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

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

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

<u>Ex</u> $x \vee y \vee \overline{z} \rightsquigarrow x + y + (1-z) \geq 1$

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

Derivation rules

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

Addition $\dfrac{\sum_i a_i x_i \geq A \qquad \sum_i b_i x_i \geq B}{\sum_i (a_i + b_i) x_i \geq A + B}$

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

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

Note the rounding! very powerful

Clearly sound. Also implicationally complete (needs to be proven, of course)

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.

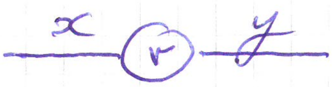
Let us look at another example.

EVEN COLOURING FORMULA $EC(G)$ [Markström 2006] IV

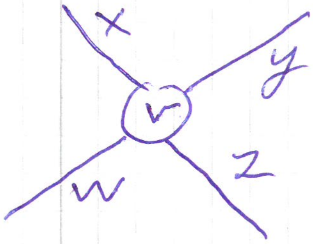
Undirected graph G; all vertices even degree $O(1)$
Variables = edges (also assumed to be connected)

For every vertex v, have CNF constraints

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

Ex 

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



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

OBSERVATION

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

FACT(?)

If G is a well-connected enough graph (of even degree) 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]
might be good thesis project

LEMMA If G is a graph with $|E(G)|$ odd and all vertices having even degree, then cutting planes can refute $EC(G)$ 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 $EC(G)$ 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) $q_{k,1} \lor q_{k,2} \lor \cdots \lor q_{k,n}$ $\quad k \in [m]$

(some vertex kth member of clique)

(b) $\overline{q}_{k,i} \lor \overline{q}_{k,j}$ $\quad i,j \in [n],\ i<j,\ k \in [m]$

(kth clique member uniquely defined)

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

(clique members connected by edge)

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

(every vertex has a colour)

(e) $\overline{p}_{i,j} \lor \overline{r}_{i,\ell} \lor \overline{r}_{j,\ell}$ $\quad i,j \in [n],\ i<j,\ \ell \in [m-1]$

$p_{i,j}$ = "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

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

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

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

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

Suppose unsat CNF $A(\vec{p},\vec{q}) \wedge B(\vec{p},\vec{r})$
where A CNF over $\vec{p},\vec{q}$
B —"— $\vec{p},\vec{r}$ $\quad$ $\vec{p},\vec{q},\vec{r}$ all disjoint

Can plug in assignment $\vec{\alpha}$ to $\vec{p}$ and simplify — get two disjoint formulas $A(\vec{\alpha},\vec{q})$ and $B(\vec{\alpha},\vec{r})$ one of which is unsat (or both)

A Boolean formula $I(\vec{p})$ is an **INTERPOLANT** if

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

Such an interpolant always exist (by definition)
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 short resolution refutation!

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

$\vec{\alpha}$ partial truth value assignment or **RESTRICTION**

How to simplify? (a) Remove satisfied clauses
(b) Remove falsified literals

Example $F = (x \vee y) \wedge (\bar{x} \vee z) \wedge (\bar{y} \vee \bar{z})$
$\alpha = \{z \mapsto 0\}$

$$F\restriction_\alpha = (x \vee y) \wedge \bar{x}$$

PROOF STRATEGY

- Start with formula $A(\vec{p},\vec{q}) \wedge B(\vec{p},\vec{r})$
- Assume exists short refutation
- Deduce existence of small interpolating circuit
- Appeal to (already known) circuit cplx lower bound saying no such small circuit exists.
- Contradiction! Hence there is no short refutation either, Q.E.D.

Proof systems for which this strategy works are said to have **FEASIBLE INTERPOLATION**

Resolution has feasible interpolation — yet another way to prove lower bounds

For cutting planes, this turns out also to work and is the <u>only known</u> lower bound technique

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

Today: Illustrate proof using resolution

Next two lectures: Do lower bound for CP

$\boxed{\text{MONOTONE CIRCUIT}}$

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

THEOREM [Razborov '85]
Let an undirected graph G be represented by $\binom{n}{2}$ bits encoding its edges and non-edges. Then for $m < \sqrt[4]{n}$ there is no monotone circuit of size $2^{o(\sqrt{m})}$ 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-colclique formula does!

<u>Remark</u> 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).

X

Recall

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

Just syntactic sugar

Will build circuits with gates $(\wedge, \vee, \mathrm{sel})$

[sel is not monotone function and needs to be removed in the end]

THEOREM [Pudlák 1997; based on Krajíček 1994]

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 $(\wedge, \vee, \mathrm{sel})$ such that

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

(2) Can construct from π resolution refutation

$$\left.\begin{array}{l} \pi_A : A(\vec{\alpha}, \vec{q}) \vdash \bot \text{ if } C(\vec{\alpha}) = 0 \\ \pi_B : B(\vec{\alpha}, \vec{r}) \vdash \bot \text{ if } C(\vec{\alpha}) = 1 \end{array}\right\} \text{ in length} \leq L$$

(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

$\boxed{q\text{-clause}}$ Clause in $A(\vec{p},\vec{q})\restriction_{\vec{\alpha}}$
or derived only from $A(\vec{p},\vec{q})\restriction_{\vec{\alpha}}$

$\boxed{r\text{-clause}}$ 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

<u>Base case</u> Axioms are either q-clauses or r-clauses — set $\tilde{C}_i = C_i\restriction_{\vec{\alpha}}$

<u>Induction step</u> 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

<u>Case 1</u> $\dfrac{C \vee p_k \quad D \vee \bar{p}_k}{C \vee D}$

$\alpha(p_k) = 0 \Rightarrow$ 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 $\quad \dfrac{C \vee q_k \quad D \vee \bar{q}_k}{C \vee D}$

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 $\tilde{C} = \tilde{C}' \vee q_k \quad \tilde{D} = \tilde{D}' \vee \bar{q}_k$
and both are q-clauses.
Resolve to get $\tilde{C}' \vee \tilde{D}'$ and replace with this clause

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

Dual of case 2. Dealt with in exactly analogous way

$C_\lambda = \bot$ and $\tilde{C}_\lambda \subseteq C_\lambda\restriction_{\vec{\alpha}} = \bot$

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

If $\tilde{C}_\lambda$ q-clause, derived from $A(\vec{p}, \vec{q})\restriction_{\vec{\alpha}}$
$= A(\vec{\alpha}, \vec{q})$ by resolution

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

Proves part 2 of thm

To prove part 1, build circuit over $\{\wedge, \vee, sel\}$ from Π

Note that every line C_i in proof has been classified as q-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

$0 =$ q-clause
$1 =$ r-clause

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 q-clause

$$z = x \vee y$$

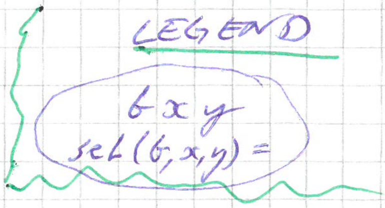
Case 3 $C \vee r_k$ (val x) $D \vee \bar{r}_k$ (val y)

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

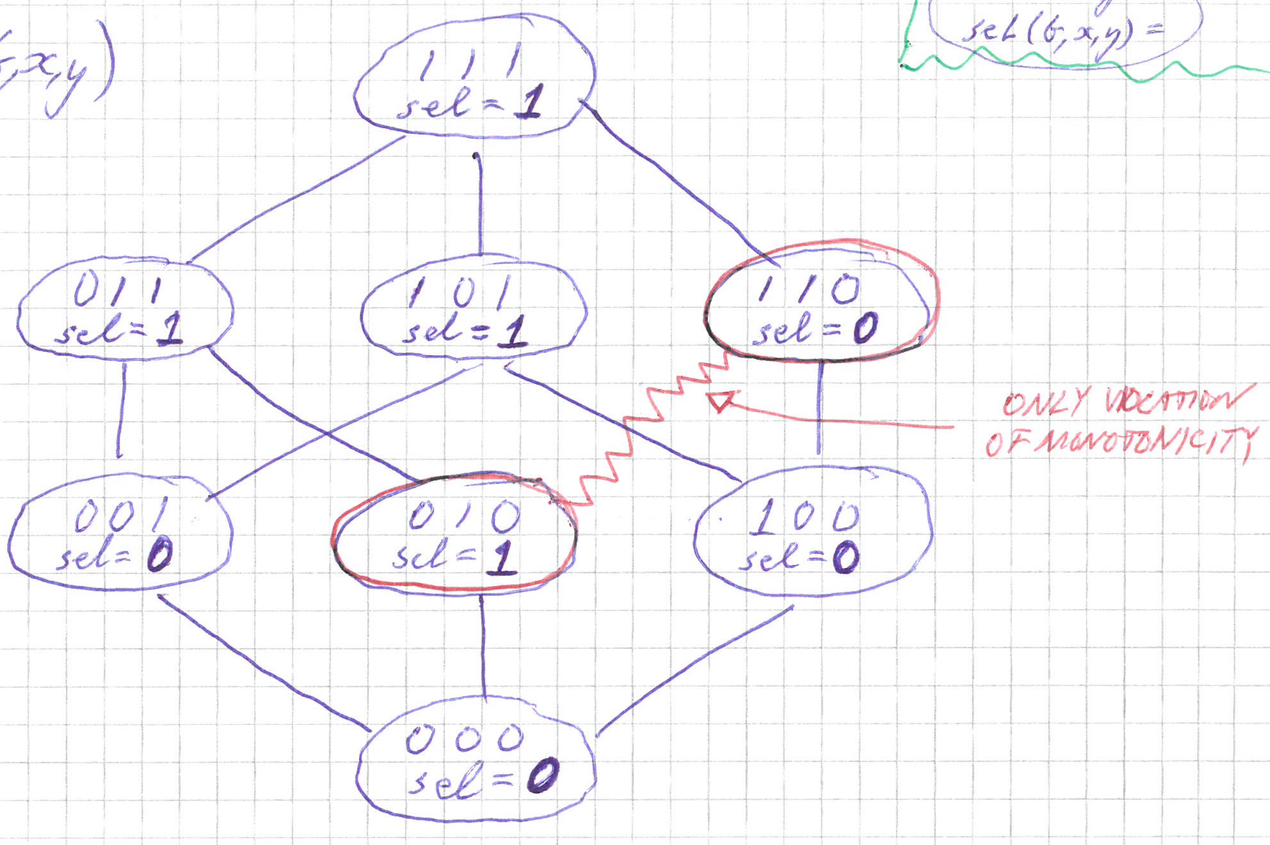
$$z = x \wedge y$$

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

But... Circuit not monotone, because $sel(b,x,y)$ is not monotone



$sel(b,x,y)$



Suppose $\vec{p}$ only appears positively in $A(\vec{p},\vec{q})$
(Other case is analogous)

Let's replace $sel(b,x,y)$ by $\boxed{(b \vee x) \wedge y}$ MONOTONE

Only difference for $(b,x,y) = 010 \mapsto 0$ instead of 1

When does this happen in proof?

$\alpha(p_k) = 0$, so we should have picked type from $\tilde{C}$, which is r-clause since $x = 1$. Instead we now pick q-clause $\tilde{D}$

<u>WRONG</u> if $\tilde{D}$ contains $\overline{p_k}$, because then $\tilde{D}\restriction_{\vec{\alpha}} = 1$ but $C \vee D\restriction_{\vec{\alpha}} \neq 1$, so condition

$$\tilde{D} \subseteq C \vee D\restriction_{\vec{\alpha}}$$

is violated and proof breaks.

But $\tilde{D}$ is a q-clause and so is derived only from $A(\vec{p}, \vec{q})$. And by assumption $\vec{p}$ only appears positively in $A(\vec{p}, \vec{q})$.

So this never happens! (Phew...)

This proves part 3 of the theorem and we are done. $\boxed{}$

Now if we combine this with the monotone circuit lower bound of Razborov we can deduce that for clique-coclique formulas with $m \approx \sqrt[4]{n}$ resolution needs refutations of length $\exp(n^\delta)$ for $\delta \approx 1/8$ or so.

Next two lectures:

- Prove this for cutting planes
- Also requires stronger circuit lower bound (for circuits computing not just with $\{0,1\}$ but arbitrary real numbers.