Final lecture today.

We are in the middle of proving that resolution and tree-like resolution are unlikely to be automatizable.

I.e., worst case it is likely not possible to find refutation of $F$ in time polynomial in the smallest refutation.

Result obtained by reduction from circuit complexity.

Given monotone circuit $C$, it is assumed to be hard to tell what is the smallest number of inputs that needs to be 1 in order to satisfy circuit $C$.

Let us jump straight into where we were — the proof of the main technical lemma.
\[
\text{Inputs to } F: \text{ choosing vector } \mathbf{a} \text{ at } j \text{ for column } j
\]
\[
\text{Inputs to } f_i: \text{ choosing circuit copy for row } i
\]
\[
\text{Value of node } v \text{ evaluated on row } i \text{ if circuit copy } c
\]
\[
\text{Notational shorthands}
\]
\[
[\text{col}_j = \mathbf{a}] \implies " F_j (x_j^1, ..., x_j^5) = \mathbf{a}"
\]
\[
[\text{ctrl}_i = c] \implies " f_i (y_i^1, ..., y_i^5) = c"
\]
\[
\overline{x_j^5} = (x_j^1)^{\overline{5}} \land (x_j^2)^{\overline{5}} \land ... \land (x_j^5)^{\overline{5}}
\]
\[
-x_j^5 = (x_j^1)^{-5} \lor (x_j^2)^{-5} \lor ... \lor (x_j^5)^{-5}
\]
\[
(x \land y) \rightarrow z = \overline{x} \lor \overline{y} \lor \overline{z}
\]

\text{Clauses Expansion to CNF of}

(i) \quad \exists \ y_i \in \text{Dom}(f_i) \quad \forall i \in [m]

(ii) \quad (\forall j \quad \exists \mathbf{a} \quad \exists \mathbf{c} \quad \forall i \in [m] \quad \alpha_i = 1)

(iii) \quad (\forall j \quad \exists \mathbf{a} \quad \exists \mathbf{c} \quad \forall i \in [m] \quad \alpha_i = 1)

(iv) \quad \forall i \quad \exists \mathbf{c} \quad \overline{Z_i} = \{z_i^1, z_i^2, ..., z_i^5\}

\text{sometimes also write}

\{z_i^1, z_i^2, ..., z_i^5\} = \{x_i^1, x_i^2, ..., x_i^5\}
Given $A \in \{0,1\}^m$, define
\[
d_1(A) = \max \{ d \mid \text{s.t. for any } d \text{ vectors } \hat{a}^{(1)}, \ldots, \hat{a}^{(d)} \in A \text{ if } i \in [m] \text{ s.t.} \\
\hat{a}^{(i)}_1 = \ldots = \hat{a}^{(d)}_i = 1 \}
\]
\[
d_0(A) = \max \{ d \mid \text{s.t. for any } d \text{ distinct } i_1, \ldots, i_d \in [m] \text{ if } \hat{a} \in A \text{ s.t.} \\
\hat{a}_{i_1} = \ldots = \hat{a}_{i_d} = 0 \}
\]

For $D$ choose over $\text{Vars}(T(C, b, F, f))$ define
\[
W_x(D) = \# \text{ x-variables in } D \\
W_y(D) = \# \text{ y-variables in } D \\
W_c(D) = \# \text{ variables } z^c \text{ in } D \\
\text{(note that } c \text{ fixed)}
\]

The \textit{controlled width} of $D$ is
\[
\tilde{W}(D) = W_x(D) + W_y(D) + r \cdot \min_{c \in [r]} W_c(D)
\]

Recall $k(C) = \text{minimum Hamming weight}$ of any satisfying assignment for $C$
We have a monotone circuit $C(p_1, \ldots, p_n)$ and a set of vectors \( \mathcal{A} \subseteq \{0,1\}^m \). There are functions $F_1, \ldots, F_n : \{0,1\}^S \to \mathbb{R}$ such that $f_i$ possibly partial, and $m, r, s$ are arbitrary positive integer parameters such that
\[ r = \Omega(s) \]

Then
\[ (a) \quad \chi(C) \leq d_{\chi}(\mathcal{A}) \]
\[ \ell_{\mathcal{R}}(\mathcal{T}(C, \mathcal{A}, F, F) + 1) = O(1)^{1.2^s(k(c) + 1)} \]

\[ (b) \quad \tilde{W}(\mathcal{T}(C, \mathcal{A}, F, F) + 1) \geq \frac{c2}{2} \min \{k(c), d_{0}(\mathcal{A})\} \]

\[ (c) \quad \ell_{\mathcal{R}}(\mathcal{T}(C, \mathcal{A}, F, F) + 1) = \exp(2^{\log(2)(\frac{r^2}{2} \min\{k(c), d_{0}(\mathcal{A})\})}) \]

Did proof of (a) last time.

$k(C) \leq d_{\chi}(\mathcal{A}) \Rightarrow$ for any choice of vectors $\exists$ row $i$ forcing $C$ to 1, say $(1^k 0^{n-k})$.

But $\mathcal{T}(C, \mathcal{A}, F, F)$ claims $C$ evaluates to 0 on this input.

Do top-down proof in circuit showing that not all k+1 first inputs can be 1 — contradiction.
Define "progress measure" \( \mu : \text{clauses} \rightarrow \mathbb{N} \) such that

(i) \( \mu(\text{axiom}) = 1 \)
(ii) \( \mu \) subadditive, i.e. \( \mu(BvC) \leq \mu(Bvx) + \mu(Cv\overline{x}) \)
(iii) \( \mu(\bot) \) large

Hence any refutation \( T : T(Cit, \overline{v}, \overline{f}) \vdash \bot \)
must contain clause \( D \) with \( \mu(D) \) medium-large.

(iv) Prove \( \mu(D) \) medium-large
    \[ \Rightarrow \tilde{W}(D) \text{ large} \]

Note that all axioms in \( T(Cit, \overline{v}, \overline{f}) \) refer
to one specific row \( i \). Let

\[ R_i = \{ \text{all axioms greeking about row } i \} \]

and

\[ \mu(D) = \min \{ |I| : I \subseteq [m], \cup_i R_i = D \} \]

Properties (i) & (ii) above are immediate

Let us describe intuitively how to
do (iii) and (iv). Need to
prove Claims 1 & 2 on next page,
after which Part (6) follows.
**Claim 1** \[ \mu(I) > d_0(A) \]

**Proof sketch**

Equivalently, if \(|I| \leq d_0(A)\)

then \( \bigcup_{i \in I} R_i \) is satisfiable.

For any such \( I \), pick \( \tilde{a} \in A \) s.t.

\( \tilde{a}_i = 0 \) for \( i \in I \) (possible since \(|I| \leq d_0(A)\))

Consider matrix \( M = \begin{pmatrix} \frac{1}{\tilde{a}} & \cdots & \frac{1}{\tilde{a}} \\ 1 & \cdots & 1 \end{pmatrix} \)

C evaluates to 0 on all rows \( i \in I \) of \( M \), so \( \bigcup_{i \in I} R_i \) satisfiable \( \square \)

Hence \( \exists D \in \Pi \) with \( \frac{d_0(A)}{2} < \mu(D) \leq d_0(A) \)

**Claim 2** If \( \mu(D) \leq d_0(A) \), then

\[ \widehat{\nu}(D) = \mu(D) \cdot \min \left\{ k(c), \frac{d_0(A)}{2} \right\} \]

\[ + \cdot \min \left\{ k(c), \mu(D) \right\} \]

**Proof sketch**

Fix \( I \in \mathbb{I} \) minimal such that

\[ \bigcup_{i \in I} R_i = D \]

i.e., \( \mu(D) = |I| \). By minimality, \( \forall i \in I \)

\[ \bigcup_{i \in I \setminus \{i\}} \neq D \]
i.e., we can evaluate all rows in \( I \) except \( i_0 \) correctly and still falsify \( D \).

Now if \( \tilde{W}(D) \) too small, can find

(a) \( > n - k(c) \) columns \( \tilde{A} \) where \( D \) mentions \( < r \) variables \( \tilde{y} \), choosing column vectors

(b) row \( i_0 \) where \( D \) mentions \( < r \) variables \( \tilde{y}_{i_0} \), choosing circuit copy

(c) control \( C_0 \) such that \( D \) doesn't say anything about row \( i_0 \) being evaluated in \( C_0 \)

Do the following:

(a') change \( n - k(c) \) columns to vector \( \tilde{A} \) such that \( \tilde{a}_i = 0 \) for \( i \in I \) (by \( r \)-surjectivity of \( \sigma \))

without assigning to variables in \( D \)

(b') change variables \( \tilde{y}_{i_0} \) to choose circuit copy \( C_0 \) for row \( i_0 \) (again by \( r \)-surjectivity of \( \sigma \))

(c') Evaluate row \( i_0 \) correctly on circuit \( C_0 \), yielding output 0 since \( < k(c) \) positions are 1.

This satisfies \( R_{i_0} \).

\( \forall i \in I \setminus \{i_0\} \) still satisfied (requires assignment)

But \( D \) false, since we didn't touch \( \text{Vars}(D) \).

Contradiction
Formal proof of Claim 1

Fix any $I \subseteq [m]$, $|I| \leq d_0(A)$
Choose $\bar{a}^* \in \mathcal{T}$ s.t. $\bar{a}^*_i = 0$ for $i \in I$.
Choose $\delta_j \in \{0,1\}^m$ s.t. $F_j(\delta_j) = \bar{a}^*$
for all $j \in [n]$ (possible since $F_j$ onto)
Set $\bar{x}_j = \delta_j$

Set $\bar{y}_i$, $i \in [m]$ in any way that satisfies axioms (ii) (possible since $f_i$ surjective, and hence defined somewhere)
Set $\bar{x}_i, \bar{z}_i = 0$ for all $i \in I$

Now verify that this assignment satisfies $V_{i \in I} R_i$.

Axioms (i) OK by construction above

Axioms (ii) OK since all such axioms will have $\bar{a} \neq \bar{a}^*$ and hence $[col_j = \bar{a}]$ will be false.

Axioms (iii) & (iv) OK since all $z$-variables set to false, and this is a correct computation since all inputs are false.

Hence $V_{i \in I} R_i$ satisfiable if $|I| \leq d_0(A)$, so $\mu(1) > d_0(A)$ as claimed. \(\Box\)
Formal proof of Claim 2

Fix any $D$ such that $\mu(D) \leq d_0(t)$

Fix any minimal-size $I \subseteq [m]$ such that

$$\forall i \in I \quad R_i \models D$$  \hspace{1cm} (1)

Will show that if $\tilde{W}(D)$ too small, then can find assignment satisfying $\forall i \in I \quad R_i$ but falsifying $D$ — contradiction.

If $\forall i \not\in I$ we have one of the following

1. $D$ contains $\geq r$ variables in $\{y_i \mid v \in S\}$, or
2. $\forall v \in [r] \quad D$ contains at least one variable among $\{z_{i,v} \mid v \text{ code in } C\}$

then we are done. In case (1) we get a contribution $\geq r$ to $W_j$ and in case (2) a contribution $\geq r \cdot \text{min}_{c \in [r]} W_c(D)$

So suppose $\exists i_0 \in I$ s.t. neither (1) nor (2) holds.

Then $\exists c_0 \in [r]$ s.t. no variable $z_{i_0,v}$ appears in $D$, i.e. $D$ doesn't talk at all about evaluating row $i_0$ in circuit copy $C_{c_0}$
Fix assignment $\alpha$ to $\text{Vars}(E(\sigma t, p, f))$ that satisfies

$$\forall i \in I \backslash \{i_0\}, R_i$$

and falsifies $D$ (must exist since $I$ was chosen minimal).

Let $J_0$ consist of those $j \in [n]$ for which $D$ contains at least $r$ variables from $\{x_j^v \mid v \in [s]\}$.

If $|J_0| \geq k(c)$ then $\tilde{W}(D)$ is as large as claimed, so suppose $|J_0| < k(c)$.

Now we will change $\alpha$ to $\alpha'$ such that

$$\alpha'(\forall i \in I, R_i) = 1$$

without assigning to $\text{Vars}(D)$.

Fix $\tilde{\alpha}^* \in \tilde{A}$ s.t. $\tilde{\alpha}^* = 0 \quad \forall i \in I$

**STEP 1** For every $j \in [n] \backslash J_0$, change values of $\{x_j^v \backslash \text{Vars}(D)\}$ so that

$$F_j(x_j^v) = \tilde{\alpha}^*$$

This is possible since $F_j$ is $r$-surjective.

**STEP 2** Change values in $\tilde{g}_{i_0} \backslash \text{Vars}(D)$ so that

$$f_{i_0}(\tilde{g}_{i_0}) = c_0$$

This uses $r$-surjectivity of $f_{i_0}$
STEP 3: Reassign all variables

\{ Z_{i_0,v} \mid v \in C \}

to the values computed by \( C \) when fed the characteristic vector \( \mathbf{1}[T_0] \) of \( T_0 \) as input, i.e., the vector in \( \{0,1\}^n \) s.t.

\[
\mathbf{1}[T_0]_i = \begin{cases} 1 & \text{if } i \in T_0 \\ 0 & \text{otherwise} \end{cases}
\]

Note that \( Z_{i_0,v} \) gets set to 0 since \( |T_0| < k(C) \).

Claim 3: \( x' \) as constructed above satisfies \( \forall i \in R' \) but falsifies \( D \).

Proof: We never changed \( \text{Vars}(D) \), so \( x'(D) = x(D) = 0 \) by assumption.

\( R_{i_0} \): axioms are satisfied — we know inputs \( I \) can only appear in positions in \( T_0 \), and \( C_{i_0} \) is evaluated to zero correctly even assuming all positions in \( T_0 \) are 1.

For \( \forall i \in E_{i_0} \setminus R' \), axioms of type (i), (iii) and (iv) are OK — we didn't touch these variables when modifying \( x \) to get \( x' \).
What about axioms (ii)?

Intuitively we should be OK since we are just flipping inputs in columns \( \hat{C}_n \setminus \hat{C}_0 \) from 1 to 0 and \( C \) is monotone.

Formal case analysis:

(a) \( j \in T_0, i \neq i_0 \):

No variable values were changed — OK

(b) \( j \notin T_0 \):

The chosen column \( \alpha_i \) might have been changed (to \( \alpha_i^* \)), but when doing so the only thing that happened in rows I was that 1s changed to 0s. So if \( \hat{F}(z_i^*, \hat{p}_j) = 0 \) before, then that is because we had chosen a vector \( F(\bar{z}_i) = \bar{\alpha}_i \) such that \( \alpha_i = 0 \) and this holds for \( \alpha^* \) as well.

(c) \( j \in T_0, i = i_0 \):

Such axioms of type (ii) get satisfied dummy step 3, since row \( i_0 \) is now evaluated in circuit copy \( C_{i_0} \) and this evaluation is correct on the characteristic vector of \( T_0 \).

This establishes subclaim 3, and claim 2 follows.
Part (c) standard random restriction argument

1. Design distribution $R$ s.t. for $g \in R$
   $T(C \land \neg \overline{F}, \overline{F}) \models g = T(C \land \neg \overline{F}, \overline{F})$

2. Show for wide clauses $D$ over
   $\text{Vars}(T(C, \overline{x}, \overline{F}, \overline{F}))$ that
   $D \models g = 1$ except with exponentially small probability

3. For a short refutation $T : T(C, \overline{x}, \overline{F}, \overline{F}) \vdash \bot$
   by union bound $\exists g \in R$ s.t.
   $\Gamma \cup \neg g$ has no wide clauses

4. But such a refutation $\Gamma \cup \neg g$ of
   $T(C, \overline{x}, \overline{F}, \overline{F})$ contradicts the
   width lower bound in part (b).

Distribution $\mathcal{P}_{d, \overline{R}}$

$d \in \mathbb{N}^+, \overline{d} \leq r \quad \overline{R} \subseteq [r]$

a) For every $i \in [m]$ pick $d$ variables
   in $Y_i$ randomly and set randomly
   (uniformly and independently to 0/1)

b) For every $j \in [n]$ pick $d$-variables
   in $Z_j$ randomly and set randomly

c) Set all variables $\cap \forall \overline{z}_i \cup \overline{c} \in [r] \setminus \overline{R}$
   randomly
Think of $R$ as circuit copies that might evaluate correctly. 
$L \setminus R$ are circuit copies that are broken and must not be used.

Our (random) restrictions

Think of $[\ldots]$ as restriction followed by pruning step

1) $G_j = F_j \mid s$ for $j \in [n]$

2) $g_i = f_i \mid s$ for $i \in [m]$

Set $\text{Dom}(g_i) = \{ o \mid g_i(o) \in R \}$

Then, for $o \in \text{Dom}(g_i)$, we add axioms

$g_i \in \text{Dom}(g_i)$

which subsume all axioms $(ii), (iii), (iv)$ for circuit copies $C \in L \setminus R$.

Consider $\tau(C, t, \vec{G}, \vec{g})$.

Since $\tau(C, t, F, f)$ can be derived from this formula by weakening any refutation of $\tau(C, t, F, f)$, it also refutes $\tau(C, t, \vec{G}, \vec{g})$. 

Random restriction $R \subseteq \mathcal{R}$

- Choose $R \sim R$ randomly, where $R$ uniform distribution over all subsets of $\mathcal{S}$ of size $r/2$.
- Then choose $g \in \mathcal{R}_{r/2, R}$ randomly as above.

$\tilde{g} = g/F$, and $\tilde{f} = f/G$ are $r/2$-surjective.

Hence any restriction of $\tilde{f}(C, t, \tilde{F}, \tilde{f})/g$ contains a clause of controlled width $\frac{r}{4} \min \{k(C), d_0(t)\}$.

Claim: If $\tilde{W}(D) \geq \frac{r}{4} \min \{k(C), d_0(t)\}$

then $\Pr_{g \in \mathcal{R}_{r/2, R}} [D|g = 1] \geq 1 - \exp \left(-\frac{r^2}{5} \min \{k(C), \frac{d_0(t)}{5}\} \right)$

**Proof sketch:** If $\tilde{W}(D)$ large, then $D$ contains

1) many $x$-variables as inputs to $\tilde{F}$,
2) many $y$-variables as inputs to $\tilde{f}$, or
3) many $z$-variables describing circuit evaluations in different copies.

In all cases (a)-(c), $g$ will set many such variables randomly, and so $D$ is very likely to get satisfied."
Formal proof of Claim 4

We must have that either \( W_x(D) \) or \( W_y(D) \), or (3) \( r \cdot \min_{c \in C} W_c(D) \) is bounded from below by

\[
-\Omega \left( r \cdot \min \{ k(\epsilon), d_0(x)^2 \} \right)
\]

Case 1: \( W_x(D) \) large

Let \( W_{x,y}(D) = \# \text{ variables } x_j \) in \( D \)

\( S \) chooses \( r/2 \) out of \( S \) variables \( x_j \)

Expected size of intersection \( \frac{r}{2} - W_{x,y}(D) \)

Will get at least half of this except with exponentially small probability

Every variable in this intersection satisfies \( D \) with probability \( 1/2 \) when set by \( S \)

So probability \( D \) not satisfied by \( j \)th group

\[
\leq \exp \left( -\Omega \left( \frac{r}{S} W_{x,y}(D) \right) \right)
\]

Different groups are independent, so total probability \( D \) not satisfied

\[
\leq \prod_i \exp \left( -\Omega \left( \frac{r}{S} W_{x,y}(D) \right) \right)
\]

\[
= \exp \left( -\Omega \left( \sum_{i} \frac{r}{S} W_{x,y}(D) \right) \right)
\]

\[
= \exp \left( -\Omega \left( \frac{r}{S} W_x(D) \right) \right)
\]
Plugging in the assumption
\[ W_x(D) = \Omega\left( r \cdot \min \{ k(c), d_0(t) \frac{3}{5} \} \right) \]
yields that \( D \) is "killed" (i.e., satisfied)
except with probability
\[ \leq \exp\left( -\Omega\left( \frac{r^2}{5} \min \{ k(c), d_0(t) \frac{3}{5} \} \right) \right) \]
as desired.

**Case 2:** \( W_y(D) \)
Treated in the same way as case 1

**Case 3:** \( r \cdot \min_{c \in [r]} W_c(D) \) large

Note that \( \gamma \) sets all \( Z_{i,v} \)-variables
for \( r/2 \) controls \( c \) uniformly and
independently at random.
For any such control \( c \), clearly the
number of variables present in \( D \)
is at least \( \min_{c \in [r]} W_c(D) \).
Hence, \( D \) is satisfied except with prob
\[ \leq 2 - \frac{r}{2} \cdot \min_{c \in [r]} W_c(D) \]
\[ \leq \exp\left( -\Omega\left( \frac{r^2}{5} \min \{ k(c), d_0(t) \frac{3}{5} \} \right) \right) \]
using the above-assumption.

Then \( \Gamma \) is optimum.
Fact 5

If \( \pi \) is a resolution refutation of length \( L \).
\( \mathcal{R} \) is a distribution of random restrictions s.t.
\( w \)-wide clause \( D \) gets killed except
with probability \( \leq 1/k \).

then \( \exists g \in \mathcal{R} \) s.t. \( \Pi /g \) contains
no \( w \)-wide clauses.

Combine:
- part (b) of lemma
- Claim 4
- Fact 5

to deduce that
\[
\mathcal{L}_{\mathcal{R}}(\pi(C, g, \bar{F}, \bar{F})) = \\
= \exp\left( -\frac{r^2}{5} \min \{k(C), d_0(t)\beta\} \right)
\]

Part (c) follows.

We are done with the main technical
lemma.
Only a few small details missing...

Actually many details missing, and won't have time to do all — several more lectures would be required.

But let us try to do something.


**Main Reduction Lemma**

There is poly-time $R$ taking inputs $(C, \Sigma_m)$, $C$ monotone circuit, $m \in \mathbb{N}^+$, and outputting unsatisfiable CNF formula $F(C, m)$ such that

a) $L_R(F(\Sigma_m) + 1) \leq 1 C \cdot m O\left(\min E_k(C), \log m^2\right)$

b) $L_R(F(\Sigma_m) + 1) = m O\left(\min E_k(C), \log m^2\right)$

Proof uses tools from different areas of TCS and math. Going into all details beyond scope of this course. Let us look at ingredients...
Proof sketch

Pick the smallest prime $p > m$.

Fact: $m \leq p \leq 2m$

Since $p = O(m)$, can just assume $m$ is prime — this won’t change the bounds in the lemma.

Let $P_m = m \times m$ PALEY MATRIX

given by

$$a_{ij} = \begin{cases} 1 & \text{if } i \neq j \text{ and } y(i-j) \\ 0 & \text{otherwise} \end{cases}$$

is a QUADRATIC RESIDUE mod $m$

if there is an integer $s_i \in [m-1]$ such that $s_i^2 \equiv q \pmod{m}$.

Let $A = \text{columns of } P_m$

Then $|A| = m$

Fact $d_0(A), d_2(A) \geq \frac{1}{4} \log m$

Let $h \in \mathbb{N}^+$ suitable constant to be fixed later.

Let $r = \sqrt{\log m}$

$s = h \cdot \sqrt{\log m}$
$(n, k, d)_2$ - ERROR CORRECTING CODE

$2^k$ messages think of as just set $S$ code words
Every $m \in S$ encoded to $E(m) \in \{0,1\}^n$
For $m_1, m_2 \in S$, $E(m_1)$ and $E(m_2)$
always differ in $\geq d$ positions - have
HAMILTON DISTANCE $d$.

This means that if someone corrupts
$\leq \frac{d-1}{2}$ bits of $E(m)$, e.g., because
of noise in a transmission channel,
we can still uniquely recover $m$.

Error-correcting codes can be constructed
efficiently.

Fix code with minimum distance $d \geq 2r = 2^{\lceil \log m \rceil}$
dimension $k = r = \lceil \log m \rceil$
block length $n = s = k \cdot \lceil \log m \rceil$

Encode $a^{(0)}, \ldots, a^{(m)} \in A$ using $E$
Define $F_j(\sigma)$ by $F_j(\sigma) = a^{(i)}$ if
$\sigma$ within distance $r$ from $E(a^{(i)})$
For other $\sigma$ define arbitrarily.
Do the same for functions $f_i$, i.e $\bar{c} \\

Now we have defined $\bar{C}, \bar{F}, \bar{f}$ and can generate $\bar{C}(\bar{c}, \bar{\bar{F}}, \bar{\bar{f}})$

size of formula (and time for generation) polynomial in $|c|, m$, $2^{O(m)}$.

All $F_i$ and $f_i$ are $r$-surjective.

Suppose we want $\bar{F}_j(\bar{x}_j) = \bar{a}$.

Fix $\leq r$ variables $x^j_i$ adversarially.

We can pretend these are the positions corrupted in $\bar{F}(\bar{a})$. Since we have an error-correcting code, we can recover $\bar{a}$ from the remaining, uncorrupted positions.

Part (c) of main tech lemma yields lower bound.

We might not have condition $k(c) \leq d, (d)$ satisfied, though. Might even be hard to compute.

Instead, do a trick. Let $G_m$ be some fixed (poly-time constructible) CNF formula s.t. $\Delta_k(G_m+1) = \Theta(2^k(G_m+1)) = m \Theta(2^k m)$

and in more detail (5) is valid for CNF (m) \[ \text{wrt} \bar{c} \bar{c} \bar{c} \bar{c} \]
Choose variable names so that
\[ \text{Vars} (G_m) \cap \text{Vars} (\tau (C, \overline{F}, F)) = \emptyset. \]
Set \[ F(C, m) = G_m \land \tau (C, \overline{F}, F). \]
Since \( G_m \) and \( \tau (C, \overline{F}, F) \) disjoint, any refutation must refute completely one of these formulas. So lower bound still holds, and new upper bound in tree-like resolution also OK.

Using weak reduction lemma + assumed automaticality, can estimate \( k(e) \)

**LEMMA** If resolution or tree-like resolution is automaticable, then \( \exists \) absolute constant \( k \) and algorithm \( \Phi \) s.t.

1. \( \Phi \) takes input \( C, k \)
2. Running time \( \exp (O(k^2)) \text{ poly } (|C|) \)
3. If \( k(e) \leq k \), then \( \Phi(C, k) = 1 \)
4. If \( k(e) > k \cdot k \), then \( \Phi(C, k) = 0 \)

This solves a "gap version" of the problem. Use self-improvement to blow up \( C \) to \( C^{(d)} \) s.t. \( k(C^{(d)}) = k(C) \cdot d \)
Then run the algorithm \( \Phi \) on inputs \((C, 1), (C, 2), (C, 3), \ldots\)
until we get answer 1 from \( \Phi \).

With parameters set appropriately, this yields:

**Theorem.** If resolution or tree-like resolution is automatizable, then for any fixed \( \varepsilon > 0 \) there is an algorithm that takes monotone circuit \( C \), runs in time \( \exp(\text{poly}(k(C))) \), and approximates \( k(C) \) to within factor \((1 + \varepsilon)\).

One further problem is that the running time has very bad dependence on \( \varepsilon \). To get the full result that "if resolution or tree-like resolution is automatizable, then \( W[P] \) is tractable" some further work is needed.

But it is time to wrap up this course.
What did we see during this course?

Proof systems
Resolution
k-DNF resolution
Bounded-depth Frege
Cutting planes

TECHNIQUES / OTHER TOPICS

Graph theory (expanders)
Circuit complexity
Interpolation
Communication complexity (Parr's lemmas)
Switching lemmas
Parameterized complexity
Today even abstract algebra error-correcting codes

(General theme in TCS: it's all connected...)

What did we not see?

Most of proof expa... E.g.:<br />
- Upper bounds for Frege
- Algebraic proof systems such as polynomial calculus and even stronger systems based on algebraic circuits
- Proof systems formalizing breadth and semidefinite programming hierarchies (super-hot topic)
- Study of other proof complexity measures such as width/degree/rank, space, etc
- And some more...
PSET 3
Should be out this week
Deadline and peer evaluation in January

SCRIBE NOTES
Both you and we believed schedule would be good to have them done before Christmas — will help you when you work on pset 3

FINALLY
Hope you enjoyed the course!
We always have interesting thesis projects for strong students.
And if you really got hooked then you should consider applying for a PhD position (we are hiring)