started this course looking at Resolution
lines in proofs are clauses
Resolution rule: \[ \frac{C \lor x, D \lor \neg x}{C \lor D} \]
Then detour to Cutting Planes
geometric proof system
lines in proofs are linear inequalities
= hyperplanes in \( \mathbb{R}^n \) (\( n = \# \text{variables} \))
Now go back to proof systems where lines are Boolean formulas
Can allow more general formulas as proof lines
Can generalize resolution rule to
CUT RULE:
\[ \frac{F \lor H, G \lor \neg H}{F \lor G} \]
(Plus other rules for syntactic manipulation of formulas)
Most general form with essentially no restrictions on formulas
FREEZE PROOF SYSTEMS
Very strong. Do not know how to prove strong lower bounds (or almost any lower bounds) for these systems
Best lower bounds are quadratic.
BOUNDDED-DEPTH Frege

Formulas must have bounded number of alternations between ∧ and ∨

Only clauses $V_i a_i$: Depth-1 Frege = resolution

DNF formulas $V_i V_j a_{ij}$: Depth-2 Frege

Disjunctions of CNF formulas $V_i V_j V_k a_{ijk}$: Depth-3 Frege

Et cetera

Bounded-depth Frege (vanilla definition)

Start with CNF formula, as before

All lines in proof are formulas of depth $\leq d$ for some fixed $d \in \mathbb{N}^+$

using cut rule or synthetic messaging rules

Prove lower bound by showing for some CNF formula family $\{F_n\}_{n=1}^\infty$ that minimum-size refutations scale super-polynomially

Cutting planes and bounded-depth Frege both right at the research frontier

Major progress has been made in the last few years. But still many open problems

Already talked a bit about cutting planes

Now more on to bounded-depth Frege
But a bit cautiously...
Next few lectures focus on proof systems strictly between resolution and depth-2 Frege

"Resolution with formula conjunctions" or
"d-DNF resolution" or "Res (d)" or "R(d)"

lines in proofs are d-DNF formulas
(disjunctions not of literals, but of
conjunctions or terms of size d)

Resolution rule generalized to

\[ F \lor (a_1, a_2, \ldots, a_d) \quad G \lor \overline{a_1}, \overline{a_2}, \ldots, \overline{a_d} \]

\[ \overline{F \lor G} \]

Proof system defined by Krajíček in 2001
We will follow papers [Segerlind, Buss, Impagliazzo 2004]
[Alekhnovich 2001]
(journal versions of slightly earlier conference papers) to show

1. PHP formulas hard for d-DNF resolution
2. Random k-CNF formulas

We will not show, but it is true, that:

3. (d+1)-DNF resolution is exponentially
   stronger than d-DNF resolution
Proof system often called k-DNF resolution. But since we want to talk about refutation of k-CNF formulas, and that k is often different, we will try (at least in this lecture) to say "d-DNF resolution". We will sometimes use the shorthand "R(d)" for brevity. Also, will try to reserve "F" for CNF formulas, from now on, using G and H for d-DNF formulas.

Let us now give some formal definitions

PRELIMINARIES

Term: conjunction a, a2, ..., ad

d-term: a, literals size of term = d

DNF formula: disjunction of terms

d-DNF formula: disjunction of terms of size ≤ d

(A clause is a 1-DNF formula.)

Two terms t, t' are consistent if the term t ∨ t' is satisfiable, i.e., if there is no literal a with a ∈ t, a ∈ t' (We assume that a term is consistent with itself)

Will also consider terms as sets of literals when convenient, so, e.g., |t| = size of term
\( \text{\textit{d-\textit{DNF resolution inference rules}}} \)

\[ \text{\textit{d-CUT}} \quad \frac{G, H, \text{\textit{d-DNF formulas}}}{(a, \ldots, a_d, 1) \lor G \quad \bar{a}, \ldots, \bar{a}_d, \lor H}{G \lor H \quad d_1 \leq d} \]

\[ \text{\textit{\Lambda-INTRODUCTION}} \quad \frac{G \lor t \quad G \lor t'}{G \lor (t \land t') \quad |t \land t'| \leq d} \]

\[ \text{\textit{\Lambda-\textit{EQUATION}}} \quad \frac{G \lor t}{G \lor t'} \quad t' \leq t \]

\[ \text{\textit{WEAKENING}} \quad \frac{G}{G \lor H} \quad H \text{ any d-DNF formula} \]

There are slightly different definitions in the literature, but the variations don't really matter. We will go with this definition, at least for now.

\[ \text{\textit{d-DNF resolution of CNF formula} } F \]

\[ F = (G_1, G_2, \ldots, G_k) \]

Each \( G_i \) is either (a) axiom clause \( \text{EF} \) or (b) derived from previous lines using the inference rules above. \( G_k \) is empty d-DNF formula (denoted \( \bot \))
Side note 2

Empty clause = falsity; no literal can satisfy it
Empty d-DNF formula = falsity; no term can satisfy it
Empty term = truth; no literal can falsify it

Somewhat analogous to

\[ \sum_{i=1}^{0} a_i = 0 \quad \prod_{i=1}^{0} a_i = 1 \]

\[ \sum_{i=1}^{d} 2^i (\binom{n}{i}) = O(n^d) \text{ terms of size } d \] (assuming \( d = O(1) \))

\[ \text{where } \binom{n}{i} \text{ is the binomial coefficient} \]

So we usually don't care too much to distinguish between the two.

We also don't care too much about exactly how d-DNF resolution is defined, because we will only use that the derivation rules are STRONGLY SOUND as defined next.
**Definition 1 (Strong Soundness)**

Let \( G_i, i \in \{S\} \), and \( H \) be \( d\)-DNF formulas. We say that \( G_1, \ldots, G_S \) strongly implies \( H \) if for any set of mutually consistent terms \( t_i \in G_i, i \in \{S\} \), it holds that there is a term \( t \in H \) such that

\[
\bigwedge_{i=1}^S t_i \models t.
\]

We say that a proof system (operating with \( d\)-DNFs) is strongly sound if whenever \( H \) is derived from \( G_1, \ldots, G_S \) it holds that \( G_1, \ldots, G_S \) strongly implies \( H \).

Recall that \( G \models H \) if for any (total) truth value assignment \( \alpha \) s.t. \( \alpha(G) = 1 \) it holds that \( \alpha(H) = 1 \).

**Observation 2**

If \( G_1, \ldots, G_S \) strongly imply \( H \), then \( G_1, \ldots, G_S \) imply \( H \) in the standard sense of \( G_1 \land \ldots \land G_S = H \). The opposite direction does not hold.

\[ \text{Proof: Exercise (likely to end up on problem set 2).} \]

So strong implication is indeed stronger than just implication.
Observation 3

A DNF resolution is strongly sound.

Proof: Inspect the rules and do a (simple) case analysis.

---

Detour: Hardness of PTP and random k-CNFs

Important part of proof complexity study different families of formulas understand their hardness in different proof systems.

Pigeonhole principle PTP is extremely well-studied (but still many interesting open problems).

What happens when we vary not only \( n \to \infty \) but also \( m = m(n) \)?

\[
\begin{align*}
\text{m} &\leq \text{n} & \text{ satisfiable, not so interesting} \\
\text{m} &= \text{n} + 1 & \text{exponentially hard for resolution} \ [\text{Haken '85}] \\
\text{m} &= cn, \quad c \geq 1 & \text{exponentially hard for resolution} \ [\text{Krajíček, Pudlák, Woods '95}] \\
\text{m} &= cn, \quad c \geq 2 & \text{exponentially hard for resolution} \ [\text{Segerind, Hruschka, Impagliazzo '07}]
\end{align*}
\]

Also for bounded-depth Frege

\[
\begin{align*}
\text{m} &= n^c, \quad c \geq 1 & \text{exponentially hard for resolution} \ [\text{Haken '85}] \\
\text{m} &= 2n & \text{exponentially hard for } R(d)
\end{align*}
\]

Haken's proof still works for resolution

Proof crashes for stronger proof systems

\[
\begin{align*}
\text{m} &= cn, \quad c \geq 2 & \text{exponentially hard for resolution} \ [\text{Segerind, Hruschka, Impagliazzo '07}]
\end{align*}
\]
But for $\mathbb{F}_2\{\text{polylog}(n)\}$

DNFs with slowly growing terms
$\text{polylog}(n) = \log^k(n)$ for some $k \geq 1$

$\text{PHP}_{n^m}$ is not too hard

Exist refutations in quasipolynomial size
$\exp(\text{polylog}(n)) = n^{\log^k(n)}$ for some $k \geq 1$

Superpolynomial, but not by too much.

$m = n^2$

"Weak pigeonhole principle"

Itken's proof breaks down

But actually even for arbitrarily many
pigeons $m$ it holds that resolution
refutations require length
$\exp(\Omega(n^d))$ for some $d > 0$

[Raz '01]

In fact true for all flavors of
resolution, even with functionality
and/or onto axioms
[Raz Goos '03, '04] (There are
depth papers.)

How hard are random $k$-CNF formulas?

Hard for resolution [Chvátal-Szemerédi '88]
$d^2$-CNFs hard for $\mathbb{F}_2\{d\}$ [CB1 '04]
$3$-CNFs hard for $\mathbb{F}_2\{d\}$ [Alekhnovich '11]

Bounded-depth Frege? Big open problem.
A key tool for the lower bounds that we will prove in future lectures are random restrictions. Let us recall what a restriction is.

**Restrictions**

Partial assignment $f$ to variables in a formula $g: Vars(F) \to \{0, 1, *\}$

$f(x) = *$ means that $f$ does not assign $x$.

When representing $g$, can omit *-assignments.

Can hit formula with restrictions and simplify "in obvious ways".

For terms: $0 \land t = 0$, $1 \land t = t$

For clauses: $0 \lor C = C$, $1 \lor C = 1$

For formulas of higher depth, simplify layer by layer.

**Example**

$G = (x_1 \land y_1 \land z) \lor (\overline{x_1} \land \overline{z} \land w)$

$s_1 = \{x \rightarrow 1\}$, $G/s_1 = y \land z$

$s_2 = \{x \rightarrow 1, z \rightarrow 0\}$, $G/s_2 = 1$ (contradictory)

$s_3 = \{x \rightarrow 1, y \rightarrow 1, z \rightarrow 1\}$, $G/s_3 = 1$ (truthful)

Sometimes also think of $s$ as literals set to true, so

$s_2 = \{x, \overline{z}\}$, $s_3 = \{x, y, \overline{z}\}$ can be convenient for notation.
General fact (true, with small twists, for all proof systems we will study).

For \( \pi = (G_1, G_2, \ldots, G_n) \) define

\[ \pi \beta = (G_1 \beta, G_2 \beta, \ldots, G_n \beta) \]

Then if \( \pi \) is a refutation of \( F \), it holds that \( \pi \beta \) is a refutation of \( F \beta \).

(Might also end up as an exercise for problem set 2 for cutting planes and/or d-DNF resolution).

Random restrictions & sampling from suitable distributions \( D \) can be a powerful tool to prove lower bounds. Let us see an example for simplicity using resolution.

Take formulas \( \text{PHP}_{n}^{n+1} \) again.

Prove, firstly, that for any resolution refutation \( \tilde{\pi} : \text{PHP}_{n}^{n+1} \vdash \bot \), there has to be some clause which mentions a lot about \( \frac{n}{2} \) pigeons in the following way.

For every \( i \in I \), \( |I| = \frac{n}{2} \), one of two cases hold:

1. \( \exists \beta \text{ literal \overline{x}_{ij} in C} \)
2. \( \exists n/2 \text{ positive literals } x_{ij_1}, \ldots, x_{ij_{n/2}} \) for different \( j_1, \ldots, j_{n/2} \).
Secondly take a random matching of \( n/2 \) pigeons to \( n/2 \) and define the restriction \( \tilde{\mathcal{F}}_n \) by

\[
\tilde{g}(x_{i,j}) = \begin{cases} 
1 & \text{if } \left( \tilde{i}, \tilde{j} \right) \in \mathcal{E}L, \\
0 & \text{if } \left( \tilde{i}, \tilde{j}' \right) \in \mathcal{E}L \text{ for } j' \neq j, \\
* & \text{otherwise}. 
\end{cases}
\]

Prove that for any clause \( C \) that for \( |I'| \geq n/4 \) pigeons \( i \in I' \) contains

1. \( \overline{x}_{i,j} \), or
2. \( x_{i,j}, x_{i,j'}, v x_{i,j''} v' v x_{j,n/4} \)

it holds that \( \Pr[\tilde{C} \in \tilde{\mathcal{F}}_n] \leq p \)

(think of \( p = 2^{-\alpha n}, \alpha > 0 \)).

Now set \( \Delta = 1/p \) and suppose

\( \Pi: \tilde{P}^{\alpha n} \tilde{P}_{n/2} \tilde{P} \) has length \( \leq \Delta \)

We have that

\[ \Pi \tilde{g}_{\tilde{\mathcal{F}}_n} \quad \text{for any } \tilde{\mathcal{F}}_n \]

is in fact a resolution refutation of

\( \tilde{P}^{\alpha n/2} \tilde{P}_{n/2} \) (after renaming of variables)

What is the probability (over \( \tilde{\mathcal{F}}_n \)) that \( \Pi \tilde{g}_{\tilde{\mathcal{F}}_n} \) contains some fat clause?
Two cases
1. $C$ not fat $\Rightarrow$ clearly $C \upharpoonright \beta_n$ is fat with probability 0 (for any restriction, actually)
2. $C$ is fat $\Rightarrow$ then we have proven $Pr[C \upharpoonright \beta_n + 1] < p = 1/2$ (and satisfied clauses are just removed from the restricted refutation).

$$Pr[\exists \pi \beta_n \text{ contains fat clause}] \leq$$

$$\leq Pr[\exists C \in \pi \text{ s.t. } C \text{ fat and } C \upharpoonright \beta_n + 1] \leq$$

$$\leq \sum_{C \in \pi} Pr[C \text{ fat and } C \upharpoonright \beta_n + 1] <$$

$$< \sum_{C \in \pi} 1/2 \leq 2^0 1/2 = 1$$

So $Pr[\exists \pi \beta_n \text{ contains fat clause}] < 1$

This means $\exists g^* \in \mathbb{O}$ s.t. $\pi \upharpoonright g^*$ has no fat clauses (otherwise we would have probability = 1)

But $\pi \upharpoonright g^*$ is a refutation of PHP$^{\omega_1}_{n/2}$, and we started by arguing that any such refutation has fat clause. Contradiction! Hence no refutation in length $\leq x = 1/p = 2^{5n}$ can exist!
Sounds familiar?

This is actually the Prosecutor-Defendant lower bound we did in Lecture 2, only described in a slightly different way (and with slightly different names).

How to prove $R(d)$ lower bounds for PHP?

Terms are only of size $d$. Random restriction likely to either

(a) satisfy a term (and that whole literal remains)
(b) falsify the term (removing it from the formula)
(c) leave just one literal which will give
use a clause.

So if we are lucky:

Take $R(d)$ refutation $\Pi$ of PHP
Hit with random restriction
Argue that we only have clauses left, so this is a resolution refutation.
Use resolution lower bound!

Bad news! Won't work.

But something in a somewhat similar spirit will.

Take short $R(d)$ refutation & hit with random restriction.

Terms refutation into sequence of small decision cores.
Can be transformed to resolution refutation with clauses
of small width. But such refutations cannot exist.
DECISION TREE for function \( f: \{0,1\}^n \rightarrow \{0,1\} \)

Binary tree.
Internal nodes labelled by variables \( x, y, z \).
Outgoing edges labelled 0 & 1.
Leaves labelled 0/1.
Every total assignment \( \alpha \) defines path to leaf \( \nu_\alpha \)
\( T \) represents \( f \) if \( f(\alpha) = \text{label}(\nu_\alpha) \).
\( T \) represents d-DNF \( H \) if \( T \) represents the function computed by \( H \).
Path from root to leaf \( \nu \) defines partial assignment \( \beta \).
For \( b \in \{0,1\} \), let \( \beta \uplus_b (T) = \{ \text{partial assignments to leaves labelled } b \} \).

\( T/\beta \) is the decision tree obtained by:
(a) deleting edges conflicting with \( \beta \) (and subtrees below these edges).
(b) contracting edges agreeing with \( \beta \).

\( T \) strongly represents d-DNF formula \( H \)
if for every \( \phi \in \beta_0 (T) \) and for all \( t \in H \), it holds that \( t/\beta = 0 \); and for every \( \phi \in \beta_1 (T) \) and every there exists a \( t \in H \) such that \( t/\beta = 1 \).

The representation height \( h(H) \) of a DNF formula \( H \)
is the minimum height of a decision tree strongly representing \( H \).
Ex  \[ H = (x \land y) \lor (y \land z) \]

\[ T_1 \]

\[
\begin{array}{c}
0 \\
1 \\
0 \\
0 \\
1 \\
0 \\
1 \\
1 \\
1 \\
0 \\
0 \\
1 \\
1 \\
0 \\
1 \\
\end{array}
\]

\[ T_1 \] represents \( H \), but does not represent \( H \) strongly, because

\[ H \land \text{xor, y or z} = z \lor \bar{z} \]

\[ T_2 \]

\[
\begin{array}{c}
0 \\
1 \\
0 \\
0 \\
1 \\
1 \\
1 \\
1 \\
0 \\
1 \\
0 \\
0 \\
1 \\
1 \\
\end{array}
\]

\[ T_2 \] represents \( H \) strongly
**Observation**

If \( f : \{0, 13\}^n \rightarrow \{0, 1\} \) can be computed by a decision tree of height \( h \), then \( f \) can be computed both by a \( k \)-CNF formula and a \( h \)-DNF formula.

**Proof sketch** The CNF formula \( F \) can be chosen as \( \bigwedge_{g \in \mathcal{G}_1} \bigvee_{a \in \mathcal{A}} \) and the DNF formula \( H \) as \( \bigvee_{g \in \mathcal{G}_2} \bigwedge_{a \in \mathcal{A}} \)

(if we think of \( \mathcal{G} = \{ \text{set of wreath set to true by } g \} \))

How likely a \( d \)-DNF formula \( \mathcal{G} \) to be satisfied by a random restriction can be estimated by how many variables in different terms in \( \mathcal{H} \) intersect. This is captured by the concept of **covering number**

**Definition** Let \( \mathcal{H} \) be a DNF formula and \( \mathcal{S} \) be a set of variables. We say that \( \mathcal{S} \) is a cover of \( \mathcal{H} \) if every term in \( \mathcal{H} \) contains a variable from \( \mathcal{S} \). The covering number of \( \mathcal{H} \), denoted \( \text{cov}(\mathcal{H}) \), is the minimum cardinality of a cover of \( \mathcal{H} \).

**Example** For a clause \( C = a_1 \lor \ldots \lor a_w \), the covering number is \( w \). The formula \( H = (x \land y \land z) \lor (\neg x) \lor (y \lor w) \) has \( \text{cov}(H) = 2 \).
THEOREM (Swiching lemma for d-DNF formulas)

Let \( d, s, t \in \mathbb{N}^+ \), \( \varepsilon, \delta \in (0, 1) \), and let \( D \) be a distribution on partial assignments such that for every d-DNF formula \( G \), it holds that

\[
\Pr_{p \sim D} \left[ G \ supp p \neq 1 \right] \leq t \cdot 2^{-\delta (\text{cov}(G)) \varepsilon}.
\]

Then for every d-DNF formula \( H \)

it holds that

\[
\Pr_{p \sim D} \left[ h(H/\varepsilon) > 2s \right] \leq dt \cdot 2^{-\delta' \varepsilon t}.
\]

where \( \delta' = 2(\delta/4)^d \) and \( \varepsilon' = \varepsilon / d \).

Compare

For PHP and resolution, our random restriction satisfies ("kills") a clause of width \( w \) except with probability \( 2^{-\sqrt{w}} \).

Since resolution is partial matching, never falsifies formula.

For d-DNF resolution, want to find random restrictions that

(a) don't falsify the formula \( F \) being refuted

(b) kill d-DNF formula \( H \) with probability roughly

\[
2 - (\text{cov}(H)) \delta
\]

for some \( \delta > 0 \).
THEOREM  Let $F$ be a $k$-CNF formula. If $F$ has a $d$-DNF resolution refutation of size $t$ such that for every line $H \in \pi$ it holds that $k(H) \leq k$, then there is a resolution refutation $\pi'$ of $F$ in width $W(\pi') \leq 2^d t$.

Given these two theorems, we can prove lower bounds for $d$-DNF resolution in the following way.

1. Find a good distribution $\mathcal{D}$ of random restrictions that satisfy the assumption of the switching lemma.

2. Argue that for short refutations of $F$, we get shallow decision trees for $F|_{\mathcal{D}}$ for some $\mathcal{D}$ (by a union bound argument).

3. Prove that $F|_{\mathcal{D}}$ requires too large width in resolution for the decision-tree-to-resolution-refutation conversion to work.

Hence, there could be no short $d$-DNF resolution refutation of $F$.

Next lecture we will prove these two theorems. (Switching lemma and translation from decision trees to resolution refutations)