Today (and part of next week)

① Frege Proofs – 2 views

- Prover/Liar view
- Axiomatic view (PK – propositional Sequent Calculus)

② Bounded arithmetic + connections to Frege Proofs

- S_2^1 and Extended Frege
- $S_2(f)$ and AC_0-Frege

Prover-Liar game for UNSAT F

Let $F = C_1 \wedge C_2 \wedge \ldots \wedge C_m$ unsat over $x_1 .. x_n$

Liar claims to have a satisfying assignment for F

Prover wants to force Liar into a simple contradiction by asking questions

First set of Questions (For free):

Is C_1 true ? ⟵ Yes (says Liar)

Is C_2 true ? ⟵ yes "

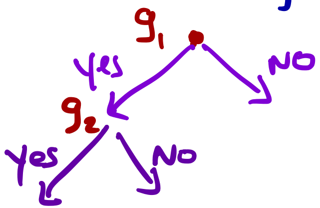
⋮

Is C_m true ? ⟵ yes "

Then Prover can ask an arbitrary q's over $x_1 ... x_n$

Is g_1 true ?

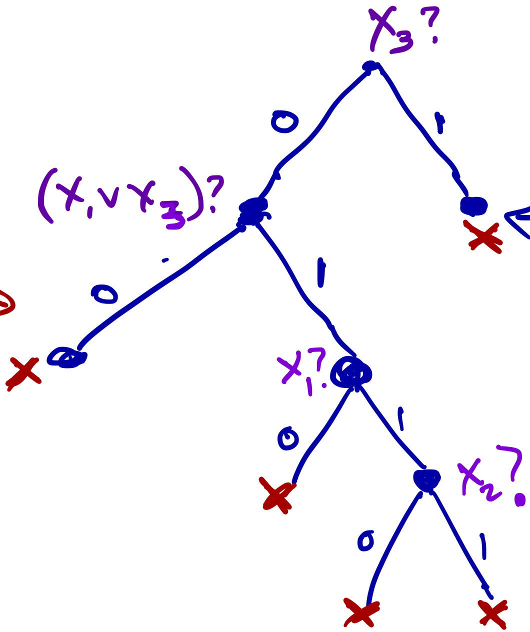
Is g_2 true ?



Prover wants to force Liar into a contradiction regardless of how Liar answers the q's

(Simple) Example of a Liar/Prover Proof.

$$(x_2)(\bar{x}_1 \vee \bar{x}_2)(x_1 \vee x_3)(\bar{x}_3)$$



caught you.
$(x_1 \vee x_3)=0$
but $x_3=1$
violates tt
defn of OR

$x_3=1$

$x_3=0$ ← C_4

Caught you! Since C_4 is true & now you say $x_3=0$ and $x_3=1$

At leaves are truth table contradictions — which violate a truth table for AND, OR or NEG

$\vee, \neg$

		$\vee$
0	0	0
0	1	1
1	0	1
1	1	1

$\neg$	
0	1
1	0

$A, B, A \vee B$

$A=0 \quad B=0 \quad A \vee B = 1$

A	$\neg A$
0	0
1	1

Less Trivial Example – PHP^{n+1}_{n} (onto, 1-1 version)

Prover asks $\text{Count}(\{P_{ij} : i \le n+1, j \le n\}, n+1)$?

Count$(\vec{v}, a)$: Formula that returns true iff # 1's in $\vec{v}$ is equal to a

If Liar says no, then use Pigeon axioms to (asserting $\forall i \, \text{count}(\{P_{ij} : j \le n\}, 1) = 1$) force a contradiction

If Liar says yes, ask $\text{Count}(\{P_{ij} : i \le n+1, j \le n\}, n)$?

If yes force contradiction since Liar has said $\text{count}(\{P_{ij}\}, n) = 1$ and $\text{Count}(\{P_{ij}\}, n+1) = 1$

If NO use Hole axioms (asserting $\forall j \, \text{count}(\{P_{ij} : i \le n+1\}, 1) = 1$) to force a contradiction

Axiomatic View of Frege

One particularly nice Frege system is the sequent calculus (PK)

Lines in a PK proof are <u>sequents</u>

$$\underbrace{A_1, \dots, A_k}_{\Gamma} \to \underbrace{B_1, \dots, B_m}_{\Delta}$$

Intended meaning:

$$A_1 \wedge A_2 \wedge \dots \wedge A_k \to B_1 \vee B_2 \vee \dots \vee B_m$$

PK rules

Axiom: $A \to A$

Logical Rules:

$$\frac{\Gamma \to \Delta, A}{\neg A, \Gamma \to \Delta} \qquad \frac{A, \Gamma \to \Delta}{\Gamma \to \Delta, \neg A} \qquad \neg \text{ rules}$$

$$\frac{A, B, \Gamma \to \Delta}{A \wedge B, \Gamma \to \Delta} \qquad \frac{\Gamma \to \Delta, A \qquad \Gamma \to \Delta, B}{\Gamma \to \Delta, A \wedge B} \qquad \wedge \text{ rules}$$

$$\frac{\Gamma \to \Delta, A, B}{\Gamma \to \Delta, A \vee B} \qquad \frac{\Gamma, A \to \Delta \qquad \Gamma, B \to \Delta}{\Gamma, A \vee B \to \Delta} \qquad \vee \text{ rules}$$

Nonlogical rules

$$\frac{\Gamma \to \Delta}{A, \Gamma \to \Delta} \qquad \frac{\Gamma \to \Delta}{\Gamma \to \Delta, A} \qquad \text{weakening}$$

$$\frac{\Gamma, A, B \to \Delta}{\Gamma, B, A \to \Delta} \qquad \frac{\Gamma \to A, B, \Delta}{\Gamma \to B, A, \Delta} \qquad \text{exchange}$$

$$\frac{A, A, \Gamma \to \Delta}{A, \Gamma \to \Delta} \qquad \frac{\Gamma \to \Delta, A, A}{\Gamma \to \Delta, A} \qquad \text{contraction}$$

Cut Rule

$$\frac{A, \Gamma \to \Delta \qquad \Gamma \to A, \Delta}{\Gamma \to \Delta}$$

A PK proof of a formula A is a sequence of sequents, where final one is $\rightarrow A$ and each follows from previous by a valid rule/axiom

A PK refutation of an unsat formula B is a PK proof of $B \rightarrow$

The size of a refutation/proof is sum of sizes of all formulas in pf

---

Cook-Reckhow Frege system is robust
(Nearly all sound/complete axiomatizations are poly-equivalent)

Restrictions / Circuit Classes

AC^0_d-Frege: Frege (PK) pf where all formulas have depth (# of alternations of connectives) $\leq d$

Dag vs tree Like

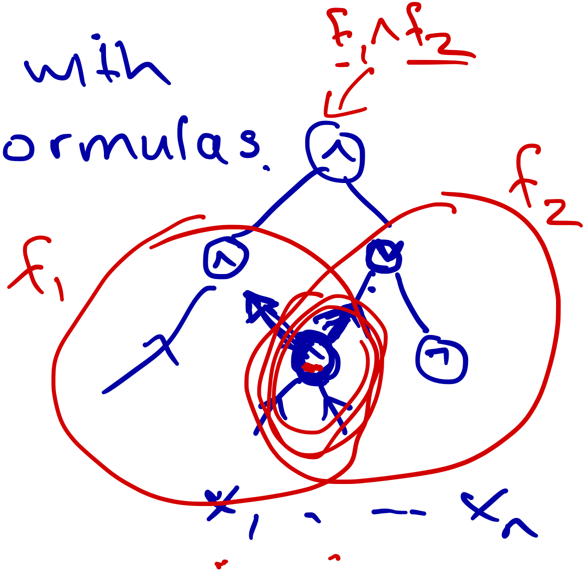
Proof structure tree like if each derived formula used only once; otherwise dag-like

Thm Dag $\overset{\text{poly}}{\approx}$ tree-like

AC^0_{d+1} tree-like Frege $\approx AC^0_d$ dag-like

Extended Frege

Is a way to reason with circuits instead of formulas.



Add new axioms to sequent calculus

$p \leftrightarrow f(x_1 \dots x_n)$

formula

new variable

$(\neg p \vee f) \wedge (\neg f \vee p)$

$q \leftrightarrow f'(p, x_1 \dots x_n)$

$r \leftrightarrow f''(\quad)$

Bounded Arithmetic

Lets us reason about polytime concepts (or concepts in some bounded complexity class).

Language:

$\leq, \geq, =, \underbrace{+, \cdot,}$ $\lfloor \frac{1}{2}x \rfloor$, $|x|$, $\#$, S

length

$\cancel{x}$ $\qquad \underbrace{x \cdot x \cdot x \cdot \ldots}$ $\qquad \cancel{x^c}$ $\qquad |x|^c$

$|x| = \log x \qquad c \log x = |x^c|$

$\cancel{2^x}$

$x \# y = 2^{|x| \cdot |y|} \qquad \underbrace{x \# x \# x \# \cdots \# x}_{c} = 2^{c \cdot |x|}$

Bounded Quantifiers

n

$\forall x \le t$

$\exists x \le t$

Sharply Bded Quantifiers

Σ^b_0: only sharply bded quantifiers

$\forall x \le |t|$

$\exists x \le |t|$

Hierarchy of formulas

Σ^b_k = at most k alternations of bounded quantifiers

Σ: outermost $\exists x \le t$

Π^b_k ← outermost $\forall x \le t$

Induction

1. Σ^b_k - IND

$$A(0) \wedge \forall x\,(A(x) \to A(x+1)) \to \forall x\, A(x)$$

$A \in \Sigma^b_k$

2. Σ^b_k - PIND (faster induction)

$$A(0) \wedge \forall x\,(A(\lfloor \tfrac{1}{2}x \rfloor) \to A(x)) \Rightarrow \forall x\, A(x)$$

0

$\forall x \exists y\, A(x,y)$

00111011

16

$f(x)=y \Leftrightarrow A(x,y)$

S_2^1: Theory with above language plus "Basic Axioms"

$(+, \cdot, s, \#, \leq, =)$

$x+y = y+x$

plus Σ_1^b-PIND

T_2^1: same but with Σ_1^b-IND

S_2^i: same as S_2^1 but with Σ_i^b PIND

T_2^i: " T_2^1 " Σ_i^b IND

Provably Total Functions

A function $f: \mathbb{N}^k \to \mathbb{N}$ is Σ_i^b-definable in R if there is a Σ_i^b-formula $A(\vec{x}, y)$ such that

1. $\forall \vec{n}\ A(\vec{n}, f(\vec{n}))$ is true
2. $R \vdash \forall \vec{x} \exists y\ A(\vec{x}, y)$
3. $R \vdash \forall \vec{x}, y, z$
$$A(\vec{x}, y) \wedge A(\vec{x}, z) \Rightarrow y = z$$

R a theory
ie $R = S_2^1$

Theorem (Buss, Cook) ← PV

The Σ^b_1-definable functions of S^1_2 are precisely the functions in FP

The Σ^b_i-def functions of S^i_2 are precisely the functions in $FP^{\Sigma^?_{i-1}}$

To Do:

- We can formalize S_2^i nicely in sequent calculus

- We want to see translation between proofs in bdded arith. & prop. pf systems

2 of them

unrelativized 1. $\forall\Sigma_1^b$ in S_2^1 $\Longrightarrow$ polysized family of extended Frege pfs

relativized 2. $\underbrace{S_2^i(\alpha)}_{\forall\Sigma_i^b}$ $\Longrightarrow$ family of AC_0 Frege pfs of quasipoly size

Formulating Bounded Arithmetic in Sequent Calc.

① Add rules for $\forall, \exists$:

$$\frac{A(b), \Gamma \to \Delta}{\exists x A(x), \Gamma \to \Delta} \qquad \frac{\Gamma \to \Delta, A(t)}{\Gamma \to \Delta, \exists x A(x)} \qquad \exists$$

$$\frac{A(t), \Gamma \to \Delta}{\forall x A(x), \Gamma \to \Delta} \qquad \frac{\Gamma \to \Delta, A(b)}{\Gamma \to \Delta, \forall x A(x)} \qquad \forall$$

② Add rules for bded $\forall, \exists$:

$$\frac{b \le s, A(b), \Gamma \to \Delta}{\exists x \le s, A(x), \Gamma \to \Delta} \qquad \frac{\Gamma \to \Delta, A(t)}{t \le s, \Gamma \to \Delta, \exists x \le s A(x)} \qquad \le\exists$$

$$\frac{A(t), \Gamma \to \Delta}{t \le s, \forall x \le s A(x), \Gamma \to \Delta} \qquad \frac{b \le s, \Gamma \to \Delta, A(b)}{\Gamma \to \Delta, \forall x \le s A(x)}$$

b free, not in lower sequent

③ Add Basic Axioms

④ Induction Axiom (PIND)

$$\frac{A(\lfloor \tfrac{1}{2}b \rfloor), \Gamma \to \Delta, A(b)}{A(0), \Gamma \to \Delta, A(t)}$$

Translations

① S^1_2 and EF (for $A \in \Sigma^b_1$ where $S^1_2 \vdash \forall x\, A(x)$)

② $S^i_2(f)$ and AC^0 Frege

We'll discuss ② with an example

$S^i_2(f)$: Σ^b_i PIND

f function symbol

Briefly:

$f(i)=j$ converts to P_{ij}

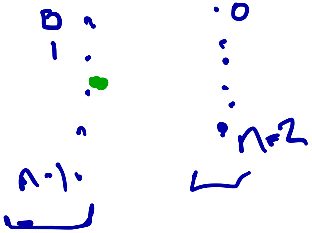
$\forall x \le t \; A(x)$ convert to a big $\bigwedge [A(x)]^{PW}$

$\exists x \le t \; A(x)$ " " $\bigvee [\;]^{PW}$

$PHP(f, n): \forall x < n \; \exists y < n-1 \;\; f(x) = y$

free var

$\Longrightarrow \exists x_1 \exists x_2 < n \; \exists y < n-1 \; [f(x_1) = y \wedge f(x_2) = y]$



$$PHP(f,n): \forall x<n \; \exists y<n-1 \; f(x)=y \implies$$
$$\exists x_1 \exists x_2 < n \; \exists y < n-1 \; [x_1 \neq x_2 \wedge f(x_1)=y \wedge f(x_2)=y]$$

$$\Downarrow$$

$$\bigwedge_{i=0,\dots,n-1} \; \bigvee_{j=0..n-2} P_{ij} \implies$$

$$\bigvee_{\substack{i_1,i_2 \in [n-1] \\ i_1 \neq i_2}} \; \bigvee_{j \in [n-1]} P_{i_1 j} \wedge P_{i_2 j}$$

$$\{pPHP(n) \mid n \in \mathbb{N}\}$$

Briefly If $\forall n\, PHP(f,n)$ has an $S_2^i(f)$ proof, then $\{pPHP(n) \mid n \in \mathbb{N}\}$ has quasi-poly sized depth i Frege proofs

---

1. Start with $S_2^i(f)$ proof P of $\forall n PHP(f,n)$
   use cut-elimination thm to assume wlog that P has no* cuts so all formulas in P are $\underbrace{\Sigma_i^b(f)}$

2. fix n Translate P to prop version by translating each line

~~FAA~~

* except for cuts on induction f's

3. Prove by induction that each line in translated P follows from 2 prev lines by a valid (set) of Sequent Calc rules

Main step: Induction

Unwind induction using cut-rule

Note: could have PIND or IND