Course "Propositional Proof Complexity", JASS'09

Frege Systems

Michael Herrmann

Department of Computer Science
TU Munich

May 10, 2009

Table Of Contents

Motivation

Question: Why even dealing with proof systems?

We differ between two kinds of proofs.

- Social proofs. Proofs consisting of social conventions with that scientists reciprocal convince each other of the truth of theorems. This is done in natural language and with some symbols and figures.
- Formal proofs. A proof is a string, which satisfies some precisely stated set of rules.

Of course our motivation in studying formal proof systems is to develop a formal proof system.

But there is a greater impact on proof systems to complexity theory.

Repetition NP and coNP

$\mathcal{P}$ is the set of decision problems, which can be solved by a deterministic Turing machine in polynomial time.

$\mathcal{NP}$ is the set of decision problems, for which the answer *yes* has simple proofs if the answer is indeed yes.

$co\mathcal{NP}$ a element $\mathcal{X}$ is in $co\mathcal{NP}$ if and only if the element $\bar{\mathcal{X}}$ is in $\mathcal{NP}$.

A important question is, whether $\mathcal{NP}$ is closed under complementation, i.e. $\Sigma^* - L$ is in $\mathcal{NP}$ whenever L is in $\mathcal{NP}$.

Proposition 1

$\mathcal{NP}$ is closed under complementation if and only if TAUT is in $\mathcal{NP}$.

Definition 2

$\mathcal{F}$ is a set of functions $f : \Sigma_1^* \to \Sigma_2^*$, with Σ_1, Σ_2 are any finite alphabets, such that f can be computed by a deterministic Turing machine in time bounded by a polynomial in the length of the input.

For the proof we need the following result: There is a function $f \in \mathcal{F}$ with that every set L is reducible to the complement of the tautologies.

Proof.

Assume $\mathcal{NP}$ is closed under complementation. To verify that a formula is not a tautology one can guess a truth assignment and verify that it falsifies the formula. Because we assumed, that $\mathcal{NP}$ is closed under complementation, the set of tautologies is also in $\mathcal{NP}$.

Assume that the set of tautologies is in $\mathcal{NP}$. So a non deterministic procedure for accepting the complement of L would be : On input x, compute $f(x)$ (the result of above) and accept if x is a tautology. Hence the complement of L is in $\mathcal{NP}$. $\square$

Definition 3

Let $L \subseteq \Sigma^*$, a *proof system* for L is a function $f : \Sigma_1^* \to L$ for some alphabet Σ_1 and $f \in \mathcal{F}$ such that f is onto.

Definition 4

A proof system is *polynomially bounded* if and only if there is a polynomial $p(n)$ such that for all $y \in L$ there is $x \in \Sigma_1^*$ such that $y = f(x)$ and $|x| \leq p(|y|)$.

Proposition 5

A set L is in $\mathcal{NP}$ if and only if $L = \emptyset$ or L has a polynomially bounded proof system.

Proof.

Assume $L \in \mathcal{NP}$. That means. there is a non deterministic Turing Machine M, that accepts L in polynomial time. If $L \neq \emptyset$, the proof system calculates for the case that M accepts y, $f(x) = y$. Where x is the calculation on an output tape of M on input y. Otherwise it sets $f(x) = y_0$, for a fixed y_0.

Let f be a polynomially bounded proof system for L. On input y guess an proof for x and accept if $f(x) = y$. □

Putting things together

Proposition 1 says that $\mathcal{NP}$ is closed under complementation iff TAUT $\in \mathcal{NP}$ and Proposition 5 says that any Language $L \in \mathcal{NP}$ iff L has an polynomially bounded proof system.
That leads directly to:

Proposition 6

$\mathcal{NP}$ is closed under complementation if and only if TAUT has a polynomially bounded proof system.

With that we are able to get a further result. But we need at first the definition of *p-simulation*.

Definition 7

If $f_1 : \Sigma_1^* \rightarrow L$ and $f_2 : \Sigma_2^* \rightarrow L$ are proof systems for L, then f_2 p-simulates f_1 if there is a function $g_1 : \Sigma_1^* \rightarrow \Sigma_2^*$ such that g is in $\mathcal{F}$ and $f_2(g(x)) = f_1(x)$ for all x.

Proposition 8

If a proof system f_2 for L p-simulates a polynomially bounded proof system f_1, then is f_2 also polynomially bounded.

Proof.

Since p-simulation means that there is a $g \in \mathcal{F}$, and polynomially bounded means that $|x| \leq p(|y|)$ the equation $|g(x)| \leq p(|f(g(x))|)$ still holds. $\square$

Frege Systems

Definition 9

A *Frege System* is a three tuple $(\mathcal{L}, \mathcal{A}, \mathcal{R})$. Where

- $\mathcal{L}$ is the propositional language.
- $\mathcal{A}$ is a finite set of axioms.
- $\mathcal{R}$ is a finite set of rules.

The language $\mathcal{L}$ is identified by the connectives that are allowed. We mark the set of connectives with κ. For example the "standard basis" is $\{\neg, \wedge, \vee\}$.
We say a Frege System is *propositionally complete* if every formula ϕ over the "standard basis" has an equivalent formula ϕ' over $\mathcal{L}$.

A rule is a system of formulas $(C_1, C_2, ..., C_n)/D$, where $(C_1, C_2, ..., C_n) \models D$.

If $n = 0$ the rule is an axiom.

Example 10

An example for an Frege System:

- **Language** with the connectives $\kappa = \{\neg, \wedge, \vee, \rightarrow\}$
- **Rule of inference** $$\frac{P \qquad (P \rightarrow Q)}{Q}\,\mathrm{MP}$$

Axioms See next slide.

Axioms:

$$(P \wedge Q) \rightarrow P$$
$$(P \wedge Q) \rightarrow Q$$
$$P \rightarrow (P \vee Q)$$
$$Q \rightarrow (P \vee Q)$$
$$(P \rightarrow Q) \rightarrow ((P \rightarrow \neg Q) \rightarrow \neg P)$$
$$(\neg\neg P) \rightarrow P$$
$$P \rightarrow (Q \rightarrow P \wedge Q)$$
$$(P \rightarrow R) \rightarrow ((Q \rightarrow R) \rightarrow (P \vee Q \rightarrow R))$$
$$P \rightarrow (Q \rightarrow P)$$
$$(P \rightarrow Q) \rightarrow (P \rightarrow (Q \rightarrow R)) \rightarrow (P \rightarrow R)$$

Further conditions of Frege systems

- **Soundness:** A Frege system is sound if every theorem is valid.
- **Completeness:** A Frege system is complete if every valid formula has a proof.
- **Implicational Soundness:** Whenever $\phi \vdash \psi$ then $\phi \models \psi$.
- **Implicational Completeness:** Whenever $\phi \models \psi$ then $\phi \vdash \psi$.

There exist many sound and complete Frege proof systems.

Some definitions

- **atoms** Propositional variables.
- **derivation** π Finite set of lines and ends with the line which is proved.
- **hypothesis** A derivation of 0 or more lines.

Every row in a proof must be either a hypothesis or derivable by a rule.

Frege proof

A Frege proof Π in a Frege system $\mathcal{F} = (\mathcal{L}, \mathcal{A}, \mathcal{R})$ is a sequence $A = (A_1, A_2, ..., A_m)$ such that for all i, either:

- A_i is an instance of an axiom.
- It exists $j_1, ..., j_k$ with $k < i$ and with a k-ary rule $R \in \mathcal{R}$ such that $A_i = R(A_{j_1}, ..., A_{j_k})$.

Then Π is a proof of the theorem A_m. We may write then $\vdash A_m$. Or $\mathcal{F} \vdash A_m$, respectively $\vdash_{\mathcal{F}} A_m$, to state that A_m has a proof in the Frege system $\mathcal{F}$.

Complexity of proofs

The complexity of a Frege proof is the symbol length of the proof:
$n = |\Pi| = \sum_{i=1}^{m} |A_i|$

Open Problem: Do the tautologies have polynomial-size Frege proofs?
(Is there a polynomial p that for all $A \in \mathrm{TAUT}$, there exists a proof with length at most $p(|A|)$?)

If so, then NP $=$ coNP.

Before we introduce the next theorem we need some terminology.

- $A_1, ..., A_n \vdash^{\pi}_{\mathcal{F}} B$ means that there is the derivation π in the system $\mathcal{F}$ from $A_1, ..., A_n$ to B.
- $A_1, ..., A_n \vdash_{\mathcal{F}} B$ means that there is some derivation in the system $\mathcal{F}$ from $A_1, ..., A_n$ to B.
- $l(A)$ is the number of atoms (variables) in the formula or sequence A.
- $\lambda(\pi)$ is the number of lines in the derivation.
- $\rho(\pi) = \max_i l(A_i)$, if π is $A_1, ..., A_n$.
- $|\pi|$ or $|A|$ is the length as string.

A substitution is $\sigma = (D_1, ..., D_k)/(P_1, ..., P_k)$. And σA is the formula, which results in replacing P_i by D_i for $1 \leq i \leq k$.

Theorem 11

For any two Frege systems $\mathcal{F}_1$ and $\mathcal{F}_2$ over κ there is a function $f \in \mathcal{F}$ and constant c such that for all formulas $A_1, ..., A_n, B$ and derivations π, if $(A_1, A_2, ..., A_n) \vdash^{\pi}_{\mathcal{F}_1} B$ then $(A_1, A_2, ..., A_n) \vdash^{f(\pi)}_{\mathcal{F}_2} B$, and $\lambda(f(\pi)) \leq c_1 \lambda(\pi)$ and $\rho(f(\lambda)) \leq c_2 \rho(\pi)$.

Lemma 12

Let $A_1, \ldots, A_k$ be some formulas and π is the derivation of B from these formulas, then $\sigma(\pi)$ is a derivation of σA from $\sigma B_1, \ldots, \sigma B_k$ for any substitution σ.

Proof.

By induction over the length of σ. □

Proof of Theorem 11

Let $\mathcal{F}_1$ and $\mathcal{F}_2$ be two complete and implicationally complete Frege systems over κ. Then there is for every rule $R = (C_1, ..., C_m)/D$ in $\mathcal{F}_1$ a derivation π_r of D from $C_1, ..., C_m$ in $\mathcal{F}_2$.

Now let π be a derivation of B from $A_1, A_2, ..., A_n$ in $\mathcal{F}_1$ and suppose $\pi = (B_1, B_2, ..., B_k)$. To construct the $\mathcal{F}_2$-derivation $f(\pi)$ from π do the following: If B_i follows from earlier B_j's by the $\mathcal{F}_1$ rule R_i and substitution σ_i, simply replace B_i by the derivation $\sigma_i(\pi_{R_i})$. According to Lemma 12 $\sigma_i(\pi_{R_i})$ is the derivation of B_i from the same earlier B_j's.

Proof of Theorem 11

The condition $\lambda(f(\pi)) \leq c_1\lambda(\pi)$ holds if c_1 is the number of lines in the longest derivation π_R over all rules R.

The condition $\rho(f(\pi)) \leq c_2\rho(\pi)$ holds too, with c_2 is an upper bound on $l(A)$, with A are all formulas in the derivations π_R.
$\square$

Corollary 13

Any two Frege systems over κ p-simulate each other. Hence one Frege system over κ is polynomially bounded if and only if all Frege systems over κ are.

Proof.

Immediate result of Proposition 8 and Theorem 11. □

Soundness and implicational soundness of Frege systems

Idea:

Noting that all axioms are valid and prove that modus ponens preserves the property of an formula being valid.

Completeness of Frege systems

Theorem 14

The propositional proof system $\mathcal{F}$ is complete and is implicationally complete.

1. *If ϕ is a tautology, then $\vdash \phi$.*
2. *If $\psi \models \phi$, then $\psi \vdash \phi$*

Proof.

(Idea) Part (2) can be reduced to part (1).

Show (1), since the proof is very lengthy we skip here. □

Extended Frege Systems

An extended Frege system $e\mathcal{F}$ is an ordinary Frege system with one additional proof rule.

A extended Frege proof is a sequence of formulas $A_1, A_2, \ldots, A_n$ such that for all i:

- A_i is an instance of an axiom.
- It exists $j_1, \ldots, j_k$ with $k < i$ and with a k-ary rule $R \in \mathcal{R}$ such that $A_i = R(A_{j_1}, \ldots, A_{j_k})$.

Or:

- A_i is an *extension formula* of the form $P_i \equiv \phi$

Where ϕ is any formula and P_i is a fresh extension variable.

We say that P_i is a defined atom and $P_i \equiv \phi$ is it's defining formula.

The idea of the extension rule is, that P_i can be used as an abbreviation for ϕ in all subsequent steps of the proof.

$\Rightarrow$ This can reduce the proof complexity (number of used symbols) greatly.

Soundness of $e\mathcal{F}$

Proposition 15

If π is a derivation of B from $A_1, ..., A_n$ in a extended Frege system $e\mathcal{F}$, then $A_1, ..., A_m \models B$.

Proof.

Let τ be any truth assignment to the atoms of $A_1, ..., A_n$ and B, which satisfies $A_1, ..., A_n$ (normal Frege). Now we extend τ to make each line in the derivation true. In particular, if $P_i \equiv \phi$ is a defining formula, then P has not occurred earlier in the derivation. That means that we are able to extend τ so $\tau(P_i) = \tau(\phi_i)$. Hence $\tau(B)$ is true since B is the last line of derivation. $\square$

Open Problems:

- Can Frege proof systems (p-)simulate $e\mathcal{F}$ systems?
- Can we p-simulate with $e\mathcal{F}$ proof systems every other proof system?

The propositional Pigeonhole Principle PHP

This principle states that, given two natural numbers n and m with $n > m$, if n pigeons are put into m pigeonholes, then at least one pigeonhole must contain more than one item.

A not very surprisingly result is that in a family with three children there must be at least two children with the same gender,

A, in the first moment unexpected result, is that in a city with population over 1 million, there must be at least two inhabitants with the same number of hairs.

There are many more of such examples.

PHP model

Let P_{ij} with $1 \leq i \leq n, 1 \leq j \leq n-1$ be a set of axioms. Whose meaning is that i is mapped to j.

Let $\mathcal{S}_n$ be the set:
$\{P_{i1} \vee ... \vee P_{i,n-1} | 1 \leq i \leq n\} \cup \{\neg P_{ik} \vee \neg P_{jk} | 1 \leq i < j \leq n, 1 \leq k \leq n-1\}$

Example 16

For $n = 3$:
$\{P_{i1} \vee P_{i,n-1} | 1 \leq i \leq n\} = \{(P_{11} \vee P_{12}), (P_{21} \vee P_{22}), (P_{31} \vee P_{32})\}$
$\{\neg P_{ik} \vee \neg P_{jk} | 1 \leq i < j \leq n, 1 \leq k \leq n-1\} =$
$\{(\neg P_{11} \vee \neg P_{21}), (\neg P_{21} \vee \neg P_{31}), (\neg P_{12} \vee \neg P_{22}), (\neg P_{22} \vee \neg P_{32}), \}$

We can this also represent as a function, with following properties:

1. From $\{0, 1, ..., n\} \rightarrow \{0, 1, ..., n-1\}$
2. Injective.

Defining f

Since we proof the pigeon-hole principle by induction we need a inductive definition of f. Let us assume, that $f : \{0, 1, ..., n\} \rightarrow \{0, 1, ..., n-1\}$ is an injective function. Then is f' defined by:

$$f'(i) = \begin{cases} f(i) & f(i) \neq n-1 \\ f(n) & \text{else} \end{cases}$$

f' is also injective.

Frege proof

To do the proof, we try to deduce $\mathcal{S}_{n-1}$ from $\mathcal{S}_n$. For each i, j we introduce a formula B_{ij}, which means $f'(i) = j$ and is defined by $B_{ij} = P_{ij} \vee (P_{i,n-1} \wedge P_{nj})$ with $1 \leq i \leq n-1, 1 \leq j \leq n-2$.

Because f is injective implies f' is also injective we get $\mathcal{S}_n \models \sigma_{n-1}(\mathcal{S}_{n-1})$. Since our Frege system is complete we have $\mathcal{S}_n \vdash \sigma_{n-1}(\mathcal{S}_{n-1})$.

The same holds for $n-1$: $\mathcal{S}_{n-1} \models \sigma_{n-1}(\mathcal{S}_{n-2})$. And so, by Lemma 12, we know, that there is a derivation $\sigma_{n_1}(\mathcal{S}_{n-1}) \models \sigma_{n-1}\sigma_{n-2}(\mathcal{S}_{n-2})$.

Frege proof

Proceeding this way, we finally obtain a derivation showing $\mathcal{S}_n \vdash \sigma_{n_1}...\sigma_2(\mathcal{S}_2)$.

But $\mathcal{S}_2 = \{P_{11}, P_{21}, \neg P_{21} \vee \neg P_{21}\}$. For which we can't find a truth assignment, which makes the formula true.

So we can conclude, that $\vdash \neg\mathcal{S}_n$, and that means $\vdash A_n$. $\square$

Upper bound

There is a Frege system with that the derivation of $\sigma_{n-1}(\mathcal{S}_{n-1})$ from $\mathcal{S}_n$ can be done in $\mathcal{O}(n^3)$. Because we have n derivations we come to an upper bound of $\mathcal{O}(n^4)$.

The problem is, that every application of the substitution triples the length of a formula, so the longest formula in the proof of a_n grows exponentially in n.

Extended Frege proof

We are using the possibility to use abbreviation formulas to reduce the proof length significantly.

For the first step:
We define a atom $\mathcal{Q}_{ij}^1 \equiv (P_{ij} \vee (P_{i,n-1} \wedge P_{n,j}))$ with $1 \leq i \leq n, 1 \leq j \leq n-2$. With that formula and with $\mathcal{S}_n$ the formula $\tau_{n-1}(\mathcal{S}_{n-1})$ can be derived, where τ_{n-1} is the substitution $\mathcal{Q}_{ij}^1/P_{ij}$.

In general we set:
$\mathcal{Q}_{ij}^{k+1} \equiv (\mathcal{Q}_{ij}^{k} \vee (\mathcal{Q}_{i,n-k-1}^{k} \wedge \mathcal{Q}_{n-k,j}^{k}))$.

With that the formulas $\tau_{n-k-1}(\mathcal{S}_{n-k-1})$ can be derived from $\tau_{n-k}(\mathcal{S}_{n-k})$ where τ_{n-k} is the substitution Q_{ij}^{k}/Pij.

With that we get a contradiction in $\mathcal{O}(n^4)$, with every formula has the length only $\mathcal{O}(n)$. That makes a totally upper bound of $\mathcal{O}(n^5)$.

Sequent Calculus

The sequent calculus PK consists of a set of sequence rules for creating new rules from existing ones.

With a rule we can derive from exiting sequences new sequences. A rule R looks in general like:

$$\frac{\text{premise}}{\text{conclusion}}\ \mathrm{R}$$

Furthermore we have axioms, which are rules without a premise.

If we find a derivation so that all all leaf sequences are atoms, then we found a proof for the tautology.

If there is not such a derivation, then we know that the formula is no tautology.

The on the next slide introduced sequent calculus is sound. Proof idea is to observe, that all rules of inference preserve the property of formulas being tautologies.

We are showing now the rules of an sound and complete sequent calculus.

$$\frac{}{\Gamma, \phi \vdash \Delta, \phi} \text{ (Ax)}$$

$$\frac{}{\Gamma \vdash \Delta, 1} \text{ (1-Ax)} \qquad \frac{}{\Gamma, 0 \vdash \Delta} \text{ (0-Ax)}$$

$$\frac{\Gamma \vdash \Delta, \phi}{\Gamma, \neg\phi \vdash \Delta} \text{ (}\neg\text{L)} \qquad \frac{\Gamma, \phi \vdash \Delta}{\Gamma \vdash \Delta, \neg\phi} \text{ (}\neg\text{R)}$$

$$\frac{\Gamma, \phi \vdash \Delta \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \vee \psi \vdash \Delta} \text{ (}\vee\text{L)} \qquad \frac{\Gamma \vdash \Delta, \phi, \psi}{\Gamma \vdash \Delta, \phi \vee \psi} \text{ (}\vee\text{R)}$$

$$\frac{\Gamma, \phi, \psi \vdash \Delta}{\Gamma, \phi \wedge \psi \vdash \Delta} \text{ (}\wedge\text{L)} \qquad \frac{\Gamma \vdash \Delta, \phi \qquad \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \phi \wedge \psi} \text{ (}\wedge\text{R)}$$

Summery

Introduction

- Motivation
- Basics

Proof systems

- Frege systems
- Extended Frege systems

The propositional Pigeonhole Principle

- PHP model for Frege proof
- Frege proof
- Extended Frege proof

Sequent Calculus