The Deduction Theorem, Optimal Proof Systems, and Complete Disjoint NP-Pairs

Olaf Beyersdorff

Institute of Computer Science
Humboldt-University Berlin
Germany

Computability in Europe
2007

Outline

Proof Systems
- Frege systems

Deduction
- Classical Deduction
- Weak Deduction Properties

Applications
- Optimal Systems
- Polynomially Bounded Proof Systems
- Disjoint NP-Pairs

Propositional Proof Systems

Definition (Cook, Reckhow 79)

- A propositional proof system is a polynomial time computable function P with $rng(P) = TAUT$.
- A string π with $P(\pi) = \varphi$ is called a P-proof of φ.
- $P \vdash_{\leq m} \varphi \overset{df}{\iff} \varphi$ has a P-proof of size $\leq m$.

Motivation

Proofs can be easily checked.

Examples

truth-table method, resolution, Frege systems

Frege Systems

Frege systems F use:

- axiom schemes: $\varphi \to \varphi, \quad \varphi \to \varphi \lor \psi, \quad \dots$
- rules: $\dfrac{\varphi \quad \varphi \to \psi}{\psi}$ (modus ponens)

A Frege proof of a formula φ is a sequence

$$(\varphi_1, \dots, \varphi_n = \varphi)$$

of propositional formulas such that for $i = 1, \dots, n$:

- φ_i is a substitution instance of an axiom, or
- φ_i was derived by modus ponens from φ_j, φ_k with $j, k < i$.

Extensions of Frege Systems

Extended Frege *EF*

Abbreviations for complex formulas: $p \equiv \varphi$,
where p is a new propositional variable.

Frege systems with substitution *SF*

Substitution rule: $$\frac{\varphi}{\sigma(\varphi)}$$
for arbitrary substitutions σ

Extensions of *EF*

Let Φ be a polynomial-time computable set of tautologies.

- $EF \cup \Phi$: Φ as new axioms
- $EF + \Phi$: Φ as axiom schemes

Simulations Between Proof Systems

Definition (Cook, Reckhow 79)

A proof system Q simulates a proof system P ($P \leq Q$), if Q-proofs are at most polynomially longer than P-proofs.

Theorem (Krajíček, Pudlák 89)

Every proof system is simulated by a proof system of the form $EF + \Phi$.

Definition

P is optimal, if P simulates all proof systems.

Problem (Krajíček, Pudlák 89)

Do optimal proof systems exist?

The Deduction Theorem

Classical Deduction Theorem

For all formulas φ, ψ we have

$$F \cup \varphi \vdash \psi \quad \Longleftrightarrow \quad F \vdash \varphi \rightarrow \psi \quad .$$

The Deduction Theorem

Classical Deduction Theorem

For all formulas φ, ψ we have

$$F \cup \varphi \vdash \psi \quad \Longleftrightarrow \quad F \vdash \varphi \to \psi \quad .$$

Proof.

"$\Longleftarrow$": Given an F-proof of $\varphi \to \psi$, we construct an $F \cup \varphi$-proof of ψ by one application of modus ponens. $\square$

The Deduction Theorem

Classical Deduction Theorem

For all formulas φ, ψ we have

$$F \cup \varphi \vdash \psi \quad \Longleftrightarrow \quad F \vdash \varphi \rightarrow \psi \ .$$

Proof.

"$\Longleftarrow$": Given an F-proof of $\varphi \rightarrow \psi$, we construct an $F \cup \varphi$-proof of ψ by one application of modus ponens. $\square$

Efficient Deduction Theorem (Bonet, Buss 93)

For all formulas φ, ψ we have

$$F \cup \varphi \vdash_{\leq m} \psi \quad \Longrightarrow \quad F \vdash_{\leq O(m^2+|\varphi|)} \varphi \rightarrow \psi \ .$$

The Deduction Property

The deduction theorem does not hold for EF and SF, for example $SF \cup p \vdash q$, but $SF \nvdash p \rightarrow q$.

The Deduction Property

The deduction theorem does not hold for EF and SF, for example $SF \cup p \vdash q$, but $SF \nvdash p \to q$.

Question

Is there a notion of efficient deduction that applies for strong systems like EF or SF?

The Deduction Property

The deduction theorem does not hold for EF and SF, for example $SF \cup p \vdash q$, but $SF \not\vdash p \to q$.

Question

Is there a notion of efficient deduction that applies for strong systems like EF or SF?

Definition

A proof system P has the deduction property, if there exists a polynomial p such that for all finite subsets $\Phi \subset TAUT$ we have:

$$P \cup \Phi \vdash_{\leq m} \psi \quad \Longrightarrow \quad P \vdash_{\leq p(m+m')} \Big(\bigwedge_{\varphi \in \Phi} \varphi\Big) \to \psi$$

with $m' = |\bigwedge_{\varphi \in \Phi} \varphi|$.

A Weak Deduction Property

Definition

$\Phi = \{\varphi_0, \varphi_1, \dots\}$ is called printable, if there exists a polynomial-time algorithm that outputs the formula φ_n on input 1^n.

Definition

A proof system P has weak deduction, if for all printable sets $\Phi \subset TAUT$ there exists a polynomial p such that

$$P \cup \Phi \vdash_{\leq m} \psi \quad \Longrightarrow \quad P \vdash_{\leq p(m+m')} \Big(\bigwedge_{\varphi \in \Phi_0} \varphi\Big) \rightarrow \psi$$

for some finite set $\Phi_0 \subseteq \Phi$ and $m' = |\bigwedge_{\varphi \in \Phi_0} \varphi|$.

A Problem with a Conditional Answer

Question

Do *EF* or *SF* satisfy the deduction or the weak deduction property?

A Problem with a Conditional Answer

Question

Do *EF* or *SF* satisfy the deduction or the weak deduction property?

Answer

Probably not.

A Problem with a Conditional Answer

Question

Do *EF* or *SF* satisfy the deduction or the weak deduction property?

Answer

Probably not.

EF/SF have deduction $\iff$ EF/SF are polynomially bounded.

A Problem with a Conditional Answer

Question

Do *EF* or *SF* satisfy the deduction or the weak deduction property?

Answer

Probably not.

EF / *SF* have deduction	$\Longleftrightarrow$	*EF* / *SF* are polynomially bounded.
EF / *SF* have weak deduction	$\Longleftrightarrow$	*EF* / *SF* are optimal.

Weak Deduction

Theorem

Optimal proof systems P have weak deduction.

Proof.

Assume $P \cup \Phi \vdash_{\leq m} \psi$.
Then there exists some finite set $\Phi_0 \subseteq \Phi$ such that $P \cup \Phi_0 \vdash_{\leq m} \psi$.
By the optimality of P we get $P \cup \Phi \leq P$.
The P-proof is constructed as follows:

- derive Φ_0,
- simulate the $P \cup \Phi_0$-proof of ψ,
- derive $(\bigwedge_{\varphi \in \Phi_0} \varphi) \to \psi$.

$\square$

Existence of Optimal Proof Systems

Theorem

Let $P \geq EF$ be a Hilbert-style proof system that fulfills the following conditions:

1. *P is closed under modus ponens and substitutions by constants.*
2. *For all printable sets of tautologies Φ the proof system $P \cup \Phi$ is closed under substitutions of variables.*
3. *P has the weak deduction property.*

Then P is an optimal proof system.

Optimality of *EF*

Theorem

The following conditions are equivalent:

1. *EF has the weak deduction property.*
2. *EF is optimal.*
3. *For all polynomial-time decidable sets $\Phi \subset TAUT$ the proof system $EF \cup \Phi$ is closed under substitutions.*

Optimality of *EF*

Theorem

The following conditions are equivalent:

1. *EF has the weak deduction property.*
2. *EF is optimal.*
3. *For all polynomial-time decidable sets $\Phi \subset TAUT$ the proof system $EF \cup \Phi$ is closed under substitutions.*

Corollary

There exists an optimal proof system if and only if there exists a printable set $\Psi \subset \mathrm{TAUT}$ such that $EF + \Psi$ has weak deduction.

Polynomially Bounded Proof Systems

Theorem

Let $P \geq EF$ be a Hilbert-style proof system that fulfills the following conditions:

1. *P is closed under modus ponens and substitutions by constants.*
2. *There exists a polynomial p such that for all printable sets of tautologies Φ the proof system $P \cup \Phi$ is closed under substitutions of variables with respect to p.*
3. *P has the deduction property.*

Then P is a polynomially bounded proof system.

Polynomially Bounded Proof Systems

Theorem

Let $P \geq EF$ be a Hilbert-style proof system that fulfills the following conditions:

1. *P is closed under modus ponens and substitutions by constants.*
2. *There exists a polynomial p such that for all printable sets of tautologies Φ the proof system $P \cup \Phi$ is closed under substitutions of variables with respect to p.*
3. *P has the deduction property.*

Then P is a polynomially bounded proof system.

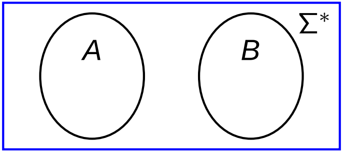
Corollary

EF has the efficient deduction property if and only if EF is polynomially bounded.

Disjoint NP-Pairs

Definition (Grollmann, Selman 88)

(A, B) is a disjoint NP-Pair if $A, B \in \mathrm{NP}$ and $A \cap B = \emptyset$.



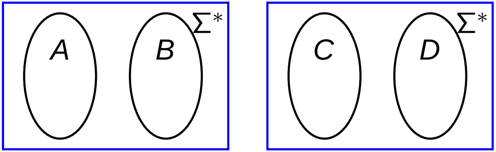
Applications

- security of public-key crypto systems
- propositional proof complexity

Reductions Between Pairs

Definition (Grollmann, Selman 88)

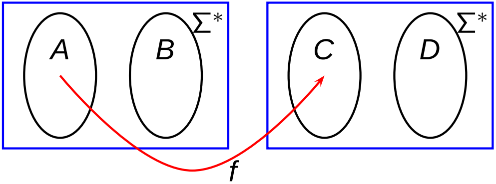
$(A,B) \leq_p (C,D) \overset{df}{\Longleftrightarrow}$ there exists a polynomial time computable function f such that $f(A) \subseteq C$ and $f(B) \subseteq D$.



Reductions Between Pairs

Definition (Grollmann, Selman 88)

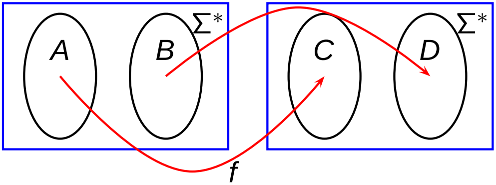
$(A, B) \leq_p (C, D) \overset{df}{\iff}$ there exists a polynomial time computable function f such that $f(A) \subseteq C$ and $f(B) \subseteq D$.



Reductions Between Pairs

Definition (Grollmann, Selman 88)

$(A, B) \leq_p (C, D) \overset{df}{\iff}$ there exists a polynomial time computable function f such that $f(A) \subseteq C$ and $f(B) \subseteq D$.



Canonical NP-Pairs

Definition (Razborov 94)

To a proof system P we associate a canonical pair:

$$\begin{aligned} Ref(P) &= \{(\varphi, 1^m) \mid P \vdash_{\leq m} \varphi\} \\ Sat^* &= \{(\varphi, 1^m) \mid \neg\varphi \text{ is satisfiable}\} \end{aligned}$$

Canonical NP-Pairs

Definition (Razborov 94)

To a proof system P we associate a canonical pair:

$$\begin{aligned} Ref(P) &= \{(\varphi, 1^m) \mid P \vdash_{\leq m} \varphi\} \\ Sat^* &= \{(\varphi, 1^m) \mid \neg\varphi \text{ is satisfiable}\} \end{aligned}$$

Problem (Razborov 94)

Do there exists complete disjoint NP-pairs?

Canonical NP-Pairs

Definition (Razborov 94)

To a proof system P we associate a canonical pair:

$$\begin{aligned} Ref(P) &= \{(\varphi, 1^m) \mid P \vdash_{\leq m} \varphi\} \\ Sat^* &= \{(\varphi, 1^m) \mid \neg\varphi \text{ is satisfiable}\} \end{aligned}$$

Problem (Razborov 94)

Do there exists complete disjoint NP-pairs?

Theorem (Razborov 94)

If P is an optimal proof system, then the canonical pair of P is a complete disjoint NP-pair.

On Complete Disjoint NP-Pairs

Theorem

Let P be a Hilbert-style proof system that fulfills the following conditions:

1. *P is closed under modus ponens.*
2. *For all printable sets of tautologies Φ the proof system $P \cup \Phi$ is closed under substitutions by constants.*
3. *P has the weak deduction property.*

Then the canonical pair of P is a complete disjoint NP-pair.

Existence of Optimal Proof Systems

Theorem

Let $P \geq EF$ be a Hilbert-style proof system that fulfills the following conditions:

1. *P is closed under modus ponens and substitutions by constants.*
2. *For all printable sets of tautologies Φ the proof system $P \cup \Phi$ is closed under substitutions of variables.*
3. *P has the weak deduction property.*

Then P is an optimal proof system.

On Complete Disjoint NP-Pairs

Theorem

Let P be a Hilbert-style proof system that fulfills the following conditions:

1. *P is closed under modus ponens.*
2. *For all printable sets of tautologies Φ the proof system $P \cup \Phi$ is closed under substitutions by constants.*
3. *P has the weak deduction property.*

Then the canonical pair of P is a complete disjoint NP-pair.

Further Implications

Corollary

Assume that for all printable sets of tautologies Φ the system $F \cup \Phi$ is closed under substitutions by constants. Then the canonical Frege pair is a complete disjoint NP-pair.

Corollary

Assume that $F \cup \Phi \equiv EF \cup \Phi$ for all printable sequences Φ of tautologies. Then the canonical Frege pair is a complete disjoint NP-pair.

Summary

Even weak versions of the deduction theorem are very powerful for strong proof systems.

Summary

Even weak versions of the deduction theorem are very powerful for strong proof systems.

- Frege systems have classical deduction, while *EF* and *SF* fail to have this property.

Summary

Even weak versions of the deduction theorem are very powerful for strong proof systems.

- Frege systems have classical deduction, while *EF* and *SF* fail to have this property.
- Deduction for *EF* and its extensions characterizes the existence of polynomially bounded proof systems.

Summary

Even weak versions of the deduction theorem are very powerful for strong proof systems.

- Frege systems have classical deduction, while *EF* and *SF* fail to have this property.
- Deduction for *EF* and its extensions characterizes the existence of polynomially bounded proof systems.
- Weak deduction for *EF* and its extensions characterizes the existence of optimal proof systems.

Summary

Even weak versions of the deduction theorem are very powerful for strong proof systems.

- Frege systems have classical deduction, while *EF* and *SF* fail to have this property.
- Deduction for *EF* and its extensions characterizes the existence of polynomially bounded proof systems.
- Weak deduction for *EF* and its extensions characterizes the existence of optimal proof systems.
- Weak deduction yields sufficient conditions for the existence of complete disjoint NP-pairs.