Logic in Computer Science II

4th lesson
the graphs of proofs

- directed acyclic graph (DAG)
- nodes = labeled by
  1. formulas or sequents and
  2. rules applied
- arrows = indicate which assumptions used
- sources = axioms
- sink = the formula/sequent proved

4th lesson
the graphs of proofs

- directed acyclic graph (DAG)
- nodes = labeled by
  1. formulas or sequents and
  2. rules applied
- arrows = indicate which assumptions used
- sources = axioms
- sink = the formula/sequent proved

Example

$$\frac{A, A \supset B}{B}$$

$$[A; \ldots] \searrow \quad [B; \textit{modus ponens}] \quad \swarrow [A \supset B; \ldots]$$

trees and DAGs

Two forms of proofs

1. general, DAG-like
2. tree-like, useful for analyzing proofs

trees and DAGs

Two forms of proofs

1. general, DAG-like
2. tree-like, useful for analyzing proofs

The transformation from a DAG-like to tree-like may result in exponential blowup

trees and DAGs

Two forms of proofs

1. general, DAG-like
2. tree-like, useful for analyzing proofs

The transformation from a DAG-like to tree-like may result in exponential blowup

A similar distinction for Boolean circuits:

1. general Boolean circuits, DAG-like
2. tree-like, propositional formulas

Krajíček's idea

From a given proof in a weak proof system we may be able to construct an interpolant, or

Krajíček's idea

From a given proof in a weak proof system we may be able to construct an interpolant, or

From a given proof P and an assignment $\vec{a}$ to common variables we may decide which formula is a tautology.

Krajíček's idea

From a given proof in a weak proof system we may be able to construct an interpolant, or

From a given proof P and an assignment $\vec{a}$ to common variables we may decide which formula is a tautology. If

$$P \vdash \alpha(\vec{p}, \vec{q}) \vee \beta(\vec{p}, \vec{r})$$

and $\vec{p} \mapsto \vec{a} \in \{0, 1\}^n$, then

$$\models \alpha(\vec{a}, \vec{q}) \quad \text{or} \quad \models \beta(\vec{a}, \vec{r})$$

Krajíček's idea

From a given proof in a weak proof system we may be able to construct an interpolant, or

From a given proof P and an assignment $\vec{a}$ to common variables we may decide which formula is a tautology. If

$$P \vdash \alpha(\vec{p}, \vec{q}) \vee \beta(\vec{p}, \vec{r})$$

and $\vec{p} \mapsto \vec{a} \in \{0, 1\}^n$, then

$$\models \alpha(\vec{a}, \vec{q}) \quad \text{or} \qquad \models \beta(\vec{a}, \vec{r})$$

We want to decide which of the two is true.

Krajíček's idea

From a given proof in a weak proof system we may be able to construct an interpolant, or

From a given proof P and an assignment $\vec{a}$ to common variables we may decide which formula is a tautology. If

$$P \vdash \alpha(\vec{p}, \vec{q}) \vee \beta(\vec{p}, \vec{r})$$

and $\vec{p} \mapsto \vec{a} \in \{0,1\}^n$, then

$$\models \alpha(\vec{a}, \vec{q}) \quad \text{or} \quad \models \beta(\vec{a}, \vec{r})$$

We want to decide which of the two is true.

In terms of disjoint NP-sets:

Given a proof P of

$$A \cap B = \emptyset$$

and given $a \in A \cup B$, we want to decide which of the two

$$a \in A \qquad \text{or} \qquad a \in B$$

is true.

feasible interpolation for cut-free proofs

Theorem

Given a tree-like cut-free proof

$$P \vdash \neg\alpha(\vec{p}, \vec{q}) \to \beta(\vec{p}, \vec{r})$$

we can construct in polynomial time a formula $I(\vec{p})$ s.t.

$$\vdash \neg\alpha(\vec{p}, \vec{q}) \to I(\vec{p}) \to \beta(\vec{p}, \vec{r}),$$

feasible interpolation for cut-free proofs

Theorem

Given a tree-like cut-free proof

$$P \vdash \neg\alpha(\vec{p},\vec{q}) \rightarrow \beta(\vec{p},\vec{r})$$

we can construct in polynomial time a formula $I(\vec{p})$ s.t.

$$\vdash \neg\alpha(\vec{p},\vec{q}) \rightarrow I(\vec{p}) \rightarrow \beta(\vec{p},\vec{r}),$$

or equivalently

$$\vdash I(\vec{p}) \rightarrow \alpha(\vec{p},\vec{q}),$$

$$\vdash \neg I(\vec{p}) \rightarrow \beta(\vec{p},\vec{r})$$

feasible interpolation for cut-free proofs

Theorem

Given a tree-like cut-free proof

$$P \vdash \neg\alpha(\vec{p},\vec{q}) \rightarrow \beta(\vec{p},\vec{r})$$

we can construct in polynomial time a formula $I(\vec{p})$ *s.t.*

$$\vdash \neg\alpha(\vec{p},\vec{q}) \rightarrow I(\vec{p}) \rightarrow \beta(\vec{p},\vec{r}),$$

or equivalently

$$\vdash I(\vec{p}) \rightarrow \alpha(\vec{p},\vec{q}),$$

$$\vdash \neg I(\vec{p}) \rightarrow \beta(\vec{p},\vec{r})$$

Hence given $\vec{p} \mapsto \vec{a}$*, we can decide in polynomial time which of the two is true*

$$\models \alpha(\vec{a},\vec{q}) \quad \textit{or} \quad \models \beta(\vec{a},\vec{r}).$$

Theorem

Given a general cut-free proof

$$P \vdash \neg\alpha(\vec{p}, \vec{q}) \rightarrow \beta(\vec{p}, \vec{r})$$

we can construct in polynomial time a circuit $C(\vec{p})$ s.t.

$$\models C(\vec{p}) \rightarrow \alpha(\vec{p}, \vec{q}),$$

$$\models \neg C(\vec{p}) \rightarrow \beta(\vec{p}, \vec{r})$$

Theorem

Given a general cut-free proof

$$P \vdash \neg\alpha(\vec{p}, \vec{q}) \rightarrow \beta(\vec{p}, \vec{r})$$

we can construct in polynomial time a circuit $C(\vec{p})$ s.t.

$$\models C(\vec{p}) \rightarrow \alpha(\vec{p}, \vec{q}),$$

$$\models \neg C(\vec{p}) \rightarrow \beta(\vec{p}, \vec{r})$$

Hence given $\vec{p} \mapsto \vec{a}$, we can decide in polynomial time which of the two is true

$$\models \alpha(\vec{a}, \vec{q}) \quad \text{or} \quad \models \beta(\vec{a}, \vec{r}).$$

feasible interpolation for Resolution

Theorem

Given a Resolution proof P of contradiction from a set of clauses $\{A_i(\vec{p}, \vec{q})\}_i \cup \{B_j(\vec{p}, \vec{r})\}_j$, in symbols:

$$P : \{A_i(\vec{p}, \vec{q})\}_i \cup \{B_j(\vec{p}, \vec{r})\}_j \to \bot,$$

we can construct in polynomial time a circuit C s.t. for all assignements $\vec{a}$

$$C(\vec{a}) = 0 \to \{A_i(\vec{p}, \vec{q})\}_i \text{ is unsatatisfiable}$$

$$C(\vec{a}) = 1 \to \{B_j(\vec{p}, \vec{r})\}_j \text{ is unsatatisfiable}$$

splitting Resolution proofs

Theorem

Given a Resolution proof P of contradiction

$$P : \{A_i(\vec{p}, \vec{q})\}_i \cup \{B_j(\vec{p}, \vec{r})\}_j \to \bot,$$

and an assignment for $\vec{p} \mapsto \vec{a}$, we can construct in polynomial time two proofs

- P^A *a proof from* $\{A_i(\vec{a}, \vec{q})\}_i$,
- P^B *a proof from* $\{B_j(\vec{a}, \vec{r})\}_j$,

such that one of them is a proof of contradiction.

splitting Resolution proofs

Theorem

Given a Resolution proof P of contradiction

$$P : \{A_i(\vec{p}, \vec{q})\}_i \cup \{B_j(\vec{p}, \vec{r})\}_j \to \bot,$$

and an assignment for $\vec{p} \mapsto \vec{a}$, we can construct in polynomial time two proofs

- P^A *a proof from* $\{A_i(\vec{a}, \vec{q})\}_i$,
- P^B *a proof from* $\{B_j(\vec{a}, \vec{r})\}_j$,

such that one of them is a proof of contradiction.

Proof.

See my paper: *Lower bounds for resolution and cutting planes proofs and monotone computations.*

splitting Resolution proofs

Theorem

Given a Resolution proof P of contradiction

$$P : \{A_i(\vec{p}, \vec{q})\}_i \cup \{B_j(\vec{p}, \vec{r})\}_j \to \bot,$$

and an assignment for $\vec{p} \mapsto \vec{a}$, we can construct in polynomial time two proofs

- P^A *a proof from* $\{A_i(\vec{a}, \vec{q})\}_i$,
- P^B *a proof from* $\{B_j(\vec{a}, \vec{r})\}_j$,

such that one of them is a proof of contradiction.

Proof.

See my paper: *Lower bounds for resolution and cutting planes proofs and monotone computations.*

Missing argument: We need to show that after the substitution $\vec{p} := \vec{a}$ none of the chosen clauses disappears. This follows by induction. □

splitting Resolution proofs

Theorem

Given a Resolution proof P of contradiction

$$P : \{A_i(\vec{p}, \vec{q})\}_i \cup \{B_j(\vec{p}, \vec{r})\}_j \to \bot,$$

and an assignment for $\vec{p} \mapsto \vec{a}$, we can construct in polynomial time two proofs

- P^q *a proof from* $\{A_i(\vec{a}, \vec{q})\}_i$,
- P^r *a proof from* $\{B_j(\vec{a}, \vec{r})\}_j$,

such that one of them is a proof of contradiction.

proof

q-clause = clause with only variables $\vec{p}, \vec{q}$
r-clause = clause with only variables $\vec{p}, \vec{r}$
otherwise, mixed clause

proof

q-clause = clause with only variables $\vec{p}, \vec{q}$
r-clause = clause with only variables $\vec{p}, \vec{r}$
otherwise, mixed clause

Idea: We want to have only q-clauses and r-clauses.

- the initial clauses are OK
- a mixed clauses appears when we resolve a q-clause with an r-clause
- in such a case the resolved variable must be from $\vec{p}$

proof

q-clause = clause with only variables $\vec{p}, \vec{q}$
r-clause = clause with only variables $\vec{p}, \vec{r}$
otherwise, mixed clause

Idea: We want to have only q-clauses and r-clauses.

- the initial clauses are OK
- a mixed clauses appears when we resolve a q-clause with an r-clause
- in such a case the resolved variable must be from $\vec{p}$

Let $\vec{p} \mapsto \vec{a}$. We gradually transform the clause from the proof $C \quad \mapsto \quad C'$ as follows:

- if we resolve w.r.t. some q_i or r_i in the given proof, we do the same;

- if we resolve w.r.t. some p_i then, if $a : p_i \mapsto 0$, then

$$\frac{\Gamma \vee p, \quad \Delta \vee \neg p}{\Gamma \vee \Delta} \quad \mapsto \quad \frac{\Gamma' \vee p, \quad \Delta' \vee \neg p}{\Gamma'}$$

otherwise

$$\mapsto \frac{\Gamma' \vee p, \quad \Delta' \vee \neg p}{\Delta'}$$

- this is not a logically valid derivation;
- if $C \quad \mapsto \quad C'$, then $C' \subseteq C$;
- hence $\bot \ \mapsto \ \bot$.

- if we resolve w.r.t. some p_i then, if $a : p_i \mapsto 0$, then

$$\frac{\Gamma \vee p, \quad \Delta \vee \neg p}{\Gamma \vee \Delta} \quad \mapsto \quad \frac{\Gamma' \vee p, \quad \Delta' \vee \neg p}{\Gamma'}$$

  otherwise

$$\mapsto \frac{\Gamma' \vee p, \quad \Delta' \vee \neg p}{\Delta'}$$

- this is not a logically valid derivation;
- if $C \quad \mapsto \quad C'$, then $C' \subseteq C$;
- hence $\bot \;\mapsto\; \bot$.

Next substitute $\vec{a}$ and $C' \;\mapsto\; C''$:

- if C' has a true literal, then $C'' := \top$
- otherwise $C'' := C'$-less literals from $\vec{p}$.

- if we resolve w.r.t. some p_i then, if $a : p_i \mapsto 0$, then

$$\frac{\Gamma \vee p, \quad \Delta \vee \neg p}{\Gamma \vee \Delta} \quad \mapsto \quad \frac{\Gamma' \vee p, \quad \Delta' \vee \neg p}{\Gamma'}$$

  otherwise

$$\mapsto \frac{\Gamma' \vee p, \quad \Delta' \vee \neg p}{\Delta'}$$

- this is not a logically valid derivation;
- if $C \quad \mapsto \quad C'$, then $C' \subseteq C$;
- hence $\bot \ \mapsto \ \bot$.

Next substitute $\vec{a}$ and $C' \ \mapsto \ C''$:

- if C' has a true literal, then $C'' := \top$
- otherwise $C'' := C'$-less literals from $\vec{p}$.

Claim The resulting set of clauses is a valid Resolutions proof of $\bot$.

- if $a : p_i \mapsto 0$, then

$$\frac{\Gamma' \vee p, \quad \Delta' \vee \neg p}{\Gamma'} \quad \mapsto \quad \frac{\Gamma'', \quad \top}{\Gamma''}$$

- if we resolve with q or r and $C_1' \mapsto \top$ then

$$\frac{C_1', \quad C_2'}{C'} \quad \mapsto \frac{\top \quad C_2''}{\top}$$

- etc.

$\square$

applications of feasible interpolation

1. program verification
2. lower bounds on the complexity of proofs

applications of feasible interpolation

1. program verification
2. lower bounds on the complexity of proofs

Theorem

Suppose that $\mathbf{NP} \cap \mathbf{coNP} \not\subseteq \mathbf{P}/poly$. *Then there are sequences of tautologies that do not have polynomial size proofs in any propositional proof system that has feasible interpolation.*

applications of feasible interpolation

1. program verification
2. lower bounds on the complexity of proofs

Theorem

Suppose that $\mathbf{NP} \cap \mathbf{coNP} \not\subseteq \mathbf{P}/poly$*. Then there are sequences of tautologies that do not have polynomial size proofs in any propositional proof system that has feasible interpolation.*

It suffices to assume that *there exist two disjoint* $\mathbf{NP}$ *sets that cannot be separated by a set in* $\mathbf{P}/poly$*.*

applications of feasible interpolation

1. program verification
2. lower bounds on the complexity of proofs

Theorem

Suppose that $\mathbf{NP} \cap \mathbf{coNP} \not\subseteq \mathbf{P}/poly$*. Then there are sequences of tautologies that do not have polynomial size proofs in any propositional proof system that has feasible interpolation.*

It suffices to assume that *there exist two disjoint* **NP** *sets that cannot be separated by a set in* $\mathbf{P}/poly$*.*

$\mathbf{P}/\mathrm{poly}$ = the nonuniform version of **P** = sets definable by polynomial size Boolean circuits.

Proof.

Let A, B be disjoint **NP** sets that cannot be separated by a set in **P**/poly. Let

$A := \{\bar{u} \mid \exists \bar{v}\ \neg\alpha_n(\bar{u}, \bar{v}), n \in \mathbb{N}\},$

$B := \{\bar{u} \mid \exists \bar{w}\ \neg\beta_n(\bar{u}, \bar{w}), n \in \mathbb{N}\}$

Then the sequence of formulas

$$\alpha_n(\bar{u}, \bar{v}) \vee \beta_n(\bar{u}, \bar{w})$$

expresses that $A \cap B = \emptyset$. Hence they are tautologies.

Proof.

Let A, B be disjoint **NP** sets that cannot be separated by a set in **P**/poly. Let

$A := \{\bar{u} \mid \exists \bar{v}\ \neg\alpha_n(\bar{u}, \bar{v}), n \in \mathbb{N}\}$,

$B := \{\bar{u} \mid \exists \bar{w}\ \neg\beta_n(\bar{u}, \bar{w}), n \in \mathbb{N}\}$

Then the sequence of formulas

$$\alpha_n(\bar{u}, \bar{v}) \vee \beta_n(\bar{u}, \bar{w})$$

expresses that $A \cap B = \emptyset$. Hence they are tautologies.

Let $\mathcal{P}$ be a proof system with feasible interpolation and suppose $\mathcal{P}$ has polynomial size proofs P_n of these tautologies. By feasible interpolation, for every $\bar{a}$, we can decide in polynomial time whether

$$\alpha_n(\bar{a}, \bar{v}) \quad \text{or} \quad \beta_n(\bar{a}, \bar{w})$$

is a tautology, i.e., whether $\bar{a} \notin A$ or $\bar{a} \notin B$.

Proof.

Let A, B be disjoint **NP** sets that cannot be separated by a set in **P**/poly. Let

$A := \{\bar{u} \mid \exists \bar{v}\ \neg\alpha_n(\bar{u}, \bar{v}), n \in \mathbb{N}\},$

$B := \{\bar{u} \mid \exists \bar{w}\ \neg\beta_n(\bar{u}, \bar{w}), n \in \mathbb{N}\}$

Then the sequence of formulas

$$\alpha_n(\bar{u}, \bar{v}) \vee \beta_n(\bar{u}, \bar{w})$$

expresses that $A \cap B = \emptyset$. Hence they are tautologies.

Let $\mathcal{P}$ be a proof system with feasible interpolation and suppose $\mathcal{P}$ has polynomial size proofs P_n of these tautologies. By feasible interpolation, for every $\bar{a}$, we can decide in polynomial time whether

$$\alpha_n(\bar{a}, \bar{v}) \quad \text{or} \quad \beta_n(\bar{a}, \bar{w})$$

is a tautology, i.e., whether $\bar{a} \notin A$ or $\bar{a} \notin B$.

From polynomial time algorithm we can construct polynomial

we cannot prove $\mathbf{NP} \cap \mathbf{coNP} \not\subseteq \mathbf{P}/\mathrm{poly}$, yet ...

we cannot prove $\mathbf{NP} \cap \mathbf{coNP} \not\subseteq \mathbf{P}/\text{poly}$, yet ...

Monotone Interpolation: if $\bar{u}$ occurs

- only positively in $\alpha(\vec{p}, \vec{q})$ or
- only negatively in $\beta(\vec{p}, \vec{r})$,

then there exists a monotone polynomial size circuit $C(\vec{p})$ s.t.

$$\models C(\vec{p}) \to \alpha(\vec{p}, \vec{q}),$$

$$\models \neg C(\vec{p}) \to \beta(\vec{p}, \vec{r}).$$

we cannot prove NP∩coNP$\not\subseteq$P/poly, yet ...

Monotone Interpolation: if $\bar{u}$ occurs

- only positively in $\alpha(\vec{p}, \vec{q})$ or
- only negatively in $\beta(\vec{p}, \vec{r})$,

then there exists a monotone polynomial size circuit $C(\vec{p})$ s.t.

$$\models C(\vec{p}) \to \alpha(\vec{p}, \vec{q}),$$

$$\models \neg C(\vec{p}) \to \beta(\vec{p}, \vec{r}).$$

We do have exponential lower bounds on monotone circuits separating disjoint **NP** sets, hence we can prove lower bounds in this way.

no feasible interpolation for strong proof systems

no feasible interpolation for strong proof systems

In strong proof systems we do have polynomial size proofs $A \cap B = \emptyset$ for sets that we *believe* cannot be separated by a set in $\mathbf{P}$. Hence we believe that these systems do not have feasible interpolation.

no feasible interpolation for strong proof systems

In strong proof systems we do have polynomial size proofs $A \cap B = \emptyset$ for sets that we *believe* cannot be separated by a set in **P**. Hence we believe that these systems do not have feasible interpolation.

Theorem

If the factoring problem is not solvable in polynomial time, then Frege systems, sequent calculi with cut and natural deduction system do not have feasible interpolation.

no feasible interpolation for strong proof systems

In strong proof systems we do have polynomial size proofs $A \cap B = \emptyset$ for sets that we *believe* cannot be separated by a set in $\mathbf{P}$. Hence we believe that these systems do not have feasible interpolation.

Theorem

If the factoring problem is not solvable in polynomial time, then Frege systems, sequent calculi with cut and natural deduction system do not have feasible interpolation.

Factoring is the problem to find nontrivial factors of a given composed integer.

proof theory of 1st order logic

(See Buss's chapter in Handbook)

proof theory of 1st order logic

(See Buss's chapter in Handbook)

Syntax

proof theory of 1st order logic

(See Buss's chapter in Handbook)

Syntax

Primitive concepts

- relation and function symbols $R, S, \dots, f, g, \dots$
- the equality sign $=$
- variables $x, y, \dots$ (for elements) and constants $c, d, \dots$
- propositional connectives $\neg, \wedge, \dots$
- quantifiers $\forall, \exists$
- parentheses (,)

proof theory of 1st order logic

(See Buss's chapter in Handbook)

Syntax

Primitive concepts

- relation and function symbols $R, S, \ldots, f, g, \ldots$
- the equality sign $=$
- variables $x, y, \ldots$ (for elements) and constants $c, d, \ldots$
- propositional connectives $\neg, \wedge, \ldots$
- quantifiers $\forall, \exists$
- parentheses (,)

Terms and formulas

- terms $t, s, \ldots$, e.g., $f(c, g(d))$
- atomic formulas $R(t_1, \ldots, t_n)$, $t_1 = t_2$, where t_i are terms
- general formulas may have free variables
- sentences = formulas with no free variables
- prenex formulas/sentences = all quantifiers are in the prefix

proof theory of 1st order logic

(See Buss's chapter in Handbook)

Syntax

Primitive concepts

- relation and function symbols $R, S, \ldots, f, g, \ldots$
- the equality sign $=$
- variables $x, y, \ldots$ (for elements) and constants $c, d, \ldots$
- propositional connectives $\neg, \wedge, \ldots$
- quantifiers $\forall, \exists$
- parentheses (,)

Terms and formulas

- terms $t, s, \ldots$, e.g., $f(c, g(d))$
- atomic formulas $R(t_1, \ldots, t_n)$, $t_1 = t_2$, where t_i are terms
- general formulas may have free variables
- sentences = formulas with no free variables
- prenex formulas/sentences = all quantifiers are in the prefix

I suppose that you know what a well-formed formula is, what the scope of a quantifier is, which variables are bounded etc.

Semantics

Fact [attributed to A. Tarski] There is a well defined relation of satisfaction of a formula $\phi(x_1, \ldots, x_n)$ by elements $a_1, \ldots, a_n$ in a model M, which is denoted by

$$M \models \phi[a_1, \ldots, a_n].$$

Proof.
Define inductively on the complexity of terms and formulas. □

Semantics

Fact [attributed to A. Tarski] There is a well defined relation of satisfaction of a formula $\phi(x_1, \dots, x_n)$ by elements $a_1, \dots, a_n$ in a model M, which is denoted by

$$M \models \phi[a_1, \dots, a_n].$$

Proof.

Define inductively on the complexity of terms and formulas. □

Definition

A sentence ϕ is logically valid, if for every model M (of appropriate signature) $M \models \phi$.

Hilbert-style calculus

Frege system for propositional axioms and rules

+ quantifier axioms and rules:

Hilbert-style calculus

Frege system for propositional axioms and rules

+ quantifier axioms and rules:

Axioms (I am now using $\rightarrow$ for implication.)

$$\phi(t) \rightarrow \exists x.\phi(x) \qquad (\forall x.\phi(x)) \rightarrow \phi(t)$$

t is a term not containing any bound variables.

Hilbert-style calculus

Frege system for propositional axioms and rules

+ quantifier axioms and rules:

Axioms (I am now using $\rightarrow$ for implication.)

$$\phi(t) \rightarrow \exists x.\phi(x) \qquad (\forall x.\phi(x)) \rightarrow \phi(t)$$

t is a term not containing any bound variables.

Rules

$$\frac{\phi(x) \rightarrow \psi}{(\exists x.\phi(x)) \rightarrow \psi} \qquad \frac{\psi \rightarrow \phi(x)}{\psi \rightarrow \forall x.\phi(x)}$$

where x is not free in ψ.

Hilbert-style calculus

Frege system for propositional axioms and rules

+ quantifier axioms and rules:

Axioms (I am now using $\rightarrow$ for implication.)

$$\phi(t) \rightarrow \exists x.\phi(x) \qquad (\forall x.\phi(x)) \rightarrow \phi(t)$$

t is a term not containing any bound variables.

Rules

$$\frac{\phi(x) \rightarrow \psi}{(\exists x.\phi(x)) \rightarrow \psi} \qquad \frac{\psi \rightarrow \phi(x)}{\psi \rightarrow \forall x.\phi(x)}$$

where x is not free in ψ.

Proofs are sequences of formulas.

Hilbert-style calculus

Frege system for propositional axioms and rules

+ quantifier axioms and rules:

Axioms (I am now using $\to$ for implication.)

$$\phi(t) \to \exists x.\phi(x) \qquad (\forall x.\phi(x)) \to \phi(t)$$

t is a term not containing any bound variables.

Rules

$$\frac{\phi(x) \to \psi}{(\exists x.\phi(x)) \to \psi} \qquad \frac{\psi \to \phi(x)}{\psi \to \forall x.\phi(x)}$$

where x is not free in ψ.

Proofs are sequences of formulas.

Formalizations with MP only and sentences are known.

axioms of equality

See Buss's chapter.

axioms of equality

See Buss's chapter.

Exercise

1. Derive the axiom of the nonempty domain

$$\exists x(x = x)$$

2. Can one prove that the domain is nonempty without using equality? How can one state such an axiom?

the sequent calculus

Useful convention: $a, b, \ldots$ free variables, $x, y, \ldots$ bounded variables.

Notation: $\Rightarrow$ for the arrow in sequents.

the sequent calculus

Useful convention: $a, b, \ldots$ free variables, $x, y, \ldots$ bounded variables.

Notation: $\Rightarrow$ for the arrow in sequents.

No axioms for quantifiers!

the sequent calculus

Useful convention: $a, b, \ldots$ free variables, $x, y, \ldots$ bounded variables.

Notation: $\Rightarrow$ for the arrow in sequents.

No axioms for quantifiers!

Quantifier rules

$$\text{(weak)} \qquad \frac{\Gamma \Rightarrow \Delta, \phi(t)}{\Gamma \Rightarrow \Delta, \exists x.\phi(x)} \qquad \frac{\phi(t), \Gamma \Rightarrow \Delta}{\forall x.\phi(x), \Gamma \Rightarrow \Delta}$$

where t is a term not containing any bound variables.

$$\text{(strong)} \qquad \frac{\Gamma \Rightarrow \Delta, \phi(a)}{\Gamma \Rightarrow \Delta, \forall x.\phi(x)} \qquad \frac{\phi(a), \Gamma \Rightarrow \Delta}{\exists x.\phi(x), \Gamma \Rightarrow \Delta}$$

where a does not occur in ψ.

the sequent calculus

Useful convention: $a, b, \ldots$ free variables, $x, y, \ldots$ bounded variables.

Notation: $\Rightarrow$ for the arrow in sequents.

No axioms for quantifiers!

Quantifier rules

$$\text{(weak)} \qquad \frac{\Gamma \Rightarrow \Delta, \phi(t)}{\Gamma \Rightarrow \Delta, \exists x.\phi(x)} \qquad \frac{\phi(t), \Gamma \Rightarrow \Delta}{\forall x.\phi(x), \Gamma \Rightarrow \Delta}$$

where t is a term not containing any bound variables.

$$\text{(strong)} \qquad \frac{\Gamma \Rightarrow \Delta, \phi(a)}{\Gamma \Rightarrow \Delta, \forall x.\phi(x)} \qquad \frac{\phi(a), \Gamma \Rightarrow \Delta}{\exists x.\phi(x), \Gamma \Rightarrow \Delta}$$

where a does not occur in ψ.

Axioms of equality: same, but stated as sequents (See Buss's chapter)

examples of wrong applications

$$\frac{\Rightarrow \forall x \; (f(x) = f(x))}{\Rightarrow \exists y \forall x \; (f(x) = y)}$$

examples of wrong applications

$$\frac{\Rightarrow \forall x\ (f(x) = f(x))}{\Rightarrow \exists y \forall x\ (f(x) = y)}$$

$$\frac{a = b \Rightarrow a = b}{a = b \Rightarrow \forall x (x = b)}$$

Natural Deduction

quantifier rules

Natural Deduction

quantifier rules

∀-intro $$\frac{A(b)}{(\forall x)A(x)}$$

∀-elim $$\frac{(\forall x)A(x)}{A(t)}$$

∃-intro $$\frac{A(t)}{(\exists x)A(x)}$$

∃-elim $$\frac{(\exists x)A(x) \qquad \begin{matrix}[A(b)] \\ B\end{matrix}}{B}$$

Lesson 5
cut-elimination in the sequent calculus

Preprocessing:

- put the proof into a tree-like form
- ensure the free variable normal form — use distinct free variables whenever possible

Lesson 5
cut-elimination in the sequent calculus

Preprocessing:

- put the proof into a tree-like form
- ensure the free variable normal form — use distinct free variables whenever possible

Caveat:

- When transforming the proof watch for possible conflicts of free variables in the strong q. rules!
- Also do not forget about contractions!

example

$P_1(a, b)$ $\qquad\qquad$ $P_2(s, t)$

$$
\dfrac{\dfrac{\text{contraction}\ \dfrac{\dfrac{\dfrac{\cdots}{A(a), A(b), \Gamma \longrightarrow \Delta}}{\exists x A(x), A(b), \Gamma \longrightarrow \Delta}}{\exists x A(x), \exists x A(x), \Gamma \longrightarrow \Delta}}{\exists x A(x), \Gamma \longrightarrow \Delta} \qquad \text{contraction}\ \dfrac{\dfrac{\dfrac{\dfrac{\cdots}{\Gamma \longrightarrow A(s), A(t), \Delta}}{\Gamma \longrightarrow \exists x A(x), A(t) \Delta}}{\Gamma \longrightarrow \exists x A(x), \exists x A(x) \Delta}}{\Gamma \longrightarrow \exists x A(x), \Delta}}{\Gamma \longrightarrow \Sigma}\ \text{cut}
$$

example

$$P_1(a, b) \qquad\qquad P_2(s, t)$$

$$\text{cut}\ \dfrac{\text{contraction}\ \dfrac{\dfrac{\dfrac{\dfrac{\dots}{A(a), A(b), \Gamma \longrightarrow \Delta}}{\exists x A(x), A(b), \Gamma \longrightarrow \Delta}}{\exists x A(x), \exists x A(x), \Gamma \longrightarrow \Delta}}{\exists x A(x), \Gamma \longrightarrow \Delta} \qquad \text{contraction}\ \dfrac{\dfrac{\dfrac{\dfrac{\dots}{\Gamma \longrightarrow A(s), A(t), \Delta}}{\Gamma \longrightarrow \exists x A(x), A(t) \Delta}}{\Gamma \longrightarrow \exists x A(x), \exists x A(x) \Delta}}{\Gamma \longrightarrow \exists x A(x), \Delta}}{\Gamma \longrightarrow \Sigma}$$

$$P_1(a, b) \ \mapsto \ P_1(s, s), P_1(t, t)$$

$$\text{cut}\ \dfrac{\dfrac{\dfrac{\dots}{A(s), A(s), \Gamma \longrightarrow \Delta}}{A(s), \Gamma \longrightarrow \Delta} \qquad \text{cut}\ \dfrac{\dfrac{\dfrac{\dots}{A(t), A(t), \Gamma \longrightarrow \Delta}}{A(t), \Gamma \longrightarrow \Delta} \qquad \dfrac{\dots}{\Gamma \longrightarrow A(s), A(t) \Delta}}{A(s), \Gamma \longrightarrow \Sigma}}{\Gamma \longrightarrow \Sigma}$$

What is a direct ancestor?

Example

$$\dfrac{\dfrac{\dfrac{\cdots}{A(a) \longrightarrow B(a)}}{A(a) \longrightarrow \exists x B(x)}}{\exists x A(x) \longrightarrow \exists x B(x)}$$

What is a direct ancestor?

Example

$$\dfrac{\dfrac{\dfrac{\ldots}{A(a) \longrightarrow B(a)}}{A(a) \longrightarrow \exists x B(x)}}{\exists x A(x) \longrightarrow \exists x B(x)}$$

$$\dfrac{\dfrac{\ldots}{A(t) \longrightarrow B(t)}}{A(t) \longrightarrow \exists x B(x)}$$

Definition

A is a generalized subformula of B if it is a substitution instance of a subformula of B.

Proposition

Every formula in a cut-free proof is a generalized subformula of a formula in the last sequent.

mid-sequent theorem

Theorem

Suppose ϕ is a provable sentence in a prenex form. Then there exists a (cut-free) proof of $\rightarrow \phi$ in which there a sequent $\rightarrow \Delta$ (the mid-sequent) such that

- *there are no quantifier rules above $\rightarrow \Delta$ (thus the mid-sequent does not contain quantifiers)*
- *there are only quantifier rules and structural rules below $\rightarrow \Delta$.*

mid-sequent theorem

Theorem

Suppose ϕ is a provable sentence in a prenex form. Then there exists a (cut-free) proof of $\to \phi$ in which there a sequent $\to \Delta$ (the mid-sequent) such that

- *there are no quantifier rules above $\to \Delta$ (thus the mid-sequent does not contain quantifiers)*
- *there are only quantifier rules and structural rules below $\to \Delta$.*

Proof.

1. Take a cut-free proof in the free-variable normal form.
2. Whenever a propositional rule is below a quantifier rule, switch the rules.

□

mid-sequent theorem

Theorem

Suppose ϕ is a provable sentence in a prenex form. Then there exists a (cut-free) proof of $\to \phi$ in which there a sequent $\to \Delta$ (the mid-sequent) such that

- *there are no quantifier rules above $\to \Delta$ (thus the mid-sequent does not contain quantifiers)*
- *there are only quantifier rules and structural rules below $\to \Delta$.*

Proof.

1. Take a cut-free proof in the free-variable normal form.
2. Whenever a propositional rule is below a quantifier rule, switch the rules.

□

Simple idea, tedious verification.

digression — some history

Gerhard Gentzen (1909-1945)

- calculus of natural deduction, sequent calculus
- cut-elimination theorem
- consistency of Peano Arithmetic assuming ϵ_0 is a well-ordering, the first result in *ordinal analysis of theories*

digression — some history

Gerhard Gentzen (1909-1945)

- calculus of natural deduction, sequent calculus
- cut-elimination theorem
- consistency of Peano Arithmetic assuming ϵ_0 is a well-ordering, the first result in *ordinal analysis of theories*

Jacques Herbrand (1908-1931)

- algebraic number fields
- logic – Herbrand's theorem
- computability theory – the Gödel-Herbrand recursive functions

Herbrand's Theorem

Theorem (basic version)

Let A be an existential sentence

$$\exists x_1 \dots \exists x_n \phi(x_1, \dots, x_n)$$

(ϕ an open, i.e., quantifier-free formula). Then TFAE

1. *A is logically valid ($\equiv$ provable)*
2. *there exist terms t_{ij}, $i = 1, \dots, n$, $j = 1, \dots, m$ in the language of A such that*

$$\bigvee_{j=1}^{m} \phi(t_{1j}, \dots, t_{nj})$$

is a propositional tautology.

Proof.

Let $\rightarrow \Gamma$ be the mid-sequent in a proof of $\rightarrow A$, then $\rightarrow \Gamma$ is

$$\rightarrow \phi(t_{11}, \ldots, t_{n1}), \ldots, \phi(t_{1m}, \ldots, t_{nm})$$

□

exercise

Prove the following generalization:

Theorem (basic version)

Let A be a $\forall\exists$ *prenex sentence sentence*

$$\forall y_1 \dots \forall y_k \exists x_1 \dots \exists x_n \phi(x_1, \dots, x_n)$$

Then TFAE

1. *A is logically valid*
2. *there exist terms* t_{ij}, $i = 1, \dots, n$, $j = 1, \dots, m$ *in the language of A such that*

$$\bigvee_{j=1}^{m} \phi(a_1, \dots, a_k, t_{1j}, \dots, t_{nj})$$

is a propositional tautology.

example

Let P be predicate, $\mathsf{0}$ a constant, and S a unary function. We will write $S^n x$ for S n-times iterated.

example

Let P be predicate, 0 a constant, and S a unary function. We will write $S^n x$ for S n-times iterated.

The following is a logically true sentence for every concrete n:

$$(P(0) \wedge \forall x(P(x) \to P(Sx))) \to P(S^n 0)$$

We can prove it in $O(\log n)$ steps by deriving gradually

$$\forall x(P(x) \to P(S^2 x)), \forall x(P(x) \to P(S^4 x)), \forall x(P(x) \to P(S^8 x)), \ldots$$

from $\forall x(P(x) \to P(Sx))$.

example

Let P be predicate, 0 a constant, and S a unary function. We will write $S^n x$ for S n-times iterated.

The following is a logically true sentence for every concrete n:

$$(P(0) \wedge \forall x(P(x) \rightarrow P(Sx))) \rightarrow P(S^n 0)$$

We can prove it in $O(\log n)$ steps by deriving gradually

$$\forall x(P(x) \rightarrow P(S^2 x)), \forall x(P(x) \rightarrow P(S^4 x)), \forall x(P(x) \rightarrow P(S^8 x)), \ldots$$

from $\forall x(P(x) \rightarrow P(Sx))$.

Write it as an existential formula:

$$\exists x(\neg P(0) \vee (P(x) \wedge \neg P(Sx)) \vee P(S^n 0))$$

example, contd

The mid-sequent is $\to \Delta$ where Δ contains all

$$\neg P(0) \vee (P(S^i 0) \wedge \neg P(S^{i+1} 0)) \vee P(S^n 0), \quad i = 0, \ldots, , n-1.$$

Applying $\exists$-right rule to terms $t := S^i 0$ we get

$$\exists x(\neg P(0) \vee (P(x) \wedge \neg P(Sx)) \vee P(S^n 0))$$

from each of the formulas from Δ. Then we contract to a single formula.

example, contd

The mid-sequent is $\rightarrow \Delta$ where Δ contains all

$$\neg P(0) \vee (P(S^i 0) \wedge \neg P(S^{i+1} 0)) \vee P(S^n 0), \quad i = 0, \ldots, , n-1.$$

Applying $\exists$-right rule to terms $t := S^i 0$ we get

$$\exists x(\neg P(0) \vee (P(x) \wedge \neg P(Sx)) \vee P(S^n 0))$$

from each of the formulas from Δ. Then we contract to a single formula.

Herbrand's theorem gives us:

$$\neg P(0) \vee$$
$$(P(0) \wedge \neg P(S0)) \vee (P(S0) \wedge \neg P(SS0)) \vee (P(SS0) \wedge \neg P(SSS0)) \vee \ldots$$
$$\vee P(S^n(0))$$

The substituted terms are $0, S0, SS0, SSS0, \ldots, S^{n-1}0$.

example, contd

The mid-sequent is $\to \Delta$ where Δ contains all

$$\neg P(0) \vee (P(S^i 0) \wedge \neg P(S^{i+1} 0)) \vee P(S^n 0), \quad i = 0, \ldots, , n-1.$$

Applying $\exists$-right rule to terms $t := S^i 0$ we get

$$\exists x(\neg P(0) \vee (P(x) \wedge \neg P(Sx)) \vee P(S^n 0))$$

from each of the formulas from Δ. Then we contract to a single formula.

Herbrand's theorem gives us:

$$\neg P(0) \vee \\ (P(0) \wedge \neg P(S0)) \vee (P(S0) \wedge \neg P(SS0)) \vee (P(SS0) \wedge \neg P(SSS0)) \vee \ldots \\ \vee P(S^n(0))$$

The substituted terms are $0, S0, SS0, SSS0, \ldots, S^{n-1}0$.

Exponentially more formulas than in a proof with cuts.

$\exists\forall$ formulas

Theorem

TFAE:

1. $\exists x \forall y . \phi(x, y)$ *is logically valid,*
2. *there exist terms* $t_1, \ldots, t_n$ *such that*

$$\phi(t_1, b_1) \vee \phi(t_2(b_1), b_2) \vee \cdots \vee \phi(t_n(b_1, \ldots, b_{n-1}), b_n)$$

is a propositional tautology, where $t_i(b_1, \ldots, b_{i-1})$ *may only contain some* $b_1, \ldots, b_{i-1}$.

Interpretation: *Teacher-Student Game*

- Teacher asks student to find t such that $\forall y.\phi(t, y)$ holds true.
- Student tries t_1, Teacher gives a counterexample b_1; $\neg\phi(t_1, b_1)$
- knowing b_1, Student tries t_2, Teacher gives a counterexample b_2, $\neg\phi(t_2, b_2)$;
- etc.
- eventually, for some $i \leq n$, there is no counterexample, hence t_i is a solution.

Proof.
1. $\rightarrow$ 2. Let

$$\rightarrow \phi(t_1, b_1), \phi(t_2, b_2), \ldots, \phi(t_n, b_n)$$

be the mid-sequent of a proof of $\exists x \forall y.\phi(x, y)$.

- Let $\phi(t_n, b_n)$ be the formula to which the first $\forall$-rule is applied. Then none of $t_1, \ldots, t_n$ contains b_n. (We could apply $\forall$-rule if b_n were in t_n, but then we would not be able to apply $\exists$-rule to t_n.)
- Let $\phi(t_{n-1}, b_{n-1})$ be the formula to which the next $\forall$-rule is applied. Then none of $t_1, \ldots, t_{n-1}$ contains b_{n-1}.
- ...
- Let $\phi(t_1, b_1)$ be the formula to which the last $\forall$-rule is applied. Then t_1 does not contain any $b_1, \ldots, b_n$.

2. $\to$ 1. Write the disjunction as the sequent

$$\to \phi(t_1, b_1), \phi(t_2(b_1), b_2), \ldots, \phi(t_n(b_1, \ldots, b_{n-1}), b_n)$$

- Introduce $\forall$ for b_n, then $\exists$ for t_n,
- introduce $\forall$ for b_{n-1}, then $\exists$ for t_{n-1},
- etc.
- contract.

$\square$

the general Herbrand theorem

The previous theorem can be extended to $\forall\exists\forall\exists$ prefixes. For more complex prefixes, we do not have such a simple description.

Exercise

Do it!

the general Herbrand theorem

The previous theorem can be extended to $\forall\exists\forall\exists$ prefixes. For more complex prefixes, we do not have such a simple description.

Exercise

Do it!

Therefore we use new function symbols, Herbrand functions, to reduce a general prenex formula to an existential.

the general Herbrand theorem

Example

Consider $A := \exists x \forall y \exists z \forall u.\phi(x, y, z, u)$. *We translate* A *to*

$$He(A) \;:=\; \exists x \exists z.\phi(x, f(x), z, g(x, z))$$

where f, g *are new function symbols.*

the general Herbrand theorem

Example

Consider $A := \exists x \forall y \exists z \forall u. \phi(x, y, z, u)$. *We translate A to*

$$He(A) \ := \ \exists x \exists z. \phi(x, f(x), z, g(x, z))$$

where f, g *are new function symbols. Think of* f *and* g *as counterexamples in case A is not true.*

the general Herbrand theorem

Example

Consider $A := \exists x \forall y \exists z \forall u . \phi(x, y, z, u)$. *We translate A to*

$$He(A) \ := \ \exists x \exists z . \phi(x, f(x), z, g(x, z))$$

where f, g *are new function symbols. Think of* f *and* g *as counterexamples in case* A *is not true.*

If A *is true, no counterexample is possible, hence* $He(A)$ *is also true.*

In general, for a prenex formula A, $He(A)$ is obtained by

1. omitting all $\forall$ and
2. substituting the term $f(x_1, \ldots, x_k)$ for every y universally quantified, where f is a new function symbol and $x_1, \ldots, x_k$ are the existentially quantified variables before the universal quantifier $\forall y$.

N.B. if A starts with $\forall$, we use "nullary" function symbols, i.e., *constants.*

Theorem (Herbrand's Theorem)

Let A be a prenex sentence, let

$$He(A) := \exists x_1 \dots \exists x_k \psi(x_1, \dots, x_k).$$

(The Herbrand functions are implicit in ψ.) Then A is logically valid iff there exist terms t_{ij}, $i = 1, \dots, n$, $j = 1, \dots, m$, in the language of $He(A)$ such that

$$\bigvee_{j=1}^{m} \psi(t_{1j}, \dots, t_{nj})$$

is a propositional tautology.

Theorem (Herbrand's Theorem)

Let A be a prenex sentence, let

$$He(A) := \exists x_1 \dots \exists x_k \psi(x_1, \dots, x_k).$$

(The Herbrand functions are implicit in ψ.) Then A is logically valid iff there exist terms t_{ij}, $i = 1, \dots, n$, $j = 1, \dots, m$, in the language of $He(A)$ such that

$$\bigvee_{j=1}^{m} \psi(t_{1j}, \dots, t_{nj})$$

is a propositional tautology.

Proof.

We only need to show that $\vdash A$ iff $\vdash He(A)$.

1. One can easily show that in fact $\vdash A \to He(A)$.
2. If $\vdash He(A)$ then $\vdash A$ — see below.

□

Skolem functions

Skolem functions and $Sk(A)$ are dual to Herbrand functions and $He(A)$.

Example

$Sk(\forall x \exists y \forall z \exists u. \phi(x, y, z, u)) := \forall x \forall z. \phi(x, f(x), z, g(x, z))$.

Skolem functions

Skolem functions and $Sk(A)$ are dual to Herbrand functions and $He(A)$.

Example

$Sk(\forall x \exists y \forall z \exists u.\phi(x, y, z, u)) := \forall x \forall z.\phi(x, f(x), z, g(x, z))$.

Lemma

Let $M \models A$. Then one can extend M with functions interpreting the Skolem functions of $Sk(A)$ so that in the extended model $M' \models Sk(A)$.

Proof.

Consider the sentence above.

- For $c \in M$, define $f^M(c) = d$ by choosing some d such that $M \models \forall z \exists u \phi(c, d, z, u)$.
- For $c, d \in M$, define $g^M(c, d) = e$ by choosing some e such that $\phi(c, f(c), d, e)$.

□

Skolem functions

Skolem functions and $Sk(A)$ are dual to Herbrand functions and $He(A)$.

Example

$Sk(\forall x \exists y \forall z \exists u.\phi(x, y, z, u)) := \forall x \forall z.\phi(x, f(x), z, g(x, z))$.

Lemma

Let $M \models A$. Then one can extend M with functions interpreting the Skolem functions of $Sk(A)$ so that in the extended model $M' \models Sk(A)$.

Proof.

Consider the sentence above.

- For $c \in M$, define $f^M(c) = d$ by choosing some d such that $M \models \forall z \exists u \phi(c, d, z, u)$.
- For $c, d \in M$, define $g^M(c, d) = e$ by choosing some e such that $\phi(c, f(c), d, e)$.

□

We now prove that $\vdash \mathsf{He}(A)$ implies $\vdash A$ by proving the contrapositive implication.

We now prove that $\vdash \mathit{He}(A)$ implies $\vdash A$ by proving the contrapositive implication.

Assume $\not\vdash A$. Let $M \models \neg A$. Then $M \models \mathit{Sk}(\neg A)$. But $\vdash \mathit{Sk}(\neg A) \equiv \neg \mathit{He}(A)$. Hence $M' \models \neg \mathit{He}(A)$. $\square$