Automated Reasoning

Georg Moser

Institute of Computer Science @ UIBK

Winter 2013

Summary Last Lecture

Theorem (Model Existence Theorem)

1. *if S^* is a set of formula sets of $\mathcal{L}^+$ having the satisfaction properties, then $\forall$ formula sets $\mathcal{G} \in S^*$ of $\mathcal{L}$, $\exists$ $\mathcal{M}$, $\mathcal{M} \models \mathcal{G}$*
2. *$\forall$ elements m of $\mathcal{M}$: m denotes term in $\mathcal{L}^+$*

Definition

let $\mathcal{G}$ be a set of formulas, F a formula

- if $\exists$ a natural deduction proof from of F from finite $\mathcal{G}_0 \subseteq \mathcal{G}$, we write $\mathcal{G} \vdash F$

Theorem

first-order logic is sound and complete: $\mathcal{G} \models F \iff \mathcal{G} \vdash F$

Outline of the Lecture

Propositional Logic

short reminder of propositional logic, soundness and completeness theorem, natural deduction, propositional resolution

First Order Logic

introduction, syntax, semantics, undecidability of first-order, Löwenheim-Skolem, compactness, model existence theorem, natural deduction, completeness, sequent calculus, normalisation

Properties of First Order Logic

Craig's Interpolation Theorem, Robinson's Joint Consistency Theorem, Herbrand's Theorem

Limits and Extensions of First Order Logic

Intuitionistic Logic, Curry-Howard Isomorphism, Limits, Second-Order Logic

Outline of the Lecture

Propositional Logic

short reminder of propositional logic, soundness and completeness theorem, natural deduction, propositional resolution

First Order Logic

introduction, syntax, semantics, undecidability of first-order, Löwenheim-Skolem, compactness, model existence theorem, natural deduction, completeness, sequent calculus, normalisation

Properties of First Order Logic

Craig's Interpolation Theorem, Robinson's Joint Consistency Theorem, Herbrand's Theorem

Limits and Extensions of First Order Logic

Intuitionistic Logic, Curry-Howard Isomorphism, Limits, Second-Order Logic

Definition

- the expression $A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m$ is called a sequent
- intuitively this means $A_1 \wedge \cdots \wedge A_n \rightarrow B_1 \vee \cdots \vee B_m$

Definition

- the expression $A_1, \dots, A_n \Rightarrow B_1, \dots, B_m$ is called a sequent
- intuitively this means $A_1 \wedge \cdots \wedge A_n \rightarrow B_1 \vee \cdots \vee B_m$

Example

the following expression is a sequent

$$\exists x \mathrm{P}(x), \forall x \forall y (\mathrm{P}(x) \rightarrow \mathrm{Q}(y)) \Rightarrow \forall y \mathrm{Q}(y)$$

Definition

- the expression $A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m$ is called a sequent
- intuitively this means $A_1 \wedge \cdots \wedge A_n \to B_1 \vee \cdots \vee B_m$

Example

the following expression is a sequent

$$\exists x \mathsf{P}(x), \forall x \forall y (\mathsf{P}(x) \to \mathsf{Q}(y)) \Rightarrow \forall y \mathsf{Q}(y)$$

Definitions

- the formulas A_i, B_j are called sequent formulas; let $\Gamma = \{A_1, \ldots, A_n\}$, $\Delta = \{B_1, \ldots, B_m\}$, then Γ is the antecedent, Δ the succedent
- sequences of sequent formulas are considered as multisets
- Greek capital letters $\Gamma, \Delta, \Lambda, \ldots$ are used to denote multisets of sequent formulas

Rules of Sequent Calculus

	left	right
$\wedge$	$\dfrac{E, \Gamma \Rightarrow \Delta}{E \wedge F, \Gamma \Rightarrow \Delta}\ \wedge : \mathsf{l}$ $\dfrac{F, \Gamma \Rightarrow \Delta}{E \wedge F, \Gamma \Rightarrow \Delta}\ \wedge : \mathsf{l}$	$\dfrac{\Gamma \Rightarrow \Delta, E \quad \Gamma \Rightarrow \Delta, F}{\Gamma \Rightarrow \Delta, E \wedge F}\ \wedge : \mathsf{r}$
$\vee$	$\dfrac{E, \Gamma \Rightarrow \Delta \quad F, \Gamma \Rightarrow \Delta}{E \vee F, \Gamma \Rightarrow \Delta}\ \vee : \mathsf{l}$	$\dfrac{\Gamma \Rightarrow \Delta, E}{\Gamma \Rightarrow \Delta, E \vee F}\ \vee : \mathsf{r}$ $\dfrac{\Gamma \Rightarrow \Delta, F}{\Gamma \Rightarrow \Delta, E \vee F}\ \vee : \mathsf{r}$
$\rightarrow$	$\dfrac{\Gamma \Rightarrow \Delta, E \quad F, \Gamma \Rightarrow \Delta}{E \rightarrow F, \Gamma \Rightarrow \Delta}\ \rightarrow : \mathsf{l}$	$\dfrac{\Gamma, E \Rightarrow \Delta, F}{\Gamma \Rightarrow \Delta, E \rightarrow F}\ \rightarrow : \mathsf{l}$

Sequent Calculus (cont'd)

	left	right
$\neg$	$\dfrac{\Gamma \Rightarrow \Delta, E}{\neg E, \Gamma \Rightarrow \Delta}\ \neg\colon \mathsf{l}$	$\dfrac{E, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg E}\ \neg\colon \mathsf{r}$
$=$	$\Rightarrow t = t$	$s_1 = t_1, \ldots, s_n = t_n \Rightarrow f(\overline{s}) = f(\overline{t})$ $s_1 = t_1, \ldots, s_n = t_n \Rightarrow P(\overline{s}) = P(\overline{t})$
$\exists$	$\dfrac{F(x), \Gamma \Rightarrow \Delta}{\exists x F(x), \Gamma \Rightarrow \Delta}\ \exists\colon \mathsf{l}$	$\dfrac{\Gamma \Rightarrow \Delta, F(t)}{\Gamma \Rightarrow \Delta, \exists x F(x)}\ \exists\colon \mathsf{r}$
$\forall$	$\dfrac{F(t), \Gamma \Rightarrow \Delta}{\forall x F(x), \Gamma \Rightarrow \Delta}\ \forall\colon \mathsf{l}$	$\dfrac{\Gamma \Rightarrow \Delta, F(x)}{\Gamma \Rightarrow \Delta, \forall x F(x)}\ \forall\colon \mathsf{r}$

variable x in $\exists\colon \mathsf{l}$, $\forall\colon \mathsf{r}$ must not occur free in lower sequent
(eigenvariable condition)

Sequent Calculus Structural Rules

	left	right
axiom and cut	$A \Rightarrow A$	$\dfrac{\Gamma \Rightarrow \Delta, A \quad A, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta}$
contraction	$\dfrac{A, A, \Gamma \Rightarrow \Delta}{A, \Gamma \Rightarrow \Delta}$ c: l	$\dfrac{\Gamma \Rightarrow \Delta, A, A}{\Gamma \Rightarrow \Delta, A}$ c: r
weakening	$\dfrac{\Gamma \Rightarrow \Delta}{A, \Gamma \Rightarrow \Delta}$ w: l	$\dfrac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, A}$ w: r

Sequent Calculus Structural Rules

	left	right
axiom and cut	$A \Rightarrow A$	$\dfrac{\Gamma \Rightarrow \Delta, A \quad A, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta}$
contraction	$\dfrac{A, A, \Gamma \Rightarrow \Delta}{A, \Gamma \Rightarrow \Delta}$ c: l	$\dfrac{\Gamma \Rightarrow \Delta, A, A}{\Gamma \Rightarrow \Delta, A}$ c: r
weakening	$\dfrac{\Gamma \Rightarrow \Delta}{A, \Gamma \Rightarrow \Delta}$ w: l	$\dfrac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, A}$ w: r

Observation

we note the link between elimination (introduction) rules in natural deduction and left (right) rules in sequent calculus

Example revisited

Example

1		$\exists x \mathrm{P}(x)$	premise
2		$\forall x \forall y (\mathrm{P}(x) \rightarrow \mathrm{Q}(y))$	premise
3	y		
4	x	$\mathrm{P}(x)$	assumption
5		$\forall y (\mathrm{P}(x) \rightarrow \mathrm{Q}(y))$	$2, \forall$: e
6		$\mathrm{P}(x) \rightarrow \mathrm{Q}(y)$	$5, \forall$: e
7		$\mathrm{Q}(y)$	$4, 6, \rightarrow$: e
8		$\mathrm{Q}(y)$	$1, 4-7, \exists$: e
9		$\forall y \mathrm{Q}(y)$	$3-8, \forall$: i

Example revisited

Example

$$
\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\mathsf{P}(x) \Rightarrow \mathsf{P}(x)}{\mathsf{P}(x) \Rightarrow \mathsf{Q}(y), \mathsf{P}(x)}\ \mathsf{w}\colon \mathsf{l} \qquad \cfrac{\mathsf{Q}(y) \Rightarrow \mathsf{Q}(y)}{\mathsf{P}(x), \mathsf{Q}(y) \Rightarrow \mathsf{Q}(y)}\ \mathsf{w}\colon \mathsf{l}}{\mathsf{P}(x), \mathsf{P}(x) \rightarrow \mathsf{Q}(y) \Rightarrow \mathsf{Q}(y)}\ \rightarrow\colon \mathsf{l}}{\mathsf{P}(x), \forall y(\mathsf{P}(x) \rightarrow \mathsf{Q}(y)) \Rightarrow \mathsf{Q}(y)}\ \forall\colon \mathsf{l}}{\mathsf{P}(x), \forall x \forall y(\mathsf{P}(x) \rightarrow \mathsf{Q}(y)) \Rightarrow \mathsf{Q}(y)}\ \forall\colon \mathsf{l}}{\exists x \mathsf{P}(x), \forall x \forall y(\mathsf{P}(x) \rightarrow \mathsf{Q}(y)) \Rightarrow \mathsf{Q}(y)}\ \exists\colon \mathsf{l}}{\exists x \mathsf{P}(x), \forall x \forall y(\mathsf{P}(x) \rightarrow \mathsf{Q}(y)) \Rightarrow \forall y \mathsf{Q}(y)}\ \forall\colon \mathsf{r}}{}
$$

Normalisation

Motivation

- consider the following two abstract derivations:

$$\dfrac{\dfrac{\begin{matrix}\Pi_1 \\ E\end{matrix} \quad \begin{matrix}\Pi_2 \\ F\end{matrix}}{E \wedge F}\wedge\colon \mathrm{i}}{E}\wedge\colon \mathrm{e} \qquad\qquad\qquad \begin{matrix}\Pi_2 \\ E\end{matrix}$$

- clearly the right derivation can replace the left one
- the situation is called detour
- the rewrite step is called normalisation

Normalisation

Motivation

- consider the following two abstract derivations:

$$\dfrac{\dfrac{\begin{matrix}\Pi_1 \\ E\end{matrix} \quad \begin{matrix}\Pi_2 \\ F\end{matrix}}{E \wedge F}\ \wedge\!:\mathrm{i}}{E}\ \wedge\!:\mathrm{e} \qquad\qquad\qquad \begin{matrix}\Pi_2 \\ E\end{matrix}$$

- clearly the right derivation can replace the left one
- the situation is called detour
- the rewrite step is called normalisation

Definition

- process of eliminating all detours is called normalisation
- strong normalisation means that normalisation terminates for all possible reduction sequences

Definition (Minimal Propositional Logic)

- minimal logic contains $\bot$ as truth constant, and $\wedge$, $\vee$, $\rightarrow$
- negation is defined:
$$\neg A := A \rightarrow \bot$$
- natural deduction for minimal logic consists of:
$$\wedge : \mathsf{i}, \wedge : \mathsf{e} \quad \vee : \mathsf{i}, \vee : \mathsf{e} \quad \rightarrow : \mathsf{i}, \rightarrow : \mathsf{e}$$

Definition (Minimal Propositional Logic)

- minimal logic contains $\bot$ as truth constant, and $\wedge$, $\vee$, $\rightarrow$
- negation is defined:
$$\neg A := A \rightarrow \bot$$
- natural deduction for minimal logic consists of:
$$\wedge : \mathsf{i}, \wedge : \mathsf{e} \quad \vee : \mathsf{i}, \vee : \mathsf{e} \quad \rightarrow : \mathsf{i}, \rightarrow : \mathsf{e}$$

Lemma

- *in minimal logic* $\neg A, A \nvdash B$*;*

Definition (Minimal Propositional Logic)

- minimal logic contains $\bot$ as truth constant, and $\land$, $\lor$, $\rightarrow$
- negation is defined:
$$\neg A := A \rightarrow \bot$$
- natural deduction for minimal logic consists of:
$$\land: \mathsf{i}, \land: \mathsf{e} \quad \lor: \mathsf{i}, \lor: \mathsf{e} \quad \rightarrow: \mathsf{i}, \rightarrow: \mathsf{e}$$

Lemma

- *in minimal logic $\neg A, A \nvdash B$; minimal logic is restriction of classical logic (and also of intuitionistic logic)*

Definition (Minimal Propositional Logic)

- minimal logic contains $\bot$ as truth constant, and $\wedge$, $\vee$, $\rightarrow$
- negation is defined:

$$\neg A := A \rightarrow \bot$$

- natural deduction for minimal logic consists of:

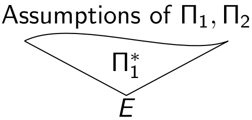
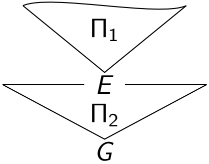
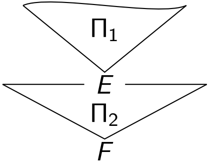
$$\wedge : \mathrm{i}, \wedge : \mathrm{e} \quad \vee : \mathrm{i}, \vee : \mathrm{e} \quad \rightarrow : \mathrm{i}, \rightarrow : \mathrm{e}$$

Lemma

- *in minimal logic $\neg A, A \nvdash B$; minimal logic is restriction of classical logic (and also of intuitionistic logic)*
- *to obtain classical logic, we may add the following proof by contradiction (PBC)*

$$\dfrac{\boxed{\begin{array}{l} \neg E \\ \vdots \\ \bot \end{array}}}{E}\ \bot$$

Immediate Reductions

	detour	*contraction*
$\wedge$	$\dfrac{\dfrac{\begin{array}{cc}\Pi_1 & \Pi_2\\ E & F\end{array}}{E \wedge F}\ \wedge:\mathrm{i}}{E}\ \wedge:\mathrm{e}$	
$\vee$	$\dfrac{\dfrac{\begin{array}{c}\Pi_1\\ E\end{array}}{E \vee F}\ \vee:\mathrm{i} \quad \begin{array}{c}\Pi_2\\ \boxed{\begin{array}{c}E\\ \vdots\\ G\end{array}}\end{array} \quad \begin{array}{c}\Pi_3\\ \boxed{\begin{array}{c}F\\ \vdots\\ G\end{array}}\end{array}}{G}\ \vee:\mathrm{e}$	
$\to$	$\dfrac{\begin{array}{c}\Pi_1\\ E\end{array} \quad \dfrac{\begin{array}{c}\Pi_2\\ \boxed{\begin{array}{c}E\\ \vdots\\ F\end{array}}\end{array}}{E \to F}\ \to:\mathrm{i}}{F}\ \to:\mathrm{e}$	

(Strong) Normalisation Theorem

Definitions

- Π is immediately reduced to Ψ, if Ψ is obtained by an immediate reduction

(Strong) Normalisation Theorem

Definitions

- Π is immediately reduced to Ψ, if Ψ is obtained by an immediate reduction
- a sequence of immediate reduction steps is a reduction

(Strong) Normalisation Theorem

Definitions

- Π is immediately reduced to Ψ, if Ψ is obtained by an immediate reduction
- a sequence of immediate reduction steps is a reduction
- a proof is normal, if it has no immediate reduction

(Strong) Normalisation Theorem

Definitions

- Π is immediately reduced to Ψ, if Ψ is obtained by an immediate reduction
- a sequence of immediate reduction steps is a reduction
- a proof is normal, if it has no immediate reduction
- a reduction sequence is a sequence of proofs $\Pi_1, \dots, \Pi_n$, such that Π_{i+1} is an immediate reduct of Π_i and Π_n is normal

(Strong) Normalisation Theorem

Definitions

- Π is immediately reduced to Ψ, if Ψ is obtained by an immediate reduction
- a sequence of immediate reduction steps is a reduction
- a proof is normal, if it has no immediate reduction
- a reduction sequence is a sequence of proofs $\Pi_1, \dots, \Pi_n$, such that Π_{i+1} is an immediate reduct of Π_i and Π_n is normal

Theorem (Normalisation and Strong Normalisation)

let Π be a proof in minimal logic

1. $\exists$ *a reduction sequence* $\Pi = \Pi_1, \dots, \Pi_n$
2. $\exists$ *computable upper bound n on the maximal length of any reduction sequence*

Normalisation in General

Theorem (Gentzen, Prawitz)

let Π be a proof in intuitionistic logic; then Π reduces to a normal proof Ψ and any reduction sequence terminates

Normalisation in General

Theorem (Gentzen, Prawitz)

let Π be a proof in intuitionistic logic; then Π reduces to a normal proof Ψ and any reduction sequence terminates

Theorem (Stalmarck)

let Π be a proof in classical logic; then Π reduces to a normal proof Ψ and any reduction sequence terminates

Normalisation in General

Theorem (Gentzen, Prawitz)

let Π be a proof in intuitionistic logic; then Π reduces to a normal proof Ψ and any reduction sequence terminates

Theorem (Stalmarck)

let Π be a proof in classical logic; then Π reduces to a normal proof Ψ and any reduction sequence terminates

Facts

- normalisation or strong normalisation theorem holds for many many logics
- normalisation in natural deduction corresponds to cut-elimination in sequent calculus

Consistency Proofs

Lemma (Subformula Property)

let Π be a normal proof of A, any formula B in Π fulfils one of the following assertions:

1. *B is a subformula of A*
2. *B is (closed) assumption of PBC; $B = \neg C$ and C is a subformula of A*
3. *$B = \perp$ and is used as result of PBC*

Consistency Proofs

Lemma (Subformula Property)

let Π be a normal proof of A, any formula B in Π fulfils one of the following assertions:

1. *B is a subformula of A*
2. *B is (closed) assumption of PBC; $B = \neg C$ and C is a subformula of A*
3. *$B = \perp$ and is used as result of PBC*

Corollary

$\neg\ \exists$ *normal derivation of* $\perp$

Craig's Interpolation Theorem

Lemma

if sentence $A \to C$ holds, $\exists$ sentence B such that

1. $A \to B$ *and* $B \to C$
2. *all axioms in B occur in both A and C*

Craig's Interpolation Theorem

Lemma

if sentence $A \to C$ holds, $\exists$ sentence B such that

1. $A \to B$ *and* $B \to C$
2. *all constants in* B *occur in both* A *and* C

Craig's Interpolation Theorem

Lemma

if sentence $A \rightarrow C$ holds, $\exists$ sentence B such that

1. $A \rightarrow B$ *and* $B \rightarrow C$
2. *all constants in B occur in both A and C*

Example

consider $\underbrace{\exists x F(x) \wedge \exists x \neg F(x)}_{A} \rightarrow \underbrace{\exists x \exists y \; x \neq y}_{C}$ but $\neg \exists$ interpolant B

Craig's Interpolation Theorem

Lemma

if sentence $A \rightarrow C$ holds, $\exists$ sentence B such that

1. $A \rightarrow B$ *and* $B \rightarrow C$
2. *all constants in B occur in both A and C*

Example

consider $\underbrace{\exists x F(x) \wedge \exists x \neg F(x)}_{A} \rightarrow \underbrace{\exists x \exists y\ x \neq y}_{C}$ but $\neg\ \exists$ interpolant B

Theorem

if sentence $A \rightarrow C$ holds, $\exists$ sentence B such that

1. $A \rightarrow B$ *and* $B \rightarrow C$
2. *all nonlogical constants in B occur in both A and C*

Proof of Craig's Interpolation Theorem

Degnerated Cases

- suppose A is unsatisfiable:

  use $\exists x\ x \neq x$ as interpolant

- suppose C is valid:

  use $\exists x\ x = x$ as interpolant

Proof of Craig's Interpolation Theorem

Degnerated Cases

- suppose A is unsatisfiable:

$$\text{use } \bot \text{ as interpolant}$$

- suppose C is valid:

$$\text{use } \top \text{ as interpolant}$$

Proof of Craig's Interpolation Theorem

Degnerated Cases

- suppose A is unsatisfiable:

$$\text{use } \bot \text{ as interpolant}$$

- suppose C is valid:

$$\text{use } \top \text{ as interpolant}$$

Definitions

- $\mathcal{L}$ contains all the nonlogical symbols occurring in both A and C and its extension $\mathcal{L}^+$ contains infinitely many individual constants

Proof of Craig's Interpolation Theorem

Degnerated Cases

- suppose A is unsatisfiable:

  use $\bot$ as interpolant

- suppose C is valid:

  use $\top$ as interpolant

Definitions

- $\mathcal{L}$ contains all the nonlogical symbols occurring in both A and C and its extension $\mathcal{L}^+$ contains infinitely many individual constants
- set of sentences $\mathcal{G}$ (of $\mathcal{L}^+$) are *A-sentences* if all sentences in $\mathcal{G}$ contain only predicate constants that occur in A

Proof of Craig's Interpolation Theorem

Degnerated Cases

- suppose A is unsatisfiable:

  use $\bot$ as interpolant

- suppose C is valid:

  use $\top$ as interpolant

Definitions

- $\mathcal{L}$ contains all the nonlogical symbols occurring in both A and C and its extension $\mathcal{L}^+$ contains infinitely many individual constants
- set of sentences $\mathcal{G}$ (of $\mathcal{L}^+$) are A-sentences if all sentences in $\mathcal{G}$ contain only predicate constants that occur in A
- set of sentences $\mathcal{G}$ (of $\mathcal{L}^+$) are C-sentences if all sentences in $\mathcal{G}$ contain only predicate constants that occur in C

Definition

a pair of set of sentences $(\mathcal{G}_1, \mathcal{G}_2)$ is barred by B if

1. $\mathcal{G}_1$ are satisfiable A-sentences, $\mathcal{G}_2$ are satisfiable C-sentences
2. B is both an A-sentence and a C-sentence
3. $\mathcal{G}_1 \models B$ and $\mathcal{G}_2 \models \neg B$

Definition

a pair of set of sentences $(\mathcal{G}_1, \mathcal{G}_2)$ is barred by B if

1. $\mathcal{G}_1$ are satisfiable A-sentences, $\mathcal{G}_2$ are satisfiable C-sentences
2. B is both an A-sentence and a C-sentence
3. $\mathcal{G}_1 \models B$ and $\mathcal{G}_2 \models \neg B$

Example

suppose $A \to C$ is valid, doesn't contain function constant, but there is no interpolant B; then no sentence B bars $(\{A\}, \{\neg C\})$

Definition

a pair of set of sentences $(\mathcal{G}_1, \mathcal{G}_2)$ is barred by B if

1. $\mathcal{G}_1$ are satisfiable A-sentences, $\mathcal{G}_2$ are satisfiable C-sentences
2. B is both an A-sentence and a C-sentence
3. $\mathcal{G}_1 \models B$ and $\mathcal{G}_2 \models \neg B$

Example

suppose $A \rightarrow C$ is valid, doesn't contain function constant, but there is no interpolant B; then no sentence B bars $(\{A\}, \{\neg C\})$

Definition

a sets of sentences $\mathcal{G}$ admits unbarred division, if

1. $\exists$ pair $(\mathcal{G}_1, \mathcal{G}_2)$ of A-sentences and C-sentences
2. $\mathcal{G} = \mathcal{G}_1 \cup \mathcal{G}_2$, $\mathcal{G}_1$ and $\mathcal{G}_2$ are satisfiable
3. no sentence bars $\mathcal{G}_1, \mathcal{G}_2$

Proof of Craig's Interpolation Theorem (no $=$, no functions).

1. assume $\neg\,\exists$ interpolant B

Proof of Craig's Interpolation Theorem (no $=$, no functions).

1. assume $\neg\,\exists$ interpolant B
2. define collection S of sets of sentences such that $\{A, \neg C\} \in S$ and S will fulfil the satisfaction properties

Proof of Craig's Interpolation Theorem (no $=$, no functions).

1. assume $\neg\,\exists$ interpolant B
2. define collection S of sets of sentences such that $\{A, \neg C\} \in S$ and S will fulfil the satisfaction properties
3. $S =$ collection of sentences $\mathcal{G}$ that admit an unbarred division

Proof of Craig's Interpolation Theorem (no $=$, no functions).

1. assume $\neg\ \exists$ interpolant B
2. define collection S of sets of sentences such that $\{A, \neg C\} \in S$ and S will fulfil the satisfaction properties
3. $S =$ collection of sentences $\mathcal{G}$ that admit an unbarred division
4. verify that S admits the satisfaction properties, wlog we only show

   let $\mathcal{G} \in S$, if $(E \vee F) \in \mathcal{G}$, then either $\mathcal{G} \cup \{E\} \in S$ or $\mathcal{G} \cup \{F\} \in S$

Proof of Craig's Interpolation Theorem (no $=$, no functions).

1. assume $\neg\,\exists$ interpolant B
2. define collection S of sets of sentences such that $\{A, \neg C\} \in S$ and S will fulfil the satisfaction properties
3. $S =$ collection of sentences $\mathcal{G}$ that admit an unbarred division
4. verify that S admits the satisfaction properties, wlog we only show

   let $\mathcal{G} \in S$, if $(E \vee F) \in \mathcal{G}$, then either $\mathcal{G} \cup \{E\} \in S$ or $\mathcal{G} \cup \{F\} \in S$
5. $\exists\ (\mathcal{G}_1, \mathcal{G}_2)$ such that $\mathcal{G} = \mathcal{G}_1 \cup \mathcal{G}_2$ and $(\mathcal{G}_1, \mathcal{G}_2)$ is unbarred

Proof of Craig's Interpolation Theorem (no $=$, no functions).

1. assume $\neg\,\exists$ interpolant B
2. define collection S of sets of sentences such that $\{A, \neg C\} \in S$ and S will fulfil the satisfaction properties
3. $S =$ collection of sentences $\mathcal{G}$ that admit an unbarred division
4. verify that S admits the satisfaction properties, wlog we only show

   let $\mathcal{G} \in S$, if $(E \vee F) \in \mathcal{G}$, then either $\mathcal{G} \cup \{E\} \in S$ or $\mathcal{G} \cup \{F\} \in S$
5. $\exists\ (\mathcal{G}_1, \mathcal{G}_2)$ such that $\mathcal{G} = \mathcal{G}_1 \cup \mathcal{G}_2$ and $(\mathcal{G}_1, \mathcal{G}_2)$ is unbarred
6. wlog $(E \vee F) \in \mathcal{G}_1$

Proof of Craig's Interpolation Theorem (no $=$, no functions).

1. assume $\neg\,\exists$ interpolant B
2. define collection S of sets of sentences such that $\{A, \neg C\} \in S$ and S will fulfil the satisfaction properties
3. $S =$ collection of sentences $\mathcal{G}$ that admit an unbarred division
4. verify that S admits the satisfaction properties, wlog we only show

   let $\mathcal{G} \in S$, if $(E \vee F) \in \mathcal{G}$, then either $\mathcal{G} \cup \{E\} \in S$ or $\mathcal{G} \cup \{F\} \in S$
5. $\exists\ (\mathcal{G}_1, \mathcal{G}_2)$ such that $\mathcal{G} = \mathcal{G}_1 \cup \mathcal{G}_2$ and $(\mathcal{G}_1, \mathcal{G}_2)$ is unbarred
6. wlog $(E \vee F) \in \mathcal{G}_1$
7. it suffices to show that $(\mathcal{G}_1 \cup \{E\}, \mathcal{G}_2)$ or $(\mathcal{G}_1 \cup \{F\}, \mathcal{G}_2)$ forms an unbarred division of $\mathcal{G} \cup \{E\} \in S$

Proof of Craig's Interpolation Theorem (no $=$, no functions).

1. assume $\neg\,\exists$ interpolant B
2. define collection S of sets of sentences such that $\{A, \neg C\} \in S$ and S will fulfil the satisfaction properties
3. $S =$ collection of sentences $\mathcal{G}$ that admit an unbarred division
4. verify that S admits the satisfaction properties, wlog we only show

   let $\mathcal{G} \in S$, if $(E \vee F) \in \mathcal{G}$, then either $\mathcal{G} \cup \{E\} \in S$ or $\mathcal{G} \cup \{F\} \in S$
5. $\exists\ (\mathcal{G}_1, \mathcal{G}_2)$ such that $\mathcal{G} = \mathcal{G}_1 \cup \mathcal{G}_2$ and $(\mathcal{G}_1, \mathcal{G}_2)$ is unbarred
6. wlog $(E \vee F) \in \mathcal{G}_1$
7. it suffices to show that $(\mathcal{G}_1 \cup \{E\}, \mathcal{G}_2)$ or $(\mathcal{G}_1 \cup \{F\}, \mathcal{G}_2)$ forms an unbarred division of $\mathcal{G} \cup \{E\} \in S$
8. wlog $\mathcal{G}_1 \cup \{E\}$ and $\mathcal{G}_1 \cup \{F\}$ are satisfiable

Proof of Craig's Interpolation Theorem (no $=$, no functions).

1. assume $\neg \exists$ interpolant B
2. define collection S of sets of sentences such that $\{A, \neg C\} \in S$ and S will fulfil the satisfaction properties
3. $S =$ collection of sentences $\mathcal{G}$ that admit an unbarred division
4. verify that S admits the satisfaction properties, wlog we only show

   let $\mathcal{G} \in S$, if $(E \vee F) \in \mathcal{G}$, then either $\mathcal{G} \cup \{E\} \in S$ or $\mathcal{G} \cup \{F\} \in S$
5. $\exists$ $(\mathcal{G}_1, \mathcal{G}_2)$ such that $\mathcal{G} = \mathcal{G}_1 \cup \mathcal{G}_2$ and $(\mathcal{G}_1, \mathcal{G}_2)$ is unbarred
6. wlog $(E \vee F) \in \mathcal{G}_1$
7. it suffices to show that $(\mathcal{G}_1 \cup \{E\}, \mathcal{G}_2)$ or $(\mathcal{G}_1 \cup \{F\}, \mathcal{G}_2)$ forms an unbarred division of $\mathcal{G} \cup \{E\} \in S$
8. wlog $\mathcal{G}_1 \cup \{E\}$ and $\mathcal{G}_1 \cup \{F\}$ are satisfiable
9. assume further both alternatives fail to be unbarred divisions; then we derive a contradiction that $\mathcal{G}$ admits an unbarred division

Proof of Craig's Interpolation Theorem (no $=$, no functions).

1. assume $\neg\,\exists$ interpolant B
2. define collection S of sets of sentences such that $\{A, \neg C\} \in S$ and S will fulfil the satisfaction properties
3. $S =$ collection of sentences $\mathcal{G}$ that admit an unbarred division
4. verify that S admits the satisfaction properties, wlog we only show

   let $\mathcal{G} \in S$, if $(E \vee F) \in \mathcal{G}$, then either $\mathcal{G} \cup \{E\} \in S$ or $\mathcal{G} \cup \{F\} \in S$
5. $\exists\ (\mathcal{G}_1, \mathcal{G}_2)$ such that $\mathcal{G} = \mathcal{G}_1 \cup \mathcal{G}_2$ and $(\mathcal{G}_1, \mathcal{G}_2)$ is unbarred
6. wlog $(E \vee F) \in \mathcal{G}_1$
7. it suffices to show that $(\mathcal{G}_1 \cup \{E\}, \mathcal{G}_2)$ or $(\mathcal{G}_1 \cup \{F\}, \mathcal{G}_2)$ forms an unbarred division of $\mathcal{G} \cup \{E\} \in S$
8. wlog $\mathcal{G}_1 \cup \{E\}$ and $\mathcal{G}_1 \cup \{F\}$ are satisfiable
9. assume further both alternatives fail to be unbarred divisions; then we derive a contradiction that $\mathcal{G}$ admits an unbarred division

Recall: Application Program Analysis

- abstract interpretations represent the behaviour of programs
- logical products of interpretations allows combination of interpreters
- based on Nelson-Oppen methodology

Recall: Application Program Analysis

- abstract interpretations represent the behaviour of programs
- logical products of interpretations allows combination of interpreters
- based on Nelson-Oppen methodology

Observation

the Nelson-Oppen method allows to combining decision procedures of different theories S, T to obtain a decision procedure for $S \cup T$

Recall: Application Program Analysis

- abstract interpretations represent the behaviour of programs
- logical products of interpretations allows combination of interpreters
- based on Nelson-Oppen methodology

Observation

the Nelson-Oppen method allows to combining decision procedures of different theories S, T to obtain a decision procedure for $S \cup T$

Definition

- a theory in a language $\mathcal{L}$ is a set of sentences of $\mathcal{L}$ that is closed under logical consequence

Recall: Application Program Analysis

- abstract interpretations represent the behaviour of programs
- logical products of interpretations allows combination of interpreters
- based on Nelson-Oppen methodology

Observation

the Nelson-Oppen method allows to combining decision procedures of different theories S, T to obtain a decision procedure for $S \cup T$

Definition

- a theory in a language $\mathcal{L}$ is a set of sentences of $\mathcal{L}$ that is closed under logical consequence
- an element of a theory is a theorem

Recall: Application Program Analysis

- abstract interpretations represent the behaviour of programs
- logical products of interpretations allows combination of interpreters
- based on Nelson-Oppen methodology

Observation

the Nelson-Oppen method allows to combining decision procedures of different theories S, T to obtain a decision procedure for $S \cup T$

Definition

- a theory in a language $\mathcal{L}$ is a set of sentences of $\mathcal{L}$ that is closed under logical consequence
- an element of a theory is a theorem
- a theory T is satisfiable if the set of sentences T is satisfiable

Robinson's Joint Consistency Theorem

Definition

- a theory T is complete if $\forall$ sentence F of $\mathcal{L}$: $F \in T$ or $\neg F \in T$

Robinson's Joint Consistency Theorem

Definition

- a theory T is complete if $\forall$ sentence F of $\mathcal{L}$: $F \in T$ or $\neg F \in T$
- T' is an extension of theory T, if $T \subseteq T'$

Robinson's Joint Consistency Theorem

Definition

- a theory T is complete if $\forall$ sentence F of $\mathcal{L}$: $F \in T$ or $\neg F \in T$
- T' is an extension of theory T, if $T \subseteq T'$
- an extension T' of T is conservative
  if any $A \in T'$ of the language of T, is a theorem of T

Robinson's Joint Consistency Theorem

Definition

- a theory T is complete if $\forall$ sentence F of $\mathcal{L}$: $F \in T$ or $\neg F \in T$
- T' is an extension of theory T, if $T \subseteq T'$
- an extension T' of T is conservative
  if any $A \in T'$ of the language of T, is a theorem of T

Lemma

the union $S \cup T$ of two theories S and T is satisfiable iff there is no sentence in S whose negation is in T

Robinson's Joint Consistency Theorem

Definition

- a theory T is complete if $\forall$ sentence F of $\mathcal{L}$: $F \in T$ or $\neg F \in T$
- T' is an extension of theory T, if $T \subseteq T'$
- an extension T' of T is conservative
  if any $A \in T'$ of the language of T, is a theorem of T

Lemma

the union $S \cup T$ of two theories S and T is satisfiable iff there is no sentence in S whose negation is in T

Definitions

- $\mathcal{L}_0$, $\mathcal{L}_1$, $\mathcal{L}_2$ are languages such that $\mathcal{L}_0 = \mathcal{L}_1 \cap \mathcal{L}_2$
- T_i is theory in $\mathcal{L}_i$ $(i \in \{0, 1, 2\})$

Theorem

if T_1, T_2 are conservative extensions of T_0, then T_3 is a conservative extension of T_0, where $T_3 = \{A \mid T_1 \cup T_2 \models A\}$

Theorem

if T_1, T_2 are conservative extensions of T_0, then T_3 is a conservative extension of T_0, where $T_3 = \{A \mid T_1 \cup T_2 \models A\}$

Proof.

1. suppose A is a sentence of $\mathcal{L}_0$ that is a theorem of T_3

Theorem

if T_1, T_2 are conservative extensions of T_0, then T_3 is a conservative extension of T_0, where $T_3 = \{A \mid T_1 \cup T_2 \models A\}$

Proof.

1. suppose A is a sentence of $\mathcal{L}_0$ that is a theorem of T_3
2. set $U_2 := \{B \mid T_2 \cup \{\neg A\} \models B\}$

Theorem

if T_1, T_2 are conservative extensions of T_0, then T_3 is a conservative extension of T_0, where $T_3 = \{A \mid T_1 \cup T_2 \models A\}$

Proof.

1. suppose A is a sentence of $\mathcal{L}_0$ that is a theorem of T_3
2. set $U_2 := \{B \mid T_2 \cup \{\neg A\} \models B\}$
3. $T_1 \cup U_2$ is unsatisfiable; by the lemma $\exists\ C \in T_1$ such that $\neg C \in U_2$

Theorem

if T_1, T_2 are conservative extensions of T_0, then T_3 is a conservative extension of T_0, where $T_3 = \{A \mid T_1 \cup T_2 \models A\}$

Proof.

1. suppose A is a sentence of $\mathcal{L}_0$ that is a theorem of T_3
2. set $U_2 := \{B \mid T_2 \cup \{\neg A\} \models B\}$
3. $T_1 \cup U_2$ is unsatisfiable; by the lemma $\exists\ C \in T_1$ such that $\neg C \in U_2$
4. C, $\neg C$ are sentences of $\mathcal{L}_0$

Theorem

if T_1, T_2 are conservative extensions of T_0, then T_3 is a conservative extension of T_0, where $T_3 = \{A \mid T_1 \cup T_2 \models A\}$

Proof.

1. suppose A is a sentence of $\mathcal{L}_0$ that is a theorem of T_3
2. set $U_2 := \{B \mid T_2 \cup \{\neg A\} \models B\}$
3. $T_1 \cup U_2$ is unsatisfiable; by the lemma $\exists\ C \in T_1$ such that $\neg C \in U_2$
4. C, $\neg C$ are sentences of $\mathcal{L}_0$
5. $\neg A \to \neg C \in \mathcal{L}_0$

Theorem

if T_1, T_2 are conservative extensions of T_0, then T_3 is a conservative extension of T_0, where $T_3 = \{A \mid T_1 \cup T_2 \models A\}$

Proof.

1. suppose A is a sentence of $\mathcal{L}_0$ that is a theorem of T_3
2. set $U_2 := \{B \mid T_2 \cup \{\neg A\} \models B\}$
3. $T_1 \cup U_2$ is unsatisfiable; by the lemma $\exists\ C \in T_1$ such that $\neg C \in U_2$
4. C, $\neg C$ are sentences of $\mathcal{L}_0$
5. $\neg A \to \neg C \in \mathcal{L}_0$
6. by assumption C is a theorem of T_0

Theorem

if T_1, T_2 are conservative extensions of T_0, then T_3 is a conservative extension of T_0, where $T_3 = \{A \mid T_1 \cup T_2 \models A\}$

Proof.

1. suppose A is a sentence of $\mathcal{L}_0$ that is a theorem of T_3
2. set $U_2 := \{B \mid T_2 \cup \{\neg A\} \models B\}$
3. $T_1 \cup U_2$ is unsatisfiable; by the lemma $\exists\, C \in T_1$ such that $\neg C \in U_2$
4. C, $\neg C$ are sentences of $\mathcal{L}_0$
5. $\neg A \to \neg C \in \mathcal{L}_0$
6. by assumption C is a theorem of T_0
7. moreover $\neg A \to \neg C \in T_2$ thus a theorem of T_0

Theorem

if T_1, T_2 are conservative extensions of T_0, then T_3 is a conservative extension of T_0, where $T_3 = \{A \mid T_1 \cup T_2 \models A\}$

Proof.

1. suppose A is a sentence of $\mathcal{L}_0$ that is a theorem of T_3
2. set $U_2 := \{B \mid T_2 \cup \{\neg A\} \models B\}$
3. $T_1 \cup U_2$ is unsatisfiable; by the lemma $\exists\ C \in T_1$ such that $\neg C \in U_2$
4. C, $\neg C$ are sentences of $\mathcal{L}_0$
5. $\neg A \to \neg C \in \mathcal{L}_0$
6. by assumption C is a theorem of T_0
7. moreover $\neg A \to \neg C \in T_2$ thus a theorem of T_0
8. this yields that A is theorem of T_0

∎

Robinson's Joint Consistency Theorem

Corollary

if T_0 is complete and T_1, T_2 are satisfiable extensions of T_0, then $T_1 \cup T_2$ is satisfiable

Robinson's Joint Consistency Theorem

Corollary

if T_0 is complete and T_1, T_2 are satisfiable extensions of T_0, then $T_1 \cup T_2$ is satisfiable

Proof.

1. a satisfiable extension of a complete theory T is conservative

Robinson's Joint Consistency Theorem

Corollary

if T_0 is complete and T_1, T_2 are satisfiable extensions of T_0, then $T_1 \cup T_2$ is satisfiable

Proof.

1. a satisfiable extension of a complete theory T is conservative
2. a conservative extension of a satisfiable theory is satisfiable

Robinson's Joint Consistency Theorem

Corollary

if T_0 is complete and T_1, T_2 are satisfiable extensions of T_0, then $T_1 \cup T_2$ is satisfiable

Proof.

1. a satisfiable extension of a complete theory T is conservative
2. a conservative extension of a satisfiable theory is satisfiable
3. set $T_3 = \{A \mid T_1 \cup T_2 \models A\}$

Robinson's Joint Consistency Theorem

Corollary

if T_0 is complete and T_1, T_2 are satisfiable extensions of T_0, then $T_1 \cup T_2$ is satisfiable

Proof.

1. a satisfiable extension of a complete theory T is conservative
2. a conservative extension of a satisfiable theory is satisfiable
3. set $T_3 = \{A \mid T_1 \cup T_2 \models A\}$
4. by assumption (and the above) T_1, T_2 are conservative

Robinson's Joint Consistency Theorem

Corollary

if T_0 is complete and T_1, T_2 are satisfiable extensions of T_0, then $T_1 \cup T_2$ is satisfiable

Proof.

1. a satisfiable extension of a complete theory T is conservative
2. a conservative extension of a satisfiable theory is satisfiable
3. set $T_3 = \{A \mid T_1 \cup T_2 \models A\}$
4. by assumption (and the above) T_1, T_2 are conservative
5. by previous theorem T_3 is conservative extension of T_0

Robinson's Joint Consistency Theorem

Corollary

if T_0 is complete and T_1, T_2 are satisfiable extensions of T_0, then $T_1 \cup T_2$ is satisfiable

Proof.

1. a satisfiable extension of a complete theory T is conservative
2. a conservative extension of a satisfiable theory is satisfiable
3. set $T_3 = \{A \mid T_1 \cup T_2 \models A\}$
4. by assumption (and the above) T_1, T_2 are conservative
5. by previous theorem T_3 is conservative extension of T_0
6. by the above T_3 is satisfiable, hence $T_1 \cup T_2$ is satisfiable

∎

Outline of the Lecture

Propositional Logic

short reminder of propositional logic, soundness and completeness theorem, natural deduction, propositional resolution

First Order Logic

introduction, syntax, semantics, undecidability of first-order, Löwenheim-Skolem, compactness, model existence theorem, natural deduction, completeness, sequent calculus, normalisation

Properties of First Order Logic

Craig's Interpolation Theorem, Robinson's Joint Consistency Theorem, Herbrand's Theorem

Limits and Extensions of First Order Logic

Intuitionistic Logic, Curry-Howard Isomorphism, Limits, Second-Order Logic

Outline of the Lecture

Propositional Logic

short reminder of propositional logic, soundness and completeness theorem, natural deduction, propositional resolution

First Order Logic

introduction, syntax, semantics, undecidability of first-order, Löwenheim-Skolem, compactness, model existence theorem, natural deduction, completeness, sequent calculus, normalisation

Properties of First Order Logic

Craig's Interpolation Theorem, Robinson's Joint Consistency Theorem, Herbrand's Theorem

Limits and Extensions of First Order Logic

Intuitionistic Logic, Curry-Howard Isomorphism, Limits, Second-Order Logic

Definition (Prenex Normal Form)

1. a formula F is in prenex normal form if it has the form

$$Q_1 x_1 \cdots Q_n x_n \underbrace{G}_{\text{matrix}} \qquad\qquad Q_i \in \{\forall, \exists\}$$

   G is quantifier-free

Definition (Prenex Normal Form)

1. a formula F is in prenex normal form if it has the form

$$Q_1 x_1 \cdots Q_n x_n \underbrace{G}_{\text{matrix}} \qquad\qquad Q_i \in \{\forall, \exists\}$$

   G is quantifier-free

2. if G is a conjunction of disjunctions of literals, we say F is in conjunctive prenex normal form (CNF for short)

Definition (Prenex Normal Form)

1. a formula F is in prenex normal form if it has the form

$$\mathsf{Q}_1 x_1 \cdots \mathsf{Q}_n x_n \underbrace{G}_{\text{matrix}} \qquad\qquad \mathsf{Q}_i \in \{\forall, \exists\}$$

   G is quantifier-free

2. if G is a conjunction of disjunctions of literals, we say F is in conjunctive prenex normal form (CNF for short)

Example

consider $\forall x F(x) \leftrightarrow G(a)$ or more precisely

$$(\neg\forall x F(x) \vee G(a)) \wedge (\neg G(a) \vee \forall x F(x))$$

one CNF would be

$$\forall x \exists y((\neg F(y) \vee G(a)) \wedge (\neg G(a) \vee F(x)))$$

Theorem

$\forall$ first-order formula F, $\exists$ G such that G is in prenex normal form and $F \equiv G$; furthermore G can be effectively constructed from F

Theorem

$\forall$ first-order formula F, $\exists$ G such that G is in prenex normal form and $F \equiv G$; furthermore G can be effectively constructed from F

Proof.

use the following operations

Theorem

$\forall$ first-order formula F, $\exists$ G such that G is in prenex normal form and $F \equiv G$; furthermore G can be effectively constructed from F

Proof.

use the following operations

1. rename bound variables such that each quantifier introduces a unique bound variable

Theorem

$\forall$ *first-order formula* F, $\exists$ G *such that* G *is in prenex normal form and* $F \equiv G$; *furthermore* G *can be effectively constructed from* F

Proof.

use the following operations

1. rename bound variables such that each quantifier introduces a unique bound variable
2. replace $E \to F$ by $\neg E \vee F$

Theorem

$\forall$ first-order formula F, $\exists$ G such that G is in prenex normal form and $F \equiv G$; furthermore G can be effectively constructed from F

Proof.

use the following operations

1. rename bound variables such that each quantifier introduces a unique bound variable
2. replace $E \to F$ by $\neg E \vee F$
3. pull quantifiers out using

$$\neg\forall x F(x) \equiv \exists x \neg F(x)$$
$$\neg\exists x F(x) \equiv \forall x \neg F(x)$$
$$\mathsf{Q} x E(x) \odot F \equiv \mathsf{Q} x (E(x) \odot F)$$

where $\mathsf{Q} \in \{\forall, \exists\}$, $\odot \in \{\wedge, \vee\}$ and x not free in F

Theorem

$\forall$ first-order formula F, $\exists$ G such that G is in prenex normal form and $F \equiv G$; furthermore G can be effectively constructed from F

Proof.

use the following operations

1. rename bound variables such that each quantifier introduces a unique bound variable
2. replace $E \to F$ by $\neg E \vee F$
3. pull quantifiers out using

$$\neg \forall x F(x) \equiv \exists x \neg F(x)$$
$$\neg \exists x F(x) \equiv \forall x \neg F(x)$$
$$\mathsf{Q} x E(x) \odot F \equiv \mathsf{Q} x (E(x) \odot F)$$

where $\mathsf{Q} \in \{\forall, \exists\}$, $\odot \in \{\wedge, \vee\}$ and x not free in F

Definition

- an existential formula F is of form $\exists x_1 \cdots \exists x_m\ G(x_1, \dots, x_m)$

such that G is quantifier free

Definition

- an existential formula F is of form $\exists x_1 \cdots \exists x_m \; G(x_1, \dots, x_m)$
- a universal formula is of form $\forall x_1 \cdots \forall x_m \; G(x_1, \dots, x_m)$

such that G is quantifier free

Definition

- an existential formula F is of form $\exists x_1 \cdots \exists x_m \; G(x_1, \dots, x_m)$
- a universal formula is of form $\forall x_1 \cdots \forall x_m \; G(x_1, \dots, x_m)$

such that G is quantifier free

Definition (Skolem Normal Form)

a formula F is in Skolem normal form (SNF for short) if F is universal and in CNF

Definition

- an existential formula F is of form $\exists x_1 \cdots \exists x_m\ G(x_1, \ldots, x_m)$
- a universal formula is of form $\forall x_1 \cdots \forall x_m\ G(x_1, \ldots, x_m)$

such that G is quantifier free

Definition (Skolem Normal Form)

a formula F is in Skolem normal form (SNF for short) if F is universal and in CNF

let $\mathcal{L}$ be a language and $\mathcal{L}^+$ an extension of $\mathcal{L}$

Definition

- an existential formula F is of form $\exists x_1 \cdots \exists x_m\ G(x_1, \dots, x_m)$
- a universal formula is of form $\forall x_1 \cdots \forall x_m\ G(x_1, \dots, x_m)$

such that G is quantifier free

Definition (Skolem Normal Form)

a formula F is in Skolem normal form (SNF for short) if F is universal and in CNF

let $\mathcal{L}$ be a language and $\mathcal{L}^+$ an extension of $\mathcal{L}$

Definition

1. suppose $\mathcal{I}$ is an interpretation of $\mathcal{L}$ and $\mathcal{I}^+$ an interpretation of $\mathcal{L}^+$ that coincides with $\mathcal{I}$ on $\mathcal{L}$

Definition

- an existential formula F is of form $\exists x_1 \cdots \exists x_m \; G(x_1, \ldots, x_m)$
- a universal formula is of form $\forall x_1 \cdots \forall x_m \; G(x_1, \ldots, x_m)$

such that G is quantifier free

Definition (Skolem Normal Form)

a formula F is in Skolem normal form (SNF for short) if F is universal and in CNF

let $\mathcal{L}$ be a language and $\mathcal{L}^+$ an extension of $\mathcal{L}$

Definition

1. suppose $\mathcal{I}$ is an interpretation of $\mathcal{L}$ and $\mathcal{I}^+$ an interpretation of $\mathcal{L}^+$ that coincides with $\mathcal{I}$ on $\mathcal{L}$
2. then $\mathcal{I}^+$ is an expansion of $\mathcal{I}$

Definition (Skolemisation)

given a sentence F, we define its Skolemisation F^S as follows

Definition (Skolemisation)

given a sentence F, we define its Skolemisation F^S as follows

1. transform F into a CNF F'
   such that $F' = \mathsf{Q}_1 x_1 \cdots \mathsf{Q}_m x_m \; G(x_1, \ldots, , x_m)$

Definition (Skolemisation)

given a sentence F, we define its Skolemisation F^S as follows

1. transform F into a CNF F'
   such that $F' = Q_1 x_1 \cdots Q_m x_m \; G(x_1, \ldots, , x_m)$
2. set $F'' = F'$ and repeatedly transform F''

   $$\forall x_1 \cdots \forall x_{i-1} \exists x_i Q_{i+1} x_{i+1} \cdots Q_m x_m \; G(x_1, \ldots, x_i, \ldots, x_m)$$

   by $s(F'')$

   $$\forall x_1 \cdots \forall x_{i-1} Q_{i+1} x_{i+1} \cdots Q_m x_m \; G(x_1, \ldots, f(x_1, \ldots, x_{i-1}), \ldots, x_m)$$

   where f denotes a fresh function symbol of arity $i - 1$

Definition (Skolemisation)

given a sentence F, we define its Skolemisation F^S as follows

1. transform F into a CNF F'
   such that $F' = \mathsf{Q}_1 x_1 \cdots \mathsf{Q}_m x_m \; G(x_1, \dots, , x_m)$
2. set $F'' = F'$ and repeatedly transform F''

   $$\forall x_1 \cdots \forall x_{i-1} \exists x_i \mathsf{Q}_{i+1} x_{i+1} \cdots \mathsf{Q}_m x_m \; G(x_1, \dots, x_i, \dots, x_m)$$

   by $s(F'')$

   $$\forall x_1 \cdots \forall x_{i-1} \mathsf{Q}_{i+1} x_{i+1} \cdots \mathsf{Q}_m x_m \; G(x_1, \dots, f(x_1, \dots, x_{i-1}), \dots, x_m)$$

   where f denotes a fresh function symbol of arity $i - 1$

Definition

formulas F and G are equivalent for satisfiability ($F \approx G$) whenever F is satisfiable iff G is satisfiable

Theorem

$\forall$ first-order formula, F $\exists$ formula in SNF G such that $F \approx G$; furthermore G can be effectively constructed from F

Theorem

$\forall$ first-order formula, F $\exists$ formula in SNF G such that $F \approx G$; furthermore G can be effectively constructed from F

Proof.

Theorem

$\forall$ first-order formula, F $\exists$ formula in SNF G such that $F \approx G$; furthermore G can be effectively constructed from F

Proof.

- set

$$F = \forall x_1 \cdots \forall x_{i-1} \exists x_i \cdots \mathsf{Q}_m x_m \; G(x_1, \dots, x_m)$$
$$s(F) = \forall x_1 \cdots \forall x_{i-1} \cdots \mathsf{Q}_m x_m \; G(x_1, \dots, f(x_1, \dots, x_{i-1}), \dots, x_m)$$
$$H(x_1, \dots, x_i) = \mathsf{Q}_{i+1} x_{i+1} \cdots \mathsf{Q}_m x_m \; G(x_1, \dots, x_m)$$

Theorem

$\forall$ first-order formula, F $\exists$ formula in SNF G such that $F \approx G$; furthermore G can be effectively constructed from F

Proof.

- set

$$F = \forall x_1 \cdots \forall x_{i-1} \exists x_i \cdots \mathsf{Q}_m x_m \; G(x_1, \dots, x_m)$$
$$s(F) = \forall x_1 \cdots \forall x_{i-1} \cdots \mathsf{Q}_m x_m \; G(x_1, \dots, f(x_1, \dots, x_{i-1}), \dots, x_m)$$
$$H(x_1, \dots, x_i) = \mathsf{Q}_{i+1} x_{i+1} \cdots \mathsf{Q}_m x_m \; G(x_1, \dots, x_m)$$

- suppose $F = \forall x_1 \cdots \forall x_{i-1} \exists x_i H(x_1, \dots, x_i)$ is satisfiable

Theorem

$\forall$ first-order formula, F $\exists$ formula in SNF G such that $F \approx G$; furthermore G can be effectively constructed from F

Proof.

- set

$$F = \forall x_1 \cdots \forall x_{i-1} \exists x_i \cdots \mathsf{Q}_m x_m \ G(x_1, \dots, x_m)$$
$$s(F) = \forall x_1 \cdots \forall x_{i-1} \cdots \mathsf{Q}_m x_m \ G(x_1, \dots, f(x_1, \dots, x_{i-1}), \dots, x_m)$$
$$H(x_1, \dots, x_i) = \mathsf{Q}_{i+1} x_{i+1} \cdots \mathsf{Q}_m x_m \ G(x_1, \dots, x_m)$$

- suppose $F = \forall x_1 \cdots \forall x_{i-1} \exists x_i H(x_1, \dots, x_i)$ is satisfiable
- $\exists$ model $\mathcal{M}$ of F, then $\exists$ expansion $\mathcal{M}^+$ of $\mathcal{M}$ such that

$$\mathcal{M}^+ \models H(x_1, \dots, x_{i-1}, f(x_1, \dots, x_{i-1}))$$

Theorem

$\forall$ first-order formula, F $\exists$ formula in SNF G such that $F \approx G$; furthermore G can be effectively constructed from F

Proof.

- set

$$F = \forall x_1 \cdots \forall x_{i-1} \exists x_i \cdots Q_m x_m \; G(x_1, \ldots, x_m)$$
$$s(F) = \forall x_1 \cdots \forall x_{i-1} \cdots Q_m x_m \; G(x_1, \ldots, f(x_1, \ldots, x_{i-1}), \ldots, x_m)$$
$$H(x_1, \ldots, x_i) = Q_{i+1} x_{i+1} \cdots Q_m x_m \; G(x_1, \ldots, x_m)$$

- suppose $F = \forall x_1 \cdots \forall x_{i-1} \exists x_i H(x_1, \ldots, x_i)$ is satisfiable
- $\exists$ model $\mathcal{M}$ of F, then $\exists$ expansion $\mathcal{M}^+$ of $\mathcal{M}$ such that

$$\mathcal{M}^+ \models H(x_1, \ldots, x_{i-1}, f(x_1, \ldots, x_{i-1}))$$

- $\forall x_1 \cdots \forall x_{i-1} H(x_1, \ldots, f(x_1, \ldots, x_{i-1})) = s(F)$ is satisfiable

Theorem

$\forall$ first-order formula, F $\exists$ formula in SNF G such that $F \approx G$; furthermore G can be effectively constructed from F

Proof.

- set

$$F = \forall x_1 \cdots \forall x_{i-1} \exists x_i \cdots \mathsf{Q}_m x_m \; G(x_1, \dots, x_m)$$
$$s(F) = \forall x_1 \cdots \forall x_{i-1} \cdots \mathsf{Q}_m x_m \; G(x_1, \dots, f(x_1, \dots, x_{i-1}), \dots, x_m)$$
$$H(x_1, \dots, x_i) = \mathsf{Q}_{i+1} x_{i+1} \cdots \mathsf{Q}_m x_m \; G(x_1, \dots, x_m)$$

- suppose $F = \forall x_1 \cdots \forall x_{i-1} \exists x_i H(x_1, \dots, x_i)$ is satisfiable
- $\exists$ model $\mathcal{M}$ of F, then $\exists$ expansion $\mathcal{M}^+$ of $\mathcal{M}$ such that

$$\mathcal{M}^+ \models H(x_1, \dots, x_{i-1}, f(x_1, \dots, x_{i-1}))$$

- $\forall x_1 \cdots \forall x_{i-1} H(x_1, \dots, f(x_1, \dots, x_{i-1})) = s(F)$ is satisfiable

∎

Example

consider $\forall y \forall x (x > y \rightarrow \exists z (x > z \wedge z > y))$; its SNF is

$$\forall y \forall x (\neg(x > y) \vee x > \mathsf{f}(x, y)) \wedge (\neg(x > y) \vee \mathsf{f}(x, y) > y)$$

Example

consider $\forall y \forall x (x > y \rightarrow \exists z (x > z \wedge z > y))$; its SNF is

$$\forall y \forall x (\neg(x > y) \vee x > \mathsf{f}(x,y)) \wedge (\neg(x > y) \vee \mathsf{f}(x,y) > y)$$

a term t is closed if no variable occurs in t

Example

consider $\forall y \forall x (x > y \rightarrow \exists z (x > z \wedge z > y))$; its SNF is

$$\forall y \forall x (\neg(x > y) \vee x > \mathsf{f}(x,y)) \wedge (\neg(x > y) \vee \mathsf{f}(x,y) > y)$$

a term t is closed if no variable occurs in t

Definition

- a Herbrand universe for a language $\mathcal{L}$ is the set of all closed terms

Example

consider $\forall y \forall x (x > y \to \exists z (x > z \land z > y))$; its SNF is

$$\forall y \forall x (\neg(x > y) \lor x > \mathsf{f}(x,y)) \land (\neg(x > y) \lor \mathsf{f}(x,y) > y)$$

a term t is closed if no variable occurs in t

Definition

- a Herbrand universe for a language $\mathcal{L}$ is the set of all closed terms
- we add fresh constant c if $\mathcal{L}$ doesn't contain one

Example

consider $\forall y \forall x (x > y \to \exists z (x > z \land z > y))$; its SNF is

$$\forall y \forall x (\neg(x > y) \lor x > \mathsf{f}(x,y)) \land (\neg(x > y) \lor \mathsf{f}(x,y) > y)$$

a term t is closed if no variable occurs in t

Definition

- a Herbrand universe for a language $\mathcal{L}$ is the set of all closed terms
- we add fresh constant c if $\mathcal{L}$ doesn't contain one

Example

let $\mathcal{L} = \{\mathsf{c}, \mathsf{f}, \mathsf{P}\}$, then the Herbrand universe H of $\mathcal{L}$ is

$$H = \{\mathsf{c}, \mathsf{f}(\mathsf{c}), \mathsf{f}(\mathsf{f}(\mathsf{c})), \mathsf{f}(\mathsf{f}(\mathsf{f}(\mathsf{c}))), \dots\}$$

Definition

- an interpretation $\mathcal{I}$ (of $\mathcal{L}$) is Herbrand interpretation if
  1. its universe is the Herbrand universe H for $\mathcal{L}$
  2. interpretation $\mathcal{I}$ sets $t^{\mathcal{I}} = t$ for any closed term t

Definition

- an interpretation $\mathcal{I}$ (of $\mathcal{L}$) is Herbrand interpretation if
  1. its universe is the Herbrand universe H for $\mathcal{L}$
  2. interpretation $\mathcal{I}$ sets $t^{\mathcal{I}} = t$ for any closed term t
- a Herbrand interpretation $\mathcal{M}$ is a Herbrand model of a set of formulas $\mathcal{G}$ if $\mathcal{M} \models \mathcal{G}$

Definition

- an interpretation $\mathcal{I}$ (of $\mathcal{L}$) is Herbrand interpretation if
  1. its universe is the Herbrand universe H for $\mathcal{L}$
  2. interpretation $\mathcal{I}$ sets $t^{\mathcal{I}} = t$ for any closed term t
- a Herbrand interpretation $\mathcal{M}$ is a Herbrand model of a set of formulas $\mathcal{G}$ if $\mathcal{M} \models \mathcal{G}$

Example

- consider $F = \forall x \mathsf{P}(x)$ and $\mathcal{L} = \{\mathsf{c}, \mathsf{f}, \mathsf{P}\}$

Definition

- an interpretation $\mathcal{I}$ (of $\mathcal{L}$) is Herbrand interpretation if
  1. its universe is the Herbrand universe H for $\mathcal{L}$
  2. interpretation $\mathcal{I}$ sets $t^{\mathcal{I}} = t$ for any closed term t
- a Herbrand interpretation $\mathcal{M}$ is a Herbrand model of a set of formulas $\mathcal{G}$ if $\mathcal{M} \models \mathcal{G}$

Example

- consider $F = \forall x \mathsf{P}(x)$ and $\mathcal{L} = \{\mathsf{c}, \mathsf{f}, \mathsf{P}\}$
- the Herbrand model $\mathcal{M}$ interprets P as follows:

$$\begin{array}{ccc} c \in \mathsf{P}^{\mathcal{M}} & \mathsf{f}(\mathsf{c}) \in \mathsf{P}^{\mathcal{M}} & \mathsf{f}(\mathsf{f}(\mathsf{c})) \in \mathsf{P}^{\mathcal{M}} \\ \mathsf{f}(\mathsf{f}(\mathsf{f}(\mathsf{c}))) \in \mathsf{P}^{\mathcal{M}} & \mathsf{f}(\mathsf{f}(\mathsf{f}(\mathsf{f}(\mathsf{c})))) \in \mathsf{P}^{\mathcal{M}} & \dots \end{array}$$

Definition

- an interpretation $\mathcal{I}$ (of $\mathcal{L}$) is Herbrand interpretation if
  1. its universe is the Herbrand universe H for $\mathcal{L}$
  2. interpretation $\mathcal{I}$ sets $t^{\mathcal{I}} = t$ for any closed term t
- a Herbrand interpretation $\mathcal{M}$ is a Herbrand model of a set of formulas $\mathcal{G}$ if $\mathcal{M} \models \mathcal{G}$

Example

- consider $F = \forall x \mathsf{P}(x)$ and $\mathcal{L} = \{\mathsf{c}, \mathsf{f}, \mathsf{P}\}$
- the Herbrand model $\mathcal{M}$ interprets P as follows:

$$\begin{array}{ccc} c \in \mathsf{P}^{\mathcal{M}} & \mathsf{f}(\mathsf{c}) \in \mathsf{P}^{\mathcal{M}} & \mathsf{f}(\mathsf{f}(\mathsf{c})) \in \mathsf{P}^{\mathcal{M}} \\ \mathsf{f}(\mathsf{f}(\mathsf{f}(\mathsf{c}))) \in \mathsf{P}^{\mathcal{M}} & \mathsf{f}(\mathsf{f}(\mathsf{f}(\mathsf{f}(\mathsf{c})))) \in \mathsf{P}^{\mathcal{M}} & \dots \end{array}$$

- note that $\mathcal{M}$ is representable as the set of true atoms

Herbrand's Theorem

Jacques Herbrand (1908–1931) proposed to

Herbrand's Theorem

Jacques Herbrand (1908–1931) proposed to

- transform first-order into propositional logic

Herbrand's Theorem

Jacques Herbrand (1908–1931) proposed to

- transform first-order into propositional logic
- basis of Gilmore's prover

Herbrand's Theorem

Jacques Herbrand (1908–1931) proposed to

- transform first-order into propositional logic
- basis of Gilmore's prover

Corollary

$\mathcal{G}$ is satisfiable iff $\mathcal{G}$ has a Herbrand model (over $\mathcal{L}$)

Proof.

follows from the proof of completeness ∎

Herbrand's Theorem

Jacques Herbrand (1908–1931) proposed to

- transform first-order into propositional logic
- basis of Gilmore's prover

Corollary

$\mathcal{G}$ is satisfiable iff $\mathcal{G}$ has a Herbrand model (over $\mathcal{L}$)

Proof.

follows from the proof of completeness ∎

$\mathcal{G}$ a set of universal sentences (of $\mathcal{L}$) without $=$

Definition

$$\mathrm{Gr}(\mathcal{G}) = \{\, G(t_1, \ldots, t_n) \mid \forall x_1 \cdots \forall x_n G(x_1, \ldots, x_n) \in \mathcal{G},\ t_i \text{ closed terms}\}$$

Definition

$$\mathrm{Gr}(\mathcal{G}) = \{G(t_1, \ldots, t_n) \mid \forall x_1 \cdots \forall x_n G(x_1, \ldots, x_n) \in \mathcal{G}, t_i \text{ closed terms}\}$$

Theorem

the following is equivalent

1. $\mathcal{G}$ *is satisfiable*
2. $\mathcal{G}$ *has a Herbrand model*

Definition

$$\mathrm{Gr}(\mathcal{G}) = \{G(t_1, \dots, t_n) \mid \forall x_1 \cdots \forall x_n G(x_1, \dots, x_n) \in \mathcal{G}, t_i \text{ closed terms}\}$$

Theorem

the following is equivalent

1. $\mathcal{G}$ *is satisfiable*
2. $\mathcal{G}$ *has a Herbrand model*
3. $\forall$ *finite* $\mathcal{G}_0 \subseteq \mathrm{Gr}(\mathcal{G})$, $\mathcal{G}_0$ *has a Herbrand model*

Definition

$$\mathrm{Gr}(\mathcal{G}) = \{G(t_1, \ldots, t_n) \mid \forall x_1 \cdots \forall x_n G(x_1, \ldots, x_n) \in \mathcal{G}, t_i \text{ closed terms}\}$$

Theorem

the following is equivalent

1. *$\mathcal{G}$ is satisfiable*
2. *$\mathcal{G}$ has a Herbrand model*
3. *$\forall$ finite $\mathcal{G}_0 \subseteq \mathrm{Gr}(\mathcal{G})$, $\mathcal{G}_0$ has a Herbrand model*

Proof.

- $\forall$ finite $\mathcal{G}_0 \subseteq \mathrm{Gr}(\mathcal{G})$, $\mathcal{G}_0$ has a Herbrand model

Definition

$$\mathrm{Gr}(\mathcal{G}) = \{G(t_1, \dots, t_n) \mid \forall x_1 \cdots \forall x_n G(x_1, \dots, x_n) \in \mathcal{G}, t_i \text{ closed terms}\}$$

Theorem

the following is equivalent

1. *$\mathcal{G}$ is satisfiable*
2. *$\mathcal{G}$ has a Herbrand model*
3. *$\forall$ finite $\mathcal{G}_0 \subseteq \mathrm{Gr}(\mathcal{G})$, $\mathcal{G}_0$ has a Herbrand model*

Proof.

- $\forall$ finite $\mathcal{G}_0 \subseteq \mathrm{Gr}(\mathcal{G})$, $\mathcal{G}_0$ has a Herbrand model
- hence $\mathrm{Gr}(\mathcal{G})$ has a Herbrand model

Definition

$$\mathrm{Gr}(\mathcal{G}) = \{G(t_1,\ldots,t_n) \mid \forall x_1 \cdots \forall x_n G(x_1,\ldots,x_n) \in \mathcal{G}, t_i \text{ closed terms}\}$$

Theorem

the following is equivalent

1. *$\mathcal{G}$ is satisfiable*
2. *$\mathcal{G}$ has a Herbrand model*
3. *$\forall$ finite $\mathcal{G}_0 \subseteq \mathrm{Gr}(\mathcal{G})$, $\mathcal{G}_0$ has a Herbrand model*

Proof.

- $\forall$ finite $\mathcal{G}_0 \subseteq \mathrm{Gr}(\mathcal{G})$, $\mathcal{G}_0$ has a Herbrand model
- hence $\mathrm{Gr}(\mathcal{G})$ has a Herbrand model
- as $\mathcal{G}$ contains only universal sentences and by definition of a Herbrand model this implies that $\mathcal{G}$ has a Herbrand model

Definition

$$\mathrm{Gr}(\mathcal{G}) = \{G(t_1, \dots, t_n) \mid \forall x_1 \cdots \forall x_n G(x_1, \dots, x_n) \in \mathcal{G}, t_i \text{ closed terms}\}$$

Theorem

the following is equivalent

1. *$\mathcal{G}$ is satisfiable*
2. *$\mathcal{G}$ has a Herbrand model*
3. *$\forall$ finite $\mathcal{G}_0 \subseteq \mathrm{Gr}(\mathcal{G})$, $\mathcal{G}_0$ has a Herbrand model*

Proof.

- $\forall$ finite $\mathcal{G}_0 \subseteq \mathrm{Gr}(\mathcal{G})$, $\mathcal{G}_0$ has a Herbrand model
- hence $\mathrm{Gr}(\mathcal{G})$ has a Herbrand model
- as $\mathcal{G}$ contains only universal sentences and by definition of a Herbrand model this implies that $\mathcal{G}$ has a Herbrand model ∎

Corollary

$\mathcal{G}$ has a Herbrand model or $\mathcal{G}$ is unsatisfiable; in the latter case the following statements hold (and are equivalent):

1. $\exists$ *finite subset* $S \subseteq \mathrm{Gr}(\mathcal{G})$*; conjunction* $\bigwedge S$ *is unsatisfiable*
2. $\exists$ *finite subset* $S \subseteq \mathrm{Gr}(\mathcal{G})$*; disjunction* $\bigvee\{\neg A \mid A \in S\}$ *is valid*

Corollary

$\mathcal{G}$ has a Herbrand model or $\mathcal{G}$ is unsatisfiable; in the latter case the following statements hold (and are equivalent):

1. $\exists$ *finite subset* $S \subseteq \mathrm{Gr}(\mathcal{G})$*; conjunction* $\bigwedge S$ *is unsatisfiable*
2. $\exists$ *finite subset* $S \subseteq \mathrm{Gr}(\mathcal{G})$*; disjunction* $\bigvee\{\neg A \mid A \in S\}$ *is valid*

Corollary

$\exists x_1 \cdots \exists x_n G(x_1, \dots, x_n)$ *is valid iff there are ground terms* $t_1^k, \dots, t_n^k$, $k \in \mathbb{N}$ *and the following is valid*

$$G(t_1^1, \dots, t_n^1) \vee \cdots \vee G(t_1^k, \dots, t_n^k)$$

Corollary

$\mathcal{G}$ has a Herbrand model or $\mathcal{G}$ is unsatisfiable; in the latter case the following statements hold (and are equivalent):

1. $\exists$ *finite subset* $S \subseteq \mathrm{Gr}(\mathcal{G})$; *conjunction* $\bigwedge S$ *is unsatisfiable*
2. $\exists$ *finite subset* $S \subseteq \mathrm{Gr}(\mathcal{G})$; *disjunction* $\bigvee \{\neg A \mid A \in S\}$ *is valid*

Corollary

$\exists x_1 \cdots \exists x_n G(x_1, \dots, x_n)$ *is valid iff there are ground terms* $t_1^k, \dots, t_n^k$, $k \in \mathbb{N}$ *and the following is valid*

$$G(t_1^1, \dots, t_n^1) \vee \cdots \vee G(t_1^k, \dots, t_n^k)$$

transform first-order into propositional logic

Corollary

$\mathcal{G}$ has a Herbrand model or $\mathcal{G}$ is unsatisfiable; in the latter case the following statements hold (and are equivalent):

1. $\exists$ *finite subset* $S \subseteq \mathrm{Gr}(\mathcal{G})$*; conjunction* $\bigwedge S$ *is unsatisfiable*
2. $\exists$ *finite subset* $S \subseteq \mathrm{Gr}(\mathcal{G})$*; disjunction* $\bigvee\{\neg A \mid A \in S\}$ *is valid*

Corollary

$\exists x_1 \cdots \exists x_n G(x_1, \ldots, x_n)$ *is valid iff there are ground terms* $t_1^k, \ldots, t_n^k$, $k \in \mathbb{N}$ *and the following is valid*

$$G(t_1^1, \ldots, t_n^1) \lor \cdots \lor G(t_1^k, \ldots, t_n^k)$$

transform first-order into propositional logic

Definition (Gilmore's Prover)

1. F be an arbitrary sentence in language $\mathcal{L}$

Definition (Gilmore's Prover)

1. F be an arbitrary sentence in language $\mathcal{L}$
2. consider its negation $\neg F$
   wlog $\neg F = \forall x_1 \cdots \forall x_n G(x_1, \dots, x_n)$ in SNF

Definition (Gilmore's Prover)

1. F be an arbitrary sentence in language $\mathcal{L}$
2. consider its negation $\neg F$
   wlog $\neg F = \forall x_1 \cdots \forall x_n G(x_1, \dots, x_n)$ in SNF
3. consider all possible Herbrand interpretations of $\mathcal{L}$

Definition (Gilmore's Prover)

1. F be an arbitrary sentence in language $\mathcal{L}$
2. consider its negation $\neg F$
   wlog $\neg F = \forall x_1 \cdots \forall x_n G(x_1, \ldots, x_n)$ in SNF
3. consider all possible Herbrand interpretations of $\mathcal{L}$
4. F is valid if $\exists$ finite unsatisfiable subset $S \subseteq \mathrm{Gr}(\neg F)$

Definition (Gilmore's Prover)

1. F be an arbitrary sentence in language $\mathcal{L}$
2. consider its negation $\neg F$
   wlog $\neg F = \forall x_1 \cdots \forall x_n G(x_1, \ldots, x_n)$ in SNF
3. consider all possible Herbrand interpretations of $\mathcal{L}$
4. F is valid if $\exists$ finite unsatisfiable subset $S \subseteq \mathrm{Gr}(\neg F)$

$\mathcal{A} = \{A_0, A_1, A_2, \ldots\}$ be atomic formulas over Herbrand universe of $\mathcal{L}$

Definition (Gilmore's Prover)

1. F be an arbitrary sentence in language $\mathcal{L}$
2. consider its negation $\neg F$
   wlog $\neg F = \forall x_1 \cdots \forall x_n G(x_1, \ldots, x_n)$ in SNF
3. consider all possible Herbrand interpretations of $\mathcal{L}$
4. F is valid if $\exists$ finite unsatisfiable subset $S \subseteq \mathrm{Gr}(\neg F)$

$\mathcal{A} = \{A_0, A_1, A_2, \ldots\}$ be atomic formulas over Herbrand universe of $\mathcal{L}$

Definition (Semantic Tree)

the semantic tree T for F:

Definition (Gilmore's Prover)

1. F be an arbitrary sentence in language $\mathcal{L}$
2. consider its negation $\neg F$
   wlog $\neg F = \forall x_1 \cdots \forall x_n G(x_1, \ldots, x_n)$ in SNF
3. consider all possible Herbrand interpretations of $\mathcal{L}$
4. F is valid if $\exists$ finite unsatisfiable subset $S \subseteq \mathrm{Gr}(\neg F)$

$\mathcal{A} = \{A_0, A_1, A_2, \ldots\}$ be atomic formulas over Herbrand universe of $\mathcal{L}$

Definition (Semantic Tree)

the semantic tree T for F:

- the root is a semantic tree

Definition (Gilmore's Prover)

1. F be an arbitrary sentence in language $\mathcal{L}$
2. consider its negation $\neg F$
   wlog $\neg F = \forall x_1 \cdots \forall x_n G(x_1, \dots, x_n)$ in SNF
3. consider all possible Herbrand interpretations of $\mathcal{L}$
4. F is valid if $\exists$ finite unsatisfiable subset $S \subseteq \mathrm{Gr}(\neg F)$

$\mathcal{A} = \{A_0, A_1, A_2, \dots\}$ be atomic formulas over Herbrand universe of $\mathcal{L}$

Definition (Semantic Tree)

the semantic tree T for F:

- the root is a semantic tree
- let I be a node in T of height n; then I is either a
  1. leaf node or

Definition (Gilmore's Prover)

1. F be an arbitrary sentence in language $\mathcal{L}$
2. consider its negation $\neg F$
   wlog $\neg F = \forall x_1 \cdots \forall x_n G(x_1, \ldots, x_n)$ in SNF
3. consider all possible Herbrand interpretations of $\mathcal{L}$
4. F is valid if $\exists$ finite unsatisfiable subset $S \subseteq \mathrm{Gr}(\neg F)$

$\mathcal{A} = \{A_0, A_1, A_2, \ldots\}$ be atomic formulas over Herbrand universe of $\mathcal{L}$

Definition (Semantic Tree)

the semantic tree T for F:

- the root is a semantic tree
- let I be a node in T of height n; then I is either a
  1. leaf node or
  2. the edges e_1, e_2 leaving node I are labelled by A_n and $\neg A_n$

Fact

path in T gives rise to a (partial) Herbrand interpretation $\mathcal{I}$ of F'

Fact

path in T gives rise to a (partial) Herbrand interpretation $\mathcal{I}$ of F'

Definition

Fact

path in T gives rise to a (partial) Herbrand interpretation $\mathcal{I}$ of F'

Definition

- let $I \in T$, Herbrand interpretation induced by I is denoted as $\mathcal{I}$

Fact

path in T gives rise to a (partial) Herbrand interpretation $\mathcal{I}$ of F'

Definition

- let $I \in T$, Herbrand interpretation induced by I is denoted as $\mathcal{I}$
- I is closed, if $\exists\ G \in \mathrm{Gr}(\neg F)$ such that $\mathcal{I} \not\models G$ and thus $\mathcal{I} \not\models \neg F$

Fact

path in T gives rise to a (partial) Herbrand interpretation $\mathcal{I}$ of F'

Definition

- let $I \in T$, Herbrand interpretation induced by I is denoted as $\mathcal{I}$
- I is closed, if $\exists\ G \in \mathrm{Gr}(\neg F)$ such that $\mathcal{I} \not\models G$ and thus $\mathcal{I} \not\models \neg F$

Lemma

if all nodes in T are closed then F is valid

Fact

path in T gives rise to a (partial) Herbrand interpretation $\mathcal{I}$ of F'

Definition

- let $I \in T$, Herbrand interpretation induced by I is denoted as $\mathcal{I}$
- I is closed, if $\exists\ G \in \mathrm{Gr}(\neg F)$ such that $\mathcal{I} \not\models G$ and thus $\mathcal{I} \not\models \neg F$

Lemma

if all nodes in T are closed then F is valid

Proof.

- all nodes in T are closed
- $\exists$ finite unsatisfiable $S \subseteq \mathrm{Gr}(\neg F)$
- by Herbrand's theorem $\neg F$ is unsatisfiable, hence F is valid ∎

Eliminating Function Symbols and Identity

Definition

1. wlog assume that in F individual and function constants occur only to the right hand of $=$
2. we replace all occurrences of $y = f(x_1, \dots, x_n)$ by $P(x_1, \dots, x_n, y)$, where P is fresh
3. the result of this transformation is denoted as F''

Eliminating Function Symbols and Identity

Definition

1. wlog assume that in F individual and function constants occur only to the right hand of $=$
2. we replace all occurrences of $y = f(x_1, \ldots, x_n)$ by $P(x_1, \ldots, x_n, y)$, where P is fresh
3. the result of this transformation is denoted as F''

Definition (Functionality)

let $C(f)$ denote the following sentence, denoted as functionality axiom:

$$\forall x_1 \cdots \forall x_n \exists y \forall z (P(x_1, \ldots, x_n, z) \leftrightarrow z = y)$$

Eliminating Function Symbols and Identity

Definition

1. wlog assume that in F individual and function constants occur only to the right hand of $=$
2. we replace all occurrences of $y = f(x_1, \dots, x_n)$ by $P(x_1, \dots, x_n, y)$, where P is fresh
3. the result of this transformation is denoted as F''

Definition (Functionality)

let $C(f)$ denote the following sentence, denoted as functionality axiom:

$$\forall x_1 \cdots \forall x_n \exists y \forall z (P(x_1, \dots, x_n, z) \leftrightarrow z = y)$$

Lemma

F is satisfiable if and only if $F'' \wedge C(f)$ is satisfiable

Definition (Equivalence and Congruence)

- let E denote the following equivalence axioms : $\forall x\ x \fallingdotseq x \wedge \forall x \forall y\ (x \fallingdotseq y \wedge y \fallingdotseq x) \wedge \forall x \forall y \forall z\ ((x \fallingdotseq y \wedge y \fallingdotseq z) \rightarrow x \fallingdotseq z)$

Definition (Equivalence and Congruence)

- let E denote the following equivalence axioms : $\forall x\ x \fallingdotseq x \wedge \forall x \forall y\ (x \fallingdotseq y \wedge y \fallingdotseq x) \wedge \forall x \forall y \forall z\ ((x \fallingdotseq y \wedge y \fallingdotseq z) \rightarrow x \fallingdotseq z)$
- let $C(P)$ denote the following congruence axioms:

$$\forall x_1 \cdots \forall x_n \forall y_1 \cdots \forall y_n\, ((x_1 \fallingdotseq y_1 \wedge \cdots \wedge x_n \fallingdotseq y_n) \rightarrow (P(x_1, \dots, x_n) \leftrightarrow P(y_1, \dots, y_n))$$

Definition (Equivalence and Congruence)

- let E denote the following equivalence axioms : $\forall x\ x \fallingdotseq x \land \forall x \forall y\ (x \fallingdotseq y \land y \fallingdotseq x) \land \forall x \forall y \forall z\ ((x \fallingdotseq y \land y \fallingdotseq z) \to x \fallingdotseq z)$
- let $C(P)$ denote the following congruence axioms:

$$\forall x_1 \cdots \forall x_n \forall y_1 \cdots \forall y_n\, ((x_1 \fallingdotseq y_1 \land \cdots \land x_n \fallingdotseq y_n) \to (P(x_1, \dots, x_n) \leftrightarrow P(y_1, \dots, y_n))$$

let F''' denote the result of replacing $=$ everywhere by $\fallingdotseq$

Lemma

F is satisfiable if and only if $F''' \land E \land \bigwedge_{P \in F} C(P)$ is satisfiable

Definition (Equivalence and Congruence)

- let E denote the following equivalence axioms : $\forall x\ x \risingdotseq x \land \forall x \forall y\ (x \risingdotseq y \land y \risingdotseq x) \land \forall x \forall y \forall z\ ((x \risingdotseq y \land y \risingdotseq z) \to x \risingdotseq z)$
- let $C(P)$ denote the following congruence axioms:

$$\forall x_1 \cdots \forall x_n \forall y_1 \cdots \forall y_n\, ((x_1 \risingdotseq y_1 \land \cdots \land x_n \risingdotseq y_n) \to (P(x_1, \dots, x_n) \leftrightarrow P(y_1, \dots, y_n))$$

let F''' denote the result of replacing $=$ everywhere by $\risingdotseq$

Lemma

F is satisfiable if and only if $F''' \land E \land \bigwedge_{P \in F} C(P)$ is satisfiable

Theorem

$\forall$ formula F, $\exists$ formula G not containing individual, nor function constants, nor $=$ such that $F \approx G$