Automated Theorem Proving

Georg Moser

Institute of Computer Science @ UIBK

Winter 2015

Completeness of First-Order Resolution

Definitions

- a clause is called ground if it doesn't contain variables
- a ground substitution is a substitution whose range contains only terms without variables
- let $\Box \notin \mathrm{Res}^*(\mathcal{C})$, then $\mathcal{C}$ is consistent

Completeness of First-Order Resolution

Definitions

- a clause is called ground if it doesn't contain variables
- a ground substitution is a substitution whose range contains only terms without variables
- let $\square \notin \mathrm{Res}^*(\mathcal{C})$, then $\mathcal{C}$ is consistent

Lemma

- *let S denote the set of all consistent ground clause sets*
- *then S is a first-order consistency property with respect to $\mathcal{L}$*

Completeness of First-Order Resolution

Definitions

- a clause is called ground if it doesn't contain variables
- a ground substitution is a substitution whose range contains only terms without variables
- let $\square \notin \text{Res}^*(\mathcal{C})$, then $\mathcal{C}$ is consistent

Lemma

- *let S denote the set of all consistent ground clause sets*
- *then S is a first-order consistency property with respect to $\mathcal{L}$*

Proof.

on the whiteboard ∎

Lifting Lemmas

Lemma

- *let* τ_1 *and* τ_2 *be ground substitutions and consider*

$$\frac{C\tau_1 \vee A\tau_1 \quad D\tau_2 \vee \neg B\tau_2}{C\tau_1 \vee D\tau_2}$$

where $A\tau_1 = B\tau_2$

- $\exists$ *mgu* σ *of* A *and* B*, such that* σ *is more general then* τ_1 *and* τ_2 *and the following resolution step is valid:*

$$\frac{C \vee A \quad D \vee \neg B}{(C \vee D)\sigma}$$

Lifting Lemmas

Lemma

- *let* τ_1 *and* τ_2 *be ground substitutions and consider*

$$\frac{C\tau_1 \vee A\tau_1 \quad D\tau_2 \vee \neg B\tau_2}{C\tau_1 \vee D\tau_2}$$

where $A\tau_1 = B\tau_2$

- $\exists$ *mgu* σ *of* A *and* B*, such that* σ *is more general then* τ_1 *and* τ_2 *and the following resolution step is valid:*

$$\frac{C \vee A \quad D \vee \neg B}{(C \vee D)\sigma}$$

Proof.

on the whiteboard ∎

Lemma

- *let* τ *be ground substitutions and consider the following ground factoring step:*

$$\frac{C\tau \vee A\tau \vee B\tau}{C\tau \vee A\tau}$$

  where $A\tau = B\tau$

- $\exists$ *mgu* σ*, such that* σ *is more general then* τ *and the following resolution step is valid:*

$$\frac{C \vee A \quad D \vee \neg B}{(C \vee D)\sigma}$$

Lemma

- *let τ be ground substitutions and consider the following ground factoring step:*

$$\frac{C\tau \vee A\tau \vee B\tau}{C\tau \vee A\tau}$$

  where $A\tau = B\tau$

- *$\exists$ mgu σ, such that σ is more general then τ and the following resolution step is valid:*

$$\frac{C \vee A \quad D \vee \neg B}{(C \vee D)\sigma}$$

Proof.

again the lemma follows from the properties of an mgu ■

Theorem

resolution is complete; if F a sentence and $\mathcal{C}$ its clause form, then $\Box \in \text{Res}^*(\mathcal{C})$ if F is unsatisfiable

Theorem

resolution is complete; if F a sentence and $\mathcal{C}$ its clause form, then $\Box \in \mathrm{Res}^*(\mathcal{C})$ if F is unsatisfiable

Proof.

1. suppose F is unsatisfiable

Theorem

resolution is complete; if F a sentence and $\mathcal{C}$ its clause form, then $\square \in \mathsf{Res}^*(\mathcal{C})$ *if F is unsatisfiable*

Proof.

1. suppose F is unsatisfiable
2. $\exists$ a set of ground clauses $\mathcal{C}'$ that are instances of the clauses in $\mathcal{C}$ such that $\mathcal{C}'$ is unsatisfiable

Theorem

resolution is complete; if F a sentence and $\mathcal{C}$ its clause form, then $\square \in \mathrm{Res}^*(\mathcal{C})$ if F is unsatisfiable

Proof.

1. suppose F is unsatisfiable
2. $\exists$ a set of ground clauses $\mathcal{C}'$ that are instances of the clauses in $\mathcal{C}$ such that $\mathcal{C}'$ is unsatisfiable
3. suppose $\square \notin \mathrm{Res}^*(\mathcal{C}')$

Theorem

resolution is complete; if F a sentence and $\mathcal{C}$ its clause form, then $\square \in \mathrm{Res}^*(\mathcal{C})$ *if F is unsatisfiable*

Proof.

1. suppose F is unsatisfiable
2. $\exists$ a set of ground clauses $\mathcal{C}'$ that are instances of the clauses in $\mathcal{C}$ such that $\mathcal{C}'$ is unsatisfiable
3. suppose $\square \notin \mathrm{Res}^*(\mathcal{C}')$
4. by definition $\mathcal{C}'$ is consistent

Theorem

resolution is complete; if F a sentence and $\mathcal{C}$ its clause form, then $\square \in \mathrm{Res}^*(\mathcal{C})$ if F is unsatisfiable

Proof.

1. suppose F is unsatisfiable
2. $\exists$ a set of ground clauses $\mathcal{C}'$ that are instances of the clauses in $\mathcal{C}$ such that $\mathcal{C}'$ is unsatisfiable
3. suppose $\square \notin \mathrm{Res}^*(\mathcal{C}')$
4. by definition $\mathcal{C}'$ is consistent
5. by model existence $\mathcal{C}'$ is satisfiable

Theorem

resolution is complete; if F a sentence and $\mathcal{C}$ its clause form, then $\square \in \mathrm{Res}^*(\mathcal{C})$ if F is unsatisfiable

Proof.

1. suppose F is unsatisfiable
2. $\exists$ a set of ground clauses $\mathcal{C}'$ that are instances of the clauses in $\mathcal{C}$ such that $\mathcal{C}'$ is unsatisfiable
3. suppose $\square \notin \mathrm{Res}^*(\mathcal{C}')$
4. by definition $\mathcal{C}'$ is consistent
5. by model existence $\mathcal{C}'$ is satisfiable
6. contradiction to our assumption, hence $\square \in \mathrm{Res}^*(\mathcal{C}')$

Theorem

resolution is complete; if F a sentence and $\mathcal{C}$ its clause form, then $\square \in \mathrm{Res}^*(\mathcal{C})$ if F is unsatisfiable

Proof.

1. suppose F is unsatisfiable
2. $\exists$ a set of ground clauses $\mathcal{C}'$ that are instances of the clauses in $\mathcal{C}$ such that $\mathcal{C}'$ is unsatisfiable
3. suppose $\square \notin \mathrm{Res}^*(\mathcal{C}')$
4. by definition $\mathcal{C}'$ is consistent
5. by model existence $\mathcal{C}'$ is satisfiable
6. contradiction to our assumption, hence $\square \in \mathrm{Res}^*(\mathcal{C}')$
7. the lifting lemmas allows to lift this derivation to show $\square \in \mathrm{Res}^*(\mathcal{C})$

$\blacksquare$

Summary of Last Lecture

Theorem

- *let* Γ *be a resolution refutation of a clause set* $\mathcal{C}$
- *let* n *denote the length* $|\Gamma|$ *of this refutation (counting the number of clauses in the refutation)*
- *then* $\mathrm{HC}(\mathcal{C}) \leqslant 2^{2^n}$

Definition

$$2_0 = 1 \qquad 2_{n+1} = 2^{2_n}$$

NB: note that 2_n is a non-elementary function

Theorem

$\exists$ *a (finite) set of clauses* $\mathcal{C}_n$ *such that* $\mathrm{HC}(\mathcal{C}_n) \geqslant \frac{1}{2} \cdot 2_n$

Outline of the Lecture

Early Approaches in Automated Reasoning

Herbrand's theorem for dummies, Gilmore's prover, method of Davis and Putnam

Starting Points

resolution, tableau provers, Skolemisation, ordered resolution, redundancy and deletion

Automated Reasoning with Equality

paramodulation, ordered completion and proof orders, superposition

Applications of Automated Reasoning

Neuman-Stubblebinde Key Exchange Protocol, Robbins problem

Outline of the Lecture

Early Approaches in Automated Reasoning

Herbrand's theorem for dummies, Gilmore's prover, method of Davis and Putnam

Starting Points

resolution, tableau provers, Skolemisation, ordered resolution, redundancy and deletion

Automated Reasoning with Equality

paramodulation, ordered completion and proof orders, superposition

Applications of Automated Reasoning

Neuman-Stubblebinde Key Exchange Protocol, Robbins problem

Theorem

$\exists$ *clause sets whose refutation in resolution is non-elementarily longer than its refutation in natural deduction*

Theorem

∃ clause sets whose refutation in resolution is non-elementarily longer than its refutation in natural deduction

Proof.

1. consider Statman's example $\mathcal{C}_n$
2. the shortest resolution refutation is $\Omega(2_{n-1})$
3. the length of the informal refutation is $O(n)$ and can be formalised in natural deduction ∎

How to Skolemise Properly

Definitions

- if $\forall x$ occurs positively (negatively) then $\forall x$ is called strong (weak)
- dual for $\exists x$

How to Skolemise Properly

Definitions

- if $\forall x$ occurs positively (negatively) then $\forall x$ is called strong (weak)
- dual for $\exists x$

Definitions

- a formula is called rectified if different quantifiers bind different variables
- a formula is in negation normal form (NNF), if it does not contain implication, and every negation sign occurs directly in front of an atomic formula

Inner and Outer (Refutational) Skolemisation

Definition

- let A be a rectified formula and $\mathsf{Q}x\ G$ a subformula of A
- for any subformula $\mathsf{Q}'y\ H$ of G we say $\mathsf{Q}'y$ is in scope of $\mathsf{Q}x$; denoted as $\mathsf{Q}x <_A \mathsf{Q}'y$

Inner and Outer (Refutational) Skolemisation

Definition

- let A be a rectified formula and $\mathsf{Q}x\ G$ a subformula of A
- for any subformula $\mathsf{Q}'y\ H$ of G we say $\mathsf{Q}'y$ is in scope of $\mathsf{Q}x$; denoted as $\mathsf{Q}x <_A \mathsf{Q}'y$

Definition

- let A be rectified sentence in NNF

Inner and Outer (Refutational) Skolemisation

Definition

- let A be a rectified formula and $\mathsf{Q}x\ G$ a subformula of A
- for any subformula $\mathsf{Q}'y\ H$ of G we say $\mathsf{Q}'y$ is in scope of $\mathsf{Q}x$; denoted as $\mathsf{Q}x <_A \mathsf{Q}'y$

Definition

- let A be rectified sentence in NNF
- let $\exists x B$ a subformula of A at position p
- let $\{y_1, \ldots, y_k\} = \{y \mid \forall y <_A \exists x\}$ and let $\{z_1, \ldots, z_l\} = \mathcal{FV}\mathrm{ar}(\exists x B)$

Inner and Outer (Refutational) Skolemisation

Definition

- let A be a rectified formula and $\mathsf{Q}x\ G$ a subformula of A
- for any subformula $\mathsf{Q}'y\ H$ of G we say $\mathsf{Q}'y$ is in scope of $\mathsf{Q}x$; denoted as $\mathsf{Q}x <_A \mathsf{Q}'y$

Definition

- let A be rectified sentence in NNF
- let $\exists x B$ a subformula of A at position p
- let $\{y_1, \ldots, y_k\} = \{y \mid \forall y <_A \exists x\}$ and let $\{z_1, \ldots, z_l\} = \mathcal{FV}\mathrm{ar}(\exists x B)$
- $A[B\{x \mapsto f(y_1, \ldots, y_k)\}]$ is obtained by an outer Skolemisation step

Inner and Outer (Refutational) Skolemisation

Definition

- let A be a rectified formula and $\mathsf{Q}x\ G$ a subformula of A
- for any subformula $\mathsf{Q}'y\ H$ of G we say $\mathsf{Q}'y$ is in scope of $\mathsf{Q}x$; denoted as $\mathsf{Q}x <_A \mathsf{Q}'y$

Definition

- let A be rectified sentence in NNF
- let $\exists x B$ a subformula of A at position p
- let $\{y_1, \dots, y_k\} = \{y \mid \forall y <_A \exists x\}$ and let $\{z_1, \dots, z_l\} = \mathcal{FV}\mathrm{ar}(\exists x B)$
- $A[B\{x \mapsto f(y_1, \dots, y_k)\}]$ is obtained by an outer Skolemisation step
- $A[B\{x \mapsto f(z_1, \dots, z_l)\}]$ is obtained by an inner Skolemisation step

Structural Skolem Form

Definition

let A be closed, rectified, and in NNF

Structural Skolem Form

Definition

let A be closed, rectified, and in NNF we define the mapping rsk as follows:

$$\mathsf{rsk}(A) = \begin{cases} A & \text{no existential quant. in } A \\ \mathsf{rsk}(A_{-\exists y})\{y \mapsto f(x_1, \dots, x_n)\} & \forall x_1, \dots, \forall x_n <_A \exists y \end{cases}$$

Structural Skolem Form

Definition

let A be closed, rectified, and in NNF we define the mapping rsk as follows:

$$\mathsf{rsk}(A) = \begin{cases} A & \text{no existential quant. in } A \\ \mathsf{rsk}(A_{-\exists y})\{y \mapsto f(x_1, \dots, x_n)\} & \forall x_1, \dots, \forall x_n <_A \exists y \end{cases}$$

1. $\exists y$ is the first existential quantifier in A
2. $A_{-\exists y}$ denotes A after omission of $\exists y$
3. the Skolem function symbol f is fresh

Structural Skolem Form

Definition

let A be closed, rectified, and in NNF we define the mapping rsk as follows:

$$\mathsf{rsk}(A) = \begin{cases} A & \text{no existential quant. in } A \\ \mathsf{rsk}(A_{-\exists y})\{y \mapsto f(x_1, \dots, x_n)\} & \forall x_1, \dots, \forall x_n <_A \exists y \end{cases}$$

1. $\exists y$ is the first existential quantifier in A
2. $A_{-\exists y}$ denotes A after omission of $\exists y$
3. the Skolem function symbol f is fresh

the formula $\mathsf{rsk}(A)$ is the (refutational) structural Skolem form of A

Prenex and Antiprenex Skolem Form

Definitions

- let A be a sentence and A' a prenex normal form of A; then $\mathrm{rsk}(A')$ is the prenex Skolem form of A

Prenex and Antiprenex Skolem Form

Definitions

- let A be a sentence and A' a prenex normal form of A; then $\mathrm{rsk}(A')$ is the prenex Skolem form of A
- the antiprenex form of A is obtained my minimising the quantifier range by quantifier shifting rules

Prenex and Antiprenex Skolem Form

Definitions

- let A be a sentence and A' a prenex normal form of A; then $\mathsf{rsk}(A')$ is the prenex Skolem form of A
- the antiprenex form of A is obtained my minimising the quantifier range by quantifier shifting rules
- if A' is the antiprenex form of A, then $\mathsf{rsk}(A')$ is the antiprenex Skolem form

Prenex and Antiprenex Skolem Form

Definitions

- let A be a sentence and A' a prenex normal form of A; then $\mathsf{rsk}(A')$ is the prenex Skolem form of A
- the antiprenex form of A is obtained my minimising the quantifier range by quantifier shifting rules
- if A' is the antiprenex form of A, then $\mathsf{rsk}(A')$ is the antiprenex Skolem form

Theorem

let A be a closed formula in NNF, then $A \approx \mathsf{rsk}(A)$

Example

consider $F = \forall x(\exists y \mathrm{P}(x, y) \wedge \exists z \mathrm{Q}(z)) \wedge \forall u(\neg \mathrm{P}(\mathrm{a}, u) \vee \neg \mathrm{Q}(u))$

$$G_1 = \forall x(\mathrm{P}(x, \mathrm{f}(x)) \wedge \mathrm{Q}(\mathrm{g}(x))) \wedge \forall u(\neg P(\mathrm{a}, u) \vee \neg \mathrm{Q}(u))$$
$$G_2 = \forall x \mathrm{P}(x, \mathrm{f}(x)) \wedge \mathrm{Q}(\mathrm{c}) \wedge \forall u(\neg P(\mathrm{a}, u) \vee \neg \mathrm{Q}(u))$$
$$G_3 = \forall x \forall u(\mathrm{P}(x, \mathrm{h}(x, u)) \wedge \mathrm{Q}(\mathrm{i}(x, u)) \wedge \neg P(\mathrm{a}, u) \vee \neg \mathrm{Q}(u))$$

G_1 denotes the refutational structural Skolemisation, G_2 the antiprenex refutational Skolemisation, and G_3 is the prenex refutational Skolemisation

Example

consider $F = \forall x(\exists y \mathrm{P}(x,y) \wedge \exists z \mathrm{Q}(z)) \wedge \forall u(\neg \mathrm{P}(\mathrm{a},u) \vee \neg \mathrm{Q}(u))$

$$G_1 = \forall x(\mathrm{P}(x,\mathrm{f}(x)) \wedge \mathrm{Q}(\mathrm{g}(x))) \wedge \forall u(\neg P(\mathrm{a},u) \vee \neg \mathrm{Q}(u))$$
$$G_2 = \forall x \mathrm{P}(x,\mathrm{f}(x)) \wedge \mathrm{Q}(\mathrm{c}) \wedge \forall u(\neg P(\mathrm{a},u) \vee \neg \mathrm{Q}(u))$$
$$G_3 = \forall x \forall u(\mathrm{P}(x,\mathrm{h}(x,u)) \wedge \mathrm{Q}(\mathrm{i}(x,u)) \wedge \neg P(\mathrm{a},u) \vee \neg \mathrm{Q}(u))$$

G_1 denotes the refutational structural Skolemisation, G_2 the antiprenex refutational Skolemisation, and G_3 is the prenex refutational Skolemisation

Theorem

1. *$\exists$ a set of sentences $\mathcal{D}_n$ with* $\mathrm{HC}(\mathcal{D}'_n) = 2^{2^{2^{\mathrm{O}(n)}}}$ *for the structural Skolem form $\mathcal{D}'_n$*
2. $\mathrm{HC}(\mathcal{D}''_n) \geqslant \frac{1}{2} 2_n$ *for the prenex Skolem form*

Definition (Andrew's Skolem form)

let A be a rectified sentence in NNF; (refutational) Andrew's Skolem form is defined as follows:

$$\mathrm{rsk}_A(A) = \begin{cases} A & \text{no existential quantifiers} \\ \mathrm{rsk}_A(A_{-\exists y})\{y \mapsto f(\vec{x})\} & \forall x_1, \dots, \forall x_n <_A \exists y \end{cases}$$

1. $\exists y\ B$ is a subformula of A and $\exists y$ is the first existential quantifier in A
2. all $x_1, \dots, x_n$ occur free in $\exists y\ B$

Definition (Andrew's Skolem form)

let A be a rectified sentence in NNF; (refutational) Andrew's Skolem form is defined as follows:

$$\mathsf{rsk}_A(A) = \begin{cases} A & \text{no existential quantifiers} \\ \mathsf{rsk}_A(A_{-\exists y})\{y \mapsto f(\vec{x})\} & \forall x_1, \dots, \forall x_n <_A \exists y \end{cases}$$

1. $\exists y\ B$ is a subformula of A and $\exists y$ is the first existential quantifier in A
2. all $x_1, \dots, x_n$ occur free in $\exists y\ B$

Theorem

let A be a closed formula in NNF, then $A \approx \mathsf{rsk}_A(A)$

Example

consider $\forall z \forall y\ (\exists x\ \mathrm{P}(y, x) \lor \mathrm{Q}(y, z))$; Andrew's Skolem form is given as follows:

$$\forall z \forall y\ (\mathrm{P}(y, \mathrm{f}(y)) \lor \mathrm{Q}(y, z))$$

on the other hand the antiprenex Skolem form is less succinct:

$$\forall z \forall y\ (\mathrm{P}(y, \mathrm{g}(z, y)) \lor \mathrm{Q}(y, z))$$

Example

consider $\forall z \forall y\ (\exists x\ P(y,x) \lor Q(y,z))$; Andrew's Skolem form is given as follows:

$$\forall z \forall y\ (P(y, f(y)) \lor Q(y,z))$$

on the other hand the antiprenex Skolem form is less succinct:

$$\forall z \forall y\ (P(y, g(z,y)) \lor Q(y,z))$$

Example

consider $\forall y \forall z\ \exists x (P(y,x) \lor Q(y,z))$, then Andrew's Skolem form is:

$$\forall y \forall z\ (P(y, h(y,z)) \lor Q(y,z))$$