Automated Reasoning

Georg Moser

Institute of Computer Science @ UIBK

Winter 2013

Summary Last Lecture

Definition (expansion rules)

$$\frac{\gamma}{\gamma(x)} \quad x \text{ a free variable} \qquad \frac{\delta}{\delta(f(x_1,\dots,x_n))} \quad f \text{ a Skolem function}$$

- $x_1, \dots, x_n$ denote all free variables of the formula δ
- Skolem function f must be new on the branch

Definition (atomic closure rule)

1. $\exists$ branch in tableau T that contains two literals A and $\neg B$
2. $\exists$ mgu σ of A and B
3. then $T\sigma$ is also a tableau

Theorem

if the sentence F has a free-variable tableau proof, then F is valid

Definition

a strategy S is fair if . . .

Theorem

1. *S be a fair strategy*
2. *F be a valid sentence*
3. *F has a tableau proof with the following properties:*
   - *all tableau expansion rules are considered first and follow strategy S*
   - *a block of atomic closure rules closes the tableau*

Outline of the Lecture

Early Approaches in Automated Reasoning

short recollection of Herbrand's theorem, Gilmore's prover, method of Davis and Putnam

Starting Points

resolution, tableau provers, Skolemisation, redundancy and deletion

Automated Reasoning with Equality

ordered resolution, paramodulation, ordered completion and proof orders, superposition

Applications of Automated Reasoning

Neuman-Stubblebinde Key Exchange Protocol, group theory, resolution and paramodulation as decision procedure, . . .

Outline of the Lecture

Early Approaches in Automated Reasoning

short recollection of Herbrand's theorem, Gilmore's prover, method of Davis and Putnam

Starting Points

resolution, tableau provers, Skolemisation, redundancy and deletion

Automated Reasoning with Equality

ordered resolution, paramodulation, ordered completion and proof orders, superposition

Applications of Automated Reasoning

Neuman-Stubblebinde Key Exchange Protocol, group theory, resolution and paramodulation as decision procedure, . . .

Herbrand Complexity and Proof Length

Recall

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

Herbrand Complexity and Proof Length

Recall

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

Definition

- let $\mathcal{C}$ be an unsatisfiable set of clauses
- $\mathrm{Gr}(\mathcal{C})$ denotes the ground instances of $\mathcal{C}$
- the Herbrand complexity of $\mathcal{C}$ is:

$$\mathrm{HC}(\mathcal{C}) = \min\{|\mathcal{C}'| \colon \mathcal{C}' \text{ is unsatisfiable and } \mathcal{C}' \subseteq \mathrm{Gr}(\mathcal{C})\}$$

Herbrand Complexity and Proof Length

Recall

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

Definition

- let $\mathcal{C}$ be an unsatisfiable set of clauses
- $\mathrm{Gr}(\mathcal{C})$ denotes the ground instances of $\mathcal{C}$
- the Herbrand complexity of $\mathcal{C}$ is:

$$\mathrm{HC}(\mathcal{C}) = \min\{|\mathcal{C}'| \colon \mathcal{C}' \text{ is unsatisfiable and } \mathcal{C}' \subseteq \mathrm{Gr}(\mathcal{C})\}$$

Example

consider $\mathcal{C} = \{\mathsf{P}(x), \neg\mathsf{P}(\mathsf{f}(x)) \vee \neg\mathsf{P}(\mathsf{g}(x))\}$ and we see $\mathrm{HC}(\mathcal{C}) \leqslant 3$; furthermore all $\mathcal{C}' \subseteq \mathrm{Gr}(\mathcal{C})$ with $|\mathcal{C}'| \leqslant 2$ are satisfiable: $\mathrm{HC}(\mathcal{C}) = 3$

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* $\mathsf{HC}(\mathcal{C}) \leqslant 2^{2n}$

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* $\mathsf{HC}(\mathcal{C}) \leqslant 2^{2n}$

Proof.

1. it suffices to define a suitable grounding Γ' of the refutation, as $\mathsf{HC}(\mathcal{C}) \leqslant |\Gamma'|$

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* $\mathrm{HC}(\mathcal{C}) \leqslant 2^{2n}$

Proof.

1. it suffices to define a suitable grounding Γ' of the refutation, as $\mathrm{HC}(\mathcal{C}) \leqslant |\Gamma'|$
2. we show: let Γ be a derivation of C_n from $\mathcal{C}$ with $|\Gamma| \leqslant n$
   $\exists$ ground derivation Γ' of a ground instance C_n' of C_n
   from $\mathcal{C}' \subseteq \mathrm{Gr}(\mathcal{C})$ of length $\leqslant 2^{2n}$

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* $\mathsf{HC}(\mathcal{C}) \leqslant 2^{2^n}$

Proof.

1. it suffices to define a suitable grounding Γ' of the refutation, as $\mathsf{HC}(\mathcal{C}) \leqslant |\Gamma'|$
2. we show: let Γ be a derivation of C_n from $\mathcal{C}$ with $|\Gamma| \leqslant n$
   $\exists$ ground derivation Γ' of a ground instance C_n' of C_n
   from $\mathcal{C}' \subseteq \mathsf{Gr}(\mathcal{C})$ of length $\leqslant 2^{2^n}$
3. we argue inductively

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* $\mathrm{HC}(\mathcal{C}) \leqslant 2^{2n}$

Proof.

1. it suffices to define a suitable grounding Γ' of the refutation, as $\mathrm{HC}(\mathcal{C}) \leqslant |\Gamma'|$
2. we show: let Γ be a derivation of C_n from $\mathcal{C}$ with $|\Gamma| \leqslant n$
$\exists$ ground derivation Γ' of a ground instance C_n' of C_n
from $\mathcal{C}' \subseteq \mathrm{Gr}(\mathcal{C})$ of length $\leqslant 2^{2n}$
3. we argue inductively
4. assuming induction hypothesis, we fix a derivation of length $n + 1$

Proof (cont'd).

5. in Γ suppose the last step is a resolution of $E\sigma \vee F\sigma$ from $E \vee A$ and $F \vee \neg B$, where σ is the mgu of A and B

Proof (cont'd).

5. in Γ suppose the last step is a resolution of $E\sigma \vee F\sigma$ from $E \vee A$ and $F \vee \neg B$, where σ is the mgu of A and B
6. $\exists$ ground substitution τ such that $A\tau = B\tau$

Proof (cont'd).

5. in Γ suppose the last step is a resolution of $E\sigma \vee F\sigma$ from $E \vee A$ and $F \vee \neg B$, where σ is the mgu of A and B
6. $\exists$ ground substitution τ such that $A\tau = B\tau$
7. $\exists$ derivations Γ'_1, Γ'_2 of $E\tau \vee A\tau$ and $F\tau \vee \neg B\tau$

Proof (cont'd).

5. in Γ suppose the last step is a resolution of $E\sigma \vee F\sigma$ from $E \vee A$ and $F \vee \neg B$, where σ is the mgu of A and B
6. $\exists$ ground substitution τ such that $A\tau = B\tau$
7. $\exists$ derivations Γ_1', Γ_2' of $E\tau \vee A\tau$ and $F\tau \vee \neg B\tau$
8. $|\Gamma_1'| \leqslant 2^{2n}$; $|\Gamma_2'| \leqslant 2^{2n}$

Proof (cont'd).

5 in Γ suppose the last step is a resolution of $E\sigma \vee F\sigma$ from $E \vee A$ and $F \vee \neg B$, where σ is the mgu of A and B

6 $\exists$ ground substitution τ such that $A\tau = B\tau$

7 $\exists$ derivations Γ_1', Γ_2' of $E\tau \vee A\tau$ and $F\tau \vee \neg B\tau$

8 $|\Gamma_1'| \leqslant 2^{2n}$; $|\Gamma_2'| \leqslant 2^{2n}$

9 then there exists a derivation of $C_{n+1}' = E\tau \vee F\tau$ from $\mathcal{C}' \subseteq \mathsf{Gr}(\mathcal{C})$ of length $\leqslant 2 \cdot 2^{2n} + 1 \leqslant 2^{2(n+1)}$

Proof (cont'd).

5 in Γ suppose the last step is a resolution of $E\sigma \vee F\sigma$ from $E \vee A$ and $F \vee \neg B$, where σ is the mgu of A and B

6 $\exists$ ground substitution τ such that $A\tau = B\tau$

7 $\exists$ derivations Γ_1', Γ_2' of $E\tau \vee A\tau$ and $F\tau \vee \neg B\tau$

8 $|\Gamma_1'| \leqslant 2^{2n}$; $|\Gamma_2'| \leqslant 2^{2n}$

9 then there exists a derivation of $C_{n+1}' = E\tau \vee F\tau$ from $\mathcal{C}' \subseteq \mathrm{Gr}(\mathcal{C})$ of length $\leqslant 2 \cdot 2^{2n} + 1 \leqslant 2^{2(n+1)}$

10 similarly for factoring

■

Proof (cont'd).

5. in Γ suppose the last step is a resolution of $E\sigma \vee F\sigma$ from $E \vee A$ and $F \vee \neg B$, where σ is the mgu of A and B
6. $\exists$ ground substitution τ such that $A\tau = B\tau$
7. $\exists$ derivations Γ'_1, Γ'_2 of $E\tau \vee A\tau$ and $F\tau \vee \neg B\tau$
8. $|\Gamma'_1| \leqslant 2^{2n}$; $|\Gamma'_2| \leqslant 2^{2n}$
9. then there exists a derivation of $C'_{n+1} = E\tau \vee F\tau$ from $\mathcal{C}' \subseteq \mathrm{Gr}(\mathcal{C})$ of length $\leqslant 2 \cdot 2^{2n} + 1 \leqslant 2^{2(n+1)}$
10. similarly for factoring

∎

Theorem

$\exists$ a sequence of clause sets $\mathcal{C}_n$, refutable with a resolution refutation of length $\mathrm{O}(n)$, such that $\mathrm{HC}(\mathcal{C}_n) > 2^n$

Proof.

1. we define $\mathcal{C}_n$

$$\mathsf{P}(\mathsf{a}) \qquad \neg\mathsf{P}(x) \vee \mathsf{P}(\mathsf{f}(x)) \qquad \neg\mathsf{P}(\mathsf{f}^{2^n}(\mathsf{a}))$$

Proof.

1. we define $\mathcal{C}_n$

$$\mathsf{P}(\mathsf{a}) \qquad \neg \mathsf{P}(x) \lor \mathsf{P}(\mathsf{f}(x)) \qquad \neg \mathsf{P}(\mathsf{f}^{2^n}(\mathsf{a}))$$

2. the (non-ground) refutation makes use of self-resolvents

$$\frac{\neg \mathsf{P}(x) \lor \mathsf{P}(\mathsf{f}^{m}(x)) \quad \neg \mathsf{P}(x) \lor \mathsf{P}(\mathsf{f}^{m}(x))}{\neg \mathsf{P}(x) \lor \mathsf{P}(\mathsf{f}^{2m}(x))}$$

∎

Proof.

1. we define $\mathcal{C}_n$

$$\mathsf{P}(\mathsf{a}) \qquad \neg\mathsf{P}(x) \vee \mathsf{P}(\mathsf{f}(x)) \qquad \neg\mathsf{P}(\mathsf{f}^{2^n}(\mathsf{a}))$$

2. the (non-ground) refutation makes use of self-resolvents

$$\frac{\neg\mathsf{P}(x) \vee \mathsf{P}(\mathsf{f}^{m}(x)) \quad \neg\mathsf{P}(x) \vee \mathsf{P}(\mathsf{f}^{m}(x))}{\neg\mathsf{P}(x) \vee \mathsf{P}(\mathsf{f}^{2m}(x))}$$

3. this is impossible for a ground refutation

■

Proof.

1. we define $\mathcal{C}_n$

$$\mathsf{P}(\mathsf{a}) \qquad \neg\mathsf{P}(x) \vee \mathsf{P}(\mathsf{f}(x)) \qquad \neg\mathsf{P}(\mathsf{f}^{2^n}(\mathsf{a}))$$

2. the (non-ground) refutation makes use of self-resolvents

$$\frac{\neg\mathsf{P}(x) \vee \mathsf{P}(\mathsf{f}^{m}(x)) \quad \neg\mathsf{P}(x) \vee \mathsf{P}(\mathsf{f}^{m}(x))}{\neg\mathsf{P}(x) \vee \mathsf{P}(\mathsf{f}^{2m}(x))}$$

3. this is impossible for a ground refutation

■

Definition

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

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

Proof.

1. we define $\mathcal{C}_n$

$$\mathsf{P}(\mathsf{a}) \qquad \neg\mathsf{P}(x) \lor \mathsf{P}(\mathsf{f}(x)) \qquad \neg\mathsf{P}(\mathsf{f}^{2^n}(\mathsf{a}))$$

2. the (non-ground) refutation makes use of self-resolvents

$$\frac{\neg\mathsf{P}(x) \lor \mathsf{P}(\mathsf{f}^{m}(x)) \quad \neg\mathsf{P}(x) \lor \mathsf{P}(\mathsf{f}^{m}(x))}{\neg\mathsf{P}(x) \lor \mathsf{P}(\mathsf{f}^{2m}(x))}$$

3. this is impossible for a ground refutation

■

Definition

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

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

Theorem

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

Statman's Example

Example

consider the following clause set:

$$\begin{aligned}
\mathcal{C}_n &= \mathsf{ST} \cup \mathsf{ID} \cup \{\mathsf{p} \cdot \mathsf{q} \neq \mathsf{p} \cdot ((\mathsf{T}_n \cdot \mathsf{q}) \cdot \mathsf{q})\} \\
\mathsf{ST} &= \{\mathsf{S}xyz = (xz)(yz), \mathsf{B}xyz = x(yz), \mathsf{C}xyz = (xz)y, \\
&\qquad \mathsf{I}x = x, \mathsf{p}x = \mathsf{p}(\mathsf{q}x)\} \\
\mathsf{ID} &= \text{"equality axioms"} \\
\mathsf{T} &= (\mathsf{SB})((\mathsf{CB})\mathsf{I}) \\
\mathsf{T}_1 &= \mathsf{T} \\
\mathsf{T}_{k+1} &= \mathsf{T}_k\mathsf{T}
\end{aligned}$$

Lemma

$\mathsf{T}yx = y(yx)$ *is derivable*

Lemma

$\mathsf{T}yx = y(yx)$ *is derivable*

Proof.

$$(\mathsf{SB})((\mathsf{CB})\mathsf{I})yx = (\mathsf{B}y)((\mathsf{CB})\mathsf{I}y)x =$$
$$= (\mathsf{B}y)((\mathsf{B}y)\mathsf{I})x = y((\mathsf{B}y\mathsf{I})x) = y(y(\mathsf{I}x)) = y(yx)$$

Lemma

$\mathsf{T}yx = y(yx)$ *is derivable*

Proof.

$$(\mathsf{SB})((\mathsf{CB})\mathsf{I})yx = (\mathsf{B}y)((\mathsf{CB})\mathsf{I}y)x =$$
$$= (\mathsf{B}y)((\mathsf{B}y)\mathsf{I})x = y((\mathsf{B}y\mathsf{I})x) = y(y(\mathsf{I}x)) = y(yx)$$

■

Lemma

$\mathsf{T}yx = y(yx)$ *is derivable*

Proof.

$$\begin{aligned}(\mathsf{SB})((\mathsf{CB})\mathsf{I})yx = (\mathsf{B}y)((\mathsf{CB})\mathsf{I}y)x = \\ = (\mathsf{B}y)((\mathsf{B}y)\mathsf{I})x = y((\mathsf{B}y\mathsf{I})x) = y(y(\mathsf{I}x)) = y(yx)\end{aligned}$$

■

Definition

$$\mathsf{H}_1(y) = \forall x\ \mathsf{p}x = \mathsf{p}(yx) \qquad \mathsf{H}_{m+1}(y) = \forall x\ (\mathsf{H}_m(x) \to \mathsf{H}_m(yx))$$

Lemma

$\mathsf{T}yx = y(yx)$ *is derivable*

Proof.

$$(\mathsf{SB})((\mathsf{CB})\mathsf{I})yx = (\mathsf{B}y)((\mathsf{CB})\mathsf{I}y)x =$$
$$= (\mathsf{B}y)((\mathsf{B}y)\mathsf{I})x = y((\mathsf{B}y\mathsf{I})x) = y(y(\mathsf{I}x)) = y(yx)$$

■

Definition

$$\mathsf{H}_1(y) = \forall x\ \mathsf{p}x = \mathsf{p}(yx) \qquad \mathsf{H}_{m+1}(y) = \forall x\ (\mathsf{H}_m(x) \to \mathsf{H}_m(yx))$$

Lemma

$\mathsf{H}_1(y) \to \mathsf{H}_1(\mathsf{T}y)$ *and* $\forall y\ (\mathsf{H}_1(y) \to \mathsf{H}_1(\mathsf{T}y))$ $(= \mathsf{H}_2(\mathsf{T}))$ *are derivable*

Lemma

$\mathsf{H}_{m+1}(y) \to H_{m+1}(\mathsf{T}y)$ *and* $\forall y\ (\mathsf{H}_{m+1}(y) \to H_{m+1}(\mathsf{T}y))$ $(= \mathsf{H}_{m+2}(\mathsf{T}))$ *are derivable*

Lemma

$\mathsf{H}_{m+1}(y) \rightarrow H_{m+1}(\mathsf{T}y)$ *and* $\forall y\ (\mathsf{H}_{m+1}(y) \rightarrow H_{m+1}(\mathsf{T}y))\ (= \mathsf{H}_{m+2}(\mathsf{T}))$ *are derivable*

Proof.

1. $\forall x\ (A(x) \rightarrow A(yx)) \rightarrow \forall x(A(x) \rightarrow A(y(yx)))$ is derivable

Lemma

$\mathrm{H}_{m+1}(y) \to H_{m+1}(\mathrm{T}y)$ *and* $\forall y\ (\mathrm{H}_{m+1}(y) \to H_{m+1}(\mathrm{T}y))$ $(= \mathrm{H}_{m+2}(\mathrm{T}))$ *are derivable*

Proof.

1. $\forall x\ (A(x) \to A(yx)) \to \forall x(A(x) \to A(y(yx)))$ is derivable
2. using $y(yx) = \mathrm{T}yx$ and setting $A = \mathrm{H}_m$ we have

$$\mathrm{H}_{m+1}(y) \to H_{m+1}(\mathrm{T}y) \qquad \forall y\ (\mathrm{H}_{m+1}(y) \to H_{m+1}(\mathrm{T}y))$$

Lemma

$\mathrm{H}_{m+1}(y) \rightarrow H_{m+1}(\mathrm{T}y)$ and $\forall y\ (\mathrm{H}_{m+1}(y) \rightarrow H_{m+1}(\mathrm{T}y))$ $(= \mathrm{H}_{m+2}(\mathrm{T}))$ are derivable

Proof.

1. $\forall x\ (A(x) \rightarrow A(yx)) \rightarrow \forall x(A(x) \rightarrow A(y(yx)))$ is derivable
2. using $y(yx) = \mathrm{T}yx$ and setting $A = \mathrm{H}_m$ we have

$$\mathrm{H}_{m+1}(y) \rightarrow H_{m+1}(\mathrm{T}y) \qquad \forall y\ (\mathrm{H}_{m+1}(y) \rightarrow H_{m+1}(\mathrm{T}y))$$

∎

Lemma

$\mathrm{H}_{m+1}(y) \rightarrow H_{m+1}(\mathrm{T}y)$ *and* $\forall y\ (\mathrm{H}_{m+1}(y) \rightarrow H_{m+1}(\mathrm{T}y))$ $(= \mathrm{H}_{m+2}(\mathrm{T}))$ *are derivable*

Proof.

1. $\forall x\ (A(x) \rightarrow A(yx)) \rightarrow \forall x(A(x) \rightarrow A(y(yx)))$ is derivable
2. using $y(yx) = \mathrm{T}yx$ and setting $A = \mathrm{H}_m$ we have

$$\mathrm{H}_{m+1}(y) \rightarrow H_{m+1}(\mathrm{T}y) \qquad \forall y\ (\mathrm{H}_{m+1}(y) \rightarrow H_{m+1}(\mathrm{T}y))$$

∎

Corollary

$\mathrm{H}_2(\mathrm{T}), \dots, \mathrm{H}_{n+1}(\mathrm{T})$ *are derivable by short proofs*

NB: “short” refers to proofs whose length is independent on n

Lemma

Statman's example is unsatisfiable; which can be shown with a proof linear in n

Lemma

Statman's example is unsatisfiable; which can be shown with a proof linear in n

Proof.

$$
\dfrac{pq \neq p(T_nq)q \qquad \dfrac{\dfrac{\forall x\ px = p(qx) \qquad \dfrac{\dfrac{\dfrac{H_n(T) \qquad \dfrac{\forall x\ (H_n(x) \to H_n(Tx))\ (= H_{n+1}(T))}{H_n(T) \to H_n(T_2)}}{\forall x\ (H_{n-1}(x) \to H_{n-1}(T_2x))\ (= H_n(T_2))}}{\overline{H_2(T_n)}}}{\forall x\ px = p(qx) \to \forall x\ px = p(T_nq)x}}{\forall x\ px = p(T_nq)x}}{pq = p(T_nq)q}}{\square}
$$

Lemma

Statman's example is unsatisfiable; which can be shown with a proof linear in n

Proof.

$$
\dfrac{pq \neq p(T_n q)q \qquad \dfrac{\dfrac{\forall x\ px = p(qx) \qquad \dfrac{\dfrac{\dfrac{H_n(T) \qquad \dfrac{\forall x\ (H_n(x) \to H_n(Tx))\ (= H_{n+1}(T))}{H_n(T) \to H_n(T_2)}}{\forall x\ (H_{n-1}(x) \to H_{n-1}(T_2 x))\ (= H_n(T_2))}}{\overline{H_2(T_n)}}}{\forall x\ px = p(qx) \to \forall x\ px = p(T_n q)x}}{\forall x\ px = p(T_n q)x}}{pq = p(T_n q)q}}{\Box}
$$

■

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 above refutation is $\mathrm{O}(n)$ and can be formalised 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 above refutation is $O(n)$ and can be formalised in natural deduction ■

Definitions

- a formula is called rectified if different quantifiers bind different variables
- if $\forall x$ occurs positively (negatively) then $\forall x$ is called strong (weak)
- dual for $\exists x$

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 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 closed and rectified

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 closed and rectified
- we define the mapping rsk as follows:

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

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 closed and rectified
- 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

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 closed and rectified
- 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 $\mathsf{rsk}(A')$ 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
- if A' is the antiprenex form of A, then $\mathrm{rsk}(A')$ 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 $\mathrm{rsk}(A')$ is the prenex Skolem form of A
- the antiprenex form of A is obtained my minimising the quantifier range by quantifier shifting rules
- if A' is the antiprenex form of A, then $\mathrm{rsk}(A')$ is the antiprenex Skolem form

Theorem

let A be a closed formula, then $A \sim \mathrm{rsk}(A)$

Example

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

$$
\begin{aligned}
G_1 &= \forall x(\mathrm{P}(x,\mathrm{f}(x)) \land \mathrm{Q}(\mathrm{g}(x))) \land \forall u(\neg P(\mathrm{a},u) \lor \neg \mathrm{Q}(u))\\
G_2 &= \forall x \mathrm{P}(x,\mathrm{f}(x)) \land \mathrm{Q}(\mathrm{c}) \land \forall u(\neg P(\mathrm{a},u) \lor \neg \mathrm{Q}(u))\\
G_3 &= \forall x \forall u(\mathrm{P}(x,\mathrm{h}(x,u)) \land \mathrm{Q}(\mathrm{i}(x,u)) \land \neg P(\mathrm{a},u) \lor \neg \mathrm{Q}(u))
\end{aligned}
$$

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

Structural Skolemisation

Example

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

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

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; (refutational) Andrew's Skolem form is defined as follows:

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

4. $\exists y \; B$ is a subformula of A and $\exists y$ is the first existential quantifer in A
5. all $x_1, \dots, x_n$ occur free in $\exists y \; B$

Definition (Andrew's Skolem form)

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

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

4. $\exists y\ B$ is a subformula of A and $\exists y$ is the first existential quantifer in A
5. all $x_1, \dots, x_n$ occur free in $\exists y\ B$

Example

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

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

on the other hand consider $\forall y, z\ \exists x (\mathrm{P}(y, x) \lor \mathrm{Q}(y, z))$

Inner and Outer (Refutational) Skolemisation

Definition

- let A be rectified sentence in negation normal form (NNF)
- let $\exists x B$ a subformula of A at position p

Inner and Outer (Refutational) Skolemisation

Definition

- let A be rectified sentence in negation normal form (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 $\{z_1, \dots, z_l\} = \mathcal{FV}\mathrm{ar}(\exists x B)$

Inner and Outer (Refutational) Skolemisation

Definition

- let A be rectified sentence in negation normal form (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 rectified sentence in negation normal form (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

Inner and Outer (Refutational) Skolemisation

Definition

- let A be rectified sentence in negation normal form (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

Example

1. structural Skolemisation is a variation of outer Skolemisation
2. Andrew's Skolemisation is a variation of inner and outer Skolemisation

the following variants of Skolemisation improve inner Skolemisation

Definition (Optimised Skolemisation)

- let A be a sentence in NNF and $B = \exists x_1 \cdots x_k (E \wedge F)$ a subformula of A with $\mathcal{FV}\mathrm{ar}(\exists \vec{x}(E \wedge F)) = \{y_1, \dots, y_n\}$
- suppose $A = C[B]$

Definition (Optimised Skolemisation)

- let A be a sentence in NNF and $B = \exists x_1 \cdots x_k (E \wedge F)$ a subformula of A with $\mathcal{FV}\mathrm{ar}(\exists \vec{x}(E \wedge F)) = \{y_1, \ldots, y_n\}$
- suppose $A = C[B]$
- suppose $A \rightarrow \forall y_1, \ldots, y_n \exists x_1 \cdots x_k E$ is valid

Definition (Optimised Skolemisation)

- let A be a sentence in NNF and $B = \exists x_1 \cdots x_k (E \wedge F)$ a subformula of A with $\mathcal{FV}\mathrm{ar}(\exists \vec{x}(E \wedge F)) = \{y_1, \dots, y_n\}$
- suppose $A = C[B]$
- suppose $A \rightarrow \forall y_1, \dots, y_n \exists x_1 \cdots x_k E$ is valid
- we define an optimised Skolemisation step as follows

$$\mathrm{opt\_step}(A) = \forall \vec{y} E\{\dots, x_i \mapsto f_i(\vec{y}), \dots\} \wedge C[F\{\dots, x_i \mapsto f_i(\vec{y}), \dots\}]$$

where $f_1, \dots, f_k$ are new Skolem function symbols

Definition (Optimised Skolemisation)

- let A be a sentence in NNF and $B = \exists x_1 \cdots x_k (E \wedge F)$ a subformula of A with $\mathcal{FV}\mathrm{ar}(\exists \vec{x}(E \wedge F)) = \{y_1, \dots, y_n\}$
- suppose $A = C[B]$
- suppose $A \to \forall y_1, \dots, y_n \exists x_1 \cdots x_k E$ is valid
- we define an optimised Skolemisation step as follows

  $$\text{opt\_step}(A) = \forall \vec{y} E\{\dots, x_i \mapsto f_i(\vec{y}), \dots\} \wedge C[F\{\dots, x_i \mapsto f_i(\vec{y}), \dots\}]$$

  where $f_1, \dots, f_k$ are new Skolem function symbols

Example

consider a subformula of a sentence A

$$\forall x, y, z(\mathrm{R}(x,y) \wedge \mathrm{R}(x,z) \to \exists u(\mathrm{R}(y,u) \wedge \mathrm{R}(z,u)))$$

we assume $\forall y \exists u \mathrm{R}(y,u)$ is provable from A; we obtain

$$\mathrm{R}(y, \mathrm{f}(y,z)) \qquad \neg\mathrm{R}(x,y) \vee \neg\mathrm{R}(x,z) \vee \mathrm{R}(z, \mathrm{f}(y,z))$$

Theorem

optimised Skolemisation preserves satisfiability

Proof Sketch.

1. suppose A is satisfiable with some interpretation $\mathcal{I}$
2. we extent $\mathcal{I}$ to the Skolem functions such that we obtain for the extention $\mathcal{I}'$

$$\mathcal{I}' \models \forall \vec{y} E\{\dots, x_i \mapsto f_i(\vec{y}), \dots\} \qquad \mathcal{I}' \models C[F\{\dots, x_i \mapsto f_i(\vec{y}), \dots\}]$$

3. for this the extra condition is exploited

Theorem

optimised Skolemisation preserves satisfiability

Proof Sketch.

1. suppose A is satisfiable with some interpretation $\mathcal{I}$
2. we extent $\mathcal{I}$ to the Skolem functions such that we obtain for the extention $\mathcal{I}'$

$$\mathcal{I}' \models \forall \vec{y} E\{\dots, x_i \mapsto f_i(\vec{y}), \dots\} \qquad \mathcal{I}' \models C[F\{\dots, x_i \mapsto f_i(\vec{y}), \dots\}]$$

3. for this the extra condition is exploited

■

Theorem

optimised Skolemisation preserves satisfiability

Proof Sketch.

1. suppose A is satisfiable with some interpretation $\mathcal{I}$
2. we extent $\mathcal{I}$ to the Skolem functions such that we obtain for the extention $\mathcal{I}'$

$$\mathcal{I}' \models \forall\vec{y} E\{\dots, x_i \mapsto f_i(\vec{y}), \dots\} \qquad \mathcal{I}' \models C[F\{\dots, x_i \mapsto f_i(\vec{y}), \dots\}]$$

3. for this the extra condition is exploited

■

Remark

in comparison to (standard) inner Skolemisation is that some literals from clauses are deleted

Definition

- a clause C subsumes clause D, if $\exists\ \sigma$ such that the multiset of literals of $C\sigma$ is contained in the multiset of literals of D (denoted $C\sigma \subseteq D$)

Definition

- a clause C subsumes clause D, if $\exists\ \sigma$ such that the multiset of literals of $C\sigma$ is contained in the multiset of literals of D (denoted $C\sigma \subseteq D$)
- C is a condensation of D if C is a proper (multiple) factor of D that subsumes D

Definition

- a clause C subsumes clause D, if $\exists\ \sigma$ such that the multiset of literals of $C\sigma$ is contained in the multiset of literals of D (denoted $C\sigma \subseteq D$)
- C is a condensation of D if C is a proper (multiple) factor of D that subsumes D

Example

consider the clause $\mathsf{P}(x) \vee \mathsf{R}(\mathsf{b}) \vee \mathsf{P}(\mathsf{a}) \vee \mathsf{R}(z)$; its condensation is $\mathsf{R}(\mathsf{b}) \vee \mathsf{P}(\mathsf{a})$

NB: condensation forms a strong normalisation technique that is essential to remove redundancy in clauses

Definition

- a clause C subsumes clause D, if $\exists\ \sigma$ such that the multiset of literals of $C\sigma$ is contained in the multiset of literals of D (denoted $C\sigma \subseteq D$)
- C is a condensation of D if C is a proper (multiple) factor of D that subsumes D

Example

consider the clause $\mathsf{P}(x) \vee \mathsf{R}(\mathsf{b}) \vee \mathsf{P}(\mathsf{a}) \vee \mathsf{R}(z)$; its condensation is $\mathsf{R}(\mathsf{b}) \vee \mathsf{P}(\mathsf{a})$

NB: condensation forms a strong normalisation technique that is essential to remove redundancy in clauses

Example

note that the clause $\mathsf{R}(x, x) \vee \mathsf{R}(y, y)$ does not subsume $\mathsf{R}(\mathsf{a}, \mathsf{a})$

Definition

- let $B = \exists\vec{x}(E_1 \wedge \cdots \wedge E_\ell)$ be a formula

Definition

- let $B = \exists \vec{x}(E_1 \wedge \cdots \wedge E_\ell)$ be a formula
- let $\{\vec{z}_1\} = \mathcal{FV}\mathrm{ar}(E_1) \setminus \{\vec{x}\}$
- let $\{\vec{z}_i\} = \mathcal{FV}\mathrm{ar}(E_i) \setminus \left(\bigcup_{j<i} \mathcal{FV}\mathrm{ar}(E_j) \cup \{\vec{x}\}\right)$

Definition

- let $B = \exists\vec{x}(E_1 \wedge \cdots \wedge E_\ell)$ be a formula
- let $\{\vec{z}_1\} = \mathcal{FV}\mathrm{ar}(E_1) \setminus \{\vec{x}\}$
- let $\{\vec{z}_i\} = \mathcal{FV}\mathrm{ar}(E_i) \setminus \left(\bigcup_{j<i} \mathcal{FV}\mathrm{ar}(E_j) \cup \{\vec{x}\}\right)$
- we call $\langle\{\vec{z}_1\}, \dots, \{\vec{z}_\ell\}\rangle$ the (free variable) splitting of B

Definition

- let $B = \exists\vec{x}(E_1 \wedge \cdots \wedge E_\ell)$ be a formula
- let $\{\vec{z}_1\} = \mathcal{FV}\mathrm{ar}(E_1) \setminus \{\vec{x}\}$
- let $\{\vec{z}_i\} = \mathcal{FV}\mathrm{ar}(E_i) \setminus \left(\bigcup_{j<i} \mathcal{FV}\mathrm{ar}(E_j) \cup \{\vec{x}\}\right)$
- we call $\langle\{\vec{z}_1\}, \ldots, \{\vec{z}_\ell\}\rangle$ the (free variable) splitting of B

Example

consider $\exists u(\mathrm{R}(y, u) \wedge \mathrm{R}(z, u))$; its splitting is $\langle\{y\}, \{z\}\rangle$

Definition

- let $B = \exists \vec{x}(E_1 \wedge \cdots \wedge E_\ell)$ be a formula
- let $\{\vec{z}_1\} = \mathcal{FV}\mathrm{ar}(E_1) \setminus \{\vec{x}\}$
- let $\{\vec{z}_i\} = \mathcal{FV}\mathrm{ar}(E_i) \setminus \left(\bigcup_{j<i} \mathcal{FV}\mathrm{ar}(E_j) \cup \{\vec{x}\}\right)$
- we call $\langle \{\vec{z}_1\}, \dots, \{\vec{z}_\ell\} \rangle$ the (free variable) splitting of B

Example

consider $\exists u(\mathrm{R}(y,u) \wedge \mathrm{R}(z,u))$; its splitting is $\langle \{y\}, \{z\} \rangle$

Observation

Definition

- let $B = \exists \vec{x}(E_1 \wedge \cdots \wedge E_\ell)$ be a formula
- let $\{\vec{z}_1\} = \mathcal{FV}\mathrm{ar}(E_1) \setminus \{\vec{x}\}$
- let $\{\vec{z}_i\} = \mathcal{FV}\mathrm{ar}(E_i) \setminus \left(\bigcup_{j<i} \mathcal{FV}\mathrm{ar}(E_j) \cup \{\vec{x}\}\right)$
- we call $\langle\{\vec{z}_1\}, \dots, \{\vec{z}_\ell\}\rangle$ the (free variable) splitting of B

Example

consider $\exists u(\mathrm{R}(y, u) \wedge \mathrm{R}(z, u))$; its splitting is $\langle\{y\}, \{z\}\rangle$

Observation

- let $\langle\{\vec{z}_1\}, \dots, \{\vec{z}_\ell\}\rangle$ be a splitting of $\exists \vec{x}(E_1 \wedge \cdots \wedge E_\ell)$

Definition

- let $B = \exists\vec{x}(E_1 \wedge \cdots \wedge E_\ell)$ be a formula
- let $\{\vec{z}_1\} = \mathcal{FV}\mathrm{ar}(E_1) \setminus \{\vec{x}\}$
- let $\{\vec{z}_i\} = \mathcal{FV}\mathrm{ar}(E_i) \setminus \left(\bigcup_{j<i} \mathcal{FV}\mathrm{ar}(E_j) \cup \{\vec{x}\}\right)$
- we call $\langle\{\vec{z}_1\}, \dots, \{\vec{z}_\ell\}\rangle$ the (free variable) splitting of B

Example

consider $\exists u(\mathrm{R}(y, u) \wedge \mathrm{R}(z, u))$; its splitting is $\langle\{y\}, \{z\}\rangle$

Observation

- let $\langle\{\vec{z}_1\}, \dots, \{\vec{z}_\ell\}\rangle$ be a splitting of $\exists\vec{x}(E_1 \wedge \cdots \wedge E_\ell)$
- each conjunction E_i contains at least one of the variables from $\vec{x}$

Definition

- let $B = \exists \vec{x}(E_1 \wedge \cdots \wedge E_\ell)$ be a formula
- let $\{\vec{z}_1\} = \mathcal{FV}\mathrm{ar}(E_1) \setminus \{\vec{x}\}$
- let $\{\vec{z}_i\} = \mathcal{FV}\mathrm{ar}(E_i) \setminus \left(\bigcup_{j<i} \mathcal{FV}\mathrm{ar}(E_j) \cup \{\vec{x}\}\right)$
- we call $\langle\{\vec{z}_1\}, \dots, \{\vec{z}_\ell\}\rangle$ the (free variable) splitting of B

Example

consider $\exists u(\mathrm{R}(y, u) \wedge \mathrm{R}(z, u))$; its splitting is $\langle\{y\}, \{z\}\rangle$

Observation

- let $\langle\{\vec{z}_1\}, \dots, \{\vec{z}_\ell\}\rangle$ be a splitting of $\exists \vec{x}(E_1 \wedge \cdots \wedge E_\ell)$
- each conjunction E_i contains at least one of the variables from $\vec{x}$
- $\langle\{\vec{z}_1, \vec{z}_2\}, \dots, \{\vec{z}_\ell\}\rangle$ is a splitting of $\exists \vec{v}(E_2 \wedge \cdots \wedge E_\ell)\{x_i \mapsto f_i(\vec{z}_1, \vec{v})\}$ where $\vec{v}$ are new

Definition (Strong Skolemisation)

- let A be a sentence in NNF and $B = \exists \vec{x}(E_1 \wedge \cdots \wedge E_\ell)$ a subformula such that $A = C[B]$

Definition (Strong Skolemisation)

- let A be a sentence in NNF and $B = \exists\vec{x}(E_1 \wedge \cdots \wedge E_\ell)$ a subformula such that $A = C[B]$
- let $\langle\{\vec{z}_1\}, \ldots, \{\vec{z}_\ell\}\rangle$ be a free variable splitting of B

Definition (Strong Skolemisation)

- let A be a sentence in NNF and $B = \exists\vec{x}(E_1 \land \cdots \land E_\ell)$ a subformula such that $A = C[B]$
- let $\langle\{\vec{z}_1\},\ldots,\{\vec{z}_\ell\}\rangle$ be a free variable splitting of B
- a strong Skolemisation step is defined as $\mathsf{str\_step}(A) = C[D]$ where D is defined as

$$\forall\vec{w}_2,\ldots,\vec{w}_\ell E_1\{x_i \mapsto f_i(\vec{z}_1,\vec{w}_2,\ldots,\vec{w}_\ell)\} \land \cdots$$
$$\cdots \land E_\ell\{x_i \mapsto f_i(\vec{z}_1,\vec{z}_2,\ldots,\vec{z}_\ell)\}$$

Definition (Strong Skolemisation)

- let A be a sentence in NNF and $B = \exists \vec{x}(E_1 \land \cdots \land E_\ell)$ a subformula such that $A = C[B]$
- let $\langle \{\vec{z}_1\}, \dots, \{\vec{z}_\ell\} \rangle$ be a free variable splitting of B
- a strong Skolemisation step is defined as $\mathrm{str\_step}(A) = C[D]$ where D is defined as

$$\forall \vec{w}_2, \dots, \vec{w}_\ell E_1\{x_i \mapsto f_i(\vec{z}_1, \vec{w}_2, \dots, \vec{w}_\ell)\} \land \cdots$$
$$\cdots \land E_\ell\{x_i \mapsto f_i(\vec{z}_1, \vec{z}_2, \dots, \vec{z}_\ell)\}$$

Example

consider the formula $\forall x, y, z(\mathrm{R}(x,y) \land \mathrm{R}(x,z) \to \exists u(\mathrm{R}(y,u) \land \mathrm{R}(z,u)))$ strong Skolemisation yields the following clauses

$\neg \mathrm{R}(x,y) \lor \neg \mathrm{R}(x,z) \lor \mathrm{R}(y, \mathrm{f}(y,w))$ $\qquad$ $\neg \mathrm{R}(x,y) \lor \neg \mathrm{R}(x,z) \lor \mathrm{R}(z, \mathrm{f}(y,z))$

condensation yields: $\neg \mathrm{R}(x,y) \lor \mathrm{R}(y, \mathrm{f}(y,w))$

Definition (Strong Skolemisation)

- let A be a sentence in NNF and $B = \exists \vec{x}(E_1 \wedge \cdots \wedge E_\ell)$ a subformula such that $A = C[B]$
- let $\langle \{\vec{z}_1\}, \dots, \{\vec{z}_\ell\} \rangle$ be a free variable splitting of B
- a strong Skolemisation step is defined as $\text{str\_step}(A) = C[D]$ where D is defined as

$$\forall \vec{w}_2, \dots, \vec{w}_\ell E_1\{x_i \mapsto f_i(\vec{z}_1, \vec{w}_2, \dots, \vec{w}_\ell)\} \wedge \cdots$$
$$\cdots \wedge E_\ell\{x_i \mapsto f_i(\vec{z}_1, \vec{z}_2, \dots, \vec{z}_\ell)\}$$

Example

consider the formula $\forall x, y, z(\mathsf{R}(x, y) \wedge \mathsf{R}(x, z) \rightarrow \exists u(\mathsf{R}(y, u) \wedge \mathsf{R}(z, u)))$
strong Skolemisation yields the following clauses

$\neg\mathsf{R}(x, y) \vee \neg\mathsf{R}(x, z) \vee \mathsf{R}(y, \mathsf{f}(y, w))$ $\neg\mathsf{R}(x, y) \vee \neg\mathsf{R}(x, z) \vee \mathsf{R}(z, \mathsf{f}(y, z))$

condensation yields: $\neg\mathsf{R}(x, y) \vee \mathsf{R}(y, \mathsf{f}(y, w))$

Lemma

if $\exists x_1, \ldots, x_k(E \wedge F)$ *is satisfiable, then the following formula is satisfiable as well*

$$\forall w_1, \ldots, w_k E\{x_i \mapsto f_i(\vec{y}, \vec{w})\} \wedge \exists v_1, \ldots, v_k F\{x_i \mapsto f_i(\vec{y}, \vec{v})\}$$

where $\{y_1, \ldots, y_n\} = \mathcal{FV}\mathrm{ar}(E) \setminus \{x_1, \ldots, x_k\}$

Lemma

if $\exists x_1, \dots, x_k (E \wedge F)$ *is satisfiable, then the following formula is satisfiable as well*

$$\forall w_1, \dots, w_k E\{x_i \mapsto f_i(\vec{y}, \vec{w})\} \wedge \exists v_1, \dots, v_k F\{x_i \mapsto f_i(\vec{y}, \vec{v})\}$$

where $\{y_1, \dots, y_n\} = \mathcal{FV}\mathrm{ar}(E) \setminus \{x_1, \dots, x_k\}$

Theorem

strong Skolemisation preserves satisfiability

Proof Sketch.

- suppose A is satisfiable
- one shows satisfiability of str_step(A) by main induction on A and side induction on ℓ
- the base case exploits the above lemma

Lemma

if $\exists x_1, \dots, x_k (E \wedge F)$ *is satisfiable, then the following formula is satisfiable as well*

$$\forall w_1, \dots, w_k E\{x_i \mapsto f_i(\vec{y}, \vec{w})\} \wedge \exists v_1, \dots, v_k F\{x_i \mapsto f_i(\vec{y}, \vec{v})\}$$

where $\{y_1, \dots, y_n\} = \mathcal{F}\mathcal{V}\mathrm{ar}(E) \setminus \{x_1, \dots, x_k\}$

Theorem

strong Skolemisation preserves satisfiability

Proof Sketch.

- suppose A is satisfiable
- one shows satisfiability of str_step(A) by main induction on A and side induction on ℓ
- the base case exploits the above lemma ■

Assessment

structural Skolemisation

- structural (outer) Skolemisation can lead to non-elementary speed-up over prenex Skolemisation
- structural Skolemisation requires non-trivial formula transformations, in particular quantifier shiftings
- how to implement?

Assessment

structural Skolemisation

- structural (outer) Skolemisation can lead to non-elementary speed-up over prenex Skolemisation
- structural Skolemisation requires non-trivial formula transformations, in particular quantifier shiftings
- how to implement?

inner Skolemisation

- standard inner Skolemisation techniques are straightforward to implement
- optimised Skolemisation requires proof of $A \rightarrow \forall \vec{y} \exists \vec{x} E$ as pre-condition
- strong Skolemisation is incomparable to optimised Skolemisation, as larger, but more general clauses may be produced