Automated Theorem Proving

Georg Moser

Department of Computer Science @ UIBK

Summer 2017

Summary of Last Lecture

Definition

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

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

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

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

Reminder: Computational Logic

Lemma

let $\mathcal{I} = (\mathcal{A}, \ell)$ be an Herbrand interpretation of $\mathcal{L}$

1. *$\forall x F(x)$ is true in $\mathcal{I}$ iff for all $t \in \mathcal{A}$, $F(t)$ is true in $\mathcal{I}$*
2. *$\exists x F(x)$ is true in $\mathcal{I}$ iff there exists $t \in \mathcal{A}$ such that $F(t)$ is true in $\mathcal{I}$*

Lemma (Hintikka's Lemma)

if H is first-order Hintikka set with respect to language $\mathcal{L}$ with nonempty set of closed terms then H is satisfiable in Herbrand model (over $\mathcal{L}$)

Notation

Hintikka sets are called sets admitting the closure properties in the lecture notes

Yet Another Constructive Proof of Herbrand's Theorem

Fact

if $(\mathcal{A}, \ell)$ be an interpretation, F a formula, and $x_1, \dots, x_n$ denote the set of (free) variables in F; only the values $\ell(x_1), \dots \ell(x_n)$ of the environment ℓ are important for the truth value of F

Notation

instead of $(\mathcal{A}, \ell) \models F$ we also write $\mathcal{A} \models F[\ell(x_1), \dots, \ell(x_n)]$

Theorem (Revisited)

set $\mathcal{G}$ of universal sentences without $=$ is satisfiable iff $\mathcal{G}$ has a Herbrand model (over $\mathcal{L}$)

Proof.

negation of Herbrand expansion not a tautology

follows from Hintikka's lemma together with: collection of all Herbrand-consistent sets is first-order consistency property, cf. CL ∎

Assumption

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

Definition (revisited)

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

Theorem (revisited)

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.

it remains to show the implication (3) $\Rightarrow$ (1); on the blackboard ∎

Corollary

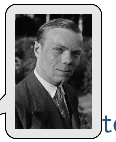
$\mathcal{G}$ has a Herbrand model or $\mathcal{G}$ is unsatisfiable; in the latter case the following statements hold (and are equivalent):

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

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

foundation of  ted reasoning

Herbrand Complexity and Proof Length

Definition

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

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:

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

Example

consider $\mathcal{C} = \{\mathrm{P}(x), \neg\mathrm{P}(\mathrm{f}(x)) \vee \neg\mathrm{P}(\mathrm{g}(x))\}$ 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: $\mathrm{HC}(\mathcal{C}) = 3$

First-Order Resolution

Definition

resolution

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

factoring

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

σ is a mgu of the atomic formulas A and B

Definition

let $\mathcal{C}$ be a set of clauses; define resolution operator $\text{Res}(\mathcal{C})$

- $\text{Res}(\mathcal{C}) = \{D \mid D$ is resolvent or factor with premises in $\mathcal{C}\}$
- $\text{Res}^0(\mathcal{C}) = \mathcal{C}$; $\text{Res}^{n+1}(\mathcal{C}) = \text{Res}^n(\mathcal{C}) \cup \text{Res}(\text{Res}^n(\mathcal{C}))$
- $\text{Res}^*(\mathcal{C}) = \bigcup_{n \geqslant 0} \text{Res}^n(\mathcal{C})$

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

Proof.

1. it suffices to define a suitable instance Γ' of the refutation: for Γ' it is easy to see that $\text{HC}(\mathcal{C}) \leqslant |\Gamma'|$
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 $\mathcal{C}' \subseteq \text{Gr}(\mathcal{C})$ 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
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 $\mathcal{C}' \subseteq \text{Gr}(\mathcal{C})$ 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 $\text{O}(n)$, such that $\text{HC}(\mathcal{C}_n) > 2^n$

Proof.

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

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

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

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

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

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

Statman's Example

Example

consider the following clause set:

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

NB: $\cdot$ is the only function symbol, which is left associative

Lemma

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

Proof.

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

∎

Definition

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

Lemma

$\mathrm{H}_1(y) \to \mathrm{H}_1(\mathrm{T}y)$ *and* $\forall y\ (\mathrm{H}_1(y) \to \mathrm{H}_1(\mathrm{T}y))$ $(= \mathrm{H}_2(\mathrm{T}))$ *are 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* $(m \geqslant 0)$

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

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

∎

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 an informl proof that is linear in n

Proof.

$$\dfrac{\mathrm{pq} \neq \mathrm{p}(\mathrm{T}_n\mathrm{q})\mathrm{q} \qquad \dfrac{\dfrac{\forall x\ \mathrm{p}x = \mathrm{p}(\mathrm{q}x) \qquad \dfrac{\dfrac{\dfrac{\mathrm{H}_n(\mathrm{T}) \qquad \dfrac{\forall x\ (\mathrm{H}_n(x) \to \mathrm{H}_n(\mathrm{T}x))\ (= \mathrm{H}_{n+1}(\mathrm{T}))}{\mathrm{H}_n(\mathrm{T}) \to \mathrm{H}_n(\mathrm{T}_2)}}{\forall x\ (\mathrm{H}_{n-1}(x) \to \mathrm{H}_{n-1}(\mathrm{T}_2x))\ (= \mathrm{H}_n(\mathrm{T}_2))}}{\mathrm{H}_2(\mathrm{T}_n)}}{\forall x\ \mathrm{p}x = \mathrm{p}(\mathrm{q}x) \to \forall x\ \mathrm{p}x = \mathrm{p}(\mathrm{T}_n\mathrm{q})x}}{\forall x\ \mathrm{p}x = \mathrm{p}(\mathrm{T}_n\mathrm{q})x}}{\mathrm{pq} = \mathrm{p}(\mathrm{T}_n\mathrm{q})\mathrm{q}}}{\square}$$

∎

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 ∎

Exercises (Part I)

- Give a direct proof of the fact that any set $\mathcal{G}$ of universal sentences without $=$ is satisfiable iff $\mathcal{G}$ has a Herbrand model (over $\mathcal{L}$).
- Problem 6.3
- Problem 10.11

Break

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

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 $\mathsf{Q}x <_A \mathsf{Q}'y$

Definition

- let A be rectified sentence in NNF
- let $\exists xB$ a subformula of A at position p
- let $\{y_1, \dots, y_k\} = \{y \mid \forall y <_A \exists x\}$ and let $\{z_1, \dots, z_l\} = \mathcal{FV}\mathrm{ar}(\exists xB)$
- $A[B\{x \mapsto f(y_1, \dots, y_k)\}]$ 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 we define the mapping rsk as follows:

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

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

NB: generalises to arbitrary formulas, replacing "existential" by "weak"

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

Definitions (quantifier shifts)

suppose C is free for x

- $\forall x A(x) \land C \equiv \forall x(A(x) \land C)$
- $\forall x A(x) \to C \equiv \exists x(A(x) \to C)$
- $\forall x A(x) \land \forall x B(x) \equiv \forall x(A(x) \land B(x))$

Theorem

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

Example

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

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

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 $\mathrm{HC}(\mathcal{D}'_n) = 2^{2^{2^{O(n)}}}$ 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 $\exists y\ B$

Theorem

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

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

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

Definition (Optimised Skolemisation)

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

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

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

Example

consider a subformula of a sentence A

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

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

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

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

Remark
note that in optimised Skolemisation some literals are deleted from 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) positive or negative factor of D that subsumes D

Example
consider the clause $\mathrm{P}(x) \lor \mathrm{R}(\mathrm{b}) \lor \mathrm{P}(\mathrm{a}) \lor \mathrm{R}(z)$; its condensation is $\mathrm{R}(\mathrm{b}) \lor \mathrm{P}(\mathrm{a})$

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

Example
note that the clause $\mathrm{R}(x,x) \lor \mathrm{R}(y,y)$ does not subsume $\mathrm{R}(\mathrm{a},\mathrm{a})$

Definition
- let $B = \exists \vec{x}(E_1 \land \cdots \land E_\ell)$ 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 $\exists u(\mathrm{R}(y,u) \land \mathrm{R}(z,u))$; its splitting is $\langle\{y\},\{z\}\rangle$

Observation
- let $\langle\{\vec{z}_1\}, \dots, \{\vec{z}_\ell\}\rangle$ be a splitting of $\exists \vec{x}(E_1 \land \cdots \land E_\ell)$
- assume each conjunct 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 $\exists \vec{v}(E_2 \land \cdots \land E_\ell)\{x_i \mapsto f_i(\vec{z}_1, \vec{v})\}$ where $\vec{v}$ are new

Definition (Strong Skolemisation)
- let A be a sentence in NNF and $B = \exists \vec{x}(E_1 \land \cdots \land E_\ell)$ 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

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

Example
consider the formula $\forall x \forall y \forall z(\mathrm{R}(x,y) \land \mathrm{R}(x,z) \to \exists u(\mathrm{R}(y,u) \land \mathrm{R}(z,u)))$
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 of the first clause yields: $\neg\mathrm{R}(x,y) \lor \mathrm{R}(y,\mathrm{f}(y,w))$

Lemma

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

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

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

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?

inner Skolemisation

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

Exercises (Part II)

- Optional: Read-up on intuitionistic predicate logic and prove that the following quantifier shifts are not intuitionistically valid (where x is free for C)
  1. $\forall x(A(x) \lor C) \to (\forall x A(x) \lor C)$
  2. $(\forall x A(x) \to C) \to \exists x(A(x) \to C)$
  3. $(C \to \exists x A(x)) \to \exists x(C \to A(x))$

  NB: these are the only quantifier shifts which are not intuitionistically valid
- Problem 10.14
- Problem 10.15
- Problem 10.16