First-order syntax and proofs

Text: Melvin Fitting, *FOLATP (2nd ed.)*, Sections 5.7,6.5,9.3; Daniel Kroening and Ofer Strichman, *DP*, Section 9.2.1

Kamal Lodaya

March 2021

FOL satisfaction (Alfred Tarski 1933)

$$t ::= \quad x \in V \mid c \in C \mid f(t_1, \ldots, t_n),\ f \in F_n$$
$$A ::= \quad P(t_1, \ldots, t_n),\ P \in R_n \mid t_1 \approx t_2 \mid True \mid False$$
$$\mid (\neg A) \mid (A \vee B) \mid (A \wedge B) \mid (A \supset B) \mid (A \equiv B) \mid \exists x A \mid \forall x A$$

Definition (Given $M = (D, I)$, assignment $s : V \to D$)

- *Assignment r is an x-variant of s if r, s differ at most on the value assigned to variable x.*
- *Satisfaction of formula A extends that of ZOL:*

$$M, s \models P(t_1, \ldots, t_n) \text{ iff } (t_1^{I,s}, \ldots, t_n^{I,s}) \in I(P)$$
$$\ldots$$
$$M, s \models \forall x A \text{ iff } M, r \models A \text{ for all } r\ x\text{-variant of } s$$
$$M, s \models \exists x A \text{ iff } M, r \models A \text{ for some } r\ x\text{-variant of } s$$

(Thus r ranges over mapping x to all values in D)

Exercise (Coincidence lemma)

Show that if assignments s, r coincide on the free variables of formula A, then $M, s \models A$ iff $M, r \models A$.

Prenex normal form algorithm (Thoralf Skolem 1920)

Theorem (Kroening and Strichman, Lemma 9.5)

There is a linear-time algorithm to convert an FOL sentence into prenex normal form, preserving validity.

Example: $\{\forall x(\exists y A(y) \vee (\exists z B(z) \supset C(x)))\}$

1. Eliminate operators other than $\neg, \wedge, \vee$:
   $\{\forall x(\exists y A(y) \vee (\neg\exists z B(z) \vee C(x)))\}$
2. Push negations inside:
   $\{\forall x(\exists y A(y) \vee (\forall z \neg B(z) \vee C(x)))\}$
3. Rename to get distinct variables
4. Move quantifiers out:
   $\{\forall x \exists y \forall z (A(y) \vee (\neg B(z) \vee C(x))\}$

Axiom systems (Bernays, Hilbert-Ackermann 1928)

$$\begin{array}{rl} t ::= & x \in V \mid c \in C \mid f(t_1, \ldots, t_n),\ f \in F_n \\ A ::= & P(t_1, \ldots, t_n),\ P \in R_n \mid t_1 \approx t_2 \mid True \mid False \\ & \mid (\neg A) \mid (A \vee B) \mid (A \wedge B) \mid (A \supset B) \mid (A \equiv B) \mid \exists x A \mid \forall x A \end{array}$$

Proof system fHB: zHB +

(UInst) $\forall x A(x) \supset A(t)$, (EInst) $A(t) \supset \exists x A(x)$

(UGen) If $\vdash A \supset B(p)$, then $\vdash A \supset \forall x B(x)$, for p parameter not occurring in $A, \forall x B$

(UGen) If $\vdash A \supset \neg B(p)$, then $\vdash A \supset \neg\exists x B(x)$, for p parameter not occurring in $A, \exists x B$

One can get derived rules like:

(EGen) If $\vdash A(p) \supset B$, then $\vdash \exists x A(x) \supset B$, provided p parameter not occurring in $A, \exists x B$

Exercise (Witness)

Show that if $\exists x A(x)$ is consistent, so is $A(p)$ where p is a fresh parameter.

- (UInst) easily sound. BD axiom $\forall x \forall y(x + y \approx y + x)$ implies $\forall y(3 + y \approx y + 3)$ which implies $3 + 2 \approx 2 + 3$.
- Soundness of (UGen) can also be seen by an example. Suppose you are trying to show that for every real x, $x^2 + 1 \geq 2x$. Then one way to write this is:
- Let p be a (parametric) real number. Then so is $p - 1$ and $0 \leq (p - 1)^2 = p^2 - 2p + 1 = (p^2 + 1) - 2p$. The result follows.
- Since p is arbitrary, its interpretation could be any element of the domain. The result holds for every real x.

Derivation from theory $Th = \{\forall x(P(x) \supset Q(x)), \forall x P(x)\}$:

1	$\forall x P(x)$	*Premiss*
2	$P(p)$	1, *UInst*
3	$\forall x(P(x) \supset Q(x))$	*Premiss*
4	$P(p) \supset Q(p)$	3, *UInst*
5	$Q(p)$	2, 4, *MP*
6	$\forall x Q(x)$	*UGen*

Derivation from theory $Th = \{\forall x(P(x) \supset Q(x)), \forall x P(x)\}$:

1	$\forall x P(x)$	*Premiss*
2	$P(p)$	1, *UInst*
3	$\forall x(P(x) \supset Q(x))$	*Premiss*
4	$P(p) \supset Q(p)$	3, *UInst*
5	$Q(p)$	2, 4, *MP*
6	$\forall x Q(x)$	*UGen*

Derivation from theory $\{\forall y R(p, y)\}$:

1	$\forall y R(p, y)$	*Premiss*
2	$R(p, q)$	1, *UInst*
3	$\exists x R(x, q)$	2, *EGen*
4	$\forall y \exists x R(x, y)$	3, *UGen*

Derivation from theory $Th = \{\forall x(P(x) \supset Q(x)), \forall x P(x)\}$:

1	$\forall x P(x)$	*Premiss*
2	$P(p)$	1, *UInst*
3	$\forall x(P(x) \supset Q(x))$	*Premiss*
4	$P(p) \supset Q(p)$	3, *UInst*
5	$Q(p)$	2, 4, *MP*
6	$\forall x Q(x)$	*UGen*

Derivation from theory $\{\forall y R(p, y)\}$:

1	$\forall y R(p, y)$	*Premiss*
2	$R(p, q)$	1, *UInst*
3	$\exists x R(x, q)$	2, *EGen*
4	$\forall y \exists x R(x, y)$	3, *UGen*

By the Deduction theorem, $\forall y R(p, y) \supset \forall y \exists x R(x, y)$.
By (EGen), $\exists x \forall y R(x, y) \supset \forall y \exists x R(x, y)$.

Exercise

Show that the converse does not hold.

Conversion to prenex normal form

Derivation from theory $\{\forall x \exists y \forall z (A(y) \vee (B(z) \supset C(x))\}$:

1	$\exists y \forall z (A(y) \vee (B(z) \supset C(p)))$	*Premiss*, *UInst*
2	$\exists y (A(y) \vee (B(t) \supset C(p)))$	1.1 *UInst*, *EGen*
3	$\exists y A(y) \vee (\exists z B(z) \supset C(p))$	2, *EInst*, *PC*, *EGen*
4	$\forall x (\exists y A(y) \vee (\exists z B(z) \supset C(x)))$	3, *UGen*

Conversion to prenex normal form

Derivation from theory $\{\forall x \exists y \forall z (A(y) \vee (B(z) \supset C(x))\}$:

1	$\exists y \forall z (A(y) \vee (B(z) \supset C(p)))$	*Premiss*, *UInst*
2	$\exists y (A(y) \vee (B(t) \supset C(p)))$	1.1 *UInst*, *EGen*
3	$\exists y A(y) \vee (\exists z B(z) \supset C(p))$	2, *EInst*, *PC*, *EGen*
4	$\forall x (\exists y A(y) \vee (\exists z B(z) \supset C(x)))$	3, *UGen*

Derivation from theory $\{\forall x (\exists y A(y) \vee (\exists z B(z) \supset C(x)))\}$:

1	$\exists y A(y) \vee (\exists z B(z) \supset C(q))$	*Premiss*, *UInst*
2	$A(p) \vdash A(p) \vee (B(u) \supset C(q))$	*PC*
3	$\exists y A(y) \vdash A(p) \vee (B(u) \supset C(q))$	2, *EGen*, *Ded*
4	$\neg B(u) \vdash B(u) \supset C(q)$	*PC*
5	$\neg \exists z B(z) \vdash A(p) \vee (B(u) \supset C(q))$	4, *UInst*, *Ded*
6	$C(q) \vdash A(p) \vee B(u) \supset C(q)$	*PC*
7	$A(p) \vee (B(u) \supset C(q))$	3, 5, 6, *Or*, 1, *MP*
8	$\forall x \exists y \forall z (A(y) \vee (B(z) \supset C(x))$	7, *UGen*, *EGen*, *UGen*

FOL Deduction theorem (Hilbert-Bernays 1934)

Theorem (Deduction, Fitting, Theorem 6.5.1)

For theory Th, formulas A, B and a Hilbert-Bernays proof system with (Positive paradox), (Self-distribution) and only the inference rules (MP),(UGen),(EGen),
$Th \cup \{A\} \vdash B$ iff $Th \vdash (A \supset B)$.

Proof.

One of the cases considered in the deduction from $Th \cup \{A\}$ will now be that $Z_j = Y \supset B(p)$ and a later $Z_i = Y \supset \forall x B(x)$.

FOL Deduction theorem (Hilbert-Bernays 1934)

Theorem (Deduction, Fitting, Theorem 6.5.1)

For theory Th, formulas A, B and a Hilbert-Bernays proof system with (Positive paradox), (Self-distribution) and only the inference rules (MP),(UGen),(EGen),
$Th \cup \{A\} \vdash B$ iff $Th \vdash (A \supset B)$.

Proof.

One of the cases considered in the deduction from $Th \cup \{A\}$ will now be that $Z_j = Y \supset B(p)$ and a later $Z_i = Y \supset \forall x B(x)$.

Parameter p cannot occur in $Y, \forall x B$, and we can assume p does not occur in A and in the derivation from $Th \cup \{A\}$.

FOL Deduction theorem (Hilbert-Bernays 1934)

Theorem (Deduction, Fitting, Theorem 6.5.1)

For theory Th, formulas A, B and a Hilbert-Bernays proof system with (Positive paradox), (Self-distribution) and only the inference rules (MP),(UGen),(EGen),
$Th \cup \{A\} \vdash B$ iff $Th \vdash (A \supset B)$.

Proof.

One of the cases considered in the deduction from $Th \cup \{A\}$ will now be that $Z_j = Y \supset B(p)$ and a later $Z_i = Y \supset \forall x B(x)$.

Parameter p cannot occur in $Y, \forall x B$, and we can assume p does not occur in A and in the derivation from $Th \cup \{A\}$.

We are trying to construct a new derivation from Th, where we have $A \supset (Y \supset B(p))$ derived by induction in the place of Z_j.

FOL Deduction theorem (Hilbert-Bernays 1934)

Theorem (Deduction, Fitting, Theorem 6.5.1)

For theory Th, formulas A, B and a Hilbert-Bernays proof system with (Positive paradox), (Self-distribution) and only the inference rules (MP),(UGen),(EGen),
$Th \cup \{A\} \vdash B$ iff $Th \vdash (A \supset B)$.

Proof.

One of the cases considered in the deduction from $Th \cup \{A\}$ will now be that $Z_j = Y \supset B(p)$ and a later $Z_i = Y \supset \forall x B(x)$.

Parameter p cannot occur in $Y, \forall x B$, and we can assume p does not occur in A and in the derivation from $Th \cup \{A\}$.

We are trying to construct a new derivation from Th, where we have $A \supset (Y \supset B(p))$ derived by induction in the place of Z_j.

By PL $(A \wedge Y) \supset B(p)$. As p does not occur in $Y, \forall x B, A$, (UGen) gives $(A \wedge Y) \supset \forall x B(x)$. Again PL derives $A \supset (Y \supset \forall x B(x))$, as required in the place of Z_i. □

FOL Hintikka theory (Jaakko Hintikka 1955)

Definition (Fitting, Definition 5.7.1)

An FOL Hintikka theory Th (also called downwards consistent) has the following conditions in addition to propositional ones.

1. $False, \neg True \notin Th$; for P in At, $\{P, \neg P\} \not\subseteq Th$
2. ... and so on for the propositional conditions seen earlier
3. If $\forall x A$ in Th, then $\{A(t) \mid t \text{ closed term}\} \subseteq Th$
4. If $\neg \exists x A$ in Th, then $\{\neg A(t) \mid t \text{ closed term}\} \subseteq Th$
5. If $\exists x A$ in Th, then $A(p) \in Th$ for fresh parameter p
6. If $\neg \forall x A$ in Th, then $\neg A(p) \in Th$ for fresh parameter p

Thus Hintikka closure of single sentence $\forall x \forall y (E(x, y) \supset E(y, x))$ will convert a directed graph into an undirected graph.

Items (5) and (6) of the definition are tricky.