Доказательство теорем в системе Isabelle / HOL. Интенсивный курс.

- Данный курс подготовлен на основе курса формальных методов за авторством Тобиаса Нипкова (Tobias Nipkow), профессора Мюнхенского Технологического Университета.

- Note: this material is based on the original course developed by Prof. Tobias Nipkow from TUM University. For more details see http://isabelle.in.tum.de/coursematerial/PSV2009-1/

Примечание*

Переведено и озвучено:

- Якимов И.А.
  - ivan.yakimov.research@yandex.ru
- Кузнецов А.С.
  - askuznetsov@sfu-kras.ru

Слайды, отмеченные звездочкой*, добавлены переводчиками, так же добавлены некоторые примечания.

На момент перевода и чтения курса в СФУ оригинальный курс отрыт и доступен публично http://isabelle.in.tum.de/coursematerial/PSV2009-1/

HOL: пропозициональная логика

Обзор

- Натуральная дедукция
- Применение правил в Isabelle/HOL

Нотация

$$\frac{A_1 \ldots A_n}{A}$$ вместо $$[\![A_1 \ldots A_n]\!] \Longrightarrow A$$

Натуральная дидукция

Натуральная дедукция

Для <u>каждого</u> логического оператора ○ введены два вида правил:

- **Интродукция**: *как* я могу *получить* A ○ B?
- **Элиминация**: *что* я могу *вывести из* A ○ B?

*Isabelle/HOL Tuturial

An introduction rule tells us when we can infer a formula containing a specific logical symbol. For example, the conjunction introduction rule says that if we have P and if we have Q then we have $P \wedge Q$. In a mathematics text, it is typically shown like this:

$$\frac{P \quad Q}{P \wedge Q}$$

The rule introduces the conjunction symbol ($\wedge$) in its conclusion. In Isabelle proofs we mainly reason backwards. When we apply this rule, the subgoal already has the form of a conjunction; the proof step makes this conjunction symbol disappear.

In Isabelle notation, the rule looks like this:

$$[\![?P;\ ?Q]\!] \Longrightarrow\ ?P \wedge\ ?Q \qquad \texttt{(conjI)}$$

*Isabelle/HOL Tutorial

Elimination rules work in the opposite direction from introduction rules. In the case of conjunction, there are two such rules. From $P \wedge Q$ we infer P. also, from $P \wedge Q$ we infer Q:

$$\frac{P \wedge Q}{P} \qquad \frac{P \wedge Q}{Q}$$

Now consider disjunction. There are two introduction rules, which resemble inverted forms of the conjunction elimination rules:

$$\frac{P}{P \vee Q} \qquad \frac{Q}{P \vee Q}$$

Правила дедукции для пропозициональной логики

$$\frac{A \quad B}{A \wedge B}\ \texttt{conjI} \qquad \frac{A \wedge B \quad [\![A;B]\!] \Longrightarrow C}{C}\ \texttt{conjE}$$

$$\frac{A}{A \vee B} \quad \frac{B}{A \vee B}\ \texttt{disjI1/2} \qquad \frac{A \vee B \quad A \Longrightarrow C \quad B \Longrightarrow C}{C}\ \texttt{disjE}$$

$$\frac{A \Longrightarrow B}{A \longrightarrow B}\ \texttt{impI} \qquad \frac{A \longrightarrow B \quad A \quad B \Longrightarrow C}{C}\ \texttt{impE}$$

$$\frac{A \Longrightarrow B \quad B \Longrightarrow A}{A = B}\ \texttt{iffI} \qquad \frac{A{=}B}{A \Longrightarrow B}\ \texttt{iffD1} \quad \frac{A{=}B}{B \Longrightarrow A}\ \texttt{iffD2}$$

$$\frac{A \Longrightarrow \mathit{False}}{\neg A}\ \texttt{notI} \qquad \frac{\neg A \quad A}{C}\ \texttt{notE}$$

Интерпретация

$$\frac{A_1 \ldots A_n}{A}$$

Интродукция:

Чтобы доказать A, достаточно доказать A_1 … A_n

Элиминация:

Если я знаю что A_1 и хочу доказать A, то достаточно доказать A_2 … A_n

Эквивалентность

$$\frac{}{t = t}\ \mathtt{refl} \qquad \frac{s = t}{t = s}\ \mathtt{sym} \qquad \frac{r = s \quad s = t}{r = t}\ \mathtt{trans}$$

$$\frac{s = t \quad A(s)}{A(t)}\ \mathtt{subst}$$

Применяется редко, т.к. неявно используется в simp

Больше правил

$$\frac{A \longrightarrow B \quad A}{B}\ \mathrm{mp}$$

$$\frac{\neg A \Longrightarrow False}{A}\ \mathtt{ccontr} \qquad \frac{\neg A \Longrightarrow A}{A}\ \mathtt{classical}$$

Ремарка:

ccontr и classical невыводимы из ND-правил.

Они делают логику «классической», т. е. «неконструктивной».

Доказательство через предположение

$$\frac{A_1 \quad \ldots \quad A_n}{A_i}\,\texttt{assumption}$$

Применение правил: базовая идея

Применение правила $\llbracket A1; \ldots; An \rrbracket \Longrightarrow A$ к подцели C:

- Унификация A и C
- Замена C на n подцелей A1 … An

Работает в обратном порядке, как Prolog!

Пример:

правило: $\llbracket ?P; ?Q \rrbracket \Longrightarrow ?P \wedge ?Q$

подцель: 1. $A \wedge B$

результат: 1. A 2. B

Применение правил: детали

Правило: $[\![A1; \ldots; An]\!] \Longrightarrow A$

Подцель: 1. $[\![B1; \ldots\ Bm]\!] \Longrightarrow C$

Подстановка: $\sigma(A) \equiv \sigma(C)$

Новые подцели: $\sigma([\![B1; \ldots; Bm]\!] \Longrightarrow A1)$

...

$\sigma([\![B1; \ldots; Bm]\!] \Longrightarrow An)$

Команда

apply (rule <имя>)

Доказательства через предположение

apply *assumption*

докажет

1. $\llbracket B1;...;Bm \rrbracket \Longrightarrow C$

унификацией C с одной из посылок (Bi) — бэктрекинг!

Элиминация, `erule`

Как rule, но также

- унифицирует первую посылку правила с предположением
- отбрасывает это предположение

Пример:

Правило: $\llbracket ?P \land ?Q; \llbracket ?P; ?Q \rrbracket \Longrightarrow ?R \rrbracket \Longrightarrow ?R$

Подцель: 1. $\llbracket X; A \land B; Y \rrbracket \Longrightarrow Z$

Унификация: $?P \land ?Q \equiv A \land B$ и $?R \equiv Z$

Новая подцель: 1. $\llbracket X;Y \rrbracket \Longrightarrow \llbracket A;B \rrbracket \Longrightarrow Z$

тоже что и: 1. $\llbracket X;Y;A;B; \rrbracket \Longrightarrow Z$

Доказательство через натуральную дедукцию

Правила интродукции проводят декомпозицию формулы справа от $\Longrightarrow$

Правила элиминации проводят декомпозицию формулы слева от $\Longrightarrow$

Для дальнейшего изучения

- Isabelle/HOL Tutorial — стр. 67-72