Лабораторная 4. Лекции 7-8

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

В данной работе мы закрепим материал по симплификации, а также потренируемся структурировать доказательства.
Нам понадобится следующая таблица с правилами:

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

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

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

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

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

Рис. 1: Правила вывода

Эти правила можно читать сверху вниз — каждый раз, когда верны все посылки (выражения над чертой), верно следствие (выражение внизу). Для перевода в нотацию Isabelle нужно использовать ==>. Например, при вводе команды
thm conjI
мы получим в окне вывода следующее:
?P ⟹ ?Q ⟹ ?P ∧ ?Q
Доказательства буду проводиться в Isar. Типичное доказательство имеет формат:

```
proof
  assume "the-assm"
  have "..."          — intermediate result
  ⋮
  have "..."          — intermediate result
  show "the-concl"
qed
```

Рис. 2: Типичный Isar

О доказательствах было рассказано на лекции, здесь же будет предложен шаблон, по которому можно легко выполнить лабораторную. Ниже приведен пример простого доказательства в Isar.

```
lemma "A ∧ B ⟹ B ∧ A"
proof -
 assume ab: "A ∧ B"
 from ab have a: "A" by (rule conjunct1)
 from ab have b: "B" by (rule conjunct2)
 from b a show "B ∧ A" by (rule conjI)
qed
```

Рис. 3: Типичный Isar на примере

Доказательство похоже на фрагмент математического текста. Оно производится в прямом порядке, то есть от посылки к следствию при помощи правил вывода. Разберем его по шагам.

- В первой строке формулируется утверждение леммы: каждый раз, когда верно «A ∧ B», верно «B ∧ A».
- Далее следует ключевое слово proof, которое сообщает Isabelle что доказательство будет производиться с помощью Isar. Черта отключает автоматическое доказательство.
- Далее, как в «обычном» математическом доказательстве следует фраза «Предположим, что A ∧ B верно», выглядит это так: assume ab: «A ∧ B». Гипотеза именуется с тем, чтобы к ней можно было обращаться далее по тексту теоремы.
- Следом идут две строчки, в которых мы выводим истинность A и B по-отдельности. Это следует из определения A ∧ B. В данном случае используются правила отделения (elemination rule) conjunct1 и conjunct2 вида ?P ∧ ?Q ⟹ ?P и ?P ∧ ?Q ⟹ ?Q. В данном случае правила применяются в *прямом порядке* - левая часть уравнения заменяется правой.
- Наконец из истинности «A» и «B» мы выводим, что «B ∧ A» тоже истинно: from b a show «B ∧ A» by (rule conjI). Здеь conjI имеет вид ?P ⟹ ?Q ⟹ ?P ∧ ?Q

Задание

Вам нужно, согласно варианту, выполнить структурированное доказательство леммы, приведенной в вашем варианте работы. Леммы носят элементарный характер и доказываются в один шаг. Можно использовать только правила, никаких auto, simp и т. д. Ключ к выполнению работы — рисунок 1 (правила вывода). За основу возьмите пример доказательства (рисунок 3).

Варианты

Выберите любые две «леммы», и выполните для них задание:

```
lemma "⟦A; B⟧ ⟹ A ∧ B" [5 lines]
lemma "A ⟹ A ∨ B" [4 lines]
lemma "⟦A ∧ B; ⟦A;B⟧ ⟹ C⟧ ⟹ C" [5 lines]
lemma "⟦(A ⟹ B); (B ⟹ A)⟧ ⟹ A = B" [5 lines]
lemma "⟦A ∨ B; (A ⟹ C); (B ⟹ C)⟧ ⟹ C" [6 lines]
lemma "⟦A ⟶ B; A; (B ⟹ C)⟧ ⟹ C" [6 lines]
```