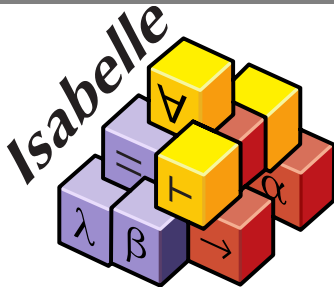


Theorembeweiserpraktikum

Anwendungen in der Sprachtechnologie

LEHRSTUHL PROGRAMMIERPARADIGMEN



Teil I

Einleitung

Ziele des Praktikums

- Kennenlernen der Arbeit mit Theorembeweisern
- Erlernen des Beweisassistenten Isabelle/HOL
- Eigenständige Verifikation eines Projekts aus der Sprachtechnologie

- Termin: Di, 14.00 – 15.30, Praktikumpool -143, Geb. 50.34
- Unterlagen: auf der Webseite
<http://pp.ipd.kit.edu/lehre/SS2018/tba/>
- Master-SPO 2015:
 - Modul *Theorembeweiserpraktikum: Anwendungen in der Sprachtechnologie [M-INFO-102666]*
 - Vertiefungsfach *Theoretische Grundlagen*
 - Vertiefungsfach *Softwaretechnik und Übersetzerbau*
 - oder Wahlbereich
 - 3 ECTS-Punkte

Das Praktikum teilt sich in 2 Hälften

■ 1. Hälfte à 7 Veranstaltungen:

- Übungsblätter
- eigenständige Bearbeitung
- Abgabe jeweils folgender Montag, 12.00 Uhr
- Über https://praktomat.cs.kit.edu/tba_2018_ss/, SCC-Login

■ 2. Hälfte:

- Bearbeitung eines Projekts
- in Zweiergruppen
- Bearbeitungszeitraum: 5.6. – 9.7.2018, 12.00 Uhr
- wieder über den Praktomaten
- 10.7.2018: Informationen zur Projektpräsentation
- letzter Termin 17.7.2018, **10:00 Uhr**, Projektpräsentation im Oberseminar
- An den Dienstagsterminen Zeit für Fragen, Problembesprechung, etc.
(bitte vorher Bescheid geben)

Was wird erwartet?

- Bearbeitung und Abgabe aller Übungsblätter (einzeln)
- Bearbeitung und Abgabe des Projekts als Zweiergruppe
- Anwesenheit an allen Übungsterminen, bei Projektvorstellung und -präsentation
- kurze Abschlusspräsentation im Oberseminar des Lehrstuhls
- keine schriftlichen Ausarbeitungen

Teil II

Was ist ein Theorembeweiser?

Was ist ein Theorembeweiser?

Ein Theorembeweiser beweist Aussagen über **formale Strukturen** durch Anwendung von Regeln.

- Typen und Datentypen (natürliche Zahlen, Listen, Paare, ...)
- Mengen, Relationen, Funktionen
- (funktionale) Programme
- definiert im jeweiligen System!

Was ist ein Theorembeweiser?

Ein Theorembeweiser **beweist Aussagen** über formale Strukturen durch Anwendung von Regeln.

automatisch

- Theorembeweiser versucht Ziel eigenständig zu lösen
- bei Nichtgelingen Meldung, woran gescheitert und Abbruch
- Hilfslemmas zeigen und zum Beweisprozess hinzufügen
- nochmals versuchen, Ziel zu zeigen

prozedural

- Stelle Regeln und automatisierte Prozesse als “Taktiken” bereit
- Beweis ist eine Sequenz von Taktiken
- Fokus auf dem “wie”, Teilziele sind nicht im Beweisskript erkennbar

deklarativ

- Benutzer gibt Beweisstruktur und Teilziele vor
- Taktiken dienen nur, um Schlussfolgerungen zu überprüfen, sollten nicht die Beweisstruktur beeinflussen
- aufwändiger, aber robuster als nur prozedural

Ein Theorembeweiser beweist Aussagen über formale Strukturen durch **Anwendung von Regeln**.

- *Deduktives System*: Anwendung von Regeln auf bestehende Fakten ergibt neue Fakten
- Beweis \equiv vollständiger Regelbaum
- Unifikation und Substitution
- Einführung und Elimination
- Induktion (natürlich, wohlfundiert, strukturell, Regel-Induktion, . . .)

Was ist Unifikation?

- Verfahren, um zwei Terme identisch zu machen
- eventuell durch Ersetzen der schematischen Variablen durch Terme
- Beispiel: Pattern Matching

Beispiel: Unifikation der Terme ($?x, ?y, ?z$ Variablen, a Konstante)

$$f(h(a), g(h(a), h(a))) \quad \text{und} \quad f(h(a), g(h(a), h(a)))$$

1. Schritt: $?x = h(a)$
2. Schritt: $?z = h(a)$
3. Schritt: $?y = a$

Was ist Substitution?

Ersetzung von (logisch) äquivalenten Termen.

Regel:

$$\frac{s = t \quad P[s/x]}{P[t/x]}$$

$P[t/x]$: ersetze x in P durch t

Eselsbrücke: Multiplikation mit einem Bruch: $x(t/x) = t$

Was ist Introdution/Elimination?

- Jeder logische Operator besitzt zwei grundlegende Arten von Regeln:

Introdution: Wie erhalte ich diese Formel?

Elimination: Was kann ich aus dieser Formel folgern?

Beispiel:

Introdution von Disjunktion: $\frac{P}{P \vee Q} \quad \frac{Q}{P \vee Q}$

Elimination von Disjunktion: $\frac{P \vee Q \quad \frac{P}{R} \quad \frac{Q}{R}}{R}$

mehr in den Übungen!

Was ist Induktion?

natürliche Induktion:

zeige $P(0)$ und $P(n) \rightarrow P(n+1)$

strukturelle Induktion:

Induktion über rekursive Datentypen

Beispiel: Polymorphe Listen

datatype $'a \text{ list} = [] \mid 'a \# ('a \text{ list})$

($[]$ = leere Liste, $\#$ = Konkatenation)

Induktion: zeige $P([])$ und $P(xs) \rightarrow P(x \# xs)$

wohlfundierte Induktion:

Induktion über Relationen

Beispiel: $<$ (auch: *starke Induktion*)

zeige $(\forall k < n. P(k)) \rightarrow P(n)$

mehr in den Übungen!

Theorembeweiser sind mächtig, aber kein „goldener Hammer“!

- Kann Sicherheit bzgl. Aussagen beträchtlich erhöhen
- aber “schnell mal etwas formalisieren und beweisen” unmöglich
- meistens werden Aussagen über **Kernprobleme** formalisiert und bewiesen

Sind „Papier und Bleistift“ Beweise nicht einfacher?

- Formalisierung in Theorembeweiser braucht viel Formalisierungsarbeit, auch für scheinbar ‚triviale‘ Dinge
- doch Beweise von Hand enthalten oftmals Fehler, vor allem für komplexe Strukturen
- Viel Aufwand, dafür garantierte Korrektheit!

Wie kann ich sicher sein, dass meine Abstraktion das gewählte Problem beschreibt?

- Im Allgemeinen: gar nicht!
- Je genauer am konkreten Problem, desto größer die Sicherheit, aber ‚Formalisierungslücke‘ bleibt

Teil III

Einführung in Isabelle/HOL

Isabelle

Autoren: Larry Paulson, Tobias Nipkow,
Markus (Makarius) Wenzel

Land: Großbritannien, Deutschland

Sprache: *SML*

Webseite: isabelle.in.tum.de



generisch, d.h. instantiierbar z.B. mit Typ- (HOL)
oder Mengentheorie (Zermelo-Fraenkel) (als *Objektlogiken*)

Beweiserstellung

prozedural mittels **unstrukturierten** Taktikskripten („*apply-Skripten*“)

deklarativ mittels strukturierten **Isar** Beweisskripten
(nahe an üblicher mathematischer Notation)

Im Praktikumpool schon vorinstalliert unter
`/opt/Isabelle2017/bin/isabelle`

Für eigene Installation:

- Auf Seite <http://isabelle.in.tum.de/download.html> gehen
- Isabelle2017-Bundle herunterladen und installieren (ist erklärt)

Starten:

- `Isabelle-Pfad/bin/isabelle jedit`
- oder `Isabelle-Pfad/Isabelle2017`

- Isabelle-Dateien haben die Endung `.thy`
- Eine Datei beginnt mit:
`theory Dateiname imports Basisdateiname (Standard: Main) begin`
- Dann folgt die Formalisierung, die automatisch im Hintergrund geprüft wird
- Wichtig sind dabei die Informationen in den Fenstern „State“ und „Output“
- Das Ende der Datei wird mit `end` markiert

- allgemeine Form: $P_1 \implies P_2 \implies P_3 \implies Q$
- P_1, P_2, P_3 sind Prämissen der Regel (Annahmen)
- Q die Konklusion (Schlussfolgerung)
- \implies heißt “Meta-Implikation” und ist *rechts*-assoziativ.
- Also: “Wenn P_1, P_2 und P_3 , dann Q ”
- Beispiel **Modus Ponens**: $P \rightarrow Q \implies P \implies Q$

- alternative Form: $\llbracket P_1; P_2; P_3 \rrbracket \implies Q$
Plugins \rightarrow Plugin Options... \rightarrow Isabelle \rightarrow General \rightarrow Print Mode = *brackets*

Es gibt folgende logische Operatoren in Isabelle/**HOL**:

<i>Name</i>	<i>Anzeige</i>	<i>Sourcecode</i>	<i>jEdit-Kürzel</i>
Negation	\neg	<code>\<not></code>	<code>~</code>
Konjunktion	\wedge	<code>\<and></code>	<code>/\</code>
Disjunktion	\vee	<code>\<or></code>	<code>\/</code>
Implikation	\longrightarrow	<code>\<longrightarrow></code>	<code>-- ></code>
Gleichheit	$=$		
Ungleichheit	\neq	<code>\<noteq></code>	<code>~=</code>

Die jEdit-Kürzel werden evt. mit einem TAB abgeschlossen.

Achtung: \longrightarrow und \implies sind verschieden

- Jeder Operator besitzt eine Introduktionsregel, wobei der Operator in der Konklusion steht (Standardname ... *I*)
„Was brauche ich, damit die Formel gilt?“
Beispiel: $\text{conj}I: P \implies Q \implies P \wedge Q$
- Jeder Operator besitzt eine Eliminationsregel, wobei der Operator in der ersten Prämisse steht (Standardname ... *E*)
„Was kann ich aus der Formel folgern?“
Beispiel: $\text{conj}E: P \wedge Q \implies (P \implies Q \implies R) \implies R$
- Regeln kann man mittels **thm** $\langle \text{lemma-Name} \rangle$ anzeigen lassen

- In Isabelle werden zu zeigende Aussagen mit dem Schlüsselwort **lemma** eingeleitet (auch möglich: **corollary** und **theorem**)
- danach folgt optional ein Name, beendet durch :
- danach folgt die zu zeigende Aussage in Anführungszeichen

Beispiel:

lemma *imp_uncurry*: " $(P \longrightarrow (Q \longrightarrow R)) \longrightarrow P \wedge Q \longrightarrow R$ "

Dem Lemma folgt dann der Beweis...

- Ein Beweis beginnt mit **proof** (*rule* \langle Regel \rangle) und endet mit **qed**
- Dazwischen werden Zwischenschritte angegeben, in drei Varianten:
 - **assume** " \langle Aussage \rangle " führt eine Aussage ein, die angenommen wird (also nicht bewiesen werden muss).
 - **have** " \langle Aussage \rangle " \langle Beweis \rangle führt eine bewiesene Hilfsaussage ein.
 - **show** " \langle Aussage \rangle " \langle Beweis \rangle beweist eine Aussage, die einen Fall des Beweises abschließt.
- Mehrere Fälle werden durch **next** getrennt

proof unifiziert die Konklusion der Regel mit der zu zeigenden Aussage. Die Prämissen der Regel sind die zu zeigenden Teilziele.

Zur Erinnerung:

$$\text{conjI}: P \implies Q \implies P \wedge Q$$

Beispiel:

```
lemma "foo  $\wedge$  bar"  
proof (rule conjI)  
  show "foo"  $\langle$ proof $\rangle$   
next  
  show "bar"  $\langle$ proof $\rangle$   
qed
```

- Aussagen, die der **proof** von **have** und **show** direkt verwenden soll, werden mit **from** aufgezählt. Sie werden benannt durch
 - Die Aussage in Cartouches (*Aussage*) (`\<open>` bzw. `<<`, `\<close>` bzw. `>>`),
 - oder Namen, die der Aussage optional mit Doppelpunkt vorangestellt wurden oder
 - mit *this*, was stets die letzte gemachte Aussage ist.
- Diese werden, in der angegebenen Reihenfolge, mit den (Konklusionen der) Annahmen der Regel unifiziert
- Bei „**proof** -“ wird *keine* Regel angewandt.
- Bei **qed** dürfen nur noch Fälle offen sein, deren Ziele bereits unter den aufgesammelten Annahmen sind.

Beispiel:

```
from  $\langle A \wedge B \rangle$ 
have "A"
proof (rule conjE)
  assume "A"
  from this
  show "A".
proof - qed
qedby (rule conjE)
```

Zur Erinnerung:

$$\text{conjE: } P \wedge Q \implies (P \implies Q \implies R) \implies R$$

- **then** \equiv **from** *this*
- **with** *a b* \equiv **from** *a b this* (Reihenfolge beachten!)
- **by** (*rule* \langle Regel \rangle) \equiv **proof** (*rule* \langle Regel \rangle) **qed**
- **proof** \equiv **proof** (*rule*) (passende Regel wird automatisch gewählt)
- **..** \equiv **by** (*rule*)
- **.** \equiv **by** - \equiv **proof** - **qed**

Und Abkürzungen anderer Art sind die Beweise

- **oops**: Bricht den aktuellen Beweis ab.
- **sorry**: Beweist alles (und sollte in fertigen Theorien nicht stehen).

Und jetzt Sie

Viel Spaß beim Ausprobieren!

Teil IV

Quantoren in Isabelle/HOL

Die üblichen zwei Quantoren der Logik:

Existenzquantor: \exists (geschrieben `\<exists>`, Kürzel `?`), Syntax: $\exists x. P x$

Allquantor: \forall (geschrieben `\<forall>`, Kürzel `!`), Syntax: $\forall x. P x$

Niedrigere Präzedenz als logische Operatoren, aber höhere als \implies

Beispiele

$\forall x. P x \implies Q x$ In Konklusion x nicht gebunden durch Allquantor

$\forall x. P x \implies \exists x. Q x \implies R$

Zwei verschiedene x in den Annahmen

gleichbedeutend mit $\forall y. P y \implies \exists z. Q z \implies R$

(gebundene Namen sind Schall und Rauch)

$\forall x. P x \longrightarrow Q x$ gleiches x für P und Q

Wie sagt man es Isabelle...?

Argumentation mit Quantoren erfordert Aussagen über *beliebige* Werte
Nur: Wie weiß Isabelle, dass ein Wert *beliebig* ist?

Lösung: Meta-Logik

Syntax: $\bigwedge x. \dots \implies \dots$

\bigwedge heisst **Meta-Allquantor**, Variablen dahinter **Parameter**

Achtung: Niedrigere Präzedenz als \implies

Beispiel: $\bigwedge x y. \forall y. P y \longrightarrow Q z y \implies Q x y \implies \exists x. Q x y$

entspricht $\bigwedge x y. \forall y_1. P y_1 \longrightarrow Q z y_1 \implies Q x y \implies \exists x_1. Q x_1 y$

\forall und \longrightarrow sind nicht identisch mit \bigwedge und \implies , die ersten beiden nur in HOL!

Wir haben übrigens schon mit Meta-Allquantoren gearbeitet: Freie Variablen in Lemmas werden automatisch meta-allquantifiziert!

lemma " $A \bigwedge B \longrightarrow A \vee B$ "

lemma " $\bigwedge A B. A \bigwedge B \longrightarrow A \vee B$ "

Jeder Quantor hat Introduktions- und Eliminationsregel:

■ $allI: (\wedge x. P x) \implies \forall x. P x$

Eine Aussage gilt für beliebige x (Meta-Ebene), also gilt sie auch für alle (HOL-Ebene)

■ $allE: \forall x. P x \implies (P x \implies R) \implies R$

Eine Aussage gilt für alle x , also folgt die Konklusion, wenn ich sie unter Verwendung der Aussage für einen (selbst wählbaren) Term zeigen kann

■ $exI: P x \implies \exists x. P x$

Eine Aussage gilt für einen Term x , also gibt es ein x , wofür sie gilt

■ $exE: \exists x. P x \implies (\wedge x. P x \implies Q) \implies Q$

Eine Aussage gilt für ein x , also folgt die Konklusion, wenn ich sie unter Verwendung der Aussage für einen beliebigen, nicht weiter bestimmten Term zeigen kann

Der Befehl **fix** korrespondiert mit \wedge .

```
have " $\forall x. P x$ "  
proof (rule allI)  
  fix x  
  show " $P x$ "  $\langle$ Beweis $\rangle$   
qed
```

```
from  $\langle \forall x. P x \rangle$   
have " $Q (f x)$ "  
proof (rule allE)  
  assume " $P (f x)$ "  
  then show " $Q (f x)$ "  $\langle$ Beweis $\rangle$   
qed
```

```
have " $\exists x. P x$ "  
proof (rule exI)  
  show " $P (f 0)$ "  $\langle$ Beweis $\rangle$   
qed
```

```
from  $\langle \exists x. P x \rangle$   
have " $R$ "  
proof (rule exE)  
  fix x  
  assume " $P x$ "  
  show " $R$ "  $\langle$ Beweis $\rangle$   
qed
```

Letzteres geht auch ohne neuen Scope:

```
from  $\langle \exists x. P x \rangle$   
obtain x where " $P x$ " by (rule exE)
```

Teil V

Fallunterscheidung

In (klassischen) Beweisen Fallunterscheidung wichtiges Hilfsmittel

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

In Isabelle: Mit der Regel `case_split`: $(P \implies Q) \implies (\neg P \implies Q) \implies Q$

Beispiel:

have "BB \vee \neg BB"

proof (rule case_split)

assume "BB"

then show "BB \vee \neg BB"..
next

assume " \neg BB"

then show "BB \vee \neg BB"..
qed

Statt **proof** (rule case_split) geht auch **proof** (cases "BB").
Vorteil: Die Annahmen sind gleich die richtigen (sonst erfährt Isabelle erst beim ersten **show** was P sein sollte – das klappt ggf. nicht zuverlässig).

Fallunterscheidung: Beispiel

Dieses Lemma wäre ohne Fallunterscheidung so **nicht** (einfach) **lösbar!**

lemma " $B \wedge C \longrightarrow (A \wedge B) \vee (\neg A \wedge C)$ "

proof

assume " $B \wedge C$ " **then have** " B "..

from $\langle B \wedge C \rangle$ **have** " C "..

show " $(A \wedge B) \vee (\neg A \wedge C)$ "

proof (cases A)

assume " A "

from $\langle A \rangle \langle B \rangle$ **have** " $A \wedge B$ "..

then show ?thesis..

next

assume " $\neg A$ "

from $\langle \neg A \rangle \langle C \rangle$ **have** " $\neg A \wedge C$ "..

then show ?thesis..

qed

qed

Teil VI

Definition

Ermöglicht, einen Term zu benennen, so darüber zu abstrahieren und die Abstraktion gezielt zu öffnen

Beispiel:

```
definition answer :: "nat"  
where "answer = 42"
```

Erzeugt Regel: *answer_def*: *answer* = 42

So können auch Funktionen definiert werden:

Beispiel:

```
definition nand :: "bool  $\Rightarrow$  bool  $\Rightarrow$  bool"  
where "nand A B = ( $\neg$  (A  $\wedge$  B))"
```

Erzeugt Regel: *nand_def*: *nand* A B = (\neg (A \wedge B))

definition – Syntaxdefinition

`nand` ist binärer Operator
 \implies Infixoperator bietet sich an

Syntaxdefinition (Infix-Notation)

Schreibe (**infixl** "*Operatorsymbol*" *n*) an die Deklarationszeile, wobei

- **infixl** für linksgebundenen Infixoperator steht, **infixr** für rechtsgebundene
- *Operatorsymbol* ein beliebig wählbares Symbol für den Operator ist,
- *n* eine Zahl ist, welche die Präzedenz dieses Operators angibt

Beispiel: Operator `nand`

definition `nand` :: "*bool* \Rightarrow *bool* \Rightarrow *bool*" (**infixl** " \boxtimes " 36)

where "*A* \boxtimes *B* = (\neg (*A* \wedge *B*))"

Jetzt: *A* \boxtimes *B* \boxtimes *C* gleichbedeutend mit `nand (nand A B) C`

Teil VII

Gleichungen

Das Arbeiten mit Gleichungen ist eine sehr wichtige Beweistechnik. Die Hauptregel dabei ist die Substitution:

$$\frac{s = t \quad P[s/x]}{P[t/x]}$$

Diese Regel gibt es auch in Isabelle:

```
subst: s = t  $\implies$  P s  $\implies$  P t
```

Beispiel:

```
assume "correct answer"
```

```
with answer_def
```

```
have "correct 42" by (rule subst)
```

Auch nützlich:

```
ssubst: s = t  $\implies$  P t  $\implies$  P s
```

```
arg_cong: x = y  $\implies$  f x = f y
```

Gleichheit ist transitiv, auch in Isabelle:

trans: $r = s \implies s = t \implies r = t$

Aber umständlich:

```
lemma "foo = qux"  
proof (rule trans)  
  show "foo = bar" <Beweis 1>  
next  
  show "bar = qux"  
  proof (rule trans)  
    show "bar = baz" <Beweis 2>  
  next  
    show "baz = qux" <Beweis 3>  
  qed  
qed
```

Besser mit **also** und **finally**:

```
lemma "foo = qux"  
proof -  
  have "foo = bar" <Beweis 1>  
  also  
  have "bar = baz" <Beweis 2>  
  also  
  have "baz = qux" <Beweis 3>  
  finally show "foo = qux".  
qed
```

Aber oft **proof** (*rule trans*) zu schreiben wäre sehr umständlich.
Statt dessen: Gleichungsketten!

- Die Befehle **also** und **finally** sollten jeweils einer Aussage (**assume** oder **have**) folgen, die eine Gleichung ist.
- Das abschließende **finally** kombiniert die Aussagen per Transitivität und stellt das Ergebnis (wie **from**) bereit.
- Die Abkürzung *?thesis* steht für die Konklusion des aktuell zu beweisende Lemmas (vor Anwendung von Regeln!).

Typisches Muster:

```
proof -  
  { ... }  
  finally show ?thesis.  
qed
```

- In Ausdrücken steht `...` für die rechte Seite der letzten Aussage.
- Ist ein Lemma *foo* falsch herum, kann man *foo[symmetric]* verwenden.

Gleichungsketten (Beispiel)

lemma " $(A \wedge (A \vee B)) = A$ "

proof -

from *conj_disj_distribL*

have " $(A \wedge (A \vee B)) = ((A \wedge A) \vee (A \wedge B))$ ".

also

from *conj_absorb*

have " $((A \wedge A) \vee (A \wedge B)) = (A \vee (A \wedge B))$ " **by** (*rule arg_cong*)

also

have " $(A \vee (A \wedge B)) = A$ "

proof

<a nested proof>

qed

finally

show " $(A \wedge (A \vee B)) = A$ ".

qed

Gleichungsketten (Beispiel mit Abkürzungen)

lemma " $(A \wedge (A \vee B)) = A$ "

proof -

from *conj_disj_distribL*

have " $(A \wedge (A \vee B)) = ((A \wedge A) \vee (A \wedge B))$ ".

also

from *conj_absorb*

have " $\dots = (A \vee (A \wedge B))$ " **by** (*rule_arg_cong*)

also

have " $\dots = A$ "

proof

<a nested proof>

qed

finally

show *?thesis.*

qed

Randbemerkung: moreover und ultimately

Die **also..finally**-Struktur hat einen kleinen Bruder: **moreover..ultimately**. Hier werden die Aussagen nicht per Transitivität verbunden, sondern einfach gesammelt.

Damit können Verschachtelungen vermieden werden, die Beweise natürlicher aufgebaut und Wiederholungen in **from**-Befehlen verringert werden:

```
have "A ∧ B"  
proof  
  show A  
    ⟨Beweis A⟩  
next  
  show B  
    ⟨Beweis B⟩  
qed
```

```
have A  
  ⟨Beweis A⟩  
moreover  
  have B  
    ⟨Beweis B⟩  
ultimately  
  have "A ∧ B"..
```

Teil VIII

Quick and Dirty: apply-Skripte Oder: Wie es wirklich geht!

Isabelle arbeitet im Wesentlichen mit 3 Modi

theory mode: Deklarationen, Definitionen, Lemmas

state mode: Zwischenaussagen, Fixes, etc.

prove mode: Anwendung von Beweistaktiken

Befehle schalten zwischen den Modi hin und her

Beispiele:

definition: *theory mode* \rightarrow *theory mode*

lemma: *theory mode* \rightarrow *prove mode*

proof: *prove mode* \rightarrow *state mode*

assume: *state mode* \rightarrow *state mode*

show: *state mode* \rightarrow *prove mode*

by: *prove mode* \rightarrow *state mode* | *theory mode*

qed: *state mode* \rightarrow *state mode* | *theory mode*

apply: *prove mode* \rightarrow *prove mode*

verändert das aktuelle Beweisziel (*subgoal*) durch Anwendung der gegebenen *Taktik(en)*

Beispiel:

lemma *conjCommutes*: " $A \wedge B \implies B \wedge A$ "

apply (*rule conjI*)

apply (*erule conjE*)

apply *assumption*

apply (*erule conjE*)

apply *assumption*

done

done: *prove mode* \rightarrow *state mode* | *theory mode*

beendet einen Beweis

- Beweisziel** ist immer das aktuell zu zeigende Ziel unter `subgoal`.
- aktuelle Fakten** sind die gesammelten Fakten unter `this`.
- gegebene ...** sind die Parameter der Taktik.

manuelle Taktiken

- **(minus)**: Fügt die aktuellen Fakten dem Beweisziel hinzu.
 - fact**: Setzt aus den gegebenen Fakten das Beweisziel zusammen (modulo Unifikation und schematischen Typ- und Termvariablen).
- assumption**: Löst das Beweisziel, wenn eine passende Annahme vorhanden ist.
- this**: Wendet die aktuellen Fakten der Reihe nach als Regel auf das Beweisziel an.
- rule**: Wendet die gegebene(n) Regel(n) auf das Beweisziel an. Die aktuellen Fakten werden verwendet, um die Annahmen der Regel zu instanzieren.

- unfold:** Ersetzt die gegebenen Definitionen in allen Beweiszielen.
- fold:** Kollabiert die gegebenen Definitionen in allen Beweiszielen.
- insert:** Fügt die gegebenen Fakten in alle Beweisziele ein.
- erule:** Wendet die gegebene Regel als Eliminationsregel an.
- drule:** Wendet die gegebene Regel als Destruktionsregel an.
- frule:** Wie *drule*, aber hält die verwendete Annahme im Beweisziel.
- intro:** Wendet die gegebenen Regeln **wiederholt** als Introduktionsregel an.
- elim:** Wendet die gegebenen Regeln **wiederholt** als Eliminationsregel an.

Introduktion: Operator steht in der Konklusion (Standardname ... *I*)
„Was brauche ich, damit die Formel gilt?“

Beispiel: *conjI*: $\llbracket P; Q \rrbracket \Longrightarrow P \wedge Q$

Was passiert bei *rule*?

Konklusionen der Regel und des Beweisziels werden unifiziert. Jede Prämisse der Regel wird als neues Beweisziel hinzugefügt.

Elimination: Operator steht in der ersten Prämisse (Standardname ... *E*)
„Was kann ich aus der Formel folgern?“

Beispiel: *conjE*: $\llbracket P \wedge Q; \llbracket P; Q \rrbracket \Longrightarrow R \rrbracket \Longrightarrow R$

Was passiert bei *erule*?

Konklusionen der Regel und des Beweisziels werden unifiziert. Dann wird die erste Prämisse der Regel mit der ersten passenden Prämisse des Beweisziels unifiziert. Die übrigen Prämissen der Regel werden als neue Beweisziele hinzugefügt.

Destruktion: Operator steht in der ersten Prämisse
„Ich benötige eine schwächere Aussage.“

Beispiel: *conjunct1*: $P \wedge Q \implies P$

Was passiert bei *drule*?

Die erste Prämisse der Regel wird mit der ersten passenden Prämisse des Beweisziels unifiziert.
Die übrigen Prämissen der Regel werden als neue Beweisziele hinzugefügt.

Als letztes wird ein neues Beweisziel hinzugefügt, welches die Konklusion der Regel als Prämisse enthält.

Teil IX

Automatische Taktiken

Viele automatische Taktiken für den *logical reasoner* unterscheiden sich in

- der verwendeten Regelmenge,
- ob nur auf ein oder alle Zwischenziele angewendet,
- ob Abbruch bei nichtgelösten Zielen oder Rückgabe an Benutzer,
- ob der Simplifier mitverwendet wird oder nicht,
- ob mehr Zwischenziele erzeugt werden dürfen oder nicht

Im Folgenden werden ein paar Taktiken vorgestellt

- Simplifikationsregeln: Gleichungen
- entsprechende Taktik: `simp` (nur erstes Ziel) bzw. `simp_all` (alle Ziele)
 - besitzt Pool an Termersetzungsregeln
 - prüft für jede solche Regel, ob Term mit linker Seite einer Gleichung unifizierbar
 - falls ja, ersetzen mit entsprechend unifizierter rechter Seite
- genauer: Termersetzung (weil Ausdruck rechts in der Gleichung nicht notwendigerweise einfacher)

Beispiel:

aktuelles Subgoal: $C \implies P$ (*if False then A else B \longrightarrow D*)

`simp` wendet folgende Termersetzungsregel an:

HOL.if_False: (if False then ?x else ?y) = ?y

Resultat: $C \implies P$ (*B \longrightarrow D*)

Auch bedingte Ersetzungsregeln sind möglich, also in der Form

$$[[\dots]] \implies \dots = \dots$$

Dazu: Prämissen der Regel aus aktuellen Annahmen *via Simplifikation* herleitbar

Simplifier modifizieren:

- selbstgeschriebene Simplifikationslemmas zu Taktik hinzufügen:
`apply (simp add: Regel1 Regel2 ...)`
- nur bestimmte Ersetzungsregeln verwenden:
`apply (simp only: Regel1 Regel2 ...)`
- Ersetzungsregeln aus dem Standardpool von `simp` entfernen:
`apply (simp del: Regel1 Regel2 ...)`

Auch möglich: Ersetzungsregeln in den Standardpool von `simp` einfügen
Zwei Varianten:

- Zusatz `[simp]` hinter Lemmanamen
Beispiel: **lemma** `bla [simp]: "A = True \implies A \wedge B = B"`
- mittels **declare** ... `[simp]`
Beispiel: **declare** `foo [simp] bar [simp]`
Analog: mittels **declare** `[simp del]` Ersetzungsregeln
aus Standardpool entfernen
- Analog in einem **proof**-Block: Mit **have** resp. **note**.

Vorsicht!

- Nur Regeln zu Standardpool hinzufügen, deren rechte Seite einfacher als linke Seite!
- Sicherstellen, dass `simp` durch neue Regeln nicht in Endlosschleifen hängenbleibt!

- nur „offensichtliche“ logische Regeln
- nur auf oberstes Zwischenziel angewendet
- nach Vereinfachung Rückgabe an Benutzer
- *clarify* ohne Simplifier, *clarsimp* = *clarify* + *simp*
- kein Aufteilen in Zwischenziele

Oft verwendet um aktuelles Zwischenziel leichter lesbar zu machen

- mächtige Regelmenge
- nur auf oberstes Zwischenziel angewendet
- versucht Ziel komplett zu lösen, ansonsten Abbruch
- kein Simplifier

Schnellster *logical reasoner*, gut auch bei Quantoren

- mächtige Regelmenge, da basierend auf *blast*
- auf alle Zwischenziele angewendet
- nach Vereinfachung Rückgabe an Benutzer, wenn nicht gelöst
- mit Simplifier
- Aufteilen in Zwischenziele

oft verwendete „ad-hoc“-Taktik

force wie *auto*, nur sehr aggressives Lösen und Aufteilen, deswegen anfällig für Endlosschleifen und Aufhängen

- große Regelmenge
- nur auf oberstes Zwischenziel angewendet
- versucht Ziel komplett zu lösen, ansonsten Abbruch
- Simplifier, *fast* nur *logical reasoner*

fastforce ist eine in der Praxis oft gut brauchbare Taktik für das Lösen eines Zwischenziels

- Simplifikationsregeln: möglich bei allen Taktiken mit `Simplifier`
normalerweise `simp:Regelname`, z.B. `apply(auto simp:bla)`
bei `simp` und `simp_all` stattdessen `add:`, z.B. `apply(simp add:bla)`
für Einschränken der Regelmenge: `simp del:` bzw. `simp only:`
`apply(fastforce simp del:bla)` bzw. `apply(auto simp only:bla)`
- Deduktionsregeln: alle Taktiken mit `logical reasoner`
Unterscheidung zwischen Introduktions-, Eliminations- und Destruktionsregeln
 - Einführung: `intro:`, z.B. `apply(blast intro:foo)`
 - Elimination: `elim:`, z.B. `apply(auto elim:foo)`
 - Destruktion: `dest:`, z.B. `apply(fastforce dest:foo)`
- alles beliebig kombinierbar, z.B.
`apply(auto dest:foo intro:bar simp:zip zap)`

- Resolutionskalkül
- nur auf oberstes Zwischenziel angewendet
- versucht Ziel komplett zu lösen, ansonsten Abbruch
- es müssen alle Regeln angegeben werden, die verwendet werden sollen

metis kann sehr gut mit Gleichungen umgehen, wenn diese nicht nur von links nach rechts angewendet werden sollen.

Teil X

Datentypen und primitive Rekursion

Algebraische Datentypen werden über eine Menge von *Konstruktoren* beschrieben, die wiederum weitere Typen als *Parameter* haben. Jeder Wert des Typs ist durch genau einen Konstruktor und den Werten dessen Parameters beschrieben.

Ein Parameter kann auch der definierte Datentyp selbst sein. In dem Fall spricht man von einem rekursiven Datentyp.

Beispiele:

- Eine natürliche Zahl ist entweder Null, oder der Nachfolger einer natürlichen Zahl
- Eine Liste ist entweder leer oder eine weitere List mit zusätzlichem Kopfelement.

Formalisierung in Isabelle/HOL am Bsp. natürliche Zahlen:

datatype *nat* = 0 | Suc *nat*

Also Konstruktoren von nat: 0 und Suc

Soll der Typ eines Konstruktorparameters nicht festgelegt sein, verwendet man den Parametertyp 'a.

Beispiel: Listen mit Typparameter

```
datatype 'a list =  
  Nil      ("[]")  
  | Cons 'a "'a list"    (infixr "#" 65)
```

Konstruktoren von list: [] und # (Infix) ($x\#[] = [x]$)

Damit kann man z.B. folgende Typen bilden:

```
foo :: "nat list  $\Rightarrow$  bool"  
bar :: "nat  $\Rightarrow$  bool list  $\Rightarrow$  nat"  
baz :: "'a list  $\Rightarrow$  'a"
```

Definition von Funktionen über rekursive Datentypen: **fun**
ein Parameter der Funktion kann dabei in seine Konstruktoren aufgeteilt werden.

Auf der rechten Seite der Gleichungen sollte die definierte Funktion höchstens auf die Parameter des Konstruktors angewandt werden.

Beispiel:

```
fun length :: "'a list ⇒ nat"  
  where "length [] = 0"  
        | "length (x#xs) = Suc (length xs)"
```

```
fun tl :: "'a list ⇒ 'a list"  
  where "tl [] = []"  
        | "tl (x#xs) = xs"
```

Es müssen nicht alle Konstruktoren spezifiziert werden:

```
fun hd :: "'a list ⇒ 'a"  
  where "hd (x#xs) = x"
```

```
fun last :: "'a list ⇒ 'a"  
  where "last (x#xs) = (if xs=[] then x else last xs)"
```

Bei nicht enthaltenen Konstruktoren wie z.B. `hd []` nimmt die Funktion den Wert `undefined` an, ein fester Wert in jedem Typ, über den nichts bekannt ist.

weiterer Infixoperator: @ hängt Listen zusammen

Beispiel: $[0,4] @ [2] = [0,4,2]$

rev dreht Listen um, also $rev [0,4,2] = [2,4,0]$

Wie lautet die entsprechende Definition?

```
fun rev :: "'a list  $\Rightarrow$  'a list"  
  where "rev [] = []"  
  | "rev (x#xs) = rev xs @ [x]"
```

„Wenn eine Aussage für jeden möglichen Konstruktor gilt, dann auch für alle Werte des Typs.“

Regel für Listen:

$list.exhaust: (xs = [] \implies P) \implies (\bigwedge a\ as. xs = a \# as \implies P) \implies P$

Wird meist mit der Beweistaktik `cases` verwendet:

lemma `hd_Cons_tl`: `"xs ≠ [] → hd xs # tl xs = xs"`

proof (`rule impI`)

assume `"xs ≠ []"` **show** `"hd xs # tl xs = xs"`

proof (`cases xs`)

assume `"xs = []"`

with `<xs ≠ []>` **have** `False..`

then show `?thesis..`

next

fix `y ys`

assume `"xs = y # ys"`

then show `?thesis` **by** `simp`

qed

qed

Warum **proof** (*cases ..*) und nicht einfach **proof** (*rule List.exhaust*)?
Wegen benannter Fälle!

```
lemma hd_Cons_tl: "xs ≠ [] → hd xs # tl xs = xs"
```

```
proof (rule impI)
```

```
  assume "xs ≠ []"
```

```
  show "hd xs # tl xs = xs"
```

```
  proof (cases xs)
```

```
    case Nil
```

```
    with ⟨xs ≠ []⟩ have False..
```

```
    thus ?thesis..
```

```
  next
```

```
    case (Cons y ys)
```

```
    then show ?thesis by simp
```

```
  qed
```

```
qed
```

(Bei *cases* auf Aussagen heißen die Fälle *True* und *False*.)

Hier geht natürlich auch einfach

```
lemma hd_Cons_tl: "xs ≠ [] ⇒ hd xs # tl xs = xs"
```

```
by (cases xs) auto
```

Fallunterscheidung genügt bei rekursiven Datentypen nicht immer, weil man die Aussage schon für die rekursiven Parameter braucht. Dann hilft **strukturelle Induktion**

z.B. für Listen sieht die Regel wie folgt aus:

$$\text{list.induct: } \llbracket P [] ; \bigwedge x \text{ xs. } P \text{ xs} \implies P (x \# \text{xs}) \rrbracket \implies P \text{ xs}$$

Komfortabler als *rule* ist die Methode *induction*:

- Benannte Fälle wie bei *cases*
- *Fall.IH* ist die Induktionshypothese, also die Aussage für die rekursiven Parameter
- ggf. *Fall.premis* sind die Annahmen, wie sie im Lemma stehen.
- ggf. *Fall.hyps* sind zusätzliche Aussagen, die durch die Induktionsregel eingefügt werden.

Beispiel für strukturelle Induktion

lemma "length (xs @ ys) = length xs + length ys"

proof (induction xs)

case Nil

have "length ([] @ ys) = length ys" **by** simp

also have "... = 0 + length ys" **by** simp

also have "... = length [] + length ys" **by** simp

finally show ?case.

next

case (Cons x xs)

have "length ((x # xs) @ ys) = length (x # (xs @ ys))" **by** simp

also have "... = Suc (length (xs @ ys))" **by** simp

also from Cons.IH **have** "... = Suc (length xs + length ys)"..

also have "... = Suc (length xs) + length ys" **by** simp

also have "... = length (x # xs) + length ys" **by** simp

finally show ?case.

qed

oder natürlich einfach

by (induction xs) auto

Problem: zu spezielle Induktionshypothesen

lemma " $rev\ xs = rev\ ys \implies xs = ys$ "

proof (*induction xs*)

- Fall $[]$ mit *simp* lösbar:

case Nil then show ?case by simp

- bei Induktionsschritt bekommen wir:

Cons.IH: $rev\ xs = rev\ ys \implies xs = ys$

*Cons.prem*s: $rev\ (x \# xs) = rev\ ys$

aber $rev\ ys$ kann nicht gleichzeitig $rev\ xs$ **und** $rev\ (a \# xs)$ sein!

\Rightarrow Induktionshypothese nicht verwendbar

\Rightarrow So kommen wir nicht weiter.

Lösung:

ys muss in der Induktionshypothese eine freie Variable sein!

Umsetzung:

ys nach Schlüsselwort *arbitrary* in der Induktionsanweisung. Damit wird die Induktionshypothese für ys meta-allquantifiziert:

lemma " $rev\ xs = rev\ ys \implies xs = ys$ "

proof (*induction xs arbitrary: ys*)

Nun liefert uns

case (*Cons x xs ys*)

diese Aussagen:

Cons.IH: $rev\ xs = rev\ ?ys \implies xs = ?ys$

Cons.prem: $rev\ (x \# xs) = rev\ ys$

wobei die Variable mit dem Fragezeichen frei ist, also mit jeder beliebigen Liste verwendet werden kann.

Heuristiken für (bisher scheiternde) Induktionen:

- alle freien Variablen (außer Induktionsvariable) mit *arbitrary*
- Induktion immer über das Argument, über das die Funktion rekursiv definiert ist
- Generalisiere zu zeigendes Ziel: Ersetze Konstanten durch Variablen

Teil XI

Eigene Lemmas als Regeln

Lemmas und Regeln

Man kann bewiesene Lemmas als Regeln verwenden!
(Wenig überraschend)

```
lemma mylemma: "even (42::nat)" by simp
```

```
lemma "∃ x. even (x::nat)"
```

```
proof
```

```
  show "even (42::nat)" by (rule mylemma)
```

```
qed
```


Lemmas und Regeln: Annahmen

Man kann bewiesene Lemmas als Regeln verwenden!
Dabei sollten Annahmen mit der Meta-Implikation angegeben werden.

```
lemma mylemma2: "even n  $\implies$  even (3 * n)" by simp
```

```
lemma "even 126"
```

```
proof -
```

```
  have "even 42" by (rule mylemma)
```

```
  then have "even (3 * 42)" by (rule mylemma2)
```

```
  also have "3 * 42 = (126::nat)" by simp
```

```
  finally show ?thesis.
```

```
qed
```

Lemmas und Regeln: Annahmen vs. Isar

Man kann bewiesene Lemmas als Regeln verwenden!
Dabei sollten Annahmen mit der Meta-Implikation angegeben werden.
Das ist in Isar-Beweisen nicht so schön (Annahmen müssen zweimal genannt werden):

```
lemma "even n  $\implies$  even (9 * n)"  
proof -  
  assume "even n"  
  have "even (3 * (3 * n))"  
  proof (rule mylemma2)  
    from (even n)  
    show "even (3 * n)" by (rule mylemma2)  
  qed  
  then show ?thesis by simp  
qed
```

In Isar sind mit den Schlüsselwörter **assumes** und **shows** die Annahmen direkt verfügbar, sie können benannt werden und Attribute wie `[simp]` gesetzt werden.

Außerdem bezeichnet `assms` immer alle Annahmen.

```
lemma times9:
  assumes n_is_even: "even n"
  shows "even (9 * n)"
proof -
  have "even (3 * (3 * n))"
  proof (rule mylemma2)
    from n_is_even — oder from ⟨even n⟩ oder from assms
    show "even (3 * n)" by (rule mylemma2)
  qed
  then show ?thesis by simp
qed
```

Will man die Annahme(n) der ersten Beweismethode übergeben, so fügt man vor **proof** noch **using** `assms` ein. Wichtig bei Induktionsbeweisen!

So wie **assumes** dem \implies entspricht, entspricht **fixes** dem \wedge .
Damit lassen sich die freien Variablen des Lemmas besser betonen und ihr Typ kann festgelegt werden:

```
lemma times9:
  fixes n :: nat
  assumes n_is_even: "even n"
  shows "even (9 * n)"
proof -
  from n_is_even
  have "even (3 * n)" by (rule mylemma2)
  then have "even (3 * (3 * n))" by (rule mylemma2)
  also have "3 * (3 * n) = 9 * n" by simp
  finally show ?thesis.
qed
```

Teil XII

Allgemeine Rekursion

Oftmals ist primitive Rekursion mit einer Regel pro Konstruktor zu einschränkend.

Manche rekursive Definitionen haben z.B. zwei Basisfälle oder brauchen Rekursion in mehr als einem Parameter.

Beispiel “mehrere Basisfälle”: Fibonacci-Zahlen

```
fun fib :: "nat  $\Rightarrow$  nat"  
  where "fib 0 = 1"  
        | "fib (Suc 0) = 1"  
        | "fib (Suc (Suc n)) = fib n + fib (Suc n)"
```

Beispiel “Rekursion in mehreren Parametern”: Zippen von Listen

```
fun zip :: "'a list  $\Rightarrow$  'b list  $\Rightarrow$  ('a  $\times$  'b) list"  
  where "zip [] [] = []"  
        | "zip (a#as) (b#bs) = (a,b)#zip as bs"
```

fun definiert Funktionen durch *Pattern Matching*.

Dabei werden nur “lineare Patterns” unterstützt: Variablen dürfen auf den linken Seiten jeweils nur höchstens einmal vorkommen.

Es ist erlaubt, dass sich Patterns überlappen. Es wird die erste passende Regel angewandt.

Damit sind Defaultregeln möglich, die alle restlichen Fälle behandeln.

Beispiel: Separatorzeichen zwischen je zwei Elemente einer Liste

```
fun sep :: "'a ⇒ 'a list ⇒ 'a list"  
where "sep a (x#y#zs) = x#a#sep a (y#zs)"  
      | "sep a xs      = xs"
```

In **fun** definierte Regeln landen im Simplifier, können auch direkt mit `Funktionsname.simps` angesprochen werden.

Beispiel: `fib.simps`:

```
fib 0 = 1
fib (Suc 0) = 1
fib (Suc (Suc ?n)) = fib ?n + fib (Suc ?n)
```

Beispiel: `sep.simps`

```
sep ?a (?x # ?y # ?zs) = ?x # ?a # sep ?a (?y # ?zs)
sep ?a [] = []
sep ?a [?v] = [?v]
```

Beachte: Die Defaultregel (`sep a xs = xs`) generiert **zwei** Regeln, damit das Pattern-Matching vollständig ist.

Analog definiert **fun** auch für jede Funktion eine Induktionsregel

Funktionsname.induct

Diese kann man im Induktionsbeweis verwenden:

proof (*induction Funktionsparameter rule:Funktionsname.induct*)

Das nennt man *Regelinduktion*.

Beispiel: *sep.induct*

$$\llbracket \bigwedge a \ x \ y \ zs. \ ?P \ a \ (y \ \# \ zs) \implies \ ?P \ a \ (x \ \# \ y \ \# \ zs); \bigwedge a. \ ?P \ a \ []; \bigwedge a \ v. \ ?P \ a \ [v] \rrbracket \implies \ ?P \ ?a0.0 \ ?a1.0$$

lemma "map f (sep x ys) = sep (f x) (map f ys)"

proof (*induction x ys rule:sep.induct*) generiert folgende 3 subgoals:

1. $\bigwedge a \ x \ y \ zs. \ \text{map } f \ (\text{sep } a \ (y \ \# \ zs)) = \text{sep } (f \ a) \ (\text{map } f \ (y \ \# \ zs)) \implies \text{map } f \ (\text{sep } a \ (x \ \# \ y \ \# \ zs)) = \text{sep } (f \ a) \ (\text{map } f \ (x \ \# \ y \ \# \ zs))$
2. $\bigwedge a. \ \text{map } f \ (\text{sep } a \ []) = \text{sep } (f \ a) \ (\text{map } f \ [])$
3. $\bigwedge a \ v. \ \text{map } f \ (\text{sep } a \ [v]) = \text{sep } (f \ a) \ (\text{map } f \ [v])$

fun ist sehr mächtig und in den meisten Fällen ausreichend, um rekursive Funktionen zu definieren.

Aber: auch mit **fun** kann es Probleme geben, z.B. bei wechselseitiger Rekursion oder falls **fun** die Termination nicht selbst beweisen kann.

Lösung: function

Braucht jedoch selbstgeschriebenen Vollständigkeits- und Terminationsbeweis...

Mehr dazu im **function**-Tutorial unter

<http://isabelle.in.tum.de/dist/Isabelle/doc/functions.pdf>

Teil XIII

Wechselseitige Rekursion

Ein bisher ungelöstes Problem bei Rekursion: Was tun bei mehreren Datentypen, die sich gegenseitig bei der Definition verwenden?

datatype

```
'a aexp = — arithmetische Ausdrücke  
  Const nat  
  | Var 'a  
  | Sum "'a aexp" "'a aexp"  
  | Diff "'a aexp" "'a aexp"  
  | IF "'a bexp" "'a aexp" "'a aexp"
```

and

```
'a bexp = — boole'sche Ausdrücke  
  Less "'a aexp" "'a aexp"  
  | And "'a bexp" "'a bexp"  
  | Neg "'a bexp"
```

Definitionen eines Größenmaßes für arithmetische Ausdrücke

Ansatz:

```
fun asize :: "'a aexp  $\Rightarrow$  nat"
  and bsize :: "'a bexp  $\Rightarrow$  nat"

  where "asize (Const n) = 1"
        | "asize (IF b a1 a2) = 1 + asize a1 + asize a2 + ?"
        | ...

        | "bsize (Neg b) = 0"
        | "bsize (Less a1 a2) = 1 + asize a1 + asize a2"
```

Wir brauchen eine Definition für die Größe von boole'schen Ausdrücken!

Dazu gleichzeitige Definition der Funktion *asize* für *'a aexp*
und *bsize* für *'a bexp*.

Beweisen mit wechselseitig rekursiv definierten Datentypen

Wir wollen nun zeigen, dass die Größe jedes arithmetischen Ausdrucks mindestens 1 ist

1. 2. 3. Versuch:

lemma

fixes $a::\text{'a aexp}$ **and** $b::\text{'a bexp}$

shows "asize $a > 0$ " **and** "bsize $b > 0$ "

proof (induction a **and** b) **qed** auto

müssen beide Parameter getrennt durch **and** angeben

Problem: Wegen automatischer Verallgemeinerung des Lemmas haben a und b unterschiedliche Variablentypen! $a::\text{'a aexp}$, $b::\text{'b bexp}$

Komisches subgoal: ?P2.0

Wir haben keine Aussage über die Größe von boole'schen Ausdrücken!

Lemma für wechselseitige Rekursion hat so viele “Teillemmas” wie Datentypen rekursiv definiert.

Was passiert jedoch, wenn ein “Teillemma” nur gezeigt werden kann, wenn in der Induktionshypothese bestimmte Variablen allquantifiziert werden müssen?

Wir kennen die Lösung schon: **arbitrary**

lemma "P t" "Q a t ts"

proof (induction t **and** ts **arbitrary**: **and** a)

q braucht a in der Induktionshypothese quantifiziert, also in einem **arbitrary**

Auch hinter **arbitrary** werden die zu quantifizierenden Variablen für jedes Lemma mit **and** getrennt.

Teil XIV

Abkürzungen

abbreviation

Das Schlüsselwort **abbreviation** führt eine rein syntaktische Abkürzung ein, die bei der Eingabe verwendet werden kann und automatisch bei der Ausgabe berücksichtigt wird.

abbreviation `"sort \equiv sort_key ($\lambda x. x$)"`

Auf Typeebene funktioniert das mit **type_synonym**.

type_synonym `'a env = "'a \Rightarrow nat"`

Innerhalb eines Isar-Beweises können Terme **let**-gebunden werden.

Beispiel „Cantors Theorem“

```
theorem "∃ S. S ∉ range (f :: 'a ⇒ 'a set)"
```

```
proof
```

```
  let ?S = "{x. x ∉ f x}"
```

```
  show "?S ∉ range f"
```

```
  ...
```

Auch möglich: **define** führt eine neue (lokale) Konstante ein.

```
define S where "S = {x. x ∉ f x}"
```

Die definierende Gleichung von s heißt (standardmäßig) S_def .

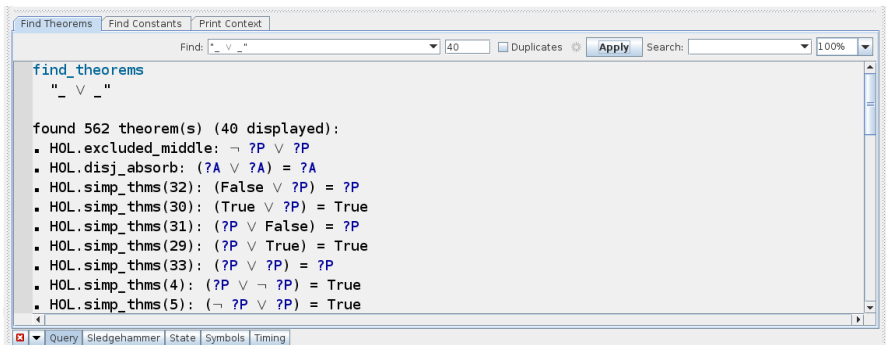
Teil XV

Theoreme finden

Befehle, um Theoreme zu finden:

- **find_theorems**
zeigt alle Theoreme an (wenig hilfreich).
- **find_theorems** *name:classic*
findet alle Theoreme mit *classic* im Namen.
- **find_theorems** *length*
find_theorems *"?a ∨ ?a"*
find_theorems *"_ ∨ (_ ∨ _)"*
findet alle Theoreme, die den entsprechend Term enthalten.
- **find_theorems** *length name:induct*
kombiniert die Suchkriterien.
- **find_theorems** *(100) name:induct*
zeigt bis zu 100 Theoreme an.
- **print_theorems**
zeigt alle durch den vorherigen Befehl (z.B. **fun**) erzeugten Theoreme.

Oder:



The screenshot shows a software interface with three tabs: "Find Theorems", "Find Constants", and "Print Context". The "Find Theorems" tab is active. The search input field contains the query `"_ ∨ _"`. To the right of the input field, there is a dropdown menu showing the number "40", a checkbox for "Duplicates", and an "Apply" button. Further right, there is a "Search:" label, another dropdown menu, and a "100%" zoom level dropdown.

The main content area displays the following text:

```
find_theorems
  "_ ∨ _"

found 562 theorem(s) (40 displayed):
  HOL.excluded_middle:  $\neg ?P \vee ?P$ 
  HOL.disj_absorb:  $(?A \vee ?A) = ?A$ 
  HOL.simp_thms(32):  $(\text{False} \vee ?P) = ?P$ 
  HOL.simp_thms(30):  $(\text{True} \vee ?P) = \text{True}$ 
  HOL.simp_thms(31):  $(?P \vee \text{False}) = ?P$ 
  HOL.simp_thms(29):  $(?P \vee \text{True}) = \text{True}$ 
  HOL.simp_thms(33):  $(?P \vee ?P) = ?P$ 
  HOL.simp_thms(4):  $(?P \vee \neg ?P) = \text{True}$ 
  HOL.simp_thms(5):  $(\neg ?P \vee ?P) = \text{True}$ 
```

At the bottom of the interface, there is a status bar with a red square icon, a dropdown menu showing "Query", and three buttons: "Sledgehammer", "State", and "Timing".

Teil XVI

Induktive Prädikate und Mengen

Schlüsselwort: **inductive**, Syntax wie **fun**

Beispiel 1: Die geraden Zahlen als induktives Prädikat

```
inductive even :: "nat  $\Rightarrow$  bool"  
  where "even 0"  
  | "even n  $\implies$  even (n + 2)"
```

Beispiel 2:

Welche Eigenschaft über Strings beschreibt folgendes Prädikat?

```
inductive foo :: "string  $\Rightarrow$  bool"  
  where "foo [c]"  
  | "foo [c,c]"  
  | "foo s  $\implies$  foo (c#s@[c])"
```

Der Parameterstring ist ein Palindrom!

Induktive Prädikate werden nicht rekursiv über Datentypen definiert, sondern über ein **Regelwerk**, normalerweise bestehend aus

- einer oder mehreren Basisregeln und
- einer oder mehreren induktiven Regeln, wobei das Prädikat in den Prämissen mit “kleineren” Parametern vorkommt (evtl. auch mehrfach).

Das Prädikat gilt für bestimmte Parameter, wenn es durch (endliche) Anwendung der Basis- und induktiven Regeln konstruiert werden kann

Jeder Regel kann einzeln ein Name gegeben werden:

```
inductive palin :: "string  $\Rightarrow$  bool"  
  where OneElem: "palin [c]"  
        | TwoElem: "palin [c,c]"  
        | HdLastRec: "palin s  $\Longrightarrow$  palin (c#s@[c])"
```

Diese Regeln zusammengefasst als *palin.intros*
(allgemein *Prädikatname.intros*)
sieht wie folgt aus:

```
palin [?c]  
palin [?c, ?c]  
palin ?s  $\Longrightarrow$  palin (?c # ?s @ [?c])
```

Meist verwendet man jedoch die einzelnen Regelnamen.

Da das Prädikat aus Regeln aufgebaut wird ist eine “Fallunterscheidung” möglich, mit welcher Regel das Prädikat erzeugt wurde.

Diese Argumentation über den Regelaufbau heißt *Regelinversion*.

Die entsprechende Regel heißt *Prädikatname.cases* und wird mit der Taktik *cases* oder als Eliminationsregel (in automatischen Taktiken) verwendet:

Beispiel *palin.cases*:

$$\llbracket \text{palin } ?a; \bigwedge c. ?a = [c] \implies ?P; \bigwedge c. ?a = [c, c] \implies ?P; \\ \bigwedge s c. \llbracket ?a = c \# s @ [c]; \text{palin } s \rrbracket \implies ?P \rrbracket \implies ?P$$

from $\langle \text{palin } s \rangle$ **have** "hd s = last s"

proof (*cases rule: palin.cases*)

liefert 3 Teilziele:

1. $\bigwedge c. s = [c] \implies \text{hd } s = \text{last } s$
2. $\bigwedge c. s = [c, c] \implies \text{hd } s = \text{last } s$
3. $\bigwedge sa c. \llbracket s = c \# sa @ [c]; \text{palin } sa \rrbracket \implies \text{hd } s = \text{last } s$

Oftmals ist Fallunterscheidung nicht genug und wir brauchen eine Induktionshypothese für Prädikate in der Prämisse einer Regel.

Dafür gibt es die Induktionsregel *Prädikatname.induct*.

Beispiel *palin.induct*:

$$\llbracket \text{palin } ?x; \bigwedge c. ?P [c]; \bigwedge c. ?P [c, c]; \\ \bigwedge s c. \llbracket \text{palin } s; ?P s \rrbracket \implies ?P (c \# s @ [c]) \rrbracket \implies ?P ?x$$

from $\langle \text{palin } s \rangle$ **have** "hd s = last s"

proof (induction rule: *palin.induct*)

liefert Teilziele

1. $\bigwedge c. \text{hd } [c] = \text{last } [c]$
2. $\bigwedge c. \text{hd } [c, c] = \text{last } [c, c]$
3. $\bigwedge s c. \llbracket \text{palin } s; \text{hd } s = \text{last } s \rrbracket \\ \implies \text{hd } (c \# s @ [c]) = \text{last } (c \# s @ [c])$

Wechselseitigkeit ist auch bei induktiven Definitionen möglich und funktioniert analog zu wechselseitiger Rekursion.

Beispiel:

```
inductive even :: "nat  $\Rightarrow$  bool"  
  and odd :: "nat  $\Rightarrow$  bool"  
  where "even 0"  
    | "odd n  $\implies$  even (Suc n)"  
    | "even n  $\implies$  odd (Suc n)"
```

generiert Regeln *eval.cases*, *odd.cases*, *even_odd.induct* and *even_odd.inducts*

Wie bei **fun**: Erstere Induktionsregel benötigt \wedge -Verknüpfung von *even* und *odd* in Konklusion, zweite liefert *zwei* Regeln für zwei **and**-verbundene Lemmas.

Statt induktiver Präkate sind auch **induktive Mengen** möglich.
Das Schlüsselwort ist **inductive_set** und die Signatur verwendet
entsprechend `'a set` statt `'a \Rightarrow bool`.

Manchmal braucht man fixe Parameter, die beim Induktionsschritt der
Induktionsregel konstant bleiben.

Diese müssen nach **for** mit Namen und Signatur angegeben werden.

Beispiel: Reflexive, transitive Hülle

```
inductive rtc :: ('a  $\Rightarrow$  'a  $\Rightarrow$  bool)  $\Rightarrow$  'a  $\Rightarrow$  'a  $\Rightarrow$  bool
```

```
for r :: "'a  $\Rightarrow$  'a  $\Rightarrow$  bool"
```

```
where refl: "rtc r a a"
```

```
| trans: "[[ rtc r a b; r b c ] ]  $\Longrightarrow$  rtc r a c"
```

```
rtc.induct: [[rtc ?r ?x ?y;  $\wedge$ r a. ?P r a a;
```

```
 $\wedge$ r a b c. [[rtc r a b; ?P r a b; r b c]]  $\Longrightarrow$  ?P r a c]
```

```
 $\Longrightarrow$ ?P ?r ?x ?y   rtc.induct: [[rtc ?r ?x ?y;  $\wedge$ a. ?P a a;
```

```
 $\wedge$ a b c. [[rtc ?r a b; ?P a b; ?r b c]]  $\Longrightarrow$  ?P a c]
```

```
 $\Longrightarrow$ ?P ?x ?y
```

Teil XVII

Verknüpfung von Beweismethoden

Hintereinanderausführung mit Backtracking

lemma " $\forall x. P x \implies \forall x. Q x \implies Q a$ "

apply (*erule allE*)

by *assumption* \longleftarrow geht schief!

stattdessen:

lemma " $\forall x. P x \implies \forall x. Q x \implies Q a$ "

by (*erule allE, assumption*) \longleftarrow geht gut!

, wendet Beweismethoden hintereinander an und verwendet dabei gemeinsamen Backtracking-Stack.

Structural Composition

apply $(m_1; m_2)$ wendet m_2 auf alle Teilziele an, die durch die Anwendung von m_1 neu entstehen.

Alternative Choices

apply $(m_1 | m_2)$ wendet m_1 an. (Nur) falls m_1 fehlschlägt wird m_2 angewendet.

Try

apply $m?$ wendet m an, bricht aber nicht ab falls Anwendung fehlschlägt.

Repeat

apply $m+$ wendet m mehrfach an (min. 1 mal), bis m fehlschlägt.

Restriction to subgoals

apply $m[n]$ wendet m an und schränkt den Beweiszustand dabei auf die ersten n Teilziele ein.

Teil XVIII

Automatische Beweissuche

“ISABELLE/HOL used SLEDGEHAMMER. It’s super effective!”

Das Kommando **sledgehammer** führt eine automatische Beweissuche auf dem aktuellen Teilziel durch.

Optionen

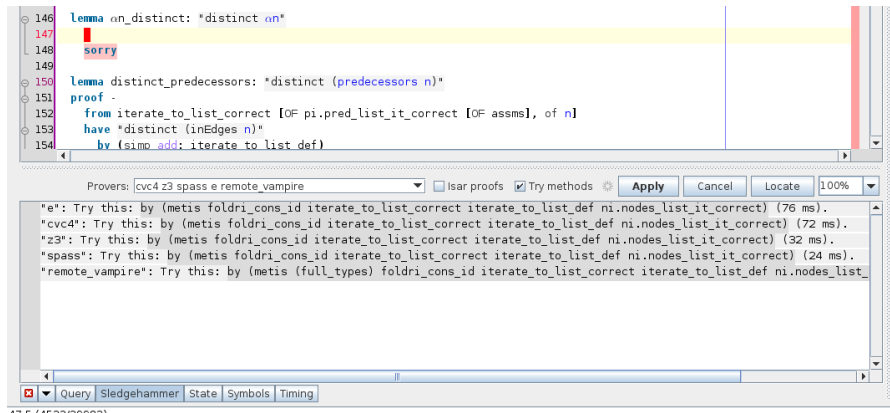
timeout Setzt die maximale Suchdauer in Sekunden fest.
Beispiel `[timeout = 360]`

isar_proofs Erzeuge Isar-Beweise anstelle von Ein-Zeilern (verwendet nur ATPs, keine SMT-Solver).

provers Verwende nur die angegebenen Beweiser.
Beispiel `[provers = e spass remote_vampire]`

Siehe auch: `isabelle doc sledgehammer`

sledgehammer ist in Isabelle/jEdit auch als Panel verfügbar:



```
146 lemma on_distinct: "distinct on"
```

```
147 sorry
```

```
148
```

```
149
```

```
150 lemma distinct_predecessors: "distinct (predecessors n)"
```

```
151 proof -
```

```
152   from iterate_to_list_correct [OF pi.pred_list_it_correct [OF assms], of n]
```

```
153   have "distinct (inEdges n)"
```

```
154   by (simp add: iterate_to_list_def)
```

Provers: `cvc4 z3 spass e remote_vampire` Isar proofs Try methods 100%

"e": Try this: by (metis foldri_cons_id iterate_to_list_correct iterate_to_list_def ni.nodes_list_it_correct) (76 ms).
"cvc4": Try this: by (metis foldri_cons_id iterate_to_list_correct iterate_to_list_def ni.nodes_list_it_correct) (72 ms).
"z3": Try this: by (metis foldri_cons_id iterate_to_list_correct iterate_to_list_def ni.nodes_list_it_correct) (32 ms).
"spass": Try this: by (metis foldri_cons_id iterate_to_list_correct iterate_to_list_def ni.nodes_list_it_correct) (24 ms).
"remote_vampire": Try this: by (metis (full_types) foldri_cons_id iterate_to_list_correct iterate_to_list_def ni.nodes_list_it_correct)

Query Sledgehammer State Symbols Timing

Teil XIX

Split-Regeln

“Some people, when confronted with a subgoal, think ‘I know, I’ll use a split rule.’ Now they have two subgoals.”

Für jeden mit **datatype** erzeugten Typ T , wird auch eine Konstante $case_T$ erzeugt, welche für *Pattern Matching* verwendet wird.

Beispiel

```
datatype color = Red | Black
```

```
datatype 'a rbt = Empty | Node color "'a rbt" 'a "'a rbt"
```

liefert

```
case_color :: "'a ⇒ 'a ⇒ color ⇒ 'a"
```

```
case_rbt :: "'a ⇒ (color ⇒ 'b rbt ⇒ 'b ⇒ 'b rbt ⇒ 'a) ⇒ 'b rbt  
⇒ 'a"
```

mit Syntax

```
case_color f g c ≡ case c of Red ⇒ f | Black ⇒ g
```

```
case_rbt f g t ≡ case t of Empty ⇒ f | Node c l v r ⇒ g c l v r
```

Wie kann der Simplifier mit *case*-expressions umgehen?

Lösung: Splitter

- Der *Splitter* ist Teil des Simplifiers.
- Wird aufgerufen, wenn Rewriting abgeschlossen.
- Wendet eine Split-Regel an (falls möglich).
- Startet Simplifikation auf dem/n neue/n Teilziel/en.

Split-Regel für *color*:

`color.split: P (case color of Red \Rightarrow f1 | Black \Rightarrow f2)`

`$\longleftrightarrow (color = Red \longrightarrow P f1) \wedge (color = Black \longrightarrow P f2)$`

Split-Regeln gibt es in zwei Varianten:

für Konklusion: $?P (f ?a ?b ?c) \longleftrightarrow ?Q ?a ?b ?c$

- Splitter unifiziert linke Seite mit Teiltermen der Konklusion aus dem aktuellen Ziel.
- Ersetze unifizierten Teilterm durch rechte Seite.

für Annahmen: $?P (f ?a ?b ?c) \longleftrightarrow \neg ?Q ?a ?b ?c$

- Splitter unifiziert linke Seite mit Teiltermen der Annahmen aus dem aktuellen Ziel.
- Ersetze unifizierten Teilterm durch rechte Seite
- **und** löse einige logische Verknüpfungen auf:
 - Top-Level Disjunktionen in $?Q$ werden zu Teilzielen
 - Konjunktionen in $?Q$ werden zu einzelnen Annahmen (des jeweiligen Teilziels)
 - Negationen von $?P$ in $?Q$ werden „richtig rumgedreht“.

Split in Konklusion:

```
lemma fixes n :: nat
  shows "even (case c of Red  $\Rightarrow$  2*n | Black  $\Rightarrow$  4*n)"
  by (simp split: color.split)
```

Split in Annahme:

```
lemma fixes n :: nat
  assumes "even (case c of Red  $\Rightarrow$  n | Black  $\Rightarrow$  m)"
  shows "even (n*m)"
  by (simp split: color.split_asm)
```

```
color.split: P (case color of Red  $\Rightarrow$  f1 | Black  $\Rightarrow$  f2)
 $\longleftrightarrow$  (color = Red  $\longrightarrow$  P f1)  $\wedge$  (color = Black  $\longrightarrow$  P f2)
```

```
color.split_asm: P (case color of Red  $\Rightarrow$  f1 | Black  $\Rightarrow$  f2)
 $\longleftrightarrow$   $\neg$  (color = Red  $\wedge$   $\neg$  P f1  $\vee$  color = Black  $\wedge$   $\neg$  P f2)
```

```
color.splits = color.split color.split_asm
```


Split-Regeln gibt es nicht nur für *case*-expressions eines Datentyps, sondern für beliebige Funktionssymbole.

Beispiel: *if*

split_if:

$$P (\text{if } Q \text{ then } x \text{ else } y) \longleftrightarrow (Q \longrightarrow P x) \wedge (\neg Q \longrightarrow P y)$$

split_if_asm:

$$P (\text{if } Q \text{ then } x \text{ else } y) \longleftrightarrow \neg (Q \wedge \neg P x \vee \neg Q \wedge \neg P y)$$

Teil XX

Maps

Map: partielle Abbildung, also rechte Seite undefiniert für manche linke Seite

Typen inklusive Undefiniertheit in Isabelle: *'a option*

datatype *'a option = None | Some 'a*

- enthält alle Werte in *'a* mit *Some* vorangesetzt
- spezieller Wert *None* für Undefiniertheit

Beispiel: *bool option* besitzt die Elemente *None*, *Some True* und *Some False*

Maps in Isabelle von Typ $'a$ nach $'b$ haben Typ $'a \Rightarrow 'b$ *option* oder kurz $'a \rightarrow 'b$ (\rightarrow ist $\langle \text{rightarrow} \rangle$, Kürzel \rightarrow)

- leere Map (also überall undefiniert): *empty*
- Update der Map M , so dass x auf y zeigt: $M(x \mapsto y)$ (\mapsto : $| - \rangle$)
- Wert von x in Map M auf undefiniert setzen: $M(x := None)$
(Hinweis: $M(x \mapsto y)$ entspricht $M(x := Some\ y)$)
- x hat in Map M Wert y , wenn gilt: $M\ x = Some\ y$
- x ist in Map M undefiniert, wenn gilt: $M\ x = None$
- um Map eigenen Typnamen zu geben: **type_synonym**
Beispiel: **type_synonym** *nenv = nat \rightarrow bool*

Falls mehr Infos zu Maps nötig: *Isabelle-Verzeichnis/src/HOL/Map.thy*

- Projektbeginn: 5.6.2018 (heute)
- Bearbeitung in Zweierteams
- Isabelle-Rahmen zu den Projekten sind vorgegeben
- Abgabe: 9.7.2018, 12:00 Uhr via Praktomat
- ab jetzt: freiwillige Dienstagstermine mit weiterführendem Material
Wünsche dazu gerne an uns.
- bei Problemen **frühzeitig** melden!
- Projektpräsentation: 17.7.2018, **10:00 Uhr** (SR 010)
- Infos dazu: 10.7.2018, 14:00 Uhr (Poolraum -143)

Teil XXI

Formale Semantik

“there are formal semantics, informal semantics, and then there’s the C standard” – @johnregehr

Zwei Konzepte bei Programmiersprachen (analog zu natürlicher Sprache), *Syntax* und *Semantik*

- Syntax:**
- Regeln für korrekte Anordnung von Sprachkonstrukten
 - In Programmiersprachen meist durch Grammatik, vor allem in BNF (Backus-Naur-Form) gegeben
 - Angegeben im Sprachstandard

- Semantik:**
- Bedeutung der einzelnen Sprachkonstrukte
 - Bei Programmiersprachen verschiedenste Darstellungsweisen:
 - implizit (über eine Implementierung definiert)
 - informal (Beispiele, erläuternder Text etc.)
 - **formal (Regelsysteme, Funktionen etc.)**
 - Angegeben im Sprachstandard (oft sehr vermischt mit Syntax)

- Simuliert Zustandsübergänge auf abstrakter Maschine
- nahe an tatsächlichem Programmverhalten
- *Small-Step-Semantik:*
Programm (= initiale Anweisung) + Startzustand wertet je einen Schritt zu Folgeprogramm + Folgezustand aus
Syntax: $\langle c, \sigma \rangle \rightarrow \langle c', \sigma' \rangle$
Anweisung c in Zustand σ wertet zu Anweisung c' und Zustand σ' aus
- *Big-Step-Semantik:*
Programm (= initiale Anweisung) + Startzustand wertet zu Endzustand aus
Syntax: $\langle c, \sigma \rangle \Rightarrow \sigma'$
Anweisung c in Zustand σ liefert Endzustand σ'

Äquivalenz zwischen Big-Step- und Small-Step-Semantik

$$\langle c, \sigma \rangle \Rightarrow \sigma' \iff \langle c, \sigma \rangle \xrightarrow{*} \langle \text{Skip}, \sigma' \rangle$$

arithmetische/boole'sche Ausdrücke: Zwei Werte *Intg* und *Bool*

- Konstanten val
- Variablenzugriffe var
- binäre Operatoren «Eq», «And», «Less», «Add» und «Sub»
für $==$, $\&\&$, $<$, $+$, $-$

Programmanweisungen:

- Skip
- Variablenzuweisung $x ::= e$
- sequentielle Komposition (Hintereinanderausführung) $c_1 ; ; c_2$
- if-then-else IF (b) c_1 ELSE c_2
- while-Schleifen WHILE (b) c'

Zustand:

beschreibt, welche Werte aktuell in den Variablen (Map)

$\llbracket a \rrbracket \sigma$ Auswertung von arithm. oder boole'schem Ausdruck a in Zustand σ
Verwende Map, da Resultat undefiniert sein kann (z.B. bei $5 + \text{true}$)

$$\langle x ::= a, \sigma \rangle \rightarrow \langle \text{Skip}, \sigma(x \mapsto \llbracket a \rrbracket \sigma) \rangle$$

$$\langle \text{Skip}; c, \sigma \rangle \rightarrow \langle c, \sigma \rangle \quad \frac{\langle c, \sigma \rangle \rightarrow \langle c', \sigma' \rangle}{\langle c; c'', \sigma \rangle \rightarrow \langle c'; c'', \sigma' \rangle}$$

$$\frac{\llbracket b \rrbracket \sigma = \text{Some true}}{\langle \text{IF } (b) \ c \ \text{ELSE } c', \sigma \rangle \rightarrow \langle c, \sigma \rangle} \quad \frac{\llbracket b \rrbracket \sigma = \text{Some false}}{\langle \text{IF } (b) \ c \ \text{ELSE } c', \sigma \rangle \rightarrow \langle c', \sigma \rangle}$$

$$\langle \text{WHILE } (b) \ c, \sigma \rangle \rightarrow \langle \text{IF } (b) \ c; \text{WHILE } (b) \ c \ \text{ELSE } \text{Skip}, \sigma \rangle$$

$\llbracket a \rrbracket \sigma$ Auswertung von arithm. oder boole'schem Ausdruck a in Zustand σ
Verwende Map, da Resultat undefiniert sein kann (z.B. bei $5 + \text{true}$)

$$\langle \text{Skip}, \sigma \rangle \Rightarrow \sigma \quad \langle x ::= a, \sigma \rangle \Rightarrow \sigma(x \mapsto \llbracket a \rrbracket \sigma)$$

$$\frac{\llbracket b \rrbracket \sigma = \text{Some true} \quad \langle c, \sigma \rangle \Rightarrow \sigma'}{\langle \text{IF } (b) \ c \ \text{ELSE } c', \sigma \rangle \Rightarrow \sigma'} \quad \frac{\llbracket b \rrbracket \sigma = \text{Some false} \quad \langle c', \sigma \rangle \Rightarrow \sigma'}{\langle \text{IF } (b) \ c \ \text{ELSE } c', \sigma \rangle \Rightarrow \sigma'}$$

$$\frac{\llbracket b \rrbracket \sigma = \text{Some true} \quad \langle c, \sigma \rangle \Rightarrow \sigma' \quad \langle \text{WHILE } (b) \ c, \sigma' \rangle \Rightarrow \sigma''}{\langle \text{WHILE } (b) \ c, \sigma \rangle \Rightarrow \sigma''}$$

$$\frac{\llbracket b \rrbracket \sigma = \text{Some false}}{\langle \text{WHILE } (b) \ c, \sigma \rangle \Rightarrow \sigma} \quad \frac{\langle c, \sigma \rangle \Rightarrow \sigma' \quad \langle c, \sigma' \rangle \Rightarrow \sigma''}{\langle c; ; c', \sigma \rangle \Rightarrow \sigma''}$$

Erweiterung der Auswertungsfunktionen für Ausdrücke und der Big-Step-Semantik um einen Zeitbegriff:

Konstanten: 1

Variablen: 1

je bin. Operation: 1 + Auswertung beider Argumente

Skip: 1

LAss: 1 + Auswertung des arith. Ausdrucks

Seq: 1 + Auswertung beider Anweisungen

If: 1 + Auswertung des bool. Ausdrucks
+ Dauer des gew. Zweigs

While-False: 1 + Auswertung des bool. Ausdrucks

While-True: 1 + Auswertung des bool. Ausdrucks
+ Dauer für Rumpf + Rest-Dauer

Formalisierung in Isabelle

Siehe Rahmen

Teil XXII

Typsystem

“It type checks! Ship it!” – Edwin Brady’s T-shirt

Typsystem ordnet jedem Ausdruck Typ zu

Zwei Typen: *Boolean* und *Integer*

Typumgebung Γ : Map von Variablen nach Typ

Zwei Stufen:

1. Ausdruck e hat Typ T unter Typumgebung Γ
Syntax: $\Gamma \vdash e : T$
2. Anweisung c ist wohltypisiert unter Typumgebung Γ
Syntax: $\Gamma \vdash c$

auch Typsystem definiert als induktives Prädikat

Ausdrücke:

- Konstanten haben Typ des Werts
- Variablen haben den in Typumgebung gespeicherten Typ
- Operatoren haben, wenn Unterausdrücke Typen passend zu Operator, Typ des Resultats
z.B. bei «Less»: Unterausdrücke *Integer*, ganzer Operator *Boolean*

Anweisungen:

- `Skip` typt immer
- $x ::= e$ typt, wenn Typ der Variable x in Typumgebung Γ gleich Typ des Ausdruck e
- Sequenz typt, wenn beide Unteranweisungen typen
- `if` und `while` typen, wenn Unteranweisungen typen und Prädikat vom Typ *Boolean*

Formalisierung in Isabelle

Siehe Rahmen

Teil XXIII

Projekt: Konstantenfaltung und -propagation

“The easy part of laundry is putting it in the washer and dryer. The part I dislike about it is the constant folding. :/” – @Andrewanthony91

- Konstantenfaltung und -propagation sind wichtige Optimierungen in Compilern
- verringern *Registerdruck* (Anzahl der benötigten Register)
- Korrektheit dieser Optimierungen essentiell
- Korrektheit zu zeigen bzgl. formaler Semantik

Optimierung für Ausdrücke

- Wenn Berechnungen nur auf Konstanten, Ergebnis einfach einsetzen:
Val(Intg 5) «Add» Val(Intg 3) wird zu Val(Intg 8)
Val(Intg 4) «Eq» Val(Intg 7) wird zu Val false
- Wenn mind. eine Variable, einfach beibehalten:
Var y «Sub» Val(Intg 3) bleibt Var y «Sub» Val(Intg 3)
- nicht sinnvolle Ausdrücke auch beibehalten:
Val(Intg 5) «And» Val true bleibt Val(Intg 5) «And» Val true
- Wenn Ausdruck nur Konstante oder Variable, auch beibehalten:
Val(Intg 5) bleibt Val(Intg 5), Var y bleibt Var y

Optimierung für Anweisungen

- Idee: Merken von Variablen, die konstant deklariert sind
- ermöglicht Ersetzen der Variable durch konstanten Wert
- dadurch möglich, `if`-Anweisungen zu vereinfachen
- Benötigt *Map* von Variablen nach Werten
- verwendet auch Konstantenfaltung

```
x ::= Val(Intg 7);;  
y ::= Val(Intg 3);;  
IF (Var x «Eq» Var y)  
  (y ::= Var x «Add» Val(Intg 2))  
ELSE (y ::= Var x «Sub» Var z);;  
z ::= Var y
```

wird zu

```
x ::= Val(Intg 7);;  
y ::= Val(Intg 3);;  
y ::= Val(Intg 7) «Sub» Var z;;  
z ::= Var y
```

finale Map: $(x \mapsto \text{Val}(\text{Intg } 7))$

```
x ::= Val(Intg 2);;  
y ::= Var x;;  
b ::= Var x «Eq» Var y;;  
IF (Var b)  
  (z ::= Var x «Add» Var y)  
ELSE (z ::= Var x)
```

wird zu

```
x ::= Val(Intg 2);;  
y ::= Val(Intg 2);;  
b ::= Val true;;  
z ::= Val(Intg 4)
```

finale Map: $(x \mapsto \text{Val}(\text{Intg } 2),$
 $y \mapsto \text{Val}(\text{Intg } 2), b \mapsto \text{Val true},$
 $z \mapsto \text{Val}(\text{Intg } 4))$

Wie IF könnte man auch WHILE vereinfachen:

- falls Prädikat konstant *false*, komplettes WHILE durch Skip ersetzen
- falls Prädikat konstant *true*, Prädikat umschreiben, ansonsten Schleife beibehalten und in Schleifenkörper weiter Konstanten propagieren

Problem: Konstanten im Schleifenkörper beeinflussen auch Prädikat!
Beispiel:

```
x ::= Val(Intg 5);; y ::= Val(Intg 1);;
WHILE (Var x «Less» Val(Intg 7))
  (IF (Var y «Eq» Val(Intg 4))
    (x ::= Val(Intg 9))
  ELSE Skip;;
  y ::= Var y «Add» Val(Intg 1))
```

Darf das Prädikat von WHILE vereinfacht werden?

- Kompletter Algorithmus bräuchte Fixpunktiteration!
- Zu kompliziert, deshalb Vereinfachung:
Ist das Prädikat konstant `false`, ist alles in Ordnung. Ansonsten löschen wir beim `WHILE` die bisher gesammelte Konstanteninformation, verwenden also `empty Map`
- Ergebnis ist immer noch korrekt, aber nicht optimal vereinfacht
- Algorithmus so aber viel einfacher zu formalisieren

1. Beweis, dass die vorgeg. Semantik deterministisch ist (sowohl im Endzustand, als auch im Zeitbegriff)
2. Formalisierung von Konstantenpropagation inklusive -faltung
3. Beweis, dass Konstantenpropagation Semantik erhält
anders gesagt: "Endzustand ist der Gleiche, egal ob man im gleichen Anfangszustand Originalanweisung oder resultierende Anweisung der Konstantenpropagation verwendet"
4. Beweis, dass sich die Ausführungsgeschwindigkeit durch Konstantenpropagation nicht verringert
5. Beweis, dass zwei-/mehrfache Anwendung der Konstantenpropagation das Programm nicht weiter verändert
6. Beweis, dass Konstantenpropagation Typisierung erhält
anders gesagt: "Wenn Originalanweisung typt, dann auch resultierende Anweisung der Konstantenpropagation"

Beweise sollten verständlich und (komplett) in Isar geschrieben werden

- Isabelle-Dokumentation verwenden! Vor allem die Tutorials zu Isabelle/HOL, Isar und Function Definitions sollten helfen
- erst formalisieren, dann beweisen!
Beispiele mittels `value` prüfen (z.B. Beispielprogramme in `Semantics.thy`)
- verwendet `quickcheck`, `nitpick` oder `sledgehammer` um Aussagen vor einem Beweis zu prüfen (spart oft unnötige Arbeit)
- falls Funktionsdefinitionen mit `fun` nicht funktionieren:
 - oftmals Probleme mit Termination
 - Fehlermeldung genau ansehen (wo Probleme mit Termination?)
oft hilft eigene `[simp]` Regel
 - auch möglich: Zu `function` übergehen und versuchen, Termination explizit zu zeigen (siehe Tutorial zu Function Definitions)
- für die Beweise überlegen: welche Beziehungen müssen zwischen Semantikzustand, Typumgebung und Konstantenmap existieren?

- *case*-Ausdrücke statt *if-then-else* verwenden wo möglich
 - ⇒ Entsprechende *split*-Regeln verwenden
 - ⇒ Mehr Automatismus

Beispiel

```
lemma "case v of None ⇒ f 0 | Some x ⇒ f x ⇒ ∃ n. f n"  
  by (cases v) auto by (auto split: option.splits)
```

Teil XXIV

Attribute

Allgemein: Attribute verändern Fakten.

Syntax:

```
theoremname[attribut1, attribut2, attribut mit optionen]
```

Kann überall verwendet werden, wo ein Fakt erwartet wird:

```
...by (rule foo[bar])
```

```
from foo[bar] have...
```

```
declare neuer_name = foo[bar]
```

```
note neuer_name = foo[bar]
```

```
...
```

Manchmal nötig, um Variablen vor Regelanwendung festzulegen (z.B. wenn Isabelle passende Terme nicht inferieren kann), dann:

- Attribut *of*, danach einer oder mehrere Terme
- müssen natürlich zu Typ der Variable passen
- Reihenfolge wie erstes Auftreten in Regel
- `_` für Variablen, die man nicht instantiiieren möchte

Beispiel:

$iffE$:	$\llbracket ?P = ?Q; \llbracket ?P \longrightarrow ?Q; ?Q \longrightarrow ?P \rrbracket \Longrightarrow ?R \rrbracket \Longrightarrow ?R$
$iffE[of X]$:	$\llbracket X = ?Q; \llbracket X \longrightarrow ?Q; ?Q \longrightarrow X \rrbracket \Longrightarrow ?R \rrbracket \Longrightarrow ?R$
$iffE[of _ Y]$:	$\llbracket ?P = Y; \llbracket ?P \longrightarrow Y; Y \longrightarrow ?P \rrbracket \Longrightarrow ?R \rrbracket \Longrightarrow ?R$
$iffE[of X Y Z]$:	$\llbracket X = Y; \llbracket X \longrightarrow Y; Y \longrightarrow X \rrbracket \Longrightarrow Z \rrbracket \Longrightarrow Z$

Syntax:

Regel [*where* $v=T$]

Wobei

- v die zu spezifizierende Variable in der Regel *Regel* ist
- T der einzusetzende Term ist

Beispiel:

iffE: $[[?P = ?Q; [[?P \longrightarrow ?Q; ?Q \longrightarrow ?P]] \implies ?R]] \implies ?R$

iffE[*where* $Q="X \wedge Y"$]: $[[?P = X \wedge Y; [[?P \longrightarrow X \wedge Y; X \wedge Y \longrightarrow ?P]] \implies ?R]] \implies ?R$

Analog zu *of*: ganze Prämissen instantiieren

- Attribut *OF* gefolgt von Regelnamen.
- Konklusion der Regel und entspr. Prämisse müssen unifizieren.
- Entspr. Prämissen werden durch Prämissen der eingefügten Regel ersetzt.
- Mit `_` werden Prämissen übersprungen.
- Gut bei Induktionshypothesen in Isar einsetzbar (*Foo.IH[OF bar]*).

Beispiel:

```
conjI:                [[?P; ?Q]] ==> ?P & ?Q
ccontr:               (¬ ?P ==> False) ==> ?P
conjI[OF ccontr]:    [[¬ ?P ==> False; ?Q]] ==> ?P & ?Q
conjI[OF ccontr, of X]: [[¬ X ==> False; ?Q]] ==> X & ?Q
```


Konklusion umdrehen mit *symmetric*

Wenn die Konklusion einer Regel eine Gleichheit falsch herum hat, hilft *foo[symmetric]*:

Beispiel:

```
drop_all:           length ?xs ≤ ?n ⇒ drop ?n ?xs = []  
drop_all[symmetric]: length ?xs ≤ ?n ⇒ [] = drop ?n ?xs
```

Definitionen falten mit *folded* und *unfolded*

Man kann eine Gleichung (meist eine Definition) in einer Regel substituieren, je nach Richtung mit *foo[folded equality]* oder *foo[unfolded equality]*:

Beispiel:

<i>solution_def:</i>	<i>solution = 42</i>
<i>foo:</i>	<i>?P solution \implies ?Q 42</i>
<i>foo[unfolded solution_def]:</i>	<i>?P 42 \implies ?Q 42</i>
<i>foo[folded solution_def]:</i>	<i>?P solution \implies ?Q solution</i>

Das Attribut `[simplified]` lässt den Simplifier eine Regel vereinfachen. Das sollte man bei bewiesenen Lemmas eigentlich nicht brauchen (die kann man direkt „richtig“ formulieren), aber in Kombination mit `DF` oder `of` ist es oft der beste Weg die Regel wieder in eine Form zu kriegen, mit der z.B. `auto intro`: arbeiten kann.

(Sehr konstruiertes) Beispiel:

```
take_add:  
  take (?i + ?j) ?xs = take ?i ?xs @ take ?j (drop ?i ?xs)  
take_add[of 5 10]:  
  take (5 + 10) ?xs = take 5 ?xs @ take 10 (drop 5 ?xs)  
take_add[of 5 10, simplified]:  
  take 15 ?xs = take 5 ?xs @ take 10 (drop 5 ?xs)
```

Das Attribut kann auch in der Form `[simplified regel1 regel2...]` verwendet werden. Dann verwendet der Simplifier nur die angegebenen Regeln.

Teil XXV

Universelle Fallunterscheidung

Wir kennen bereits Fallunterscheidung

- klassisch (mit `case_split`),
- nach Datentypkonstruktor (Bsp. `list.exhaust`),
- als Regelinversion bei induktiven Prädikaten (Bsp. `palin.cases`),
- nach Pattern-Matching bei **fun**-Definitionen (Bsp. `BigNat.add'.cases`).

Alle diese Regeln folgen dem Muster:

$(Fall11 \implies P) \implies$

$(Fall12 \implies P) \implies$

$(Fall13 \implies P) \implies$

$\dots \implies P$

Im Allgemeinen kann jede Regel dieser Form als Fallunterscheidungsregel verwendet werden. Z.B.:

$(even\ n \implies P) \implies (odd\ n \implies P) \implies P$

Eigene Fallunterscheidungsregeln anwenden

```
lemma even_odd_cases [case_names even odd]:  
  obtains (even) "even n" | (odd) "odd n" assumes "even n  $\implies$  P"  
    and "odd n  $\implies$  P"  
  shows "P"
```

Freie Variablen der Regel müssen instanziiert werden:

```
have "P (n::nat)"  
proof (cases n rule: even_odd_cases)  
  case even  
  ...  
qed
```

Fallunterscheidung ist auch lokal in einem Isar-Beweis mit dem Kommando **consider** möglich:

```
consider (even) "even n" | (odd) "odd n" by blast
then show ?thesis
proof cases
  case even
  ...
next
  case odd
  ...
qed
```

Dabei auch „obtainen“ von Variablen möglich:

```
consider (zero) "n = 0" | (succ) x where "n = Suc x"
then have "even n"
proof cases
  case (succ x) ...
```

Teil XXVI

Strukturierte Zwischenziele

Ähnlich wie **assumes** und **shows** kann man auch für Zwischenziele (**have**) eines Isar-Beweises die Aussage strukturieren:

```
have "P x"  
  if meine_annahme_1: "Q x"  
  and meine_annahme_2: "R x"  
for x :: nat
```

- Annahmen nach **if** *nicht* im Beweiszustand.
Dafür gibt es die Variable *that*, welche alle **if**-Annahmen enthält.
- Benannte Annahmen
- (Meta-)Allquantifizierte Variablen

if und **for** auch mit **assume** möglich – nicht aber mit **assumes**. Also nur innerhalb eines Beweises.

Teil XXVII

Locales

⇒ Verwende **Locales**

locale: Definiert neuen Beweiskontext

fixes: Legt Funktionssymbol fest (wird zu Parameter der Locale)

assumes: Macht Annahmen über die Locale-Parameter

context <locale> begin ... end: Öffnet Beweiskontext

Beispiel:

```
locale Magma =  
  fixes M :: "'a set"  
  fixes bop :: "'a ⇒ 'a ⇒ 'a"  
  assumes closed: "a ∈ M ⇒ b ∈ M ⇒ bop a b ∈ M"  
  
context Magma begin <Definitionen, Beweise, ...> end
```

Locales lassen sich mit “+” erweitern:

Beispiel:

```
locale Semigroup = Magma +  
  assumes assoc: "..."
```

Auch “Verschmelzen” von Locales möglich:

Beispiel:

```
locale Ring = AbelianGroup "M" "add" "zero" + Magma "M" "mul"  
  for M :: "'a set"  
  and add :: "'a ⇒ 'a ⇒ 'a"  
  and zero :: "'a"  
  and mul :: "'a ⇒ 'a ⇒ 'a"  
+ assumes assoc: "..."
```

Instanziierung der Locales mit

interpretation: im Theoriekontext

interpret: in Beweiskontexten

Vorgehen:

- Angabe der konkreten Parameter
- Locale-Definition “auspacken” mit Taktik **unfold_locales**
- Beweis der Locale-Annahmen

Beispiel:

interpretation *Mod3*:

```
Ring "{0::nat,1,2}" "λa b. a + b mod 3" "0" "λa b. a * b mod 3"  
by (unfold_locales) auto
```

Spezielle Locales mit genau einem Typparameter

Beispiel:

```
class Magma =  
  fixes M :: "'a set"  
  fixes bop :: "'a  $\Rightarrow$  'a  $\Rightarrow$  'a"  
  assumes closed: " $a \in M \implies b \in M \implies bop\ a\ b \in M$ "  
  
context Magma begin <Definitionen, Beweise, ...> end
```

Instanziierung mittels **instantiation**

Vorteil: Alle Deklarationen innerhalb der Typklasse sind auch auf dem Top-Level verfügbar, die notwendige Instanz wird bei Anwendung durch *Typklasseninferenz* ermittelt.

Mehr dazu: Tutorial **classes** in der Isabelle-Dokumentation

Teil XXVIII

Typedef

Eigene Typen in HOL definieren

In Isabelle/HOL können eigene Typen definiert werden. Dazu benötigt man

- eine Teilmenge eines existierenden Typs sowie
- ein Beweis, dass diese Teilmenge nicht leer ist.

(Leere Typen würden HOL inkonsistent machen, d.h. man könnte *False* beweisen.)

Syntax

```
typedef typename = "Menge" morphisms rep_fun abs_fun by proof
```

- *typename* ist der Name des neuen Typs. Hier dürfen auch Typvariablen verwendet werden ($(\text{'a}, \text{'b}) \textit{typename}$).
- *Menge* ist ein Ausdruck vom Typ *irgendwas set*.
- Morphismen konvertieren zwischen der Menge und dem neuen Typ:
 $\textit{rep_fun} :: \textit{typename} \Rightarrow \textit{irgendwas}$ und $\textit{abs_fun} :: \textit{irgendwas} \Rightarrow \textit{typename}$
- Default-Morphismennamen: *Rep_typname* und *Abs_typname*.
- Das Beweisziel ist $\exists x. x \in \textit{Menge}$.
- Erzeugt (u. a. und v. a.) diese Lemmas:
 $\textit{rep_fun}: \quad \textit{rep_fun} \textit{?x} \in \textit{Menge}$
 $\textit{rep_fun_inverse}: \quad \textit{abs_fun} (\textit{rep_fun} \textit{?x}) = \textit{?x}$
 $\textit{rep_abs_inverse}: \quad \textit{?y} \in \textit{Menge} \implies \textit{rep_fun} (\textit{abs_fun} \textit{?y}) = \textit{?y}$

Beispiel: Nicht-Leere Liste

Wir erstellen einen Typ für **nicht-leere Listen** und beginnen mit der Typ-Definition:

```
typedef 'a ne = "{xs :: 'a list . xs ≠ []}"  
  by (rule exI[where x = "[undefined]"], simp)
```

Weiter ein paar Funktionen auf nicht-leeren Listen:

```
definition singleton :: "'a ⇒ 'a ne"  
  where "singleton x = Abs_ne [x]"
```

```
definition append :: "'a ne ⇒ 'a ne ⇒ 'a ne"  
  where "append l1 l2 = Abs_ne (Rep_ne l1 @ Rep_ne l2)"
```

```
definition head :: "'a ne ⇒ 'a"  
  where "head l = hd (Rep_ne l)"
```

```
definition tail :: "'a ne ⇒ 'a ne"  
  where "tail l = Abs_ne (tl (Rep_ne l))"
```

Beispiel: Lemmas zu Nicht-Leeren Liste

Bei Append kommt der Head der Liste immer von der linken Liste (für allgemeine Listen nicht wahr!):

```
lemma "head (append l1 l2) = head l1"  
  unfolding head_def append_def  
  apply (subst Abs_ne_inverse)  
  using Rep_ne[of l1] apply simp  
  using Rep_ne[of l1] apply simp  
  done
```

Beispiel: Mehr Lemmas zu Nicht-Leeren Liste

Head und Tail ergeben wieder die gesamte Liste:

```
lemma "append (singleton (head l)) (tail l) = l"  
  unfolding head_def append_def singleton_def tail_def  
  apply (subst Abs_ne_inverse)  
  apply simp  
  apply (subst Abs_ne_inverse)  
  defer  
  using Rep_ne[of l]  
  apply simp  
  apply (rule Rep_ne_inverse)  
  apply simp  
oops
```

Problem: Das Lemma ist „eigentlich“ richtig, aber `tail [a]` ist undefiniert, da keine nicht-leere Liste.

Beispiel: Richtige Lemmas zu Nicht-Leeren Liste

Tail muss eine „normale“ Liste zurückgeben:

```
definition tail' :: "'a ne  $\Rightarrow$  'a list"
  where "tail' l = tl (Rep_ne l)"
```

```
definition append' :: "'a ne  $\Rightarrow$  'a list  $\Rightarrow$  'a ne"
  where "append' l1 l2 = Abs_ne (Rep_ne l1 @ l2)"
```

```
lemma "append' (singleton (head l)) (tail' l) = l"
  unfolding head_def append'_def singleton_def tail'_def
  apply (subst Abs_ne_inverse, simp)
  using Rep_ne[of l, simplified]
  apply simp
  apply (rule Rep_ne_inverse)
  done
```

Teil XXIX

Lifting und Transfer

Rückblick: Eigene Typen in HOL definieren

```
typedef 'a ne = "{xs :: 'a list . xs ≠ []}"  
  by (rule exI[where x = "[undefined]"], simp)
```

```
definition singleton :: "'a ⇒ 'a ne"  
  where "singleton x = Abs_ne [x]"
```

```
definition append :: "'a ne ⇒ 'a ne ⇒ 'a ne"  
  where "append l1 l2 = Abs_ne (Rep_ne l1 @ Rep_ne l2)"
```

```
definition head :: "'a ne ⇒ 'a"  
  where "head l = hd (Rep_ne l)"
```

```
lemma "head (append l1 l2) = head l1"  
  unfolding head_def append_def  
  apply (subst Abs_ne_inverse)  
  using Rep_ne[of l1] apply simp  
  using Rep_ne[of l1] apply simp  
  done
```

Das Beweisen mit den Abstraktions- und Repräsentationsfunktionen ist mühsam und unnatürlich: So wird die Erhaltung einer Invariante beim Verwenden der Funktion bewiesen, und nicht beim Definieren (siehe *tail*).

Die Isabelle-Pakete *Lifting* und *Transfer* erlauben es, Funktionen einmal bei der Definition als „korrekt“ zu beweisen und Lemmas mit einem Methodenaufruf in die Welt der zugrundeliegenden Repräsentation zu übertragen und dann dort zu beweisen.

1. Typ registrieren:

setup_lifting *type_definition_tynname*

2. Definitionen liften:

lift_definition *name* :: *type* **is** "*ausdruck*"

Beweis

wobei *ausdruck* die Definition von *name* auf den konkreten Datentyp ist und der *Beweis* beweist dass die Typ-Invarianten respektiert werden.

3. Aussagen auf die konkreten Typen übertragen: **apply transfer**
Ersetzt das aktuelle Ziel durch ein gleichwertiges auf dem konkreten Datentyp, indem die per **lift_definition** definierten Funktionen durch ihre konkrete Definition ersetzt werden.

Beispiel: Sortierte Listen

Typ registrieren:

```
typedef slist = "{xs. sorted xs}" morphisms list_of as_sorted  
  by (rule exI[where x = "[]"]) simp
```

```
setup_lifting type_definition_slist
```

Definitionen:

```
lift_definition Singleton :: "nat  $\Rightarrow$  slist" is " $\lambda x. [x]$ " by simp
```

```
lift_definition set_of :: "slist  $\Rightarrow$  nat set" is "List.set" .
```

```
lift_definition hd :: "slist  $\Rightarrow$  nat" is "List.hd" ..
```

```
lift_definition take :: "nat  $\Rightarrow$  slist  $\Rightarrow$  slist" is "List.take" ..
```

```
lift_definition smerge :: "slist  $\Rightarrow$  slist  $\Rightarrow$  slist" is "Scratch.merge" by  
(rule sorted_merge_sorted)
```

Beispiel: Sortierte Listen

Lemmas zu Definitionen auf dem abstrakten Typ:

lemma *set_of_Singleton [simp]*: "set_of (Singleton x) = {x}"

Aktuelles Ziel: $\text{set_of (Singleton } x) = \{x\}$

apply *transfer*

Aktuelles Ziel: $\bigwedge x. \text{set } [x] = \{x\}$

apply *simp*

Aktuelles Ziel: *No subgoals!*

done

oder gleich

by *transfer simp*

Beispiel: Sortierte Listen

Lemmas können Invarianten nutzen:

lemma "*list_of xs = a#b#ys $\implies a \leq b$* "

Aktuelles Ziel: *list_of xs = a # b # ys $\implies a \leq b$*

apply *transfer*

Aktuelles Ziel: $\bigwedge xs\ a\ b\ ys. \llbracket \text{sorted } xs; xs = a \# b \# ys \rrbracket \implies a \leq b$

apply *simp*

Aktuelles Ziel: *No subgoals!*

done

Beispiel: Sortierte Listen

Lemmas mit rein abstrakten Definitionen:

definition *insert* :: "nat \Rightarrow slist \Rightarrow slist"
 where "insert x xs = smerge xs (Singleton x)"

lemma *set_of_insert* [simp]: "x \in set_of (insert x xs)"

Erster Versuch:

apply *transfer*

Hier bringt *transfer* einen nicht weiter!

Zweiter Versuch:

unfolding *insert_def* **by** *transfer simp*

Schöner ist:

lemma *set_of_smerge*: "set_of (smerge xs ys) = set_of xs \cup set_of ys"
by *transfer simp*

und dann

unfolding *insert_def* **by** (*simp add: set_of_smerge*)

Teil XXX

Erzeugung von ausführbarem Code

Isabelle kann Formalisierungen nach **SML**, **OCaml**, **Haskell** bzw. **Scala** exportieren.

⇒ Dadurch sind verifizierte *ausführbare* Programme möglich.

- Jede HOL-Funktion wird in eine entsprechende Funktion der Zielsprache übersetzt.
- Jeder HOL-Typ wird ein entsprechenden Typ der Zielsprache übersetzt.
- **Basis:** Code-Gleichungen

Code-Erzeugung mit Befehl:

```
export_code f in Sprache module_name Modul file Datei
```

Die definierenden HOL-Gleichungen von *f* werden 1:1 in die Zielsprache übersetzt.

Nicht alle HOL-Funktionen können direkt übersetzt werden.

Beispiel

Wie kann die Funktion

```
doubled xs =  
  (if ( $\exists$  ys. xs = ys @ ys) then Some (THE ys. xs = ys @ ys) else None)
```

übersetzt werden?

Problem: Existenzquantor nur für enum-Typen ausführbar.

Lösung: Beweise alternative Code-Gleichung:

```
lemma doubled_code [code]: "doubled xs =  
  (let ys = take (length xs div 2) xs in  
  (if (xs = ys @ ys) then Some ys else None)"
```


Eine Gleichung kann als Code-Gleichung für f verwendet werden, wenn

- f das oberste (und einzige) Funktionssymbol im linken Term ist,
- Patternmatching auf die Parameter von f nur via Datentyp-Konstruktoren erfolgt, und
- für alle Funktionssymbole auf der rechten Seite Code-Gleichungen existieren.

Insbesondere ist es nicht (direkt) möglich „partielle“ Code-Gleichungen anzugeben.

Späteres hinzufügen einer Gleichung als Code-Gleichung mit

declare *lemma* [*code*]

möglich.

Beispiel

Siehe Formalisierung

- Das Kommando

value *[code]* "*t*"

übersetzt den Term t und wertet ihn aus.

- **eval** ist eine Beweis-Taktik, welche versucht, das aktuelle Ziel durch „ausrechnen“ (Brute-Force) zu zeigen.
- **code_thms** f zeigt alle registrierten Code-Gleichungen an, die zur Auswertung von f benötigt werden.
- **print_codesetup** zeigt *alle* registrierten Code-Gleichungen an.

Lifting arbeitet gut mit dem Code-Generator zusammen: Es registriert `as_sorted` als Konstruktor für den Typ `slist` und definierte alle Operationen darauf. Man kann keine Code-Gleichung angeben die mittels `as_sorted x` ein Wert vom Typ `slist` konstruiert, ohne bewiesen zu haben, dass `sorted x` gilt.

```
export_code insert take list_of set_of  
in Haskell
```

Manuell: Auch möglich, dann mit **code_datatype**, `[code abstype]` und `[code abstract]` arbeiten.

⇒ siehe isabelle doc codegen.

Vor Anwendung der Code-Gleichungen werden diese vom Code-Präprozessor bearbeitet.

- Rewrite-System mit ähnlicher Mächtigkeit wie Simplifier
- Attribute **code_abbrev** bzw. **code_unfold** verwenden, um Gleichungen zu registrieren
- **print_codeproc** zeigt das Präprozessor-Setup an

Teil XXXI

Koinduktion

Duales Prinzip zu Induktion

Induktive Definition:

kleinster Fixpunkt, der die definierende Gleichung erfüllt.

Induktionsprinzip: Um eine Eigenschaft für alle Elemente zu zeigen, genügt es sie für eine beliebige Menge zu zeigen, die die definierende Gleichung erfüllt. (Der kleinste Fixpunkt muss darin enthalten sein)

Koinduktive Definition:

größter Fixpunkt, der die definierende Gleichung erfüllt.

Koinduktionsprinzip: Jede Menge, die die definierende Gleichung erfüllt, ist in der koinduktiven Definition enthalten.

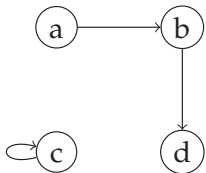
Beispiel: Reflexiv transitive Hülle

coinductive $rtc :: "('a \Rightarrow 'a \Rightarrow bool) \Rightarrow 'a \Rightarrow 'a \Rightarrow bool"$

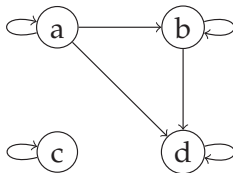
for $r :: "('a \Rightarrow 'a \Rightarrow bool)"$

where $refl: "rtc\ r\ x\ x"$

| $trans: "r\ x\ y \Longrightarrow rtc\ r\ y\ z \Longrightarrow rtc\ r\ x\ z"$



(a) Graph r



(b) Inductive RTC r

aus © Andreas Lochbihler, DOI 10.5445/KSP/1000028867, KIT Scientific Publishing, Karlsruhe, 2012



Induktionsschema für rtc : $rtc.induct$

$$\begin{aligned}rtc\ r\ a\ b &\implies (\bigwedge x. P\ x\ x) \\ &\implies (\bigwedge x\ y\ z. r\ x\ y \implies rtc\ r\ y\ z \implies P\ y\ z \implies P\ x\ z) \\ &\implies P\ a\ b\end{aligned}$$

Koinduktionsschema für rtc : $rtc.coinduct$

$$\begin{aligned}X\ a\ b &\implies \\ &(\bigwedge a\ b. X\ a\ b \implies \\ &\quad (\exists x. a = x \wedge b = x) \vee \\ &\quad (\exists x\ y\ z. a = x \wedge b = z \wedge r\ x\ y \wedge (X\ y\ z \vee rtc\ r\ y\ z))) \implies \\ &rtc\ r\ a\ b\end{aligned}$$

Beweismethoden: *coinduct/coinduction* – analog zu *induct/induction*

Beispiel: Lazy Listen

```
codatatype 'a llist = lnull: LNil | LCons (lhd: 'a) (ltl: "'a llist")
```

Auch hier *duale Sichtweise*: Elemente werden erzeugt, statt abgebaut.

Beispiel: Iterate

```
primcorec literate :: "('a ⇒ 'a) ⇒ 'a ⇒ 'a llist"  
where "literate f s = LCons s (literate f (f s))"
```

Mehr: siehe Sitzung.

Teil XXXII

Dokumentenerzeugung

Isabelle kann Theorien mit \LaTeX schön setzen.

Dazu muss man eine *Sitzung* definieren. Am einfachsten geht das mit
`isabelle mkroot -d name`.

Die Datei `ROOT` führt alle verwendeten Theorien auf.
Die Datei `document/root.tex` enthält den \LaTeX -Rahmen.

Man lässt Isabelle mit
`isabelle build -D .`
die Theorien verarbeiten und die PDF-Dateien erzeugen.

Normaler Text (einschließlich \LaTeX -Makros) kann mittels **text** `\text{<bla bla>}` eingefügt werden.

Kommentare (`\comment{<bla bla>}`) erscheinen *nicht* im Dokument!

Statt \LaTeX -Befehle wie `\section`, `\subsection` etc. in **text**-Blöcke einzubauen kann man die entsprechenden Isabelle-Befehle

- **chapter** (bei geeigneter `\documentclass`)
- **section**
- **subsection**
- **subsubsection**

verwenden.

Ähnlich wie in Markdown können Listen auch ohne \LaTeX -Befehl angegeben werden. Dazu werden spezielle Bullet-Points verwendet. Diese kann man in jEdit mittels `\item` für ungeordnete und `\enum` für geordnete Listen eingeben.

Man kann Ausdrücke verschiedener Art von Isabelle in das Dokument einfügen lassen:

Nach

definition $N :: nat$ **where** $"N = 0"$

theorem $great_result: "N = N * P"$ **unfolding** N_def **by** $simp$
wird aus

text \langle

*After defining $\@{\thm N_def}$ we were finally able
to prove $\@{\thm great_result}$.*

\rangle

in der Dokumentausgabe

After defining $N = 0$ we were finally able to prove $N = N * ?P$.

Neben `@{thm ...}` sind noch nützlich:

- `@{theory ...}` verweist auf einen (importierten) Theorie-Namen,
- `@{term ...}` setzt einen Term,
- `@{term_type ...}` ebenso, aber mit Typ,
- `@{typ ...}` setzt einen Typ,
- `@{value ...}` evaluiert einen Term und zeigt das Ergebnis,
- `@{text ...}` setzt beliebigen Text im Isabelle-Stil.

Während `@{thm ...}` garantiert, dass nur bewiesenes gedruckt wird, überprüfen die anderen nur die Typisierung, und mit `@{text ...}` lässt sich alles ausgeben.

Beim Ausgeben von Lemmas ist oft `@{thm great_result[no_vars]}` schöner als `@{thm great_result}`.

Standardmäßig enthält `document/root.tex` den Befehl `\input{session}` und `session.tex` (von Isabelle erstellt) enthält für jede Theorie `foo` eine Zeile `\input{Example.tex}`.

Man kann natürlich auch die Theorie-Dateien direkt in `document/root.tex` einbinden, etwa um dazwischen noch Text wie Kapitelüberschriften oder Einleitungen zu setzen.

Auch will man vielleicht in der Einleitung schon auf alle Definitionen und Ergebnisse vorgreifen. Dazu erstellt man z.B. eine Theorie `Introduction` und bindet diese in `document/root.tex` am Anfang ein.

Für Theorien, die in `ROOT` mit der Option `document = false` versehen sind, werden nicht in das Dokument aufgenommen (die trotzdem erzeugte `.tex`-Datei ist leer).

Mehr Informationen

zu mehr Anti-Quotations siehe das Isabelle Referenz-Handbuch
(`isabelle doc isar-ref`).

Für mehr \LaTeX -Spielereien wie z.B. die Ausgabe

$$\frac{P \ 0 \quad \bigwedge_{\text{nat.}} \frac{P \ \text{nat}}{P \ (\text{Suc} \ \text{nat})}}{P \ \text{nat}}$$

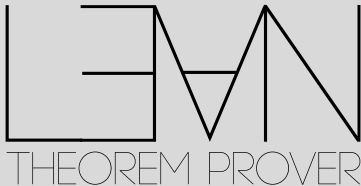
für

```
text  $\langle \backslash \text{begin}\{center\}$   
   $\@{\thm}\{mode=Rule\} \ \text{nat.}\ \text{induct}\ [no\_vars]\}$   
 $\backslash \text{end}\{center\} \rangle$ 
```

siehe `isabelle doc sugar`.

Teil XXXIII

Lean: Mit starken Typen abhängen



Demo: Aussagenlogik

Terme	\leftrightarrow	Beweise
Typen	\leftrightarrow	Aussagen
Polymorphe Typen	\leftrightarrow	Aussagenlogik zweiter Ordnung
???	\leftrightarrow	Prädikatenlogik
$\prod x : A. B$		$\forall x : A. B$

\Rightarrow Eine Sprache, ein Typsystem sowohl für Definitionen als auch Beweise

- Einfach getypter Lambda-Kalkül

$$\frac{\Gamma, x : \tau_1 \vdash t : \tau_2}{\Gamma \vdash \lambda x : \tau_1. t : \tau_1 \rightarrow \tau_2}$$
$$\frac{\Gamma \vdash e_1 : \tau_1 \rightarrow \tau_2 \quad \Gamma \vdash e_2 : \tau_1}{\Gamma \vdash e_1 e_2 : \tau_2}$$

- Calculus of Constructions [Coquand, Huet 1986]

$$\frac{\Gamma, x : \tau_1 \vdash t : \tau_2}{\Gamma \vdash \lambda x : \tau_1. t : \Pi x : \tau_1. \tau_2}$$
$$\frac{\Gamma \vdash e_1 : \Pi x : \tau_1. \tau_2 \quad \Gamma \vdash e_2 : \tau_1}{\Gamma \vdash e_1 e_2 : \tau_2[e_2/x]}$$

$$\tau_1 \rightarrow \tau_2 \equiv \Pi _ : \tau_1. \tau_2$$

Demo: Prädikatenlogik

Syntaktischer Vergleich

Isabelle/HOL	Lean
\Rightarrow \Longrightarrow \longrightarrow \wedge \forall	Π
<code>f x</code> <code>g [of x]</code> <code>h [OF g]</code>	<code>f x</code> <code>g x</code> <code>h g</code>
<code>record, locale, class</code> <code>datatype, predicate</code>	<code>structure</code> <code>inductive</code>

Typen gut, alles gut?

Ein stärkeres Typsystem erschwert leider auch die Implementierung von Automation. Lean hat bisher

- ein grundsätzliches `simp`, “conditional term rewriter”
- SMT-Primitive wie E-Matching und Congruence Closure
- kein `auto`, ...
- keinen Sledgehammer

Typen gut, alles gut?

Isabelle	Lean
erstes Release 1986	erstes Release 2015
680.000 LOC (HOL) + 2.100.000 LOC (AFP)	28.000 LOC + 68.000 LOC (mathlib)

- Benutze Lean als seine eigene Metaprogrammiersprache
 - Definiere Taktiken, Syntaxerweiterungen, Debugger, ... in Lean
 - Strikte Trennung zu konsistentem Sprachteil
- Führe Metaprogramme in (relativ effizienter) VM aus
- Baue auf effizienten in C++ definierten Primitiven auf
- *A Metaprogramming Framework for Formal Verification*
Ebner, Ullrich, Roesch, Avigad, de Moura; ICFP 2017

- Teilweiser Rewrite begonnen 2018
- Interne Vereinfachungen und Refactorings
- Neuer Parser implementiert in Lean
 - Erlaubt erweitertes Backtracking
 - Baut einen verlustfreien konkreten Syntaxbaum auf
 - ⇒ Basis für Refactorings, Editorunterstützung, Dokumentenerzeugung, ...
 - Lisp/Racket-artiges Makrosystem für hygienische Abkürzungen
- Neues Backend implementiert in Lean
 - Anbindung an LLVM für JIT- und native Kompilierung
 - ⇒ Lean als allgemeine Programmiersprache

`https://leanprover.github.io`

Theorem Proving in Lean – mit Online-Editor

`https://leanprover.github.io/theorem_proving_in_lean/`

Teil XXXIV

Projektvorstellungsvorbereitung

- Ergebnisse werden im Oberseminar des Lehrstuhls vorgestellt
- Termin: 17. Juli 2018, **10 Uhr**
- Ort: Seminarraum 010
- 15 Minuten pro Gruppe
- Folien als PDF vorher per Mail an `ullrich@kit.edu`
oder `denis.lohner@kit.edu`
oder auf USB-Stick mitbringen.

- 1. Gruppe: H., P.
 - Syntax und Semantik vorstellen
 - Determinismusbeweis (nur sehr kurz)
 - Definition der Konstantenpropagation und -Faltung
 - Semantikerhaltung und Beschleunigungsaussage
 - Idempotenzbeweis
 - Erfahrungen, Feedback, Statistiken (lines of code, Anzahl der Lemmas)

- 2. Gruppe: J., R.
 - Definition der Konstantenpropagation und -Faltung
 - Semantikerhaltung und Beschleunigungsaussage
 - Typsystem vorstellen
 - Typisierbarkeitserhaltung
 - Erfahrungen, Feedback, Statistiken (lines of code, Anzahl der Lemmas)

- Beweisideen deutlich machen
- Beweismethode nennen (Induktion etc.)
- Bei Induktion Verallgemeinerung und Invarianten zeigen und begründen
- Nicht jeden Fall eines Beweises einzeln durchnudeln

Siehe auch Termin zur Dokumentenerzeugung! Generierten LaTeX-Code aus `output/document/Theorie.tex` kopieren ist ok und üblich.

Teil XXXV

Dokumentenerzeugung

Isabelle kann Theorien mit \LaTeX schön setzen.

Dazu muss man eine *Sitzung* definieren. Am einfachsten geht das mit
`isabelle mkroot -d name`.

Die Datei `ROOT` führt alle verwendeten Theorien auf.
Die Datei `document/root.tex` enthält den \LaTeX -Rahmen.

Man lässt Isabelle mit
`isabelle build -D .`
die Theorien verarbeiten und die PDF-Dateien erzeugen.

Normaler Text (einschließlich \LaTeX -Makros) kann mittels **text** `\text{bla bla}` eingefügt werden.

Kommentare (`\comment{bla bla}`) erscheinen *nicht* im Dokument!

Statt \LaTeX -Befehle wie `\section`, `\subsection` etc. in **text**-Blöcke einzubauen kann man die entsprechenden Isabelle-Befehle

- **chapter** (bei geeigneter `\documentclass`)
- **section**
- **subsection**
- **subsubsection**

verwenden.

Ähnlich wie in Markdown können Listen auch ohne \LaTeX -Befehl angegeben werden. Dazu werden spezielle Bullet-Points verwendet. Diese kann man in jEdit mittels `\item` für ungeordnete und `\enum` für geordnete Listen eingeben.

Man kann Ausdrücke verschiedener Art von Isabelle in das Dokument einfügen lassen:

Nach

definition $N :: nat$ **where** "N = 0"

theorem *great_result*: "N = N * P" **unfolding** *N_def* **by** *simp*
wird aus

text <

*After defining @{\thm N_def} we were finally able
to prove @{\thm great_result}.*

>

in der Dokumentausgabe

After defining $N = 0$ we were finally able to prove $N = N * ?P$.

Neben `@{thm ...}` sind noch nützlich:

- `@{theory ...}` verweist auf einen (importierten) Theorie-Namen,
- `@{term ...}` setzt einen Term,
- `@{term_type ...}` ebenso, aber mit Typ,
- `@{typ ...}` setzt einen Typ,
- `@{value ...}` evaluiert einen Term und zeigt das Ergebnis,
- `@{text ...}` setzt beliebigen Text im Isabelle-Stil.

Während `@{thm ...}` garantiert, dass nur bewiesenes gedruckt wird, überprüfen die anderen nur die Typisierung, und mit `@{text ...}` lässt sich alles ausgeben.

Beim Ausgeben von Lemmas ist oft `@{thm great_result[no_vars]}` schöner als `@{thm great_result}`.

Standardmäßig enthält `document/root.tex` den Befehl `\input{session}` und `session.tex` (von Isabelle erstellt) enthält für jede Theorie `foo` eine Zeile `\input{Example.tex}`.

Man kann natürlich auch die Theorie-Dateien direkt in `document/root.tex` einbinden, etwa um dazwischen noch Text wie Kapitelüberschriften oder Einleitungen zu setzen.

Auch will man vielleicht in der Einleitung schon auf alle Definitionen und Ergebnisse vorgreifen. Dazu erstellt man z.B. eine Theorie `Introduction` und bindet diese in `document/root.tex` am Anfang ein.

Für Theorien, die in `ROOT` mit der Option `document = false` versehen sind, werden nicht in das Dokument aufgenommen (die trotzdem erzeugte `.tex`-Datei ist leer).

zu mehr Anti-Quotations siehe das Isabelle Referenz-Handbuch (isabelle doc isar-ref).

Für mehr \LaTeX -Spielereien wie z.B. die Ausgabe

$$\frac{P \ 0 \quad \bigwedge_{\text{nat.}} \frac{P \ \text{nat}}{P \ (\text{Suc} \ \text{nat})}}{P \ \text{nat}}$$

für

```
text  $\langle \backslash \text{begin}\{center\}$   
   $\@{\thm}\{mode=Rule\} \ \text{nat.}\ \text{induct}\ [no\_vars]\}$   
 $\backslash \text{end}\{center\} \rangle$ 
```

siehe isabelle doc sugar.