Projektbericht
Beweise in der Gleichungslogik (2011.229)

Harald Zankl

12. Dezember 2011

1 Motivation

Gegeben seien die drei Gleichungen:

$$(G1)\colon (x \circ y) \circ z \approx x \circ (y \circ z) \qquad (G2)\colon x \circ \mathsf{e} \approx x \qquad (G3)\colon x \circ x^{-1} \approx \mathsf{e}$$

Die Terme $(x \circ y) \circ \mathsf{e}$ und $x \circ y$ sind äquivalent, da der erste Term mithilfe der Gleichungen (G1-G3) in den anderen überführt werden kann, z.B.

$$(x \circ y) \circ \mathsf{e} \stackrel{(G1)}{\approx} x \circ (y \circ \mathsf{e}) \stackrel{(G2)}{\approx} x \circ y$$

Um die Terme $x \circ x^{-1}$ und $x^{-1} \circ x$ äquivalent zu zeigen, ist mehr Aufwand notwendig wie die nachstehende Kette von Gleichheiten zeigt.

$$\begin{aligned}
x \circ x^{-1} \stackrel{(G3)}{\approx} \mathsf{e} \stackrel{(G3)}{\approx} (x^{-1} \circ \mathsf{e}) \circ (x^{-1} \circ \mathsf{e})^{-1} \stackrel{(G1)}{\approx} x^{-1} \circ (\mathsf{e} \circ (x^{-1} \circ \mathsf{e})^{-1}) \stackrel{(G2)}{\approx}& \\
\stackrel{(G2)}{\approx} x^{-1} \circ (\mathsf{e} \circ x^{-1-1}) \stackrel{(G3)}{\approx} x^{-1} \circ ((x \circ x^{-1}) \circ x^{-1-1}) \stackrel{(G1)}{\approx}& \\
\stackrel{(G1)}{\approx} x^{-1} \circ (x \circ (x^{-1} \circ x^{-1-1})) \stackrel{(G3)}{\approx} x^{-1} \circ (x \circ \mathsf{e}) \stackrel{(G2)}{\approx}& \\
\stackrel{(G2)}{\approx} x^{-1} \circ x&
\end{aligned}$$

Solche Äquivalenzen per Hand zu zeigen ist aus zwei Gründen schwierig. Einerseits ist unklar, ob die zwei untersuchten Terme überhaupt äquivalent sind, dh., ob solch eine Kette von Gleichheiten zwischen den Termen existiert. Falls dem so ist, kann diese Kette aber sehr lang sein und in jedem Schritt besteht eine Wahlmöglichkeit welche Regel angewendet werden soll.

Solchen Beweisen begegnen Studierende der Informatik in unterschiedlichen Vorlesungen/Proseminaren/Klausuren. Auch müssen sie (für einfache Gleichungen, wie hier etwa G1-G3) solche Beweise führen. Dabei werden aber oft die Gleichungen falsch angewendet, eine händische Korrektur (etwa durch Proseminarleiter) ist sehr zeitaufwändig. Das im Zuge dieses Projektes erstellte Programm kann solche Beweisketten automatisch erzeugen, wodurch sich Studierende mit dem korrekten Anwenden der Gleichungen besser vertraut machen können.

2 Knuth-Bendix Vervollständigung

Die Knuth-Bendix Vervollständigung ist ein zentrales Verfahren in der Informatik. Für eine Menge von Gleichungen als Eingabe liefert das Verfahren (sofern erfolgreich) eine Menge von orientierten Gleichungen als Resultat. Somit können Berechnungen durch "Ersetzung gemäß orientierten Gleichungen" erfolgen. Im Zuge eines Vorprojektes (E-Learning Projekt 2010.189) wurde eine Software erstellt, welche dieses Verfahren sowohl halbautomatisch als auch vollautomatisch löst.

Die Knuth-Bendix Vervollständigung liefert für die Gleichungen (G1-G3) z.B. folgende Regeln (R1-R10) (orientierte Gleichungen):

$$\begin{array}{llll}
(R1): & (x \circ y) \circ z \to x \circ (y \circ z) & (R2): & x \circ \mathsf{e} \to x \\
(R3): & x \circ x^{-1} \to \mathsf{e} & (R4): & x \circ (x^{-1} \circ z) \to z \\
(R5): & x^{-1-1} \to x & (R6): & x^{-1} \circ x \to \mathsf{e} \\
(R7): & \mathsf{e} \circ x \to x & (R8): & \mathsf{e}^{-1} \to \mathsf{e} \\
(R9): & x^{-1} \circ (x \circ y) \to y & (R10): & (y \circ x)^{-1} \to x^{-1} \circ y^{-1}
\end{array}$$

Die Äquivalenz der Terme $x \circ x^{-1}$ und $x^{-1} \circ x$ ist jetzt einfacher zu zeigen, da die Regeln nur mehr in eine Richtung angewendet werden können, z.B.,

$$x \circ x^{-1} \overset{(R3)}{\to} \mathsf{e} \overset{(R6)}{\leftarrow} x^{-1} \circ x$$

Zudem können Terme jetzt auch als nicht äquivalent gezeigt werden, indem beide Terme so weit als möglich mit den Regeln (R1-R10) vereinfacht werden. Sind die Resultate unterschiedlich, so sind die Ausgangsterme nicht äquivalent wie nachstehende Kette zeigt:

$$x \circ x^{-1} \overset{(R3)}{\to} \mathsf{e} \not\approx x \overset{(R2)}{\leftarrow} x \circ \mathsf{e} \overset{(R6)}{\leftarrow} x \circ (x^{-1} \circ x)$$

Die Knuth-Bendix Vervollständigung kann somit die Äquivalenz von Termen entscheiden, eine Beweiskette (wie auf Seite 1) bezüglich der ursprünglichen Gleichungen kann sie aber nicht erstellen.

Oftmals ist es aber erwünscht, dass die Ausgangsterme bezüglich der ursprünglichen Gesetze (G1-G3) als gleich gezeigt werden.

3 Projektziel

Ziel des Projektes ist die automatische Erstellung von Beweisketten, wie auf Seite 1 angeführt. Um diese Ketten zu erstellen, muss das Verfahren der Knuth-Bendix Vervollständigung derart erweitert werden, dass aus einer Beweiskette mittels der orientierten Gleichungen (hier Regeln R1-R10) eine Beweiskette mittels der ursprünglichen Gleichungen (hier G1-G3) erstellt werden kann.

Somit wird die Knuth-Bendix Vervollständigung intern zwar zur Berechnung der Beweisketten verwendet, bleibt vor der Endbenutzerin / dem Endbenutzer aber versteckt, was den Einsatzbereich der Software erhöht.

Um solche Beweisketten automatisch zu erstellen, wird das Vorgängerprojekt (E-Learning Projekt 2010.189) um die Berechnung und Ausgabe dieser Beweisketten erweitert. Eine beispielhafte Ausgabe eines automatisch erstellten Beweises ist in Abbildung 1 ersichtlich.

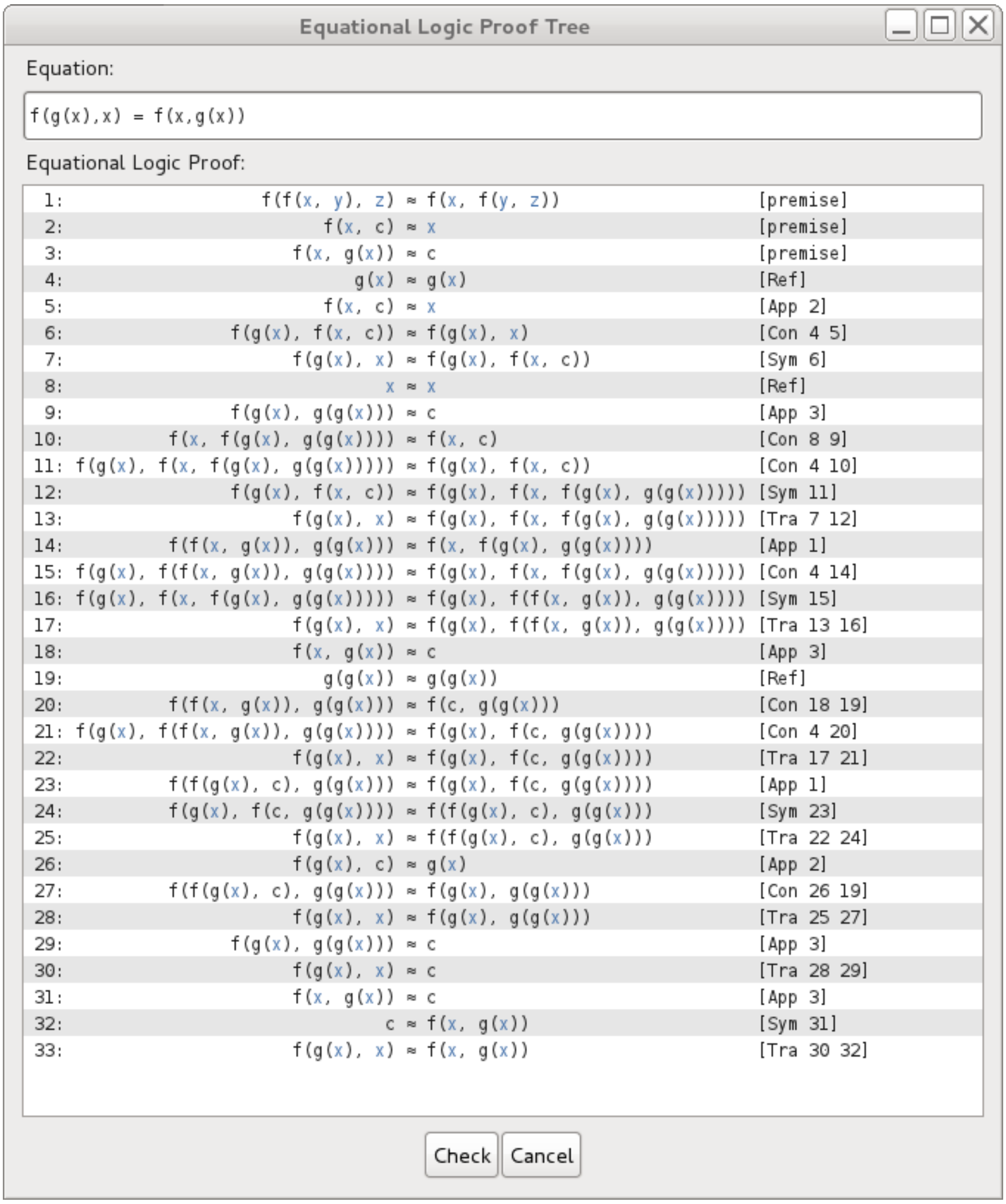

Abbildung 1: Automatisch erstellter Beispielbeweis.

4 Projektverlauf

Im Juni 2011 wurde der Vervollständigungsalgorithmus derart erweitert, dass eine Beweiskette (bezüglich der orientierten Gleichungen) in eine Beweiskette (bezüglich der originalen Gleichungen) umgewandelt werden kann.

Im Juli 2011 wurde ein Format für die übersichtliche Darstellung von Beweisketten erstellt.

Von August 2011 bis September 2011 erfolgte die Erweiterung des Programms, damit es solche Beweisketten automatisch berechnen und darstellen kann.

In der Projektabschlussphase schließlich wurde das Programm von Studierenden getestet, worauf kleinere Verbesserungen vorgenommen wurden.

Somit wurden die Projektziele erreicht.

5 Schlussbemerkungen

Projektbeteiligte

Dr. Harald Zankl, Thomas Sternagel, BSc.

Verfügbarkeit

Das Programm ist samt Dokumentation unter folgendem Link verfügbar:

`http://cl-informatik.uibk.ac.at/software/kbcv`

Dort steht auch eine benutzerfreundliche Applet-Version bereit, die eine leicht eingeschränkte Funktionalität bietet.

Die erstellte Software ist unter der *GNU Lesser General Public License*[1] frei verfügbar. Dies wurde durch einen entsprechenden Antrag beim ProjektServiceBüro der Universität Innsbruck bewerkstelligt.

[1] `http://www.gnu.org/licenses/lgpl.html`