Technische Hochschule Rosenheim

Programmcodevalidierung mit Coq

Lukas Kiederle
Fakultät für Informatik

WS 2019/20

Kurzfassung

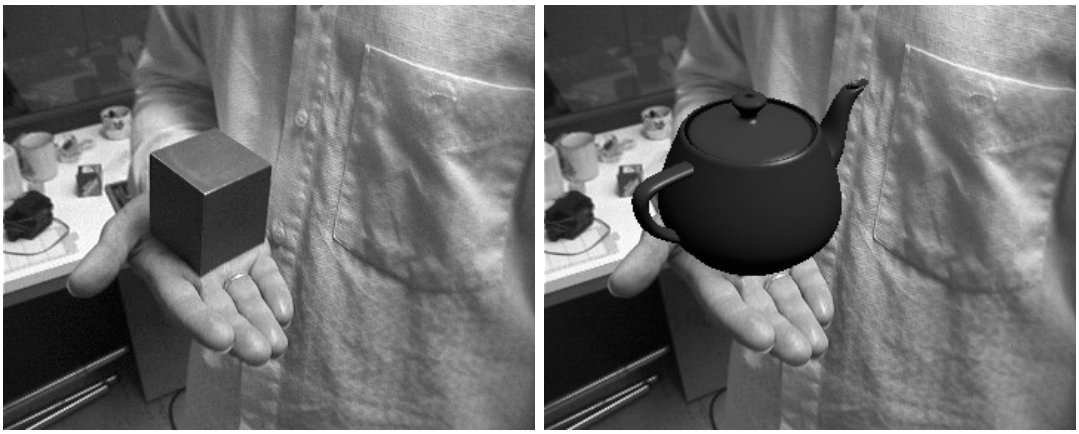
Schlagworte:

- Proof Assistant
- Coq
- Program code validation

Leseanleitung

Hinweise auf referenzierte Literatur und die daraus entnommenen Zitate, welche in eckigen Klammern angegebenen sind, werden im Literaturverzeichnis am Ende der Arbeit aufgeführt. Soll ein Begriff oder eine Formulierung besonders hervorgehoben werden, ist diese *kursiv* geschrieben. Abkürzungen werden bei erstmaligem Auftreten einmal in runden Klammern, anschließend an das Wort ausgeschrieben. Um den Lesefluss nicht zu stören, werden alle darauf folgenden Wiederholungen der Abkürzungen nicht immer explizit ausgeschrieben.
Möglicherweise unbekannte Begriffe und Fachbegriffe werden bei ihrer ersten Nennung **fett** gedruckt. Diese sind im Glossar in alphabetischer Reihenfolge aufgelistet und werden näher erklärt. Einzige Ausnahme hierbei sind Überschriften von Tabellen. Um ein zusammenhängendes Lesen der Arbeit zu erleichtern, werden bei Bedarf Erklärungen bereits im Text gegeben. Dabei wird davon ausgegangen, dass der Leser bereits mit grundlegenden Begriffen der Informatik vertraut ist. Ausgehend vom Wissensstand eines entsprechend vorgebildeten Lesers, werden demzufolge nur fachlich speziellere Begriffe erklärt.
Um Unklarheiten zu vermeiden, werden Fachbegriffe in und zur Beschreibung von Bildern und Prozessen in ihrer originalen Sprache Englisch verwendet und nicht immer übersetzt.
An den Stellen, an denen es der Ausführung des Textes dient, sind kurze Codebeispiele im Text eingebunden. Außerdem werden Abbildungen zur Veranschaulichung verwendet, um komplexe Prozesse einfacher und verständlicher zu machen. Größere Abbildungen befinden sich im Anhang und werden im passenden Textabschnitt referenziert. Damit soll der Lesefluss nicht gestört werden.

Inhaltsverzeichnis



(a) Originalbild (b) erweitertes Bild

Abbildung 1: Beispiel eines Augmented Reality Systems: es folgt eine Beschreibung (Bilder aus [Sch01])

Sequence	ARTS	wman	stcams	ARTVZ	ARTSUZ
# Frames	190	40	400	270	190
# relative movements	17955	780	79800	36315	17955
# movements after pre-sel.	14336	623	37915	21788	14343
min. angle in seq.	0.233°	5.95°	0.154°	0.00000171°	0.0388°
max. angle in seq.	81.7°	180°	47.3°	80.3°	80.9°
min. angle after pre-sel.	12.9°	21.1°	17.3°	16.3°	12.9°
max. angle after pre-sel.	81.7°	161°	47.3°	80.3°	80.9°

Tabelle 1: Datenselektion für verschiedene Testdatensätze.

1 Einleitung

Hier kommt die Einleitung.

1.1 Ein Abschnitt der Einleitung

Einen Überblick findet man z. B. in [Aue00].

Ein Beispiel wird in Abb. 1 gezeigt. Das verwendete Objekt ist in Abb. 1a dargestellt, das Ergebnis in Abb. 1b.

Eine Formel

$$f(x) = \frac{1}{3}x + 5, \quad x \in \mathbb{R}. \tag{1}$$

Und noch eine:

$$\boldsymbol{M} = \boldsymbol{A}\boldsymbol{x}\pi, \quad \boldsymbol{A} \in \mathbb{R}^{2\times 2}, \boldsymbol{x} \in \mathbb{R}^2. \tag{2}$$

Tabelle 1 gibt einen Überblick über XYZ.

2 Motivation

CompCert und Verifizierung von Programmcode (Compilercode)

3 Grundlagen

3.1 Was ist Coq

3.2 Was ist ein Proof Assisstant

https://www.youtube.com/watch?v=95VlaZTaWgc&t=2646s

3.2.1 Proof Verifier

3.2.2 Theorem Provers

4 Programmatische Coq-Grundlagen

4.1 Sprache

4.2 Beispielbeweise

5 Zusammenspiel Proof - Program

6 Anwendung

6.1 CompCert

7 Fazit

8 Aussicht

9 Glossar

A Erster Abschnitt des Anhangs

In diesem Anhang wird ...

Literatur

[Aue00] T. Auer. *Hybrid Tracking for Augmented Reality.* Dissertation, Technische Universität Graz, Graz, Austria, 2000.

[Sch01] J. Schmidt, I. Scholz und H. Niemann. Placing Arbitrary Objects in a Real Scene Using a Color Cube for Pose Estimation. In B. Radig und S. Florczyk, Hg., *Pattern Recognition, 23rd DAGM Symposium*, Bd. 2191 von *Lecture Notes in Computer Science*, S. 421–428. Springer-Verlag, Berlin, Heidelberg, New York, 2001.