EXPLIZITE UND IMPLIZITE INDUKTION

SIGISMUND RÜSTIG

Informatik Bachelor

ZUSAMMENFASSUNG. Anhand einer Reihe sogenannter expliziter und impliziter Kalküle zum Beweise induktiver Theoreme in einheitlicher Darstellung wird versucht, ein explizites und implizites Induktionsprinzip herauszuarbeiten. Die einzelnen Kalküle werden miteinander verglichen und voneinander abgegrenzt, die Beziehungen der beiden Grundsätze näher erläutert. Kursorisch wird auf die Übertragung der Ergebnisse auf die erweiterte Vervollständigung eingegangen.

A computer is a mathematical machine.
A program is a mathematical expression.
A programming language is a mathematical theory.
Programming is a mathematical activity.
— C. A. R. Hoare, *Essays in Computer Science* (1989)

1. EINLEITUNG

Seit der Arbeit von Rod Burstall über die Verwendung der strukturellen Induktion zur Verifikation von Programmen 1969 hat das Gebiet der automatisierten Induktion im Bereich maschineller Beweiser stark an Bedeutung gewonnen. Das von Burstall so erfolgreich angewendete Prinzip führte unter Aufnahme des vollständigen Induktionsschemas für die natürlichen Zahlen zu mechanisierbaren Varianten der noetherschen Induktion, die sonst meist in Gestalt der Wahl eines minimalen Gegenbeispiels bzgl. einer wohlfundierten Ordnung auftrat. Bei der folgenden stürmischen Entwicklung übernahmen – neben etwa der `LISP`-nahen Formulierung der *computational logic* von Robert S. Boyer und J Strother Moore – vornehmlich algebraische Spezifikationen und Termersetzungssysteme als Vermittler zwischen ausführbarem Computerprogramm und abstrakter mathematischer Notation die Rolle der Sprache, in der einerseits die gestellten Probleme und andererseits die zu beweisenden Theoreme formuliert wurden. Dieser formale Rahmen wurde aber nicht nur für induktive Theorembeweiser genutzt, sondern insbesondere in Ergänzung der sonst vorherrschenden Resolution und Paramodulation auch für maschinelle gleichungstheoretische Beweiser.

Aus diesem Bereich konnte ab 1980 durch die Veröffentlichung "On Proving Inductive Properties of Abstract Data Types" von David R. Musser das dort sehr fruchtbringende Verfahren von Donald E. Knuth (siehe Abbildung 1) und Paul B. Bendix zur sogenannten Vervollständigung von Termersetzungssystemen auch auf die induktive Theorie übertragen werden. Damit trat der direkten, *expliziten* Verwendung des noetherschen Induktionsprinzips in der strukturellen Induktion oder bei nach dem von Boyer und Moore erklärten *shell principle* definierten `LISP`-Funktionen die *induktionslose* oder *implizite Induktion* zur Seite; diese Bezeichnungen des Musserschen Verfahrens leiten dabei ihre Namen aus der Tatsache ab, daß es die Gültigkeit induktiver Theoreme gerade ohne die (offensichtliche) Verwendung von Induktion zeigt. Im Laufe der achtziger Jahre wurde das Vorgehen von Gérard Huet und Jean-Marie Hullot, Nachum Dershowitz, Jean-Pierre Jouannaud und Emmanuel Kounalis, Laurent Fribourg, Deepak Kapur, Paliath

Abbildung 1: Donald Ervin Knuth

Narendran und Hantao Zhang sowie Leo Bachmair in mannigfacher Weise ausgebaut und verfeinert.
Wir verweisen, insbesondere was die grundlegenden Resultate anbetrifft, auf die Übersichtsartikel von Dershowitz und Jouannaud [DJ90], David A. Plaisted [PZ97] und Jan W. Klop [Klo90].

2. Voraussetzungen

In einem zentralen Begriff der induktionslosen Induktion manifestiert sich zunächst ein wesentlicher Unterschied zur gleichungstheoretischen Knuth–Bendix–Vervollständigung (auf die wir hier wieder nur verweisen können (cf. insbesondere Bachmair [BD92], Bewers und Levi [BL90]):

Definition 1. Sei (Σ, R) eine Spezifikation mit adäquater Variablenmenge V. Ein Term $t \in \mathscr{T}(\Sigma, V)$ heißt *grundreduzibel bei einer Stellenmenge* $U \subseteq \mathscr{O}'(t)$ *bzgl.* $R' \subseteq R$, falls für jede Grundinstanz $t\gamma$ mit $\gamma \in \mathrm{G}\mathscr{S}(\Sigma, \mathrm{var}(t) \subseteq V)$ ein $u \in \mathscr{O}(t\gamma)$ existiert, sodaß entweder $u \in U$ und $t\gamma$ reduzibel bzgl. R' bei u oder $u \notin \mathscr{O}'(t)$ und $t\gamma$ reduzibel bzgl. R bei u.
Insbesondere heißt t *grundreduzibel bzgl.* R, wenn ein $U \subseteq \mathscr{O}'(t)$ existiert, sodaß t grundreduzibel bei U bzgl. R ist.

3. Explizite Induktion

Die Grundlage aller hier vorzustellenden Kalküle ist das noethersche Induktionsprinzip; wir formulieren es in einer speziell an Spezifikationen angepaßten Weise.
Dazu dehnen wir einerseits Stabilordnungen auf Termen auch auf Gleichungen durch die sogenannte Maximumserweiterung aus: es werden die Multimengen der maximalen Elemente der beiden Gleichungsseiten bzgl. der Multimengenerweiterung der ursprünglichen Stabilordnung verglichen; den Begriff einer Stabilordnung verwenden wir dabei für alle Mengen, für die ein Substitutionsbegriff erklärt ist.

Definition 2. Sei Σ eine Signatur, V eine Σ-adäquate Variablenmenge und $\preceq$ eine Stabilordnung auf $\mathscr{T}(\Sigma, V)$. Für eine Gleichungsmenge $E \subseteq \mathscr{E}(\Sigma, V)$ und eine Gleichung

$e \in \mathscr{E}(\Sigma, V)$ heißt die Menge $\{E \preceq e\} = \{f\sigma : f \in E,\ f\sigma \preceq e\}$ (nach oben durch e) *beschränkte Instanzenmenge* von E. Die Menge $\{E \prec e\} = \{f\sigma : f \in E,\ f\sigma \prec e\}$ heißt (nach oben durch e) *echt beschränkte Instanzenmenge* von E.

Mit diesen Vorbereitungen hat man

Satz 3. Sei (Σ, R) eine Spezifikation mit adäquater Variablenmenge V, $\preceq$ eine Stabilordnung auf $\mathscr{E}(\Sigma, V)$ und $e \in \mathscr{E}(\Sigma, V)$. Dann gilt:

$$\forall \gamma \in \mathrm{G}\mathscr{S}(\Sigma, \mathrm{var}(e) \subseteq V) : R \cup \{\{e\} \prec e\gamma\} \vdash e\gamma \supset R \vdash_{\mathrm{i}} e.$$

Beweis. Angenommen, die Behauptung wäre falsch. Dann gibt es eine Grundsubstitution $\gamma \in \mathrm{G}\mathscr{S}(\Sigma, \mathrm{var}(e) \subseteq V)$, sodaß $R \nvdash e\gamma$; sei $e\gamma$ minimal bzgl. $\prec$ mit dieser Eigenschaft. Nach der Voraussetzung gibt es einen Beweis $R \cup \{\{e\} \prec e\gamma\} \vdash e\gamma$, und da dabei nur kleinere Grundinstanzen von e als $e\gamma$ bzgl. $\prec$ benutzt werden, diese also wegen der Minimalität von $e\gamma$ aus R sämtlich ableitbar sind, gibt es auch einen Beweis $R \vdash e\gamma$, im Widerspruch zur Annahme. □

4. Implizite Induktion

Aus systematischen Gründen und als Kontrastierung des bereits eingeführten (expliziten) noetherschen Induktionsprinzips beginnen wir mit einer Axiomatisierung von Bronsard, Reddy und Hasker, die in ihrer Arbeit "Induction Using Term Orderings" [BRH96] eine nur scheinbar unwesentliche Verfeinerung des noetherschen Induktionsprinzips angeben haben, die zur Grundlage der impliziten Induktion gemacht werden kann:

Satz 4. Sei (Σ, R) eine Spezifikation mit adäquater Variablenmenge V, $\preceq$ eine Stabilordnung auf $\mathscr{E}(\Sigma, V)$ und $e \in \mathscr{E}(\Sigma, V)$. Dann gilt:

$$\forall \gamma \in \mathrm{G}\mathscr{S}(\Sigma, \mathrm{var}(e) \subseteq V) : \exists e' \in \mathscr{E}(\Sigma, V) : \\ \big(e'\gamma \prec e\gamma \wedge R \cup \{e'\gamma\} \vdash e\gamma \wedge R \cup \{\{e\} \preceq e'\gamma\} \vdash e'\gamma\big) \supset R \vdash_{\mathrm{i}} e.$$

Beweis. Angenommen, die Behauptung wäre falsch. Dann gibt es eine Grundsubstitution $\gamma \in \mathrm{G}\mathscr{S}(\Sigma, \mathrm{var}(e) \subseteq V)$, sodaß $R \nvdash e\gamma$; sei $e\gamma$ minimal bzgl. $\prec$ mit dieser Eigenschaft. Nach der Voraussetzung gibt es ein $e' \in \mathscr{E}(\Sigma, V)$ mit $e'\gamma \prec e\gamma$, $R \cup \{e'\gamma\} \vdash e\gamma$ und $R \cup \{\{e\} \preceq e'\gamma\} \vdash e'\gamma$. Da für den letzten Beweis nur kleinere oder quasigleiche Grundinstanzen von e als $e'\gamma$ bzgl. $\preceq$, also nur kleinere Grundinstanzen als $e\gamma$ bzgl. $\prec$ benutzt werden, und diese wegen der Minimalität von $e\gamma$ aus R sämtlich ableitbar sind, gibt es auch Beweise $R \vdash e'\gamma$ und damit $R \vdash e\gamma$, im Widerspruch zur Annahme. □

Die Verbesserung liegt also einmal darin, daß zum Beweis einer Grundinstanz einer Gleichung nicht nur Instanzen derselben Gleichung herangezogen werden dürfen; das findet man aber auch schon in den Anwendungen des noetherschen Induktionsprinzips im vorigen Kapitel verwirklicht, die wechselseitige Induktion erlauben. Weiter kann durch die zusätzliche Kleinerbedingung an die Hilfsgleichung zu deren Beweis die nicht mehr notwendig echt beschränkte Instanzenmenge herangezogen werden; dies gestattet eventuell ein einfacheres Vorgehen.

5. Zusammenfassung

Die Forschung hat in den letzten Jahren das Thema einer Verbindung der beiden Prinzipien der expliziten und impliziten Induktion desöftern aufgegriffen, wie etwa die eigene Sektion "Implict and Explicit Induction" auf der letzten "Conference on Automated Deduction" 1994 belegt. Dementgegen sieht Gramlich bereits 1992 nach der Arbeit von

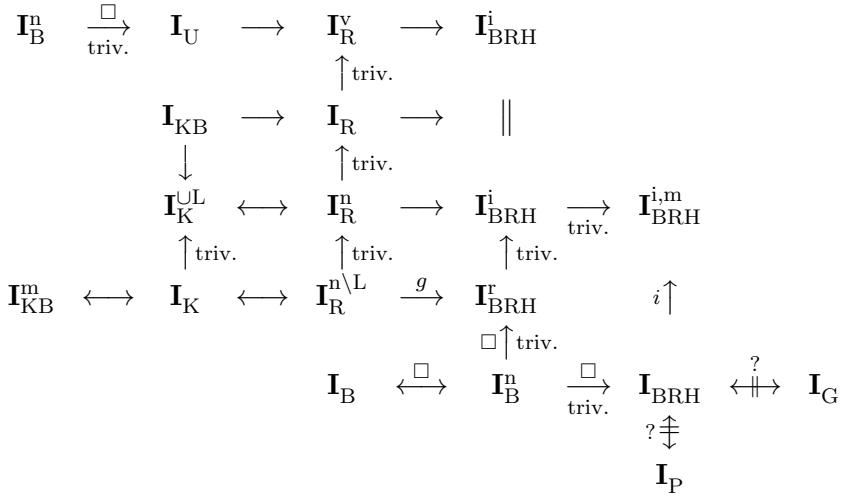

Abbildung 2: Ergebnisüberblick

Reddy und einigen eigenen Veröffentlichungen einen schon so engen Zusammenhang, daß er den Begriff *inductionless induction* nur noch auf die Konsistenzbeweismethode, sozusagen einen negativen Ansatz, anwendet [Gra92, S. 8]. Dem setzt er Induktionsbeweiser gegenüber, die Induktionsschemata, also (heuristische) Verfahren zur Auswahl von Induktionsvariablen oder Induktionskontexten benutzen. Wir sind hier nicht auf solche – zum Teil, wie der induktive Theorembeweiser von Boyer und Moore zeigt, sehr erfolgreiche – Ansätze eingegangen, sondern lediglich auf die Grundlagen der expliziten Verfahren, d. h. im wesentlichen die Organisation der Induktionshypothesen und ihre Anwendung, und auch der impliziten Verfahren.
Insgesamt erhält man aus unserer Untersuchung das Überblicksbild in Abb. 2.

Literatur

[BD92] Bachmair, Leo ; Dershowitz, Nachum: Equational Inference, Canonical Proofs, And Proof Orderings. In: *Journal of the ACM* 41 (1992), S. 236–276

[BL90] Bevers, Eddy ; Lewi, Johan: Proof by Consistency in Conditional Equational Theories. In: *CTRS*, 1990, S. 194–205

[BRH96] Bronsard, François ; Reddy, Uday S. ; Hasker, Robert W.: Induction Using Term Orders. In: *J. Autom. Reasoning* 16 (1996), Nr. 1-2, S. 3–37

[DJ90] Dershowitz, Nachum ; Jouannaud, Jean-Pierre: Rewrite Systems. In: *Handbook of Theoretical Computer Science, Volume B: Formal Models and Sematics (B)*. MIT Press, 1990, S. 243–320

[Gra92] Gramlich, Bernhard: Towards Intelligent Inductive Proof Engineering / Fachbereich Informatik, Universität Kaiserslautern. 1992 (SR-92-01). – Forschungsbericht

[Klo90] Klop, Jan W.: Term Rewriting Systems: From Church-Rosser to Knuth-Bendix and Beyond. In: *ICALP*, 1990, S. 350–369

[PZ97] Plaisted, David A. ; Zhu, Yunshan: Equational Reasoning using AC Constraints. In: *In Proceedings of the Fifteenth International Joint Conference on Artificial Intelligence (IJCAI-97*, 1997, S. 108–113