Tableau-Based Automation for Typed Finite Sets

Alexander Anisimov

Advisors: Chrisian Doczkal, Gert Smolka
Supervisor: Gert Smolka

Saarland University
Programming Systems Lab

September 11, 2015

Languages of the Calcului

Definition

$$set ::= \dot{\emptyset} \mid x \mid \langle set \rangle \mid set \dot{\cup} set \mid set \dot{-} set \mid \dot{\mathcal{P}}(set) \mid \langle x \dot{\in} set \mid form \rangle$$

$$rel ::= set \dot{\in} set \mid set \dot{\subseteq} set \mid set \dot{=} set$$

$$form ::= \dot{\bot} \mid rel \mid \dot{\neg} form \mid form \dot{\wedge} form \mid form \dot{\vee} form \mid form \dot{\to} form$$

- Minimal calculus $\subseteq$ Powerset extension $\subseteq$ Separation extension (by accumulation of the operators)
- A *branch* is a finite set of well-typed formulas
- A branch is closed if it contains $\dot{\bot}$ and open otherwise
- In the following: every relation we state is well-typed

Set Representation

Definition (*fset*)

Let T be a *choiceType*. Then ($fset\ T$) is the type of finite sets with elements of type T.

- $fset\ T$ is again a choice type
- *choiceTypes* allow for an extensional set representation
- We can build stratified hierarchies of fsets

Definition (Level)

$lv(s) :=$ the number of toplevel *fset* constructors in the type of s

$S_l(\Gamma) :=$ all sets s with $lv(s) = l$ occurring in Γ

$L_\Gamma :=$ the highest populated level

Saturation Rules

Propositional rules:

$$\text{(P1)}\ \frac{s \dot{\wedge} t}{s \quad\quad t} \qquad \text{(P2)}\ \frac{s \dot{\vee} t}{s \mid t} \qquad \text{(P3)}\ \frac{s \dot{\rightarrow} t}{\dot{\neg} s \mid t}$$

$$\text{(P4)}\ \frac{\dot{\neg}(s \dot{\wedge} t)}{\dot{\neg} s \mid \dot{\neg} t} \qquad \text{(P5)}\ \frac{\dot{\neg}(s \dot{\vee} t)}{\dot{\neg} s \quad\quad \dot{\neg} t} \qquad \text{(P6)}\ \frac{\dot{\neg}(s \dot{\rightarrow} t)}{s \quad\quad \dot{\neg} t}$$

$$\text{(P7)}\ \frac{\dot{\neg}\dot{\neg} s}{s}$$

Branch-closing rules:

$$\text{(D1)}\ \frac{b \quad\quad \dot{\neg} b}{\dot{\bot}} \qquad \text{(D2)}\ \frac{x \dot{\neq} x}{\dot{\bot}} \qquad \text{(D3)}\ \frac{x \dot{\in} \dot{\emptyset}}{\dot{\bot}}$$

Saturation Rules

Regular saturation rules:

$$(\mathrm{S1})\ \frac{x \dot{\in} A \qquad A \dot{\subseteq} B}{x \dot{\in} B} \qquad (\mathrm{S2})\ \frac{x \dot{\notin} A \qquad B \dot{\subseteq} A}{x \dot{\notin} B}$$

$$(\mathrm{S3})\ \frac{A \dot{\not\subseteq} B}{x_{AB} \dot{\in} A \qquad x_{AB} \dot{\notin} B} \qquad (\mathrm{S4})\ \frac{A \dot{=} B}{A \dot{\subseteq} B \qquad B \dot{\subseteq} A}$$

$$(\mathrm{S5})\ \frac{A \dot{\neq} B}{\begin{array}{c|c} x_{AB} \dot{\in} A & x_{BA} \dot{\in} B \\ x_{AB} \dot{\notin} B & x_{BA} \dot{\notin} A \end{array}} \qquad (\mathrm{S6})\ \frac{x \dot{=} y \qquad y \dot{\in} A}{x \dot{\in} A}$$

$$(\mathrm{S7})\ \frac{x \dot{=} y \qquad y \dot{=} z}{x \dot{=} z} \qquad (\mathrm{S8})\ \frac{x \dot{=} y}{y \dot{=} x}$$

Saturation Rules

Regular saturation rules:

$$(\mathrm{S9})\ \frac{x \dot{\in} \langle y \rangle}{x \dot{=} y} \qquad (\mathrm{S10})\ \frac{x \dot{\notin} \langle y \rangle}{x \dot{\neq} y}$$

$$(\mathrm{S11})\ \frac{\langle x \rangle \dot{\subseteq} A}{x \dot{\in} A} \qquad (\mathrm{S12})\ \frac{x \dot{\in} A \dot{\cup} B}{x \dot{\in} A \mid x \dot{\in} B}$$

$$(\mathrm{S13})\ \frac{x \dot{\notin} A \dot{\cup} B}{x \dot{\notin} A \qquad x \dot{\notin} B} \qquad (\mathrm{S14})\ \frac{x \dot{\in} A \dot{-} B}{x \dot{\in} A \qquad x \dot{\notin} B}$$

$$(\mathrm{S15})\ \frac{x \dot{\notin} A \dot{-} B}{x \dot{\notin} A \mid x \dot{\in} B}$$

Saturation Rules

Cut rules:

$$(\mathrm{C1})\ \frac{X \in S_l(\Gamma) \qquad Y \in S_l(\Gamma)}{X \dot{=} Y \mid X \dot{\neq} Y} \qquad (\mathrm{C2})\ \frac{x \in S_l(\Gamma) \qquad A \in S_{l+1}(\Gamma)}{x \dot{\in} A \mid x \dot{\notin} A}$$

$$(\mathrm{C3})\ \frac{A \in S_l(\Gamma) \qquad B \in S_l(\Gamma)}{A \dot{\subseteq} B \mid A \dot{\nsubseteq} B}$$

Extension rules:

$$(\mathrm{Q1})\ \frac{A \dot{\in} \dot{\mathcal{P}}(B)}{A \dot{\subseteq} B} \qquad (\mathrm{Q2})\ \frac{A \dot{\notin} \dot{\mathcal{P}}(B)}{x_{AB} \dot{\in} A \qquad x_{AB} \dot{\notin} B}$$

$$(\mathrm{R1})\ \frac{y \dot{\in} \langle x \dot{\in} A \mid p \rangle}{y \dot{\in} A \qquad p^x_y} \qquad (\mathrm{R2})\ \frac{y \dot{\notin} \langle x \dot{\in} A \mid p \rangle}{y \dot{\notin} A \mid \dot{\neg} p^x_y}$$

Termination and Nontermination

The calculus with powerset extension terminates

- $\mathcal{S}(\Gamma)$ is the closure of sets that possibly can be generated in Γ
- $\mathcal{S}(\Gamma)$ is finite
- No literal is removed or added twice
- Finitely many possible relations between finitely many sets
- Number of literals is upper bounded by $6|\mathcal{S}(\Gamma)|$

The calculus with the separation extension diverges

$$F := \langle a \dot{\in} A \mid B \dot{\not\subseteq} \langle a \rangle \dot{\cup} C \rangle$$

$x \dot{\in} F, B \dot{\subseteq} F$	
$x \dot{\in} A,\ B \dot{\not\subseteq} \langle x \rangle \dot{\cup} C$	(R1)
$y \dot{\in} B,\ y \dot{\notin} \langle x \rangle \dot{\cup} C$	(S3)
$y \dot{\in} F$	(S1)
$y \dot{\in} A,\ B \dot{\not\subseteq} \langle y \rangle \dot{\cup} C$	(R1)

Cut-Rules in

The Minimal System

Example

The following branch cannot be closed without cut rules:

<table>
<tr><td colspan="3">$A \dot{-} B \dot{\subseteq} \dot{\emptyset}$
$x \dot{\in} A$
$x \dot{\notin} B$</td></tr>
<tr><td rowspan="2">$x \dot{\in} A \dot{-} B$
$x \dot{\in} \dot{\emptyset}$
$\dot{\bot}$</td><td colspan="2">$x \dot{\notin} A \dot{-} B$</td></tr>
<tr><td>$x \dot{\notin} A$
$\dot{\bot}$</td><td>$x \dot{\in} B$
$\dot{\bot}$</td></tr>
</table>

- No direct relation between A and B
- No direct relation between x and $A \dot{-} B$

$\Rightarrow$ cut rules needed for the minimal system to be complete

The Powerset Extension

In the powerset extension, cut rules are needed significantly more often

Example

The following branch is representative for a large class of problems:

<table>
<tr><td colspan="2">$\dot{\mathcal{P}}(A)\dot{\subseteq}\dot{\mathcal{P}}(B)$
$A\dot{\not\subseteq}B$</td></tr>
<tr><td>$A\dot{\in}\dot{\mathcal{P}}(A)$
$A\dot{\in}\dot{\mathcal{P}}(B)$
$A\dot{\subseteq}B$
$\dot{\bot}$</td><td>$A\dot{\notin}\dot{\mathcal{P}}(A)$
$x_{AA}\dot{\in}A$
$x_{AA}\dot{\notin}A$
$\dot{\bot}$</td></tr>
</table>

- No other rules to infer something from subset relations only
- No connecting relation between the levels $lv(A)$ and $lv(\dot{\mathcal{P}}(A))$

Model

Definition (Variable Assignment)

A variable assignment is a function J of type

$$J : \forall l.\ vars_l(\Gamma) \rightarrow fset^l(D)$$

Definition (Model)

Let J be a variable assignment. We define the *model* induced by J as follows:

$$\begin{aligned}
\hat{J}\dot{\emptyset} &:= \emptyset \\
\hat{J}A &:= JA \text{ if } A \in vars_l(\Gamma) \text{ for some } l \in \mathbb{N} \\
\hat{J}\langle x\rangle &:= \{\hat{J}x\} \\
\hat{J}A \dot{\cup} B &:= \hat{J}B \cup \hat{J}C \\
\hat{J}A \dot{-} B &:= \hat{J}B \setminus \hat{J}C
\end{aligned}$$

Definition (Satisfiability)

Let J be a variable assignment and $\hat{J}$ the model induced by it.

$$J \models A \dot{\circ} B :\Leftrightarrow \hat{J}A \circ \hat{J}B$$

for $\dot{\circ} \in \{\dot{\in}, \dot{\notin}, \dot{\subseteq}, \dot{\nsubseteq}, \dot{=}, \dot{\neq}\}$ and $\circ$ the corresponding semantic relation. We define satisfiability of formulas as follows:

$$\begin{aligned} J \models \dot{\neg} s \quad &:\Leftrightarrow \quad \neg J \models s \\ J \models s \dot{\wedge} t \quad &:\Leftrightarrow \quad J \models s \wedge J \models t \\ J \models s \dot{\vee} t \quad &:\Leftrightarrow \quad J \models s \vee J \models t \\ J \models s \dot{\rightarrow} t \quad &:\Leftrightarrow \quad J \models s \rightarrow J \models t \end{aligned}$$

Γ is called *satisfiable*, if there exists some J such that for all formulas $\phi \in \Gamma$ we have $J \models \phi$.

Completeness

Definition (Saturated Branch)

A branch is saturated if none of the tableau rules is applicable.

Definition (Completeness)

A tableau system is complete, if every open saturated branch is satisfiable.

Set Interpretation

Let Γ be an open saturated branch.

Definition (Interpretation)

$$D_\Gamma := S_0(\Gamma)/\doteq$$

$$\mathcal{I} : \quad \forall l \in \mathbb{N}.\ S_l(\Gamma) \to fset^l(D_\Gamma)$$

$$\mathcal{I}_l(X) := \begin{cases} [X]_{\doteq} & l = 0 \\ \{\mathcal{I}_{l-1}(x) \mid x \dot{\in} X \in \Gamma\} & l > 0 \end{cases}$$

For the interpretation to be well-defined we have to show the following

Lemma

$\doteq$ is an equivalence relation in Γ.

'Model'-Property of the Interpretation $\mathcal{I}$

Lemma

Let $X, Y \in \mathcal{S}(\Gamma)$ and $\dot{\circ} \in \{\dot{\in}, \dot{\notin}, \dot{\subseteq}, \dot{\nsubseteq}, \dot{=}, \dot{\neq}\}$. Then,

$$\mathcal{I}X \circ \mathcal{I}Y \Leftrightarrow X \dot{\circ} Y \in \Gamma.$$

Proof by induction on $l = lv(Y)$.

I.S.: $l \to l + 1 = lv(Y)$

($\dot{\in}$) "$\Rightarrow$" Let $\mathcal{I}X \in \mathcal{I}Y$.

$\Rightarrow \mathcal{I}X \in \{\mathcal{I}y \mid y \dot{\in} Y \in \Gamma\}$
$\Rightarrow \exists y \in \mathcal{S}(\Gamma).\ y \dot{\in} Y \in \Gamma \ \wedge\ \mathcal{I}X = \mathcal{I}y$
$\Rightarrow X \dot{=} y \in \Gamma$ by I.H.
$\Rightarrow X \dot{=} y, y \dot{\in} Y \in \Gamma \Rightarrow X \dot{\in} Y \in \Gamma$ due to (S6)

"$\Leftarrow$" Let $X \dot{\in} Y \in \Gamma$. Then, $\mathcal{I}X \in \{\mathcal{I}x \mid x \dot{\in} Y \in \Gamma\} = \mathcal{I}Y$

Model

Definition

We define $I := \mathcal{I}|_{vars(\Gamma)}$ to be our variable assignment and $\hat{I}$ the corresponding model.

Lemma

a) $\mathcal{I}\dot{\emptyset} = \emptyset$

b) $\langle x \rangle \in \mathcal{S}(\Gamma) \Rightarrow \mathcal{I}\langle x \rangle = \{\mathcal{I}x\}$

c) $A \dot{\cup} B \in \mathcal{S}(\Gamma) \Rightarrow \mathcal{I}(A \dot{\cup} B) = \mathcal{I}A \cup \mathcal{I}B$

d) $A \dot{-} B \in \mathcal{S}(\Gamma) \Rightarrow \mathcal{I}(A \dot{-} B) = \mathcal{I}A \backslash \mathcal{I}B$

$\Rightarrow \hat{I}|_{\mathcal{S}(\Gamma)} = \mathcal{I}$

Completeness Proof

Theorem

The minimal system is complete.

Proof.

- Γ is open and saturated
- $\forall X, Y \in \mathcal{S}(\Gamma).\ \mathcal{I}X \circ \mathcal{I}Y \Leftrightarrow X \dot{\circ} Y \in \Gamma$
- $\hat{I}|_{\mathcal{S}(\Gamma)} = \mathcal{I}$

$\Rightarrow \quad \forall X, Y \in \mathcal{S}(\Gamma).\ \hat{I}X \circ \hat{I}Y \Leftrightarrow X \dot{\circ} Y \in \Gamma$

$\Rightarrow \quad \forall \phi \in \Gamma.\ \hat{I} \models \phi$

$\Rightarrow \quad \Gamma$ is satisfiable. □

Tableaux in Coq

- A branch is realized as goal
  - Assumptions are interpreted as formulas
  - The conclusion is `False`
- Every rule is stated and proven as a lemma
- If the premisses of a rule are on the branch its conclusion can be posed and proven
- We branch by posing a disjunction and destructing it
- Boolean connectives are eliminated by tableau rules
- The rules are grouped by their structure
  - branch closing
  - non-branching
  - branching
  - cut rules

Final Tactics

```
Ltac core :=
  repeat(
    genSubst; (* reflect equalities and call subst *)
    repeat nonbranching; (* all possible nb-rules *)
    try closebranch;
    genSubst; (* in case you generated new equalities *)
    try branching; (* exactly one branching rule *)
    try closebranch
  ).

Ltac fset_dec :=
  preproc; (* normalize goal *)
  repeat(
    try closebranch;
    core;
    try cutrules (* apply exactly one cut rule *)
  ).

Ltac fset_nocut := preproc; try closebranch; core.
```

Examples I

- The example for the necessity of cuts in the basic ruleset
  $A \dot{-} B \dot{\subseteq} \dot{\emptyset} \rightarrow x \dot{\in} A \rightarrow x \dot{\in} B$
  is solved instantaneously.
- The propositions
  $A \dot{\subseteq} C \rightarrow B \dot{\subseteq} C \rightarrow ((C \dot{-} A) \dot{\cup} (C \dot{-} B)) \doteq (C \dot{-} (A \dot{\cap} B))$
  $A \dot{\subseteq} C \rightarrow B \dot{\subseteq} C \rightarrow ((C \dot{-} A) \dot{\cap} (C \dot{-} B)) \doteq (C \dot{-} (A \dot{\cup} B))$
  are proved either in less than half a second.
- $\dot{\mathcal{P}}(A) \dot{-} \langle A \rangle \ \dot{\subseteq} \ \dot{\emptyset} \rightarrow A \doteq \dot{\emptyset}$
  requires application of cut rules and is solved in less than one second.

Examples II

- The example for the importance of cut rules in the powerset extension
  $\dot{\mathcal{P}}(A) \dot{\subseteq} \dot{\mathcal{P}}(B) \rightarrow A \dot{\subseteq} B$
  is solved in 2.73 seconds.
- The proposition
  $\dot{\mathcal{P}}(A \dot{\cup} B) \dot{\subseteq} \dot{\mathcal{P}}(A) \dot{\cup} \dot{\mathcal{P}}(B) \rightarrow A \dot{\subseteq} B \dot{\vee} B \dot{\subseteq} A$
  requires application of cut rules and is solved in about 45 seconds. A larger context may cause the tactic to run even longer.

Related Work I

- Domenico Cantone 1991: *Decision procedures for elementary sublanguages of set theory: X. Multilevel syllogistic extended by the singleton and powerset operators.*
  - Completeness of a fragment of set theory with unrestricted powerset operator
- Domenico Cantone, Calogero G. Zarba 1999: *A Tableau-Based Decision Procedure for a Fragment of Set Theory Involving a Restricted Form of Quantification.*
  - States that the decidability of the fragment of ZF set theory with unrestricted universal quantification is an open problem
  - Correspondence between universal quantification and set separations

Related Work II

- Benjamin Shults 1997: *Comprehension and Description in Tableaux.*
  - Efficient proof automation with separations
  - Different handling of extensionality
  - Usage of substitution
- Bernhard Beckert, Ulrike Hartmer 1998: *A Tableau Calculus for Quantifier-Free Set Theoretic Formulae.*
  - Termination and completeness proofs for a system similar to our minimal calculus

Outline of the Thesis

- Proof automation for boolean logic
  - Study of the technique proof by reflection
  - Implementation of a reflective boolean tautology solver
- Proof automation for typed finite sets
  - Theory: 3 tableau calculi
    - Minimal system: terminating and complete
    - Powerset extension: terminating
    - Separation extension: in general nonterminating
  - Practice: implementation of automation tactics for *fset* in Ssreflect
    - Shallow implementation of tableau saturation strategy
    - Tactics with and without cut rules
    - Possibility to give unfoldable definitions as argument

Possible Improvement

- Automation for boolean logic
  - Improve implementation
  - Use more efficient decision procedure
- Automation for typed finite sets
  - Avoid cut rules more efficiently
  - Find necessary rules for the completeness of the powerset extension
  - Find a 'harmless' subclass of the separation operator that doesn't diverge
  - Improve implementation
  - Formalize termination and conpleteness proofs in Coq

References I

Samuel Boutin:
Using Reflection to Build Efficient and Certified Decision Procedures.
TACS 1997: 515-529, Springer 1997

Bernhard Beckert, Ulrike Hartmer:
A Tableau Calculus for Quantifier-Free Set Theoretic Formulae.
TABLEAUX 1998: 93-107, Springer 1998

Domenico Cantone:
Decision procedures for elementary sublanguages of set theory: X. Multilevel syllogistic extended by the singleton and powerset operators.
J. Autom. Reasoning 7:193-230, 1991, Springer 1991

References II

- Domenico Cantone, Rosa Ruggeri Cannata:
  Deciding set-theoretic formulae with the predicate 'finite' by a tableau calculus.
  Le Matematiche Vol 50, No 1 (1995)

- Domenico Cantone, Calogero G. Zarba:
  A New Fast Tableau-Based Decision Procedure for an Unquantified Fragment of Set Theory.
  FTP (LNCS Selection) 1998: 126-136, Springer 2000

- Domenico Cantone, Calogero G. Zarba:
  A Tableau-Based Decision Procedure for a Fragment of Set Theory Involving a Restricted Form of Quantification.
  TABLEAUX 1999: 97-112, Springer 1999

References III

Domenico Cantone, Calogero G. Zarba, Rosa Ruggeri Cannata:
A Tableau-Based Decision Procedure for a Fragment of Set Theory with Iterated Membership.
J. Autom. Reasoning 34(1): 49-72 (2005), Springer 2005

Adam Chlipala:
Certified Programming with Dependent Types (2014).
http://adam.chlipala.net/cpdt/

Christian Doczkal:
Finite Sets over Countalbe Types in Ssreflect
http://www.ps.uni-saarland.de/formalizations/fset.php

References IV

Alfredo Ferro, Eugenio G. Omodeo, Jacob T. Schwartz:
Decision procedures for some fragments of set theory.
CADE 1980: 88-96, Springer 1980

Benjamin Shults:
Comprehension and Description in Tableaux.
1997

Coq Development Team:
Coq Documentation
https://coq.inria.fr/documentation