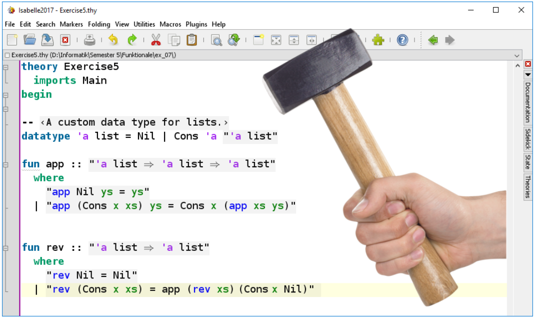
Superposition with Datatypes and Codatatypes

Jasmin Blanchette
Vrije Universiteit Amsterdam
MPI-INF Saarbrücken
Nicolas Peltier
Université Grenoble Alpes
Simon Robillard
Chalmers University of Technology

(co)datatypes everywhere!

- program verification
- metatheory of programming languages
- formalization of mathematics
- ...

Typical application of ATPs



Partial axiomatization?

Partial axiomatization?

✗ Inconvenient

Partial axiomatization?

- ✗ Inconvenient
- ✗ Inefficient

Partial axiomatization?

✗ Inconvenient

✗ Inefficient

✗ Incomplete

Example

$$
\begin{aligned}
\text{(co)datatype } \tau = {} & E : \tau \\
\mid {} & F : \tau \to \tau \\
\mid {} & G : \alpha \times \tau \to \tau
\end{aligned}
$$

Axioms for freely generated (co)datatypes

Distinctness

$\forall x, E \not\approx F(x)$ $\qquad$ $\forall \bar{x}, F(x_1) \not\approx G(x_2, x_3)$ $\qquad$ $\forall \bar{x}, G(x_1, x_2) \not\approx E$

Axioms for freely generated (co)datatypes

Distinctness

$$\forall x, E \not\approx F(x) \qquad \forall \bar{x}, F(x_1) \not\approx G(x_2, x_3) \qquad \forall \bar{x}, G(x_1, x_2) \not\approx E$$

Injectivity

$$\forall \bar{x},\; F(x_1) \approx F(x_2) \rightarrow x_1 \approx x_2$$

$$\forall \bar{x},\; G(x_1, x_1') \approx G(x_2, x_2') \rightarrow x_1 \approx x_2 \land x_1' \approx x_2'$$

Axioms for freely generated (co)datatypes

Distinctness

$$\forall x, E \not\approx F(x) \qquad \forall \bar{x}, F(x_1) \not\approx G(x_2, x_3) \qquad \forall \bar{x}, G(x_1, x_2) \not\approx E$$

Injectivity

$$\forall \bar{x},\ F(x_1) \approx F(x_2) \rightarrow x_1 \approx x_2$$
$$\forall \bar{x},\ G(x_1, x_1') \approx G(x_2, x_2') \rightarrow x_1 \approx x_2 \land x_1' \approx x_2'$$

Exhaustivity

$$\forall x\ \exists \bar{y},\ x \approx E \lor x \approx F(y_1) \lor x \approx G(y_2, y_3)$$

Acyclicity

$$\forall x,\ x \not\approx F(x)$$
$$\forall x\ y,\ x \not\approx G(y, x)$$

Acyclicity

$$\forall x,\ x \not\approx F(x)$$
$$\forall x\ y,\ x \not\approx G(y, x)$$
$$\forall x,\ x \not\approx F(F(x))$$
$$\forall x\ y,\ x \not\approx F(G(y, x))$$
$$\forall x\ y,\ x \not\approx G(y, F(x))$$
$$\forall x\ \bar{y},\ x \not\approx G(y_1, G(y_2, x))$$

Acyclicity

$$\forall x,\ x \not\approx F(x)$$
$$\forall x\ y,\ x \not\approx G(y, x)$$
$$\forall x,\ x \not\approx F(F(x))$$
$$\forall x\ y,\ x \not\approx F(G(y, x))$$
$$\forall x\ y,\ x \not\approx G(y, F(x))$$
$$\forall x\ \bar{y},\ x \not\approx G(y_1, G(y_2, x))$$
$$\forall x,\ x \not\approx F(F(F(x)))$$
$$\forall x\ y,\ x \not\approx F(F(G(y, x)))$$
$$\forall x\ y,\ x \not\approx F(G(y, F(x)))$$
$$\forall x\ \bar{y},\ x \not\approx F(G(y_1, G(y_2, x)))$$
$$\forall x\ y,\ x \not\approx G(y, F(F(F(x))))$$
$$\forall x\ \bar{y},\ x \not\approx G(y_1, F(F(G(y_2, x))))$$
$$\forall x\ \bar{y},\ x \not\approx G(y_1, F(G(y_2, F(x))))$$
$$\forall x\ \bar{y},\ x \not\approx G(y_1, F(G(y_2, G(y_3, x))))$$
$$\forall x,\ x \not\approx F(F(F(F(x))))$$
$$\forall x\ y,\ x \not\approx F(F(F(G(y, x))))$$

Acyclicity

$$\forall x,\ x \not\approx F(x)$$
$$\forall x\ y,\ x \not\approx G(y, x)$$
$$\forall x,\ x \not\approx F(F(x))$$
$$\forall x\ y,\ x \not\approx F(G(y, x))$$
$$\forall x\ y,\ x \not\approx G(y, F(x))$$

$$\forall x, x \not\approx \Gamma[x]$$

$$\forall x\ \bar{y},\ x \not\approx G(y_1, F(F(G(y_2, x))))$$
$$\forall x\ \bar{y},\ x \not\approx G(y_1, F(G(y_2, F(x))))$$
$$\forall x\ \bar{y},\ x \not\approx G(y_1, F(G(y_2, G(y_3, x))))$$
$$\forall x,\ x \not\approx F(F(F(F(x))))$$
$$\forall x\ y,\ x \not\approx F(F(F(G(y, x))))$$

Codatatype fixpoints

$$\exists! x,\ x \approx \Gamma[x]$$

Codatatype fixpoints

$$\exists! x,\ x \approx \Gamma[x]$$

Example

$$s \approx F(G(a, F(s))) \quad \wedge \quad t \approx F(G(a, F(t)))$$

implies

$$s \approx t$$

Solution 1

Conservative extension of the theory

Acyclicity

Extra predicate

$$sub(s, t)$$

"s is a subterm of t"

Recursive definition

$$\forall x, sub(x, x) \qquad \forall xy, sub(x, y) \rightarrow sub(x, F(y))$$

Acyclicity

$$\forall x, \neg sub(F(x), x)$$

Fixpoints

Extra sort

$$\boxed{G}(\bullet, \boxed{E})$$

context = term with hole(s)

Application function

$$app : context \times term \to term$$

Example

$$app(\boxed{G}(\bullet, \boxed{E}), F(E)) \approx G(F(E), E)$$

Existence of fixpoints

Extra function $cyc : context \to term$

$$\forall x, cyc(x) \approx app(x, cyc(x))$$

Existence of fixpoints

Extra function $cyc : context \to term$

$$\forall x, cyc(x) \approx app(x, cyc(x))$$

Example with $x := \boxed{G}(\bullet, \boxed{E})$

$$\begin{aligned} cyc(\boxed{G}(\bullet, \boxed{E})) &\approx app(\boxed{G}(\bullet, \boxed{E}), cyc(\boxed{G}(\bullet, \boxed{E}))) \\ &\approx G(cyc(\boxed{G}(\bullet, \boxed{E})), E) \end{aligned}$$

$cyc(\Gamma)$ **is the solution of** $y \approx \Gamma[y]$

Existence of fixpoints

Extra function $cyc : context \rightarrow term$

$$\forall x, cyc(x) \approx app(x, cyc(x))$$

Example with $x := \boxed{G}(\bullet, \boxed{E})$

$$\begin{aligned} cyc(\boxed{G}(\bullet, \boxed{E})) &\approx app(\boxed{G}(\bullet, \boxed{E}), cyc(\boxed{G}(\bullet, \boxed{E}))) \\ &\approx G(cyc(\boxed{G}(\bullet, \boxed{E})), E) \end{aligned}$$

$cyc(\Gamma)$ is the solution of $y \approx \Gamma[y]$

Uniqueness

$$\forall xy, y \not\approx \bullet \wedge x \approx app(y, x) \rightarrow x \approx cyc(y)$$

Mutually recursive types

$$\begin{aligned}
\text{(co)datatype } \alpha &= E : \alpha \\
&\mid\ F : \beta \to \alpha \\
\text{and } \beta &= G : \alpha \to \beta
\end{aligned}$$

Solution

- Datatypes
  $sub_{\alpha\alpha}$ $sub_{\alpha\beta}$ $sub_{\beta\alpha}$ $sub_{\beta\beta}$
- Codatatypes
  $\substack{\alpha \\ \beta}$-contexts with holes for $\substack{\alpha \\ \beta}$-terms

Completeness

First-order theory

- $\approx$
- No uninterpreted functions

Complete, but not finitely axiomatizable

Conservative extension

Extra symbols

✓ Encode cyclicity properties

✗ Shouldn't be used in conjecture

Conservative extension of the theory

✓ Complete

✓ Easy to implement

But can we improve proof search?

Solution 2

Dedicated inference rules

Chains and cycles

$$a \approx F(b)$$

Chains and cycles

$$a \approx F(b)$$

$$b \approx G(F(c), d)$$

Chains and cycles

$$a \approx F(b)$$

$$b \approx G(F(c), d)$$

$$c \approx F(h(e))$$

Chains and cycles

$$a \approx F(b)$$

$$b \approx G(F(c), d)$$

$$c \approx F(h(e))$$

$$h(x) \approx G(a, e)$$

Chains and cycles

$$a \approx F(b)$$

$$b \approx G(F(c), d)$$

$$c \approx F(h(e))$$

$$h(x) \approx G(a, e)$$

$$a \approx F(G(F(F(G(a, e))), d)$$

under unifier $\{x \leftarrow e\}$

The acyclicity rule

$$\frac{s_1 \approx \Gamma_1[s'_2] \vee C_1 \qquad s_2 \approx \Gamma_2[s'_3] \vee C_2 \qquad \dots \qquad s_n \approx \Gamma_n[s'_1] \vee C_n}{(C_1 \vee C_2 \vee \cdots \vee C_n)\theta}$$

The acyclicity rule

$$\frac{s_1 \approx \Gamma_1[s_2'] \lor C_1 \qquad s_2 \approx \Gamma_2[s_3'] \lor C_2 \qquad \ldots \qquad s_n \approx \Gamma_n[s_1'] \lor C_n}{(C_1 \lor C_2 \lor \cdots \lor C_n)\theta}$$

mgu

$\{s_1 \approx s_1', \ldots, s_n \approx s_n'\}$

The acyclicity rule

maximal literals

$$\frac{\boxed{s_1 \approx \Gamma_1[s_2']} \lor C_1 \qquad \boxed{s_2 \approx \Gamma_2[s_3']} \lor C_2 \qquad \ldots \qquad \boxed{s_n \approx \Gamma_n[s_1']} \lor C_n}{(C_1 \lor C_2 \lor \cdots \lor C_n)\theta}$$

mgu

$\{s_1 \approx s_1', \ldots, s_n \approx s_n'\}$

The acyclicity rule

maximal literals

$$\frac{\boxed{s_1 \approx \Gamma_1[s_2']} \vee C_1 \qquad \boxed{s_2 \approx \Gamma_2[s_3']} \vee C_2 \qquad \ldots \qquad \boxed{s_n \approx \Gamma_n[s_1']} \vee C_n}{(C_1 \vee C_2 \vee \cdots \vee C_n)\theta}$$

orientation of equalities
$s_i \not\succeq \Gamma_i[s_{i+1}]$

mgu
$\{s_1 \approx s_1', \ldots, s_n \approx s_n'\}$

Trouble with the variables

$$\frac{\boxed{t \approx F(x)} \vee p(x)}{???}$$

Trouble with the variables

$$\text{unifier} = \{x \leftarrow t\}$$

$$\frac{t \approx F(x) \lor p(x)}{p(t)}$$

Trouble with the variables

$$\text{unifier} = \{x \leftarrow \Gamma[t]\}$$

$$\frac{t \approx F(x) \lor p(x)}{p(\Gamma[t])}$$

More trouble with the variables

$$\frac{a \approx F(b(0)) \qquad b(x) \approx F(b(x+1)) \qquad b(2) \approx F(a)}{???}$$

More trouble with the variables

$$\frac{a \approx F(b(0)) \qquad b(x) \approx F(b(x+1)) \qquad b(2) \approx F(a)}{\bot}$$

$$b(0) \approx F(b(1)) \qquad b(1) \approx F(b(2))$$

The acyclicity rule (special case)

t is a variable
OR
unifiable with $s_1, \ldots, s_n$

$$\frac{\boxed{s_1 \approx \Gamma_1[s_2']} \lor C_1 \qquad \boxed{s_2 \approx \Gamma_2[s_3']} \lor C_2 \qquad \ldots \qquad \boxed{s_n \approx \Gamma_n[t]} \lor C_n}{(\neg sub(s_1, t) \lor C_1 \lor C_2 \lor \cdots \lor C_n)\theta}$$

Axioms for *sub* are included in the clauses to saturate

$$\dfrac{\dfrac{\dfrac{t \approx F(x) \vee p(x)}{\neg sub(t, x) \vee p(x)} \qquad sub(y, F(z)) \vee \neg sub(y, z)}{\neg sub(t, z) \vee p(F(z))} \qquad sub(x, x)}{p(F(z))}$$

hypothesis

$$\dfrac{\dfrac{\dfrac{t \approx F(x) \lor p(x)}{\neg sub(t, x) \lor p(x)} \qquad sub(y, F(z)) \lor \neg sub(y, z)}{\neg sub(t, z) \lor p(F(z))} \qquad sub(x, x)}{p(F(z))}$$

hypothesis

acyclicity

$$\dfrac{\dfrac{\dfrac{t \approx F(x) \lor p(x)}{\neg sub(t, x) \lor p(x)} \qquad sub(y, F(z)) \lor \neg sub(y, z)}{\neg sub(t, z) \lor p(F(z))} \qquad sub(x, x)}{p(F(z))}$$

hypothesis

acyclicity

axioms

$$\dfrac{\dfrac{\dfrac{t \approx F(x) \lor p(x)}{\neg sub(t, x) \lor p(x)} \qquad sub(y, F(z)) \lor \neg sub(y, z)}{\neg sub(t, z) \lor p(F(z))} \qquad sub(x, x)}{p(F(z))}$$

hypothesis

acyclicity

axioms

$$\dfrac{\dfrac{\dfrac{t \approx F(x) \lor p(x)}{\neg sub(t, x) \lor p(x)} \qquad sub(y, F(z)) \lor \neg sub(y, z)}{\neg sub(t, z) \lor p(F(z))} \qquad sub(x, x)}{p(F(z))}$$

Codatatype fixpoints

Existence

- Function *cyc* and its axiom

Uniqueness

- Rule based on chains (shown here simplified)

$$\frac{s_1 \approx \Gamma_1[s_2'] \lor C_1 \qquad s_2 \approx \Gamma_2[s_3'] \lor C_2 \qquad \dots \qquad s_n \approx \Gamma_n[t] \lor C_n}{(x \not\approx \Gamma[t] \lor x \approx s_1 \lor C_1 \lor C_2 \lor \cdots \lor C_n)\theta}$$

fresh variable $\qquad \Gamma = \Gamma_1[\Gamma_2[\dots\Gamma_n\dots]]$

Not shown: extra conditions about occurences of s_1 in Γ

Relaxing the superposition rule

$$F(t) \approx s$$

Superposition can rewrite s even if $F(t) \succ s$

Effect on rewrite system

$$F(t') \to s'$$

irreducible

Effect on proof search

- ✗ More applications of superposition
- ✓ Can be mitigated with good term ordering

Replacing the remaining axioms

Distinctness rules

$$\frac{F(\bar{s}) \approx G(\bar{t}) \vee C}{C} \qquad \frac{F(\bar{s}) \approx x \vee C}{C[x \leftarrow G(\bar{y})]}$$

$$\frac{F(\bar{s}) \approx u \vee C_1 \qquad G(\bar{t}) \approx u' \vee C_2}{(C_1 \vee C_2)\sigma}$$

- $\sigma = mgu(u, u')$
- Similar rules for injectivity
- Exhaustivity still requires axiom

Implementation

Both approaches implemented in **Vampire**

Challenges

- *n*-ary rules
- mgu over set of equations

Indexing technique

- Re-use existing indexes for retrieval of unifiable terms
- Build chains and mgu incrementally

Benchmarks

Isabelle problems

- 4130 problems translated by Sledgehammer
- Almost no difference between configurations
- Nothing lost vs partial axiomatization
- Acyclicity & fixpoints rarely used here

Synthetic problems

- 500 problems
- Focus on acyclicity & fixpoints

Synthetic problems

	AC ground	AC $\forall$	U ground	U $\forall$	EX
Axioms	100%	65%	10%	14%	40%
Rules	100%	82%	13%	14%	35%

Synthetic problems

$$\exists x,\, x \approx \Gamma[x]$$

	AC ground	AC $\forall$	U ground	U $\forall$	EX
Axioms	100%	65%	10%	14%	40%
Rules	100%	82%	13%	14%	35%

Synthetic problems

$$\exists xy,\, x \approx \Gamma[x] \land y \approx \Gamma[y] \land x \not\approx y$$

	AC ground	AC ∀	U ground	U ∀	EX
Axioms	100%	65%	10%	14%	40%
Rules	100%	82%	13%	14%	35%

Synthetic problems

$$\forall x, x \not\approx \Gamma[x]$$

	AC ground	AC $\forall$	U ground	U $\forall$	EX
Axioms	100%	65%	10%	14%	40%
Rules	100%	82%	13%	14%	35%

Synthetic problems

	AC ground	AC $\forall$	U ground	U $\forall$	EX
Axioms	100%	65%	10%	14%	40%
Rules	100%	82%	13%	14%	35%
Z3	100%	59%			
CVC4	100%	100%	100%	12%	0%

Induction and co-induction

First-order theory

- Complete without (co)induction
- $\left.\begin{array}{r}\text{Acyclicity}\\ \text{Fp uniqueness}\end{array}\right\}$ is a special case of $\left\{\begin{array}{l}\text{induction}\\ \text{co-induction}\end{array}\right.$

Summary

Two solutions

1. Conservative extension of the theory
2. Inference rules + axioms

- ✓ Complete (with restriction for unicity rule)
- ✓ Efficient acyclicity rule
- ✓ Implementation in Vampire

`http://github.com/vprover`

Conservative extension: acyclicity

Sub

$$sub(x, x)$$

$$sub(x, y) \rightarrow sub(x, F(\bar{z}, y, \bar{z}'))$$

Acyclicity

$$\neg sub(F(\bar{y}, x, \bar{y}'), x)$$

Conservative extension: fixpoints

App

$$app(cst(x), y) \approx x \qquad\qquad app(\bullet, x) \approx x$$

$$app(\boxed{F}(\bar{x}), y) \approx F(\overline{app(x_i, y)})$$

Hole

$$\bullet \not\approx cst(x) \qquad\qquad \bullet \not\approx \boxed{F}(\bar{x})$$

Existence & uniqueness

$$cyc(x) \approx app(x, cyc(x))$$

$$x \not\approx \bullet \land y \approx app(x, y) \rightarrow y \approx cyc(x)$$