ETH zürich

Conditional Parametricity in Isabelle/HOL

Jan Gilcher, Andreas Lochbihler, Dmitriy Traytel
Institute of Information Security, Department of Computer Science, ETH Zurich

Relational parametricity

Informal definition: parametric ≈ "truly" polymorphic

Parametric functions, whose type contains type variables, behave exactly the same, no matter what concrete type they are actually used with at run-time.

Examples and non-examples

function	parametric in α	β	reason
$(\cdot) :: \alpha \to \alpha\ \mathsf{list} \to \alpha\ \mathsf{list}$	✓	–	
$\mathsf{length} :: \alpha\ \mathsf{list} \to \mathbb{N}$	✓	–	
$\mathsf{map} :: (\alpha \to \beta) \to \alpha\ \mathsf{list} \to \beta\ \mathsf{list}$	✓	✓	
$(=) :: \alpha \to \alpha \to \mathbb{B}$	✗	–	constant iff $\lvert\alpha\rvert = 1$
$\mathsf{head} :: \alpha\ \mathsf{list} \to \alpha$	✗	–	head [] under-specified
$\mathsf{lookup} :: (\alpha \times \beta)\ \mathsf{list} \to \alpha \to \beta\ \mathsf{option}$	✗	✓	needs $(=)$ on α

Applications in Isabelle/HOL

- data refinement [Lammich, ITP'13]
- theorem transfer across subtypes and quotients [Huffman, Kunčar, CPP'13]
- productivity of non-primitively corecursive definitions [Blanchette, Bouzy, Lochbihler, Popescu, Traytel, ICFP'15, ESOP'17]
- nonuniform (co)datatypes [Blanchette, Meier, Popescu, Traytel, LICS'17]

Formal definition and examples

Types as relations, type constructors as relators

($\alpha \otimes \beta$ denotes the type of binary relations between α and β.)

function space:
related inputs are mapped to related outputs
$\Rightarrow :: \alpha \otimes \alpha' \to \beta \otimes \beta' \to (\alpha \to \beta) \otimes (\alpha' \to \beta')$
$f\ (R \Rightarrow S)\ g$ iff $\forall x\ y.\ x\ R\ y \longrightarrow (f\ x)\ S\ (g\ y)$

$$\begin{array}{ccc} x & \text{---}\ R\ \text{---} & y \\ \downarrow & & \downarrow \\ f\ x & \cdots\ S\ \cdots & g\ y \end{array} \quad (f\ (R \Rightarrow S)\ g)$$

list: same length and position-wise related elements
$\mathsf{rel}_{\mathsf{list}} :: \alpha \otimes \alpha' \to \alpha\ \mathsf{rel}_{\mathsf{list}} \otimes \alpha'\ \mathsf{rel}_{\mathsf{list}}$
$xs\ (\mathsf{rel}_{\mathsf{list}}\ R)\ ys$ iff $\lvert xs\rvert = \lvert ys\rvert \wedge \forall i \le \lvert xs\rvert.\ xs_{[i]}\ R\ ys_{[i]}$

$$\mathsf{rel}_{\mathsf{list}}\ R \quad \begin{array}{cccc} [\ x_1, & x_2, & \ldots, & x_n\ ] \\ R & R & \ldots & R \\ [\ y_1, & y_2, & \ldots, & y_n\ ] \end{array}$$

any "well-behaved" type constructor $\overline{\alpha}\ \mathsf{T}$:
relator requires same T-shape and position-wise related elements
$\mathsf{rel}_{\mathsf{T}} :: \alpha_1 \otimes \alpha_1' \to \cdots \to \alpha_n \otimes \alpha_n' \to \overline{\alpha}\ \mathsf{rel}_{\mathsf{T}} \otimes \overline{\alpha'}\ \mathsf{rel}_{\mathsf{T}}$

(Conditional) Parametricity

$c :: \overline{\alpha}\ \mathsf{T}$ is *parametric* iff $(c :: \overline{\alpha}\ \mathsf{T})\ (\mathsf{rel}_{\mathsf{T}}\ R_1\ \cdots\ R_n)\ (c :: \overline{\alpha'}\ \mathsf{T})$ for all $\overline{R}$
c is *C-parametric* if the same property holds for those $\overline{R}$ that satisfy $C\ \overline{R}$

Examples

$(\cdot) :: \alpha \to \alpha\ \mathsf{list} \to \alpha\ \mathsf{list}$
$(\cdot)\ (R \Rightarrow \mathsf{rel}_{\mathsf{list}}\ R \Rightarrow \mathsf{rel}_{\mathsf{list}}\ R)\ (\cdot)$

$\mathsf{length} :: \alpha\ \mathsf{list} \to \mathbb{N}$
$\mathsf{length}\ (\mathsf{rel}_{\mathsf{list}}\ R \Rightarrow \mathsf{rel}_{\mathbb{N}})\ \mathsf{length}$

$\mathsf{map} :: (\alpha \to \beta) \to \alpha\ \mathsf{list} \to \beta\ \mathsf{list}$
$\mathsf{map}\ ((R \Rightarrow S) \Rightarrow \mathsf{rel}_{\mathsf{list}}\ R \Rightarrow \mathsf{rel}_{\mathsf{list}}\ S)\ \mathsf{map}$

$\mathsf{refl} :: (\alpha \to \alpha \to \mathbb{B}) \to \mathbb{B}$
$\mathsf{refl}\ r = (\forall x.\ r\ x\ x)$

bi-totality

$$\frac{(\forall)\ ((R \Rightarrow \mathsf{rel}_{\mathbb{B}}) \Rightarrow \mathsf{rel}_{\mathbb{B}})\ (\forall)}{\mathsf{refl}\ ((R \Rightarrow R \Rightarrow \mathsf{rel}_{\mathbb{B}}) \Rightarrow \mathsf{rel}_{\mathbb{B}})\ \mathsf{refl}}$$

$\mathsf{del} :: \alpha \to \alpha\ \mathsf{list} \to \alpha\ \mathsf{list}$
$\mathsf{del}\ x\ [] = []$
$\mathsf{del}\ x\ (y \cdot ys) =$
$\quad (\mathsf{if}\ x = y\ \mathsf{then}\ \mathsf{del}\ x\ ys\ \mathsf{else}\ y \cdot \mathsf{del}\ x\ ys)$

bi-uniqueness

$$\frac{(=)\ (R \Rightarrow R \Rightarrow \mathsf{rel}_{\mathbb{B}})\ (=)}{\mathsf{del}\ (R \Rightarrow \mathsf{rel}_{\mathsf{list}}\ R \Rightarrow \mathsf{rel}_{\mathsf{list}} R)\ \mathsf{del}}$$

$\mathsf{sum} :: \mathsf{Monoid}\ \alpha \Rrightarrow \alpha\ \mathsf{list} \to \alpha$
$\mathsf{sum}\ [] = 0$
$\mathsf{sum}\ (x \cdot xs) = x + \mathsf{sum}\ xs$

respectfulness

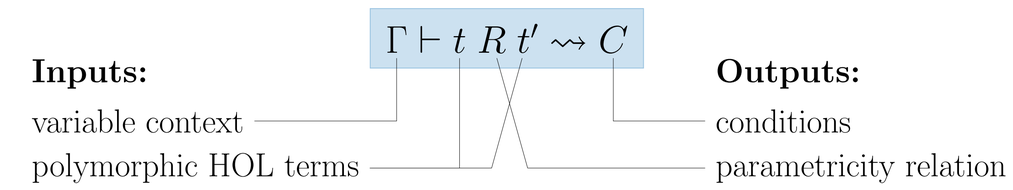
$$\frac{0\ R\ 0 \qquad (+)\ (R \Rightarrow R \Rightarrow R)\ (+)}{\mathsf{sum}\ (\mathsf{rel}_{\mathsf{list}}\ R \Rightarrow R)\ \mathsf{sum}}$$

Parametricity inference for definition $c \equiv t$

1. Infer parametricity relation $?R$ and conditions $?C$

$$\vdash t\ ?R\ t' \rightsquigarrow ?C$$

where t' is t with all type variables α replaced by unification variables $?\alpha$, using a database $\mathsf{DB}_{\mathrm{param}}$ of parametricity theorems for constants in t.



$$\frac{\Gamma, x\ R\ y \vdash t\ S\ (t'\ y) \rightsquigarrow C}{\Gamma \vdash (\lambda x :: \beta.\ t)\ (R \Rightarrow S)\ t' \rightsquigarrow C}\ y \text{ fresh}$$

$$\frac{C \Longrightarrow c\ (S_1 \Rightarrow \ldots \Rightarrow S_n \Rightarrow R)\ c' \in \mathsf{DB}_{\mathrm{param}} \qquad \forall i \le n.\ \Gamma \vdash t_i\ S_i\ t_i' \rightsquigarrow C_i}{\Gamma \vdash (c\ t_1 \ldots t_n)\ R\ (c'\ t_1' \ldots t_n') \rightsquigarrow C \wedge C_1 \wedge \ldots \wedge C_n}$$

$$\frac{x\ (S_1 \Rightarrow \ldots \Rightarrow S_n \Rightarrow R)\ x' \in \Gamma \qquad \forall i \le n.\ \Gamma \vdash t_i\ S_i\ t_i' \rightsquigarrow C_i}{\Gamma \vdash (x\ t_1 \ldots t_n)\ R\ (x'\ t_1' \ldots t_n') \rightsquigarrow C_1 \wedge \ldots \wedge C_n}$$

2. Simplify inferred conditions C by
   - removing duplicates and
   - applying rules for type constructors

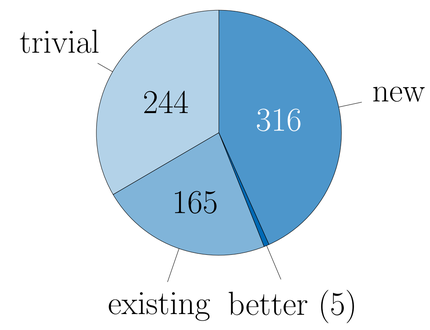
$$\frac{(=)\ (R \Rightarrow R \Rightarrow \mathsf{rel}_{\mathbb{B}})\ (=)}{(=)\ (\mathsf{rel}_{\mathsf{list}}\ R \Rightarrow \mathsf{rel}_{\mathsf{list}}\ R \Rightarrow \mathsf{rel}_{\mathbb{B}})\ (=)}$$

3. Enter parametricity theorem $C \Longrightarrow c\ R\ c'$ in database $\mathsf{DB}_{\mathrm{param}}$

Evaluation

Inferred parametricity for 730 non-recursive and primitively recursive polymorphic definitions in the Isabelle/HOL standard library using the existing database $\mathsf{DB}_{\mathrm{param}}$ of parametricity theorems.

trivial	inferred theorem is $c = c$
existing	rediscovered previously proven theorem
better	inferred theorem has **fewer** conditions than existing one
new	definition without existing parametricity theorem



Comparison with other parametricity provers

```
parametric_constant sum_def — ‹Our tool›

lemma — ‹transfer_prover (Huffman, Kunčar)›
  includes lifting_syntax
  assumes [transfer_rule]:
    ‹R 0 0› ‹(R ===> R ===> R) (op +) (op +)›
  shows ‹(list_all2 R ===> R) sum sum›
unfolding sum_def by transfer_prover

lemma — ‹Autoref (Lammich)›
  assumes ‹(0, 0) ∈ R› ‹(op +, op +) ∈ R → R → R›
  shows ‹(sum, sum) ∈ ⟨R⟩list_rel → R›
using assms unfolding sum_def by parametricity
```