"Theorems for free": a (calculational) introduction

J.N. Oliveira

Dept. Informática,
Universidade do Minho
Braga, Portugal

2003

Parametric polymorphism: why?

- Less code (**specific** solution = **generic** solution + **customization**)
- Intellectual reward
- Last but not
  least, quotation (from *Theorems for free!*, by Philip Wadler [4]):

  > *From the type of a polymorphic function we can derive a theorem that is satisfies.* (...) *How useful are the theorems so generated? Only time and experience will tell* (...)

- No doubt: free theorems are **very** useful!

Polymorphic type signatures

Polymorphic function signature:

$$f \quad : \quad t$$

where t is a functional type, according to the following "grammar" of types:

$$\begin{array}{lcll} t & ::= & t' \leftarrow t'' & \\ t & ::= & \mathsf{F}(t_1, \ldots, t_n) & \\ t & ::= & v & \text{type } \textit{variables } v\text{, cf. } \textit{polymorphism} \end{array}$$

What does it mean that f is **parametrically** polymorphic?

Free theorem of type t

Let

- V be the set of type variables involved in type t
- $\{R_v\}_{v \in V}$ be a V-indexed family of relations (f_v in case all such R_v are functions).
- R_t be a relation defined inductively as follows:

$$R_{t:=\mathsf{F}(t_1,\ldots,t_n)} = \mathsf{F}(R_{t_1}, \ldots, R_{t_n}) \quad (1)$$

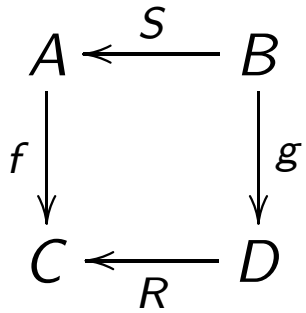
$$R_{t:=v} = R_v \quad (2)$$

$$R_{t:=t' \leftarrow t''} = R_{t'} \leftarrow R_{t''} \quad (3)$$

- What kind of relation is $R_{t'} \leftarrow R_{t''}$?

"Reynolds arrow" operator

$$f(R \leftarrow S)g \quad \equiv \quad f \cdot S \subseteq R \cdot g$$



That is to say,

$$\frac{\begin{array}{c} A \xleftarrow{S} B \\ C \xleftarrow{R} D \end{array}}{C^A \xleftarrow{R \leftarrow S} D^B}$$

For instance, $f(id \leftarrow id)g \quad \equiv \quad f = g$ that is, $id \leftarrow id \quad = \quad id$

Free theorem (FT) of type t

The following (remarkable) theorem — due to J. Reynolds [3], advertised by P. Wadler [4] and re-written by Backhouse [1] — holds:

> *Given any function $\theta : t$, and V as above, then $\theta\ R_t\ \theta$ holds, for any relational instantiation of type variables in V.*

Note that this theorem

- is a result about t
- holds **independently** of the actual definition of θ.
- holds about any function of type t

First example (*invl*)

- The target function: $\theta = invl : a^\star \leftarrow a^\star$.
- Calculation of $R_{t=a^\star \leftarrow a^\star}$:

$$
\begin{array}{ll}
 & R_{a^\star \leftarrow a^\star} \\
\equiv & \quad \{ \text{ rule } \quad R_{t=t' \leftarrow t''} \quad = \quad R_{t'} \leftarrow R_{t''} \quad \} \\
 & R_{a^\star} \leftarrow R_{a^\star} \\
\equiv & \quad \{ \text{ rule } \quad R_{t=\mathsf{F}(t_1,\ldots,t_n)} \quad = \quad \mathsf{F}(R_{t_1},\ldots,R_{t_n}) \quad \} \\
 & R_a{}^\star \leftarrow R_a{}^\star
\end{array}
$$

where

$$l \; R^\star l' \stackrel{\text{def}}{=} length \; l = length \; l' \wedge \langle \forall \; i \; : \; i \in inds \; l : \; (l \; i) R (l' \; i) \rangle$$

Calculation of FT follows.

First example (*invl*)

The FT itself will predict (R_a abbreviated to R):

$$
\begin{array}{ll}
 & invl(R^\star \leftarrow R^\star)invl \\
\equiv & \quad \{ \text{ definition } \quad f(R \leftarrow S)g \quad \equiv \quad f \cdot S \subseteq R \cdot g \quad \} \\
 & invl \cdot R^\star \subseteq R^\star \cdot invl
\end{array}
$$

In case R is a function r, the FT theorem boils down to *invl*'s **natural** property:

$$invl \cdot r^\star \;=\; r^\star \cdot invl$$

that is,

$$invl[\; r\;\; a \mid a \leftarrow l\;] \;=\; [\; r\;\; b \mid b \leftarrow invl\;\; l\;]$$

First example (*invl*)

Further calculation (back to R):

$$
\begin{array}{ll}
 & invl \cdot R^\star \subseteq R^\star \cdot invl \\
\equiv & \quad \{ \text{ shunting rule (9) } \} \\
 & R^\star \subseteq invl^\circ \cdot R^\star \cdot invl \\
\equiv & \quad \{ \text{ going pointwise } \} \\
 & \langle \forall\ l, r\ ::\ l\ R^\star r \Rightarrow (invl\ l) R^\star (invl\ r) \rangle
\end{array}
$$

An instance of this pointwise version of *invl*-FT will state that, for example, *invl* will respect element-wise orderings ($R := <$):

First example (*invl*)

$$\mathit{length}\ l = \mathit{length}\ l' \wedge \langle \forall\ i\ :\ i \in \mathit{inds}\ l :\ (l\ i) < (r\ i) \rangle$$
$$\Downarrow$$
$$\mathit{length}(\mathit{invl}\ l) = \mathit{length}(\mathit{inv}\ l')$$
$$\wedge$$
$$\langle \forall\ j\ :\ j \in \mathit{inds}\ l :\ (\mathit{invl}\ l)j < (\mathit{invl}\ r)j \rangle$$

(Guess other instances.)

Our next example calculates the FT of

$$\mathit{sort} : a^\star \leftarrow a^\star \leftarrow (\mathit{bool} \leftarrow (a \times a))$$

(the first parameter stands for the chosen ordering relation)

Second example: FT of *sort*

$$sort(R_{(a^\star \leftarrow a^\star) \leftarrow (bool \leftarrow (a \times a))})sort$$

$\equiv$ { (1, 2, 3) ; $R_{t:=bool} = id$ (cf. constant relator) }

$$sort((R^\star \leftarrow R^\star) \leftarrow (id \leftarrow (R \times R)))sort$$

$\equiv$ { (4) }

$$sort \cdot (id \leftarrow (R \times R)) \quad \subseteq \quad (R^\star \leftarrow R^\star) \cdot sort$$

$\equiv$ { shunting (9) }

$$(id \leftarrow (R \times R)) \quad \subseteq \quad sort^\circ \cdot (R^\star \leftarrow R^\star) \cdot sort$$

$\equiv$ { introduce variables f and g }

$$f(id \leftarrow (R \times R))g \quad \Rightarrow \quad (sort\ f)(R^\star \leftarrow R^\star)(sort\ g)$$

$\equiv$ { (1, 3, 4) }

$$f \cdot (R \times R) \subseteq g \quad \Rightarrow \quad (sort\ f) \cdot R^\star \subseteq R^\star \cdot (sort\ g)$$

Second example: FT of *sort*

Case $R := r$:

$$f \cdot (r \times r) = g \quad \Rightarrow \quad (sort\ f) \cdot r^\star = r^\star \cdot (sort\ g)$$

$$\equiv \qquad \{\ \text{introduce variables}\ \}$$

$$\langle \forall\ a, b\ ::\ f(r\ a, r\ b) = g(a, b) \rangle \quad \Rightarrow \quad \langle \forall\ l\ ::\ (sort\ f)(r^\star\ l) = r^\star(sort$$

Denoting predicates f, g by infix orderings $\leq, \preceq$:

$$\langle \forall\ a, b\ ::\ r\ a \leq r\ b \equiv a \preceq b \rangle \quad \Rightarrow \quad \langle \forall\ l\ ::\ sort\ (\leq)(r^\star\ l) = r^\star(sort\ (\preceq)\ l) \rangle$$

That is, for r monotonic and injective,

$$sort\ (\leq)\ [\ r\ a \mid a \leftarrow l\ ]$$

is always the same list a

$$[\ r\ a \mid a \leftarrow sort\ (\preceq)\ l\ ]$$

Second example: FT of $(\!|\_|\!)$

- $(\!|\_|\!)$ has generic type

$$(\!|\_|\!) : b \leftarrow \mathsf{F}\, a \leftarrow (b \leftarrow \mathsf{B}\,(a, b))$$

  where $\mathsf{F}\, a \cong \mathsf{B}\,(a, \mathsf{F}\, a)$.

- $(\!|\_|\!)$-FT:

$$(\!|\_|\!) \cdot (R_b \leftarrow \mathsf{B}\,(R_a, R_b)) \quad \subseteq \quad (R_b \leftarrow \mathsf{F}\, R_a) \cdot (\!|\_|\!)$$

- $(\!|\_|\!)$-FT calculation follows (R_a, R_b abbreviated to R, S):

$(\!|\_|\!)$-FT corollaries

$$
\begin{array}{lll}
 & (\!|\_|\!) \cdot (S \leftarrow \mathsf{B}\,(R,S)) & \subseteq \quad (S \leftarrow \mathsf{F}\,R) \cdot (\!|\_|\!) \\
\equiv & \quad \{ \text{ definition } \quad f(R \leftarrow S)g \quad \equiv \quad f \cdot S \subseteq R \cdot g \quad \} & \\
 & f(S \leftarrow \mathsf{B}\,(R,S))g \quad \Rightarrow \quad (\!|f|\!)(S \leftarrow \mathsf{F}\,R)(\!|g|\!) & \\
\equiv & \quad \{ \text{ idem } \} & \\
 & f \cdot \mathsf{B}\,(R,S) \subseteq S \cdot g \quad \Rightarrow \quad (\!|f|\!) \cdot \mathsf{F}\,R \subseteq S \cdot (\!|g|\!) &
\end{array}
$$

At this point, we can infer ...

$(\!|\_|\!)$-FT corollaries

From this, infer

- $(\!|\_|\!)$-*fusion* $(R, S := id, s)$:

$$(f \cdot \mathsf{B}\,(id, s) = s \cdot g) \quad \Rightarrow \quad (\!|f|\!) = s \cdot (\!|g|\!)$$

- $(\!|\_|\!)$-*absorption* $(R, S := r, id)$:

$$(f \cdot \mathsf{B}\,(r, id) = g) \quad \Rightarrow \quad (\!|f|\!) \cdot \mathsf{F}\,r = (\!|g|\!)$$

$$\equiv \qquad \{ \text{ replacement of } g \ \}$$

$$(\!|f|\!) \cdot \mathsf{F}\,r = (\!|f \cdot \mathsf{B}\,(r, id)|\!)$$

Background: relators

Relators [2] have to do with parametric datatyping: a parametric datatype G is said to be a relator wherever, given a relation from A to B, $\mathsf{G}\,R$ extends R to G-structures: it is a relation from $\mathsf{G}\,A$ to $\mathsf{G}\,B$

$$\begin{array}{ccc} A & \cdots\cdots & \mathsf{G}\,A \\ {\scriptstyle R}\downarrow & & \downarrow{\scriptstyle \mathsf{G}\,R} \\ B & \cdots\cdots & \mathsf{G}\,B \end{array} \tag{4}$$

which obeys the following properties:

$$\mathsf{G}\,id = id \tag{5}$$

$$\mathsf{G}\,(R \cdot S) = (\mathsf{G}\,R) \cdot (\mathsf{G}\,S) \tag{6}$$

$$\mathsf{G}\,(R^\circ) = (\mathsf{G}\,R)^\circ \tag{7}$$

and is monotonic:

$$R \subseteq S \;\Rightarrow\; \mathsf{G}\,R \subseteq \mathsf{G}\,S \tag{8}$$

Background

- Shunting rules:

$$f \cdot R \subseteq S \quad \equiv \quad R \subseteq f^{\circ} \cdot S \tag{9}$$

$$R \cdot f^{\circ} \subseteq S \quad \equiv \quad R \subseteq S \cdot f \tag{10}$$


K. Backhouse and R.C. Backhouse.
Safety of abstract interpretations for free, via logical relations and Galois connections.
SCP, 15(1–2):153–196, 2004.


R.C. Backhouse, P. de Bruin, P. Hoogendijk, G. Malcolm, T.S. Voermans, and J. van der Woude.
Polynomial relators.
In *AMAST'91*, Workshops in Computing, pages 303–362. Springer, 1992.


J.C. Reynolds.
Types, abstraction and parametric polymorphism.
Information Processing 83, pages 513–523, 1983.


P.L. Wadler.
Theorems for free!
In *4th International Symposium on Functional Programming Languages and Computer Architecture*, London, Sep. 1989. ACM.