Hierarchical Reflection

Luís Cruz-Filipe[1,2] and Freek Wiedijk[1]

Brouwer Seminar

February 16, 2004

[1]University of Nijmegen, The Netherlands

[2]Centro de Lógica e Computação, Portugal

From 1.9.2004 *the University of Nijmegen will be called Radboud University of Nijmegen*

Hierarchical Reflection

1. Motivation
2. (Partial) Reflection
3. Normalization Function
4. Uninterpreted Function Symbols
5. Hierarchical Reflection
6. Tighter Integration
7. Conclusions

Equational Reasoning via (Partial) Reflection

Syntactic expressions: $E ::= \mathbb{Z} \mid \mathbb{V} \mid E + E \mid E \cdot E \mid E/E$

Normalization function: $\mathcal{N} : E \;\rightarrow\; E$

Interpretation *relation*: $]\!]_\rho \subseteq E \times A$

1. well defined: $e \;]\!]_\rho\, a \;\wedge\; e \;]\!]_\rho\, b \;\Rightarrow\; a =_A b$

2. $\mathcal{N}$ is correct: $e \;]\!]_\rho\, a \;\Rightarrow\; \mathcal{N}(e) \;]\!]_\rho\, a$

Equational Reasoning via Partial Reflection (tactic)

1. $e \;]\![_\rho\, a \;\wedge\; e \;]\![_\rho\, b \;\Rightarrow\; a =_A b$

2. $e \;]\![_\rho\, a \;\Rightarrow\; \mathcal{N}(e) \;]\![_\rho\, a$

$$\begin{tikzcd}
e \in E \arrow[rr, "\mathcal{N}"] & & \mathcal{N}(e) = \mathcal{N}(f) \arrow[ddl, "]\![_\rho"] \arrow[ddr, "]\![_\rho"'] & & f \in E \arrow[ll, "\mathcal{N}"'] \\
& (2) & (1) & (2) & \\
& a \in A \arrow[uul, dashed] \arrow[rr, leftrightarrow, "=_A"] & & b \in A \arrow[uur, dashed] &
\end{tikzcd}$$

1'. $e \;]\![_\rho\, a \;\wedge\; e = 0/e' \;\Rightarrow\; a =_A 0$

Normalization Function

$$\begin{array}{rcl} F & ::= & P/P \\ P & ::= & M + P \mid \mathbb{Z} \\ M & ::= & \mathbb{V} \cdot M \mid \mathbb{Z} \end{array}$$

M are “lists of variables” ($\cdot$ is “cons”, integers are “nil”)

P are “lists of monomials” ($+$ is “cons”, integers are “nil”)

Normal forms are formal “quotients of sorted lists” without duplication:

$$\mathcal{N}\left(\frac{1}{x-y}+\frac{1}{x+y}\right)=\frac{x\cdot 2+0}{x\cdot x\cdot 1+y\cdot y\cdot(-1)+0}$$

Normalization Function (definition)

Recursively defined functions

$$\begin{array}{lclclcl}
- \cdot_{M\mathbb{Z}} - & : & M & \times & \mathbb{Z} & \to & M \\
- \cdot_{M\mathbb{V}} - & : & M & \times & \mathbb{V} & \to & M \\
- \cdot_{MM} - & : & M & \times & M & \to & M \\
- +_{MM} - & : & M & \times & M & \to & M \\
- +_{PM} - & : & P & \times & M & \to & P \\
- +_{PP} - & : & P & \times & P & \to & P \\
- \cdot_{PM} - & : & P & \times & M & \to & P \\
- \cdot_{PP} - & : & P & \times & P & \to & P \\
- +_{FF} - & : & F & \times & F & \to & F \\
- \cdot_{FF} - & : & F & \times & F & \to & F \\
- /_{FF} - & : & F & \times & F & \to & F
\end{array}$$

Normalization Function (examples)

$$e \cdot_{MM} f := \begin{cases} (e_2 \cdot_{MM} f) \cdot_{MV} e_1 & \text{if } e = e_1 \cdot e_2 \\ f \cdot_{M\mathbb{Z}} i & \text{if } e = i \in \mathbb{Z} \end{cases}$$

$$e +_{PM} f := \begin{cases} j +_{MM} i & \text{if } e = j \in \mathbb{Z},\ f = i \in \mathbb{Z} \\ f + i & \text{if } e = i \in \mathbb{Z} \\ e_1 + (e_2 +_{PM} i) & \text{if } e = e_1 + e_2,\ f = i \in \mathbb{Z} \\ e_2 +_{PM} (e_1 +_{MM} f) & \text{if } e = e_1 + e_2,\ e_1 =_M f \\ e_1 + (e_2 +_{PM} f) & \text{if } e = e_1 + e_2,\ e_1 <_{\text{lex}} f \\ f + e & \text{if } e = e_1 + e_2,\ e_1 >_{\text{lex}} f \end{cases}$$

$$\mathcal{N}(e/f) := N(e) \,/_{FF} N(f)$$

$$\mathcal{N}(v) := \frac{v \cdot 1 + 0}{1}$$

Uninterpreted Function Symbols

Goal: $f(a+b) = f(b+a)$

$$f(a+b) \rightsquigarrow x,\ f(b+a) \rightsquigarrow y,\ \mathcal{N}(x-y) = \frac{x \cdot 1 + y \cdot (-1) + 0}{1}$$

Solution: extend E with $\mathbb{V}_1 : E \to E$

$$E \quad ::= \quad \mathbb{Z} \mid \mathbb{V}_0 \mid \mathbb{V}_1(E) \mid E+E \mid E \cdot E \mid E/E$$

Normal forms:

$$\begin{array}{rcl} F & ::= & P/P \\ P & ::= & M + P \mid \mathbb{Z} \\ M & ::= & \mathbb{V}_0 \cdot M \mid \mathbb{V}_1(F) \cdot M \mid \mathbb{Z} \end{array}$$

ordered. . .

Uninterpreted Function Symbols (order)

Ordering on E (assumes $<_{\mathbb{V}_0}$ on $\mathbb{V}_0$ and $<_{\mathbb{V}_1}$ on $\mathbb{V}_1$):

$$x <_E i <_E e + f <_E e \cdot f <_E e/f <_E v(e)$$

Expressions with the same operator are sorted lexicographically.

Example (with $x <_{\mathbb{V}_0} y$ and $u <_{\mathbb{V}_1} v$):

$$x <_E y <_E 34 <_E x/4 <_E u(x+3) <_E u(2 \cdot y) <_E v(x+3)$$

Same normalization function with added rule

$$\mathcal{N}(v(e)) := \frac{v(\mathcal{N}(e)) \cdot 1 + 0}{1}$$

Uninterpreted Function Symbols (valuations)

Two valuations $\rho_0 : \mathbb{V}_0 \to A$ and $\rho_1 : \mathbb{V}_1 \to (A \to A)$

Once again, one can prove

$$e \rrbracket_{\rho_0,\rho_1} a \;\wedge\; e \rrbracket_{\rho_0,\rho_1} b \;\Rightarrow\; a =_A b$$
$$e \rrbracket_{\rho_0,\rho_1} a \;\Rightarrow\; \mathcal{N}(e) \rrbracket_{\rho_0,\rho_1} a$$

Goal: $f(a+b) = f(b+a)$

$$f \rightsquigarrow v,\; a \rightsquigarrow x,\; b \rightsquigarrow y$$

$$\mathcal{N}(v(x+y)) = \mathcal{N}(v(y+x)) = \frac{v\left(\frac{x\cdot 1 + y\cdot 1 + 0}{1}\right)\cdot 1 + 0}{1}$$

Binary functions, partial functions similarly treated.

Hierarchical Reflection

Similar procedures for other structures?

$$\begin{tikzcd}
E_F \arrow[r, "\rrbracket\llbracket^{F}_{\rho}"] & F : \text{Field} \arrow[d] \\
E_R \arrow[u, "\subseteq"] \arrow[r, "\rrbracket\llbracket^{R}_{\rho}"] & R : \text{Ring} \arrow[d] \\
E_G \arrow[u, "\subseteq"] \arrow[r, "\rrbracket\llbracket^{G}_{\rho}"] & G : \text{Group}
\end{tikzcd}$$

but better is

$$\begin{tikzcd}
 & F : \text{Field} \arrow[d] \\
E \arrow[ur, "\rrbracket\llbracket^{F}_{\rho}"] \arrow[r, "\rrbracket\llbracket^{R}_{\rho}"] \arrow[dr, "\rrbracket\llbracket^{G}_{\rho}"'] & R : \text{Ring} \arrow[d] \\
 & G : \text{Group}
\end{tikzcd}$$

making use of the *partiality* of the interpretation

Hierarchical Reflection (interpretation relations)

But. . .

If $\rho(x) = a$, then $a + a$ is represented by $x + x$, but

$$\mathcal{N}(x + x) = \frac{x \cdot 2 + 0}{1} \;]\![^{G}_{\rho}\; a + a$$

does not hold.

We need to interpret $e/1$ and $e \cdot i$ when we can interpret e

Hierarchical Reflection (interpretation relations)

	$][^{G}_{\rho}$	$][^{R}_{\rho}$	$][^{F}_{\rho}$
$v \in \mathbb{V}$	yes	yes	yes
$i \in \mathbb{Z}$	if $i = 0$	yes	yes
$e + f$	yes	yes	yes
$e \cdot f$	if $f \in \mathbb{Z}$	yes	yes
e/f	if $f = 1$	if $f = 1$	if $f \neq 0$

In the last three cases the additional requirement that e (and eventually f) be interpreted is implicit.

Hierarchical Reflection (correctness)

To prove

$$e \;]\![^G_\rho\; a \;\Rightarrow\; \mathcal{N}(e) \;]\![^G_\rho\; a$$

one needs to use the knowledge that the auxiliary functions will only be applied to the “right” arguments.

For example, correctness of $\cdot_{MM}$ w.r.t. $]\![^F_\rho$ states that

$$e \;]\![^F_\rho\; a \;\wedge\; f \;]\![^F_\rho\; b \;\Rightarrow\; e \cdot_{MM} f \;]\![^F_\rho\; a \cdot b$$

but $a \cdot b$ has no meaning in a group!

Hierarchical Reflection (correctness)

However,

$$e \;]\![_\rho^F\; a \;\wedge\; f \;]\![_\rho^F\; b \;\Rightarrow\; e \cdot_{MM} f \;]\![_\rho^F\; a \cdot b$$

is equivalent to

$$e \cdot f \;]\![_\rho^F\; a \cdot b \;\Rightarrow\; e \cdot_{MM} f \;]\![_\rho^F\; a \cdot b$$

and the same property w.r.t. $]\![_\rho^G$ can be written down as

$$e \cdot f \;]\![_\rho^G\; c \;\vee\; f \cdot e \;]\![_\rho^G\; c \;\Rightarrow\; e \cdot_{MM} f \;]\![_\rho^G\; c$$

(the disjunction is needed because $\cdot_{MM}$ can swap the order of its arguments)

Hierarchical Reflection (optimization for rings and groups)

To avoid divisions by 1, one can forget about the type F altogether and define $\mathcal{N}_R$ directly using $\cdot_{MM}$ and the like; the base case now looks like

$$\mathcal{N}(v) := v \cdot 1 + 0$$

Also, in groups and rings normal forms *are* unique, so the last subtraction can also be avoided.

Tighter Integration?

$$\begin{tikzcd}
 & F : \text{Field} \arrow[d] \\
E \arrow[ur, "\rrbracket_{\rho}^{F}"] \arrow[r, "\rrbracket_{\rho}^{R}"] \arrow[dr, "\rrbracket_{\rho}^{G}"'] & R : \text{Ring} \arrow[d] \\
 & G : \text{Group}
\end{tikzcd}$$

but better would be

$$\begin{tikzcd}
 & F : \text{Field} \arrow[d] \\
E \arrow[ur, "\rrbracket_{\rho}"] \arrow[r, "\rrbracket_{\rho}"] \arrow[dr, "\rrbracket_{\rho}"'] & R : \text{Ring} \arrow[d] \\
 & G : \text{Group}
\end{tikzcd}$$

The first requires *all* functions $+_{MM}$, $\cdot_{MM}$, etc. to be proved correct w.r.t. $\rrbracket_{\rho}^{G}$, $\rrbracket_{\rho}^{R}$ and $\rrbracket_{\rho}^{F}$.

Most of these proofs are (almost) the same, yet they cannot be reused!

Tighter Integration?

Instead of defining $]\!]_\rho^G$, $]\!]_\rho^R$ and $]\!]_\rho^F$ by e.g.

$$
\begin{aligned}
e \;]\!]_\rho^G\, x \;\wedge\; f \;]\!]_\rho^G\, y \;&\Rightarrow\; e+f \;]\!]_\rho^G\, x+y \\
e \;]\!]_\rho^R\, x \;\wedge\; f \;]\!]_\rho^R\, y \;&\Rightarrow\; e\cdot f \;]\!]_\rho^R\, x\cdot y \\
e \;]\!]_\rho^F\, x \;\wedge\; f \;]\!]_\rho^F\, y \;\wedge y\#0 \;&\Rightarrow\; e/f \;]\!]_\rho^F\, x/y
\end{aligned}
$$

define $]\!]_\rho^- : \Pi_{A:\mathsf{Setoid}} E \to A$ s.t.

$$
\begin{aligned}
A \text{ is group } \wedge\; e \;]\!]_\rho^A\, x \;\wedge\; f \;]\!]_\rho^A\, y \;&\Rightarrow\; e+f \;]\!]_\rho^A\, x+y \\
A \text{ is ring } \wedge\; e \;]\!]_\rho^A\, x \;\wedge\; f \;]\!]_\rho^A\, y \;&\Rightarrow\; e\cdot f \;]\!]_\rho^A\, x\cdot y \\
A \text{ is field } \wedge\; e \;]\!]_\rho^A\, x \;\wedge\; f \;]\!]_\rho^A\, y \;\wedge y\#0 \;&\Rightarrow\; e/f \;]\!]_\rho^A\, x/y
\end{aligned}
$$

using subtyping of algebraic structures.

Tighter Integration (the bad news)

Does not work!

Proving

$$e \;]\![_{\rho}^{A}\, a \;\wedge\; e \;]\![_{\rho}^{A}\, b \;\Rightarrow\; a =_{A} b$$

requires a strong induction principle — the K-axiom:

$$\langle x, y[x] \rangle = \langle x', y'[x'] \rangle \;\Rightarrow\; x = x' \;\wedge\; y = y'$$

The K-axiom, although consistent with, is not provable within Coq.

Conclusions

- Powerful tactics for equational reasoning
- Can now deal with functions e.g. absolute value on $\mathbb{R}$
- Reuse of code for fields, rings and groups
- Improvement possible using K-axiom