Programming Languages meets Program Verification: The Chalmers University's approach

Andrés Sicard-Ramírez

Logic and Computation Seminar
EAFIT University
27 Feb 2007

Abstract

We will give an overview of the CoVer project (Combining Verification Methods in Software Development) at Chalmers University, Sweden. The goal of this project is to provide an environment for Haskell programming which provides access to tools for automatic and interactive correctness proofs as well as to tools for testing. Moreover, we will show a short demo of two tools developed around CoVer project: Agda, a proof assistant using dependent type theory, and QuickCheck, a property based random testing tool for Haskell.

Sweden

- Area: 449.964 km^2. • Pop: 9.1 million • Capital: Stockholm

Gothenburg

- Area: 450 km^2. • Pop: 487.627

Independent types I

Definition (Independent types (abstract syntax))

$$V ::= v \mid V' \quad \text{(type variables)}$$
$$C ::= c_1 \mid \cdots \mid c_n \quad \text{(type constants)}$$

$$\begin{aligned}
\mathbb{T} ::=& V \\
&\mid C \\
&\mid \mathbb{T} \to \mathbb{T} \quad \text{(function types)} \\
&\mid \mathbb{T} \times \mathbb{T} \quad \text{(product types)} \\
&\mid \mathbb{T} + \mathbb{T} \quad \text{(disjoint union types)}
\end{aligned}$$

Independent types II

Example (Haskell's types)

- Type variables: `a,b,…`
- Type constants: `Int,Integer,Char,etc.`
- Function types: e.g. `Int` $\rightarrow$ `Int`
- Product types: e.g. `(Int,Char)`
- Disjoint union types: e.g.
  `data Sum a b = Inl a | Inr b`

λ-calculus (untyped) I

Intuitively

λ-calculus element	Denotes
$\lambda x.x^2 + 1$ (abstraction)	Fn. $x \mapsto x^2 + 1$
$(\lambda x.x^2 + 1)3$ (application)	Fn. $x \mapsto x^2 + 1$ applied to 3
$(\lambda x.x^2 + 1)3 =_\beta 3^2 + 1$ (β-reduction)	The value of fn. $x \mapsto x^2 + 1$ applied to 3

Definition (λ-terms)

$$V ::= v \mid V' \quad \text{(variables)}$$

$$\Lambda ::= V \mid (\Lambda\Lambda) \mid (\lambda V \Lambda) \quad (\lambda\text{-terms})$$

λ-calculus (untyped) II

Definition (β-conversion)

$$(\lambda x.M)N =_\beta M[x := N] \quad \beta\text{-conversion}$$

Conventions

1. $x, y, z, \ldots$ denote variables
2. $M, N, L, \ldots$ denote λ-terms
3. $FM_1 M_2 \ldots M_n$ denotes $(\ldots((FM_1)M_2)\ldots M_n)$ (application uses association to the left)
4. $\lambda x_1 \ldots x_n.M$ denotes $(\lambda x1(\ldots(\lambda x_n(M))\ldots))$ (abstraction uses association to the right)
5. Outermost parentheses are not written

λ-calculus (untyped) III

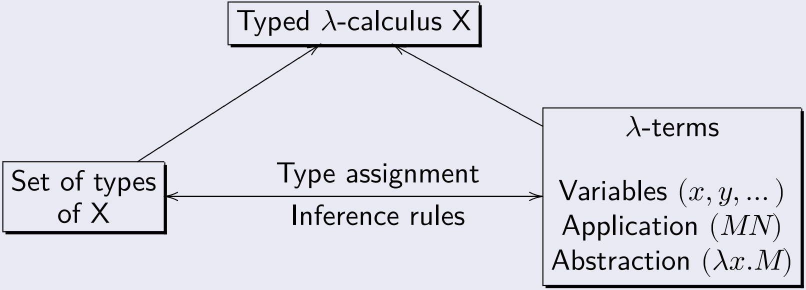
Examples

$$I \equiv \lambda x.x \qquad \text{(identity function)}$$
$$K \equiv \lambda xy.x \qquad \text{(first coordinate projection)}$$
$$S \equiv \lambda xyz.xz(yz)$$

$$IM =_\beta M$$
$$KMN =_\beta M$$

Typed λ-calculus I

General picture



Typed λ-calculus II

Definition (Simple typed λ-calculus (à la Curry))

Types $\mathbb{T}$:

type variables: $\alpha, \alpha', \ldots \in \mathbb{T}$

function space types: $\sigma, \tau \in \mathbb{T} \Rightarrow (\sigma \to \tau) \in \mathbb{T}$

Inference rules:

$$\frac{}{x : \sigma \vdash x : \sigma} \text{ (Axiom,Variable)}$$

$$\frac{\Gamma \vdash M : (\sigma \to \tau) \qquad \Gamma \vdash N : \sigma}{\Gamma \vdash (MN) : \tau} \text{ ($\to$-elimination, Application)}$$

$$\frac{\Gamma, x : \sigma \vdash M : \tau}{\Gamma \vdash (\lambda x.M) : (\sigma \to \tau)} \text{ ($\to$-introduction, Abstraction)}$$

Typed λ-calculus III

Example (Proof in simple typed λ-calculus)

$$\dfrac{\dfrac{\dfrac{}{x : \sigma, y : \tau \vdash x : \sigma}\,(\text{Var})}{x : \sigma \vdash \lambda y.x : \tau \to \sigma}\,(\text{Abs})}{\vdash \lambda xy.x : \sigma \to \tau \to \sigma}\,(\text{Abs})$$

Example (Haskell)

```
k m n = m
k = \m n -> m

*Main> :t k
k :: a -> b -> a
```

Dependent types

Definition (Dependent types)

"*A dependent type is a type that may depend on a value, typically like an array type, which depends on its length.*" (Barthe and Coquand 2002, p. 2)[1]

[1] G. Barthe and T. Coquand (2002). An Introduction to Dependent Type Theory. In: *Applied Semantics*. Ed. by G. Barthe, P. Dybjer, L. Pinto, and J. Saraiva. Vol. 2395. LNCS, pp. 1–41.

Dependent types

Definition (Set theory: Dependent function space)

Let $(B_x)_{x \in A}$ be an indexed family of sets.

$$\Pi_{x \in A} B_x = \{f \colon A \to \cup_{x \in A} B_x \mid (\forall x \in A)(f(x) \in B_x)\}$$

Note

If $B_x = B$ for all $x \in A$, then $\Pi_{x \in A} B_x = A \to B$.

Definition (Type theory: Pi types)

$\Pi x : A.B(x)$ is the type of terms f such that, for every $a : A$ then $f\ a : B(a)$.

Dependent types

Definition (Set theory: Sum (disjoint union) of a family of sets)

Let $(B_x)_{x \in A}$ be an indexed family of sets.

$$\Sigma_{x \in A} B_x = \{(x, b) \mid x \in A, b \in B_x\}$$

Note

If $B_x = B$ for all $x \in A$, then $\Sigma_{x \in A} B_x = A \times B$.

Note

If $A = \{0, 1\}$ then

$$\begin{aligned} \Sigma_{x \in A} B_x &= \{(0, b) \mid b \in B_0\} \cup \{(1, b) \mid b \in B_1\} \\ &= A + B. \end{aligned}$$

Dependent types

Definition (Type theory: Sigma types)

$\Sigma x : A.B$ is the type of pairs $(M, N)_{\Sigma x : A\,.\,B}$ such that $M : A$ and $N : B(M)$.

Constructive interpretation of logical constants

Definition

"*a proposition is defined by laying down what counts as proof of the proposition …a proposition is true if it has a proof, that is, if a proof of it can be given.*" (Martin-Löf 1984, p. 11)[1]

[1] P. Martin-Löf (1984). *Intuitionistic Type Theory*. Notes by Giovanni Sambin of a series of lectures given in Padua, June 1980. Bibliopolis.

Constructive interpretation of logical constants

a proof of the proposition	consist of (BHK-interpretation)	has the form
$A \wedge B$	a proof of A and a proof of B	(a, b), where a is a proof of A and b is a proof of B
$A \vee B$	a proof of A or a proof of B	$inl(a)$, where a is a proof of A, or $inr(b)$, where b is a proof of B
$\bot$	has not proof	
$A \supset B$	a method which takes any proof of A into a proof of B	$\lambda x.b(x)$, where $b(a)$ is a proof of B provided a is a proof of A
$(\forall x)B(x)$	a method which takes an arbitrary individual a into a proof of $B(a)$	$\lambda x.b(x)$, where $b(a)$ is a proof of $B(a)$ provided a is a proof of A
$(\exists x)B(x)$	an individual a and a proof of $B(a)$	(a, b), where a is an individual and b is a proof of $B(a)$

Curry-Howard isomorphism

"*If we take seriously the idea that a proposition is defined by laying down how its canonical proofs are formed and accept that a set is defined by prescribing how its canonical elements are formed, then it is clear that it would only lead to unnecessary duplication to keep the notions of proposition and set (...) apart.*" (Martin-Löf 1984, p. 13)[1]

[1] P. Martin-Löf (1984). *Intuitionistic Type Theory*. Notes by Giovanni Sambin of a series of lectures given in Padua, June 1980. Bibliopolis.

Curry-Howard isomorphism

A	$a : A$	
A is a set	a is an element of the set A	$A \neq \emptyset$
A is a proposition	a is a proof (construction) of the proposition A	A is true
A is a problem	a is a method of solving the problem A	A is solvable
A is a specification	a is a program than meets the specification A	A is satisfiable

Curry-Howard isomorphism

Curry-Howard isomorphism (propositions-as-sets, formulas-as-types)

$$A \wedge B = A \times B$$
$$A \vee B = A + B$$
$$A \supset B = A \to B$$
$$\bot = \emptyset$$
$$\neg A = A \to \bot$$
$$(\forall x) B(x) = \Pi_{x \in A} B_x$$
$$(\exists x) B(x) = \Sigma x : A.B$$

Curry-Howard isomorphism

Example (Curry-Howard isomorphism working)

$\lambda \to$: simple typed λ-calculus
$IPC(\to)$: Implicational fragment of intuitionistic propositional logic

$$\dfrac{\dfrac{\dfrac{}{x : \sigma, y : \tau \vdash_{\lambda\to} x : \sigma}\ (\text{Var})}{x : \sigma \vdash_{\lambda\to} \lambda y.x : \tau \to \sigma}\ (\text{Abs})}{\vdash_{\lambda\to} \lambda xy.x : \sigma \to \tau \to \sigma}\ (\text{Abs})$$

$$\dfrac{\dfrac{\dfrac{}{\sigma, \tau \vdash_{IPC(\to)} \sigma}\ (\text{Ax})}{\sigma \vdash_{IPC(\to)} \tau \to \sigma}\ (\to\text{-intro})}{\vdash_{IPC(\to)} \sigma \to \tau \to \sigma}\ (\to\text{-intro})$$

References

Remark: The other slides shown in talk, that is to say, Prof. Dybjer's slides, can be found in `http://www.cs.chalmers.se/~peterd/` under the "Combining testing and proving" link.

Acknowledgements

- We thank Peter Dybjer and Ana Bove (Chalmers University of Technology), Alberto Pardo (Universidad de la República), and Francisco Correa (Universidad EAFIT) for help us in all issues related to our visit to Chalmers University.
- We thank Universidad EAFIT and LerNET project for financial support.