Proceedings of the 4th DIKU-IST Joint Workshop on the Foundations of Software

Glück, Robert; Henglein, Fritz; Hu, Zhenjiang; Takeichi, Masato

Publication date: 2011

Document version: Publisher's PDF, also known as Version of record

Document license: Unspecified

Citation for published version (APA):

Download date: 22. sep., 2021
Preface

These proceedings contain the contributions presented at the 4th DIKU-IST Joint Workshop on Foundations of Software held at Tokyo, Japan, January 10-14, 2011. The workshop featured talks and discussions on program optimization and parallel programming, formal semantics and algorithms, reversible and bidirectional computing, and demonstrations of software prototypes.

After the success of the first three joint workshops, which took place at Dragør, Copenhagen (2005), Shonan Village, Japan (2006) and Roskilde, Denmark (2007) with proceedings as DIKU Technical Reports 05/07, 06/07 and 07/07, the 4th DIKU-IST workshop took again place in Japan. It aimed to provide a forum for presenting the latest research and promoting the research collaboration between the Department of Computer Science (DIKU), University of Copenhagen, and the Graduate School of Information Science and Technology (IST), University of Tokyo. In 2004, IST and the Faculty of Science at the University of Copenhagen entered an Academic and Student Exchange Agreement during the State Visit of Queen Margrethe II to Japan. Today, both universities are partners in the International Alliance of Research Universities (IARU).

Computer science provides one of the keys to the technologies of the 21st century. Its applications have found their way into all areas of daily life, often unnoticed by their users, and software has become a decisive factor for commercial success in many areas of modern business and society. This series of workshops between DIKU and IST is devoted to the scientific foundations of software. Theory and practice of programming languages are very important and visible research fields at both research institutions in Copenhagen and Tokyo. The objective of these joint workshops is to give researchers and graduate students at both institutions the opportunity to exchange the latest research ideas and to jointly engage in outstanding international research.

The workshop had about 50 participants from Japan and Denmark. The organizers would like to thank all speakers, participants, and the local organizers for making this meeting both successful and enjoyable. Special thanks to Masami Hagiya, Dean of IST, for supporting the workshop, Yasuo Kuniiyoshi, Professor of IST, for the visit to the robotics laboratory, and to Kaori Sato of the Office of International Relations for organizing the student program.

Copenhagen and Tokyo, February 2011

Robert Glück
Fritz Henglein
Zhenjiang Hu
Masato Takeichi
Organization

The *DIKU-IST Joint Workshop on Foundations of Software* was organized by the Graduate School of Information Science and Technology, University of Tokyo, together with the Department of Computer Science, University of Copenhagen.

Meeting

Program committee: Robert Glück  
Fritz Henglein  
Zhenjiang Hu  
Masato Takeichi

Local arrangements: Kazuyuki Asada  
Keisuke Nakano

Proceedings: Tom Hvitved

Sponsoring Institutions

This workshop was supported by Grant-in-Aid for Scientific Research (A) 192000-02, a joint research project at National Institute of Informatics, and The International Alliance of Research Universities (IARU) fund of the University of Copenhagen. Thanks also to the Danish National Advanced Technology Foundation (Højteknologifonden), the Danish Strategic Research Council (Det Strategiske Forskningsråd) and the Danish Free Research Council (Det Frie Forskningsråd).
Table of Contents

Introduction
Opening Address .......................................................... 1
Masato Takeichi

Session 1
Programming in Biomolecular .......................................... 3
Lars Hartmann, Neil D. Jones, and Jakob Grue Simonsen
Reinvestigation of Symmetric Lambda Calculus — Functional
Derivation of Small-Step Semantics for Symmetric Lambda Calculus (SLC) 10
Kenichi Asai and Yayoi Ueda
Report on a Self-applicable Online Partial Evaluator for a Recursive
Flowchart Language ..................................................... 31
Robert Glück

Session 2
A Universal Reversible Turing Machine .............................. 33
Holger Bock Axelsen and Robert Glück
Generating Input-Erasing Efficient Clean Reversible Programs for
Injective Functions ....................................................... 42
Tetsuo Yokoyama
Reversible Coroutines .................................................... 47
Poul J. Clementsen, Robert Glück, and Holger Bock Axelsen

Session 3
Monadic Effects in Operational Semantics .......................... 54
Andrzej Filinski
Report on using Generic Multiset Discrimination for a Probability Monad 58
Ken Friis Larsen
A Trace-based Model for Multi-Party Contracts .................... 64
Tom Hvitved, Felix Klaedtke, and Eugen Zălinescu

Session 4
Semantic Patch Inference ............................................... 71
Jesper Andersen
A Short Review: Left Inverses vs. Right Inverses ............................. 80
Kazutaka Matsuda

Session 5
Towards a Software Model Checker for ML .................................. 89
Naoki Kobayashi, Ryosuke Sato, Hiroshi Unno, Luke Ong, Naoshi
Tabuchi, and Takeshi Tsukada
Modal-μ Definable Graph Transduction ........................................ 98
Kazuhiro Inaba
Determining the Valid Parameters for the Weight-Balanced Tree Algorithm 110
Yoichi Hirai and Kazuhiko Yamamoto

Session 6
An Adversarial Approach to Interaction Specifications .................... 122
Anders Starcke Henriksen
Jigsaw Radix Conversion ......................................................... 129
Keisuke Nakano
Compositional Data Types — A Report from the Field .................... 141
Patrick Bahr, Tom Hvitved, and Morten Ib Nielsen

Session 7
From Parametric Polymorphism to Balanced Tree Structures for
Parallel Programming .............................................................. 150
Akimasa Morihata and Kiminori Matsuzaki
A Homomorphism-based MapReduce Framework for Systematic
Parallel Programming ............................................................. 156
Yu Liu
Specification and Implementation of ERP Requirements ............... 167
Mikkel Jønsson Thomsen

Session 8
Marker-directed Optimization of UnCAL Graph Algebra revisited:
Optimizing Bidirectional Graph Transformations ........................ 172
Soichiro Hidaka
Functional Graph Transformation with Structural Recursion .......... 183
Hiroyuki Kato
Semantic Structures of Bidirectional Programming .................... 197
Kazuyuki Asada
Session 9

Regular Expressions as Types ........................................ 208
  Fritz Henglein and Lasse Nielsen

Workflows as Session Types ........................................... 224
  Lasse Nielsen, Nobuko Yoshida, and Kohei Honda

Session 10

Semirings for Free! — An Algebraic Approach to Efficient Parallel Algorithms for Nested Reductions .................. 228
  Kento Emoto

Semiring Fusion .......................................................... 237
  Sebastian Fischer

Session 11

Partial Evaluation of Janus ............................................. 247
  Torben Ægidius Mogensen

On Determination of Backward Graph Transformation ........... 269
  Zhenjiang Hu

Author Index ............................................................. 279
The Fourth DIKU-IST
Joint Workshop on
Foundations of Software

Asakusa View Hotel and Univ. Tokyo

January 10-14, 2011

Academic Exchange Agreement Ceremony
between Faculty of Science, University of Copenhagen
and Graduate School of IST, University of Tokyo

November 15, 2004

Works after the 1st DIKU-IST Workshop at Copenhagen

September 24, 2005
Participants of the 2nd DIKU-IST Workshop at Shonan-Village, Japan

April 21-22, 2006

3rd DIKU-IST Joint Workshop on Foundations of Software
Fri & Sat, 5-6 October 2007, Comwell Hotel, Roskilde, Denmark

John Andersen
(Director of International Affairs, University of Copenhagen)

Masaki Okada
(Ambassador of Japan in Denmark)

40+ participants
(11 from IST, University of Tokyo)

The Fourth DIKU-IST Joint Workshop on Foundations of Software

10 – 14 January, 2011
Japan

Objective
After the success of the first, second, and third DIKU-IST workshops, the fourth DIKU-IST workshop aims to provide a forum for exchanging research ideas among researchers on programming languages and formal methods. The workshop is hosted by the Department of Computer Science (DIKU) at University of Copenhagen and Graduate School of Information Science and Technology (IST) at University of Tokyo.
PROGRAMMING IN BIOMOLECULAR COMPUTATION

Lars Hartmann
Neil D. Jones
Jakob Grue Simonsen
+Visualization by Søren Bjerregaard Vrist

(All now or recently at the University of Copenhagen)

DIKU-IST (January 2011)

Sources:
▶ June 2010 conference CS2BIO Computer Science to Biology
▶ Journal Scientific Annals of Computer Science (to appear)
▶ Festschrift for Carolyn Talcott (to appear)

— 0 —

UNIVERSALITY AND PROGRAMMING IN A
BIOCHEMICAL SETTING

Turing completeness results for biomolecular computation:
▶ Cardelli, Chapman, Danos, Reif, Shapiro, Wolfram, . . .
▶ Net effect: any computable function can be computed, in some sense, by various biological mechanisms.
▶ Not completely compelling from a programming perspective.
▶ Our aim: a computation model where
  • “program” is clearly visible and natural, and
  • Turing completeness is not artificial or accidental, but a natural part of biomolecular computation

— 1 —

CONNECTIONS EXIST BETWEEN BIOLOGY AND COMPUTATION, but . . .
WHERE ARE THE PROGRAMS?

Our proposal: a model of computation that is
▶ biologically plausible: semantics by chemical-like reaction rules;
▶ programmable (a bit like low-level computer machine code);
▶ uniform: new “hardware” not needed to solve new problems;
▶ stored-program: programs = data;
  programs are executable and compilable and interpretable
▶ universal: all computable functions can be computed
▶ Turing complete in a strong sense: ∃ a universal algorithm
  (able to execute any program, asymptotically efficient)

— 2 —
BUT WHERE ARE THE PROGRAMS?

In existing models of biomolecular computation
it’s hard to see anything like a program that realises or
directs a computational process.

► In cellular automata, “program” is expressed only in the ini-
tial cell configuration, or in the global transition function
► Many examples: given a problem, authors cleverly devise a
biomolecular system that can solve this particular problem
► The algorithm being implemented is hidden in the details of
the system’s construction, hard to see.

Our purpose is to fill this gap,
► to establish a biologically feasible framework in which
► programs are first-class citizens.

— 3 —

OTHER COMPUTATIONAL FRAMEWORKS

Circuits, BDDs, finite automata: Nonuniform, Turing incomplete
Turing machine:
► Pro Visible program; complete; universal machine exists
► Con Asymptotically slow: universal machine takes time
\[ O(n^2) \] to simulate a program running in time \( O(n) \)

Other program-based models: Post, Minsky, LISP, RAM, RASP…
Complex, biologically implausible

Cellular automata: von Neumann, LIFE, Wolfram,…
► Pro Can simulate a Turing machine
► Con Complex, biologically implausible (synchronisation!)
  There is no natural universal cellular automaton.
  It’s very hard to see “the program”.

— 4 —

“DIRECT” PROGRAM EXECUTION

Write \([\text{program}]\) for the meaning or net effect of running \(\text{program}\):

\[ [\text{program}] (\text{data}_{in}) = \text{data}_{out} \]

► program is an active agent.
► It is activated (run) by applying the semantic function \([\cdot]\).
► Some mechanism is needed to execute program, i.e., to apply
  \([\cdot]\) to program and \(\text{data}_{in} : \) hardware (“wetware”).

— 5 —
THE BIOLOGICAL WORLD IS NOT HARDWARE!

We must re-examine programming language assumptions. Computers have programmer-friendly conveniences, e.g.,

- A large address space of randomly accessible data
- Pointers to data, perhaps at a great “distance” from the current program or data
- address arithmetic, index registers,…
- Unbounded fan-in: many pointers to the same data item…

None of these is biologically plausible! Workarounds are needed if we want to do biological programming.

FOR BIOLOGICAL PLAUSIBILITY

- There is no action at a distance: all effects achieved via chains of local interactions. Biological analog: signaling.
- There are no pointers to data (addresses, links, list pointers): To be acted on, a data value must be physically adjacent to an actuator. Biological analog: chemical bond between program and data.
- No nonlocal control transfer, e.g., unbounded GOTOs or remote procedure calls. Biological analog: a bond from one part of a program to another.
- A “yes”: ∃ available resources to tap, i.e., energy to change the program control point, or to add data bonds. Biological analogs: ATP, oxygen, Brownian movement.

THE BLOB MODEL

Simplified view of a molecule and chemical interactions (Cardelli, Danos, Lanèvre,…).

Blobs are in a biological “soup” and are connected by symmetrical bonds linking their bond sites.

Picture of a blob: (Bond sites 0, 2 and 3 are bound, and 1 is unbound)

```
  1
  
  3
  2
```

A blob has 4 bond sites and 8 cargo bits (boolean values). Here: Bond sites 0, 2 and 3 are bound, and 1 is unbound. Cargo bits omitted for brevity.
KEEPING THE FOCUS

How to structure a biologically feasible model of computation?

▶ Idea: keep current program counter and data cursor always close to a focus point where all actions occur.

▶ How? Continually shift both program and data, to keep the active bits near the focus.

Running program \( p \): computing \([p](d)\)

\[
\text{Program } p \quad \text{Data } d
\]

\[
= \text{Focus point for control and data (connects the APB and the ADB)}
\]

\[
* \quad = \text{program-to-data bond: “the bug”}
\]

A MOVIE IS WORTH DURATION \( \times \) FRAMERATE \( \times \) 1000 WORDS

(Circle.avi)

— 10 —

ABOUT INSTRUCTIONS:

Instruction form:

opcode parameters (bond0, bond1, bond2, bond3)

Why exactly 4 bonds?

▶ Predecessor (1 bond); true and false successors (2 bonds);
▶ plus one bond to link the APB to the ADB.

It’s almost a von Neumann machine code, but...

▶ A bond is a two-way link between two adjacent blobs.
▶ A bond is not an address.
▶ There is no address space as in conventional computer (and hence: no address decoding hardware).
▶ Also: no registers (use the cargo bits instead).

— 11 —
INSTRUCTIONS HAVE 8 BITS

<table>
<thead>
<tr>
<th>Instruction</th>
<th>Description</th>
<th>Informal semantics (write :=: for a two-way interchange)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCG v c</td>
<td>Set CarGo bit</td>
<td>ADB.c := v; APB := APB.2</td>
</tr>
<tr>
<td>JCG c</td>
<td>Jump CarGo bit</td>
<td>if ADB.c = 0 then APB := APB.3 else APB := APB.2</td>
</tr>
<tr>
<td>JB b</td>
<td>Jump Bond</td>
<td>if ADB.b = ⊥ then APB := APB.3 else APB := APB.2</td>
</tr>
<tr>
<td>CHD b</td>
<td>CHange Data</td>
<td>ADB := ADB.b; APB := APB.2</td>
</tr>
<tr>
<td>INS b1 b2</td>
<td>INSert new bond</td>
<td>ADB := ADB.b1; ADB := ADB.b1.bs; APB := APB.2</td>
</tr>
<tr>
<td>SBS b1 b2</td>
<td>SWap Bond Sites</td>
<td>ADB.b1 := ADB.b2; APB := APB.2</td>
</tr>
<tr>
<td>SWL b1 b2</td>
<td>SWap Links</td>
<td>ADB.b1 := ADB.b2.b1; APB := APB.2</td>
</tr>
<tr>
<td>SWP3 b1 b2</td>
<td>Swap bs3 on linked</td>
<td>ADB.b1.3 := ADB.b2.3; APB := APB.2</td>
</tr>
<tr>
<td>FIN</td>
<td>Fan IN</td>
<td>APB := APB.2 (two predecessors: bond sites 1 and 3)</td>
</tr>
</tbody>
</table>

SCG, ... , EXT: Operation codes
b, b1, b2: Bond site numbers
c: Cargo site number
v: A one-bit value

EXAMPLE: EFFECT OF SCG 1 5 (SET CARGO BIT 5 TO 1)

“The bug” * has moved:
• before execution, it connected APB with ADB.
• After: it connects successor APB’ with ADB.

Also: activation bits 0, 1 have been swapped.

Instruction syntax: the 8-bit string 11001101 is grouped as

\[
\begin{array}{c}
\overset{\text{SCG}}{1}
\overset{\text{100}}{v}
\overset{\text{101}}{c}
\end{array}
\]

SEMANTICS OF SCG 1 5 BY "SOMETHING LIKE" A CHEMICAL REACTION RULE

Instruction form:

\[
\begin{array}{c}
\overset{\text{SCG}}{1}
\overset{\text{100}}{v}
\overset{\text{101}}{c}
\end{array}
\]

( = unchanged bond or cargo bit)

Similar style to: Danos and Laneve, Formal Molecular Biology.
TURING COMPLETENESS BY INTERPRETATION

Turing completeness is usually shown by simulation, e.g.,
> for any 2CM program you build a biomolecular system such that . . .

But: the biomolecular system is usually built by hand. The effect: hand computation of the $\exists$ quantifier in

$$\forall p \exists q(\llbracket p \rrbracket^E = \llbracket q \rrbracket^M)$$

In contrast, Turing’s original “Universal machine” (UM) works by interpretation, where $\exists$ is realised by machine.

The UM can execute any TM program, if coded on the UM’s tape along with its input data.

Our research follows Turing’s line, in a biological context: It does simulation by general interpretation, and not by one-problem-at-a-time constructions.

— 15 —

PROGRAM EXECUTION BY INTERPRETATION

$$\llbracket \text{interpreter} \rrbracket(\text{program}, \text{data}_{in}) = \text{data}_{out}$$

Now program is a passive data object: both program and data$_{in}$ are data for the interpreter.

program is now executed by running the interpreter program.

(Of course, some mechanism will be needed to run the interpreter, e.g., hard-, soft- or wetware.)

Self-interpretation is possible, and useful in practice.

The Universal Turing machine is a self-interpreter.

— 16 —

A “BLOB UNIVERSAL MACHINE”

We have programmed a self-interpreter for the blob formalism – analogous to Turing’s original universal machine.

This gives: Turing-completeness in a new biological framework.

— 17 —
CONTRIBUTIONS OF THIS WORK

- Programmable bio-level computation where programs = data.
- Blob semantics by abstract biochemical reaction rules.
- All computable functions are blob-computable:
  - Can do with one fixed, set of reaction rules (defining a fixed instruction set, i.e., a “machine language”)
  - Don’t need new rule sets (i.e., biochemical architectures) to solve new problems; it’s enough to write new programs.
- (Uniform) Turing-completeness
- Promise of tighter analogy between universality and self-reproduction.
- Interpreters and compilers make sense at biological level, may give useful operational and utilitarian tools.

WHERE TO NOW?

Some points to address:

- Find a true, biological (not just “feasible”) implementation of the fixed set of reduction rules in vitro.
- Programs are currently similar to classical machine code; this requires programmer skill. Solution: Devise an intermediate-level blob programming language.
- Still to analyse: The time or energy cost of performing a single program step (may depend on program/data). An appropriate and realistic cost model should be found.
- Bonus: This could initiate a study of computational complexity in the blob world.
Reinvestigation of Symmetric Lambda Calculus

Yayoi Ueda  Kenichi Asai
Ochanomizu University

Abstract

This paper presents a symmetric lambda calculus (SLC) in which both the duality between call-by-value and call-by-name and the duality between expressions and continuations hold at the same time. The idea of SLC was originally introduced by Filinski in 1989, but has not been investigated seriously since then. This paper first reformulates SLC using small-step reduction semantics in a completely symmetric way. We then show call-by-value and call-by-name evaluation strategies for SLC and prove that both enjoy various formal properties, such as subject reduction. Finally, we prove that the small-step semantics shown here coincides with Filinski’s original definition of SLC using the functional correspondence approach: the two semantics are related via defunctionalization.

Keywords: symmetric lambda calculus, control operators, functional correspondence, defunctionalization

1 Introduction

Background and related work  In 1990, Griffin [7] showed the correspondence between the law of double-negation elimination in classical logic and the control operator C introduced by Felleisen and Hieb [5]. Since then, many researchers explored the foundational theory for continuations and control operators. Parigot [8] introduced λµ-calculus and showed that it corresponds to the classical natural deduction. Curien and Herbelin [3] introduced λµ˜µ-calculus that exhibits symmetry between expressions and continuations as well as between call-by-value (CBV) and call-by-name (CBN) based on the classical sequent calculus. Selinger [12] gave a categorical semantics to λµ-calculus and showed categorical duality between CBV and CBN. These work led to Wadler’s Dual Calculus [14] that shows CBV/CBN symmetry in a particularly clear way in a simple syntax and operational semantics. Tzevelekos [13] studied the Dual Calculus in detail and showed various syntactic properties.

Underlying these work is an intuition that expressions and continuations are dual. Surprisingly, this observation was made as early as in 1989 by Filinski [6]. He presented a symmetric lambda calculus (SLC) in which expressions and continuations are treated in a complete symmetry. Just like we abstract over expressions to receive an argument expression, we can abstract over continuations in SLC to capture the current continuation. This system has many implications. The CBV/CBN duality naturally arises from the priority of execution: to execute expressions first leads to CBV and continuations first CBN. The duality between types of expressions and continuations even suggests a relationship to classical logic via de Morgan’s laws.

However, although most of the previous work mentioned Filinski’s work, none of them actually investigated the relationship to SLC seriously. This is partly because Filinski’s SLC lacks small-step reduction semantics. It makes it harder to compare Filinski’s SLC to other calculi such as Dual Calculus, because they are often defined as small-step reduction semantics. This is unfortunate because SLC not only contains the standard lambda-calculus naturally but also presents control operators in a particularly simple and intuitive way.

The name symmetric lambda calculus was independently used by Barbanera and Berardi [2]. However, their work is quite different from Filinski’s SLC. Their calculus includes a notion of symmetric application where either component of an application can be a function or an argument. They proved the strong normalization property of this calculus.

This work  This paper investigates small-step reduction semantics for Filinski’s SLC. It handles both non-deterministic, CBV, and CBN evaluation strategies. The non-deterministic semantics exhibits com-
complete symmetry, whereas CBV and CBN strategies are dual to each other. A type system for SLC is shown which satisfies various properties such as subject reduction. The paper then shows that the small-step semantics presented here and the original denotational semantics of SLC given by Filinski are in functional correspondence with each other. This work is also a non-trivial application of Danvy’s functional correspondence approach [1, 4].

Overview In the next Section, we introduce SLC, its syntax, types, typing rules, non-deterministic reduction rules, and some properties. In Section 3, we show the CBV strategy and its properties such as uniqueness of evaluation. In Section 4, we show the CBN strategy and its properties. We defunctionalize Filinski’s original CBV denotational semantics, and show the correspondence between the two SLC’s in Section 5. Finally, we also defunctionalize Filinski’s CBN semantics and show their correspondence in Section 6.

2 Symmetric Lambda Calculus

This section introduces the symmetric lambda calculus (SLC). A standard way to represent reduction semantics is to use an evaluation context: \( E[M] \sim E[M'] \) if \( M \leadsto M' \). In SLC, we represent it with a configuration \( \langle e \mid c \rangle \), where \( e \) is an expression (corresponding to \( M \)) and \( c \) is a continuation (corresponding to \( E[\] \)). In addition, SLC has three-place configuration \( \langle e \mid f \mid c \rangle \) which represents that an expression \( e \) is passed to a function \( f \) in a context \( c \). In SLC, an evaluation context and searching for a redex are both explicit in a configuration. SLC calculates an expression and a continuation in a completely dual manner.

2.1 Syntax

Figure 1 shows the syntax of SLC.\(^1\) An expression \( e \) is either a natural number \( n \), a variable \( x \), a unit (\( \) ), a pair of expressions \( (e, e) \), an application \( e \uparrow f \), or a function treated as an expression \( [f] \). An application \( e \uparrow f \) passes an expression \( e \) to a function \( f \). Unlike the standard lambda-calculus, a function \( f \) is placed after the argument \( e \). In SLC, an expression and a function are distinct syntactic objects. To treat a function as an expression (to pass a higher-order function to another function, for example), a function is tagged with \( [\] \).

A continuation is defined as a dual notion of an expression. A continuation \( c \) is either an initial continuation \( * \), a continuation variable \( y \), a continuant \( \{ \} \), a pair of continuations \( \{c, c\} \), a continuation application \( f \mid c \) which represents a continuation that applies \( f \) before passing a value to \( c \), or a function treated as a continuation \( [f] \). An initial continuation \( * \) represents a continuation that receives a natural number \( n \). When the initial continuation receives a natural number \( n \), the computation finishes with the result \( n \). The continuant \( \{\} \) represents a continuation that never receives any value.

A function is either a function variable \( g \), an expression abstraction \( p \Rightarrow e \) which binds the current expression to \( p \) and replaces the expression with \( e \), a continuation abstraction \( f \Leftarrow q \) which binds the current continuation to \( q \) and replaces the continuation with \( c \), \( \bar{e} \) an expression that evaluates to a function \( [f] \), or \( \overline{e} \) a continuation that evaluates to a function \( [f] \).

---

\(^1\)This syntax slightly deviates from Filinski’s original syntax. Filinski used \( f \uparrow e \) and \( q \Rightarrow e \) instead of our \( e \uparrow f \) and \( c \Leftarrow q \), respectively. We changed the syntax because the new syntax exhibits beautiful symmetry when written in a small-step semantics.
\[
T ::= +A \quad \text{(types of expressions } e) \\
| A \supset B \quad \text{(types of functions } f) \\
| \neg B \quad \text{(types of continuations } c)
\]
\[
A, B ::= \bot \mid \top \mid \text{int} \mid A \land B \mid A \lor B \mid A \rightarrow B \mid A - B
\]

Figure 2: Types of SLC

An expression abstraction \( p \Rightarrow e \) has a pattern \( p \) as its formal argument. If the pattern is a variable \( x \), \( x \Rightarrow e \) corresponds to \( \lambda x . e \) in the standard lambda calculus. A pattern \( p \) can also be a unit, a pair, or a function pattern \( \lceil g \rceil \). Dually, \( q \) represents a pattern for a continuation abstraction \( c \Rightarrow q \).

We assume that the sets of variable names for expressions, continuations, and functions do not overlap. We use a meta variable \( \text{var} \) to represent any of the three kinds of variables.

As an example, Filinski represented call/cc in SLC as follows [6]:

\[
\text{call/cc} = (\lceil g \rceil \Rightarrow \lceil y \allow break \rangle \uparrow g \downarrow y \leftarrow y)
\]

where \( \allow break \) represents a dummy variable not used anywhere else. It grabs the current continuation in \( y \) and replaces the current continuation with \( \lceil y \allow break \rangle \uparrow g \downarrow y \). The installed function \( \lceil g \rceil \Rightarrow \lceil y \allow break \rangle \uparrow g \downarrow y \) receives a function \( g \) and passes the representation of the current continuation \( \lceil y \allow break \rangle \) to \( g \). The passed continuation, when applied, will replace the then continuation with \( y \), achieving jump to the continuation captured in \( y \). (See Section 2.4 for an example reduction sequence for call/cc.) Similarly, Felleisen’s \( C \) operator can be defined as follows:

\[
C = (\lceil g \rceil \Rightarrow \lceil y \Rightarrow \_ \rangle \uparrow g \downarrow \_ \leftarrow y)
\]

2.2 Types

Figure 2 shows types of SLC. Since SLC consists of three syntactic objects, the types of SLC consist of three types: an expression type \( +A \), a continuation type \( \neg B \), and a function type \( A \supset B \).

The type \( +A \) represents a type of an expression. The prefix + indicates that it is a type of an expression. The type \( \neg B \) represents a type of a continuation that receives a value of type \( +A \). In this paper we use \( \neg \) for a type of continuations. The type \( A \supset B \) represents a type of functions that receive an expression of type \( +A \) and return an expression of type \( +B \). At the same time, it represents a type of functions that receive a continuation of type \( \neg B \) and return a continuation of type \( \neg A \). A function has an implicative and contrapositive type together.

A neutral type \( A, B \) forms the inner structure of types. A neutral type is either true \( \top \), false \( \bot \), integer int, conjunction \( A \land B \), disjunction \( A \lor B \), implication \( A \rightarrow B \), or minus \( A - B \). The type \( +\top \) is a type of () and \( \neg\bot \) is a type of \( \{\} \).

2.3 Typing Rules

The typing rules of SLC are shown in Figure 3. The left column shows typing rules for expressions, while the right for continuations. Let \( \Gamma \) be a type environment. We write \( \Gamma \vdash e : +A \) to mean that an expression \( e \) has a type \( +A \) under \( \Gamma \), and similarly for a continuation and for a function.

The type environment \( \Gamma \) is defined as a set of type bindings \( \text{var} : T \), where all the variables occurring in a type environment have to be distinct. Given a type environment \( \Gamma \), we define \( \Gamma_p \) as a type environment where bindings for variables in the pattern \( p \) are removed (Figure 4).

The typing rules for expressions are mostly standard. To support a nested pattern for abstractions, the judgement \( \Gamma \vdash_p p : +A \) for expression patterns (and \( \Gamma \vdash_q q : \neg B \) for continuation patterns) is introduced, which is defined in the second part of Figure 3. The typing rules for continuations are obtained by taking the dual of the ones for expressions. In the rule \( \text{_App} \), a pair of continuations is given a disjunctive continuation type. Logically, it is a de Morgan dual of \( \neg A \land \neg B \). The rule \( \text{App} \) says that \( f \downarrow c \) as a whole can be regarded as a continuation of type \( \neg A \): it receives a value of type \( +A \), turns it

\[\[\text{The intuitive logical meaning of minus operator } A - B \text{ is } \neg(\neg B - \neg A). \text{ Filinski expresses this type as } \lceil A \leftarrow B \rceil [6].\]
\[ \Gamma \cup \{ g : A \supset B \} \vdash g : A \supset B \quad \text{TFVar} \]

\[ \Gamma_x \cup \{ x : +A \} \vdash x : +A \quad \text{TVar} \]

\[ \Gamma \vdash n : \text{int} \quad \text{TInt} \]

\[ \Gamma \vdash () : +1 \quad \text{TUnit} \]

\[ \Gamma \vdash e_1 : +A \quad \Gamma \vdash e_2 : +B \quad \text{TAnd} \]

\[ \Gamma \vdash (e_1, e_2) : + (A \land B) \]

\[ \Gamma \vdash p : +A \quad \Gamma \vdash e : +B \quad \text{TFun} \]

\[ \Gamma \vdash p \Rightarrow e : A \supset B \]

\[ \Gamma \vdash e : +A \quad \Gamma \vdash f : A \supset B \quad \text{TApp} \]

\[ \Gamma \vdash e \uparrow f : +B \]

\[ \Gamma \vdash f : A \supset B \quad \Gamma \vdash c : \neg B \quad \text{TApp} \]

\[ \Gamma \vdash f \downarrow c : \neg A \]

\[ \Gamma \vdash f : A \supset B \quad \Gamma \vdash [f] : (A \supset B) \quad \text{TFClo} \]

\[ \Gamma \vdash e : +(A \supset B) \]

\[ \Gamma \vdash \pi : A \supset B \quad \text{TCFun} \]

\[ \Gamma \vdash p () : +1 \quad \text{PUnit} \]

\[ \Gamma \vdash q \{} : \neg 1 \quad \text{QUnit} \]

\[ \Gamma \vdash x \cup \{ x : +A \} \vdash_p x : +A \quad \text{PVar} \]

\[ \Gamma \cup \{ y : \neg B \} \vdash y : \neg B \quad \text{QVar} \]

\[ \Gamma \cup \{ g : A \supset B \} \vdash [g] : + (A \supset B) \quad \text{PFClo} \]

\[ \Gamma \cup \{ g : A \supset B \} \vdash q [g] : \neg (A \supset B) \quad \text{QFClo} \]

\[ \Gamma \vdash p \vdash_p p_1 : +A \quad \Gamma \vdash p \vdash_p p_2 : +B \quad \text{PAnd} \]

\[ \Gamma \vdash (p_1, p_2) : + (A \land B) \]

\[ \begin{array}{c}
\vdash e : +A \\
\vdash e \quad \vdash c : \neg A \\
\vdash \langle e \mid c \rangle
\end{array} \quad \text{TProg1} \]

\[ \begin{array}{c}
\vdash e : +A \\
\vdash e \quad \vdash f : A \supset B \\
\vdash \langle e \mid f \mid c \rangle
\end{array} \quad \text{TProg2} \]

**Figure 3**: Typing Rules for SLC

\[
\Gamma_{\text{var}} = \{(\text{var}' : T) \in \Gamma \mid \text{var}' \neq \text{var}\}
\]

\[
\begin{array}{c}
\Gamma () = \Gamma \\
\Gamma | g = \Gamma_g \\
\Gamma_{\langle g \rangle} = \Gamma_g \\
\Gamma_{\langle p_1, p_2 \rangle} = \langle \Gamma_{\langle p_1 \rangle} \rangle_{p_2} \\
\Gamma_{\{q_1, q_2 \}} = \langle \Gamma_{\langle q_1 \rangle} \rangle_{q_2}
\end{array}
\]

**Figure 4**: Definition of Environment Removed Patterns
(begin) \[ e : \text{int} \rightsquigarrow \{ e \mid \cdot \}\]
(lefl) \[ \{ (e_1, e_2) \mid e \} \rightsquigarrow \{ e_1 \mid (x \mapsto (x, e_2)) \mid e \}\]
(right) \[ \{ (e_1, e_2) \mid e \} \rightsquigarrow \{ e_2 \mid (x \mapsto (e_1, x)) \mid e \}\]
(pop) \[ \{ e \mid \overline{f} \mid e \} \rightsquigarrow \{ e \mid \overline{f} \mid e \}\]
(push) \[ \{ e \mid f \mid e \} \rightsquigarrow \{ e \mid f \mid e \}\]
(exc) \[ \{ e \mid \overline{e} \mid e \} \rightsquigarrow \{ e' \mid ([g] \Rightarrow e \uparrow g) \mid e \}\]
(βL) \[ \{ e \mid p \Rightarrow e' \mid e \} \rightsquigarrow \{ e' \mid [\mathcal{L}[p] \mapsto e] \mid e \}\]
(βR) \[ \{ e \mid p \Rightarrow e' \mid e \} \rightsquigarrow \{ e' \mid [\mathcal{R}[p] \mapsto e] \mid e \}\]
(βR) \[ \{ e \mid e' \ll q \mid e \} \rightsquigarrow \{ e \mid e' \mid [\mathcal{R}[q] \mapsto e] \}\]
(βL) \[ \{ e \mid e' \ll q \mid e \} \rightsquigarrow \{ e \mid e' \mid [\mathcal{L}[q] \mapsto e] \}\]
(prop) \[ \{ e \mid f \mid e \} \rightsquigarrow \{ e \mid f \mid e \}\]
(right) \[ \{ e \mid \{c_1, c_2\} \} \rightsquigarrow \{ e \mid \{c_1, y \mapsto y\} \mid c_2 \}\]
(lefl) \[ \{ e \mid \{c_1, c_2\} \} \rightsquigarrow \{ e \mid \{y, c_2 \mapsto y\} \mid c_1 \}\]
(end) \[ \{ n \mid \cdot \} \rightsquigarrow n\]

Figure 5: Non-Deterministic Small-Step Semantics of SLC

into a value of type \( +B \) using \( f \), and passes the result to \( c \). In other words, the function \( f \) transforms a
continuation of type \( \neg B \) to a continuation of type \( \neg A \), effectively acting as a function from \( \neg B \) to \( \neg A \).

The rules \( \text{TProg1} \) and \( \text{TProg2} \) at the bottom of Figure 3 are the typing rules for configurations. A
configuration is well-typed if all of its components are well-typed under an empty environment.

In this type system, the function \text{call/cc} has a function type \(( (A \to B) \to A) \supset A \) (what we call
Peirce’s Law).

2.4 Reduction Rules (Non-Deterministic)

In the pure lambda-calculus, reduction rules are written as a binary relation between terms because
it consists of only terms. SLC operates not only on expressions but also on continuations. Therefore,
reduction rules of SLC are written as a binary relation between configurations, \( \{ e \mid c \} \) or \( \{ e \mid f \mid c \} \).

Figure 5 shows the (non-deterministic) reduction rules of SLC.

In the standard lambda-calculus, reduction proceeds by decomposing the input into a redex and a
context, reducing the redex, and plugging the result into the context. In SLC, such decomposition and
plugging are described within the reduction rules. If the expression \( e \) in a configuration \( \{ e \mid c \} \) is an
application, its function part is popped from the application via \( \text{pop} \) and the focus of reduction moves
to the function part. In case we do not want to perform \( \beta \)-reduction of the popped function right now,
the rule \( \text{push} \) pushes the function to the continuation part and the argument is further reduced. In
case the function is not a value, on the other hand, the rule \( \text{exc} \) is used to exchange \( e \) and \( e' \) to move
the focus to \( e' \). After \( e' \) is reduced to \([f] \), the function \([g] \Rightarrow e \uparrow g \) brings it back into an application.

Similarly, \( \text{lefl} \) and \( \text{right} \) reduce the left and right elements of a pair, respectively.

SLC has two kinds of \( \beta \)-reduction, eager one (\( \beta R \)) and lazy one (\( \beta L \)), depending on how to handle
pattern matching. Eager \( \beta \)-reduction requires the argument to match the pattern at reduction time,
deconstructs it, and binds variables in the pattern to each component using \( \mathcal{R} \) defined in Figure 6. Lazy
one does not deconstruct the argument but binds variables in the pattern to code that deconstructs the
argument when the variables are used later (see the definition of \( \mathcal{L} \) in Figure 6). The former is required
to perform the real deconstruction of patterns, while the latter enables to defer pattern matching as long
as possible (like the irrefutable pattern in Haskell).

The reduction rules for continuations are defined completely symmetrically to those for expressions.
In particular, we can freely capture the current continuation using continuation abstractions, just as we
can freely receive the current expression using expression abstractions.

As an example of reduction, we can capture the current continuation in \( x \) by passing a function \([x \Rightarrow \circ] \) to \text{call/cc}. See Figure 7.
\[
\begin{align*}
\mathcal{R}[x] &\rightarrow e \\
\mathcal{R}[()] &\rightarrow e \\
\mathcal{R}[[g]] &\rightarrow [f] \\
\mathcal{R}[[p_1, p_2]] &\rightarrow (e_1, e_2) \\
\mathcal{R}[[q_1, q_2]] &\rightarrow (e_1, e_2) \\
\mathcal{R}[g] &\rightarrow [f] \\
\mathcal{R}[] &\rightarrow c \\
\mathcal{R}[y] &\rightarrow c \\
\mathcal{L}[x] &\rightarrow e \\
\mathcal{L}[()] &\rightarrow e \\
\mathcal{L}[[g]] &\rightarrow [e] \\
\mathcal{L}[[p_1, p_2]] &\rightarrow (e \uparrow (x_1, x_2 \Rightarrow x_1))[\mathcal{L}[p_2]] \\
\mathcal{L}[[q_1, q_2]] &\rightarrow (e \uparrow (x_1, x_2 \Rightarrow x_1))[\mathcal{L}[q_2]] \\
\mathcal{Z}[[g]] &\rightarrow [e] \\
\mathcal{Z}[] &\rightarrow c \\
\mathcal{Z}[y] &\rightarrow c \\
\end{align*}
\]

Figure 6: Definition of Eager and Lazy Substitution

\[
\begin{align*}
(x \Rightarrow e) | \text{call/cc} | c \\
\sim (x \Rightarrow e | ((g) \Rightarrow y \Leftarrow \uparrow g) \Downarrow y \Leftarrow y | e) \quad \text{(definition of call/cc)} \\
\sim (x \Rightarrow e | ((g) \Rightarrow [c \Leftarrow \downarrow g] \Downarrow c) \quad (\beta R) \\
\sim (x \Rightarrow e | [g] \Rightarrow [c \Leftarrow \downarrow g] \Downarrow c) \quad (\eta \nu \rho) \\
\sim ([c \Leftarrow \downarrow] \Downarrow (x \Rightarrow e) | e) \quad (\beta R) \\
\sim ([c \Leftarrow \downarrow] | x \Rightarrow e | c) \quad (\text{pop}) \\
\sim ([c \Leftarrow \downarrow] /x | c) \quad (\beta R)
\end{align*}
\]

Figure 7: Example Reduction of call/cc

There can be multiple rules that are applicable to the same configuration. Furthermore, the reduction rules are not Church-Rosser, that is, the result of evaluation can be different values. For example, the configuration \( 1 \uparrow (\bullet \Leftarrow y) | (x \Rightarrow 2) \downarrow \bullet \) has the following two different reductions:

\[
\begin{align*}
&\sim (1 \uparrow (\bullet \Leftarrow y) | (x \Rightarrow 2) \downarrow \bullet) \quad (\text{pop}) \quad \sim (1 \uparrow (\bullet \Leftarrow y) | (x \Rightarrow 2) \downarrow \bullet) \\
&\sim (1 \uparrow \bullet \Leftarrow y | (x \Rightarrow 2) \downarrow \bullet) \quad (\beta) \\
&\sim (1 \uparrow \bullet) \quad (\text{end}) \quad \sim (2 \uparrow \bullet) \quad (\beta) \\
&\sim 1 \quad (\text{end}) \quad \sim 2
\end{align*}
\]

This is not surprising. Without fixing the evaluation strategy, the result can be different. In a functional language, for example, \((\lambda x.1)(3/0)\) is reduced to 1 in CBN and an error in CBV. To recover uniqueness of evaluation, we introduce CBV evaluation strategy into SLC in Section 3 and CBN one in Section 4.

2.5 Properties of non-deterministic SLC

Without specifying the evaluation strategy, the small-step reduction semantics for non-deterministic SLC is sound with respect to the type system. Let \(\langle\rangle\) (possibly with a subscript) denote either a two-place configuration \( e | c \) or a three-place configuration \( e | f | c \). We can show the progress by simple case analysis and the preservation using the substitution lemma.

**Theorem 2.1 (Progress)**

If \(\vdash \langle\rangle_1\), then \(\langle\rangle_1 \sim \langle\rangle_2\) for some \(\langle\rangle_2\) or \(\langle\rangle_1 = \langle n | \bullet \rangle\) for some \(n\).
value \( v \) ::= \( n \) \( x \) \( (v, v) \) \( f \) \( [v \uparrow \text{inl}] \) \( [v \uparrow \text{inr}] \) \( [v \uparrow (g \downarrow c \leftarrow [g])] \)

expression \( e \) ::= \( v \) \( (e, e) \) \( e \uparrow f \)

function \( f \) ::= \( g \) \( p \rightarrow e \) \( c \leftarrow q \) \( c \)

continuation \( c \) ::= \( \bullet \) \( y \) \( \{ \} \) \( [c, c] \) \( f \downarrow c \) \( [f] \) \( [\text{inl} \downarrow c] \) \( [\text{inr} \downarrow c] \)

Figure 8: Syntax of CBV SLC

\[
\begin{align*}
\Gamma \vdash v : +A & \quad \text{TInl} \quad \Gamma \vdash c : \neg (A \lor B) \quad \text{TInl} \\
\Gamma \vdash [v \uparrow \text{lin}] : +(A \lor B) & \quad \text{TInr} \quad \Gamma \vdash [\text{inlr} \downarrow c] : \neg B \quad \text{TInr} \\
\Gamma \vdash v : +B & \quad \Gamma \vdash c : \neg B \quad \text{Tctx} \\
\Gamma \vdash [v \uparrow (g \downarrow c \leftarrow [g])] : +(A \land B) &
\end{align*}
\]

Figure 9: Additional Typing Rules for CBV SLC

Theorem 2.2 (Preservation)
Assume \( \vdash \langle \ldots \rangle_1 \). If \( \langle \ldots \rangle_1 \leadsto \langle \ldots \rangle_2 \), then \( \vdash \langle \ldots \rangle_2 \).

3 CBV SLC

The reduction rules in Figure 5 are non-deterministic. In this section, we introduce the CBV evaluation strategy into SLC. Under CBV, an argument is evaluated to a value before \( \beta \)-reduction. In SLC, it means that the evaluation goes from the expression side of the configuration \( \langle \ldots \rangle \), or from left to right of \( \langle \ldots \rangle \). To enforce this evaluation strategy, we first introduce a value into the syntax of SLC as in Figure 8. In addition to integers, variables, units, pairs of values, and higher-order functions, the value contains three frozen values that are expressions enclosed in brackets. In the non-deterministic setting, they are operationally the same as the expressions without brackets using the following interpretation:

\[
\begin{align*}
\text{inl} = y_1 \leftarrow \{y_1, y_2\} \\
\text{inr} = y_2 \leftarrow \{y_1, y_2\}
\end{align*}
\]

In the CBV setting, they are used to control the order of evaluation. Likewise, we have introduced two frozen continuations. The typing rules for the frozen values and frozen continuations are the same as those without brackets. They are summarized in Figure 9.

Currently, values include a function value of the form \([f]\). If we want to exclude this case from values, we could separate \( f \) into value functions and non-value functions, and include only the former into values.

Figure 10 shows the reduction rules for CBV SLC. The rule names with the subscript v indicate the rules that are changed from non-deterministic ones (Figure 5). The rule names with primes are the reduction rules for frozen values/continuations. The rules marked with * are ones directly obtained from Filinski’s denotational semantics. We will explain it in detail in Section 5.2. Rules in Figure 10 are restriction of the reduction rules for the non-deterministic SLC in a way the evaluation order is fixed to CBV: evaluation goes from left to right in the configuration \( \langle \ldots \rangle \). For example, the rule \((\beta R_v)\) requires that the argument is fully evaluated (and hence the use of eager pattern deconstruction \( \mathcal{R} \)); the rules \((\text{left}_v)\) and \((\text{right}_v)\) force the left-to-right evaluation order for pairs. Rules for frozen values/continuations first arise in \((\tau c)\) when a continuation appears as a function. In this case, we freeze \( v \) and \( c \) into \([v \uparrow (g \downarrow c \leftarrow [g])] \) and evaluate \( c' \). Here, we cannot remove the bracket (as in \((\tau c)\) in
The frozen value is destructed in \((e_1, e_2)\) because it would lead to non-termination in CBV: By temporarily freezing the application \((e_1, e_2)\) in CBV, the argument continuation to a continuation abstraction is not a value in general. In other words, an expression abstraction is evaluated in CBV but a continuation abstraction is evaluated \((\text{inr})\) only when the evaluation of \(e'\) is finished. Filinski called this frozen value \([v \uparrow (g \downarrow c \leftarrow [g])]\) a context.

Because the evaluation goes from left to right, an interesting asymmetry arises between expression abstractions and continuation abstractions: although the argument to an expression abstraction is always a value in CBV, the argument continuation to a continuation abstraction is not a value in general. In other words, an expression abstraction is evaluated in CBV but a continuation abstraction is evaluated in CBN.

Because the argument continuation in \((\text{inr})\) is not evaluated yet, we cannot use the eager pattern deconstruction here. Instead, we use the CBV lazy pattern deconstruction shown in Figure 11. Unlike \(\mathcal{L}\) (in Figure 6), \(\mathcal{L}_{c}\) introduces frozen injections \([\text{inl} \downarrow c]\) and \([\text{inr} \downarrow c]\) to defer the pattern deconstruction. They force the evaluation of continuations only when the pattern deconstruction is actually needed in \((\text{inr})\) or \((\text{pop})\).

### 3.1 Properties of CBV SLC

Since the CBV reduction semantics is a special case of the non-deterministic reduction semantics, the preservation holds for CBV reduction semantics. As for the progress, we can show by simple case analysis that the CBV reduction semantics satisfies the following stronger property:

\[
\begin{align*}
(b) & : \text{int} \rightarrow \{b \mid \bullet\} \\
(leftv) & : (e_1, e_2) \rightarrow (e_1 \mid (x \Rightarrow (x, e_2)) \downarrow c) \quad \text{if } e_1 \neq v \\
(rightv) & : (e_1, e_2) \rightarrow (e_2 \mid (x \Rightarrow (e_1, x)) \downarrow c) \quad \text{if } e_2 \neq v \\
(pop) & : e \uparrow f \rightarrow f \mid c \\
(pushv) & : e \mid f \rightarrow e \mid f \mid c \\
(exc) & : \langle v \mid c' \rangle \rightarrow \langle e' \mid ([g] \Rightarrow v \uparrow g) \downarrow c \rangle \\
(inl') & : \langle v \mid \text{inl} \rangle \rightarrow \langle v \rangle \\
(inr') & : \langle v \mid \text{inr} \rangle \rightarrow \langle v \rangle \\
(\text{contr}') & : (\langle v \mid \text{contr} \rangle) \rightarrow \langle v \mid f \rangle \\
(\text{inl}) & : \langle v \mid p \Rightarrow e' \mid c \rangle \rightarrow \langle e' \rangle \\
(\text{inr}) & : \langle v \mid \text{inr} \rangle \rightarrow \langle \downarrow v \rangle \\
(\text{pop}) & : \langle v \mid \text{pop} \rangle \\
(end) & : n \mid \bullet \rightarrow n
\end{align*}
\]
expression \( e ::= n \mid x \mid (\_ ) \mid ( e, e ) \mid e \mapsto f \mid [ f ] \mid [ e \mapsto f st ] \mid [ e \mapsto s nd ] \)

function \( f ::= g \mid p \Rightarrow e \mid e \Leftarrow q \mid \tau \mid \xi \)

continuation \( c ::= k \mid \{ c, c \} \mid f \downarrow k \)

covalue \( k ::= \bullet \mid y \mid \{ \} \mid \{ k, k \} \mid [ ] \mid \{ g \} \Rightarrow e \downarrow g \mid [ f s t \downarrow k ] \mid [ s nd \downarrow k ] \)

Figure 12: Syntax of CBN SLC

\[
\begin{align*}
\Gamma \vdash e : +( & ( A \land B ) ) \\
\Gamma \vdash [ e \mapsto f st ] : + A & \quad \text{TFst} \\
\Gamma \vdash k : \neg A & \quad \text{TFst} \\
\Gamma \vdash e : +( & ( A \land B ) ) \\
\Gamma \vdash [ e \mapsto s nd ] : + B & \quad \text{TSnd} \\
\Gamma \vdash k : \neg B & \quad \text{TSnd} \\
\Gamma \vdash e : + A & \quad \text{TCtx} \\
\Gamma \vdash [ [ g ] \Rightarrow k \downarrow g ] \Rightarrow e : \neg ( A \rightarrow B ) & \quad \text{TCtx}
\end{align*}
\]

Figure 13: Additional Typing Rules of CBN SLC

**Theorem 3.1** (The Uniqueness of Reduction in CBV SLC)
Under CBV, if \( \vdash \langle \ldots \rangle \), then there is exactly one reduction rule applicable to \( \langle \ldots \rangle \).

Furthermore, using the standard logical relation argument (as found in [9, Section 12]) tailored for SLC, we can show the following theorem:

**Theorem 3.2** (Termination of Evaluation in CBV SLC)
Under CBV, if \( \vdash e : + \text{int} \), then there exists a unique \( n \) such that \( e \leadsto^* n \).

4 CBN SLC

The CBN evaluation strategy evaluates expressions only when it is needed by its context. In other words, the evaluation goes from the continuation side, or from right to left of \( \langle \ldots \rangle \). Because of this duality, CBN SLC can be mechanically obtained by repeating the construction of CBV SLC in the previous section with the roles of expressions and continuations swapped: the evaluation goes from the continuation side of the configuration \( \langle \ldots \rangle \), or from right to left of \( \langle \ldots \rangle \). The result is a mirror image of CBV SLC. Furthermore, the same properties hold for CBN SLC.

Dually to CBV SLC, we first introduce a *covalue* (that is a value of continuations) into the syntax of SLC as in Figure 12. It is defined as completely dual notion of the value \( v \) in CBV SLC. Therefore the covalue contains three frozen covalues that are continuations enclosed in brackets. In the non-deterministic setting, they are operationally the same as the continuations without brackets using the following interpretation:

\[
\begin{align*}
\text{fst} & = ( ( x_1, x_2 ) \Rightarrow x_1 ) \\
\text{snd} & = ( x_1, x_2 ) \Rightarrow x_1
\end{align*}
\]

In the CBN setting, they are used to control the order of evaluation. Likewise, we have introduced two frozen expressions. Figure 14 shows typing rules for frozen covalues and frozen expressions.

Figure 14 shows the reduction rules for CBN SLC. The rule names with the subscript \( n \) indicate the rules that are changed from non-deterministic ones (Figure 5). The rule names with primes are the reduction rules for frozen expressions/covalues. The rules marked with \( * \) are the ones directly obtained from Filinski’s denotational semantics. We will explain it in detail in Section 6.2. Rules in Figure 14 are restriction of the reduction rules for the non-deterministic SLC in a way the evaluation order is fixed to CBN: evaluation goes from right to left in the configuration \( \langle \ldots \rangle \).
(begin) \hspace{1cm} e : \text{int} \rightsquigarrow (e \mid \text{•})
\star (pop_{\text{a}}) \hspace{1cm} \langle e \uparrow f \mid k \rangle \rightsquigarrow (e \mid f \mid k)
\star (exc_{\text{a}}) \hspace{1cm} \langle e \mid \text{exc} \mid k \rangle \rightsquigarrow (e' \mid ((g) \Rightarrow e \uparrow g) \downarrow k)
\star (fst) \hspace{1cm} \langle [e \uparrow fst] \mid k \rangle \rightsquigarrow (e \mid [fst \downarrow k])
\star (snd) \hspace{1cm} \langle [e \uparrow snd] \mid k \rangle \rightsquigarrow (e \mid [snd \downarrow k])
\star (\beta L_{\text{a}}) \hspace{1cm} \langle e \mid p \Rightarrow e' \mid k \rangle \rightsquigarrow (e'[\mathcal{L}_n[p] \Rightarrow e] \mid k)
\star (\beta R_{\text{a}}) \hspace{1cm} \langle e \mid e' \leftarrow q \mid k \rangle \rightsquigarrow (e \mid e'[\mathcal{R}[q] \Rightarrow k])
\star (\text{const}) \hspace{1cm} \langle [f] \mid ([g] \Rightarrow e \uparrow g) \downarrow k \rangle \rightsquigarrow (e \mid f \mid k)
\star (\text{std}) \hspace{1cm} \langle (e_1, e_2) \mid [\text{std} \downarrow k] \rangle \rightsquigarrow (e_2 \mid k)
\star (\text{fst}) \hspace{1cm} \langle (e_1, e_2) \mid [\text{fst} \downarrow k] \rangle \rightsquigarrow (e_1 \mid k)
\star (\text{exc}_{\text{a}}) \hspace{1cm} \langle e \mid e' \mid k \rangle \rightsquigarrow (e \uparrow (g \downarrow k \leftarrow [g]) \mid e')
\star (\text{push}_{\text{in}}) \hspace{1cm} \langle e \mid f \mid c \rangle \rightsquigarrow (e \uparrow f \mid c)
\star (\text{pop}) \hspace{1cm} \langle e \mid f \mid c \rangle \rightsquigarrow (e \uparrow f \mid c)
\star (\text{right}_{\text{a}}) \hspace{1cm} \langle e \mid \{c_1, c_2\} \rangle \rightsquigarrow (e \uparrow (\{c_1, y \} \Leftarrow y) \mid c_2)
\star (\text{left}_{\text{a}}) \hspace{1cm} \langle e \mid \{c_1, k_2\} \rangle \rightsquigarrow (e \uparrow (\{y, k_2 \} \Leftarrow y) \mid c_1)
\star (\text{end}) \hspace{1cm} \langle n \mid \text{•} \rangle \rightsquigarrow n

Figure 14: Small-Step Semantics for CBN SLC

\[ [\mathcal{L}_n[x] \mapsto e] = [e/x] \]
\[ [\mathcal{L}_n[\text{()}] \mapsto e] = \] \[ [\mathcal{L}_n[[g]] \mapsto e] = \mathcal{R}/g \]
\[ [\mathcal{L}_n[[p_1, p_2]] \mapsto e] = [\mathcal{L}_n[p_1] \mapsto [e \uparrow fst][\mathcal{L}_n[p_2] \mapsto [e \uparrow snd]]] \]

Figure 15: Definition of Lazy Substitution for CBN SLC

4.1 Properties of CBN SLC

Since the CBN reduction semantics is a special case of the non-deterministic reduction semantics, the preservation holds for CBN reduction semantics. As for the progress, we can show by simple case analysis that the CBN reduction semantics satisfies the following stronger property:

**Theorem 4.1** (The Uniqueness of Reduction in CBN SLC)
Under CBN, if \( \vdash (\ldots) \), then there is exactly one reduction rule applicable to \( (\ldots) \).

Furthermore, using the standard logical relation argument (as found in [9, Section 12]) tailored for SLC, we can show the following theorem:

**Theorem 4.2** (Termination of Evaluation in CBN SLC)
Under CBN, if \( \vdash e : \text{int} \), then there exists a unique \( n \) such that \( e \rightsquigarrow^* n \).

5 Functional Correspondence for CBV SLC

In this section, we show that the CBV small-step semantics of SLC presented in Section 3 corresponds to Filinski’s original definition of CBV SLC given as a denotational semantics. The method we use is the functional correspondence of interpreters and abstract machines developed by Danvy and his group [1, 4]: an abstract machine is a CPS-transformed defunctionalized interpreter. In our case, since Filinski’s denotational semantics is already in (a kind of) CPS, the small-step semantics (an abstract machine) can be obtained by defunctionalizing the denotational semantics.

Figure 16 shows Filinski’s denotational semantics for CBV SLC. Since the syntax of SLC consists of three kinds, the semantics also consists of three functions: \( E, C, \) and \( F \). In Filinski’s formulation, the patterns do not contain the function pattern. The semantic functions are not expressed in the symmetric manner, because SLC is mapped into the standard (asymmetric) lambda-calculus. In the semantics, \( \rho \)
\[ \begin{align*}
\text{Val} & = \text{Int} + \text{Unit}(+) + \text{Pair}(\text{Val} \times \text{Val}) + \text{In}_1(\text{Val}) + \text{In}_2(\text{Val}) + \\
\text{C} & = \text{Val} \to \text{Ans} \\
\text{Env} & = \text{Idc} \to (\text{Val} + \text{Cnt})
\end{align*} \]

\[ \begin{align*}
\mathcal{E} : c \to \text{Env} & \to \text{Cnt} \to \text{Ans} \\
\mathcal{E}[\cdot][\cdot][\cdot] & = \kappa n \\
\mathcal{E}[x][\cdot][\cdot] & = \text{let } \text{val}(v) = \rho x \text{ in } \kappa v \\
\mathcal{E}[(e_1, e_2)][\cdot][\cdot] & = \mathcal{E}[e_1][\rho(\lambda v_1. \mathcal{E}[e_2][\rho(\lambda v_2. \kappa \text{pair}(v_1, v_2)))] \\
\mathcal{E}[] & = \kappa \text{unit}() \\
\mathcal{E}[[c \downarrow f]][\cdot][\cdot] & = \mathcal{E}[e][\rho(\lambda v. \mathcal{F}[f][\rho v]) \\
\mathcal{E}[[f]][\cdot][\cdot] & = \kappa \text{closr}(\lambda \nu v. \mathcal{F}[f][\rho v])
\end{align*} \]

\[ \begin{align*}
\mathcal{C} : c \to \text{Env} & \to \text{Val} \to \text{Ans} \\
\mathcal{C}[\cdot][\cdot][\cdot] & = \text{let closr}(\kappa) = \rho y \text{ in } \kappa v \\
\mathcal{C}[(e_1, e_2)][\cdot][\cdot] & = \text{case } v \text{ of } \text{in}_1(v') : \mathcal{C}[e_1][\rho v'] | \text{in}_2(v') : \mathcal{C}[e_2][\rho v'] \text{ esac} \\
\mathcal{C}[] & = \text{case } v \text{ of } \text{esac} \\
\mathcal{C}[f \downarrow e][\cdot][\cdot] & = \mathcal{F}[f][\rho v(\lambda \nu v'. \mathcal{C}[e][\rho v']) \\
\mathcal{C}[[f]][\cdot][\cdot] & = \text{let contx}(v', \kappa) = v \text{ in } \mathcal{F}[[f]][\rho v'] \kappa
\end{align*} \]

\[ \begin{align*}
\mathcal{F} : f \to \text{Env} & \to \text{Val} \to \text{Cnt} \to \text{Ans} \\
\mathcal{F}[\cdot][\cdot][\cdot][\cdot] & = \mathcal{E}[e][\lambda v. \kappa \text{in}_1(v)] \\
\mathcal{F}[e \Rightarrow Y][\cdot][\cdot][\cdot] & = \mathcal{C}[e][\lambda \kappa Y \text{ in } \kappa v] \\
\mathcal{F}[[f]][\cdot][\cdot][\cdot] & = \mathcal{E}[e][\rho(\lambda v'. \text{let closr}(h) = v' \text{ in } h \text{ v } \kappa) \\
\mathcal{F}[[f]][\cdot][\cdot][\cdot] & = \mathcal{C}[e][\rho \text{contx}(v, \kappa)]
\end{align*} \]

\[ \begin{align*}
\mathcal{X} : X \to \text{Val} & \to \text{Env} \to \text{Env} \\
\mathcal{X}[x][\cdot][\cdot][\cdot] & = \rho x \text{ in } \text{val}(v) \\
\mathcal{X}[[X]][\cdot][\cdot][\cdot] & = \text{let unit()} = v \text{ in } \rho \\
\mathcal{X}[[X_1, X_2]][\cdot][\cdot][\cdot] & = \text{let pair}(v_1, v_2) = v \text{ in } \mathcal{X}[[X_1]][v_1](\mathcal{X}[[X_2]][v_2]) \rho
\end{align*} \]

\[ \begin{align*}
\mathcal{Y} : Y \to \text{Cnt} & \to \text{Env} \to \text{Env} \\
\mathcal{Y}[y][\cdot][\cdot][\cdot] & = \rho y \text{ in } \text{closr}(\kappa) \\
\mathcal{Y}[[Y]][\cdot][\cdot][\cdot] & = \rho \\
\mathcal{Y}[[Y_1, Y_2]][\cdot][\cdot][\cdot] & = \rho \kappa \text{ in } \rho \kappa \text{ in } \rho \kappa
\end{align*} \]

Figure 16: Filinski’s Denotational Semantics for CBV SLC

represents an environment, \( v \) represents a value (the result of evaluation), and \( \kappa \) represents a semantic continuation. Filinski introduces a domain for each value type (e.g., \( \text{Pair} \)) together with a constructor for it (in lower case letter, e.g., \( \text{pair} \)).

We will not go into details of this denotational semantics. Rather, we regard this semantics as a definitional interpreter for SLC and defunctionalize it. Defunctionalization, introduced by Reynolds [10], is a whole-program transformation to remove higher-order functions. Every higher-order function in a program is replaced with a unique constructor whose arguments are free variables of the higher-order function. When the higher-order function is applied, a newly introduced apply function \( \mathcal{A} \) is used instead, which, given the actual argument, will execute the body of the higher-order function. This way, all the higher-order functions are replaced with first-order data.

### 5.1 Defunctionalization

We defunctionalize two kinds of higher-order functions in Figure 16: continuations (\( \kappa \) of type \( \text{Cnt} \)) and closures (the argument of \( \text{closr} \)).\(^3\) The result of defunctionalization is found in the upper left of Figure 17.

\(^3\)The latter is sometimes called closure conversion.
Defunctionalized Semantics

\[ E : e \rightarrow \text{Env} \rightarrow \text{Cnt} \rightarrow \text{Ans} \]

\[ E[n]\rho v = \mathbb{A} \land n \]
\[ E[x]\rho v = \text{let val}(v) = \rho x \text{ in } \mathbb{A} \land v \]
\[ E[(e_1, e_2)]\rho v = E[e_1] \rho (\mathbb{E}p(e_2, \rho, \kappa)) \]
\[ E[])\rho v = \mathbb{A} \land \text{unit}() \]
\[ E[e \mid f]\rho v = E[e] \rho (\mathbb{E}p(f, \rho, \kappa)) \]
\[ E[\mathbb{F}][\rho] \mathbb{P} = \mathbb{A} \land \text{Clos}(f, \rho) \]

\[ C : c \rightarrow \text{Env} \rightarrow \text{Val} \rightarrow \text{Ans} \]

\[ C[y]\rho v = \text{let cnt}(\kappa) = \rho y \text{ in } \mathbb{A} \land v \]
\[ C[c_1, c_2] \rho (\text{in}_1(v) = C[c_1] \rho v) \]
\[ C[c_1, c_2] \rho (\text{in}_2(v) = C[c_2] \rho v) \]
\[ C[] \rho v = \text{case } v \text{ of esac} \]
\[ C[f \mid c] \rho v = \mathbb{F}[f] \rho v (\mathbb{C}pp(c, \rho)) \]
\[ C[\mathbb{F}][\rho] \text{cont}(v, \kappa) = F[\mathbb{F}]\rho v \kappa \]

\[ F : f \rightarrow \text{Env} \rightarrow \text{Val} \rightarrow \text{Cnt} \rightarrow \text{Ans} \]

\[ F[X \Rightarrow e] \rho v k = E[e] \rho (\mathbb{C}pp(X) \rightarrow v) \rho k \]
\[ F[e \Leftarrow Y] \rho v k = C[e] \rho (\mathbb{E}p(Y) \rightarrow k) \rho v \]
\[ F[e] \rho v k = E[e] \rho (\mathbb{O}penn(v, \kappa)) \]
\[ F[\mathbb{F}][\rho] \text{cont}(v, \kappa) = F[f] \rho v k \]

\[ A : \text{Cnt} \rightarrow \text{Val} \rightarrow \text{Ans} \]

\[ A(\mathbb{E}p(e_2, \rho, \kappa)) v_1 = C[e_2] \rho (\mathbb{E}p_2(v_1, \kappa)) \]
\[ A(\mathbb{E}p_2(v_1, \kappa)) v_2 = \mathbb{A} \land \text{pair}(v_1, v_2) \]
\[ A(\mathbb{E}pp(f, \rho, \kappa)) v = F[\mathbb{F}]\rho v k \]
\[ A(\mathbb{C}pp(c, \rho)) v = C[c] \rho v \]
\[ A(\mathbb{O}penn(v, \kappa)) \text{Clos}(f, \rho) = F[f] \rho v k \]
\[ A(\text{ln}(\kappa)) v = \mathbb{A} \land \text{in}_1(v) \]
\[ A(\text{ln}(\kappa)) v = \mathbb{A} \land \text{in}_2(v) \]
\[ A \text{Init} n = n \]

\[ X : X \rightarrow \text{Val} \rightarrow \text{Env} \rightarrow \text{Env} \]

\[ [X[X]] \rightarrow v \rho = \rho[x \rightarrow \text{val}(v)] \]
\[ [X[]] \rightarrow \text{unit}() \rho = \rho \]
\[ [X[(X_1, X_2)]] \rightarrow \text{pair}(v_1, v_2) \rho = [X[X_1] \rightarrow v_1][X[X_2] \rightarrow v_2] \rho \]

\[ Y : Y \rightarrow \text{Cnt} \rightarrow \text{Env} \rightarrow \text{Env} \]

\[ [Y[Y]] \rightarrow \kappa \rho = \rho[y \rightarrow \text{cnt}(\kappa)] \]
\[ [Y[]] \rightarrow \kappa \rho = \rho \]
\[ [Y[(Y_1, Y_2)]] \rightarrow \kappa \rho = [Y[Y_1] \rightarrow \text{ln}(\kappa)][Y[Y_2] \rightarrow \text{ln}(\kappa)] \rho \]

Figure 17: Defunctionalized Semantics and Corresponding Abstract Machine (CBV)
the first-order data as shown in Figure 18. The translation is mechanical: whenever \( \lambda \) is used in Figure 16, it is replaced with a first-order data and the corresponding clause is added to the apply function \( A \). For example, \( \lambda v. F[\ell]/>v_{\kappa} \) appearing in \( E \ell \) of Figure 16 is translated to \( Epp(f, \rho, \kappa) \) where the free variables of \( \lambda v. F[\ell]/p_{v_{\kappa}} \) becomes the arguments to \( Epp \). The corresponding clause is added to the definition of \( A \):

\[
A (Epp(f, \rho, \kappa)) \triangleright v = F[\ell]/p_{v_{\kappa}}
\]

so that the original body of \( \lambda v. F[\ell]/p_{v_{\kappa}} \) is executed. Since all the \( \kappa \)'s now become a first-order data, its application is replaced with a call to the apply function \( A \). For example, \( \kappa n \) in \( E[n]/p_{\kappa} \) in Figure 16 is translated to \( A \kappa n \).

5.2 Rewriting to Abstract Machine Style

Because the four semantic functions, \( E, C, F, \) and \( A \), in the defunctionalized interpreter are mutually tail-recursive, the resulting interpreter can be directly regarded as an abstract machine. The right column of Figure 17 shows the corresponding abstract machine. It is obtained by mechanically changing the notation from \( E[v]/p_{\kappa}, C[v]/p_{\rho}, F[\ell]/p_{v_{\kappa}} \), and \( A \kappa v \), to \( \langle v \mid [v]p_{\kappa} \rangle, \langle v \mid [v]p_{\rho} \rangle, \langle v \mid [\ell]p_{\kappa} \rangle, \) and \( \langle v \mid \kappa \rangle \), respectively.

From this abstract machine, we can derive our small-step reduction semantics by two more simple transformations: replacing the environment with substitution and rewriting defunctionalized first-order data in SLC syntax.

The abstract machine in Figure 17 uses an environment to realize substitution. The role of an environment is to defer the substitution until the substituted variable is found. (As a slogan, “an environment is a lazy substitution.”) We can simply remove all the environments (and semantic brackets) by performing substitution whenever the environment is extended, namely, at the first two rules for \( F \) in Figure 17. With this transformation, the first two rules for \( F \) becomes identical to the corresponding rules ((\( \beta R \)) and ((\( \beta L \))) in Figure 10. After removing the environments, all the rules for variables become useless, because they will never be used. Furthermore, the rule for a number becomes useless, because it now becomes an identity transition: \( \langle n \mid \kappa \rangle \sim \langle n \mid \kappa \rangle \).

The second transformation is to rewrite defunctionalized first-order data in SLC syntax. Rather than writing \( Epp(f, \kappa) \), for example, we can instead write \( f \downarrow \kappa \), because the rule for \( Epp(f, \kappa) \) is:

\[
\langle v \mid Epp(f, \kappa) \rangle \sim \langle v \mid f \mid \kappa \rangle
\]

By writing \( Epp(f, \kappa) \) as \( f \downarrow \kappa \), the rule becomes identical to \( \langle \rho_{f_{\kappa}} \rangle \). Likewise, we change the notation for all the first-order data as shown in Figure 18.

With the above two transformations, all the rules marked with * in Figure 17 coincide with the marked rules in the CBV small-step reduction semantics in Figure 10. The rules with \( \diamond \) do not coincide with the rules in Figure 10, but we can confirm that they can all be simulated by one or more reduction steps of Figure 10. Furthermore, since \( \mathcal{X} \) and \( \mathcal{Y} \) are transformed to \( \mathcal{R} \) and \( \mathcal{Z} \) (except for function patterns), we conclude that the CBV small-step semantics in Figure 10 correctly implements Filinski’s SLC.


Figure 18: Term Transformation for CBV Derivation
\[\begin{align*}
\text{Val} &= \text{Cnt} \rightarrow \text{Ans} \\
\text{Cnt} &= \text{Bcont} + \text{Zero} + \text{Case} (\text{Cnt} \times \text{Cnt}) + \text{Pr}_1 (\text{Cnt}) + \text{Pr}_2 (\text{Cnt}) + \text{Cntx} (\text{Val} \rightarrow \text{Cnt} \rightarrow \text{Ans}) + \text{Closr} (\text{Val} \times \text{Cnt}) \\
\text{Env} &= \text{Id}e \rightarrow \text{Val} + \text{Cnt} \\
\end{align*}\]

\[
\mathcal{E} : c \rightarrow \text{Env} \rightarrow \text{Cnt} \rightarrow \text{Ans} \\
\mathcal{E}[\text{n}]_{\rho} = \text{let } \text{bcont} = k \text{ in } n \\
\mathcal{E}[\text{x}]_{\rho} = \text{let } \text{val}(\nu) = \rho \text{ in } \nu \ k \\
\mathcal{E}[\text{e}_\text{1}, \text{e}_\text{2}]_{\rho} = \text{case } k \text{ of } \text{pr}_1(k') : \mathcal{E}[\text{e}_\text{1}]_{\rho} k' | \text{pr}_2(k') : \mathcal{E}[\text{e}_\text{2}]_{\rho} k' \\
\mathcal{E}[\text{e}]_{\rho} = \text{case } k \text{ of } \text{esac} \\
\mathcal{E}[\text{f}]_{\rho} = \mathcal{F}[\text{f}] \rho (\lambda k'. \mathcal{E}[\text{e}]_{\rho} k') k \\
\mathcal{E}[\text{e}]_{\rho} = \text{let } \text{closr}(\nu, k') = k \text{ in } \mathcal{F}[\text{f}]_{\rho} k'
\]

\[
\mathcal{C} : c \rightarrow \text{Env} \rightarrow \text{Val} \rightarrow \text{Ans} \\
\mathcal{C}[\text{y}]_{\rho} = \text{let } \text{cnt}(k) = \rho \text{ in } \nu \ k \\
\mathcal{C}[\text{e}_\text{1}, \text{e}_\text{2}]_{\rho} = \mathcal{C}[\text{e}_\text{2}]_{\rho} (\lambda k_1, \nu. \text{case}(k_1, k_2)) \\
\mathcal{C}[\{}\}_{\rho} = \nu \text{ zero()} \\
\mathcal{C}[\text{f}]_{\rho} = \mathcal{C}[\text{e}]_{\rho} (\lambda k. \mathcal{F}[\text{f}]_{\rho} k) \\
\mathcal{C}[\text{f}]_{\rho} = \nu \text{ contx} (\lambda \nu'. k. \mathcal{F}[\text{f}]_{\rho} k)
\]

\[
\mathcal{F} : f \rightarrow \text{Env} \rightarrow \text{Val} \rightarrow \text{Cnt} \rightarrow \text{Ans} \\
\mathcal{F}[\text{p} \Rightarrow \text{e}]_{\rho} = \mathcal{E}[\text{e}] (\lambda x. \nu \Rightarrow \rho) k \\
\mathcal{F}[\text{c} \Leftarrow \text{Y}]_{\rho} = \mathcal{C}[\text{y}] (\lambda y. \nu) \nu \\
\mathcal{F}[\text{e}]_{\rho} = \mathcal{E}[\text{e}]_{\rho} \text{ contx}(\nu, k) \\
\mathcal{F}[\text{e}]_{\rho} = \mathcal{C}[\text{e}]_{\rho} (\lambda k'. \text{let } \text{contx}(h) = t \text{ in } h \nu k')
\]

\[
\mathcal{X} : p \rightarrow \text{Val} \rightarrow \text{Env} \rightarrow \text{Env} \\
\mathcal{X}[\text{x}]_{\rho} = \rho(x \Rightarrow \text{val}(\nu)) \\
\mathcal{X}[\{}\]_{\rho} = \rho \nu \\
\mathcal{X}[\text{e}_\text{1}, \text{e}_\text{2}]_{\rho} = \mathcal{X}[\text{e}_\text{1}]_{\rho} (k. \text{nu} \text{ pr}_1(k)) (\mathcal{X}[\text{e}_\text{2}]_{\rho} \Rightarrow \lambda k. \nu \text{ pr}_2(k) \rho)
\]

\[
\mathcal{Y} : q \rightarrow \text{Cnt} \rightarrow \text{Env} \rightarrow \text{Env} \\
\mathcal{Y}[\text{y}]_{\rho} = \rho(y \Rightarrow \text{cnt}(k)) \\
\mathcal{Y}[\{}\]_{\rho} = \rho \nu k \\
\mathcal{Y}[\text{e}_\text{1}, \text{e}_\text{2}]_{\rho} = \text{let } \text{case}(c_1, c_2) = k \text{ in } \mathcal{Y}[\text{e}_\text{1}]_{\rho} c_1 | \mathcal{Y}[\text{e}_\text{2}]_{\rho} c_2 \rho
\]

Figure 19: Filinski's Denotational Semantics for CBN SLC

### 6 Functional Correspondence for CBN SLC

Filinski also presented denotational semantics for CBN SLC. Using the same method presented in the previous section, we can obtain the CBN small-step semantics. Although denotational semantics for CBV SLC and CBN SLC look quite different (because they are encoded in a standard non-symmetric lambda-calculus), the present results confirm that they are actually dual to each other. In this section, we show that the CBN small-step semantics of SLC presented in Section 4 corresponds to Filinski’s original definition of CBN SLC given as a denotational semantics.

Figure 19 shows denotational semantics of Filinski’s CBN SLC. In the semantics, \( k \) represents covalues (the result of evaluation), and \( \nu \) represents semantic values (that is not a result). Filinski introduces a domain for each covalue type (e.g., Case) together with a constructor for it (in lower case letter, e.g., case).
Defunctionalized Semantics

\[ E : e \rightarrow Env \rightarrow Cnt \rightarrow Ans \]
\[ E[n]_{\rho} \text{ becont } = n \]
\[ E[x]_{\rho}pk = \text{ let val}(v) = \rho x \text{ in } A \nu k \]
\[ E[(e_1, e_2)]_{\rho} pr_1(k) = E[e_1]_{\rho}pk \]
\[ E[(e_1, e_2)]_{\rho} pr_2(k) = E[e_2]_{\rho}pk \]
\[ E[()]_{\rho}pk = \text{ case } k \text{ of esac} \]
\[ E[c \mapsto f]_{\rho}pk = \mathcal{F}[f]_{\rho}(\text{Epp}(e, \rho))k \]
\[ E[\mathcal{F}[f]]_{\rho} closr(a, c) = \mathcal{F}[f]_{\rho}p_{ac} \]

\[ C : c \rightarrow Env \rightarrow Val \rightarrow Ans \]
\[ C[y]_{\rho}wv = \text{ let cnt}(k) = \rho y \text{ in } A \nu k \]
\[ C[(e_1, e_2)]_{\rho}wv = C[e_2]_{\rho}(\text{Cp2}(c_1, \rho, \nu)) \]
\[ C[\{\}]_{\rho}wv = A \nu \nu \text{ zero}(\rho) \]
\[ C[f \mapsto c]_{\rho}wv = C[c]_{\rho}(\text{Cp}(f, \rho, \nu)) \]
\[ C[\mathcal{F}[f]]_{\rho}wv = A \nu \text{ Contx}(f, k) \]

\[ A : Val \rightarrow Cnt \rightarrow Ans \]
\[ A(\text{Epp}(e, \rho), k) = C[e]_{\rho}pk \]
\[ A(\text{Cp2}(c_1, \rho, \nu), k_2) = C[e_1]_{\rho}(\text{Cp1}(k_2, \nu)) \]
\[ A(\text{Cp1}(k_2, \nu), k_1) = A \nu \text{ case}(k_1, k_2) \]
\[ A(\text{Cp}(f, \rho, \nu), k) = \mathcal{F}[f]_{\rho}pk \]
\[ A(\text{Plug}(\nu, k), \text{Contx}(f, \rho)) = \mathcal{F}[f]_{\rho}wv \]
\[ A(\text{Fst}(\nu), k) = A \nu \text{ pr}_1(k) \]
\[ A(\text{Snd}(\nu), k) = A \nu \text{ pr}_2(k) \]

\[ \mathcal{X} : p \rightarrow Val \rightarrow Env \rightarrow Env \]
\[ [X[x]]_{\rho} = \rho[x \mapsto \text{val}(v)] \]
\[ [X[]]_{\rho} = \rho \]
\[ [X[[p_1, p_2]]]_{\rho} = [X[p_1]]_{\rho} \rightarrow \text{Fst}(\nu)([X[p_2]]_{\rho} \rightarrow \text{Snd}(\nu))_{\rho} \]

\[ \mathcal{Y} : q \rightarrow Cnt \rightarrow Env \rightarrow Env \]
\[ [Y[y]]_{\rho} = \rho[y \mapsto \text{cnt}(\nu)] \]
\[ [Y[]]_{\rho} = \rho \]
\[ [Y[[q_1, q_2]]]_{\rho} = \text{case}(k_1, k_2)_{\rho} = [Y[q_1]]_{\rho} \mapsto k_1 \rightarrow [Y[q_2]]_{\rho} \mapsto k_2_{\rho} \]

Figure 20: Defunctionalized Semantics and Corresponding Abstract Machine (CBN)
6.1 Defunctionalization

We defunctionalize two kinds of higher-order functions in Figure 19: values (ν of type Val) and contexts (the argument of contx). The result of defunctionalization is found in the upper left of Figure 20. The translation is mechanical and dual to the CBV derivation in Section 5.1. For example, though we have defunctionalized a semantic continuation for e↑f in Section 5.1, here, we need to defunctionalize a semantic value for f↓c. We translate the semantic value λk.\([\text{F}][f]\rho\nu k\) to \(\text{Cpp}(f,\rho,\nu)\). The corresponding clause is added to the definition of A:

\[ A(\text{Cpp}(f,\rho,\nu)) k = \text{F}[f]\rho\nu k \]

6.2 Rewriting to Abstract Machine Style

Because the four semantic functions, E, C, F, and A, in the defunctionalized interpreter are mutually tail-recursive, the resulting interpreter can be directly regarded as an abstract machine. The right column of Figure 20 shows the corresponding abstract machine. It is obtained by mechanically changing the notation from \(E[e]pk, C[c]\rho\nu, F[f]pk,\) and \(A\nu k,\) to \(\langle [e]\rho | k \rangle, \langle \nu | [e]\rho \rangle, \langle \nu | [f]\rho | k \rangle,\) and \(\langle \nu | k \rangle,\) respectively.

From this abstract machine, we can derive our small-step reduction semantics by two more simple transformations: replacing the environment with substitution and rewriting defunctionalized first-order data in SLC syntax. First, we simply remove all the environments (and semantic brackets) by performing substitution whenever the environment is extended. After removing the environments, all the rules for variables become useless, because they will never be used. Secondly, we change the notation for all the first-order data as shown in Figure 21.

With the above two transformations, all the rules marked with * in Figure 20 coincide with the marked rules in the CBN small-step reduction semantics in Figure 14. The rules with ♦ do not coincide with the rules in Figure 14, but we can confirm that they can all be simulated by one or more reduction steps of Figure 14. Furthermore, since \(X\) and \(Y\) are transformed to \(L_n\) and \(R\) (except for function patterns), we conclude that the CBN small-step semantics in Figure 14 correctly implements Filinski’s SLC.

7 Future Direction

In this paper, we have presented a small-step reduction semantics for Filinski’s symmetric lambda calculus (SLC). Now that we obtained a small-step reduction semantics for SLC, we can express and compare various other calculi in terms of SLC. Our preliminary work shows that we can naturally encode Felleisen’s C operator as well as λµ-calculus into SLC [11]. We are also interested in if delimited continuations can be introduced into the SLC framework.
References


Functional Derivation of Small-Step Semantics for Symmetric Lambda Calculus (SLC)

Kenichi Asai
joint work with Yayoi Ueda
Ochanomizu University (Tokyo, Japan)
January 10, 2011

What is Symmetric Lambda Calculus (SLC)?

Symmetric extension of λ-calculus proposed by Filinski in 1989

- Two kinds of duality:
  - **Expressions** produce data. **CBV** expressions first
  - **Functions** transform data.
  - **Continuations** consume data. **CBN** continuations first
  \[ 1 \rightarrow A \rightarrow B \rightarrow 0 \]

- Given: denotational semantics, translation to SCL.
Good calculus for dealing with continuations.

SLC: Syntax

A configuration is either \( \langle e \mid c \rangle \) or \( \langle e \mid f \mid c \rangle \), where:

- **Expression**: \( e ::= o_T \mid x \mid (e, e) \mid [f] \mid e \uparrow f \)
- **Function**: \( f ::= g \mid x \Rightarrow e \mid (x_1, x_2) \Rightarrow e \mid [g] \Rightarrow e \mid e \)
- **Continuation**: \( c ::= \bullet_T \mid y \mid (e, c) \mid [f] \mid f \downarrow c \)

Example:

\[ \begin{align*}
\langle & 1 \uparrow x_1 \Rightarrow x_1 + 2 \uparrow x_2 \Rightarrow x_2 \ast 4 \mid \bullet_{\text{int}} \rangle \\
\sim & \langle 1 \uparrow x_1 \Rightarrow x_1 + 2 \mid x_2 \Rightarrow x_2 \ast 4 \mid \bullet_{\text{int}} \rangle \\
\sim & \langle 1 \mid x_1 \Rightarrow x_1 + 2 \mid x_2 \Rightarrow x_2 \ast 4 \downarrow \bullet_{\text{int}} \rangle \\
\sim & \langle 1 \mid x_1 \Rightarrow x_1 + 2 \mid x_2 \Rightarrow x_2 \ast 4 \downarrow \bullet_{\text{int}} \rangle \\
\sim & \langle 1 \mid 2 \mid x_2 \Rightarrow x_2 \ast 4 \downarrow \bullet_{\text{int}} \rangle \\
\sim & \langle 3 \mid x_2 \Rightarrow x_2 \ast 4 \downarrow \bullet_{\text{int}} \rangle \\
\sim & \langle 3 \mid x_2 \Rightarrow x_2 \ast 4 \downarrow \bullet_{\text{int}} \rangle \\
\sim & \langle 12 \mid \bullet_{\text{int}} \rangle
\end{align*} \]
**Functional Derivation of Small-Step Semantics for Symmetric Lambda Calculus (SLC)**

Kenichi Asai joint work with Yayoi Ueda
Ochanomizu University (Tokyo, Japan)

**Two Semantics**

- **Denotational Semantics**
- **Small-Step Semantics**

Are they the same? — Yes (…well, almost).

We can connect them via

functional correspondence [Danvy].
Functional Correspondence

Interpreter (big-step semantics)
⇓ CPS transformation
CPS interpreter
⇓ Defunctionalization
Abstract machine (small-step semantics)

Subtle Point: CBN pair destruction

In Haskell:

\[
f \ (x, \ y) = 0 \quad // \ \text{refutable pattern}
g \ ~ (x, \ y) = 0 \quad // \ \text{irrefutable pattern}
\]

*Main> undefined
*** Exception: Prelude.undefined
*Main> f undefined
*** Exception: Prelude.undefined
*Main> g undefined
0
*Main>
Subtle Point: CBN pair destruction

\( \langle e \mid (x_1, x_2) \Rightarrow e' \mid c \rangle \)

- Should we evaluate \( e \) to a pair?
  \( \langle e \mid (x_1, x_2) \Rightarrow e' \mid c \rangle \sim \langle e \mid [(x_1, x_2) \Rightarrow e' \downarrow c] \rangle \)
  \( \langle (e_1, e_2) \mid [(x_1, x_2) \Rightarrow e' \downarrow c] \rangle \sim \langle e'[e_i/x_i] \mid c \rangle \)

- Should we bind \( x_i \) to \([e \uparrow \pi_i] \)?
  \( \langle e \mid (x_1, x_2) \Rightarrow e' \mid c \rangle \sim \langle e'[\{e \uparrow \pi_i]/x_i] \mid c \rangle \)
  \( \langle [e \uparrow \pi_i] \mid c \rangle \sim \langle e \mid [\pi_i \downarrow c] \rangle \)

Summary

- Small-step semantics for SLC is shown.
- Its CBV/CBN variants coincide with the original CBV/CBN denotational semantics.
- The original SLC uses irrefutable patterns.

- Relationship to other calculi?
  (\( \lambda\mu\tilde{\mu} \)-calculus, Dual calculus, etc.)
- Delimited continuations?
Report on a Self-applicable Online Partial Evaluator for a Recursive Flowchart Language

Robert Glück

DIKU, Department of Computer Science, University of Copenhagen,
DK-2100 Copenhagen, Denmark

Summary

We describe the design and implementation of a self-applicable online partial evaluator for a flowchart language with recursive calls. Self-application of the online partial evaluator converts interpreters into compilers and produces an online compiler generator, all of which are as efficient as those known from the offline partial evaluation literature (e.g., [1, 6, 8–11]). This result is remarkable because it is assumed that online techniques unavoidably lead to inefficient and overgeneralized program generators [8]. The online partial evaluator does not require partial evaluation techniques that are stronger than those already known. Instead it requires a reorganization of the algorithm to achieve successful self-application according to all three Futamura projections [4].

Offline partial evaluation was invented in 1984 [9] specifically to solve the problem of self-application and to perform all three Futamura projections. Even though the first partial evaluators were all online and in spite of a number of attempts during the last decades, the self-application of an online partial evaluator has been an open question. The purpose of this investigation is not to determine which line of partial evaluation is better, but to show how the problem can be solved. The solution sought is a specialization algorithm that is (i) complete, (ii) purely online, that is, without binding-time analysis prior to specialization, and (iii) fully self-applicable in that all three Futamura projections yield efficient residual programs (e.g., compilers, compiler generators). The online partial evaluator that we developed satisfies all three criteria.

The offline partial evaluator mix for a flowchart language described by Gomard and Jones [6] is well suited as a reference for our online partial evaluator because mix does not follow the local binding-time annotations of a subject program, but instead bases its specialization decisions on a fixed global division of the program variables into static and dynamic, this division being precomputed by a monovariant binding-time analysis. An important advantage of using a flowchart language is that partial evaluation for flowchart languages is very well documented in the literature (e.g., [2, 3, 6–8]), which should make our results easily accessible and comparable. Flowchart languages also represent the core of many realistic imperative languages.

Our online partial evaluator presented differs from mix in two important ways: (1) the division of program variables is maintained as an updatable set of variable names at specialization time, and
recursive polyvariant specialization is performed instead of the traditional iterative version using an accumulating parameter (the pending list) [5].

Although the design of the self-applicable online partial evaluator is based on a number of known techniques, by combining them in a new way this synergetic effect can be produced.

Successful self-application of the online partial evaluator according to all three Futamura projections is demonstrated, amongst other things, by converting an interpreter for Turing machines into a compiler, an Ackermann program into a generating extension, and the partial evaluator itself into an online compiler generator. Self-application of the online partial evaluator can yield generating extensions that are more optimizing than those produced by the offline partial evaluator mix. The generating extension of the Ackermann program for example can precompute the function, thereby producing more optimized residual programs.

We believe that the online partial evaluator for the flowchart language presented here provides the clearest solution to date.

References

Overview

- Reversible Turing machines
- Universality for RTMs
- A first principles URTM

Turing machines

**Definition (Turing machine)**

A TM $T$ is a tuple $(Q, \Sigma, \delta, b, q_s, q_f)$ where $Q$ is a finite set of states, $\Sigma$ is a finite set of tape symbols, $b \in \Sigma$ is the blank symbol,

$$\delta \subseteq (Q \times ([\Sigma \times \Sigma] \cup \{\leftarrow, \downarrow, \rightarrow\}) \times Q)$$

is a partial relation defining the transition relation, $q_s \in Q$ is the starting state, and $q_f \in Q$ is the final state. There must be no transitions leading out of $q_f$ nor into $q_s$. 
**Triple format for transition rules**

\[ \delta \subseteq (Q \times ([\Sigma \times \Sigma] \cup \{\bot, \downarrow, \rightarrow\}) \times Q) \]

The form of a **triple format rule** in \( \delta \) is either:

- a **symbol rule** \((q, (s, s'), q')\) where \(s, s' \in \Sigma\), or
- a **move rule** \((q, d, q')\) where \(d \in \{\leftarrow, \downarrow, \rightarrow\}\).

(Triples can be converted to the usual quintuples, and vice versa. We use it for convenience.)

---

**Reversible Turing machines (RTMs)**

**Intuition:** RTMs are those where each configuration has a unique successor and predecessor configuration.

**Definition (Reversible Turing machine)**

A TM \( T \) is **reversible** iff it is (locally) forward and backward deterministic.

---

**Local forward/backward determinism**

**Definition (Local forward determinism)**

A TM \( T \) is **local forward deterministic** iff for any distinct pair of triples \((q_1, a_1, q'_1) \in \delta\) and \((q_2, a_2, q'_2) \in \delta\), if \(q_1 = q_2\) then \(a_1 = (s_1, s'_1)\) and \(a_2 = (s_2, s'_2)\), and \(s_1 \neq s_2\).

**Definition (Local backward determinism)**

A TM \( T \) is **local backward deterministic** iff for any distinct pair of triples \((q_1, a_1, q'_1) \in \delta\) and \((q_2, a_2, q'_2) \in \delta\), if \(q'_1 = q'_2\) then \(a_1 = (s_1, s'_1)\) and \(a_2 = (s_2, s'_2)\), and \(s'_1 \neq s'_2\).
Local backward determinism: Examples

- \((q, (a, b), p)\) and \((q, (a, c), p)\) respects bwd determinism.
- \((q, (a, b), p)\) and \((r, (c, b), p)\) breaks bwd determinism.
- \((q, (a, b), p)\) and \((r, \rightarrow, p)\) breaks bwd determinism.

RTM computability

Some important results:

- RTMs compute *injective functions*, only.
- *All* injective computable function are computable with RTMs.
- 1-tape, 3-symbol RTMs are sufficient.
- RTMs can be easily inverted...

Classical universality

A universal TM \(U\) is defined as a *self-interpreter* for Turing machines:

\[
\llbracket U \rrbracket(\llbracket \Gamma T \rrbracket, x) = \llbracket T \rrbracket(x) .
\]

Here, \(\llbracket \Gamma T \rrbracket \in \Sigma^*\) is a Gödel number representing some TM \(T\).

*Problem:* Does not work for RTMs - \(\llbracket U \rrbracket\) is non-injective.
RTM-universality

An RTM-universal TM $U_R$ is defined by

$$\left\lceil U_R \right\rceil \left( \left\lceil T \right\rceil, x \right) = \left( \left\lceil T \right\rceil, \left\lceil \left\lceil T \right\rceil \right\rceil (x) \right).$$

where $\left\lceil T \right\rceil \in \Sigma^*$ is a Gödel number representing some RTM $T$.

$\left\lceil U_R \right\rceil$ is injective and computable $\Rightarrow$ computable by some RTM.

Why a first-principles approach?

Previous approaches (Bennett, Morita) rely on reversible simulations ("reversibilization") of irreversible machines. Asymptotically very costly: As much space as time!

The URTM we give has better complexity: (Program dependent) constant factor slowdown, same space as interpreted program. Theoretical basis for the robustness of reversible models.

URTM overview

Scope:
- Interprets 1-tape, 3-symbol RTMs
  \( T = \{ Q, \{ b, 0, 1 \}, \delta, b, q_s, q_f \} \).

Structure:
- **Work tape**: Identical to $T$'s tape.
- **Program tape**: Contains the program $\left\lceil T \right\rceil$.
- **State tape**: Encoding of $T$’s internal state, $q_c$. 
Program encoding $\Gamma T^\top$

A program is a string $\Gamma T^\top$ over $\Sigma = \{b, 0, 1, B, S, M, \#\}$. $\Gamma T^\top$ lists the rules $\delta$ of $T$, with $q_s$ rule first, $q_f$ rule last.

$$\text{trans}(q, (s, s'), q') = S\#e_Q(q)s\#e_S(s')\#\text{rev}(e_Q(q'))\#S$$
$$\text{trans}(q, d, q') = M\#e_Q(q)d\#\text{rev}(e_Q(q'))\#M$$

$e_Q : Q \rightarrow \{0, 1\}^{\lceil \log |Q| \rceil}$ is an injective binary encoding of states.

$$e_\Sigma(s) = \begin{cases} B & \text{if } s = b \\ s & \text{otherwise} \end{cases}$$

$e_D(d) = \begin{cases} 10 & \text{if } d = \leftarrow \\ BB & \text{if } d = \downarrow \\ 01 & \text{if } d = \rightarrow \end{cases}$

$\text{rev} : \Sigma \rightarrow \Sigma$ reverses a string.

Program encoding, example

$\text{RTM } T = (\{q_0, q_1, q_2, q_3\}, \{b, 0, 1\}, \delta, b, q_0, q_3)$

$$\delta = \{(q_0, \rightarrow, q_1), (q_1, (0, 1), q_2), (q_1, (1, 0), q_2), (q_2, \leftarrow, q_3)\}$$

$\Gamma T^\top = M\#00\#01\#10\#MS\#01\#01\#SS\#01\#10\#01\#SM\#10\#10\#11\#M$

$e_Q$ is given as $q_0 \mapsto 00$, $q_1 \mapsto 01$, $q_2 \mapsto 10$ and $q_3 \mapsto 11$.

URTM program

Problem: Lots of irreversibilities in control flow.
URTM program

Use enclosing $S, M$ to join paths after rule tests.

Works because $q_s$ is only visited once.

String comparison

A key functionality we need to implement is string comparison.

Assume a 2-tape structure

- $#s_1 \cdots s_n#$
- $#t_1 \cdots t_n#$

with tape heads on the leftmost #.

From internal state $q$, we want to pass over the strings, ending in internal state $q_f$ if the strings match, and in internal state $q_{\neg f}$ if they don’t, with the tape heads in either case on the rightmost #.
Irreversible string comparison of \#s_1 \cdots s_n\# \\
\#t_1 \cdots t_n\#

Irreversibility at state q (and probably p).

Reversible string comparison of \#s_1 \cdots s_n\# \\
\#t_1 \cdots t_n\#

Inverse string comparison of \#s_1 \cdots s_n\# \\
\#t_1 \cdots t_n\# = \text{join}
Testing a symbol rule \((q, (s, s'), q')\)

\[
\begin{align*}
qc & = q \\
sc & = s \\
qc & = q
\end{align*}
\]

apply rule

Must resolve the join in control flow.

This assertion works for all \(T\). Still irreversible...

Only possible because \(T\) is reversible!
**Bonus: Inverse interpretation**

URTM can work as a (reversible) *inverse interpreter* with no extra overhead. A reversible inverse interpreter is a program \textit{rinvint} s.t.

\[
\text{\texttt{rinvint}}(p, y) = (p, x) \quad \text{iff} \quad \text{\texttt{rev}}(T_p) = T_y^{-1}
\]

We intentionally designed the program encoding s.t.

\[
\text{\texttt{rev}}(T_p) = T_p^{-1}
\]

Let \( R \) perform this *string reversal*. (Time linear in size of \( T_p \).)

\[
\text{\texttt{R} \circ U \circ R} (T_p, y) = (T_p^{-1}, T_y^{-1}(x))
\]

---

**Conclusion**

First URTM with
- Only constant factor slowdown (proportional to \textit{length}(\( T \)).)
- No space overhead (unlike all previous approaches.)
- Inverse interpretation for free.

The RTMs can thus simulate themselves efficiently.

References:
Generating Input-Erasing Efficient Clean Reversible Programs for Injective Functions

Tetsuo Yokoyama
Nanzan University, Japan

Existing Work and Our Approach

- A clean reversible simulation of injective programs is possible [Bennett 89]
  - 2 computation + 2 inverse computation
- We argue that for a certain class of injective programs 1 computation + 1 uncomputation are necessary.
  - Twice as fast as Bennett's.
  - Demonstration by developing lossless encoders and decoders

A new view on developing efficient reversible simulations for a certain class of injective functions

Reversible Simulations

- Bennett spying method [Bennett 73]
  - Garbage G is removed but T (garbage) remained.

- Bennett method for injective functions [Bennett 89]
  - Clean!
  - In general, we cannot reduce the number of boxes.
  - How can we optimize it for a certain class of problems?
Reversible Simulations

- The new method (for domain specific problems)
  - Twice as fast as Bennett’s general method.
  - Still, clean!
  - $G_1$ must be equal to $G_2$.

The development process of the proposed clean reversible simulation

Injectivization at programming language level

- Injective program
  - Information loss
  - Ex.
    - injective program: with information loss
    - Procedure: `if e then ... else ...` Postcondition inference is in general undecidable

- Injectivized program of $f$
  - No information loss
  - Trivial injectivization: without information loss
  - `procedure p/ if e then push(1,G) else push(2,G) f top(G) = 1`
Case Study: Run-length encoding (1)

```
AAAAABBBBBBBBBBBBBB
⇒ A5B8A3...
```

Orthogonalization by adding a garbage variable. 
No human invention required.

Recompression

```
procedure rl_gen_code
  from n=0
  loop //Count # of the same characters
    from len=0
    do len += 1
       popfront(text, c)
       n += 1
    loop c = Front(text) //Zero-clear c
    until empty(text) || cl=front(text)
  //Output the encoded text
  pushback(code, c)
  pushback(code, len)
until empty(text)
```

The variable n after computation is the same.

```
procedure rl_gen_text
  from n=0
  loop popfront(code, c)
       popfront(code, len)
  //Copy c for len times
  from empty(text) || cl=front(text)
  loop len <= 1
      pushfront(text, c)
      n += 1
  until len=0
  until empty(count)
```

One Procedure, Two meaning (2)

```
call mg_gen_text
```

```
procedure rl_gen_text
  from n=0
  loop popfront(code, c)
       popfront(code, len)
  //Copy c for len times
  from empty(text) || cl=front(text)
  loop len <= 1
      pushfront(text, c)
      n += 1
  until len=0
  until empty(count)
```

```
uncall mg_gen_text
```

Run-length encoding (3)

```
```

(a) The proposed input-erasing reversible simulation, in the case that the forward and backward garbage are the same.

```
procedure rl_encode
... copy text ...
call rl_gen_code
... restore text and backup code ...
uncall rl_gen_text
... erase backup code ...
```

44
Case study: Range coding  
(Arithmetic coding)

1. Given a text, count the numbers of characters and make a model.
2. Mapping from texts to floating numbers and return the number.

- Example
  - Encoding: "abacab" \( \rightarrow \) model \((a=3, b=2, c=1) + 0.198...\)
  - Decoding: model \((a=3, b=2, c=1) + 0.198... \rightarrow \) "abacab"

Range Coding: Encoding "abacabce" \( \Rightarrow \) "2745"  
Decoding "2745" \( \Rightarrow \) "abacabce"

\[\text{Same Garbage!}\]

```
function mg_gen_code
  range_size
  call count_freq
  from n=0
  loop popfront(text, t)  
    pushback(gbg, low)
    pushback(gbg, mg)
    //...set new low and new mg...
    if mg <= threshold then
      call expand_mg
      tmp := 1
      if tmp = 1
        pushback(gbg, tmp)
        n := n + 1
        pushback(gbg, mg)
      until empty(text)
      pushback(gbg, mg)
      pushback(gbg, n)
      code := low
      pushback(gbg, low)
```

```
function mg_gen_text
  range_size
  from n=0
  loop // set decoded characters to t, and
    pushback(gbg, low)
    pushback(gbg, mg)
    //...set new low and new mg...
    if mg >= threshold then
      call expand_mg
      tmp := 1
      if tmp = 1
        pushback(gbg, tmp)
        n := n + 1
        pushback(gbg, mg)
      until back(text) = t
      pushback(gbg, mg)
      pushback(gbg, n)
      code := low
      pushback(gbg, low)
    uncall count_freq
```

- Count the number of loops.
- Zero-clearance of variables were performed by gbg stack.

45
Wrap them up! (3)

Concluding remarks

- **The efficient (semi-)automatic reversible simulations** for every single problem domain are important.
  - There are huge amount of heritage from irreversible programming.
  - Programming reversibly from scratch is involved.
- **We proposed an optimized clean Bennett method.**
  - The execution time of the mechanically translated reversible algorithm was halved.
- **As each programming paradigm does, reversible programming needs its own programming methodology.**
  - We showed a power of the proposed method by successfully demonstrating the optimization of lossless data encoding and decoding.

References

Reversible Coroutines

Poul J. Clementsen, Robert Glück & Holger B. Axelsen
DIKU, University of Copenhagen, Denmark

4th DIKU-IST Joint Workshop on Foundations of Software
Tokyo, Japan, January 2011

Motivation

Current reversible programming languages have few program constructs because of the constraints posed by reversibility.

We show how this expressiveness can be greatly extended by adding a coroutine construct without losing reversibility.
Reversible Programming Language

Characteristics

- Forward and backward deterministic
- Reversible update of variables \( x += e \)
- Local inversion
- Control flow operators require assertions

Reversible Structured Control Flow

(a) Conditional  (b) Loop

Janus Programming Language

Example (Fibonacci pair)

```
procedure main
  x1 += 3
  x2 += 5
  uncall fib

procedure fib
  from x1 = x2
  do n -= 1
  loop x1 += x2
      x1 <=> x2
  until n = 0
```

<table>
<thead>
<tr>
<th>n</th>
<th>x1</th>
<th>x2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Janus Programming Language

Abstract Syntax

```
prog ::= (x{c})^ p^ 

p ::= procedure id s^ 

s ::= x+= e | x-= e | x<=> x | 
    if e then s' else s' fi e | 
    from e do s' loop s' until e | 
    call id | uncall id 

e ::= c | x | e ⊗ e 
⊗ ::= + | - | * | / | ···
```

Reversible Coroutine

Motivation for looking at reversible coroutine

- Coroutines are well-suited for defining
  - Cooperative tasks
  - Iterators
  - Generators
  - Infinite lists
  - Pipes
- Only reversible subroutine exist
- Gain expressiveness in a disciplined way

Reversible Coroutines in Janus

Example (Fibonacci pair generator w/ coroutine)

```
procedure main
  n += 2
  call fibco
  call fibco
  uncall fibco

  x1 += 1
  x2 += 1
  from x1 = x2
  do n -= 1
     loop yield
        x1 += x2
        x1 <=> x2
     until n = 0
```

```
<table>
<thead>
<tr>
<th>n</th>
<th>x1</th>
<th>x2</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
```
### Application of reversible coroutines

- Are coroutines well-suited for defining program components?
  - Generators
  - Iterators
  - Cooperative tasks
  - Pipes

### Reversible Pipeline using Coroutine

Example (Unix Pipe)
```
cat code | unzip | bcount | zip > code`
```

Pipeline implementation

- Communicate through circular buffer
- Define coroutines zip, unzip and bcount and methodology for communicating with pipes
- Pipeline scheduler linking the coroutines

```coroutine```
coroutine proc (IN, OUT)
  from empty (OUT)
  do yield
  loop get (IN) <=> in
    body
    put (OUT) <=> out
  until empty (IN)
```
Pipeline Implementation

```
procedure pipeline
    // ... initialize buffer code ...
call unzip(a, b)
call bcount(b, c)
call zip(c, d)
from empty(b) && empty(c) && empty(d)
do call unzip(a, b)
call bcount(b, c)
call zip(c, d)
until empty(a) && empty(b) && empty(c)
call bcount(b, c)
call zip(c, d)
coroutine bcount(in, out)
from empty(out)
do yield
loop from empty(out)
do get(in) == code
if chr = 'b'
then count += 1
fi
put(out) == chr
until empty(in)
put(out) == count
```

```
coroutine unzip(in, out)
from empty(out)
do yield
loop get(in) == code
from ppeek(out) != code || empty(out)
do length -= 1
loop put(out) == code
until length = 0
put(out) == code
until empty(in)
coroutine zip(in, out)
from empty(out)
do yield
loop get(in) == code
from length = 0
do length -= 1
loop gpeek(in) != code || empty(in)
put(out) == code
until empty(in)
put(out) == length
```

Poul J. Clementsen Reversible Coroutines DIKU-IST’11 19/19

Translation

Translation to a Reversible Instruction Set Architecture

- Preserve reversibility properties of the language
- Exploit reversibility properties of the low-level language
- Gain properties of an implementation in reversible hardware, i.e., lower heat dissipation

Poul J. Clementsen Reversible Coroutines DIKU-IST’11 19/19

Reversible Coroutine Translation Challenges

- Granularity is finer
- Control flow
- Coroutine state
- Clean translation (i.e., w/o trace data)
**Coroutine Translation**

<table>
<thead>
<tr>
<th>Programming Language</th>
<th>Coroutine</th>
<th>Application</th>
<th>Translation</th>
<th>Conclusion</th>
</tr>
</thead>
</table>
| **Coroutine Translation**

Poul J. Clementsen
Reversible Coroutines
DIKU-IST’11 16/19

<table>
<thead>
<tr>
<th>coroutine (fib_{co})</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ x_1 += 1 ]</td>
</tr>
<tr>
<td>[ x_2 += 1 ]</td>
</tr>
<tr>
<td>[ \text{from } x_1 = x_2 ]</td>
</tr>
<tr>
<td>[ \text{do } n -= 1 ]</td>
</tr>
<tr>
<td>[ \text{loop } \text{yield} ]</td>
</tr>
<tr>
<td>[ x_1 += x_2 ]</td>
</tr>
<tr>
<td>[ x_1 &lt;=&gt; x_2 ]</td>
</tr>
<tr>
<td>[ \text{until } n = 0 ]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Coroutines are a powerful way of gaining expressiveness in a disciplined way</td>
</tr>
<tr>
<td>• First step: Generator, pipeline and cooperative processes</td>
</tr>
<tr>
<td>• Adds first stateful construct in reversible languages</td>
</tr>
<tr>
<td>• Clean translation scheme</td>
</tr>
</tbody>
</table>
Future Work

- Expressive powers of coroutines need to be examined further, *i.e.*, defining cooperative tasks and state machines
- Generator and pipeline examples presented need to be refined and generalized
- Refine coroutine notation to include, *e.g.*, instances and local variables
Background and overview

- Two common approaches to uniformly specifying effectful operations in functional languages:
  - Monad of computations + pure definitions of operations
    - Translate client program using monad components, plug in operation definitions, evaluate by core semantics
    - Typically used in Haskell-like settings
  - Stylized evaluation contexts + context-rewriting operations
    - Formalize context shapes, extend core semantics with new rules for effectful operations
    - Typically used in ML/Scheme-like settings

- This talk: generically obtaining (2) from (1)
  - ... without giving up the monadic equational theory!
- In paper: details for full multimonic metalanguage
  - Here: for single effect only; expressed in Haskell subset (slightly oversimplified)
  - There is a complementary story for ML-like settings

Monadic Haskell with Int-carrying exceptions

```
Core lang.
t ::= Int | t1 -> t2 | Either t1 t2 | Mε t
e ::= id | ex | · · ·
Core lang.
e ::= n | x | λx → e | e1 e2 | Left e | Right e | case e0 of {Left x → e1; Right y → e2} | returnε e | doε x ← e1; e2 | raise e | tryε e1 with x → e2

Typing judgment

Γ ⊢ e :: Int
Γ ⊢ returnε e :: Mε t
Γ ⊢ e :: Mε t
Γ ⊢ raise e :: Mex t

Γ ⊢ e1 :: Mε t1 Γ, x :: t1 ⊢ e2 :: Mε t2
Γ ⊢ doε x ← e1; e2 :: Mε t2
Γ ⊢ tryε e1 with x → e2 :: Mε t

Superscripts ε on return, do, try added by overloading resolution.
```
Specifying exceptions with a monad

Transparent/concrete definition of exception monad:

```plaintext
type T_{ex} a = Either a Int -- not newtype
unit_{ex} :: a → T_{ex} a
unit_{ex} a = Left a
bind_{ex} :: T_{ex} a → (a → T_{ex} b) → T_{ex} b
bind_{ex} t f = case t of {Left a → f a; Right n → Right n}
```

Used to implement abstract effect of exceptions:

```plaintext
newtype M_{e} a = Reflect_{e} (T_{e} a)  Reflect_{e} :: T_{e} a → M_{e} a
reify_{e} (Reflect_{e} x) = x -- aka. run_{e}  reify_{e} :: M_{e} a → T_{e} a
return^{e} e = Reflect_{e} (unit_{e} e)
do^{e} x ← e_{1}; e_{2} = Reflect_{e} (bind_{e} (reify_{e} e_{1}) (λx → reify_{e} e_{2}))
raise e ≡ Reflect_{e} (Right e) -- definitional abbrevs.
try^{e} e_{1} with x → e_{2} ≡
case reify_{e} e_{1} of {Left a → return^{e} a; Right x → e_{2}}
```

Standard (def.-unfolding) operational semantics

```plaintext
e ::= (core) | return^{e} e | do^{e} x ← e_{1}; e_{2} | Reflect_{e} e | reify_{e} e
```

Reduction judgment \[ e \rightarrow e' \] for closed terms:

```plaintext
\[
\begin{align*}
e_{1} & \rightarrow e'_{1} \\
e_{1} e_{2} & \rightarrow e'_{1} e'_{2} \\
(λx → e_{1}) & \rightarrow e_{1}[e_{2}/x] \\
\text{case } e_{0} \text{ of } \{ \cdots \} & \rightarrow \text{case } e'_{0} \text{ of } \{ \cdots \} \\
\text{case } \text{Left } e \text{ of } \{ \text{Left } x_{1} → e_{1}; \text{Right } x_{2} → e_{2} \} & \rightarrow e_{1}[e/x] (\text{+symm})
\end{align*}
\]

```plaintext
\[
\begin{align*}
\text{return}^{e} e & \rightarrow \text{Reflect}_{e} (\text{unit}_{e} e) \\
do^{e} x ← e_{1}; e_{2} & \rightarrow \text{Reflect}_{e} (\text{bind}_{e} (\text{reify}_{e} e_{1}) (λx → \text{reify}_{e} e_{2})) \\
e & \rightarrow e' \\
\text{reify}_{e} e & \rightarrow \text{reify}_{e} e' \\
\text{reify}_{e} (\text{Reflect}_{e} e) & \rightarrow e
\end{align*}
\]

Note: tags on \text{return}^{e}, \text{do}^{e} play essential role in behavior.

Note: code for unit_{e}, bind_{e} traversed on every return^{e}, do^{e}.

Equational theory

If \((T_{e}, \text{unit}_{e}, \text{bind}_{e})\) satisfy monad laws, get additional valid reasoning principles for observational equivalence:

\[
\begin{align*}
(λx → e_{1}) e_{2} &= e_{1}[e_{2}/x] \\
λx → e &= e (\times \not\in \text{FV}(e)) \\
\vdots
\end{align*}
\]

```plaintext
\[
\begin{align*}
do^{e} x ← \text{return}^{e} e_{1}; e_{2} &= e_{2}[e_{1}/x] \\
do^{e} x ← e; \text{return}^{e} x &= e \\
do^{e} y ← (\text{do}^{e} x ← e_{1}; e_{2}); e_{3} &= \text{do}^{e} y ← e_{1}; \text{do}^{e} y ← e_{2}; e_{3} (\times \not\in \text{FV}(e_{1})) \\
\text{reify}_{e} \left(\text{return}^{e} e\right) &= \text{unit}_{e} e \\
\text{reify}_{e} \left(\text{do}^{e} x ← e_{1}; e_{2}\right) &= \text{bind}_{e} (\text{reify}_{e} e_{1}) (λx → \text{reify}_{e} e_{2}) \\
\text{reify}_{e} (\text{Reflect}_{e} e) &= e \\
\text{Reflect}_{e} (\text{reify}_{e} e) &= e
\end{align*}
\]

Can we operationalize these equations in a different way?
New (effectful) operational semantics

\[ e ::= (\text{core}) \mid \text{return } e \mid \text{do } x \leftarrow e_1; e_2 \mid \text{reify}_z e \mid \text{do } x \leftarrow \text{Reflect}_c e_1; e_2 \]

\[ \text{reflect}_c e \equiv \text{do } x \leftarrow \text{Reflect}_c e; \text{return } x \quad \text{-- for convenience} \]

\[ e \rightarrow e' \]

(Unmodified rules for the core constructs)

\[ e_1 \rightarrow e_1' \]
\[ \text{do } x \leftarrow e_1; e_2 \rightarrow \text{do } x \leftarrow e_1'; e_2 \]
\[ \text{do } x \leftarrow \text{return } e_1; e_2 \rightarrow e_2[e_1/x] \]
\[ \text{do } y \leftarrow (\text{do } x \leftarrow \text{Reflect}_c e_1; e_2); e_3 \rightarrow \text{do } x \leftarrow \text{Reflect}_c e_1; \text{do } y \leftarrow e_2; e_3 \]

\[ e \rightarrow e' \]
\[ \text{reify}_z e \rightarrow \text{reify}_z e' \]
\[ \text{reify}_z (\text{return } e) \rightarrow \text{unit}_c e \]
\[ \text{reify}_z (\text{do } x \leftarrow \text{Reflect}_c e_1; e_2) \rightarrow \text{bind}_z e_1 (\lambda x \rightarrow \text{reify}_z e_2) \]

Note: no effect-tags needed on return, do.

\[ (\ast)\text{-rules: connect } \text{Reflect}_c \text{ to nearest dynamically enclosing } \text{reify}_z. \]

Properties of reduction semantics

- **Sound**: if \( e \rightarrow e' \), then \( e = e' \) in equational theory.
- **Deterministic**: if \( e \rightarrow e' \) and \( e \rightarrow e'' \), then \( e' = e'' \).
- **Type-preserving**: if \( \vdash e : t \) and \( e \rightarrow e' \), then \( \vdash e' : t \).
- **Non-sticking**: if \( \vdash e : t \), then either \( e \) canonical, or \( e \rightarrow e' \) for some \( e' \). Canonical forms are:

\[
\begin{aligned}
\text{Int} & \mid t_1 - t_2 \\
\text{Either} & \mid \text{Left } e \mid \text{Right } e \\
M_{t_1} t & \end{aligned}
\]

\[
\begin{aligned}
\text{return } e & \mid \text{do } x \leftarrow \text{Reflect}_c e_1; e_2 \\
\text{reify}_z F[e] & \rightarrow \text{unit}_c e \\
\text{reify}_z (\text{return } e) & \rightarrow \text{unit}_c e \\
\text{reify}_z (\text{do } x \leftarrow \text{Reflect}_c e_1; e_2) & \rightarrow \text{bind}_z e_1 (\lambda x \rightarrow \text{reify}_z e_2) \end{aligned}
\]

Note: a canonical \( M \)-computation is either effect-free, or an immediate effect invocation.

- In particular, a closed term of type Int (but using monadic effects internally) must eventually reduce to an \( n \), or diverge.

Evaluation-context formulation of new semantics

General and restricted evaluation contexts:

\[
\begin{align*}
E & ::= [] \mid E e \mid \text{case } E \text{ of } \cdots \mid \text{do } x \leftarrow E; e \mid \text{reify}_z E \\
F & ::= [] \mid \text{do } x \leftarrow F; e \quad \text{(in particular, no } \text{reify}_z F) \\
\end{align*}
\]

Bigger-step judgment \( e \rightarrow e' \):

\[
\begin{align*}
e & \rightarrow e' \\
E[e] & \rightarrow E[e'] \\
(\lambda x \rightarrow e_1) e_2 & \rightarrow e_1[e_2/x] \\
\text{case } \text{Left } e \text{ of } \{ \text{Left } x_1 \rightarrow e_1; \text{Right } x_2 \rightarrow e_2 \} & \rightarrow e_1[x_1/e/x] \quad \text{(+symm)} \\
\text{do } x \leftarrow \text{return } e_1; e_2 & \rightarrow e_2[e_1/x] \\
\text{reify}_z (\text{return } e) & \rightarrow \text{unit}_c e \\
\text{reify}_z (F[\text{Reflect}_c e]) & \rightarrow \text{bind}_z e_1 (\lambda x \rightarrow \text{reify}_z F[\text{return } x]) \quad \text{(+)} \\
\end{align*}
\]

Sound: if \( e \rightarrow e' \) then \( e \rightarrow^* e' \).
Example: exceptions (again)
Recall definitions of exception monad and operations:

\[ T_{ex} a = \text{Either} a \text{ Int}; \quad \text{unit}_{ex} a = \text{Left} a; \quad \text{bind}_{ex} = \cdot \cdot \cdot \]

\[ \text{raise} \ e \equiv \text{reflect}_{ex} (\text{Right} \ e) \]

\[ \text{try} \ e_1 \ with \ x \to e_2 \equiv \]

\[ \text{case} \ \text{reify}_{ex} e_1 \text{ of} \{ \text{Left} \ a \to \text{return} \ a; \text{Right} \ x \to e_2 \} \]

Gives derivable typing and reduction rules:

\[
\Gamma \vdash e :: \text{Int} \quad \Gamma \vdash e_1 :: M_{ex} t \quad \Gamma, x :: \text{Int} \vdash e_2 :: M_x t
\]

\[
\begin{align*}
\Gamma \vdash \text{raise} \ e :: M_{ex} t \\
\Gamma \vdash \text{try} \ e_1 \ with \ x \to e_2 :: M_x t
\end{align*}
\]

\[
\begin{align*}
\text{try} \ e_1 \ with \ x \to e_2 \to \text{try} \ e'_1 \ with \ x \to e_2 \\
\text{try return} \ e_0 \with x \to e_2 \to \text{return} \ e_0
\end{align*}
\]

Example: state
Standard definitions of state monad and operations:

\[ T_{st} a = \text{Int} \to (a, \text{Int}); \quad \text{unit}_{st} a = \lambda s \to (a, s); \quad \text{bind}_{st} = \cdot \cdot \cdot \]

\[ \text{getst} \equiv \text{reflect}_{st} (\lambda s \to (s, s)) \]

\[ \text{setst} \ e \equiv \text{reflect}_{st} (\lambda s \to ((), e)) \]

\[ \text{withst} \ e_1 \ do \ e_2 \equiv \text{let} \ (a, s') = (\text{reify}_{st} e_2) \ e_1 \ in \ a \\
\quad \begin{array}{l}
\quad \begin{array}{l}
\text{run} \ e_2 \ in \ initial \ state \ e_1
\end{array}
\end{array}
\]

Derived typing and reduction rules:

\[
\begin{align*}
\Gamma \vdash \text{getst} :: M_{st} \text{Int} \\
\Gamma \vdash \text{setst} \ e :: M_{st} ()
\end{align*}
\]

\[
\begin{align*}
\text{withst} \ e_1 \ do \ e_2 \to \text{withst} \ e_1 \ do \ e'_2 \\
\text{withst} \ e_1 \ do \ \text{return} \ e_2 \to^+ \ e_2
\end{align*}
\]

\[
\begin{align*}
\text{withst} \ e \ do \ F[\text{getst}] \to^+ \ \text{withst} \ e \ do \ F[\text{return} \ e] \\
\text{withst} \ e \ do \ F[\text{setst} \ e'] \to^+ \ \text{withst} \ e' \ do \ F[\text{return} ()]
\end{align*}
\]

Summary

- Monadic definitions of effects can be given direct operational interpretation. Curry-style type system: don’t need to reconstruct types before evaluation.

- Rational reconstruction of evaluation-context semantics.
  - Related construction: taking implementation type \( M_{st} a \) to be a delimited-continuations monad \( \forall o. (a \to T_{st} o) \to T_{st} o \)

  \[ \Rightarrow \text{embedding arbitrary monadic effects in Scheme.} \]

- In paper:
  - Full core language with product, sum, function, recursive, and generalized-effect types; effect-subtyping.
  - Explicit syntax for effect definitions with layering.
  - Precise formulation of semantics (explicit and context-based), type system, type soundness – all mechanized in Twelf.

- Current work: correspondence between (domain-theoretic) denotational and operational semantics for monadic effects.
Report on using
Generic Multiset Discrimination
for a
Probability Monad

Ken Friis Larsen
Department of Computer Science
University of Copenhagen
kflarsen@diku.dk

4th DIKU-IST Workshop

Probability Monad

• Our offset is the formulation by Erwig and Kollmansberger (2006)

• That probability distributions form a monad is not new Giry (1981)

Probability Monad in Haskell

type Probability = Float

newtype Dist a = D {unD::[(a,Probability)]}

instance Monad Dist where
    return x = D[(x, 1.0)]
    dist >>= f = dist `bind` f

bind :: Dist a -> (a -> Dist b) -> Dist b
Constructing Distributions

weightedCases :: [(a, Probability)] -> Dist a
countedCases :: [(a, Int)] -> Dist a
uniform :: [a] -> Dist a

Example: Some Dice

die = uniform [1..6]

twoDice = do
    n1 <- die
    n2 <- die
    return (n1+n2)

Example: Traffic Light

data Light = Red | Green | Yellow

stopLight :: Dist Light
stopLight =
    countedCases [(Red, 50), (Yellow, 10), (Green, 40)]
Example: Driver Behavior

data Action = Stop | Drive

cautious :: Light -> Dist Action
cautious Red    = return Stop
cautious Green  = return Drive
cautious Yellow = countedCases[(Stop,9),(Drive,1)]

aggressive :: Light -> Dist Action
aggressive Red    = countedCases[(Stop,9),(Drive,1)]
aggressive Yellow = countedCases[(Stop,1),(Drive,9)]
aggressive Green  = return Drive

Implementing bind

bind :: Dist a -> (a -> Dist b) -> Dist b
bind (D d) cond =
    D [(y, p*q) | (x, p) <- d
        , (y, q) <- unD (cond x)]

We Got a Problem

> unD twoDice
[(2,2.777778e-2),(3,2.777778e-2),(4,2.777778e-2),
(5,2.777778e-2),(6,2.777778e-2),(7,2.777778e-2),
(3,2.777778e-2),(4,2.777778e-2),(5,2.777778e-2),
(6,2.777778e-2),(7,2.777778e-2),(8,2.777778e-2),
(4,2.777778e-2),(5,2.777778e-2),(6,2.777778e-2),
(7,2.777778e-2),(8,2.777778e-2),(9,2.777778e-2),
(5,2.777778e-2),(6,2.777778e-2),(7,2.777778e-2),
(8,2.777778e-2),(9,2.777778e-2),(10,2.777778e-2),
(6,2.777778e-2),(7,2.777778e-2),(8,2.777778e-2),
(9,2.777778e-2),(10,2.777778e-2),(11,2.777778e-2),
(7,2.777778e-2),(8,2.777778e-2),(9,2.777778e-2),
(10,2.777778e-2),(11,2.777778e-2),(12,2.777778e-2)]
Let’s Fix it

bind (D d) cond = D d'
where
  raw = [(y, p*q) | (x, p) <- d
         , (y, q) <- unD (cond x)]
  sorted = sortBy (\(x,p)(y,q) -> compare x y) raw
  grouped = groupBy (\(x,p)(y,q) -> x==y) sorted
  d' = map (\g -> (fst$ head g, sum$ map snd g))
       grouped

We Got an Other Problem

Could not deduce (Ord b) from the context ()
  arising from a use of `bind'
Possible fix:
  add (Ord b) to the context of the type
  signature for `>>='
In the expression: bind dist f
In the definition of `>>=': dist >>= f = bind dist f
In the instance declaration for `Monad Dist'

Using RMonad

data instance Constraints Dist a =
  Ord a => DistC
instance Ord a => Suitable Dist a where
  constraints = DistC

instance RMonad Dist where
  return  x = D[(x, 1)]
  d >>= k = Suitable.withResConstraints $ \DistC -> d `bind` k
Generic Multiset Discrimination

• We can also use Henglein’s library for Generic multiset discrimination

• Key ingredient: generic symbolic equality relations

• Key function (for this talk):
  part :: Equiv t -> [t] -> [[t]]

GMSD With RMonad

class Eqv t where
  equiv :: Equiv t

data instance Constraints Dist a =
  Eqv a => DistC
instance Eqv a => Suitable Dist a where
  constraints = DistC

instance RMonad Dist where
  return  x = D[Pr x 1]
  d >>= k = Suitable.withResConstraints $ \DistC -> d `bind` k

bind with GMSD

bind :: Eqv a =>
  Dist t -> (t -> Dist a) -> Dist a

bind (D d) cond = D flattened
  where
    raw = [Pr y (p*q) | Pr x p <- d
      , Pr y q <- unD (cond x)]
    grouped = Disc.part equiv raw
    flattened = [Pr (pfst$ head p)
        (sum$ map psnd p)
        | p <- grouped]
Near-future Work

- Performance evaluation
- Simulation framework
- Example from biology
  - Tree grows
  - Predator/Prey models

Future Work

- Monte Carlo simulation
- Examples from finance

Distant-future Work

- Symbolic representation of distributions
- Perhaps extend beyond finite discrete distributions
- Parallel execution of simulations
A Trace-based Model for Multi-Party Contracts

Tom Hvitved
hvitved@diku.dk

DIKU-IST Workshop 2011
January 11, 2011

1 Joint work with Felix Klaedtke and Eugen Zălinescu

Background

- Multi-party contract: legally binding agreement between individuals or companies that describes the commitments of each contract participant.
- For enterprises: contracts serve as the external interface to their clients. Consequently crucial to monitor execution of contracts for breaches, and to comply with them.
- Aberdeen Group studies: “the average savings of transactions that are compliant with contracts is 22%”.

Example

- **Paragraph 1.** Seller agrees to transfer and deliver to Buyer, on or before 2011-01-01, the goods: 1 laser printer.
- **Paragraph 2.** Buyer agrees to accept the goods and pay a total of €200 for them according to the terms further set out below.
- **Paragraph 3.** Buyer agrees to pay for the goods half upon receipt, with the remainder due within 30 days of delivery.
- **Paragraph 4.** If Buyer fails to pay the second half within 30 days, an additional fine of 10% has to be paid within 14 days.
- **Paragraph 5.** Upon receipt, Buyer has 14 days to return the goods to Seller in original, unopened packaging. Within 7 days thereafter, Seller has to repay the total amount to Buyer.
Trace-based Contract Model

- Abstract model for contracts.
- Contracts are driven by events.
- Depending on the sequence of events, the outcome of a contract can either be fulfillment or non-fulfillment.
- Such outcome may be suggestive of an obligation or a deadline not being met—but the model does not rely on such high-level notions.
- (Deterministic) blame assignment.
- Fundamental breaches: first breach matters.
- Compositionality (contract conjunction, contract disjunction).

Definitions (I)

- P: contract parties, A: actions, Ts: timestamps (for simplicity, Ts := N).
- Event: $\epsilon = (\tau, \alpha)$, where $\tau \in Ts$, $\alpha \in A$.
- $ts((\tau, \alpha)) := \tau$.
- Trace: finite or infinite sequence of events that satisfies the following properties:
  1. timestamps are non-decreasing, that is, $ts(\sigma[i]) \leq ts(\sigma[j])$, for all integers $i, j \in N$ with $0 \leq i \leq j < |\sigma|$.
  2. infinite traces have progress, that is, if $|\sigma| = \infty$ then for all timestamps $\tau \in Ts$, there is an integer $i \in N$ such that $ts(\sigma[i]) \geq \tau$.

Definitions (II)

- Intuitively: contract is a subset of traces.
- BUT: we generalize the traditional binary outcome to incorporate blame assignment.
- Verdicts: $V := \{ \top \} \cup \{(\tau, B) \mid \tau \in Ts \text{ and } B \subseteq P \}$.
- Contract conformance, $\top$, is not associated with a point in time.
- Require that all breaches be associated with a finite point in time.
- $|B| > 1$: simultaneous breach, e.g., a barter deal.
Definitions (III)

- A contract between parties $P \subseteq \text{fin} P$: a function $c : \text{Tr} \rightarrow V$, where
  
  if $c(\sigma) = (\tau, B)$ then $B \subseteq P$,
  
  if $c(\sigma) = (\tau, B)$ then $c(\sigma') = (\tau, B)$, for all $\sigma' \in \text{Tr}$ with $\sigma_{\tau} = \sigma'_{\tau}$.

- ($\sigma_{\tau}$ is restriction of $\sigma$ to events with time stamp at most $\tau$.)

- Contracts are deterministic.

- Traces are considered complete. Do not model: origin of events, agreement of events.

- Result: Verdict on infinite traces uniquely determined from verdicts on finite traces (contract conformance is a safety property).

Example

- Paragraph 1 as a contract, $c_1 : \text{Tr} \rightarrow V$ between $\{\text{Seller}\}$:
  
  $$c_1(\sigma) := \begin{cases} 
  \top & \text{if } \sigma[i] = (\tau, \text{delivery}), \\
  (\tau_d, \{\text{Seller}\}) & \text{for some } 0 \leq i < |\sigma| \text{ and } \tau \leq \tau_d, \\
  \text{otherwise.} & 
  \end{cases}$$

  - $\tau_d := 2011-01-01$.

  - $c_1(\varepsilon) = (2011-01-01, \{\text{Seller}\})$.

  - $c_1((2011-01-01, \text{delivery})) = \top$.

Contract Conjunction

- Present in virtually all contracts.

- Assume $\nu_i$ is verdict of $c_i$, $i = 1, 2$.

- Combined verdict:
  
  $$\nu_1 \land \nu_2 := \begin{cases} 
  \top & \text{if } \nu_1 = \nu_2 = \top, \\
  \nu_1 & \text{if either } \nu_1 = \top, \\
  \nu_2 & \text{if either } \nu_1 = \top, \\
  (\tau, B) & \text{if } \nu_1 = (\tau_1, B_1), \nu_2 = (\tau_2, B_2), \text{ and } \tau_1 < \tau_2, \\
  (\tau, B) & \text{if } \nu_1 = (\tau, B_1), \nu_2 = (\tau, B_2), \text{ and } \tau_1 > \tau_2. 
  \end{cases}$$

- ($\nu_1 \land \nu_2$)$(\sigma) := c_1(\sigma) \land c_2(\sigma)$.

- Result: $c_1 \land c_2$ contract between parties $P_1 \cup P_2$ then $c_1 \land c_2$ contract between parties $P_1 \cup P_2$. 


Contract Disjunction

- Assume νᵢ is verdict of cᵢ, i = 1, 2, and that if ν₁ = (τ, B₁) and ν₂ = (τ, B₂) then B₁ = B₂ (deterministic blame assignment).

- Combined verdict:

  \[ \nu_1 \lor \nu_2 := \begin{cases} 
  \top & \text{if } \nu_1 = \top \text{ or } \nu_2 = \top, \\
  (\tau, B_1) & \text{if } \nu_1 = (\tau, B_1), \nu_2 = (\tau, B_2) \text{ and } \tau_1 > \tau_2, \\
  (\tau, B_2) & \text{if } \nu_1 = (\tau, B_1), \nu_2 = (\tau, B_2) \text{ and } \tau_1 < \tau_2, \\
  (\tau, B) & \text{if } \nu_1 = \nu_2 = (\tau, B). 
  \end{cases} \]

- Inherently non-deterministic operator.

- \((\nu_1 \lor \nu_2)(\sigma) := \nu_1(\sigma) \lor \nu_2(\sigma).\)

- Result: c₁ (c₂) contract between parties \(P_1 (P_2)\) then \(c_1 \lor c_2\) contract between parties \(P_1 \cup P_2.\)

Contract Composition

- \((\land, \lor, \land)\) is a distributive lattice with unit element \(c_\top.,\)

- provided unique blame assignment.

- \(\nu_1 \land \nu_2 \equiv \nu_2 \land \nu_1\) (Commutativity)

- \(\nu'_2 \lor \nu_2 \equiv \nu'_2 \lor \nu'_1\) (Commutativity)

- \(\nu_1 \land (\nu_2 \land \nu_3) = (\nu_1 \land \nu_2) \land \nu_3\) (Associativity)

- \(\nu'_2 \lor (\nu'_2 \lor \nu'_3) = (\nu'_2 \lor \nu'_2) \lor \nu'_3\) (Associativity)

- \(\nu'_2 \lor (\nu'_2 \land \nu'_3) = \nu'_2\) (Absorption)

- \(\nu'_2 \land (\nu'_2 \lor \nu'_3) = \nu'_2\) (Absorption)

- \(\nu'_2 \lor (\nu'_2 \land \nu'_3) = (\nu'_2 \lor \nu'_2) \land (\nu'_2 \lor \nu'_3)\) (Distributivity)

- \(\nu_1 \land (\nu_2 \lor \nu_3) = (\nu_1 \land \nu_2) \lor (\nu_1 \land \nu_3)\) (Distributivity)

- \(\top \land \nu = \nu \land \top = \nu\) (Unit)

- \(\top \lor \nu = \nu \lor \top = \top\) (Unit)

Run-time Monitoring

- Run-time monitor: partial, finite traces. Most be computable.

- Many-valued semantics: \(V_\star := \{\nu_\star \mid \nu \in V\}, \star \in \{!, ?\}.\)

- \(\text{mon} : \text{Tr}_{\text{fin}} \rightarrow V_1 \cup V_7\) that satisfies

  \[ \text{mon}(\sigma) = \begin{cases} 
  \tau_1 & \text{if } c(\sigma') = \top \text{ whenever } \sigma \subseteq \sigma', \\
  (\tau, B) & \text{if } c(\sigma') = (\tau, B) \text{ whenever } \sigma \subseteq \sigma', \\
  \tau_3 & \text{if } c(\sigma) = \top \text{ and } c(\sigma') \neq \top \text{ for some } \sigma \subseteq \sigma', \\
  (\tau, B) & \text{if } c(\sigma) = (\tau, B) \text{ and } c(\sigma') \neq (\tau, B) \text{ for some } \sigma \subseteq \sigma'. 
  \end{cases} \]

- Impartiality and anticipation.

- Previous example:

  - \(\text{mon}(\varepsilon) = (2011-01-01, \text{Seller}),\)

  - \(\text{mon}(2011-01-01, \text{delivery}) = \top,\)

  - \(\text{mon}(2011-01-02, \text{delivery}) = (2011-01-01, \text{Seller}).\)
A Contract Specification Language

- Writing contracts directly in the abstract model is cumbersome.
- CSL provides syntax for writing contracts.
- CSL specifications denote contracts via a reduction semantics ⇒ deterministic blame assignment + compositionality.
- CSL supports (a) history sensitive contracts, (b) conditional commitments, (c) contract templates, (d) absolute and relative temporal constraints, (e) reparation clauses, (f) in-place arithmetic, and (g) potentially infinite contracts.

**Signature:**

\[ S = (K, ar, T), ar : K \rightarrow T^* \]

**Actions refined:**

\[ A := \{ k(\vec{v}) \mid k \in K, ar(k) = (t_1, \ldots, t_n), \vec{v} \in [t_1] \times \cdots \times [t_n] \} \]

**Syntax:**

\[
s ::= \text{letrec } \{ (\vec{c}) \mid c_i \}_{i=1}^n \text{ in starting } e \\
c ::= \text{fulfillment} \\
| \langle e_1 \rangle k(\vec{x}) \text{ where } e_2 \text{ due } d \text{ remaining } z \text{ then } e \text{ due immediately} \\
| \text{if } k(\vec{x}) \text{ where } e \text{ due } d \text{ remaining } z \text{ then } c_1 \text{ else } c_2 \\
| c_1 \text{ and } c_2 \\
| c_1 \text{ or } c_2 \\
| f(\vec{c_1})(\vec{c_2}) \\
e ::= x \mid \neg e \mid e_1 \star e_2 \mid e_1 \prec e_2 \\
d ::= \text{after } e_1 \text{ within } e_2
\]

**Example, revisited**

```plaintext
letrec sale(deliveryDeadline, goods, payment)(buyer, seller) = 
    (seller) Deliver(s,r,g) where s = seller \land r = buyer \land g = goods 
    due within deliveryDeadline 
then 
    (buyer) Payment(s,r,a) where s = buyer \land r = seller \land a = payment/2 
    due immediately 
then 
    ((buyer) Payment(s,r,a) where s = buyer \land r = seller 
    a = (payment/2) \times 110/100 
    due within 14D after 30D) 
or 
    (buyer) Payment(s,r,a) where s = buyer \land r = seller 
    a = (payment/2) \times 110/100 
    due within 14D after 30D)
and 
if Return(s,r,g) where s = buyer \land r = seller \land g = goods due within 14D then 
    (seller) Payment(s,r,a) where s = seller \land r = buyer \land a = payment 
    due within 7D)
in 
sale(0, "Laser printer", 200)(Buyer, Seller) starting 2011-01-01
```
Some Notes on Semantics (I)

- Type system:
  - $\Delta$: template environment, $\Lambda$: party environment, $\Gamma$: variable environment.
  - $\Delta, \Lambda, \Gamma \vdash c : \text{Clause}(P)$.
  - $\vdash s : \text{Contract}(P)$.

$$
\Gamma' = \Gamma[\vec{x} \mapsto \text{ar}(k)] \\
\Gamma_2 = \Gamma[\vec{z} \mapsto \text{Int}] \\
\Delta, \Lambda_1 \vdash e_1 : P_1 \\
\Gamma' \vdash e : \text{Bool} \\
\Delta, \Lambda_2 \vdash e_2 : \text{Deadline} \\
\Delta, \Lambda_1 \cup \Lambda_2, \Gamma \vdash c : \text{Clause}(P_2)
$$

17

Some Notes on Semantics (II)

- Reduction semantics:
  - $D, \tau \vdash c \rightarrow c'$ either $c'$ or $(\tau, B)$.

$$
\begin{align*}
\epsilon[a/b] & \equiv \text{true} \\
\epsilon & \vdash (\tau_1, \tau_2) \\
\tau_1 & \leq \tau_2 \\
D, \tau \vdash (p) k(\vec{e}) & \text{ where } e \text{ due if remaining } z \text{ then } c \\
D, \tau & \vdash (\tau_1, \tau_2) \\
\tau' & > \tau_2 \\
D, \tau \vdash (p) k(\vec{e}) & \text{ where } e \text{ due if remaining } z \text{ then } c \\
D, \tau & \vdash (\tau_1, \tau_2, \max(\tau_1, \tau_2), (p))
\end{align*}
$$

- $s \rightarrow s'$ either $s'$ or $(\tau, B)$.

$$
\begin{align*}
\epsilon[a/b] & \equiv \text{true} \\
\epsilon & \vdash (\tau_1, \tau_2) \\
\tau_1 & \leq \tau_2 \\
\tau & \vdash (\tau_1, \tau_2) \\
\epsilon[a/b] & \vdash (\tau_1, \tau_2) \\
\epsilon & \vdash (\tau_1, \tau_2) \\
\tau & \vdash (\tau_1, \tau_2) \\
\epsilon[a/b] & \vdash (\tau_1, \tau_2) \\
\tau & \vdash (\tau_1, \tau_2)
\end{align*}
$$

18

Some Notes on Semantics (III)

- Progress: if $\vdash s : \text{Contract}(P)$ then for all events $\epsilon$, there is a unique residue $s$ such that $s \rightarrow s$. Furthermore, whenever $s = (\tau, B)$ then $B \subseteq P$.

- Preservation: if $\vdash s : \text{Contract}(P)$ and $s \rightarrow s'$ then $\vdash s : \text{Contract}(P')$ with $P' \subseteq P$.

- Result: if $\vdash s : \text{Contract}(P)$ then $[s]$ is a contract between parties $P$.

- ([ ] defined using $s \rightarrow s'$.)
Some Notes on Semantics (IV)

- Reduction semantics gives rise to incremental run-time monitoring.
- But full anticipation not supported (expression language may “hide” anticipated verdicts).

Summary

- Abstract, trace-based contract model. Focus: blame assignment.
- Abstract definition of contract conjunction, contract disjunction, and run-time monitoring.
- Contract specification language, CSL.
- Incremental run-time monitoring of CSL specifications.
- Various “real-world” contracts formalized in CSL.

Future Work

- Fragments of CSL: non-negative deadlines, fulfillable obligations.
- Full run-time monitoring.
- Contract analysis:
  - Satisfiability (related to full run-time monitoring).
  - Satisfiability w.r.t. a particular party.
  - Contract portfolios.
  - Non-deterministic semantic model: determinism $\Rightarrow$ decision procedure.
- Other applications (web services, network protocols)?
  - (Implementation.)
Semantic Patch Inference

Jesper Andersen
University of (wonderful) Copenhagen
Computer Science Department (DJKU)

Joint work with
Julia Lawall
David Lo
Siaw-Cheng Khoo

Context: collateral evolution

- Many programs using the same library
- The library is updated
  - API changed

Context: collateral evolution

- Many programs using the same library
- The library is updated
  - API changed
  - Many "client programs" no longer work
Context: collateral evolution

- Many programs using the same library
- The library is updated
  - API changed
  - Many "client programs" no longer work
- **Collateral evolution**: update of many programs in response to changes in library

Problem: getting it right in the first place

- Performing a collateral evolution by hand is ...
  - ... tedious
    - Many locations have to be updated in similar fashion
  - ... error-prone
    - Humans are not very good automatons
    - Tricky reg-exp. based scripts are hard to write
      - Even more difficult for others to read
  - ... done very frequently in development of Linux device drivers
    - Often done mostly correct
    - Varied development environments
    - Developers are distributed around the globe

Coccinelle

- A program transformation and query engine
- Used for
  - Collateral evolution of Linux device drivers
  - Bug finding & fixing in systems code
- Provides the specification language SmPL
  - WYSIWYG approach
  - Abstract irrelevant details
  - Control-flow sensitive

```plaintext
$\varepsilon$ expression $X, Y$:
$\varepsilon$
- $\varepsilon (X)$
  - ...
- $g (X, Y)$
  + $g (Y)$
```
Semantic patch example

```
void foo() {
    f(42);
    if (b) {
        g(42,1);
        g(42,2);
    } else {
        g(42,10);
    }
    f(12);
}
```

```
void foo() {
    f(42);
    if (b) {
        g(1);
        g(42,2);
    } else {
        g(10);
    }
    f(12);
}
```

Problem: who will write the semantic patches?

The library developer

- Real code is more natural to work with
- Gap between library evolution and driver collateral evolution
- In what context do the changes (not) apply?

"I wish I could write a semantic patch"

The driver developer

- Real code updates are too low level
- What details are (not) important?

"If only someone had written a semantic patch"

The contribution: spdifff

- A method for automatic inference of semantic patches from example updates
  - Library developers can work on real code...
  - Driver developers can apply spdifff to real updates...
- A formalization of subpatches
  - Ensures that inferred patches "do the right thing"
  - Gives higher-level description of changes than standard diff
- Implemented in the tool "spdifff"
  - Applicable to "historic" data from Linux revision system
Simple example: "I wish I could write a semantic patch"

int foo(int a)
int x = 42;
x = bar();
foz(x);
bar();
return x;
}

int foo(int *q)
int y = *q + *q;
*q = bar();
return y;
}

Library devs. can work on (less) real code...

Old workflow
Lib v 1 p Lib v 2
d1 p1 d1'
d2 p2 d2'
d3 p3 d3'
d4 p4 d4

New workflow
Lib v 1 p Lib v 2
Apply spdiff to get sp
d1 p1 d1'
d2 p2 d2'
d3 p3 d3'
d4 p4 d4

Driver devs.: "I wish someone had written a semantic patch"

commit 072364e8064d22e4fe2e19749a19b088b4b3
Author: FUJITA Tomonori <fujita.tomonori@lab.ntt.co.jp>
Date: Thu Oct 9 11:25:42 2008 -0900

[SCSI] Be-xxxx: remove unnecessary local_irq_save/restore for scsi
sg copy API

Since the commit 50bad2e2f8a53e4f1d683d5d27592e7ef15b9 [scg
disable interrupts inside sg_copy_buffer], no need to disable
interrupts before calling scsi_sg_copy_from_buffer. So we can
simplify to Transfer internal, which disables interrupts just for
scsi_sg_copy_from_buffer.

"If only someone had written a semantic patch"
Driver devs.: "I wish someone had written a semantic patch"

diff --git a/drivers/亭/3-waaa.o b/drivers/亭/3-waaa.o
index 553720..89031e 100644
--- a/drivers/亭/3-waaa.o
+++ b/drivers/亭/3-waaa.o
@@ -1466,12 +1466,12 @@ static int tw_sync_ioctl(PW_DeviceExtension *tw_dev, int request_id)
 static void tw_transfer_int(PW_DeviceExtension *tw_dev, int request_id, void *data, unsigned int len)
 {
     struct osi_cmd *cmd = tw_dev->cmd(request_id);
-     unsigned long flags;
-     local_irq_save(flags);
-     osni_ag_copy_from_buffer(cmd, data, len);
-     local_irq_restore(flags);
+     osni_ag_copy_from_buffer(tw_dev->cmd(request_id), data, len);
 }

 /* This function is called by the ioctl to complete an inquiry command */

Driver devs.: "I wish someone had written a semantic patch"

diff --git a/drivers/亭/3-waaa.o b/drivers/亭/3-waaa.o
index 553720..89031e 100644
--- a/drivers/亭/3-waaa.o
+++ b/drivers/亭/3-waaa.o
@@ -1466,12 +1466,12 @@ static int tw_sync_ioctl(PW_DeviceExtension *tw_dev, int request_id)
 static void tw_transfer_int(PW_DeviceExtension *tw_dev, int request_id, void *data, unsigned int len)
 {
     struct osi_cmd *cmd = tw_dev->cmd(request_id);
-     unsigned long flags;
-     local_irq_save(flags);
-     osni_ag_copy_from_buffer(cmd, data, len);
-     local_irq_restore(flags);
+     osni_ag_copy_from_buffer(tw_dev->cmd(request_id), data, len);
 }

 /* This function is called by the ioctl to complete an inquiry command */

Formalization of subpatch

Main concept:

Transformation part:

\[ sp \leq (t, t') \]

sp is part of turning t into t'

\(~ does \ the \ right \ thing \ w.r.t. \ (t, t') ~\)

Given a set of examples

- Find the sp such that

1) sp does "the right thing"

Denoted: \( sp \leq C \leftrightarrow \forall (t, t') \in C : sp \leq (t, t') \)

2) sp expresses as much of the common changes as possible

\( \forall sp' : sp \leq C \\ sp' \leq sp \)
Doing the right thing

**Transformation part:**
\[ sp \leq (t, t') \iff "sp does the right thing" \] (???)

**First suggestion:** 
\[ (t, t') \] can be decomposed into \( sp \) and \( sp' \)

\[ \exists sp' \] where \( [sp]'([sp](t)) = t' \)

We need to restrict \( sp' \) or else \( \forall sp : sp \leq (t, t') \)

\( sp' \) should not "undo" things done by \( sp \)

---

Doing the right thing (cont'd)

**Transformation part:**
\[ sp \leq (t, t') \iff "commutative parts" \]

**Second suggestion:** 
\[ (t, t') \] can be decomposed into \( sp \) and \( sp' \)

and they commute with each other

\[ [sp]'([sp](t)) = [sp]'([sp](t)) = t' \]

---

Doing the right thing (final)

**Transformation part:**
\[ sp \leq (t, t') \iff [sp](t) = t'' \& \delta(t, t'') + \delta(t'', t') = \delta(t, t') \]

**Third suggestion:** "do as little work as necessary"

\[ \delta(a, b) : \text{some tree edit distance (metric)} \]

"If a subterm changed, changing it again is more costly than changing it only once"
Formalization of subpatches

What is it that "spdiff" do? How does it work?

Given a set of examples, \( C = \{(t_1,t_1'), ..., (t_n,t_n')\}\)

"Finds largest common transformation"

Find the sp such that:

1) sp does "the right thing" for each pair \((t,t') \in C\)

\[ \text{Denoted: } s_p \leq C \Rightarrow \forall (t,t') \in C : s_p \leq (t,t') \]

2) sp expresses as much of the common changes as possible (subsumption relation)

\[ \forall s'_p : s'_p \leq C \Rightarrow s'_p \leq s_p \]

---

2 algorithms for semantic patch inference

**Context-free patches**

- **Notation**
  \(\text{gp ::= } p \rightarrow p | \text{gp;gp}\)

- **Application**
  \(\text{[p\rightarrow p'](t) = \text{replace p with p'}}\)
  \(\text{[gp;gp'](t) = [gp']([gp](t))}\)

- **Example**
  \(\text{seq\_path(X1, X2\rightarrow X3.mnt, X2\rightarrow X3.dentry, X4)}\)
  \(\rightarrow\)
  \(\text{seq\_path(X1, &X2\rightarrow X3, X4)}\)

---

**Context-sensitive patches**

- **Notation**
  \(\text{sp ::= O sp | \varepsilon}\)
  \(O ::= p | \ldots | \neg p | + p\)

- **Application**

- **Example**
  - \(\text{unsigned long X8;}\)
  - \(\text{local\_irq\_save(X8);}\)
  - \(\text{... scsi\_sg\_copy\_from\_buffer(X5, X5, X7);}\)
  - \(\text{... local\_irq\_restore(X8);}\)

---

Algorithm for context-sensitive patches

**Algorithm**

Three main parts

1. Identification of changes
   - Graph differences
2. Inference of common characteristics
   - Context-sensitive patterns
3. Construction of context-sensitive patches
   - Iteratively grow patches from patterns and diffs

---

Growing semantic patches
Identify changes

```c
int foo(int a) {
    int x = 42;
    log_assign(x); // log_assign(x);
    x = bar(); // x = bar();
    foz(x); // returned(x);
    bar(); // foz(x);
    return x; // bar();
}

Chunkify...
+p*(p|-p)+p
```

Find context-sensitive patterns

2 steps:
- Find common node patterns
- Grow patterns from node patterns

```c
int foo(int a) {
    int x = 42;
    x = bar();
    foz(x);
    bar();
    return x;
}
```

Find context-sensitive patterns

```c
X0 = X1;
...
X2 = bar();
...
return X3;
```

Grow pattern
```
int foo(int *q) {
    int y = *q + *q;' // return y;
    *q = bar();
    y = bar();
    return y;
}
```
Construction of patches...

- signed int x = 42;
+ int x = 42 + 42;

+ log_assign(x);
  x = bar();
+ returned(x);

+ returned(x);
  foz(x);

Wrong:
One decl. did not change!

Construction of patches...

- signed int x = 42;
+ int x = 42 + 42;

+ log_assign(x);
  x = bar();
+ returned(x);

+ returned(x);
  foz(x);

int X0 = X1;
...
+ X0 = assign(X0);
  X0 = bar();
+ returninished(X0);
  ...
  return X0;

Maximality:
Use subsumption relation to return only largest...

Summary

In this talk

- Short description of collateral evolution
- Simple definition of "transformation parts"
  Independent of transformation language
- Use of transformation parts to implement semantic patch inference

Not in this talk / future work

- Dealing with actual real-world changesets
- Bug-hunting
  Searching for common contexts for backports
- Integration in IDEs
- Parameterize over subject language
- Relate to...
  - Semi-inversion
  - Logic programming
A Short Review: Left Inverses vs. Right Inverses

Kazutaka Matsuda (Tohoku University)
Jan. 11, 2011
DIKU-IST Workshop

This Talk

- A short review on inverse computation
- To tell difference between
  - left inverse construction
    - left inverse: what we call inverse
  - right inverse construction
    - right inverse: output -> a possible input
- To address issues in right inverse construction

(Left) Inverse

Definition

g is called a **left inverse** of f if f(x) = y implies g(y) = x for every x and y

- Only injective function has a left inverse.
- e.g.)
  - inc is a left inverse of dec
    \[ \text{inc}(\text{dec}(x)) = \text{inc}(x-1) = x \]
    \[ \text{inc}(x) = x + 1 \]
    \[ \text{dec}(x) = x - 1 \]
**Left Inverses are Useful**

- Deserialization obtained from serialization
  - classic example: runlength

- Derivation of bidirectional transformation
  [Matsuda+07]

**Approaches to Left Invs**

- Compositional approach

- Derivation approach

**Compositional Construction**

- Compositional approach to left-inverse
  [Mu+04][Foster+05,07]
  \[(f;g)^{-1} = g^{-1};f^{-1}\]

- Injectivity-preserving combinators \(\times, +, \ldots\)

- Predefined primitives
Derivational Construction

- Several known methods
  - [Matsuda+10] [Nishida&Sakai09,10]
  - [Glück&Kawabe04,05][Glück&Kawabe05]
  - [Mogensen05] ... [Gries81]
- **Injectivity** analysis for correctness and for efficiency

```
if x then e₁ {P₁}
else e₂ {P₂}
```

Short Summary

- Left inverse construction
  - Compositional: **Injectivity**
  - Derivation: Injectivity analysis
  - Complementary

Dual story: right inverses?

- Can we follow the successful stories about left-inverses?

Yes or No
**Right Inverse**

**Definition**

g is called a right inverse of f if  
g(y) = x implies f(x) = y for every x and y

- Every function has (partial) right inverse.
  - e.g.)
    * half(double(x)) = x
    * half(double'(x)) = x

*half(x) = floor(x/2)*
*double(x) = 2*x*
*double'(x) = 2*x + 1*

**Right Inverses are Useful**

- To handle lost values in bidirectional transformation [Foster+07,08, ...]
  
  ![Diagram](image)

- Data abstraction [Wang+10]
  - Join list and list

- Derivation of parallel programs
  [Gibbons96][Morita+07][Morihata+09]

**Rest of Talk**

- Methods for right inverses
  - What are keys?
- Problems
- Conclusion
**Construction of Right Inverses**

- Compositional approaches
  [Wang+10][Foster+08; Bohannon+08]

- Derivational approaches
  [Matsuda+10][Glück&Abramov02]
  [Morita+07]

**Quiz**

- $f'$: a right-inverse of $f$
- $g'$: a right-inverse of $g$

- Is $(g'; f')$ is a right inverse of $(f; g)$?

![Diagram of functions $f$ and $g$]

**No!**

- $\text{dup}'$: a right-inverse of $\text{dup}$
- $\text{fst}'$: a right-inverse of $\text{fst}$

\[
\text{dup}(x) = (x, x) \\
\text{dup}'(x, x) = x \\
\text{fst}(x, y) = x \\
\text{fst}'(x) = (0, x)
\]

![Diagram of functions $\text{dup}$, $\text{fst}$, $\text{fst}'$, and $\text{dup}'$]
Reason to fail

- $f'$: a right-inverse of $f$
- $g'$: a right-inverse of $g$

- $\text{Ran}(f) \not\subseteq \text{Dom}(g)$

Surjectivity is a Key

- $f'$: a right-inverse of surjective $f$
- $g'$: a right-inverse of surjective $g$

- $(g'; f')$ is a right inverse of $(f; g)$.

Surjectivity in Existing Work

- [Wang+10] [Foster+08; Bohannon+08]
  - Compositional Composition
  - Surjectivity is guaranteed
    - via surjectivity-preserving combinators
    - including function composition

  - Difference: Objects (\includegraphics[width=0.2\textwidth]{prev_slide.png} in prev slide)
    - [Wang+10]
      Algebraic Datatype
    - [Foster+08; Bohannon+08]
      Regular-set (with Quotient)
Derivational Construction

- [Matsuda+10]
- [Glück&Abramov02]
- [Morita+07]

[Matsuda+10]

- \( \exists x. f(x) = v \)
  - \( \begin{align*}
  \text{add}(Z, y) &= y \\
  \text{add}(S x, y) &= S(\text{add}(x, y))
  \end{align*} \)

  \( \exists xy. \text{add}(x, y) = v \Leftrightarrow \text{Add} \rightarrow * v \)

  \( \begin{align*}
  \text{Add} &\rightarrow \text{S(Add)} \\
  \text{Add} &\rightarrow \text{S(Add)} \\
  \end{align*} \)

  \( \begin{align*}
  S(S(Z)) &\rightarrow \text{S(Add)} \\
  S(S(Z)) &\rightarrow \text{S(Add)} \\
  \end{align*} \)

  \( \begin{align*}
  \text{Add} &\rightarrow \text{S(S(Z))} \\
  \text{Add} &\rightarrow \text{S(S(Z))} \\
  \end{align*} \)

  \( \begin{align*}
  \text{add}(S Z, S Z) &\rightarrow \text{S(add}(Z, S Z)) \\
  \text{add}(S Z, S Z) &\rightarrow \text{S(S(Z))} \\
  \end{align*} \)

[Glück&Abramov02]

- \( \exists x. f(x) = v \)
  - \( \begin{align*}
  \text{add}(Z, y) &= y \\
  \text{add}(S x, y) &= S(\text{add}(x, y))
  \end{align*} \)

  \( \begin{align*}
  x := Z &\rightarrow \text{add}(x, y) = S(S Z) \\
  x := Z &\rightarrow \text{add}(x, y) = S(S Z) \\
  \end{align*} \)

  \( \begin{align*}
  y := S(S Z) &\rightarrow x := S x \\
  y := S(S Z) &\rightarrow x := S x \\
  \end{align*} \)

  \( \begin{align*}
  \text{OK: } (Z, S(S Z)) &\rightarrow y := S(S Z) \\
  \text{OK: } (Z, S(S Z)) &\rightarrow y := S(S Z) \\
  \end{align*} \)

  \( \begin{align*}
  \text{add}(x, y) &= S(S Z) \\
  \text{add}(x, y) &= S(S Z) \\
  \end{align*} \)

  \( \begin{align*}
  \text{OK: } (Z, S(S Z)) &\rightarrow y := S Z \\
  \text{OK: } (S Z, S Z) &\rightarrow y := S Z \\
  \end{align*} \)

  \( \begin{align*}
  \text{OK: } (S Z, S Z) &\rightarrow y := S Z \\
  \text{OK: } (S Z, S Z) &\rightarrow y := S Z \\
  \end{align*} \)
[Morita+06]

\[ \exists x. f(x) = v \]

\[
\begin{align*}
\text{sum } [x] &= x \\
\text{sum } (a:x) &= a + \text{sum } x
\end{align*}
\]

\[
\begin{align*}
\text{template for } x \\
\text{sum'}(s) &= [t] \\
\rightarrow s &= \text{sum } [t] \\
\rightarrow s &= t
\end{align*}
\]

\[
\begin{align*}
\text{check } \text{Dom} (\text{sum'}) &\supseteq \text{Ran} (\text{sum})
\end{align*}
\]

Is \text{sum}([\cdot]) as surjective as \text{sum}?  

---

Candidate of Key Technique

\[ \exists x. f(x) = v \]

- [Matsuda+10]
  - Any \( f \) is surjective to some regular set
  - Right inverse is given by automaton
- [Glück&Abramov02]
  - Any \( f \) is surjective to some RE set
  - Right inverse does not necessary terminate
- [Morita+07]
  - Surjectivity check
  - They asks whether still \( f([x]) \) is surjective

---

Summary

- Left inverse derivation
  - Compositional: Injectivity
  - Derivation: Injectivity analysis
- Right inverse derivation
  - Compositional: Surjectivity
  - Derivation: Surjectivity check or Exact Range?
Problems

- Left-inverse derivation uses injectivity analysis
- Little discussion on right-inverse derivation with surjectivity analysis?
  - [Morita+07] is notable exception

Problems

- Functions are rarely surjective
  - Objects (A, B of f :: A → B) are simple enough to check A=B
  - Range(f) is usually more complex
    - even Range(f) ⊇ B is undecidable
- Derivation method is rarely useful to define primitives in compositional approach.
  - notable exceptions
    [Wang+10] [Foster+08;Bohannon+08]

Conclusion

- Left inverse construction
  - Compositional: Injectivity
  - Derivation: Injectivity analysis
  - Complementary

- Right inverse construction
  - Compositional: Surjectivity
  - Derivation: Surjectivity check or Exact Range?
  - Not complementary?
Towards a Software Model Checker for ML

Naoki Kobayashi
Tohoku University

Joint work with:
Ryosuke Sato and Hiroshi Unno (Tohoku University)
in collaboration with
Luke Ong (Oxford), Naoshi Tabuchi and Takeshi Tsukada (Tohoku)

This Talk

♦ Overview of our project on program verification, based on higher-order model checking (or, the model checking of higher-order recursion schemes)
- What is higher-order model checking?
- How are higher-order model checking problems solved?
- How can software model checkers be constructed on top of a higher-order model checker?

Goal: Software model checker for ML

Outline

♦ Introduction to higher-order model checking
- What are higher-order recursion schemes?
- What are model checking problems?
- How related to program verification?

♦ Model checking functional programs
- Predicate abstraction and CEGAR
- Automata-based abstractions for recursive data structures

♦ Discussion and conclusion
Higher-Order Recursion Scheme

Grammar for generating an infinite tree

Order-0 scheme
(regular tree grammar)

\[
S \rightarrow a \ c \ B \\
B \rightarrow b \ S
\]

Tree whose paths are labeled by \(a^{m+1} b^{m} c\)

Higher-Order Recursion Scheme

Grammar for generating an infinite tree

Order-1 scheme

\[
S \rightarrow A \ c \\
A \rightarrow \lambda x. \ a \times (A \ (b \ x))
\]

Tree whose paths are labeled by \(a^{m+1} b^{m} c\)

Higher-Order Recursion Scheme

Grammar for generating an infinite tree

Order-1 scheme

\[
S \rightarrow A \ c \\
A \rightarrow \lambda x. \ a \times (A \ (b \ x))
\]

Higher-order recursion schemes

\[
\approx
\]

Call-by-name simply-typed \(\lambda\)-calculus

+ recursion, tree constructors
Model Checking Recursion Schemes

Given

\( G: \) higher-order recursion scheme
\( A: \) alternating parity tree automaton (APT)
(a formula of modal \( \mu \)-calculus or MSO),
does \( A \) accept \( \text{Tree}(G) \)?

e.g.
- Does every finite path end with “c”?
- Does “a” occur eventually whenever “b” occurs?

\[ n \text{-EXPTIME-complete} \quad \text{[Ong, LICS06]} \]
(for order-\( n \) recursion scheme)

TRecS \([\text{K.}, \text{PPDP09}]\)
\[\text{http://www.kb.ecei.tohoku.ac.jp/~koba/trecs/}\]

- First model checker for recursion schemes
- Based on reduction from higher-order model checking to type checking
- Uses a practical algorithm that does not always suffer from \( n \text{-EXPTIME} \) bottleneck

Application: model-checking higher-order boolean programs

Theorem:
Given a closed term \( M \) of (call-by-name or call-by-value) simply-typed \( \lambda \)-calculus with:
- recursion
- finite base types
  (including booleans and constant “fail”)
- non-determinism,
it is decidable whether \( M \rightarrow* \) fail

Proof: Translate \( M \) into a recursion scheme \( G \)
s.t. \( M \rightarrow* \) fail if and only if
\( G \) generates a tree containing “fail”.
Example

$$\begin{align*}
\text{fun } \text{repeatEven } f x &= \text{if } \text{true} \text{ then } x \text{ else } \text{repeatOdd } f x \\
\text{fun } \text{repeatOdd } f x &= f \text{ (repeatEven } f x) \\
\text{fun main()} &= \text{if } \text{(repeatEven not true)} \text{ then } () \text{ else fail}
\end{align*}$$

$S \rightarrow \text{RepeatEven } C \text{ Not True}$

$C \ b \rightarrow if b \ e \ fail$

$\text{RepeatEven } k \ f \ x \rightarrow if * \ (k \ x) \ (\text{RepeatOdd } (f \ k) \ f \ x)$

$\text{RepeatOdd } k \ f \ x \rightarrow \text{RepeatEven } (f \ k) \ f \ x$

$\text{Not } k \ b \rightarrow \text{If } b \ (k \ False) \ (k \ True)$

$\text{If } b \ x \ y \rightarrow b \ x \ y$

$\text{True } x \ y \rightarrow x$

$\text{False } x \ y \rightarrow y$

Comparison with Other Model Checking

<table>
<thead>
<tr>
<th>Program Classes</th>
<th>Verification Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Programs with while-loops</td>
<td>Finite state model checking</td>
</tr>
<tr>
<td>Programs with 1st-order recursion</td>
<td>Pushdown model checking</td>
</tr>
<tr>
<td>Higher-order functional programs</td>
<td>Recursion scheme model checking</td>
</tr>
</tbody>
</table>

Outline

- Introduction to higher-order model checking
  - What are higher-order recursion schemes?
  - What are model checking problems?
  - How related to program verification?

- Model checking functional programs
  - Predicate abstraction and CEGAR
  - Automata-based abstractions for recursive data structures

- Discussion and conclusion

92
Recursion schemes as models of higher-order programs?

+ simply-typed $\lambda$-calculus
+ recursion
+ tree constructors
+ finite data domains (via Church encoding; true = $\lambda x.\lambda y.x$, false=$\lambda x.\lambda y.y$)
- infinite data domains (integers, lists, trees,...)
- advanced types (polymorphism, recursive types, object types, ...)
- imperative features/concurrency

Dealing with Infinite Data Domains

♦ From recursion schemes to higher-order multi-tree transducers (HMTT), to deal with algebraic data types (lists, trees, ...) [K.,Tabuchi&Unno, POPL 2010]

♦ Predicate abstraction and CEGAR (c.f. BLAST, SLAM, ...)

Predicate Abstraction and CEGAR for Higher-Order Model Checking

Program is unsafe! 

Program is safe!

Real error path?

New predicates

Property satisfied

Property not satisfied

Higher-order functional program

Predicate abstraction

$x>0$

$F(g, b) =$ if $b$ then $g(true)$ else $g(*)$

$\text{f}(g,x)=g(x+1)$
What are challenges?

ניPredicate abstraction
- How to choose predicates for each term, in such a way that the resulting HOBP is consistent?
  E.g. fun f g x = g (x+1) ... fun h y z = ... fun main() = f (h 0) u ... The same predicate should be used for z and u+1.

♦ CEgar
- How to find new predicates to abstract each term to guarantee progress (i.e. any spurious counterexample is eliminated)?

Our Approach

♦ Predicate abstraction

\textit{Abstraction types to express abstraction interface:}

\begin{tabular}{l}
  e.g. f: (x:int → int[y.y>x])  \\
  Assuming the argument \( x \) is abstracted using predicate \( x>0 \), the return value \( y \) should be abstracted using \( y>x \).  \\
  \( f(x) = \text{if} \ x>0 \text{ then } x+1 \text{ else } ... \)  \\
  \( \Rightarrow F(b) = \text{if} \ b \text{ then } \text{true} \text{ else } ... \)
\end{tabular}

♦ CEgar

\textit{Reduction from abstraction type finding problem to a refinement type inference problem for SHP (straightline higher-order program).}

Example (predicate abstraction)

\begin{tabular}{l}
  let sum n k = if n<=0 then k 0  \\
  else sum (n-1) (fun x-> k(x+n))  \\
  in sum m (fun x-> assert(x>=m))
\end{tabular}

\textit{sum: (n:int[→]→ (int[λx.x>=n]→*) →*)}

\begin{tabular}{l}
  let sum ( ) k = if * then k true  \\
  else sum ( ) (fun b-> k true)  \\
  in sum ( ) (fun b-> assert(b))
\end{tabular}
Our Approach

Predicate abstraction

Abstraction types to express abstraction interface:
- e.g. \( f : (x: \text{int} \rightarrow \text{int}[\lambda x. x>0] \rightarrow \text{int}[\lambda y. y>x]) \)
  
  Assuming the argument \( x \) is abstracted using predicate \( x>0 \),
  the return value \( y \) should be abstracted using \( y>x \).

  \[ f(x) = \begin{cases} 
  x+1 & \text{if } x>0 \\
  \ldots & \text{else} 
  \end{cases} \]

  \[ f'(b) = \begin{cases} 
  \text{true} & \text{if } b \text{ then } \text{true} \\
  \ldots & \text{else} 
  \end{cases} \]

CEGAR

Reduction from abstraction type finding problem to a refinement type inference problem for SHP (straightline higher-order program).

Example (predicate discovery)

```ocaml
let sum n k = if n<=0 then k 0 
  else sum (n-1) (fun x-> k(x+n)) 
in sum m (fun x-> assert(x>=m))
```

```
sum: (n:int -> int[ ] -> ) ->
```

```
let sum ( ) k = if * then k ( ) 
  else sum ( ) (fun ( )-> k ( )) 
in sum ( ) (fun ( )-> assert(*))
```

Spurious error path (with \( k = (\text{fun } ( ) -> \text{assert}(*)) \)):

```ocaml
sum ( ) k -> if * then k( ) else ... -> k( ) -> assert(*) -> fail
```

Example (predicate discovery)

```
let sum n k = if n<=0 then k 0 
  else sum (n-1) (fun x-> k(x+n)) 
in sum m (fun x-> assert(x>=m))
```

```
Spurious error path:
sum ( ) k -> if * then k( ) else ... -> k( ) -> assert(*) -> fail
```

Straightline higher-order program (SHP):

```
let sum n k = assume(n<=0); k 0 
in sum m (fun x -> assume(not(x>=m)); fail)
```

Typing for SHP:

```
sum: (n:int -> (x:int | x>=n) -> ) ->
```

[Unno&K. PPDP09]
Experiments

<table>
<thead>
<tr>
<th>Code</th>
<th>Cycle</th>
<th>Time (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>mc91</td>
<td>2</td>
<td>0.07</td>
</tr>
<tr>
<td>ackermann</td>
<td>3</td>
<td>0.15</td>
</tr>
<tr>
<td>a-cppr</td>
<td>6</td>
<td>3.40</td>
</tr>
<tr>
<td>a-max</td>
<td>5</td>
<td>4.78</td>
</tr>
<tr>
<td>l-zipmap</td>
<td>4</td>
<td>0.20</td>
</tr>
<tr>
<td>l-zipunzip</td>
<td>3</td>
<td>0.12</td>
</tr>
<tr>
<td>repeat</td>
<td>3</td>
<td>0.15</td>
</tr>
<tr>
<td>a-max-e</td>
<td>2</td>
<td>0.13</td>
</tr>
</tbody>
</table>

(Environment: Intel(R) Xeon(R) 3Ghz with 8GB memory)

Arrays encoded by:

``` OCaml
let mk_array n i =
    assert(0<=i && i<n); 0
let update i n a x =
    a(i);
    let a' j = if i=j then x else a(i)
    in a'
```

Outline

- Introduction to higher-order model checking
  - What are higher-order recursion schemes?
  - What are model checking problems?
  - How related to program verification?
- Model checking functional programs
  - Predicate abstraction and CEGAR
  - Automata-based abstractions for recursive data structures
- Discussion and conclusion

Remaining challenges

- More efficient higher-order model checker
  - practical fixed-parameter linear time algorithm (c.f. [K., FoSSaCS 2011])
  - efficient implementation techniques (e.g. BDD)
- Supporting more language features
  - recursive data structures
    - abstraction by automata/transducers
  - recursive types
  - objects (software model checker for Java)
- More verification power
  - Abstractions using higher-order predicates
  - Inference of auxiliary arguments
Conclusion

*New program verification method based on higher-order model checking*

- Many attractive features
  - Sound, complete, and fully automatic for certain classes of higher-order programs and verification problems
  - Subsumes first-order/pushdown model checking
  - Integration of types and model checking
    - types as certificates
    - counterexamples
- Many interesting and challenging topics

References

- K., POPL09
  From program verification to model-checking, and typing
- K.&Ong, ICALP09 Complexity of model checking
- K.&Ong, LICS09 From model-checking to type checking
- K., PPDP09 First practical higher-order model-checking algorithm
- K., Tabuchi & Unno, POPL10
  Extension to transducers and its applications
- Tsukada & K., FoSSaCS 10
  Extension to deal with more advanced types
- Unno, Tabuchi & K., APLAS 2010
  Extension of POPL10 work to deal with arbitrary tree-processing programs
- K., FoSSaCS 2011
  Practical fixed-parameter linear time algorithm for higher-order model checking
Modal-$\mu$ Definable
Graph Transduction

Kazuhiro Inaba
National Institute of Informatics, Japan

4th DIKU-IST Workshop, 2011

What We Want to Do

• Verification of Graph-to-Graph Transformations

• e.g., Queries on Graph-Structured Database
  or Transformations of XML with “id” links

What We Want to Do

• Verification of Graph-to-Graph Transformations
  with respect to input/output specifications

verify whether or not:
for any graph $G$, $G \models \varphi_{IN} \Rightarrow f(G) \models \varphi_{OUT}$
Verification by Pre-Image
(a.k.a. “weakest precondition” or “inverse type inference”)

Given \( f \) and \( \varphi_{\text{OUT}} \), compute \( \text{inv}_f(\varphi_{\text{OUT}}) \) such that:
for any graph \( G \), \( f(G) \models \varphi_{\text{OUT}} \) iff \( G \models \text{inv}_f(\varphi_{\text{OUT}}) \)

Then “for any graph \( G \), \( G \notmodels \varphi_{\text{IN}} \Rightarrow f(G) \notmodels \varphi_{\text{OUT}} \)”
“for any graph \( G \), \( G \models (\varphi_{\text{IN}} \rightarrow \text{inv}_f(\varphi_{\text{OUT}})) \)”
i.e., \( \varphi_{\text{IN}} \rightarrow \text{inv}_f(\varphi_{\text{OUT}}) \) is valid

To Be More Concrete...

- Which logic can we use for specifying \( \varphi_{\text{IN/OUT}} \)?
  - Must be strong enough to express useful conditions.
  - Must be weak enough to have decidable validity.

- What kind of transformation \( f \) can be verified?
  - We must be able to compute the pre-image.

Our Approach

- Take Modal-\( \mu \) Calculus as the specification logic
  - (At least for trees) capture all existing XML-Schemas

- Define a new model of graph transformation called Modal-\( \mu \) Definable Transduction
  - Pre-image of modal-\( \mu \) sentence can be fully automatically computed
  - Expressive enough to capture (unnested) structural recursion on graphs
Related Work

- **MSO** (Monadic 2nd-Order Logic) Definable Transduction
  - Overall structure is more or less the same.
  - Ours is a proposal to use Modal-μ instead of MSO

- Hoare-Style Verification of Imperative Programs
  - Ours don’t deal with pointers or destructive updates.
  - Rather, it is more suitable for functional programs
  - **Structural recursion** is handled without any annotations

Outline

- Two Kinds of Logics on Graphs
  - Predicate Logics
  - Modal Logics
  - **Why Modal-μ?**

- Review: Predicate-Logic Based Approach
  - MSO-Definable Graph Transduction [Courcelle 94]

- Our Work:
  - **Modal-μ Definable Graph Transduction**
  - Computation of Pre-Image

Graphs (in Today’s Talk)

- **Σ**: Finite Nonempty Alphabet
- **G = (V, E, π)**
  - **V**: Set of Nodes
  - **E ⊆ V × V**: Set of Directed Edges
  - **π : V → 2Σ**: Labels on Nodes

\[
\Sigma = \{a, b\} \\
V = \{a, b\} \\
\pi = \{a, b\} \rightarrow \{a, b\} \\
\rightarrow \{a\} \\
\rightarrow \{b\} \\
\rightarrow \{\} \\
\]
Predicate Logics on Graphs

\[ \phi ::= \]
- False | \neg \phi | \phi \lor \phi
- \sigma(x) (for \sigma \in \Sigma) “node x is labeled \sigma”
- edge(x, y) “an edge connects x to y”
- \exists x. \phi “there’s x that makes \psi hold”
- \exists S. \phi “there’s a set S that makes \psi hold”
- x \in S “x is in S”

We can define True, \phi \land \phi, \phi \rightarrow \phi, \forall x. \phi, and \forall S. \phi.

Semantics

- For a graph \(G=(\mathcal{V}, \mathcal{E}, \pi)\) and an environment \(\Gamma : \text{Var} \rightarrow \mathcal{V}\)

- \(G, \Gamma \vDash \sigma(x)\) iff \(\sigma \in \pi(\Gamma(x))\) “node x is labeled \sigma”
- \(G, \Gamma \vDash \text{edge}(x, y)\) iff \((\Gamma(x), \Gamma(y)) \in \mathcal{E}\) “an edge connects x to y”
- \(G, \Gamma \vDash \exists x. \phi\) iff there’s v \(\in \mathcal{V}\) s.t. \(G, \Gamma[x:v] \vDash \phi\)

... Modal Logics on Graphs

\[ \psi ::= \]
- False | \neg \phi | \phi \lor \phi
- \sigma (for \sigma \in \Sigma) “current node is labeled \sigma”
- \diamond \phi “current node has an outgoing edge whose destination satisfies \phi”
- X
- \mu X. \phi “least fixpoint” (X must be in even # of \neg)

We Can Define: \Box \phi (dual of \diamond) and \nu X. \phi (GreatestFixPt)
Semantics

- For a graph \( G = (V, E, \pi) \), an environment \( \Gamma : \text{Var} \rightarrow 2^V \), and the current node \( v \in V \)

- \( G, v, \Gamma \models \sigma \iff \sigma \in \pi(v) \)  
  “current node is labeled \( \sigma \)”

- \( G, v, \Gamma \models \Diamond \varphi \iff \text{there's } w \ (v, w) \in E \land G, w, \Gamma \models \varphi \)  
  “current node has an outgoing edge whose destination satisfies \( \varphi \)”

- \( G, v, \Gamma \models \mu Y. \varphi \iff \text{if } v \in \text{LFP}(F) \)  
  where \( F(A) = \{ w \in V \mid G, w, \Gamma[Y:A] \models \varphi \} \)

...
Example ($\Sigma = \{a, b, A, B\}$)

$$\text{edge}_{\text{OUT}}(x, y) \equiv \exists z. (\text{edge}(x, z) \land \text{edge}(z, y))$$

$$\text{a}_{\text{OUT}}(x) \equiv \text{b}_{\text{OUT}}(x) \equiv \text{False}$$

$$\text{A}_{\text{OUT}}(x) \equiv \text{a}(x)$$

$$\text{B}_{\text{OUT}}(x) \equiv \text{b}(x)$$

Pre-Image is Easily Obtained

$$\forall x. a(x) \rightarrow \exists y. \exists z. (\text{edge}(x, z) \land \text{edge}(z, y)) \land a(y)$$

$$\forall x. \text{A}(x) \rightarrow \exists y. \text{edge}(x, y) \land \text{A}(y)$$

Expressiveness & Complexity

- **Modal**
  - $\diamond \varphi$
    - PSPACE
  - $\mu X. \varphi$
    - Modal-$\mu$
  - Undecidable

- **FO**
  - $\exists x. \varphi$

- **MSO**
  - $\exists S. \varphi$
Expressiveness & Complexity (on “tree-like” graphs)

Modal-μ and MSO
- Complexity of Validity Checking
  - Modal-μ: EXPTIME-complete
  - MSO: Undecidable (Even in Trees, HyperEXP)

- Expressive Power
  - Modal-μ = \textit{Bisimulation-Invariant Subset of MSO} [Janin & Walukiewicz 96]
  - “Bisimulation-Invariant” ≈
    “Physical equality of pointers cannot be checked”
  - Not a severe restriction for purely functional programs!

Modal-μ Definable (1-copying) Transduction
A set of Modal-μ formulas $T = \cdot \sigma_{\text{OUT}}$ for each $\sigma \in \Sigma$
\cdot edge_{\text{OUT}} an \textit{existential} formula $Fv = \{X\}$
defines a transformation $f_T$ converting
$G = (V, E, \pi)$ into $G' = (V, E', \pi')$ where

- $\pi'(v) = \{ \sigma \mid G, v \vdash \sigma_{\text{OUT}} \}$
- $E' = \{ (v, w) \mid G, v, X:\{w\} \not\vdash \text{edge}_{\text{OUT}} \}$
Example ($\Sigma = \{a, b, A, B\}$)

$\text{edge}_{\text{OUT}} \equiv \Diamond \Box X$

$a_{\text{OUT}} \equiv b_{\text{OUT}} \equiv \text{False}$

$A_{\text{OUT}} \equiv a$

$B_{\text{OUT}} \equiv b$

$a \rightarrow \Diamond \Box a$

$A \rightarrow \Diamond A$

Existential Formula

- A formula $e$ with one free variable $X$ is \textit{existential}, if

$\text{for all } G=(V,E,\pi), v \in V, P \subseteq V$

$G, v, X: P \models e \iff \exists w \in P. G, v, X: \{w\} \models e$

- Examples:
  - "$X \lor \text{True}$" is not existential (Consider $P=\{\}$).
  - "$\Diamond X$" is existential.
  - "$\Box X$" is not (when $v$ is a leaf node ...).
  - "$\sigma$" is not, but "$X \land \sigma$" is.

Syntactic Condition

$\text{for all } G=(V,E,\pi), v \in V, P \subseteq V$

$G, v, X: P \models e \iff \exists w \in P. G, v, X: \{w\} \models e$

- Theorem:
  - $e$ is existential if it is in the following syntax

  $e ::= \text{False} \mid X \mid Y \mid e \lor e \mid \Diamond e \mid \mu Y. e$

  $\mid e \land \varphi$ where $\varphi$ is any formula without free variables

  $(\text{True}, \rightarrow, \sigma, \Box, \text{and GFP must be “guarded” by } _\land _\land)$

\text{OPEN QUESTION: is this a necessary condition?}

(i.e., do all existential formulas have logically-equivalent forms in this syntax?)
More Examples

- \( \text{edge}_{\text{OUT}} \equiv X \)
- \( \text{edge}_{\text{OUT}} \equiv \mu Y. ((X \land a) \lor \Diamond Y) \)
- \( \text{edge}_{\text{OUT}} \equiv \mu Y. ((X \land a \land \square b) \lor (\neg a \land \Diamond Y)) \)

Pre-Image Computation

For \( T = (\sigma_{\text{OUT}}, e_{\text{OUT}}) \), define

- \( \text{inv}(\text{False}) = \text{False} \)
- \( \text{inv}(\neg \varphi) = \neg \text{inv}(\varphi) \)
- \( \text{inv}(\varphi_1 \lor \varphi_2) = \text{inv}(\varphi_1) \lor \text{inv}(\varphi_2) \)
- \( \text{inv}(\sigma) = \sigma_{\text{OUT}} \)
- \( \text{inv}(\Diamond \varphi) = \text{edge}_{\text{OUT}}[X / \text{inv}(\varphi)] \)
- \( \text{inv}(Y) = Y \)
- \( \text{inv}(\mu Y. \varphi) = \mu Y. \text{inv}(\varphi) \)

**Theorem:** \( f_T(G), v \not\models \varphi \iff G, v \not\models \text{inv}(\varphi) \)

Proof of the Theorem

**Theorem:** \( f_T(G), v \not\models \varphi \iff G, v \not\models \text{inv}(\varphi) \)

- By Induction on \( \varphi \). The essential case is:
  
  \[ G, v \not\models \text{inv}(\Diamond \varphi) \]
  
  \[ \iff G, v \not\models \text{edge}_{\text{OUT}}[X / \text{inv}(\varphi)] \quad \text{(definition of inv)} \]
  
  \[ \iff \exists w (G, v, X: \{w\} \not\models \text{edge}_{\text{OUT}} \text{ and } G, w \not\models \text{inv}(\varphi)) \quad \text{(ext)} \]
  
  \[ \iff \exists w ((v, w) \in E' \text{ and } G, w \models \text{inv}(\varphi)) \quad \text{(def of E')} \]
  
  \[ \iff \exists w ((v, w) \in E' \text{ and } f_T(G), w \not\models \varphi) \quad \text{(IH)} \]
  
  \[ \iff f_T(G), v \not\models \Diamond \varphi \quad \text{(definition of } \Diamond) \]
n-copying
Modal-$\mu$ Definable Transduction

A set of Modal-$\mu$ formulas $T =$
- $\sigma^k_{\text{OUT}}$ for each $\sigma \in \Sigma$, $k \in \{1 .. n\}$
- $\text{edge}^k_{\text{OUT}}$ for each $i, k \in \{1 .. n\}$: existential

defines a transformation $f_T$ converting
$G = (V, E, \pi)$ into $G' = (V^*\{1..n\}, E', \pi')$ where

- $\pi'( <v,k> ) = \{ \sigma \mid G, v \models \sigma^k_{\text{OUT}} \}$
- $E' = \{ (<v,i>, <w,k>) \mid G, v, X:\{w\} \models \text{edge}^k_{\text{OUT}} \}$

Example ($\Sigma = \{a, b, A, B\}$)

Example (without accumulating parameters) can be dealt with.
- For the detail of structural recursion over graphs, see [Buneman, Fernandez & Suciu 00]

- $\text{fun ev}( \xrightarrow{a} x ) = ^1 A \xrightarrow{2} A \xrightarrow{3} \text{od}(x)$
- $\text{fun ev}( \xrightarrow{b} x ) = ^1 B \xrightarrow{2} \text{od}(x)$
- $\text{fun od}( \xrightarrow{a} x ) = ^3 A \xrightarrow{4} \text{ev}(x)$
- $\text{fun od}( \xrightarrow{b} x ) = ^3 B \xrightarrow{4} \text{ev}(x)$
Pre-Image Computation

- \( \text{inv}_k(\text{False}, \Delta) = \text{False} \)
- \( \text{inv}_k(\neg \varphi, \Delta) = \neg \text{inv}_k(\varphi, \Delta) \)
- \( \text{inv}_k(\varphi_1 \lor \varphi_2, \Delta) = \text{inv}_k(\varphi_1, \Delta) \lor \text{inv}_k(\varphi_2, \Delta) \)
- \( \text{inv}_k(\sigma, \Delta) = \sigma^\text{OUT} \)
- \( \text{inv}_k(\Diamond \varphi, \Delta) = \bigvee_{j}^{1..n} \text{OUT}(X / \text{inv}_j(\varphi, \Delta)) \)
- \( \text{inv}_k(Y, \Delta) = Y_k \text{ if } k \in S \)
- \( \text{inv}_k(Y, \Delta) = \mu Y_k \cdot \text{inv}_k(\varphi, \Delta[Y \rightarrow \{k\}, \varphi]) \) where \((S, \varphi) = \Delta(Y)\)
- \( \text{inv}_k(\mu Y. \varphi, \Delta) = \mu Y_k \cdot \text{inv}_k(\varphi, \Delta[Y \rightarrow \{k\}, \varphi]) \)

**Thm:** \( f_T(G), <v,k> \not\models \varphi \iff G, v \not\models \text{inv}_k(\varphi, \{\}) \)

Example

\[
\begin{align*}
\text{edge}^{11}_{\text{OUT}} & \equiv \text{edge}^{12}_{\text{OUT}} \equiv \text{edge}^{21}_{\text{OUT}} \equiv \text{edge}^{22}_{\text{OUT}} \equiv \Diamond X \\
\text{a}^1_{\text{OUT}} & \equiv \text{a}^2_{\text{OUT}} \equiv \text{a}
\end{align*}
\]

- \( f(G), <v,1> \not\models \mu Y. (a \land \Diamond Y) \)
- \( G, v \not\models \mu Y_1. \text{inv}_1(\mu Y_1 \land Y) \)
- \( G, v \not\models \mu Y_1. \mu Y_1 \cdot \text{inv}_1(\Diamond Y_1 \lor \Diamond Y_2) \)
- \( G, v \not\models \mu Y_1. \mu Y_1 \cdot \text{inv}_2(\Diamond Y_1 \lor Y_2) \)
- \( G, v \not\models \mu Y_1. \text{inv}_1(\Diamond Y_1 \lor \Diamond Y_2) \)
- \( G, v \not\models \mu Y_1. \text{inv}_2(\Diamond Y_1 \lor \Diamond Y_2) \)

Open Question: can \( \text{inv}(\mu) \) be shorter than \((n-1)! + 1\) ?

Some Useful Results

**Theorem:**

Modal-\(\mu\) Definable Transduction is closed under composition.

Construction is analogous to \(\text{inv}(\varphi)\).

**Theorem:**

Modal-\(\mu\) Definable Transduction \(\iff\) MSO Definable & Bisimulation-Invariant.

It is known that Bisimulation-Invariant MSO transduction is equal to structural recursion [Colcombet & Löding 04].
Conclusion

- Modal-\(\mu\) Definable Transduction
- Pre-Image of a modal-\(\mu\) sentence is computable
- Structural recursion is expressible
- (Not in the talk)
  - Node-erasing transformations
  - Edge-labeled graphs
  - Transformations with multiple inputs/outputs

Future Work

- Implementation
- Addition of Backward Modality
  - \((G,v \models \phi) \iff \exists (w,v) \in E \text{ s.t. } G,w \models \phi\)\)
- Syntactic necessary condition for \(\text{edge}_{\text{OUT}}\)
- More concise formula for \(\text{inv}(\mu Y.\phi)\)

References

[Trakhtenbrot 50] Impossibility of an Algorithm for the Decision Problem for Finite Classes
- Satisfiability of FO on graphs is undecidable

[Meyer 74] Weak monadic second order theory of successor is not elementary-recursive
- Satisfiability of MSO on finite strings is Non-Elementary

[Robertson 74] Structure of Complexity in the Weak Monadic Second-Order Theories of the Natural Numbers
- Satisfiability of FO[\text{-}] on finite strings is Non-Elementary

- Satisfiability of Modal Logic on graphs is PSPACE-complete

[Emerson & Julfa 88] The Complexity of Tree Automata and Logics of Programs
- Satisfiability of Modal-\(\mu\) on graphs is EXPTIME-complete

[van Benthem 86] Essays in Logical Semantics
- FO \(\cap\) Bism = Modal

[Janin & Walukiewicz 96] On the Expressive Completeness of the Propositional \(\mu\)-Calculus with Respect to Monadic Second Order Logic
- MSO \(\cap\) Bism = Modal-\(\mu\)

[Colcombet & Löding 04] On the Expressiveness of Deterministic Transducers over Infinite Trees
- MSO-Definable Graph Transduction \(\cap\) Bism = Structural Recursion

[Courcelle 94] Monadic Second-Order Definable Graph Transductions: A Survey
- On MSO-Definable Transduction
Determining the Valid Parameters for the Weight-Balanced Tree Algorithm

Yoichi Hirai
IST, the University of Tokyo

January 11, 2011

(joint work with Kazuhiko Yamamoto at Internet Initiative Japan)

History of Weight-Balanced Tree Algorithm

1972 proposed by Nievergelt and Reingold
1992 valid parameter determination and an example implementation of set operations by Adams
–1995 an implementation by Adams in MIT-Scheme (buggy)
1998 another Scheme implementation in SLIB (buggy)
–2002 Data.Map and Data.Set implementation in Hackage

2010-08-03 A bug found in Data.Map
a tree got unbalanced after a delete

buggy: violating the restriction posed by the algorithm design.
Question

- There is a parametrized binary tree algorithm
  $\Delta$ decides whether a tree is balanced
  $\Gamma$ chooses a balancing strategy:
  single/double rotation
- Wrong parameters break balance
  (found to be a common mistake)

Q. What parameters are correct?

Weight-Balanced Tree Algorithm
(Nievergelt and Reingold, 1972)

- $\Delta ::= \bot \mid \triangleleft \triangleleft$
- $#(\bot) = 0$
- $#(\triangleleft \triangleleft ) = 1 + #x + #y$

The balance condition with $\Delta$ (wrong version)

The top node is balanced iff

$$#L \leq \Delta \times #R$$

and vice versa
The balance condition with $\Delta$

The top node is balanced iff

$$\#L + 1 \leq \Delta \times (\#R + 1)$$

and vice versa

Balancing Strategy 1: Single Rotation

Balancing Strategy 1: Single Rotation is Not Enough

...when the black part is too large, this cannot balance the whole.
Balancing strategy with $\Gamma$

choose double rotation

when $\#M + 1 \geq \Gamma \times (\#R + 1)$

Two Parameters and One Question

- $\Delta$ for balance condition
- $\Gamma$ for choosing single or double

Q. Under what $(\Delta, \Gamma)$ every insert/delete keeps balance?

Nievergelt and Reingold has $(1 + \sqrt{2}, \sqrt{2})$. Comparing $(1 + \sqrt{2})m$ and $n$ is costly (taking square?).

1992: Adams’s Analysis
2010: Shadow of Doubt

On Hackage, the bug ticket was closed after they changed the parameters.

QuickCheck Result by Kazu Yamamoto

apparently bounded.

Omega: Presburger Solver

copied Coq response changed / into && and so on.
Conjecture

(sound) in the area, balance never broken
(complete) outside the area, balance can be broken

Completeness Proof

1. given any parameter pair (just) below the lower boundary,
2. take large enough $z$ so that
   $$z \geq \frac{\Gamma - \Delta + \Gamma}{1 + \Delta - \Gamma} \sim \frac{\text{positive}}{\text{small positive}}$$
3. deletion in the left subtree breaks the balance

Soundness Proof

**Goal:** Within the range, the balance is never broken.
Reasons for using proof assistant Coq rather than proving by hand:
- many cases on parameter pairs
- every operation on every tree
- nested if in every operation
- balance condition of every subtree
The Soundness Proof

12,900 lines of Coq.

The soundness proof

12,900 lines of Coq.

Required Time

- 62 days from 2010-08-18 to 2010-10-18
- 208 lines per day among other things

Arithmetic Lemmas

Lemma NR_deep_insert:
  good_params ->
  forall (a b c d e: Z),
  ?????
  (a#1) (b#1) (c#1) (d#1) (e#1).

Informally: \(a, b, c, d, e\) are

\[\begin{array}{c}
 a \\
 b+1 \\
 c \\
 d \\
 e \\
\end{array}\]

\(\leftarrow\) the tree just before rotation
Arithmetic Lemma: Expanded

good_params ->
forall a b c d e : Z,
balance (a # 1) (b # 1) ->
  ~ balance (a # 1) ((b # 1) + 1) ->
(c #1) + (d #1) + 1 + (e #1) + 1 == (b #1) + 1 ->
balance (c # 1) (d # 1) ->
balance ((c # 1) + (d # 1) + 1) (e # 1) ->

if NR_isSingleSize ((c # 1) + (d # 1) + 1) (e # 1)
then
  balance (a # 1) ((c # 1) + (d # 1) + 1) /
  balance (c # 1) (d # 1) /
  balance ((a #1) + (c #1) + (d #1) + 1 + 1) (e # 1)
else
  balance (a #1) (c #1) /
  balance (d #1) (e #1) /
  balance ((a #1) + (c #1) + 1) ((d #1) + (e #1) + 1)

Arithmetic Lemma: Proof Structure

▶ case analysis for Δ
▶ case analysis for special small trees
   needed because of this kind of reasoning:
   \( b > 2.5 \) implies \( b \geq 3 \) because \( b \in \mathbb{Z} \)
▶ reducing \( \mathbb{Q} \) argument into \( \mathbb{Z} \) argument
▶ psatz tactics

Arithmetics is Not Enough

We have to define binary trees.

Module FSet (X: OrderedType).

Definition Size := Z.
Definition k := X.t.

Inductive FSet :=
| Tip: FSet
Arithmetics is Not Enough

We have to define insertion.

Findpoint insert (kx:k) (t:FSet): FSet :=
match t with
| Tip => singleton kx
| Bin _ ky l r =>
  match X.compare kx ky with
  | GT _ => balanceL ky l (insert kx r)
  | LT _ => balanceR ky (insert kx l) r
  | EQ _ => bin l k x r
end
end.

Arithmetics is Not Enough

Definition balanceR (kx: k) (l r:FSet) :=
match (isBalanced r l) with
| true => bin k x l r
| false => rotateR k x l r
end.

Arithmetics is Not Enough

Definition rotateR :
  k -> FSet -> FSet -> FSet :=
fun k l r =>
match l with
| Tip => assert_false k l r
| Bin _ _ ll lr =>
  if isSingle lr ll then
    singleR k l r
  else
    doubleR k l r
end.
Insert and Delete

Lemma insert_balanced:
forall (t: FSet) (kx: k),
good_params ->
Is_true (balanced t) -> validsize_rec t ->
Is_true (balanced (insert kx t)).

Lemma delete_balance:
good_params ->
forall (x: k) (t: FSet),
validsize_rec t ->
Is_true (balanced t) ->
Is_true (balanced (delete x t)).

▶ induction on t
▶ case whether size changed or not

Set Operations

(request by Milan Straka, the maintainer of the containers package in Hackage)

▶ difference, union: straightforward
▶ some trick required for defining intersection
induction on two arguments

Intersection Used This Induction

Fixpoint pair (l r: Tree): TreePair :=
match l with
| Tip =>
  match r with
  | Tip => TipTip
  | Bin r1 rr => TipBin r1 rr
  end
| Bin ll lr =>
  match r with
  | Tip => BinTip ll lr
  | Bin rl rr => BinBin (pair l rl) (pair lr r)
  end
end.

Experimental Function command solved this
also, I packed two arguments in a single pair
Achievements

1972 Proposed by Nievergelt and Reingold
1992 parameter analysis and an example implementation of set operations by Adams
1995 or older MIT-Scheme implementation by Adams (buggy)
1998-02-09 SLIB implementation (buggy)
-2002 Data.Map (buggy) and Data.Set implementation in Hackage
2010-08-03 A bug: tree got unbalanced
2010-10-19 Submitted a paper to Journal of Functional Programming with a Coq proof script
2010-12-18 SLIB incorporated our change

A sequel: a bug in Z3
Z3 is an SMT (satisfiability modulo theory) solver developed by Microsoft.

1. We tried using Z3 instead of Omega Presburger solver
2. Z3 gave a different result from Omega’s result
3. Eventually, we found a bug in Z3 and reported it to Nicolaj Bjørner, whose team fixed it.

Bug highlight:

assertions.
satisfiable? → no
more assertions.
satisfiable? → yes

Small, One-Shot Project, but It Produced

- a bug fix for libraries
- new rigorous knowledge on a widely-used algorithm
- a modestly complex problem for SMT solvers
WBT is Chosen When Storing 2-Bit Information is Costly

- **AVL / Red-Black** Each node stores small information:
  - height difference / node-state

- **Weighted Balance Trees** Each node stores size of the subtree.
  - can be used for index operations
  - 2 bits can be stored efficiently in LSBs of a pointer in IA32
  - but common Haskell / Scheme implementations do not exploit this
  - a binary tree with index operations can be used instead of updatable arrays.
Motivation

The context for this talk:

- Specification and verification of concurrent and distributed systems.
- **Key concept**: interaction.

This is not a technical talk, we seek to motivate and explain two topics:

- Cooperative vs. adversarial specifications.
- Interactions viewed as games.

Introduction

An interaction happens when several parties perform certain actions affecting each other (communication scenarios, business processes, computer programs, ...)

An interaction specification is a set of requirements about the interaction:

- Something must happen/something must not happen, choices, deadlines, ...  
- Examples: Protocol specifications, business process languages, workflows, session types ...
Programming by contract - scenario

Programming by contract (PBC) facilitates modular construction of software, by means of formal specifications.

- Consider a code producer assigned with the task of producing a program satisfying some specification.
- The task is broken down into several modules, each with a formally specified interface (typically with pre- and postconditions).
- Several different programmers can now work on the different modules and then if all developed modules satisfy their specifications, the full program will also satisfy its specification.

A cooperative world?

Most formal specifications are done in a cooperative way:

- All participants work to fulfill a set of common goals.
  - Every programmer want the final program to work.

- If the goals are not formalized, the participants are expected to follow the intentions behind.
  - If the specification does not rule out infinite loops, no programmer should just implement the trivially looping program.

- There is no notion of what happens after a failure to follow the specification
  - In case of a programming error, the module must be corrected before the main program can work.

- Often based on partial correctness.
  - Enables runtime monitoring of specifications.

Problems with cooperative settings

The cooperative methodology contains hidden problems:

- It only takes one participant with conflicting goals to “topple the house of cards” (e.g. one participant who refuses to answer anything in a partial correctness setting).

- How to decide whether someone has followed the intentions?

- What if the specification is not followed? Failures do happen.

- If I am allowed to loop - why not loop always (partial correctness), what can an eventually guarantee be used for (except fulfilling another eventually guarantee?)
Problems with cooperative settings - cont.

Participants may seem to have the same goals, but in reality slightly conflicting goals:

The original specification could have been a compromise, which is not captured in the cooperative setting.

PBC scenario - cooperative problems

The scenario seems natural at first, but several problems exist:
- The programmers need to fulfill the specification, but is there anything that forces the programmer to use the best solution, or even a good solution? what happens if suboptimal solutions are used?
- How are the programmers paid (lines of code, number of finished modules, ...)? would they prefer a quick solution to a good one?
- What if a third party code is used, can the programmers just blame that? (e.g. a library picked by the programmer).

Adversarial composition

In an adversarial setting each participant is an autonomous entity:
- Each participant is potentially an adversary of the other participants.
- Each participant has its own set of goals, not necessary compatible with the goals of the other participants.
- A participant will defect from the “intended” path or even break a whole specification if it is more beneficial in terms of his own goals.
- A participant will still follow rules if the penalty for breaking them or the reward for following them, is large enough. (Cooperation by need)
- It is in general not enough for a participant to just reflect blame for a failure. The participant must assume responsibility by quantifying the penalty or reward.
PBC - adversarial view

The adversarial viewpoint illuminates the problems:

- If the programmers have their own goal, they might produce suboptimal code, unless they are penalized/rewarded accordingly.
- The consequences for breaking a specification must be clear, i.e. what is the risk. In an adversarial setting it could be broken at any time.
- In particular, we should never let a high-assurance service rely on a low-assurance one (e.g. a third party one).
- Instead of the traditional distinction between a module and its environment, one has to consider the environment not as a monolithic entity, but as a composite entity consisting of multiple parts.

Comparison - cooperative vs. adversarial

- In the cooperative setting the participants share the same goals, and therefore follow the specifications directly.
- In the adversarial setting the participants have their own goals, and are only responsible for actions in terms of rewards and penalties.
- In the cooperative setting the focus is on the “happy” path, and potential failures are ignored.
- In the adversarial setting the focus is on the “unhappy” path, and failures always have to be taken into account.

Apparently cooperative settings

Even apparently cooperative settings benefit from an adversarial viewpoint:

- Assuming responsibility in case of failure is more robust than just propagating blame.
- The cooperative participants can be seen as working together against a common adversary (e.g. the laws, Nature), whose goals not necessarily are compatible with the goals of the participants.
- No need to assume that the participants have the same goals.
- One can compare/analyse implementations in terms of the rewards/penalties.
Interaction as games

Adversarial interactions can be seen as extensive-form games:

Game-theoretic concepts

The realisation of the game-theoretic concepts are summarised in the following table:

<table>
<thead>
<tr>
<th>Concept</th>
<th>Realisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Players</td>
<td>Participants</td>
</tr>
<tr>
<td>Moves</td>
<td>Actions</td>
</tr>
<tr>
<td>Specifications</td>
<td>Game rules</td>
</tr>
<tr>
<td>Payoffs</td>
<td>Rewards/penalties</td>
</tr>
<tr>
<td>Strategies</td>
<td>Implementations (programs)</td>
</tr>
<tr>
<td>Winning strategies</td>
<td>Correct programs</td>
</tr>
<tr>
<td>Dominant strategies</td>
<td>Optimized programs</td>
</tr>
</tbody>
</table>

PBC - game-theoretic view

- To capture interaction, pre- and postconditions are generalized to extensive-form games.
- Because of the adversarial nature, using eventually guarantees as total correctness is not enough.
- Instead, we need a notion of timed total correctness, corresponding to real-time deadlines (similar to protocol specifications).
  - Enables runtime monitoring.
- Note: Deadlines are not restricted to interaction specifications. When more robust specifications are needed, they also make sense for pre- and postcondition type specifications.
Strategies

When program code is seen as the strategy, the running code can be seen as an agent operating on behalf of a principal (the programmer):
- When the strategy is chosen, the agent carries out the orders specified by the strategy and the principal cannot influence the agent anymore.
  - The running code cannot be changed at runtime, unless directly modelled as input.
- The agent does not have knowledge about or is responsible for the games of the principal, the agent might not be able to observe all moves during runtime (e.g. for a delegation scenario).

Formal models

Previous work has devised a concrete game-theoretical model\(^1\):
- Based on two-party games with quantifiable payoffs.
- Notion of conformance of a program (strategy), \(p\), with respect to a set of specifications (games), written \(\models p : s_1, \ldots, s_n\).
  - \(p\) will ensure that the total payoff is always non-negative, meaning that it will never be the first to break a specification.
- Compositionality theorem: If \(\models p_1 : s_1, s_2\) and \(\models p_2 : s_1, s_2\) and only \(s\) mentions the internal communication between \(p_1\) and \(p_2\) then \(\models p_1 \parallel p_2 : s_1, s_2\).
- \(s\) is the same specification as \(s\) but with the roles of the two players interchanged, \(p_1 \parallel p_2\) are the programs running in parallel.

\(^1\)A. S. Henriksen, T. Hvitved, A. Filinski, A game-theoretic model for distributed programming by contract.

Formal models - cont.

Current work is concerned with revising the model, key concepts include:
- Specifications based on events instead of actions.
- Hierarchical events (events definable from other events).
  - Compositionality of specification development, refinement of specifications.
- Quantitative vs. qualitative events.
  - Some properties are hard to quantify, but some specifications need to mention those properties alongside quantifiable events.
  - Mix quantitative and qualitative events in the same specification.
Perspective

This work was done in the context of the project TrustCare: Trustworthy Pervasive Healthcare Services\(^2\).

- Trustworthy it-systems in the healthcare sector.

We believe that a game-theoretic model based on an adversarial approach would serve well as a foundation for not only interaction specifications for code, but also for e.g. workflows employed in the healthcare domain.

Early work was done in cooperation with Tom Hvitved:

- Ideas were applied to business processes as well.

- Current work separates from THV’s work by being closer to game-theory (e.g. payoffs).

\(^2\)www.trustcare.eu

Summary

It might be hard to convince people to use the adversarial model:

- Existing modelling approaches are cooperative, one has to reverse engineer the scenarios behind them.

- Many scenarios seem cooperative at the first glance.

- The adversarial model forces people to consider breaches, failures etc. - which might be very hard to account for.

Regardless, we think that the adversarial model:

- Gets the problems out in the open.

- Is a generalization of the cooperative setting.

- Is fundamentally how the world works.
Jigsaw Radix Conversion

Keisuke Nakano
The University of Electro-Communications

The 4th DIMU-IST workshop, 11.01.11.

[Q] What is a binary representation for ternary representation "2 0 1"?

- First compute the number.
  - $2 \cdot 3^2 + 0 \cdot 3^1 + 1 \cdot 3^0 = 19$.
  - $0 \cdot 3 \cdot (3 \cdot 2 + 0) + 1 = 19$ with Horner scheme.

- Then divide it by 2 repeatedly.
  - $19 = 2 \cdot 9 + 1$;
  - $9 = 2 \cdot 4 + 1$;
  - $4 = 2 \cdot 2 + 0$;
  - $2 = 2 \cdot 1 + 0$; hence we have "1 0 0 1 1".

[Q] How can we solve it w/o +, -, ·, /, and %?

A solution is ...

- 6 kinds of jigsaw pieces!

- Each curve stands for a number.

  0

  1

  2
How to execute the radix conversion

[Q] What’s a binary number for "201" in ternary?

- Neither rotation nor flip is allowed.
- Each piece can be used many times.

Reveal the trick

- Each piece satisfies: $3N + E = S + 2W$.
  - Vertical edges have curve 0, 1 or 2.
  - Horizontal edges have curve 0 or 1.

- Then any $(k \times l)$-board sides satisfy:
  $$3^l \sum_{i=0}^{k-1} 2^i N_i + \sum_{j=0}^{l-1} 3^j E_j = \sum_{i=0}^{k-1} 2^i S_i + 2^l \sum_{j=0}^{l-1} 3^j W_j$$

Reveal the trick

- Each piece satisfies: $3N + E = S + 2W$.
  - Vertical edges have curve 0, 1 or 2.
  - Horizontal edges have curve 0 or 1.

- Then any $(k \times l)$-board sides satisfy:
  $$3^l \sum_{i=0}^{k-1} 2^i N_i + \sum_{j=0}^{l-1} 3^j E_j = \sum_{i=0}^{k-1} 2^i S_i + 2^l \sum_{j=0}^{l-1} 3^j W_j$$
Generalization

- $m$-to-$n$ conversion requires $mn$ kinds of pieces.
  - Each satisfies $mN + E = S + nW$
  - Horizontal: $N, S = 0, \ldots, n - 1$
  - Vertical: $E, W = 0, \ldots, m - 1$
  - Board sides satisfy
    $$m \sum_{i=0}^{k-1} n^i N_i + \sum_{j=0}^{l-1} n^j E_j = \sum_{i=0}^{k-1} n^i S_i + n^k \sum_{j=0}^{l-1} m^j W_j$$
  - It can be generalized for $n^{th}$ gray and balanced-3.

Feature of the jigsaw method

- North/East edges determine South/West ones.
  - No other result is obtained.
  - There are many possible orders to place pieces.
Feature of the jigsaw method

- North/East edges determine South/West ones.
- No other result is obtained.
- There are many possible orders to place pieces.

Feature of the jigsaw method

- North/East edges determine South/West ones.
- No other result is obtained.
- There are many possible orders to place pieces.

Other features

- Inversion \((m\text{-to-}n \text{ conv. } \Rightarrow n\text{-to-}m \text{ conv.})\)
  - \(mN + E = S + nW \iff nW + S = E + mN\)
- Base exponentation
  - Piece combination makes \(m^k\text{-to-}n^l\) radix conversion
  - 3-to-4 radix conversion (using 3-to-2 pieces)
Set of jigsaw pieces as function

\[ \text{pset} :: (\text{HCurve}, \text{VCurve}) \mapsto (\text{HCurve}, \text{VCurve}) \]

- **pset** determines \( S \) and \( W \) from \( N \) and \( E \).
  - **HCurve** - horizontal curves for \( N / S \) edges
  - **VCurve** - vertical curves for \( E / W \) edges

- **Example for 3-to-2 base conversion**
  - Set of curves
    - data \( \text{HCurve} = H_0 \quad | \quad H_1 \)
    - data \( \text{VCurve} = V_0 \quad | \quad V_1 \quad | \quad V_2 \)
  - Set of pieces
    - \( \text{pset} (H_0, V_0) = (H_0, V_0) \)
    - \( \text{pset} (H_0, V_1) = (H_1, V_0) \)
    - \( \text{pset} (H_0, V_2) = (H_0, V_1) \)
    - \( \text{pset} (H_1, V_0) = (H_1, V_1) \) (highlighted)
    - \( \text{pset} (H_1, V_1) = (H_0, V_2) \)
    - \( \text{pset} (H_1, V_2) = (H_1, V_2) \)

Jigsaw function

\[ \text{jigsaw} :: ((H, V) \mapsto (H, V))) \mapsto (\{H\}, \{V\}) \mapsto (\{H\}, \{V\}) \]

- We first consider a bounded board.
  - It will be extended for jigsaw radix conversion.
- Jigsaw functions map \( N/E \) sides onto \( S/W \) sides.
  - \( \text{(jigsaw pset)} :: (\{H\}, \{V\}) \mapsto (\{H\}, \{V\}) \)
Auxiliary functions: pflip, mealy

- **Argument flipping**
  
  \[
  \text{pflip}:: \{(a,b)\mapsto (a,b)\} \mapsto (b,a) \mapsto (b,a)
  \]

  \text{pflip } f = \text{ swap } . \ f . \ \text{swap}

  \text{ where } \ \text{swap } (x,y) = (y,x)

- **Mealy machine (automaton with output)**

  \[
  \text{mealy}_l:: \{(a,b)\mapsto (a,b)\} \mapsto (a,[b]) \mapsto (a,[b])
  \]

  \text{ where } \ (q_0,[0,0,1,2]) \Rightarrow (q_0,[0,2,1,2])

  \[
  \text{mealy}_l \ f \ (a,[\ ] ) = (a,[\ ] )
  \]

  \[
  \text{mealy}_l \ f \ (a,b;bs) = (a',b';bs')
  \]

  \text{ where } \ (a',b') = \ f \ (a,b)

  \ (a',bs') = \text{mealy}_l \ f \ (a',bs)

  \text{mealy}_r \text{ is similarly defined.}

Jigsaw constructed by Mealy

- **1-column jigsaw corresponds to mealy**

  - HCurve - state; VCurve - input/output

  - \((\text{mealy}_r \text{ pset})::(H,[V])\mapsto (H,[V])\)

    - \text{mealy}_r::(a,b)\mapsto (a,[b]) \mapsto (a,[b])

    - \text{pset}::(H,V)\mapsto (H,V)

- \text{pflip} (\text{mealy pset})::([V],H)\mapsto ([V],H)

- \text{mealy}_l (\text{pflip} (\text{mealy}_r \text{ pset}))

  :: ([V],[H])\mapsto ([V],[H])

- \text{pflip} (\text{mealy}_l (\text{pflip} (\text{mealy}_r \text{ pset})))

  :: ([H],[V])\mapsto ([H],[V])

\equiv \text{jigsaw pset}

On piece placing strategy

\[
\text{jigsaw} = \text{pflip} . \text{mealy}_l . \text{pflip} . \text{mealy}_r
\]

- It corresponds to a 'vertical' strategy.

  - First compute for each vertical line.

  - Then integrate them in horizontal way.
Jigsaw by Mealy, again

- Run 1-raw jigsaw by mealy
  - \textbf{HCurve} - input/output; \textbf{VCurve} - state
  - \texttt{mealy\_l(pflip pset)} :: (V, [H]) \rightarrow (V, [H])
  - \texttt{mealy\_l} :: (a, b) \rightarrow (a, b)
  - \texttt{pset} :: (H, V) \rightarrow (H, V)
  - \texttt{pflip(mealy\_l(pflip pset))} :: ([H], V) \rightarrow ([H], V)
  - \texttt{mealy\_r(pflip(mealy\_l(pflip pset)))} :: ([H], [V]) \rightarrow ([H], [V])
  - jigsaw pset

Jigsaw in vertical / horizontal

- ... beautiful symmetric equation!

\[
\text{jigsaw} = \text{pflip} \cdot \text{mealy\_l} \cdot \text{pflip} \cdot \text{mealy\_r} \\
= \text{mealy\_r} \cdot \text{pflip} \cdot \text{mealy\_l} \cdot \text{pflip}
\]

Other Piece Placing Strategies

- Possibly neither horizontal nor vertical
  - Diagonal way
  - Random way
  - Parallel way
Other Piece Placing Strategies

- Possibly neither horizontal nor vertical
  - Diagonal way
  - Random way
  - Parallel way

Formalization for arbitrary strategies

- Frontier-line pushing approach
  - type FrLine = [Either HCurve VCurve]
  - Left _ (L) - horizontal;
    Right _ (R) - vertical

- Placing a piece \( \equiv \) rewriting \([R E, L N] \) to \([L S, R W] \)
  - \(E, N, S,\) and \(W\) are defined by a piece.
Formalization for arbitrary strategies

- **Frontier-line pushing approach**
  - type FrLine =
    - Either HCurve VCurve
  - Left (L) - horizontal;
  - Right (R) - vertical

- Placing a piece \( \Rightarrow \) rewriting \([ R E, L N ]\) to \([ L S, R W ]\)
  - \( E, N, S \), and \( W \) are defined by a piece.

Formalization for arbitrary strategies

- **Frontier-line pushing approach**
  - type FrLine =
    - Either HCurve VCurve
  - Left (L) - horizontal;
  - Right (R) - vertical

- Placing a piece \( \Rightarrow \) rewriting \([ R E, L N ]\) to \([ L S, R W ]\)
  - \( E, N, S \), and \( W \) are defined by a piece.
Formalization for arbitrary strategies

- Frontier-line pushing approach
  - type FrLine = [Either HCurve VCurve]
  - Left _ (L) - horizontal;
  - Right _ (R) - vertical
  - [L H1, L H1, L H0, L H0, L H1, R V0, R V0, R V0]

- Placing a piece = rewriting [R E, L N] to [L S, R W]
  - E, N, S, and W are defined by a piece.

Jigsaw in frontier-line approach

- With non-deterministic pattern (pseudo code)
  - It can runs in parallel.

  ```
  push :: ((a,b)→(a,b)) → [Either a b] → [Either a b]
  push f (zs1 ++ [Right b, Left a] ++ zs2) =
  push f (zs1 ++ [Left a', Right b'] ++ zs2)
  where (a',b') = f (a,b)
  push f zs = zs

  jigsaw :: ((H,V)→(H,V)) → ([H],[V])→([H],[V]))
  jigsaw pset (hs,vs) =
  partition (push pset (map Right vs ++ map Left hs))

  -- partition :: [Either a b] → ([a],[b])
  -- It should work as you expected!
  ```

Infinitely wide board

- Board should be extended until straight-line.
  - How to extend for HCurve (b0)
  - When to stop for VCurve (p)

- Redefine only mealy_L function as mealy_L

  ```
  mealy_L :: (a→Bool)→b→((a,b)→(a,b))→(a,[b])→(a,[b])
  mealy_L p b0 f (a,[]) =
  if p a then (a,[f]) else (a',b':bs')
  where (a'',b') = f (a,b0)
        (a',bs') = mealy_L p b0 f (a'',[l])
  mealy_L p b0 f (a,b:bs) = (a',b':bs')
  where (a'',b') = f (a,b)
        (a',bs') = mealy_L p b0 f (a'',bs)
  ```
Inf. jigsaw in horizontal/vertical

- Similar equations hold!

\[
\text{jigsawX } p \ b0 \\
= \text{pflip . mealy_L } (\text{all } p) \ b0 \ . \ \text{pflip . mealy_r} \\
= \text{mealy_r . pflip . mealy_L } p \ b0 \ . \ \text{pflip}
\]

Frontier-line approach for inf.

- Just modify push function

\[
\begin{align*}
\text{pushX} &:: (a \rightarrow \text{Bool}) \rightarrow b \rightarrow \\
((a,b) \rightarrow (a,b)) \rightarrow [\text{Either } a \ b] \rightarrow [\text{Either } a \ b] \\
\text{pushX } p \ b0 \ f \ (zsl1 ++ [\text{Right } b', \ \text{Left } a'] ++ zs2) &= \\
\text{pushX } p \ b0 \ f \ (zsl1 ++ [\text{Left } a', \ \text{Right } b'] ++ zs2) \\
\text{where} \ (a',b') &= f \ (a,b) \\
\text{pushX } p \ b0 \ f \ zs \ |
\text{cond} = zs \\
\text{--- cond holds iff no } [L,R] \ \text{and all } L \ \text{satisfy } p \\
\text{pushX } p \ b0 \ f \ zs &= \text{pushX } p \ b0 \ f \ (zs++[\text{Left } b])
\end{align*}
\]

\[
\begin{align*}
\text{jigsawX} &:: (a \rightarrow \text{Bool}) \rightarrow b \rightarrow \\
((H,V) \rightarrow (H,V)) \rightarrow ((H,[V]) \rightarrow ([H],[V])) \\
\text{jigsawX } p \ b0 \ pset \ (hs,vs) &= \\
\text{partition} \\
&\quad (\text{pushX } p \ b0 \ pset \ (\text{map Right vs } ++ \text{ map Left hs}))
\end{align*}
\]

Jigsaw theorem

If \( g(z,y') = (y,z') \)
\[
\land f \ x = (y,x') \land f \ b0 = (_,b0) \\
\Rightarrow f (g z x) = (y, g z' x'),
\]
then \( \text{jigsawX } (\ldots p \ldots) b0 \)
\[
((\text{id} \times \text{fst.g}^{-1}).f.g.\text{swap}) \\
= \text{unfoldl } p \ f \ . \ \text{foldr } g \ b0
\]

- cf. Streaming theorem [BirdGibbons03]

If \( f \ z = (y,z') \Rightarrow f(g(z,x)) = (y, g(z',x)) \)
Then stream \( f \ g = \text{unfoldr } f \ . \ \text{foldl } g \)
Summary and further work

- We introduced Jigsaw radix conversion method.
  - The trick has been revealed.
  - Functional formalization is presented.

- Now working on:
  - Better formulation of jigsaw theorem
    - \( \text{jigsaw} \ (\ldots f \ . \ g \ldots) = \text{unfoldl} \ f \ . \ \text{foldr} \ g \)
  - Jigsaw fusion
    - Find \( h \) such that \( \text{jigsaw} \ f \ . \ \text{jigsaw} \ g = \text{jigsaw} \ h \)
    - \( f \) and \( g \) should have right inverse, I expect.

Other topics

- Application
  - Parsing lin. conj. grammars (like trellis automaton)
  - Sort (not efficient)

- Universality
  - Frontier-line simulates Turing machine
  - Related with Wang's tile (domino problem)

- (Parallel?) complexity
  - Depends on what to be primitive
Compositional Data Types
A Report from the Field

Patrick Bahr
paba@diku.dk

University of Copenhagen, Department of Computer Science

Fourth DIKU-IST Joint Workshop on
Foundations of Software,
January 10-14, 2011

joint work with Tom Hvitved and Morten Ib Nielsen

Outline

1. Compositional Data Types
2. A Toolbox for Prototyping Programming Languages
3. Conclusions
The Setting
Domain-Specific Languages in POETS

- We have a number of domain-specific languages.
- Each pair shares some common sublanguage.
- All of them share a common language of values.
- We have the same situation on the type level!

How do we implement this system without duplicating code!

How Can we Compose Data Structures?
...and Functions Defined on Them?

- This is easy on non-recursive data structures.
- Composition by sum or product.

For recursively defined data structures this is different.

Example (A simple expression language)

```hs
data Expr = Val Int
        | Add Expr Expr

eval :: Expr -> Int
eval (Val x) = x
eval (Add x y) = eval x + eval y
```

Compositional Data Types

Expression Problem [Phil Wadler]

The goal is to define a data type by cases, where one can add new cases to the data type and new functions over the data type, without recompiling existing code, and while retaining static type safety.

"Data Types à la Carte" by Wouter Swierstra (2008)

A solution to the expression problem: Decoupling!

- data types: decoupling of signature and term construction
  - isolated signature (expression data type without recursion)
  - explicit recursive construction of terms over arbitrary signatures
- functions: decoupling of pattern matching and recursion
  - functions are defined on signatures
  - recursion is added separately
- signatures (+ functions defined on them) can be composed
Decoupling Signature and Term Construction

The data type contains both the signature of operations and the inductive definition of terms over them through recursion.

```haskell
data Expr = Val Int
           | Add Expr Expr
```

Remove recursion from the definition

```haskell
data Sig e = Val Int
           | Add e e
```

Recursion can be added separately

```haskell
data Term f = Term (f (Term f))
```

Term Sig $\cong$ Expr

Combining Signatures

In order to extend expressions, we need a way to combine signatures.

Direct sum of signatures

Type constructor :+: of kind (* -> *) -> (* -> *) -> (* -> *):

```haskell
data (f :+: g) e = Inl (f e) | Inr (g e)
```

Example

```haskell
data Sig e = Val Int
           | Add e e
data Val e = Val Int
data Add e = Add e e
```

Val :+: Add $\cong$ Sig

Separating Function Definition from Recursion

Compositional function definitions as algebras

In the same way as we defined the types:
- define functions on the signatures (non-recursive): \( f \colon a \to a \)
- apply the resulting function recursively on the term: \( \text{Term} f \to a \)
- combine functions using type classes

Algebras

```haskell
class Eval f where
evalAlg :: f Int -> Int
```

Applying a function recursively to a term

```haskell
algHom :: Functor f => (f a -> a) -> Term f -> a
algHom f (Term t) = f (fmap (algHom f) t)
```
Defining Algebras

On the singleton signatures

```
instance Eval Val where
evalAlg (Val x) = x
instance Eval Add where
evalAlg (Add x y) = x + y
```

On sums of signatures

```
instance (Eval f, Eval g) => Eval (f :+: g) where
evalAlg (Inl x) = evalAlg x
evalAlg (Inr y) = evalAlg y
```

Applying the resulting unique homomorphism to terms

```
eval :: (Functor f, Eval f) => Term f -> Int
eval = algHom evalAlg
```

Outline

1. Compositional Data Types
2. A Toolbox for Prototyping Programming Languages
3. Conclusions

Using Compositional Data Types

Using Compositional Data Types in POETS

- Coarse-grained partition into only a few atomic signatures
  - one for base values
  - one for shared operations
  - operations for each individual language
  - syntactic sugar for each individual language
- similar on the type language

Now that we have this structure in place, can we make further use of it?
**Products on Signatures**

Annotate Syntax Trees, e.g. with source positions
- annotations are **not part of the actual language**
- annotations should be **added separately** (to the signature)
- functions that are **agnostic** to annotations should **not care** about them

**Constant Products on Signatures**

Type constructor $\mathbf{\ast} \mathbf{\ast}$ of kind $(\ast \to \ast) \to \ast \to (\ast \to \ast)$:

```haskell
data (f :\mathbf{\ast} : a) e = f e :\mathbf{\ast} : a
```

Example

```haskell
data Sig' e = Val Int SrcPos
            | Add e e SrcPos

Sig' ≅ Sig :\mathbf{\ast} : SrcPos
```

**Dealing with Annotations**

Strip away annotations

```haskell
stripP :: (s :\mathbf{\ast} : p) a \to s a
stripP (v :\mathbf{\ast} : _) = v
stripPTerm :: (Functor s)
            \to Term (s :\mathbf{\ast} : p) \to Term s
stripPTerm = algHom (Term . stripP)
```

Ignoring annotations

```haskell
liftPTerm :: (Functor s)
          \to (Term s \to t) \to (Term (s :\mathbf{\ast} : p) \to t)
liftPTerm f = f . stripPTerm
```

This can be extended to annotations on signature built with sums.

**Limitations**

Propagation of annotations

- How can we lift a function $\text{Term } f \to \text{Term } g$
- to a function $\text{Term } (f :\mathbf{\ast} : p) \to \text{Term } (g :\mathbf{\ast} : p)$?
- Even if function is given as algebra $a :: f \ (\text{Term } g) \to \text{Term } g$
  this does not work:
  ```haskell
  a . fmap stripP
  ```
  is of type $f \ (\text{Term } (g :\mathbf{\ast} : p)) \to \text{Term } g$
- We could derive an algebra from that, but then result has uniformly
  the same annotation.

Composition of algebras

- Given two algebras $a :: f \ (\text{Term } g) \to \text{Term } g$ and $b :: g \ B \to B$,
  how do we compose them to an algebra $f \ B \to B$?
- Straightforward composition $\text{homAlg } b . a$ is of type
  ```haskell
  f \ (\text{Term } g) \to A
  ```
An Example

Example (Syntactic Sugar)

type Exp = Core :+: Sugar

desugarAlg :: Exp (Term Core) -> Term Core
desugar :: Term Exp -> Term Core
desugar = algHom desugarAlg

Specialising Algebras

Problem
desugarAlg :: Exp (Term Core) -> Term Core
- Algebras are too general!
- We have to employ the fact that the domain consists of terms!
- We need something more polymorphic!

First attempt: Signature Transformation
desugarAlg :: Exp a -> Core a
- This is often too restrictive!
- Each “layer” of a term over Exp has to be transformed into exactly one “layer” of a term over Core.
  \[ \begin{align*}
  &x>y \leadsto y<x \\
  &x-y \leadsto x+(-y)
  \end{align*} \]

Contexts and Term Homomorphisms

Generalise terms to contexts
data Context f a = Term (f (Term f))
| Hole a

From signature transformations to term homomorphisms
d E Context Core a

Term homomorphisms
- type TermHom f g = forall a . f a -> Context g a
- Term homomorphisms (a.k.a. tree homomorphisms) are the term algebras that are defined uniformly. Hence, the polymorphism!

Applying term homomorphisms
termHom :: (Functor f, Functor g)
  => TermHom f g -> Term f -> Term g
Propagating Annotations

**constP :: (Functor f) => p -> Context f a -> Context (f :*: p) a**

- `constP p (Hole a) = Hole a`
- `constP p (Term t) = Term (fmap (constP p) t :*: p)`

**liftPTermAlg :: (Functor g) => TermHom f g -> TermHom (f :*: p) (g :*: p)**

- `liftPTermAlg f (v :*: p) = constP p (f v)`

Composing term homomorphisms (and algebras)

**compTermHom :: (Functor g, Functor h) => TermHom g h -> TermHom f g -> TermHom f h**

**compAlg :: (Functor g) => (g a -> a) -> TermHom f g -> (f a -> a)**

Terms as Contexts without Holes

**Contexts with GADTs**

```haskell
data Cxt :: * -> (* -> *) -> * -> * where
  Term :: f (Cxt h f a) -> Cxt h f a
  Hole :: a -> Cxt Hole f a

type Context = Cxt Hole

type Term f = Cxt NoHole f Nothing

data Hole

data NoHole

data Nothing```

~ Generalise initial algebra semantics to free algebra semantics.

~ Terms & initial algebras are a special case.

Other Extensions

- **monadic algebras**
  - using generalised sequence :: `[m a] -> m [a]`
- **(monadic) coalgebras**
  - generating terms ~ e.g. for QuickCheck
- **generic functions**
  - e.g. size, querying, unification, matching ...
  - using generalised foldl :: `(a -> b -> a) -> a -> [a] -> b`
- **generic term rewriting**
  - e.g. for performing program transformations
- **mutually recursive data types [Yakushev et al. 2009]**
  - by adding additional type argument to the signatures
  - can be extended to rational sets of trees (by bottom-up tree automata on the type level)
Performance Impact

- Composable data types simplify function definitions, provide flexibility, reduce boilerplate code and avoid code duplication!
- But how does it affect runtime performance?

The setting

- Three signatures:
  - values: integers, Booleans, pairs
  - core language operations: +, -, if, =, <, ∧, ¬, projections
  - syntactic sugar: negation, >, ∨, ⇒
- a number of different typical functions:
  - type inference
  - evaluation to normal form,
  - “desugaring” (reduce syntactic sugar to the core language)
  - computing free variables
- We compare this to an ordinary implementation using standard data types and recursive functions.

Runtime Comparison

slowdown factors compared to standard data types

<table>
<thead>
<tr>
<th>function</th>
<th>n=16</th>
<th>n=63</th>
<th>n=1290</th>
<th>n=111,279</th>
</tr>
</thead>
<tbody>
<tr>
<td>desugar Type</td>
<td>4.8</td>
<td>5.2</td>
<td>5.3</td>
<td>4.1</td>
</tr>
<tr>
<td>desugar Type'</td>
<td>4.2</td>
<td>4.9</td>
<td>5.0</td>
<td>2.5</td>
</tr>
<tr>
<td>typeSugar</td>
<td>3.2</td>
<td>3.7</td>
<td>3.7</td>
<td>4.6</td>
</tr>
<tr>
<td>desugarEval</td>
<td>15</td>
<td>11</td>
<td>11</td>
<td>15</td>
</tr>
<tr>
<td>desugarEval'</td>
<td>13</td>
<td>10</td>
<td>9.8</td>
<td>8.8</td>
</tr>
<tr>
<td>evalSugar</td>
<td>12</td>
<td>9.4</td>
<td>7.4</td>
<td>18</td>
</tr>
<tr>
<td>desugarEvalPure</td>
<td>11</td>
<td>7.1</td>
<td>6.4</td>
<td>11</td>
</tr>
<tr>
<td>desugarEvalPure'</td>
<td>6.5</td>
<td>4.4</td>
<td>4.0</td>
<td>3.8</td>
</tr>
<tr>
<td>evalSugarPure</td>
<td>7.3</td>
<td>7.0</td>
<td>4.0</td>
<td>3.6</td>
</tr>
<tr>
<td>freeVars</td>
<td>1.3</td>
<td>1.6</td>
<td>1.4</td>
<td>1.6</td>
</tr>
<tr>
<td>desugar</td>
<td>0.3</td>
<td>0.08</td>
<td>1.2 · 10⁻³</td>
<td>1.5 · 10⁻⁵</td>
</tr>
</tbody>
</table>

- monadic functions are in blue
- underlined variants use composition of algebras

Outline

1 Compositional Data Types
2 A Toolbox for Prototyping Programming Languages
3 Conclusions
Applications for Compositional Data Types

**Drawbacks**
- not as straightforward as ordinary data types
- type errors are sometimes hard to decipher
- memory and runtime overhead

**Benefits**
- minimises code duplication
- functions on shared structures can be shared as well
- it is often more convenient to define functions
- more flexible (algebras can be easily modified / lifted)
- only little runtime overhead
- sometimes asymptotically faster than ordinary recursive functions on recursive data types

References

Wouter Swierstra.
Data types à la carte.

Generic programming with fixed points for mutually recursive datatypes.
Why Parallel Programming is Hard?

- C programmers love arrays and *for*-loops
- C++ programmers love vectors and iterators
- ML programmers love lists and *foldl*
- Haskell programmers love lists and *foldr*

All are inherently sequential!!

Parallel programming requires another data structure/recursion structure

Structure for Parallel Programming

\[
\begin{align*}
\text{sum } [a] &= a \\
\text{sum } (a:x) &= a + \text{sum } x \\
\text{sum } (a) &= a \\
\text{sum } (x ++ y) &= \text{sum } x + \text{sum } y \\
\text{sum } (\text{Tip } a) &= a \\
\text{sum } (\text{Fork } x y) &= \text{sum } x + \text{sum } y
\end{align*}
\]

Bad (Sequential)  
Best!! (Optimally Parallel)  
Good (Parallel)
Balanced Trees for Parallel Program

Parallel programmers love balanced trees!!

A methodology for balanced tree is required
- How can we relate parallel algorithms and balanced trees?
- How can we develop programs on balanced trees?

Overview

Programming

Parallel computation

Develop

Algorithms

Derive

Balanced Tree Structure

Underlying vehicle:
Parametricity (Free Theorem)

Step 1:
Extract Merging Operations

\[
\begin{align*}
\text{sum} \ [a] &= a \\
\text{sum} \ (x + y) &= \text{sum} \ x + \text{sum} \ y
\end{align*}
\]

merge results of independent sublists

⇒ It raises a polymorphic function

\[
h :: \forall \beta. (A \to \beta) \to (\beta \to \beta \to \beta) \to [A] \to \beta
\]

Q. Does \( h (\lambda a. \ a\ (+)) = \text{sum} \) hold for any \( h \) having this type?
Step 2:
Specify Requirements

h :: ∀β. (A → β) → (β → β → β) → [A] → β

The type does not guarantee h (λa.a) (+) = sum
(cf. h f (⊕) (a:x) = f a ⊕ f a ⊕ h f (⊕) x)

Requirement: Don’t discard, duplicate, shuffle.
⇒ h (λa. [a]) (++) x = x

Thm. For such h, h (λa. a) (+) = sum
Proof. From parametricity

Step 3:
Construct Balanced Trees

Given x :: [A], regard t = h Tip Fork x as a “balanced tree representation” of x

\[
\begin{aligned}
data \text{BTree} a &= \text{Tip} a \mid \text{Fork} (\text{BTree} a) (\text{BTree} a) \\
\end{aligned}
\]

• There are many such t:

h Tip Fork [1,2,3] ~ \begin{aligned}
& 1 \\
& \ \ \ \ \text{or} \\
& 2 \\
& \ \ \ \ \text{3} \\
\end{aligned}

⇒ We can choose a balanced one

Summary:
Development of Balanced Tree

• sum raises a family of polymorphic functions
  h :: ∀β. (A → β) → (β → β → β) → [A] → β
  \& h (λa. [a]) (++) x = x

• h Tip Fork yields a balanced tree based on the flexibility of choosing h
  – Indeed, it is the binary search tree

• Programs on the balanced trees should be efficient parallel programs
Programming on Balanced Trees

We would like to perform \( f :: [A] \rightarrow B \)

Work out \( f' \) such that

\[ f' (h \text{ Tip Fork } x) = f x = f (\text{toList } (h \text{ Tip Fork } x)) \]

by fusion (deforestation)

\[
\begin{align*}
\text{toList } (\text{Tip } a) & = [a] \\
\text{toList } (\text{Fork } x \ y) & = \text{toList } x \ ++ \ \text{toList } y
\end{align*}
\]

No parallel programming issues are there

Example: \( \text{scan} \)

\[
\begin{align*}
\text{scan } (\oplus) \ e \ [a] & = [e] \\
\text{scan } (\oplus) \ e \ (a \ x) & = e : \text{scan } (\oplus) \ (e \oplus a) \ x
\end{align*}
\]

Let's derive \( \text{scan'} (\oplus) \ e \ x = \text{scan } (\oplus) \ e \ (\text{toList } x) \)

\[
\begin{align*}
\text{scan'} (\oplus) \ e \ (\text{Tip } a) & = \text{scan } (\oplus) \ e \ (\text{toList } (\text{Tip } a)) \\
& = [e] \\
\text{scan'} (\oplus) \ e \ (\text{Fork } x \ y) & = ... \\
& = \text{scan'} (\oplus) \ e \ x \ ++ \ \text{scan'} (\oplus) \ (e \oplus \text{reduce'} (\oplus) \ x) \ y
\end{align*}
\]

scan on Balanced Trees

\[
\begin{align*}
\text{reduce'} (+) \ (\text{Tip } a) & = a \\
\text{reduce'} (+) \ (\text{Fork } x \ y) & = \text{reduce'} (+) \ x \ + \ \text{reduce'} (+) \ y
\end{align*}
\]
scan on Balanced Trees (Contd.)

\[
\text{scan'} (+) e \text{ (Tip a)} = [e] \\
\text{scan'} (+) e \text{ (Fork } x \text{ } y) \\
\quad = \text{scan'} (+) e \times ++ \text{scan'} (+) (e + \text{reduce'} (+) e x) y
\]

Summary

Programming \quad Algorithms

- \text{sum} \quad \text{Derive} \\
- \text{scan} \quad \text{Develop} \\
- \text{Balanced Tree Structure}

Our method scales from lists to trees

Shunt Contraction Algorithm
(Abrahamson et al.'89)

- Collapse a tree by primitive contraction operations called “Shunt”
  - time \( O(n/p + \log p) \)

- The process of collapse provides a good scheduling of gathering information
  - expression evaluation, register allocation, XPath querying …
Deriving Balanced Tree

Consider

\[ h :: \forall \beta. (A \rightarrow \beta) \rightarrow (\beta \rightarrow \beta \rightarrow \beta \rightarrow \beta, \beta \rightarrow \beta \rightarrow \beta \rightarrow \beta, \beta \rightarrow \beta \rightarrow \beta \rightarrow \beta) \rightarrow \text{Tree } A \rightarrow \beta \text{ s.t. } h \text{ wrap connect } x = x \]

(connect reconstructs the tree according to Shunt)

\[ h \text{ Leaf (NN, NL, NR) } t \]

\(~\text{ ordered topology tree (Frederickson'97) }\)

\(- \text{ height } O(\log n), \text{ connect/cut: } O(\log n) \text{ time}\)

Purely Functional Implementations of Tree Accumulations (Gibbons et al.'94)

- Known implementations (Gibbons et al.'94) Shunt contraction + stacks of pointers
- Our implementations:
  Balanced tree + upsweep + downsweep (as similar to scan)

Conclusion & Future Work

High-level language

Parallel programming combinators

(scan, uAcc, dAcc,...)

Data structure

(Balanced Trees)

Parallel algorithm

Parallelization
A Homomorphism-based MapReduce Framework for Systematic Parallel Programming

Yu Liu
The Graduate University for Advanced Studies
Jan 12, 2011

Outline

- Motivations
- Brief introduction of MapReduce
- The Homomorphism-based Framework
- Case Study: Parallel sum, Maximum prefix sum, Variance of numbers
- Experimental Results

Motivation of This Talk

- Show how to make programming with MapReduce easier.
Motivation of This Talk

- Show how to make programming with MapReduce easier.
- Introduce an approach of automatic parallel program generating.

MapReduce Programming model

The Computation of MapReduce Framework

Google’s MapReduce is a parallel-distributed programming model, together with an associated implementation, for processing very large data sets in a massively parallel manner.

Components of a MapReduce program (Hadoop)

- A Mapper;
- A Partitioner that can be used shuffling data;
- A Combiner that can be used doing local reduction;
- A Reducer;
- A Comparator can be used while sorting or grouping;

MapReduce Programming model

MapReduce Data-processing flow
Outline

Motivation
Brief introduction of background
The Design of Homomorphism-based Framework on MapReduce
Case Study
Performance Evaluation

Programming Paradigm of MapReduce
List Homomorphism and Homomorphism Theorems

MapReduce Programming model

A simple functional specification of the MapReduce framework

MapReduce :: ([k1, v1] → [(k2, v2)]) → ([(k3, v3)] → [(k4, v4)]) → ([(k5, v5)])
MapReduce mapper reducer set kv = let set kv = map map mapper set kv
set [k, list v = groupByKey set list v
  in map (λ(k, kv), (h, reduce (h, kv))) set [k, list v

Function map is a set version of the map function. Function

groupByKey :: {[(k, v)]} → {(k, [v])} takes a set of list of
key-value pairs (each pair is called a record) and groups the values
of the same key into a list.

Yu Liu
A Homomorphism-based MapReduce Framework for Systematic

Maximum Prefix Sum problem

The Maximum Prefix Sum problem (mps) is to find the maximum
prefix-summation in a list:

3, -1, 4, 1, -5, 9, 2, -6, 5

This problem seems not obvious to solve this problem efficiently
with MapReduce.

Yu Liu
A Homomorphism-based MapReduce Framework for Systematic

List Homomorphism

Function h is said to be a list homomorphism

If there are a function f and an associated operator ⊕ such that
for any list x and list y

\[
\begin{align*}
  h \ [a] &= f \ a \\
  h \ (x \ ++ \ y) &= h(x) \odot h(y).
\end{align*}
\]

Where ++ is the list concatenation.

For instance, the function sum can be described as a list
homomorphism

\[
\begin{align*}
  \text{sum} \ [a] &= a \\
  \text{sum} \ (x \ ++ \ y) &= \text{sum} \ x + \text{sum} \ y.
\end{align*}
\]
List Homomorphism and Homomorphism Theorems

Leftwards function
Function $h$ is leftwards if it is defined in the following form with function $f$ and operator $\oplus$,

\[
\begin{align*}
  h[a] &= f a \\
  h([a] ++ x) &= a \oplus h x.
\end{align*}
\]

Rightwards function
Function $h$ is rightwards if it is defined in the following form with function $f$ and operator $\otimes$,

\[
\begin{align*}
  h[a] &= f a \\
  h(x ++ [a]) &= h x \otimes a.
\end{align*}
\]

Map and Reduce
For a given function $f$, the function of the form $([\cdot] \circ f, ++)$ is a map function, and is written as $\text{map } f$.

The function of the form $([\text{id}, \circ])$ for some $\circ$ is a reduce function, and is written as $\text{reduce } (\circ)$.

The First Homomorphism Theorem
Any homomorphism can be written as the composition of a map and a reduce:

\[
([f, \circ]) = \text{reduce } (\circ) \circ \text{map } f.
\]

The Third Homomorphism Theorem
Function $h$ can be described as a list homomorphism, iff $\exists \circ$ and $\exists f$ such that:

\[
\begin{align*}
  h &= ([f, \circ]) \\
  h[a] &= f a \\
  h([a] ++ x) &= a \oplus h x \\
  h(x ++ [b]) &= h x \otimes b.
\end{align*}
\]

The third homomorphism gives a necessary and sufficient condition for the existence of a list homomorphism.
To make it easy for resolving problems such as mps by MapReduce. We using the knowledge of homomorphism especially the third homomorphism theorem to wrapping MapReduce model.

```
Basic Homomorphism-Programming Interface

filter :: a → b
aggregator :: b → b → b.
```

A simple example of using this interface for computing the sum of a list

```
public class SUM implements BasicListHomomorphismInterface<LongWritable, LongWritable> {
    private static final Log LOG = LogFactory.getLog(SUM.class);
    public static LongWritable sum(List<LongWritable> x) {
        Long result = 0;
        for (LongWritable var : x) {
            result += var.get();
        }
        return new LongWritable(result);
    }
    public LongWritable filter(List<LongWritable> x) {
        return x;
    }
    public LongWritable aggregator(List<LongWritable> x) {
        return x;
    }
}
```
A homomorphism-based framework wrapping MapReduce

Programming Interface with Right Inverse

\[ \text{fold} :: [a] \rightarrow b \]
\[ \text{unfold} :: b \rightarrow [a]. \]

The implementation on Hadoop

```
public interface ThirdHomomorphismInterface<T1 extends Object,T2 extends Object> { 
  String folding_method = "fold";
  String unfolding_method = "unfold";
  public T2 fold( ArrayList<T1> values);
  public ArrayList<T1> unfold(T2 value);
}
```

A simple example of using this interface for computing the sum of a list

```
public class SUM2 implements ThirdHomomorphismInterface<LongWritable, LongWritable> {

  public LongWritable fold(ArrayList<LongWritable> values) {
    return sum(values);
  }

  public ArrayList<LongWritable> unfold(T1 value) {
    return new ArrayList<LongWritable>(){
      add(value);
    };
  }

  public static LongWritable sum(ArrayList<LongWritable> values) {
    Long rst = 0;
    for (LongWritable var : values) {
      rst = var.get();
    }
    return new LongWritable(rst);
  }
}
```

Requirements of using this interface in addition to the right-inverse property of `unfold` over `fold`.

Both leftwards and rightwards functions exist

\[ \text{fold}([a] ++ x) = \text{fold}([a] ++ \text{unfold}(\text{fold}(x))) \]
\[ \text{fold}(x ++ [a]) = \text{fold}(\text{unfold}(\text{fold}(x)) ++ [a]). \]
The implementation of homomorphism framework upon Hadoop

To implement our programming interface with Hadoop, we need to consider how to represent lists in a distributed manner.

### Set of pairs as list

We use integer as the index’s type, the list \([a, b, c, d, e]\) is represented by \(\{(3, d), (1, b), (2, c), (0, a), (4, e)\}\).

### Set of pairs as distributed List

We can represent the above list as two sub-sets \(\{((0, 1), b), ((0, 2), c), ((0, 0), a)\}\) and \(\{((1, 3), d), ((1, 4), e)\}\), each in different data-nodes.

---

**Defination of** \(\text{hom}_{\text{MR}}\)

\[
\text{hom}_{\text{MR}} : (\alpha \rightarrow \beta) \rightarrow (\beta \rightarrow \beta) \rightarrow \{(\text{ID}, \alpha)\} \rightarrow \beta
\]

\[
\text{hom}_{\text{MR}} f (\oplus) = \text{getValue} \circ \text{MapReduce mapper2 reducer2} \circ \text{MapReduce mapper1 reducer1}
\]

where

\[
\text{mapper1} : (\text{ID}, \alpha) \rightarrow [[[\text{ID}, \text{ID}], \beta]]
\]

\[
\text{mapper1} (i, a) = [[[\text{pid}, i], b]]
\]

\[
\text{reducer1} : (\text{ID}, \text{ID}) \rightarrow [\beta] \rightarrow \beta
\]

\[
\text{reducer1} ((p, j), \text{ias}) = \text{hom} f (\oplus) \text{ias}
\]

\[
\text{mapper2} : (\text{ID}, \text{ID}), \beta \rightarrow [[[\text{ID}, \text{ID}], \beta]]
\]

\[
\text{mapper2} ((p, j), b) = [[[0, j], b]]
\]

\[
\text{reducer2} : (\text{ID}, \text{ID}) \rightarrow [\beta] \rightarrow \beta
\]

\[
\text{reducer2} ((0, k), \text{jbs}) = \text{hom} (\oplus) \text{jbs}
\]

\[
\text{getValue} \{((0, b))\} = b
\]

Where, \(\text{hom} f (\oplus)\) denotes a sequential version of \([f, \oplus]\).
The **leftwards** and **rightwards** function

### Derivation by right inverse

\[
\leftarrow\text{leftwards}([a] + x) = \text{fold}([a] + \text{unfold} (\text{fold}(x)))
\]

\[
\rightarrow\text{rightwards}(x + [a]) = \text{fold} (\text{unfold} (\text{fold} x) + [a]).
\]

Now if for all \(xs\),

\[
\rightarrow\text{rightwards} \ x s = \leftarrow\text{leftwards} \ x s,
\]

then a list homomorphism \([f, \oplus]\) that computes \(\text{fold}\) can be obtained automatically, where \(f\) and \(\oplus\) are defined as follows:

\[
f \ a = \text{fold}([a])
\]

\[
a \oplus b = \text{fold} (\text{unfold} a + + \text{unfold} b).
\]

Equation (1) should be satisfied.

### Programming with this homomorphism framework

MPS

A sequential program

```java
public static LongWritable mps(ArrayList<LongWritable> xs) {
    Long rst = 0;
    Long tmp = 0;
    for (LongWritable v : xs) {
        tmp += v.get();
        if (tmp > rst) {
            rst = tmp;
        }
    }
    return new LongWritable(rst);
}
```
Programming with this homomorphism framework

MPS

A tupled function

```java
public static Pair<Long> mps_sum(ArrayList<LongWritable> xs) {
    Long mps = 0;
    Long sum = 0;
    for (LongWritable v : xs) {
        sum += v.get();
        if (sum > mps) {
            mps = sum;
        }
    }
    return new Pair<Long>(mps, sum);
}
```

We use this tupled function as the fold function. The right inverse of the tupled function, \((\text{mps} \triangle \text{sum})^\circ\):

\[
(\text{mps} \triangle \text{sum})^\circ (m, s) = [m, s - m]
\]

Noting that for the any result \((m, s)\) of the tupled function the inequality \(m \geq s\) hold.

The implementation of homomorphism framework upon Hadoop performance tests

Environment: Hardware

COE cluster in Tokyo University which has 192 computing nodes. We choose 16, 8, 4, 2 and 1 node to run the MapReduce-MPS program. Each node has 2 Xeon(Nocona) CPU with 2GB RAM.

Environment: Software

- Linux2.6.26, Hadoop0.20.2 + HDFS
- Hadoop configuration: heap size= 1024MB
- maximum mapper pre node: 2
- maximum reducer pre node: 2
### Performance

#### The input data

<table>
<thead>
<tr>
<th>length of list</th>
<th>value type</th>
<th>file size</th>
<th>compressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 million</td>
<td>Long</td>
<td>29.5MB</td>
<td>zip</td>
</tr>
<tr>
<td>10 million</td>
<td>Long</td>
<td>295.5MB</td>
<td>zip</td>
</tr>
<tr>
<td>100 million</td>
<td>Long</td>
<td>2.95GB</td>
<td>zip</td>
</tr>
</tbody>
</table>

#### The time consuming of calculate 100 million-long list

(SequenceFile, Pair $<$ Long $>$):

#### The speedup of 2-16 nodes:
The time curve indicate the system scalability with the number of computing nodes. The curve between x-axis 2 and 8 has biggest slope, when the curve reaches to 16, the slope decreased, that is because when there are more nodes, the overhead of communication increased. Totally, the curve shows the scalability is near-linear.

Overhead of 2 phases Map-Reduce.
Overhead of Java reflection.
Not support local reduction now (not implemented yet).
Background

Enterprise Resource Planning (ERP) systems is a category of systems designed to aid the management of resources in a company. The ERP category include systems like Microsoft Dynamics NAV / AX, SAP.

Major ERP systems are centered around the Double-Entry Bookkeeping financial model, and are strongly tied to the database representation of data.

In 2004, 91% of the top 500 danish companies employed an ERP system. 40% were using an MS product, 23% a SAP product.

Modeling ERP requirements

The extraction and formulation of requirements for an ERP system is a very subjective discipline that often rely on the individual experts with extensive contextual knowledge of the industry (Rikhardsson et al., 2004; de Carvalho et al., 2009).

Deploying an ERP system is a huge task that scales with the size of the company deploying it. E.g. it is estimated that the cost of implementing an ERP system represents 1-6% of a company’s turnover and that it takes an average of two to three years to complete.
The REA accounting model and the POETS ERP framework

McCarthy proposed the REA accounting model in 1982:

“An Event is some Agent(s) acting on some Resource(s)”.

The Process Oriented Event-driven Transaction System (POETS) (Henglein et al., 2009) is an implementation of this model.

“Shortening the distance between requirements and their formal expression for rapid system prototyping, implementation, and continuous adaptation to changing processes and information needs”

\[ \text{POETS(Data Model, Work Flows)} \Rightarrow \text{ERP System} \]

Architectural overview of POETS

Formulation of a transaction process

Originates from a live case study.

- Create and Negotiate sales quote, including payment terms (Fixed price or hourly rate).
- Enter sales contract (binding).
- Select DJ.
- DJ plays the job.
- DJ must receive a payment for the job. Either directly from the customer or from the company
- Customer is invoiced the amount according to the payment terms.
- Company receives and registers the incoming payment.
Modeling the Sales Process

What information is needed to model this?
- 3 Agents (Company, Customer, DJ).
- Information about the job, including date, size, type, place, etc.
- Payment details

What is needed to formalize this ontological data model?
- Entities (Records).
- Fields of Entities or simple types.
- Inheritance between entities.

Compact, easily readable syntax for formalization.

Formalizing an ontology language

\[
S ::= \text{EntityName}, \text{SupQuan EntityName}, .
\]

\[
| \text{EntityName}, \text{PropQuan EntityName}, \text{PropDecl} .
\]

\[
| \text{EntityName has comments} \text{ Cstring} .
\]

\[
| \text{EntityName is abstract} .
\]

\[
| \text{EntityName RuleExp} .
\]

\[
\text{EntityName} ::= [A-Z] [(A-Za-z)(1-9)]*
\]

\[
\text{SupQuan} ::= \text{is a} | \text{is an} | \text{is in}
\]

\[
\text{PropQuan} ::= \text{SingleQuantity} | \text{MultipleQuantity}
\]

\[
\text{PropDecl} ::= \text{called FieldName} | \text{named FieldName} | \epsilon
\]

\[
\text{FieldName} ::= [a-z] [A-Za-z-z]^{*}
\]

\[
\text{Cstring} ::= "([A-Za-z](\n{6}:::?)")^{*}
\]

\[
\text{RuleExp} ::= \text{validates ruleset} F | \text{is validated by} F
\]

\[
\text{SingleQuantity} ::= \text{has a} | \text{has an}
\]

\[
\text{MultipleQuantity} ::= \text{has a list of}
\]

Data Model for Contract

\text{DJContract is a} \text{ Contract} .
\text{DJContract has a} \text{ Company} .
\text{DJContract has a DJ} \text{ called} dj .
\text{DJContract has a} \text{ Customer} .
\text{DJContract has a} \text{ FixedPrice} \text{ called} djSalary .
\text{DJContract has a} \text{ list of GearPackage} \text{ called} gear .
\text{DJContract has an} \text{ EventType} .
\text{DJContract has an} \text{ int} \text{ called} size .
\text{DJContract has a} \text{ dateTime} \text{ called} start .
\text{DJContract has a} \text{ dateTime} \text{ called} tentativeEnd .
\text{DJContract has an} \text{ Address} \text{ called} eventAddress .
**Formalizing the work flow**

- Using multiparty contracts (Hvitved, 2009)
- Identify “Functions” and “Events” in the work flow.
- Identify deadlines and other temporal parameters.

**Conclusion**

Extracting / uncovering even the most basic requirements for ERP systems is not a trivial task.

Specialization of the POETS framework with regards to the requirements. This includes User Interfaces.

Specify a knowledge representation language for an ERP data model that is:
- Easily readable.
- Limited to the domain for which it is used.
- Strong enough to express a data model for an ERP system.

**Future work**

Deployment of a POETS implementation in a live setting will hopefully reveal whether the customizations are indeed easier to perform.


Marker-directed optimization of UnCAL graph algebra revisited: Optimizing bidirectional graph transformations

Soichiro Hidaka
National Institute of Informatics, Japan

The Fourth DIKU-IST Joint Workshop on Foundations of Software
12 Jan. 2011

Bidirectional Transformation

Graph BT Example

- Replace ‘a’ by ‘d’ and contacts ‘c’
Background

- Performance is one of the big issues
  - We are highly motivated for optimization
- Preliminary framework for today’s presentation had been mostly implemented

A Compositional Framework for Bidirectional Model Transformation

UnCAL Structural Recursion in General Form

\[ f \{\} = \{\} \]

\[ f \{l:G\} = t(l,G)@ f G \]

\[ f(G_1 \cup G_2) = f(G_1) \cup (f \ G_2) \]

\[ f = \text{rec}(\lambda(l,g).t(l,g)) \]
Example: a2d_xc

- Replace ‘a’ by ‘d’ and contracts ‘c’

\[
a2d_xc(db) = \text{rec}(\lambda (l,g). \text{if } l=a \text{ then } \{d:&\} \\
\text{else if } l=c \text{ then } \{e:&\} \\
\text{else } \{l:&\})(db)
\]

Core UnCAL Language

\[
e ::= \{\} | \{ L : e \} | e \cup e | \& x := e | \& y | () \\
| e @ e | \text{cycle}(e) \quad \{ \text{constructor} \} \\
| $\text{g} \quad \{ \text{graph variable} \} \\
| \text{if } l = l \text{ then } e \text{ else } e \quad \{ \text{conditional} \} \\
| \text{rec}(\lambda (l,$g).e)(e) \quad \{ \text{structural recursion application} \}
\]

\[
l ::= a \quad \{ \text{edge label} \} \\
| $l \quad \{ \text{label variable} \}
\]

Optimization by forward transformation itself

- Non-necessary recursion can be eliminated
- We go back to bidirectional aspect in the conclusion

\[
f \{ L : G \} = t(L,G)@ f G
\]
Structural recursion and markers

\[
\text{map } f \ (x:xs) = (f \ x) : \text{map } f \ xs
\]

\[
\text{rec } e \ (x:xs) = e(x, xs) \circ \text{rec } e \ xs
\]

Graph Constructors

Graph Constructors
Revisiting marker analysis

- Mainly run-time analysis is mentioned
  - Avoid evaluating unnecessary subexpressions
- We can now statically compute and further simplify the transformation itself

Revisiting original marker analysis

Computation of markers
Static estimation of markers for structural recursion

- Computation of structural recursion itself requires static computation of markers

Fusion rules and output marker analysis

- Removal of intermediate results in successive application of $e_1$ structural recursion.

\[
\begin{align*}
rec(e_2) \circ rec(e_1) &= rec(rec(e_2) \circ e_1) \\
&\text{if } e_2(l,t) \text{ does not depend on } t \\
rec(e_2) \circ rec(e_1) &= rec(\lambda(l,t).rec(e_2)(e_1(l,t) \oplus rec(e_1)(t))) \\
&\text{for arbitrary } e_2(l,t)
\end{align*}
\]

- If you know statically guarantee that $e_4$ does not produce any output marker, then the second rule falls back to first rule, opening another optimization opportunities.

Non-recursive query

- Join translated to nested recursion
  - Finite step traversal only
  - Body of rec does not have recursion which means the body does not have output marker
Join

• Want to return subgraphs under \( b \) with sibling \( c \)

\[
\text{sfun f}((sl, sl)) =
\text{sfun f}(c(c, slc)) =
\text{sfun f}(f(b, slb)) = slb
\]

in \( fc(sl) \)
in \( f(sb) \)

uses of common variables
implements join

introduction of id function

Other rules for rec

\[
\begin{align*}
\text{rec}(e)() &= \{} \\
\text{rec}(e)(\{l : d\}) &= e(l, d) \circ \text{rec}(e) \\
\text{rec}(e)(d_1 \cup d_2) &= \text{rec}(e)(d_1) \cup \text{rec}(e)(d_2) \\
\text{rec}(e)(\&x := d) &= \&x * \text{rec}(d) \\
Z &= \{\&z_1, ... , \&z_p \mid e \in DB_Z^x\} \\
\text{rec}(e)(\&y) &= (\&y_{1} := \&y \&z_{1}, ... \&z_{p} := \&y \&z_{p}) \\
\text{rec}(e)() &= () \\
\text{rec}(e)(d_1 \oplus d_2) &= \text{rec}(e)(d_1) \oplus \text{rec}(e)(d_2) \\
t \text{ does not occur free in } e \\
\text{rec}(\lambda(l,e))() &= \text{rec}(e)(d_1) @ \text{rec}(e)(d_2) \\
t \text{ does not occur free in } e \\
\text{rec}(\lambda(l,e))(\text{cycle}(d)) &= \text{cycle}(\text{rec}(e)(d))
\end{align*}
\]

Static marker analysis

• How about "residual" markers?

\[
d_1 \in DB_Z^X \quad d_2 \in DB_Z^Y \\
d_1 \circ d_2 \in DB_Z^X
\]
Bisimulation equivalence

- Unreachable parts may be disregarded

Residual marker

- Idiom for projection

\[
e_1 :: DB^\chi \quad e_1 ::: DB^\chi \quad e_1 \cdot e_2 \downarrow e_1
\]

Example fusion

```
select
letrec sf f2 ((name:T)) = {name:g2(T)}
| f2 (L:T) = f2(T)
and sf g2 (L:T) = {L:g2(T)}
in
letrec sf f1 ((primitiveDataType:T))
  = {primitiveDataType:g1(T)}
| f1 (L:T) = {L:f1(T)}
and sf g1 (name:T) = {typeName:g1(T)}
| g1 (L:T) = {L:g1(T)}
in f2(f1(db))
```
After desugaring

- composition of rec

```haskell
~zi@rec\ (L,T).
  if L = "name"
    then (zi1 := ("name": ~z2),
      ~z2 := ("name": ~z3))
  else (zi1 := {L: ~z2}, ~z2 := {L: ~z3})

~zi@rec\ (L,T).
  if L = "name"
    then (zi1 := ("name": ~zi1),
      ~z2 := ("typeName": ~z2))
  else if L = "primitiveDataType"
    then (zi1 := ("primitiveDataType": ~z2),
      ~z2 := ("primitiveDataType": ~z3))
  else (zi1 := {L: ~zi1}, ~z2 := {L: ~z2})
```

After fusion rule applied

- Fusion rule 1 applied
- Hand optimization required
- We could "plug" the expression in the output marker of the left hand side of @
Plugging expression to output marker expression

\[
\{ l : &y \} \oplus (&y := e) \downarrow \{ l : e \}
\]

- Further, we could eliminate the output marker expression if it will not be connected to other input nodes

Plugging rule for complex case: cycle

\[
e :: DB^X_y \quad y \notin (Y \setminus X)
\]
\[
cycle(e) \oplus (&x := e_1 \oplus &y := e_2) \downarrow \cycle(e[e_2 / &y]) \oplus (&x := e_1)
\]

Preliminary performance results

- Customer to Order composed by selection
  - Without rewriting
    - Fwd evaluation took 0.05 CPU seconds
    - Bwd evaluation took 2.58 CPU seconds
  - Rewrite only to 2nd rule for fusion
    - Fwd evaluation took 0.06 CPU seconds
    - Bwd evaluation took 2.67 CPU seconds
  - After adding rewriting to lead to 1st rule of fusion
    - Fwd evaluation took 0.04 CPU seconds
    - Bwd evaluation took 1.30 CPU seconds
Conclusion

• Static marker computation defined to exploit new optimization opportunity.
• Further optimization based on “plugging” expression reasoned about.
• Future Work
  – Canonical form
    • &x_1 := e_1, &x_2 := e_2, ..., &x_n = e_n
  – Other reasoning about what we can do statically
  – Analyze impact to reflectable updates
Graph Transformation

Graphs:
Natural direct representation of real world entities
WWW, GIS, images, videos, social networks,
Biological information, chemical information,
Models in software engineering and databases

Use of Graphs:
Transformations of one graph into another.

Native graph transformation languages

Application: Class2RDB
UnQL: Graph Querying

UnQL [VLDB Journal '00] is a well-defined graph query language

- Easy to use: select ... where ...
- Has a core graph algebra for arbitrary graph construction
- Use structural recursion for manipulating graphs
- Widely used in various applications [SAC'09][ICSE'09 NIER][ICFP'10]...

UnQL one or more graphs $\rightarrow$ one graph
SQL one or more relations $\rightarrow$ one relation
XQuery zero or more items $\rightarrow$ zero or more items

Goals

UnQL+: a graph transformation language
an extension of UnQL

* A uniform mechanism for both querying and updating.
  $\rightarrow$ all updates are transformed into structural recursion.

Edge-labelled Graphs

$g = \{a : \{a : g_1\}\} \cup \{b : \{a : g_1\}\} \cup \{c : g_2\}$
$g_1 = \{d : \{\}\\}$
$g_2 = \{c : g_2\}$
UnQL expressions are bisimulation generic.

\[ f \text{ is bisimulation generic if } g_1 \equiv g_1', \ g_2 \equiv g_2', \ldots \text{ implies } f(g_1, g_2, \ldots) \equiv f(g_1', g_2', \ldots) \]

Graph Representation: An Example

A Class Diagram:

- **Association**
  - name = "address"
  - src_of = src_of
  - dest = dest

- **Class**
  - name = "Person"
  - is_persistent = true
  - attrs
    - **Attribute**
      - name = "name"
      - is_primary = true
      - type = PrimitiveDataType
      - name = "String"

- **Association**
  - name = "phone"
  - src_of = src_of
  - dest = dest

- **Class**
  - name = "Address"
  - is_persistent = false
  - attrs
    - **Attribute**
      - name = "addr"
      - is_primary = true
      - type = PrimitiveDataType
      - name = "String"

- **Class**
  - name = "Phone"
  - is_persistent = true
  - attrs
    - **Attribute**
      - name = "number"
      - is_primary = true
      - type = PrimitiveDataType
      - name = "Integer"
Structural Recursion: Manipulating Graphs

Structural Recursion:
\[
\begin{align*}
  f(\{\}) & = \{} \\
  f(\{l : g\}) & = e(l,g) @ f(g) \\
  f(g_1 \cup g_2) & = f(g_1) \cup f(g_2)
\end{align*}
\]

Or written as:
\[
\text{sf} f(\{l : g\}) = e(l,g) @ f(g)
\]

Structural Recursion: An Example

\[
\begin{align*}
  \text{sf} \ a2d\_xc (\{l : g\}) & = \text{if } l = a \text{ then } \{d : a2d\_xc(g)\} \\
  & \quad \text{else if } l = c \text{ then } a2d\_xc(g) \\
  & \quad \text{else } \{l : a2d\_xc(g)\}
\end{align*}
\]

Structural Recursion in UnQL

- Can focus on one-dimensional graphs w.l.o.g. each node has at most one outgoing edge
  \[
  f(g_1 \cup g_2) = f(g_1) \cup f(g_2)
  \]

- No accumulation parameters can not formulate one flat mutual recursion → nested structural recursion cannot refer outer sr function in nested sr
How to extract all persistent classes?

Graph Querying in UnQL

```unql
select $class
where
{Association.(src|dest).Class: $class}
in $db,
{is_persistent.Boolean.true: _}
in $class
```

```
let sfun h1({A:$v}) = h2($v)
  | h1({f:$v}) = {}  

sfun h2({s:$v}) = h3($v)
  | h2({d:$v}) = h3($v)
  | h2({l:$v}) = {}  

sfun h3({C:$v}) = let sfun h5({i:$u}) = h6($u)
  | h5({f:$u}) = {}

sfun h6({B:$u}) = h7($u)
  | h6({l:$u}) = {}

sfun h7({t:$u}) = $v
  | h7({l:$u}) = {}
  
  in h5($v)
  | h3({l:$v}) = {}

in h1($db)
```
Language Design Policy

Two choices.

1. Updates are syntactically distinct from queries.
   + simple and clear semantics.
   + easier static analysis (e.g. typecheck).
   - less expressiveness.
   e.g. SQL, Flux

2. Update operations may appear within query exp.
   - complex semantics.
   - difficult static analysis.
   + more expressiveness.
   e.g. XQuery!, XQueryU

Graph deleting in UnQL+

How to delete all persistent classes?

```sql
delete Association.(src|dest).Class → $u
where {is_persistent.Boolean.true:_} in $u
in $db
```
How to prefix every name of the class by “class_”?

```
replace _*.Class.name.String → $u
by {("class_" + $name) : {}}
where {$name:_} in $u
in $db
```

How to add date information to each class?

```
extend _*.Class → $u
with {date: {"2011/1/12":{}}}
in $db
```

Syntax of UnQL\(^+\) for updating

```
extend r → var with e
where bs in e
replace r → tgt [under var] by e
where bs in e

tgt ::= var | {l:var} | {var:var} | {r:var}
```

```
delete r → tat [under var]
where bs in e
replace r → tgt [under var] by {}
where bs in e
```
Snapshot Semantics

Two logical phases of processing:
1. specifies nodes to be updated (snapshot)
2. updates are applied to the nodes

SQL, XQuery!, Flux, XQueryU, ...

Execution model for \textit{extend}-exp.
Execution model for \texttt{replace}-exp.

The first matching node from the root is replaced.

\[ f (\{b:g_1 \} \cup \{a:b:g_1\}) = f(\{b:g_1\}) \cup f(\{a:b:g_1\}) \]

Mapping to Structural Recursion

- Constructing a DFA for \( r \)
- Associating a sr function with each state

How to preserve the context (unchanged part)

\[
\text{sfun } h(\{l:g\}) = \{l: \ldots\}
\]

Mapping \texttt{extend}-exp. into SR

A DFA for \( r \): \((Q, \Sigma, \delta, q_0, F)\)

\[
Q = \{q_0, \ldots, q_N\} \quad \Sigma = \{l_0, \ldots, l_M, !\}
\]

\( h_i : \) associated with \( \delta(q_i, l) \)

\[
\delta : Q \times \Sigma \mapsto Q \quad \delta(q_i, l_k) \in F
\]

let \text{sfun } h_0(\{l_0:$v$\}) = ...  

\[
\ldots
\]

\[
\text{sfun } h_1(\{l_0:$v$\}) = \{l_0 : h_i^1($v$) \}
\]

\[
\ldots
\]

\[
\text{sfun } h_i(\{l_0:$v$\}) = \{l_i : h_i^i($v$) \cup \text{select } e_1 \text{ where } bs\}
\]

\[
\ldots
\]

\[
\text{sfun } ...
\]

... in \text{s1($db$)}
extend \_\_\_ (a \lor c) \rightarrow S_t\ with \ \{ee:\{}\}
where \ \{b:\$v\} \ in \ S_t
in \ S_{db}

let

sfun s1({a:$t}) = \{a: s2($t) \cup select \ \{ee:\{}\}\}

\land

s1({c:$t}) = \{c: s2($t) \cup select \ \{ee:\{}\}\}

\land

s1({$l:$t}) = \{$l: s1($t)\}
sfun s2({a:$t}) = \{a: s2($t) \cup select \ \{ee:\{}\}\}

\land

s2({c:$t}) = \{c: s2($t) \cup select \ \{ee:\{}\}\}

\land

s2({$l:$t}) = \{$l: s1($t)\}
in s1($db)

replace \_\_\_\_ (a \rightarrow $u) \ by \ \{ee:\{}\}
where \ \{sl1:$g1\} \ in \ $u,
\{sl2:$g2\} \ in \ $g1,
$sl1=$sl2
in \ $db

let sfun s1({a:$u}) = \{a: let sfun h1({sl1:$g1}) =
\land

let sfun h2({sl2:$g2}) = if $sl1=$sl2
then \ \{ee:\{}\}\nelse s2($u)
\land

in h2($g1)
in h1($u)}

\land
s1({$l:$u}) = \{$l: s1($u)\}
sfun s2({a:$u}) = ...

.....
in s1($db)

replace \_\_\_\_ (a \rightarrow $u) \ by \ \{ee:\{}\}
where \ \{sl1:$g1\} \ in \ $u,
\{sl2:$g2\} \ in \ $g1,
$sl1=$sl2
in \ $db

let sfun s1({a:$u}) =
\land

if isEmpty (select \ \{found:\{}\}\)
where \ \{sl1:$g1\} \ in \ $u, \ {sl2:$g2\} \ in \ $g1, \ $sl1=$sl2
then \ \{a:s2($u)\}\nelse \ \{a: select \ \{ee:\{}\}\\}

where \ \{sl1:$g1\} \ in \ $u, \ {sl2:$g2\} \ in \ $g1, \ $sl1=$sl2
\land
s1({$l:$u}) = \{$l: s1($u)\}
sfun s2({a:$u}) = ...

.....
in s1($db)
replace _* .a -> {d:$u} by {ee:{}}
where
{sl1:$g1} in $u,
{sl2:$g2} in $g1,
sl1=sl2
in $db

sfun s1({a:$v}) = let sfun h({d:$u}) =
  if isEmpty(select {"found"} where ...) then s2($v)
  else {a: select {ee:{}} where ...}
  | h({$l':$u}) = s2($v)
  in {a: h($v)}
  | s1({$l:$v'}) = {s1: s1($v')}
sfun s2({a:$v}) = let sfun h({d:$u}) = ...
  | s2({$l:$v'}) = {s2: s2($v')}

sfun s1({a:$v}) = {a: h($v)}
  | s1({$l:$v'}) = {s1: s1($v')}
sfun h({d:$u}) = if isEmpty(select {"found"} where ...) then d:s1($u)
  else {a: select {ee:{}} where ...}
  | h({$l':$u}) = {a: h($u')}
sfun h({$l:$u'}) = {s1: s1($u')}
sfun s2({a:$v}) = {a: h($v')}
  | s2({$l:$v'}) = {s2: s2($v')}

replace _* .a -> {d:$u} under $v by {ee:{}}
where
{sl1:$g1} in $u,
{sl2:$g2} in $v,
sl1=sl2
in $db

sfun s1({a:$v}) = let sfun h({d:$u}) =
  if isEmpty(select {"found"} where ...) then s2($v)
  else {a: select {ee:{}} where ...}
  | h({$l':$u}) = s2($v)
  in {a: h($v')}
  | s1({$l:$v'}) = {s1: s1($v')}
sfun s2({a:$v}) = let sfun h({d:$u}) = ...
  | s2({$l:$v'}) = {s2: s2($v')}

193
select $tables where
Stables in
(select $sclass where 
(Class:$class) in (select $sclass where 
(Association.(src|dest):$sclass) in $db),
{is_persistent:Boolean:true} in $sclass,
Sdests in (select (Class:$sdest) where 
(Class:$class) in $db),
{is_persistent:Boolean:true} in $sclass)
where
Stables in (select $class where 
{Class:$class} in $db),
Sdests in (select $class where 
{Class:$class} U $dests),
{is_persistent:Boolean:true} in $class,
related in (select $class where 
{Class:$class} U $dests),
{is_persistent:Boolean:true} in $class,
$related in (select $class where 
{Class:$class} U $dests),
$cols in (select $cols where 
{Class:$class} in $related),
$tables in (select $class where 
{Class:$class} U $dests),
$tables in (select (Table:{name:$cname} U $cols) where 
{name:$cname} in $class),
$tables in (extend Table -> $table with $pkeys U $fkeys in $tables where 
{cols:$cols} in $table,
{Column.name.String:{$cname:{}}} in $cols,
$pkeys in (select {pkeys:{pkey:$cols} where 
{attrs.Attribute:{is_primary:Boolean:true, 
name:String:{$pname:{}}}} in $class,
{name:$sname})} in Sdests,
{name:$sname}))
Stables in
replace Table.fkeys.$key -> $ref by {Table:$table} in $tables
where {Table:$table} in $tables,
{Column.name.String:{$cname:{}}} in $ref,
{name:$tname} in $table,
$tname = $rname

Why DFA instead of NFA

replace _ *(a | c)->$t by {ee:[]} in $db

let
sfun h1({a:$t}) = {a: {ee:[]}}
| h1({c:$t}) = {c: {ee:[]}}
| h1({l:$t}) = {l: h1($t) U h3($t)}
and
sfun h2({l:$t}) = {l:$t}
and
sfun h3({a:$t}) = {a: {ee:[]}}
| h3({c:$t}) = {c: {ee:[]}}
| h3({l:$t}) = {l:$t}
in h1($db)
Why DFA instead of NFA

replace \_\_ \_.(a \mid c)->\$t by \{ee:{}\} in $db$

let

$h1({a:\$t}) = \{a: \{ee: \{}\}\}$

$h1({c:\$t}) = \{c: \{ee: \{}\}\}$

$h1({$l:\$t}) = \{\$l: h1(\$t) \cup h3(\$t)\}$

and

$h2({\$l:\$t}) = \{\$l: \$t\}$

and

$h3({a:\$t}) = \{a: \{ee: \{}\}\}$

$h3({c:\$t}) = \{c: \{ee: \{}\}\}$

$h3({\$l:\$t}) = \{\$l: \$t\}$

in $h1(\$db)$

$\$db = \{b: \{b: \{c: \{d: {}\}\}\}\}$

replace \_\_\_ \_ (a \mid c)->\$t by \{ee: {}\} in $\$db$

let

$h1({a:\$t}) = \{a: \{ee: \{}\}\}$

$h1({c:\$t}) = \{c: \{ee: \{}\}\}$

$h1({\$l:\$t}) = \{\$l: h1(\$t) \cup h3(\$t)\}$

and

$h2({\$l:\$t}) = \{\$l: \$t\}$

and

$h3({a:\$t}) = \{a: \{ee: \{}\}\}$

$h3({c:\$t}) = \{c: \{ee: \{}\}\}$

$h3({\$l:\$t}) = \{\$l: \$t\}$

in $h1(\$db)$

$\{b: h1(b: \{c: \{d: {}\}\})\}$

$= h3({b: \{c: \{d: {}\}\})}$

$\cup h3({b: \{c: \{d: {}\}\})}$

= ...
Related work

• James Cheney: FLUX: functional updates for XML. ICFP 2008:3-14


• Soichiro Hidaka, Zhenjiang Hu, Hiroyuki Kato, Keisuke Nakano: Towards a compositional approach to model transformation for software development. SAC 2009: 468-475

Remaining work

• Mapping replace-exp. into sr without isempty. isempty introduces transitive closure.
  - use schema information (or, path-index).
  - sr extension with accumulation parameters.
  - use new graph algebra with simple sr.

Thank you
SEMANTIC STRUCTURES OF BIDIRECTIONAL PROGRAMMING

Kazuyuki Asada (The University of Tokyo)
12 January, 2011

Abstract

☐ This talk is about ...

some properties on some constructors
(like products, coproducts, ...)
in Bidirectional Programming.

Part I

Introduction:

Bidirectional Programming
Bidirectional Program

Bidirectional Programming Language

- Bidirectional Programming Language as Domain-Specific Language
  - Target: Relational DB, String, Tree, Graph, ...

- Bidirectional Programming in General-Purpose Language
  - in Haskell, Ocaml, ...

Example of Bidirectional Program

- Bidirectional Sort
  (assuming that view-operations keep list length)
- \( \text{bsort}^\triangleright : \text{List int} \rightarrow \text{List int} = \text{foldl insert \[\]} \)
- \( \text{bsort}^\triangleleft : \text{List int} \times \text{List int} \rightarrow \text{List int} \)
  - Algorithm: an input \([2 \ 4 \ 1 \ 5]\) \rightarrow its complement:
    - \([\[], \[]\] \rightarrow \([\[2\], \[0\]\]) \rightarrow \([\[2\ 4\], \[1\ 0\]\])
    - \([\[1\ 2\ 4\], \[0\ 1\ 0\]\]) \rightarrow \([\[1\ 2\ 4\ 5\], \[3\ 0\ 1\ 0\]\])
  - \( \text{bsort}^\triangleright [2 \ 4 \ 1 \ 5] \ l = \) -- using \([3\ 0\ 1\ 0]\)
    - \([\text{l-3-0-1}.0 \quad \text{l-3-0}.1 \quad \text{l-3}.0 \quad \text{l}.3\]\)
  - \( \text{bsort}^\triangleright [2 \ 4 \ 1 \ 5] \ \text{swap}(\text{bsort}^\triangleright [2 \ 4 \ 1 \ 5]) = [1 \ 4 \ 2 \ 5] \)
Example of Bidirectional Program

<table>
<thead>
<tr>
<th>name</th>
<th>age</th>
<th>address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taro</td>
<td>23</td>
<td>Asakusa</td>
</tr>
<tr>
<td>Hana</td>
<td>18</td>
<td>Hongo</td>
</tr>
</tbody>
</table>

Source DB

<table>
<thead>
<tr>
<th>name</th>
<th>age</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taro</td>
<td>20</td>
</tr>
<tr>
<td>Hana</td>
<td>18</td>
</tr>
</tbody>
</table>

GUI view of Abstracted Data

<table>
<thead>
<tr>
<th>name</th>
<th>age</th>
<th>address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taro</td>
<td>20</td>
<td>Asakusa</td>
</tr>
<tr>
<td>Hana</td>
<td>18</td>
<td>Hongo</td>
</tr>
</tbody>
</table>

Stability (GetPut law)

\[
f = (f^+, f^-) : \text{stable} \quad \text{if} \quad f^-(s, f^+ s) = s
\]

Compositional Programming

- **Basic one: Sequential Composition**

\[
f; g = (f^+; g^+, \lambda a c. f^- a (g^- (f^+ a) c))
\]

If \( f \) and \( g \) are stable, so is \( f;g \).
**Duplication-by-Split**

- Dual view, but single update: [M. Takeichi]

If $f$ and $g$ are stable, so is $\langle f, g \rangle$.

**Part II**

(Informal) Semantics of Bidirectional Programming:

Monoidal Product, Trace, Product, and Coproduct

**Categories of Bidirectional Programs**

- Design choices for bidirectional programming:
  - Arbitrary typing? or “Diagonally” typing?
  
  ![Diagram]

  With or without stability law, or other laws such as PutGet.

  Here we consider three categories:
  
  $\text{Bi}(C)$, $\text{Bi}^A(C)$, $\text{Bi}^C(C)$
**Bi(\mathcal{C})**

- For a cartesian category \( \mathcal{C} \),
  - a category \( \text{Bi}(\mathcal{C}) \) consists of
    - objects: pairs of objects in \( \mathcal{C} \), and
    - morphisms from \((A, A')\) to \((B, B')\):
      - pairs of morphisms \( f^< : A \to B \) and \( f^> : A' \to B' \).
  - Composition is the sequential composition.
  - Identity morphism on \( A \) is given by \((\text{id}_A, \pi_2)\).

**Reflection function**

- For a morphism \( f : (A, A') \to (B, B') \), we call the function \( \mathcal{C}(B, B') \to \mathcal{C}(A, A') \) reflection function.

- This does not determine the original morphism \( f = (f^>, f^<) : (A, A') \to (B, B') \), e.g.

  ![Reflection function diagram]

  This has no information of “view”, i.e., \( f^> \).

**\text{Bi}^\Delta(\mathcal{C}), \text{Bi}^\Delta_S(\mathcal{C})**

- For a cartesian category \( \mathcal{C} \),
  - a category \( \text{Bi}^\Delta(\mathcal{C}) \) is defined as
    - the full subcategory of \( \text{Bi}(\mathcal{C}) \) determined by the objects \( \{(A, A) | A \in \mathcal{C}\} \).
  - For a morphism in \( \text{Bi}^\Delta(\mathcal{C}) \), we call it stable if its reflection function maps \( \text{id}_B \) to \( \text{id}_A \).
  - Identity in \( \text{Bi}^\Delta_S(\mathcal{C}) \) is stable, and composition preserves stability, so we have a subcategory \( \text{Bi}^\Delta_S(\mathcal{C}) \) of stable morphisms.
Monoidal Product

- Parallel Composition:

- If \( f \) and \( g \) are stable, so is \( f \otimes g \).
- This \( \otimes \) is a functor and forms symmetric monoidal category.

\[
\begin{align*}
A & \otimes C \\
\rightarrow & \\
B & \otimes D \\
\downarrow & \\
A' & \otimes C' \\
\rightarrow & \\
B' & \otimes D'
\end{align*}
\]

- Monoidal unit and View operation

- The unit of the monoidal product is \((1, 1)\).
- Bidirectional morphism from \((B, B')\) to the unit \((1,1)\) in \( \text{Bi}(\mathbb{C}) \) bijectively correspond to ordinary morphism from \( B \) to \( B' \) in \( \mathbb{C} \).
- Then reflection function is just composition.

\[
\begin{align*}
A & \rightarrow B \\
\downarrow & \\
A' & \rightarrow B'
\end{align*}
\]

Trace

- For a monoidal category \( \mathbb{C} \), trace operator \( tr(-) \) is the following operator (with certain axioms).

\[
f: A \otimes C \rightarrow B \otimes C \\
tr(f): A \rightarrow B
\]

- Trace operator is for repeated computation.
  - Trace for (cartesian) products is equivalent to fixed point operator [Hyland, Hasegawa 97].
  - Trace for coproducts is called iterator (like while loop).
Geometry of Interaction is originally studied for proof nets in linear logic [Girard 89].

Categorically, it is understood by Int construction:
For a traced monoidal category \( \mathcal{C} \),
\[
\text{Int(} \mathcal{C} \text{)} \text{ consists of:}
\]
- objects: pairs \((A, A')\) of objects in \( \mathcal{C} \)
- morphisms from \((A, A')\) to \((B, B')\):
  morphisms \(A \otimes B' \to B \otimes A'\) in \( \mathcal{C} \).

If \( \mathcal{C} \) has trace, so does \( \text{Int}( \mathcal{C} ) \). (Moreover Compact closed category) [Joyal, Street and Verity 96]

**Bi vs. Int**

- \( \text{Bi(-)} \) construction can be considered for symmetric monoidal categories. (But here we skip.)
- For a cartesian category \( \mathcal{C} \),
  a morphism \( f : (A, A') \to (B, B') \) in \( \text{Int}( \mathcal{C} ) \) is (essentially) a pair of morphism \((f^\triangleright, f^\triangleleft)\) where \( f^\triangleright : A \times B' \to B, f^\triangleleft : A \times B' \to A' \) in \( \mathcal{C} \).
- Hence bidirectional program is such morphism that \( f^\triangleright \) discard \( B' \) information, and there is a symmetric monoidal functor \( J : \text{Bi}( \mathcal{C} ) \to \text{Int}( \mathcal{C} ) \) (: not faithful).

**Trace operator for Bi(\( \mathcal{C} \))**

- **Prop.**
  For a traced symmetric monoidal category \( \mathcal{C} \), (especially a cartesian category with fixed point operator,) we have a traced monoidal category \( \text{Bi}( \mathcal{C} ) \) such that the symmetric monoidal functor \( J : \text{Bi}( \mathcal{C} ) \to \text{Int}( \mathcal{C} ) \) preserves their traces.
Duplication-by-Split by products

**Prop.**

In Bi(\(\mathbb{C}\)), there are cartesian products:

\[
(A, A') \times (B, B') := (A \times B, A' + B')
\]

\[
f = (f', f') \quad g = (g', g')
\]

\[
<f, g> = \langle f', g' \rangle, (d ; [f', g'])
\]

Products vs. Monoidal Products

<table>
<thead>
<tr>
<th>Flat type (Eq)</th>
<th>Dup.-by-Split by Products</th>
<th>Dup.-by-Split by Monoidal Prod.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flat type (Eq)</td>
<td>Not required</td>
<td>Required</td>
</tr>
<tr>
<td>Property</td>
<td>Genuine cartesian</td>
<td>Only beta equality, w/o eta eq.</td>
</tr>
<tr>
<td>Where</td>
<td>in Bi((\mathbb{C}))</td>
<td>Bi(^{\Delta})((\mathbb{C}))</td>
</tr>
<tr>
<td>Stability</td>
<td>Difficult to formalize*</td>
<td>Ok</td>
</tr>
<tr>
<td>Safety(?)</td>
<td>Safe(?)</td>
<td>Unsafe(?)</td>
</tr>
</tbody>
</table>

*: On stability of products, at least the following holds:
the reflection function maps \(\pi_1; \iota_1\) and \(\pi_2; \iota_2\) to \(\text{id}_C\).

(cf. Here, \(\pi_1; \iota_1\) and \(\pi_2; \iota_2\) are pairing injective: i.e.,
\(<\pi_1; \iota_1, \pi_2; \iota_2>\) is injective.)

On Safety(?)

- For duplication by monoidal products, we can post-compose other bidirectional program \(h\) in Bi\(^{\Delta}\)(\(\mathbb{C}\)).
- Then, it is not rare at all that both \(B\) and \(C\) are changed via \(h\).
- After that, final change on \(A\) is nothing.
  This might make users write unintended programs.

- On the other hand, with cartesian product, we can constrain not to post-compose, or if we program in Bi(\(\mathbb{C}\)), no problem.
“Coproduct”

- We have a construction as the following:
  \[(A, A')+(B, B') := (A+B, A'+B')\]

- What is this?

- ... To make a mapping on morphisms, we define it in \(\text{Bi}^A(C)\):
  \[(A+C) \times (B+D)\]
  \[\sim A\times B + A\times D + C\times B + C\times D \rightarrow A+A+C+C \rightarrow A+C\]

- Then Coproduct? Or, just monoidal product?

Semi-coproduct

- Unfortunately, + is not even monoidal product.
- Since, + is not even functor.
  
  This + does not preserve identity.

- However, + preserve composition in \(\text{Bi}^A_s(C)\).
  
  This kind of structure is called semi-functor.

- Moreover, + in \(\text{Bi}^A_s(C)\) is semi-coproduct.

  (Cf. [Hayashi 85])

Properties of Semi-coproduct

- For stable bidirectional programs
  
  \[f_i: A_i \rightleftharpoons B \quad (i=1,2), \text{ there is } [f_1, f_2]: A_1 + A_2 \rightleftharpoons B.\]
  
  For types \(A_i (i=1,2)\), there is \(\ iota: A_i \rightleftharpoons A_1 + A_2.\)

- The following equations hold:
  
  \[[f_1, f_2] \ ; \ g = [f_1; g, f_2; g]\]
  
  \[\iota_i \ ; [f_1, f_2] = f_i \quad (i=1,2)\]
  
  \[[\iota_1, \iota_2] = \text{id} + \text{id}\]
Example of Bidirectional Program

<table>
<thead>
<tr>
<th>name</th>
<th>age</th>
<th>address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taro</td>
<td>23</td>
<td>Asakusa</td>
</tr>
<tr>
<td>Hana</td>
<td>18</td>
<td>Hongo</td>
</tr>
</tbody>
</table>

Source DB

<table>
<thead>
<tr>
<th>name</th>
<th>age</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taro</td>
<td>20</td>
</tr>
<tr>
<td>Hana</td>
<td>18</td>
</tr>
</tbody>
</table>

GUI view of Abstracted Data

<table>
<thead>
<tr>
<th>name</th>
<th>age</th>
<th>address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taro</td>
<td>20</td>
<td>Asakusa</td>
</tr>
<tr>
<td>Hana</td>
<td>18</td>
<td>Hongo</td>
</tr>
</tbody>
</table>

Bidirectional Programming and Monad

- **Pure Bidirectional Programming:**
  
  ![Diagram of pure bidirectional programming]

- **Bidirectional Programming with Monad T**
  (e.g. I/O Monad), or in CBV Language:
  
  ![Diagram of bidirectional programming with Monad]

Summary

- **Optional “world”s for bidirectional programming:**
  \[ \text{Bi}(C) \leftrightarrow \text{Bi}^A(C) \leftrightarrow \text{Bi}^E(C) \]

- **We have the following constructors on bidirectional programs:**
  - Monoidal product in Bi(C), Bi^A(C), Bi^E(C)
  - Trace operator in Bi(C), Bi^A(C)
  - Cartesian product in Bi(C)
  - Semi-coproduct in Bi^E(C)

- **Bidirectional programs easily accommodate with monad, and with arrow.**
More

- The same thing might hold about trace w.r.t. coproducts: i.e., “if C has iterator, then \( \text{Bi}_s(C) \) has (semi-)iterator.” However we first define the notion of semi-trace...

cf. Bidir. Progr. forms an Arrow?

- \( \text{Bi}(A, B) := (A -> B) \times (A \times B -> A) \)
- \( >>>, \) first operator seems exist, but is there arr: \((A -> B) -> \text{Bi}(A, B)\)?
- arr \( f = \lambda a \cdot (f a, \lambda b \cdot a) \) does not work, since this does not map identity to identity.
- There seems not to be arrow structure.
Most used embedded DSLs for programming

- MS Excel macro language
- SQL
- Regular expressions

Observe: They are designed to be domain-oriented, declarative and of limited expressive power.

Regular language

Definition (Regular language)

A regular language is a language (set of strings) over some finite alphabet $A$ that is accepted by some finite automaton.
Regular expression

**Definition (Regular expression)**

A regular expression (RE) over finite alphabet $A$ is an expression of the form

$$E, F ::= 0 | 1 | a | E | F | EF | E^*$$

where $a \in A$

Language interpretation of regular expressions

**Definition (Language interpretation)**

The language interpretation of a regular expression $E$ is the set of strings $L[E]$ defined by

- $L[0] = \emptyset$
- $L[1] = \{\epsilon\}$
- $L[a] = \{a\}$
- $L[E | F] = L[E] \cup L[F]$
- $L[EF] = L[E] \circ L[F]$
- $L[E^*] = \bigcup_{i \geq 0} (L[E])^i$

where $S \circ T = \{st \mid s \in S, t \in T\}$, $E^0 = \{\epsilon\}$, $E^{i+1} = EE^i$.

Kleene’s Theorem

**Theorem (Kleene 1956)**

A language is regular if and only if it is denoted by a regular expression under its language interpretation.
**Theory = Language interpretation**

What we normally learn and teach about regular expressions in theory of computing classes:

- They’re just a way to talk about finite state automata
- All equivalent regular expressions are interchangeable since they accept the same language.
- All equivalent automata are interchangeable since they accept the same language.
  - We might as well choose an efficient one (deterministic, minimal state): it processes its input in linear time and constant space.
- Complexity of containment and equivalence (PSPACE-complete).
- Closure properties, Myhill-Nerode Theorem, Pumping Lemma, Star-height problem . . .

Observe: Assumes language interpretation!

**Practice = Type interpretation**

How regular expressions are used in programming:

- Group matching: Does the RE match and where do (some of) its sub-REs match in the string?
- Substitution: Replace matched substrings by specified other strings
- Extensions: Backreferences, look-ahead, look-behind....
- Lazy vs. greedy matching, possessive quantifiers, atomic grouping
- Optimization

Observe: Language interpretation (yes/no) inappropriate, need more refined interpretation

---

Example

{(ab)(cd)(abc)}*

Match against abdabc
For each parenthesized group a substring is returned.

<table>
<thead>
<tr>
<th></th>
<th>PCRE</th>
<th>POSIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1$</td>
<td>$ab$</td>
<td>$abc$</td>
</tr>
<tr>
<td>$2$</td>
<td>$ab$</td>
<td>$\epsilon$</td>
</tr>
<tr>
<td>$3$</td>
<td>$c$</td>
<td>$\epsilon$</td>
</tr>
<tr>
<td>$4$</td>
<td>$\epsilon$</td>
<td>$abc$</td>
</tr>
</tbody>
</table>

*Or special null-value
Intermezzo: Optimization??

Optimizing regular expressions = rewriting them to equivalent form that is more efficient for matching.²

Perl-compliant regular expressions (what you get in Perl, Python, Ruby, Java) use backtracking parsing.

Does not handle “problematic” regular expressions: $E^*$ where $E$ contains $\epsilon$ – will typically crash at run-time (stack overflow).

²Friedl, Mastering Regular Expressions, chapter 6: Crafting an efficient expression

Why discrepancy between theory and practice?

● Theory is extensional: About regular languages.
  ● Does this string match the regular expression? Yes or no?
● Practice is intensional: About regular expressions as grammars.
  ● Does this string match the regular expression and if so how—which parts of the string match which parts of the RE?
● Ideally: Regular expression matching = parsing + “catamorphic” processing of syntax tree
● Reality:
  ● Naïve backtracking matching, or
  ● finite automaton + opportunistic instrumentation to get some parsing information (TCL (?), Laurikari 2000, Cox 2010).

Regular expression parsing

● Regular expression parsing: Construct parse tree for given string.
● Representation of parse tree: Regular expression as type

Example

Parse abdabc according to $((ab)(c\mid d)\mid (abc))^*$.

$p_1 = \text{inl}((a, b), \text{inr} d, \text{inr}(a, (b, c)))$
$p_2 = \text{inl}((a, b), \text{inr} d, \text{inl}((a, b), \text{inl} c))$

$p_1, p_2$ have type $\text{list} \left[ ((a \times b) \times (c + d) + a \times (b \times c)) \right]$

Compare with regular expression $((ab)(c\mid d)\mid (abc))^*$.

The elements of type $E$ correspond to the syntax trees for strings parsed according to regular expression $E$!
Type interpretation

Definition (Type interpretation)
The type interpretation $\mathcal{T}[$ ] compositionally maps a regular expression $E$ to the corresponding simple type:

- $\mathcal{T}[0] = \emptyset$  (empty type)
- $\mathcal{T}[1] = \{()\}$  (unit type)
- $\mathcal{T}[a] = \{a\}$  (singleton type)

- $\mathcal{T}[E \mid F] = \mathcal{T}[E] + \mathcal{T}[F]$  (sum type)
- $\mathcal{L}[E \mid F] = \mathcal{T}[E] \times \mathcal{T}[F]$  (product type)

- $\mathcal{T}[E^*] = \{\langle v_1, \ldots, v_n \rangle \mid v_i \in \mathcal{T}[E]\}$  (list type)

Flattening

Definition
The flattening function $\text{flat}() : \text{Val}(A) \rightarrow \text{Seq}(A)$ is defined as follows:

- $\text{flat}(()) = \epsilon$
- $\text{flat}(a) = a$
- $\text{flat}((v, w)) = \text{flat}(v) \text{flat}(w)$
- $\text{flat}([v_1, \ldots, v_n]) = \text{flat}(v_1) \ldots \text{flat}(v_n)$

Example

- $\text{flat}(\text{inl}((a, b), \text{inr}(a, (b, c)))) = abdabc$
- $\text{flat}(\text{inl}((a, b), \text{inr}(a, (b, c)), \text{inl}((a, b), \text{inl}(c)))) = abdabc$

Regular expressions as types

Informally:

\[
\text{string } s \text{ with syntax tree } p \text{ according to regular expression } E \iff \\
\text{string } \text{flat}(v) \text{ of value } v \text{ element of simple type } E
\]

Theorem

$\mathcal{L}[E] = \{\text{flat}(v) \mid v \in \mathcal{T}[E]\}$
Membership testing versus parsing

Example

\[ E = ((ab)(c|d)|(abc))^* \quad E_d = (ab(c|d))^* \]

- \( E_d \) is unambiguous: If \( v, w \in \mathcal{T}[E_d] \) and flat\( (v) = \text{flat}(w) \) then \( v = w \). (Each string in \( E_d \) has exactly one syntax tree.)
- \( E \) is ambiguous. (Recall \( p_1 \) and \( p_2 \).)
- \( E \) and \( E_d \) are equivalent: \( L[E] = L[E_d] \)
- \( E_d \) "represents" the minimal deterministic finite automaton for \( E \).
- Matching (membership testing): Easy—use \( E_d \).
- But: How to parse according to \( E \) using \( E_d \)?

Regular expression equivalence and containment

Sometimes we are interested in regular expression containment or equivalence.\(^3\)

Definition

- \( E \) is contained in \( F \) if \( L[E] \subseteq L[F] \).
- \( E \) is equivalent to \( F \) if \( L[E] = L[F] \).

Regular expression equivalence and containment are easily related: \( E \leq F \iff E + F = F \) and \( E = F \iff (E \leq F \land F \leq E) \).

---

\(^3\)See e.g. Yasuhiro’s talk.

Coercion

Definition (Coercion)

Partial coercion: Function \( f : \mathcal{T}[E] \rightarrow \mathcal{T}[F] \) such that \( f(v) = \bot \) or \( \text{flat}(v) = \text{flat}(f(v)) \).

Coercion: Function \( f : \mathcal{T}[E] \rightarrow \mathcal{T}[F] \) such that \( \text{flat}(v) = \text{flat}(f(v)) \).

Intuition:

- A coercion is a syntax tree transformer.
- It maps a syntax tree under regular expression \( E \) to a syntax tree under regular expression \( F \) for same string.
- Coercion = function where you “don’t discard, duplicate, shuffle”\(^4\)

---

\(^4\)Recall Akimasa Morihata’s talk
Example

\[ f : ((a \times b) \times (c + d)) \rightarrow (a \times (b \times (c + d))) \]

- flat\( f(v) \) = flat\( v \) for all \( v : ((a \times b) \times (c + d)) \) list.
- So \( f \) defines a coercion from \( E = ((ab)(c\{d\})| (abc))^* \) to \( E_d = (ab(c\{d\}))^* \).
- \( f \) maps each proof of membership (= syntax tree) of a string \( s \) in regular language \( L[E] \) to a proof of membership of string \( s \) in regular language \( L[E] \).
- So \( f \) is a constructive proof that \( L[E] \) is contained in \( L[F] \)!

Regular expression containment by coercion

Proposition

\[ L[E] \subseteq L[F] \]

if and only if there exists a coercion from \( T[E] \) to \( T[F] \).

Idea:

- Come up with a sound and complete inference system for proving regular expression containments.
- Interpret it as a language for defining coercions:
  - Soundness: Each proof term defines a coercion.
  - Completeness: For each valid regular expression containment there is at least one proof term.

A crash course on regular expression containment

- All classical sound and complete axiomatizations basically start with the axioms for idempotent semirings.
- Then they add various inference rules to capture the semantics of Kleene star.
- Algorithms for deciding containment are "coinductive" in nature:
  - transformation to automata or
  - regular expression containment rewriting
- The algorithms have little to do with the axiomatizations!
  - They do not produce a proof (derivation)
  - They cannot be thought of proof search in an axiomatization.
Our approach

Idea:
- Axiomatization =
  Idempotent semiring
  + finitary unrolling for Kleene-star
  + general coinduction rule (for completeness)
  - restriction on coinduction rule (for soundness)
- Each rule can be interpreted as natural coercion constructor.
- Algorithms for deciding containment can be thought of as strategies for proof search. They yield coercions, not just decisions (yes/no).

Idempotent semiring axioms

Proviso: + for alternation, × for concatenation, * for Kleene-star.

\[
\begin{align*}
E + (F + G) &= (E + F) + G \\
E + F &= F + E \\
E + 0 &= E \\
E + E &= E \\
E \times (F \times G) &= (E \times F) \times G \\
1 \times E &= E \\
E \times 1 &= E \\
E \times (F + G) &= (E \times F) + (E \times G) \\
(E + F) \times G &= (E \times G) + (F \times G) \\
0 \times E &= 0 \\
E \times 0 &= 0
\end{align*}
\]

Kleene-star

Finitary unrolling:

\[
E^* = 1 + E \times E^*
\]

General coinduction rule:

\[
\begin{array}{c}
\vdots \\
[E = F] \\
\vdots \\
E = F \\
E = F
\end{array}
\]

- Fantastically powerful rule!
- Unfortunately unsound
- But “right idea” – just needs controlling.
**Type-theoretic formulation: Idempotent semiring**

With explicit proof terms, using judgement form (due to dispatch in coinduction rule) and containment instead of equivalence:

\[
\Gamma \vdash \text{shuffle} : E + (F + G) \leq (E + F) + G \\
\Gamma \vdash \text{shuffle}^{-1} : E + (F + G) \leq (E + F) + G \\
\Gamma \vdash \text{retag} : E + F \leq F + E \\
\Gamma \vdash \text{untag} : E + E \leq E \\
\Gamma \vdash \text{tagL} : E \leq E + F \\
\Gamma \vdash \text{untagL} : E \leq F + E \\
\Gamma \vdash \text{proj} : E \times 1 \leq E \\
\Gamma \vdash \text{proj}^{-1} : E \leq E \times 1 \\
\Gamma \vdash \text{distL} : E \times (F + G) \leq (E \times F) + (E \times G) \\
\Gamma \vdash \text{distL}^{-1} : (E \times F) + (E \times G) \leq E \times (F + G) \\
\text{...}
\]

**Primitive coercions**

- Each axiom can be interpreted as a coercion; e.g.,

  \[
  \text{shuffle} \left( \text{inl} \ x \right) = \text{inl} \ (\text{inl} \ x) \\
  \text{shuffle} \left( \text{inr} \ (\text{inl} \ y) \right) = \text{inl} \ (\text{inr} \ y) \\
  \text{shuffle} \left( \text{inr} \ (\text{inl} \ y) \right) = \text{inr} \ y
  \]

- The \((p, p^{-1})\) pairs denote type isomorphisms:

  \(p \circ p^{-1} = \text{id} \) and \(p^{-1} \circ p = \text{id} \).

- \((\text{tagL}, \text{untag})\) is an embedding-projection pair, but not an isomorphism even for \(E \equiv F\):

  \(\text{untag} \circ \text{tagL} = \text{id}\), but \(\text{tagL} \circ \text{untag} \neq \text{id}\).

**Type-theoretic formulation: Kleene-star, coinduction**

\[
\Gamma \vdash \text{wrap} : 1 + E \times E^* \leq E^* \\
\Gamma \vdash \text{wrap}^{-1} : E^* \leq 1 + E \times E^* \\
\frac{\Gamma, f : E \leq F \vdash c : E \leq F}{\Gamma \vdash \text{fix} f : c : E \leq F} \quad (S_x)
\]

- Interpret \((\text{wrap}, \text{wrap}^{-1})\) as isomorphism in accordance with isorecursive interpretation of lists.

- Interpret \(\text{fix}\) as least fixed point operator; that is, as recursively defined coercion: \(\text{fix} = Y(\lambda f. c)\).

- Add side-condition \((S_x)\) that ensures that recursively defined coercions terminate.
The mother of all side conditions

**Definition**
Coercion \( c \) in \( \Gamma \vdash c : E \leq F \) is **hereditarily total** if whenever its free variables are bound to (total!) coercions then it denotes a (total!) coercion.

Side condition \( S_0 \) (Total):
\[
\text{fix } f. c \text{ is hereditarily total}
\]

**Theorem**
It is undecidable whether \( \Gamma \vdash c : E \leq F \) is hereditarily total.

Proved by Eijiro Sumii, Yasuhiro Minamide, Naoki Kobayashi, Atsushi Igarashi and Fritz Henglein at the IFIP TC 2 Working Group 2.8 meeting at Shirahama, Japan, April 11-16, 2010.

Other side conditions (informally)

**Definition (Size of value)**
- 0-size of \( v = |\text{flat}(v)| \) (length of underlying string)
- 1-size of \( v = 0\text{-size of } v + \text{number of } (\text{ occurring in } v

**Definition**
- \( S_2 \): Guarantees that recursive calls in coercions are on values of smaller 1-size.
- \( S_4 \): Guarantees that recursive calls in coercions are on values of smaller 0-size.

Soundness and completeness

**Theorem (Soundness and completeness)**
For any of the side conditions \( S_0, S_2, S_4 \):
\[
\mathcal{L}[E] \subseteq \mathcal{L}[F]
\]
if and only if there exists \( c \) such that \( \vdash c : E \leq F \)

**Theorem (Parametric soundness and completeness)**
For side conditions \( S_0, S_2 \) (but not \( S_4 \)):
For all \( E', F' \) we have
\[
\mathcal{L}[E[E'/X]] \subseteq \mathcal{L}[F[E'/X]]
\]
if and only if there exists \( c \) such that \( \vdash c : [\forall X.]E \leq F \)
Computational interpretation of proofs

It is possible to:

- code Salomaa’s and Grabmeyer’s axiomatizations of regular expression equivalence with side condition $S_4$.
- code Kozen’s axiomatization of Kleene Algebra (= regular expression equivalence) with side condition $S_2$.

Significance:

- Provides computational interpretation of their proofs: Proofs = coercions (functions that do not discard, duplicate, shuffle)
- Shows that Kozen’s axiomatization is parametric complete, but Salomaa’s ($F_1$) and Grabmeyer’s are not. (Message: Use 1-size, not 0-size.)
- Our axiomatization provides “more proofs”: Better if you are looking for an efficient proof.
  - Raises question: How to find one?

So what?

Summary so far:

- A regular expression denotes a type (“right-regular type”).
- A proof of regular expression containment denotes a coercion from one regular expression interpreted as a type to the other.

What is this good for?

Theoretical applications

Provides theoretical framework for formulating problems and (eventually) solving them:

- Parametric completeness
- Coercion synthesis
- Oracle coding (see below)
- Fast parsing (see below)
- Ambiguity resolution
- Regular expressions as refinement types for strings
Practical applications

First results:
- Bit-coded parse trees
- Bit-coded regular expression parsing

Bit coding

- Record binary choices for expanding a regular expression $E$ into a particular string $s$.
- The sequence of choices (as bits) is the bit coding of $s$ under $E$.

Example

Recall syntax trees $p_1, p_2$ for $abdac$ under $E = ((a \times b) \times (c + d) + a \times (b \times c))^*$.  

- $p_1 = [\text{inl}((a, b), \text{inr} d), \text{inr} (a, (b, c))]$
- $p_2 = [\text{inl}((a, b), \text{inr} d), \text{inl} ((a, b), \text{inl} c)]$

We can code them by storing only their inl, inr occurrences:

\[
\text{code}(p_1) = 011 \\
\text{code}(p_2) = 0100
\]

Bit decoding

There is a linear-time polytypic function $\text{decode}$ that can reconstitute the syntax trees.

Theorem

$\text{decode}_E(\text{code}_E(v)) = v$ for all $v \in T[E]$.

Example

\[
\begin{align*}
\text{decode}_E(011) &= [\text{inl}((a, b), \text{inr} d), \text{inr} (a, (b, c))] \\
\text{decode}_E(0100) &= [\text{inl} ((a, b), \text{inr} d), \text{inl} ((a, b), \text{inl} c)]
\end{align*}
\]
Bit coding: Applications

- Bit-coded parse trees are (typically substantially) smaller than serialized parse trees (e.g., source code).
  - Support efficient left-to-right traversal of parse trees.
  - Can be combined with statistical compression to obtain improved compression.
- Coercions can be automatically specialized to operate on bit codes instead of manifest parse trees (not worked out in detail yet); e.g.,
  
  $\text{retag}(0d) = 1d$
  $\text{retag}(1d) = 0d$
  $\text{assoc}(d) = d$

- Right-regular grammars yield better (more compressed) bit codes than regular expressions.

Ambiguity resolution

- All regular expression equivalences yield coercion isomorphisms, except for one: $(\text{tagL}, \text{untag}) : E = E + E$.
- This is where ambiguity is introduced/eliminated! Always choosing $\text{tagL}$ (from left to right) favors the left alternative, as in Perl.
- Eager matching seems to correspond to choosing the right alternative in $E^* = 1 + E \times E^*$; lazy matching to choosing the left alternative.

Open problem

Design an expressive annotation for regular expressions that specifies a choice function for deterministically choosing one of potentially multiple syntax trees for a string and that can (at a minimum) express POSIX and PCRE rules.

Bit coded regular expression parsing

- Problem:
  - Input: string $s$ and regular expression $E$.
  - Output: (some) parse tree $p$ such that $\text{flat}(p) = s$.
- Goal: Output bit coding $\text{code}_E(p)$ instead.
- Dual advantage:
  - Less space used for output.
  - Output faster to compute.
- How to do that? Mark the "turns" in Thompson NFA (they yield the bit coding)
**DFASIM algorithm: Outline**

1. **RE to NFA**: Build Thompson-style NFA with suitable output bits
2. **NFA to DFA**: Perform extended DFA construction (only for states required by input string), with (multiple) bit sequence annotations on edges
3. Traverse accepting path from right to left to construct bit coding by concatenating bit sequences.

**Thompson-style NFA generation with output bits**

<table>
<thead>
<tr>
<th></th>
<th>NFA</th>
<th>Extended NFA</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td><img src="image1" alt="NFA Diagram" /></td>
<td><img src="image2" alt="Extended NFA Diagram" /></td>
</tr>
<tr>
<td>1</td>
<td><img src="image3" alt="NFA Diagram" /></td>
<td><img src="image4" alt="Extended NFA Diagram" /></td>
</tr>
<tr>
<td>a</td>
<td><img src="image5" alt="NFA Diagram" /></td>
<td><img src="image6" alt="Extended NFA Diagram" /></td>
</tr>
<tr>
<td>E F</td>
<td><img src="image7" alt="NFA Diagram" /></td>
<td><img src="image8" alt="Extended NFA Diagram" /></td>
</tr>
<tr>
<td>E</td>
<td><img src="image9" alt="NFA Diagram" /></td>
<td><img src="image10" alt="Extended NFA Diagram" /></td>
</tr>
</tbody>
</table>

**Benchmark experiments**

Benchmarks from Veanes et al. (2010)
Benchmark experiment #2

![Graph](image1)

Benchmark experiment #6

![Graph](image2)

References

- Henglein, Nielsen, “Regular Expression Containment: Coinductive Axiomatization and Computational Interpretation”, POPL 2011

- Nielsen, Henglein, “Bit-coded Regular Expression Parsing”, submitted to LATA 2011
Related work

- Frisch, Cardelli (2004): Regular types corresponding to regular expressions, linear-time parsing for REs;
- Hosoya et al. (2000-): Regular expression types, proper extension of regular types (!), axiomatization of tree containment
- Rutten et al. (1998-): Coalgebraic approach to systems, including finite automata, extensional
- Brandt/Henglein (1998): Coinduction rule and computational interpretation for recursive types
- Cameron (1988), Jansson, Jeuring (1999): Bit coding for CFGs and algebraic types
- Cox (2010): RE2 regular expression library, TCL RE library (appear to be state of the Perl/POSIX-style “regex” libraries)

Regular expressions as refinement types for strings

- Add regular expressions as refinement types
- They’re already there: Regular types! What needs to be added is coercion synthesis (∼ deciding regular expression containment).
- Use bit coding for run-time representations and bit-coded coercions for bit transformations.

Open problem

Polymorphic regular type and coercion inference.

Related to Hosoya/Frisch/Castagna (2005), which is for regular expression types, however.

Future work

- Projection/substitution: efficient composition of parsing, containment (coercions) and catamorphic postprocessing.
- Analysis of ambiguity resolution.
- Build a PCRE- and RE2-killer library.
- Comparison of RE parsing with specialized algorithms (Knuth-Morris-Pratt, Boyer-Moor for single keyword; Aho-Corasick for multiple keywords)
- NFA constructions, relation to Fuh/Mishra S- and G-simplification?
- Proof-theoretic analysis of Krob-Boffa characterization of RE equivalence (50 page proof). Simplified proof?
- Regular expressions as refinement types: Type inference for script languages (Python, Thorn, etc.)
Workflow models

Aim
Formal specification of cooperative procedures
Implementation (GUI) verification

Motivation
Clinical Practice Guidelines (CPGs):
Detailed descriptions of specific healthcare procedures.

Problem
Verification is either too rigid (one to one), or (too) unsafe

Idea
Use typechecking to verify specification compliance

Outline

Introduction
Outline
Workflows and Communication Protocols
Implementation
Example
Future Work
What are Workflows

- Fixed sets of actions and participants
- Describes allowed sequences of actions performed by participants
- Used for describing Clinical Practice Guidelines (CPGs)
- Example: Doctor consultation

Extended workflow as Process Matrix

<table>
<thead>
<tr>
<th>Id</th>
<th>Name</th>
<th>Patient</th>
<th>Doctor</th>
<th>Nurse</th>
<th>Predecessors</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data</td>
<td>W</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Schedule</td>
<td>R</td>
<td>W</td>
<td>W</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>Result</td>
<td>R</td>
<td>W</td>
<td>N</td>
<td>2</td>
</tr>
</tbody>
</table>

What are Multiparty Session Types

- Fixed sets of channels and participants
- Describes allowed sequences of messages sent between participants
- Example: 1→3:1(String); 3→1:2(Date); 2→1:3(String); end
- Example could correspond to one way of completing the workflow

Idea:
If performing actions corresponds to sending messages on channels
Then we can represent some workflows as session types

Asynchronous $\pi$-calculus Multiparty Session Types

Problem: Cannot represent common decision
(Example of Social Interaction)

1EXPRESS’10: Nielsen, Yoshida and Honda
2POPL’08: Honda, Carbone and Yoshida
Process extensions

- Will not describe Asynchronous π-calculus with Multiparty sessions [POPL’08]
- New process construct: \( \text{sync}_{\tilde{s}, n} \{ I : P_i \}_{i \in L} \)
  Represents participation in a common decision with \( n \) participants
- Synchronization step:
  \[
  h \in \bigcap_{i=1}^{n} L_i \\
  \text{sync}_{\tilde{s}, n} \{ I : P_i \}_{i \in L_1} | ... | \text{sync}_{\tilde{s}, n} \{ I : P_n \}_{i \in L_n} \rightarrow P_{1h} | ... | P_{nh}
  \]
- New typing rule:
  \[
  \forall l \in L' : \Gamma \vdash P_l \triangleright \Delta, \tilde{s} : T_l \otimes (p, n) \quad L' \subseteq L \cup M \quad M \subseteq L \\
  \Gamma \vdash \text{sync}_{\tilde{s}, n} \{ I : P_i \}_{i \in L'} \triangleright \Delta, \tilde{s} : \{ I : T_i \}_{i \in L} \otimes M \otimes (p, n)
  \]

Results

- Theorem: Subject Reduction
  If \( \Gamma \vdash P \triangleright \Delta \) and \( P \rightarrow P' \)
  then \( \Gamma \vdash P' \triangleright \Delta' \) where \( \Delta \rightarrow^{0/1} \Delta' \).
- Communication safety
- Single Session Progress
- As expressive as the Process Matrix

\( \text{\&ims} \)

- Asynchronous π-calculus with Multiparty sessions and Symmetric sum
- First implementation of Asynchronous π-calculus with multiparty sessions and multiparty session types (It is however cheating!)
- Proof of concept implementation (slow and uses much memory)
- Includes synchronisation and symmetric sum type extensions
- \( \text{\&ims} \) extends the theory with user interaction (GUIs)
- There is a translation from the Process Matrix workflow model to \( \text{\&ims} \), which allows execution of workflows.
- \( \text{\&ims} \) and code examples are available from www.thelas.dk/index.php/APims.
Real World Example

Vulnerabilities:
- Bad faith implementations (Adversarial Model)
- Typechecking does not ensure correct value is sent
- Unimplemented Services (Gets stuck)
- No progress for multi-session processes.

From ProHealth’08

Future Work

- Improve Implementation (Compiler, Exploit parallelism)
- Encoding of Process Matrix has exponential size
- Add assertions by merging theory with [BHTY2010]
- Encode more workflow models (UML Activity Diagrams, GLIF, ...)
- Extend theory with temporal properties such as deadlines
- Encode in Adversarial Model

End of talk

- POPL08: Multiparty Asynchronous Session Types
  by Kohei Honda, Nobuko Yoshida and Marco Carbone (POPL 2008)
- BHTY2010: A theory of design-by-contract for distributed multiparty interactions
  by Laura Bocchi, Kohei Honda, Emilio Tuosto and Nobuko Yoshida (Concur 2010)
- SGI’09: A Game-Theoretic Model for Distributed Programming by Contract
  by Anders Starcke Henriksen, Tom Hvitved and Andrzej Filinski
- ProHealth’08: From Paper Based Clinical Practice Guidelines to Declarative
  Workflow Management
  by Karen Marie Lyng, Thomas Hildebrandt and Rakhava Rao Mukkamala
  Available from: http://www.trustcare.eu
- ArMo: www.thelas.dk/index.php/kpims
- Full version: www.thelas.dk/index.php/Symmetric_Sum_Types

Questions?
Semirings for Free!
An Algebraic Approach to Efficient Parallel Algorithms for Nested Reductions
Kento EMOTO (University of Tokyo)

Background

- Parallelism is the only way to get fast computation
  - HW benders improve HW performance mainly by parallelism
  - Parallel programming is however difficult for most users

- Our approach: automatic/systematic optimization of naïve (parallel) programs into efficient ones
  - Concise way to correct and efficient parallel programs

This Work

- Parallelism is the only way to get fast computation
  - HW benders improve HW performance mainly by parallelism
  - Parallel programming is however difficult for most users

- Our approach: automatic/systematic optimization of naïve (parallel) programs into efficient ones
  - Concise way to correct and efficient parallel programs
Semiring \((\alpha, \oplus, \otimes)\)

- **Examples:** \((\mathbb{R}, +, \times)\), \((\mathbb{Z}, \uparrow, +)\), \((\mathbb{N}, \uparrow, \times)\)

- **Definition**
  - \((\alpha, \oplus)\) is commutative monoid
  - \((\alpha, \otimes)\) is monoid
  - \(a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)\) (distributive)
  - \((a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)\)
  - \(a \otimes \tau_\oplus = \tau_\oplus \otimes a = \tau_\oplus\) (zero)
  - Monoid \((\alpha, \oplus)\)
    - \(a \oplus (b \oplus c) = (a \oplus b) \oplus c\) (associative)
    - \(\tau_\oplus \oplus a = a \oplus \tau_\oplus = a\) (the identity)
  - Commutative monoid \((\alpha, \oplus)\)
    - \((\alpha, \oplus)\) is monoid
    - \(a \oplus b = b \oplus a\) (commutative)

---

**Simple Problem:**
The Maximum Subsequence Sum

- Given a list \(x\), find the maximum sum of all subsequences
  
  \[
  \max \left\{ \sum [a \mid a \leftarrow s] \mid s \leftarrow \text{subs } x \right\}
  \]

- Example: \(x = [3, -4, 2]\)
  - \(\text{subs } x = [[3, -4, 2], [3, -4], [3, 2], [3], [-4, 2], [-4], [2], []]\)
  - The answer is 5 computed as follows,
    - \(5 = (3 + (-4 + 2) \uparrow (3 + (-4)) \uparrow (3 + 2) \uparrow 3 \uparrow (-4 + 2) \uparrow -4 \uparrow 2 \uparrow 0\)

---

**Efficient Computation via Semiring**

- Properties of the semiring give an efficient computation with a linear cost
  
  \[
  \max \left\{ \sum [a \mid a \leftarrow s] \mid s \leftarrow \text{subs } x \right\} = \sum [a \uparrow 0 \mid a \leftarrow x]
  \]

- List homomorphism with linear work
- Parallel implementation on various frameworks such as SkeTo, MapReduce, OpenMP, ...

The semiring gives the efficient parallel algorithm for the problem.

\[
= (3 \uparrow 0) + (-4 \uparrow 0) + (2 \uparrow 0)
= 3 + 0 + 2 = 5
\]
Question: Do Similar Problems Have Efficient Algorithms?

- Nested reduction:
  \[ \bigoplus \bigotimes [f \ a \mid a \leftarrow y] \mid y \leftarrow gog \ x, p \ y \]

- Examples
  1. The even-sum maximum subsequence sum
     \[ \left\lceil \sum [a \mid a \leftarrow s] \mid s \leftarrow \text{sub}s \ x, \text{evensum} \ s \right\rceil \]
  2. The even-sum maximum initial-segment sum
     \[ \left\lceil \sum [a \mid a \leftarrow s] \mid s \leftarrow \text{inits} \ x, \text{evensum} \ s \right\rceil \]
  3. \(k\)-maximum maximum initial-segment sum
     \[ \left\lceil \left[ \sum [a \mid a \leftarrow s] \mid s \leftarrow \text{inits} \ x, \text{evensum} \ s \right] \right\rceil \]
  4. The number of subsequences matching a regular expression
     \[ \sum [1 \mid s \leftarrow \text{sub}s \ x, p_{RE} \ s] \]

The Answer: **Yes!**

The Current Results of This Work

Running Example: Even-sum Maximum Subsequence Sum

- Let’s build an efficient algorithm (homomorphism) for
  \[ \left\lceil \sum [f \ a \mid a \leftarrow s] \mid s \leftarrow \text{sub}s \ x, \text{evensum} \ s \right\rceil \]

- Remember the efficient algorithm for the simplest case
  1. We can add partial results freely to get the total result
     \[ \left\lceil \sum [f \ a \mid a \leftarrow s] \mid s \leftarrow \text{sub}s \ (y \oplus z) \right\rceil \]
     \[ = \sum [f \ a \uparrow 0 \mid a \leftarrow (y \oplus z)] \]
     \[ = \sum [f \ a \uparrow 0 \mid a \leftarrow y] + \sum [f \ a \uparrow 0 \mid a \leftarrow z] \]
  2. Is EMSS of \((y \oplus z)\) a just sum of EMSSs of y and z?
    - **No.**
Possible States of Partial Subsequences

- Each sequence has two possible states: even and odd
- States changes after summations
  \[ \text{o} + \text{o} = \text{o} \quad \text{o} + \text{o} = \text{o} \quad \text{o} + \text{o} = \text{o} \quad \text{o} + \text{o} = \text{o} \]
- Candidates of EMSS of \((y + z)\) are
  - A sum of EMSSs of \(y\) and \(z\), and
  - A sum of the odd-sum MSSs of \(y\) and \(z\)
- We need to use the following new merging operator
  \[ \left[ \begin{array}{c} \text{o} \\ \text{o} \end{array} \right] + \left[ \begin{array}{c} \text{o} \\ \text{o} \end{array} \right] = \left[ \begin{array}{c} \text{o} + \text{o} \uparrow \text{o} + \text{o} \\ \text{o} + \text{o} \uparrow \text{o} + \text{o} \end{array} \right] \]

The Base Case Computation

- How is the computation of the base case \(x = [a]\)?
  - Remember that we need both EMSS and OMSS
  \[
  f' a = \text{if even } a \text{ then } \left( f a \uparrow 0 \right) \text{ else } \left( f a \uparrow 0 \right)
  = \left( \text{if even } a \text{ then } \left( f a \uparrow 0 \right) \text{ else } \left( f a \uparrow 0 \right) \right) \uparrow 0
  = f \uparrow 0
  \]
  - We got the following new operator
  \[
  \left[ \begin{array}{c} \text{o} \\ \text{o} \end{array} \right] \uparrow \left[ \begin{array}{c} \text{o} \\ \text{o} \end{array} \right] = \left[ \begin{array}{c} \text{o} \uparrow \text{o} \\ \text{o} \uparrow \text{o} \end{array} \right]
  \]

Efficient Algorithm for Even-sum Maximum Subsequence Sum

- We have built the following algorithm for EMSS
  \[
  \left[ \sum [f a \mid a \leftarrow s] \mid s \leftarrow \text{subs } x, \text{ evensum } s \right] = \pi \left( \sum [f a \uparrow 0 \mid a \leftarrow x] \right)
  \]

\[
\left[ \begin{array}{c} \text{o} \\ \text{o} \end{array} \right] \uparrow \left[ \begin{array}{c} \text{o} \\ \text{o} \end{array} \right] = \left[ \begin{array}{c} \text{o} \uparrow \text{o} \\ \text{o} \uparrow \text{o} \end{array} \right], \quad \left[ \begin{array}{c} \text{o} \\ \text{o} \end{array} \right] \uparrow \left[ \begin{array}{c} \text{o} \\ \text{o} \end{array} \right] = \left[ \begin{array}{c} \text{o} \uparrow \text{o} \uparrow \text{o} \uparrow \text{o} \\ \text{o} \uparrow \text{o} \uparrow \text{o} \uparrow \text{o} \end{array} \right]
\]

made from the property of the predicate:
\[
\text{o} + \text{o} = \text{o} \quad \text{o} + \text{o} = \text{o} \quad \text{o} + \text{o} = \text{o} \quad \text{o} + \text{o} = \text{o}
\]
Efficient Algorithm for Even-sum Maximum Subsequence Sum

We have built the following algorithm for EMSS

$$\pi(\sum [f \ a \leftarrow s] \ s \leftarrow subs \ x, \ evensum \ s)$$

G.f. the computation of MSS

$$\sum [f \ a \leftarrow s] \ s \leftarrow subs \ x$$

Efficient Algorithm for Even-sum Maximum Subsequence Sum

We have built the following algorithm for EMSS

$$\pi(\sum [f \ a \leftarrow s] \ s \leftarrow subs \ x, \ evensum \ s)$$

$$= \pi(\sum [f \ a \leftarrow 0] \ a \leftarrow x)$$

$$= \pi(\sum [f \ a \leftarrow s] \ s \leftarrow subs \ x)$$

Actually, \((\alpha^{even,odd}, \uparrow, \uplus)\) is a semiring!
The filter has been embedded into the semiring!

$$\pi(\sum [f \ a \leftarrow s])$$

$$= \text{if evensum s then } \sum [f \ a \leftarrow s] \text{ else 0}$$

Embedding Filters into Semirings

**Theorem** Given a semiring \((\alpha, \oplus, \otimes)\), a FRH predicate \(p = \text{accept}_p \circ (\oplus_{\text{fr}}, f_g)\) (where \text{accept}_p :: C_p \rightarrow \text{Bool}), a list \(g\), and a function \(f\), the following equation holds.

$$\bigoplus \bigotimes [f \ a \leftarrow y] \ y \leftarrow g, p y = \pi(\bigoplus \bigotimes [f \ a \leftarrow y] \ y \leftarrow g)$$

Here, \((\alpha^{FRH}, \oplus, \otimes)\) is the lifted semiring of \((\alpha, \oplus, \otimes)\) with \(f\), the lifted function of \(f\) with \(p\), and \(\pi\) is the unilifer with \(p\).

Here, \((\oplus, f)\) \(x = \bigoplus [f \ a \leftarrow x]\) is a list homomorphism:

\(\oplus, f) (x \leftrightarrow y) = (\oplus, f) x \oplus (\oplus, f) y\)

\(\oplus, f) [a] = f a\)

FRH = finite range homomorphic

E.g., evensum = id \circ (\text{XNOR}, \text{even})
Intuition of Lifted Semirings

- A FRH predicate \( p = \text{accept} \circ (\oplus, f) \), a FRH GoG \( gog \) is give as

\[
gog x = [\text{clean} y \mid y \leftarrow \text{subs}' x, p y].
\]

Here, \( \text{clean} x = \text{def} [\text{if} m \text{ then } [a] \text{ else } [] \mid (a, m) \leftarrow x] \) is a cleaner to remove all marks and elements marked false.

\[
\text{subs}'[1.2.3] = [(1, T), (2, T), (3, T)], [(1, T), (2, T), (3, F)], \ldots
\]

For example, we can define \text{inits} with

\[
\text{accept} (i, s, n) = i; \quad f (a, m) = (m, m, \text{not } m) \quad (i_1, a_1, n_1) \oplus (i_2, a_2, n_2) = ((i_1 \land n_2) \lor (a_1 \land i_2), a_1 \land a_2, n_1 \land n_2).
\]

We can similarly define \text{tails} to generate all tail segments.

Question: Do Similar Problems Have Efficient Algorithms?

- Nested reduction:

\[
\bigoplus \bigotimes [f \ a \mid a \leftarrow y] \mid y \leftarrow \text{gog} x, p y
\]

- Examples

  - The even-sum maximum subsequence sum  \( \text{Done!} \)

  \[
  \sum [a \mid a \leftarrow s] \mid s \leftarrow \text{subs} x, \text{even sum } s
  \]

  - The even-sum maximum initial-segment sum  \( \text{Next target} \)

  \[
  \pi \left( \left( \sum \left[i d \ a \mid a \leftarrow s \right] \mid s \leftarrow \text{inits} x \right) \right)
  \]

  - The number of subsequences matching a regular expression

  \[
  \sum [1 \mid s \leftarrow \text{subs} x, p RE \ s]
  \]

GoGs by Predicates and Boolean Markings
(based on the idea of [Sasano et al. 00])

\[
\text{Def.} \quad \text{Given a FRH predicate } p = \text{accept} \circ (\oplus, f), \text{ a FRH GoG } gog \text{ is give as }
\]

\[
gog x = [\text{clean} y \mid y \leftarrow \text{subs'} x, p y].
\]
Optimization for FRH GoGs

Now, we can use the semiring construction

\[ \bigoplus \bigotimes [f \; a \; | \; a \leftarrow y] \; \mid \; y \leftarrow \text{gog} \; x, \; p \; y \]

= \{ \text{Semiring construction} \}

\[ \tilde{\pi}(\bigoplus \bigotimes [f \; a \; | \; a \leftarrow y] \; \mid \; y \leftarrow \text{gog} \; x) \]

= \{ \text{Definition of FRH GoGs} \}

\[ \tilde{\pi}(\bigoplus \bigotimes [f \; a \; | \; a \leftarrow y] \; \mid \; y \leftarrow \{ \begin{cases} \{x\} & \text{if } m \text{ then } \{a\} \text{ else } \{ (a, m) \leftarrow x \} \mid y \leftarrow \text{subs' } x, \; p' \; y \} \}

= \{ \text{Short-cut Fusion} \}

\[ \tilde{\pi}(\bigoplus \bigotimes \tilde{f} \; a \; | \; a \leftarrow y] \; \mid \; y \leftarrow \text{subs' } x, \; p' \; y) \]

= \{ \text{Semiring construction} \}

\[ \tilde{\pi}(\tilde{\pi}'(\bigoplus \bigotimes \tilde{f}' \; a \; | \; a \leftarrow y] \; \mid \; y \leftarrow \text{subs' } x)\}

= \{ \text{The simple optimization} \}

\[ \tilde{\pi}''(\bigoplus \bigotimes a \; | \; a \leftarrow x) \]

Question:
Do Similar Problems Have Efficient Algorithms?

Nested reduction:

\[ \bigoplus \bigotimes [f \; a \; | \; a \leftarrow y] \; \mid \; y \leftarrow \text{gog} \; x, \; p \; y \]

Examples

- The even-sum maximum subsequence sum \textbf{Done!}
  \[ \left\{ \sum \{ [a \; | \; a \leftarrow s] \; | \; s \leftarrow \text{subs } x, \; \text{evensum } s \} \right\} \]

- The even-sum maximum initial-segment sum \textbf{Done!}
  \[ \left\{ \sum \{ [a \; | \; a \leftarrow s] \; | \; s \leftarrow \text{inits } x, \; \text{evensum } s \} \right\} \]

- The number of subsequences matching a regular expression
  \[ \sum \{ [1 \; | \; s \leftarrow \text{subs } x, \; \text{pRE } s] \} \]

Finding Solutions as well as Values

The even-sum maximum initial-segment sum

\[ \left\{ \sum \{ [a \; | \; a \leftarrow s] \; | \; s \leftarrow \text{inits } x, \; \text{evensum } s \} \right\} \]

We can compute the initial-segment contributing to the maximum sum:

\[ \left\{ \sum \{ [(a, [a]) \; | \; a \leftarrow s] \; | \; s \leftarrow \text{inits } x, \; \text{evensum } s \} \right\} \]

where \((a, x) \; \uparrow'(b, y) = \text{if } a \geq b \text{ then } (a, x) \text{ else } (b, y), \)

\((a, x) \; \uparrow'(b, y) = (a + b, x + y) \)

\(((a, [a]), \uparrow', +') \text{ is a semiring} \)

Segments which have the same sum are considered equivalent.
Simple Querying (generate-and-test)

- We have a linear work algorithm for generate-and-test
  - Because \( ([\alpha], \psi, \chi_{++}) \) is a semiring
    \[
    \psi \chi_{++} \{ [[a]] | a \leftarrow s \} | s \leftarrow init s x, evensum s
    \]
    where \( u \chi_{\oplus} v = \{ a \oplus b | a \in u, b \in v \} \)
    \( \psi \) is the bag concatenation.
    \{ \text{and} \} \text{ are brackets for bags (multi-sets).}
- We need to freeze the operators for efficiency

Question:
Do Similar Problems Have Efficient Algorithms?

- Nested reduction:
  \[
  \bigoplus \bigotimes \{ f \ a | a \leftarrow y \} | y \leftarrow gog x, p y
  \]
- Examples
  - The even-sum maximum subsequence sum \( \text{Done!} \)
    \[
    \{ \sum \{ a | a \leftarrow s \} | s \leftarrow subs x, evensum s \}
    \]
  - The even-sum maximum initial-segment sum \( \text{Done!} \)
    \[
    \{ \sum \{ a | a \leftarrow s \} | s \leftarrow init s x, evensum s \}
    \]
  - \( k \)-maximum maximum initial-segment sum \( \text{Done!} \)
    \[
    \{ \sum k \{ [[a]] | a \leftarrow s \} | s \leftarrow init s x, evensum s \}
    \]
  - The number of subsequences matching a regular expression
    \( \sum \{ \prod \{ w | a \leftarrow s \} | s \leftarrow subs x, pRE s \} \) \( \text{Done!} \)

Summary of the Results

\[
\bigotimes \bigoplus \{ f \ a | a \leftarrow y \} | y \leftarrow gog x, p y
\]

- Optimizeable nested reductions
  - GoG = concatMap—composition of FRH GoGs
  - \( p = \text{FRH predicates and their and/or/not} \)
  - \( (\alpha, \oplus, \otimes) \) is a semiring

Linear cost list homomorphism can be run on KestTo, MapReduce, ITBB, OpenMP, MPI, ...
Related Work

- Maximum (Multi-) Marking Problem [Sasano et al. 00, 01, 05]
  Deriving efficient sequential algorithm for nested reductions
  \[ \sum [f \ a \ {\leftarrow} y] \ | \ y \ {\leftarrow} \ subs' x, p y \]
  [Sasano et al. 05] deals with accumulative weight sum
- Parallelization for the simplest case [Matsuzaki 07]
- Pre-order construction for max-sum problems [Morihata 09]
  Similar framework focusing on semirings of pre-orders and monotonic summations
  Generic formalization of generators

Conclusion and Future Work

- Automatic derivation of efficient algorithms for nested reductions with semirings, FRH GoGs and FRH predicates
  Embedding predicates (filters) into semirings
  Very clear optimization about all-marks generation
  Serious study about optimization of nested homomorphisms
- Future work
  Implementation of the derivation
  Combinator library, DSL library, ...
  Optimization of lifted operators
  FR foldr = FR homomorphism with a large number of states
- Relational (accumulative) predicates
  Correspond to accumulative weight function in MMP [Sasano et al. 05]
- Apply semiring construction to combinatorial problems on graphs
  \[ \bigoplus \{ [f \ a \ {\leftarrow} y] \ | \ y \ {\leftarrow} \ g, p y \} = \wedge \bigoplus \{ [f \ a \ {\leftarrow} y] \ | \ y \ {\leftarrow} \ g \} \]

Reference

- Kento Emoto:
  An Algebraic Approach to Efficient Parallel Algorithms for Nested Reductions
  Technical Report METR 2011-01, 31 pages, Department of Mathematical Engineering and Information Physics, University of Tokyo, 2011.
- Available from Web:
  http://www.ipl.t.u-tokyo.ac.jp/~emoto/#METR2011-01
  or http://www.keisu.t.u-tokyo.ac.jp/research/techrep/2011.html
Programmers can write and reason about compositional programs that communicate via intermediate data easily, but processors can execute monolithic programs that do not allocate memory more efficiently. Short-cut fusion (Gill 1996; Gill et al. 1993) is a technique to eliminate intermediate data shared between composed functions.

Traditionally, short-cut fusion does not improve the complexity of the transformed algorithm. The generated program is more efficient only by a constant factor compared with the program it is derived from. Identifying the type of the eliminated intermediate data as free algebraic structure allows to apply short-cut fusion to improve the complexity of algorithms. Every algebraic structure, like monoid or semiring, gives rise to a short-cut fusion law that can be proved using a free theorem (Reynolds 1983; Wadler 1989). Using an algebraic structure that satisfies a distributive law gives rise to asymptotic improvement of algorithms transformed by short-cut fusion.

The key idea is that on the different sides of the distributive law “a · (b + c) = a · b + a · c” the number of arithmetic operations are different. Semirings are an example for a distributive algebraic structure. The following slides describe short-cut fusion with the free semiring, multisets of lists.

References


*supported by a post-doc fellowship of the German Academic Exchange Service (DAAD)
Semiring Fusion

Sebastian Fischer

DAAD Research Fellow at NII, Tokyo

Fourth DIKU-IST Joint Workshop on Foundations of Software

Quiz

How many sublists\(^1\) has \([1 \ldots n]\)?

What is the sum of products over all sublists of \([2, -1, 3]\)?

\(^1\)some (not necessarily adjacent) elements in correct order

Preview

shortcut fusion

algebraic view on shortcut fusion

semirings as underlying structure

Linear algorithms to answer the posed questions can be obtained from seemingly exponential specifications.
Shortcut Fusion

Programmers can write easily
  • compositional programs
  • that communicate via intermediate data

Processors can execute efficiently
  • tight loops
  • that do not allocate memory

Simple Example

Without intermediate data:

\[
\text{factorial} :: \text{Int} \rightarrow \text{Int} \\
\text{factorial} \ n = \\
    \text{if } n < 1 \text{ then } 1 \\
    \text{else } n \ast \text{factorial} \ (n - 1)
\]

Compositional: \(\text{factorial} = \text{product} \circ \text{downFrom}\)

\[
\text{prod} :: \text{[Int]} \rightarrow \text{Int} \\
\text{prod} \ [\] = 1 \\
\text{prod} \ (n : ns) = n \ast \text{prod} \ ns
\]

\[
\text{genDownFrom} :: \text{Int} \rightarrow (\text{Int} \rightarrow \text{list} \rightarrow \text{list}) \rightarrow \text{list} \rightarrow \text{list}
\]

Abstracting from list constructors

\[
\text{prod} \ (\text{downFrom} \ n) = \text{foldr} \ (+) \ 1 \ (\text{build} \ (\text{genDownFrom} \ n))
\]

\[= \text{genDownFrom} \ n \ (+) \ 1\]

\[= \text{factorial} \ n \quad \text{-- monolithic version}\]
**Algebraic View**

Abstracting the list interface

```haskell
class IntList list where
  cons :: Int → list → list
  nil :: list
```

Homomorphisms / folds:

```haskell
intListHom :: IntList list ⇒ [Int] → list
intListHom [] = nil
intListHom (n : ns) = cons n (intListHom ns)
```

build with overloaded function

```haskell
instance IntList [Int] where
  cons = (:
  nil = []

buildIntList :: (∀ list. IntList list ⇒ list) → [Int]
buildIntList gen = gen
```

Factorial again

```haskell
downFromIntList :: IntList list ⇒ Int → list
downFromIntList n =
  if n < 1 then nil
  else cons n (downFromIntList (n - 1))

instance IntList Int where
  cons = (*)
  nil = 1
```
Free Theorem\textsuperscript{2} for \texttt{IntList} generator

The Free Theorem for \texttt{gen :: \forall list.\texttt{IntList} list \Rightarrow \texttt{Int} \rightarrow \texttt{list}}
\[
\forall t_1, t_2 \in \text{TYPES(\texttt{IntList})}, f :: t_1 \rightarrow t_2, f \text{ respects IntList}.
\forall x :: \texttt{Int}. f (\texttt{gen}.t_1 x) = \texttt{gen}.t_2 x
\]

\texttt{f respects IntList if}
\[
\forall x :: \texttt{Int}.
\forall y :: t_1, f (\texttt{cons}.t_1 x y) = \texttt{cons}.t_2 x (f y)
\]
\[
f \texttt{nil}.t_1 = \texttt{nil}.t_2
\]

\textsuperscript{2}http://www-ps.iai.uni-bonn.de/cgi-bin/free-theorems-webui.cgi

Shortcut Fusion, revisited

- \texttt{downFromIntList :: \texttt{IntList} list \Rightarrow \texttt{Int} \rightarrow \texttt{list}}
- \texttt{intListHom} respects \texttt{IntList} (is homomorphism)
- \texttt{prod = intListHom}
- \texttt{downFrom = buildIntList} \circ \texttt{downFromIntList}

\texttt{prod} (\texttt{downFrom} \texttt{n})
\[
= \texttt{intListHom} (\texttt{buildIntList} (\texttt{downFromIntList} \texttt{n}))
= \texttt{intListHom} (\texttt{downFromIntList} \texttt{n}) \quad \text{-- by definition}
= \texttt{downFromIntList} \texttt{n} \quad \text{-- by free theorem}
\]

Monoids

Alternative list interface:

\texttt{class Monoid m where}
\[
\texttt{one} :: m
\]
\[
(\otimes) :: m \rightarrow m \rightarrow m
\]

\textbf{Must satisfy laws:}

- \texttt{one} is unit of \texttt{\otimes}: \texttt{one} \otimes x = x = x \otimes \texttt{one}
- \texttt{\otimes} is associative: \texttt{x} \otimes (\texttt{y} \otimes \texttt{z}) = (\texttt{x} \otimes \texttt{y}) \otimes \texttt{z}

241
Monoids and Homomorphisms

instance Monoid [a] where
  one = []
  (⊗) = (+)

instance Monoid Int where
  one = 1
  (⊗) = (∗)

monoidHom :: Monoid m ⇒ (a → m) → [a] → m
monoidHom f [] = one
monoidHom f [x] = f x
monoidHom f (xs ⊕ ys) = monoidHom f xs ⊗ monoidHom f ys

Monoid Generator and Free Theorem

downFromM :: Monoid m ⇒ (Int → m) → Int → m
downFromM f n =
  if n < 1 then one
  else f n ⊗ downFromM f (n − 1)

Free Theorem:

hom ◦ gen f = gen (hom ◦ f)

Consequence:

factorial
  = prod ◦ downFrom
  = monoidHom id ◦ downFromM (λx → [x])
  = downFromM (λx → monoidHom id [x]) -- by free theorem
  = downFromM id -- by definition

Associativity

Interesting:

• more freedom for implementation of homomorphisms

• parallel execution by nesting in a balanced way

Boring:

• same number of multiplications, regardless of nesting

• fusion improves efficiency only by a constant factor
Distributivity

Changes number of operations:

\[ a \cdot (b + c) = a \cdot b + a \cdot c \]
\[ (a + b) \cdot c = a \cdot c + b \cdot c \]

Extreme example:

\[
(1 + x_1) \cdot \ldots \cdot (1 + x_n) = 1 + x_1 + \ldots + x_n
+ x_1 \cdot x_2 + \ldots + x_i \cdot x_k + \ldots + x_{n-1} \cdot x_n
\vdots
+ x_1 \cdot \ldots \cdot x_n
\]

\[ O(n) \text{ vs. } O(2^n) \text{ operations} \]

Semirings

Extension of monoids:

```haskell
class Monoid s ⇒ Semiring s where
  zero :: s
  (⊕) :: s → s → s
```

Laws:

- zero is unit of ⊕
- ⊕ is associative and commutative
- ⊗ distributes over ⊕
- zero cancels multiplication

```haskell
instance Semiring Int where zero = 0; (⊕) = (+)
```

Another Semiring

```haskell
type Bag a = -- abstract type of multisets
  instance Semiring (Bag [a]) where
    zero = []
    a ⊕ b = a ∪ b
  instance Monoid (Bag [a]) where
    one = [[]]
    a ⊗ b = {x + y | x ∈ a, y ∈ b}
  single :: a → Bag [a]
  single x = {[x]}
```

Example:

\[
\text{single 1} ⊕ \text{single 2} ⊗ \text{single 3}
= ([[1]] ∪ [[2]]) ⊗ [[3]]
= [[1], [2]] ⊗ [[3]]
= [[1, 3], [2, 3]]
\]
**Homomorphisms**

\[
\text{semiringHom} :: \text{Semiring } s \Rightarrow (a \rightarrow s) \rightarrow \text{Bag } [a] \rightarrow s
\]

\[
\text{semiringHom } f \{\} = \text{zero}
\]

\[
\text{semiringHom } f \{[\]\} = \text{one}
\]

\[
\text{semiringHom } f (\text{single } x) = f x
\]

\[
\text{semiringHom } f (a \oplus b) = \text{semiringHom } f a \oplus \text{semiringHom } f b
\]

\[
\text{semiringHom } f (a \otimes b) = \text{semiringHom } f a \otimes \text{semiringHom } f b
\]

**Sublists**

\[
\text{sublists} :: [a] \rightarrow \text{Bag } [a]
\]

\[
\text{sublists } [[]] = \text{one}
\]

\[
\text{sublists } (x : xs) = (\text{one} \oplus \text{single } x) \otimes \text{sublists } xs
\]

Example:

\[
\text{sublists } [2, -1, 3] = \{[[], [2]], [[], [-1]], [[], [3]]\}
\]

\[
\text{sublists } [1 .. n] = 2^n
\]

\[O(2^n)\] operations
Sum of Products

\[
\text{prodSum} :: \text{Bag } [\text{Int}] \rightarrow \text{Int} \\
\text{prodSum} = \text{semiringHom id}
\]

\[
\begin{align*}
\text{prodSum} \ (\text{sublists } [2, -1, 3]) &= \text{prodSum} \ \{ [], [3], [-1], [-1, 3], [2], [2, 3], [2, -1], [2, -1, 3] \} \\
&= 1 + 3 - 1 - 3 + 2 + 2 \times 3 - 2 \times 1 - 2 \times 1 \times 3 \\
&= 1 + 3 - 1 - 3 + 2 + 6 - 2 - 6 \\
&= 0
\end{align*}
\]

\(O(2^n)\) operations

Generalized Sublists

\[
\text{genSublists} :: \text{Semiring } s \Rightarrow (a \rightarrow s) \rightarrow [a] \rightarrow s \\
\text{genSublists } f \ [] &= \text{one} \\
\text{genSublists } f \ (x : xs) &= (\text{one } \oplus f \ x) \odot \text{genSublists } f \ xs
\]

\[
\text{sublists} = \text{genSublists } \text{single}
\]

Semiring Fusion

Free Theorem:

\[
\text{hom} \circ \text{gen } f = \text{gen } (\text{hom} \circ f)
\]

Consequence:

\[
\begin{align*}
\text{semiringHom } f \circ \text{gen single} &= \text{gen } (\lambda x \rightarrow \text{semiringHom } f \ (\text{single } x)) \quad \text{-- by free theorem} \\
&= \text{gen } f \quad \text{-- by definition}
\end{align*}
\]
Size, efficiently

\[(\text{size } \circ \text{ sublists}) [1, 2, 3] = (\text{semiringHom } (\lambda x \rightarrow 1) \circ \text{genSublists single}) [1, 2, 3] = \text{genSublists } (\lambda x \rightarrow 1) [1, 2, 3] = (1 + 1) * (1 + 1) * (1 + 1) = 2 * 2 * 2 = 8\]

\(O(n)\) operations

Sum of Products, efficiently

\[(\text{prodSum } \circ \text{ sublists}) [2, -1, 3] = (\text{semiringHom id } \circ \text{genSublists single}) [2, -1, 3] = \text{genSublists id} [2, -1, 3] = (1 + 2) * (1 - 1) * (1 + 3) = 3 * 0 * 4 = 0\]

\(O(n)\) operations

Review

shortcut fusion can be viewed through algebraic glasses

eliminated intermediate data is free algebraic structure

distributivity gives rise to asymptotic improvement
Partial Evaluation of Janus

Torben Ægidius Mogensen
DIKU
torbenm@diku.dk
February 15, 2011

Abstract

A reversible programming language is a programming language in which you can only write reversible programs, i.e., programs that can be run both forwards (computing outputs from inputs) and backwards (computing inputs from outputs). It is interesting to study reversible programs and languages because computations on reversible computers (computers that only allow reversible programs) in theory can be done using less energy than computations on traditional irreversible computers. Janus is a reversible, structured imperative programming language.

We present a partial evaluator for the full Janus language with the exception of procedure calls. The partial evaluator converts Janus programs into reversible flowcharts, specialises these using polyvariant specialisation and converts the result back to structured form. Reversibility adds some complications, which we address in the paper. We demonstrate the results by some small examples.

We believe this to be the first partial evaluator for a deterministic reversible programming language.

This paper was first presented at the DIKU-IST 2011 workshop in Tokyo and later presented in a slightly different form at PEPM’2011 in Austin, Texas.

1 Introduction

Reversible computation [14, 19, 3, 4, 9] can theoretically be done using less energy than irreversible computation, as erasure of information necessarily dissipates energy in the form of thermodynamic entropy [14]. Most studies use low-level computational models such as reversible Turing machines [18, 3], but some studies use structured reversible programming languages[16, 1, 24, 22, 23].

Partial evaluation [13, 11] is a technique for generating specialised programs by fixing the value of some of the inputs to more general programs. The intent is that the specialised programs are more efficient than the originals, and this has often been observed in practise. Specialised programs perform fewer computations (and, hence, use less energy), so they can be of interest to further reduce energy consumption.

The partial evaluator presented in this paper handles all of the Janus language except procedure calls, which we address in a follow-up paper.
2 The reversible language Janus

Janus is a structured reversible programming language originally designed for a class at Caltech [16]. A Janus program starts with a declaration of variables divided into inputs, outputs and other variables. Variables are either integer variables or arrays of integers. The size of an array is either a constant number or given by a previously declared input variable. The main part of a Janus program is a list of parameter-less procedure declarations and a sequence of reversible statements that can use conditionals, loops and procedure calls. A special feature is that procedures can be run backwards by calling them with the keyword \texttt{uncall} instead of \texttt{call}. A grammar for Janus is shown in figure 1 and figure 2 shows a few examples of Janus programs:

(a) Fibonacci. This Janus program takes a number \(n\) and returns both the \(n\)th and the \((n+1)\)th Fibonacci numbers.

(b) Multiplication. This program takes two odd numbers \(a\) and \(b\) and returns both their product and \(b\) (unchanged) as outputs. Running this in reverse divides the product by \(b\).

(c) Postfix interpreter. This program reads a postfix expression (represented as an array of numbers) and an array of input values and then outputs the expression and its result. Outputting the expression with the result is required for reversibility. Evaluation uses two stacks: An evaluation stack \texttt{stack} and a stack \texttt{garbage} that is used to ensure reversibility. Uncalling \texttt{calc} undoes the stack operations, so the stacks are, again, empty.

2.1 Informal semantics of Janus

We will only describe Janus informally and refer to [24] for a formal semantics. Variables and array elements that are not inputs are initialised to 0 and variables and array elements that are not outputs are verified to be 0 when the program ends. A variable or array can be both input and output. Statements can take the following forms:

Update. The left-hand side of an update is either an integer variable or an element of an array. The update can either add or subtract the value of the right-hand side to this. The right-hand side can be any expression that does not contain the variable or array used on the left-hand side and if the left-hand side is an array element, the array can not be used in the expression specifying the index into the array. For example, the update \(a[a[i]] += 1\) is not legal. These restrictions ensures that the update can be reversed. Expressions can use the operators \(+\), \(-\) and \(/2\).

Swap. A statement of the form \(lv_1 \leftrightarrow lv_2\) swaps the contents of \(lv_1\) and \(lv_2\), which can be integer variables or array elements. It is possible to swap two elements of the same array, but the index expression of an array can contain none of the arrays or integer variables used in the swap statement. For example, while \(a[i] \leftrightarrow a[j]\) is legal, \(a[i] \leftrightarrow i\) is not. Again, the restriction is required for reversibility.

Sequence. Statements separated by ; are executed in sequence.

Skip. No effect.
Figure 1: Syntax of Janus

Conditional. A statement of the form \texttt{if} \; c_1 \; \texttt{then} \; s_1 \; \texttt{else} \; s_2 \; \texttt{fi} \; c_2 \) is executed by first evaluating \( c_1 \). If this is true, \( s_1 \) is executed and it is verified that \( c_2 \) is true. If \( c_1 \) is false, \( s_2 \) is executed and it is verified that \( c_2 \) is false. If the exit-assertion \( c_2 \) does not have the expected value, the program stops with an error message. A condition can compare numbers for equality (\( \texttt{==} \)), inequality (\( < \)) and test if a number is odd. Conditions can be combined by conjunction, disjunction and negation. The construction can be illustrated by the flowchart in figure 3(a), where a two-entry assertion is shown as a circle with two entry arrows marked with the expected truth value.

Loop. A statement of the form \texttt{from} \; c_1 \; \texttt{do} \; s_1 \; \texttt{loop} \; s_2 \; \texttt{until} \; c_2 \) is executed by first evaluating the assertion \( c_1 \). If this is false, the program stops with an error message, otherwise \( s_1 \) is executed and the \( c_2 \) is evaluated. If this is true, the loop terminates. Otherwise, \( s_2 \) is executed and \( c_1 \) is evaluated (again). If \( c_1 \) is true, the program stops with an error message, otherwise the loop repeats from \( s_1 \). The construction can be illustrated with the flowchart in figure 3(b).

Procedure call. A procedure call is either of the form \texttt{call} \; p \; or \texttt{uncall} \; p \), where \( p \) is a procedure name. \texttt{call} \; p \) executes the body of \( p \) and returns to the place of the call.
n -> a b;
a += 0; b += 1;
from a==0 do
  n -= 1; a <-> b; b += a
loop skip
until n==0

(a) Fibonacci

a b -> b prod with t v;
from 0==prod do
  if odd(a) then
    prod += b; t += a/2;
    a -= t+1; t -= a
  else
    t += a/2; a -= t; t -= a
  fi !(prod<b)
loop
v += b; b += v; v -= b/2
until a==0;
from prod<b+b do
  v += b/2; b -= v; v -= b
loop skip
until odd(b)

(b) Multiplication

sz exp[sz] i ins[i]
-> sz exp[sz] i ins[i] result
with pc sp stack[sz] gp garbage[sz];
call calc;
result += stack[0];
uncall calc

procedure calc
do
  if exp[pc]==0 then
    stack[sp] += exp[pc+1];
    sp += 1
  else
    if exp[pc]==1 then
      stack[sp] += ins[exp[pc+1]]; sp += 1
    else // exp[pc]==2
      sp -= 1; garbage[gp] <=> stack[sp];
      if exp[pc+1]==0 then
        stack[sp-1] += garbage[gp]
      else
        stack[sp-1] -= garbage[gp]
      fi exp[pc+1]==0;
    gp += 1
  fi exp[pc]==1
  pc += 2
loop
until pc==sz

(c) Postfix interpreter

Figure 2: Janus programs

Figure 3: Flowchart diagrams for conditional and loop
uncall $p$ executes the body of $p$ in reverse and then returns to the place of the call. The sequence call $p$; uncall $p$ has no net effect, as uncall $p$ will undo all the state changes done by call $p$.

Note that a Janus program can either terminate normally, fail or be nonterminating. We regard all failures as equivalent, i.e., we do not differentiate between failing an assertion in a loop or conditional or failing due to a non-zero non-output variable.

2.2 Reverse execution

Statements can be executed both forwards and backwards (when a procedure is called with uncall). Backwards execution can be realised by syntactically reversing the statement and then executing it forwards. A program can be reversed by swapping input and output variables and reversing the body statement. The function $R$ below shows how statements can be reversed.

$$
\begin{align*}
R(lv += e) &= lv -= e \\
R(lv -= e) &= lv += e \\
R(lv_1 <=> lv_2) &= lv_1 <=> lv_2 \\
R(s_1; s_2) &= R(s_2); R(s_1) \\
R(\text{call } p) &= \text{uncall } p \\
R(\text{uncall } p) &= \text{call } p \\
R(\text{skip}) &= \text{skip} \\
R(\text{if } c_1 \text{ then } s_1 \text{ else } s_2 \text{ fi } c_2) &= \text{if } c_2 \text{ then } R(s_1) \text{ else } R(s_2) \text{ fi } c_1 \\
R(\text{from } c_1 \text{ do } s_1 \text{ loop } s_2 \text{ until } c_2) &= \text{from } c_2 \text{ do } R(s_1) \text{ loop } R(s_2) \text{ until } c_1
\end{align*}
$$

3 Partial evaluation

Partial evaluation has been studied for many languages. Good overviews can be found in [13] and [11].

Briefly stated, partial evaluation is about producing residual programs. If a program $p$ takes two inputs and a $r$ takes one input, $r$ is a residual program of $p$ with respect to a value $s$ if, for any value $d$, running $p$ with $s$ and $d$ as inputs yields the same result as running $r$ with $d$ as input. I.e., either both terminate and produce the same result, both fail with an error or both are nonterminating. A partial evaluator is a program that given (representations of) a program $p$ and a value $s$ can produce (a representation of) a program $r$ that is residual to $p$ with respect to $s$. Often, the definition of a partial evaluator is relaxed, so it is allowed to be nonterminating for some $p$ and $s$. In this relaxed definition, the always nonterminating program is a partial evaluator, just not a very useful one.

These definitions generalise to cases where $p$ has more inputs.

We will focus on offline partial evaluation: Inputs are classified in advance as known (static) or unknown (dynamic), and it is determined which parts of the program depend only on the static inputs and which parts may depend on the remaining (dynamic) inputs. When values for the static inputs are given, this classification is used to determine which parts of the program can be executed during specialisation and which parts must be included in specialised form in the residual program. Thus, the specialisation process is divided into the following steps:

1. Classify input variables as static (to be specialised away) or dynamic (to remain in the residual program).
2. Given the input classification, automatically classify all parts of the program as static or dynamic. This is called a binding-time analysis. Input variables that in step 1 were classified as static may be reclassified as dynamic. The binding-time analysis can ensure that all residual programs obey certain properties. We will use it to ensure that residual programs are reversible.

3. Given the full program classification and the values of the inputs classified as static, produce the specialised (residual) program by executing the static parts and copying instances of the dynamic parts into the residual program. The dynamic parts of the program may contain static values as constants, so the residual program can contain several copies of the same dynamic program part with different static values as constants. This phase is called specialisation.

The residual program can now be run with the remaining (dynamic) input values and will produce the same result as running the original program with all inputs. You can run the residual program repeatedly with different dynamic input values.

As an example of offline specialisation, consider the multiplication program shown in figure 2(b). We might want to specialise the program with the value 11 for a to get a one-input program that takes b and returns b and the product of 11 and b.

In this example, all outputs depend on the dynamic input and are, hence, outputs of the residual program. But in other programs there can be outputs that only depend on static inputs. If we follow the usual definition of a residual program, the residual program must return all outputs of the original program, including outputs that don’t depend on the dynamic inputs and are, hence, the same every time. We will relax this requirement, so the partial evaluator will return both a residual program and the values of the outputs that depend only on static inputs, i.e., the static outputs. The reason for this relaxation is that reversibility often requires a Janus program to return parts of its input along with the “interesting” output. For example, an interpreter written in Janus usually returns both the interpreted program and the result of running it. If we specialise the interpreter to a program, we don’t want the residual program to return this program as part of its output. Hence, we define the following correctness criterion for offline partial evaluation for Janus:

Given a a program p and an initial classification of inputs as static or dynamic, the binding-time analysis must produce an annotated program where inputs and outputs are classified as static or dynamic. Some variables that were initially classified as static may now be classified as dynamic.

When, given the annotated program and values s of the static inputs, specialisation terminates with static output s’ and a residual program r, the following must hold:

- If running p with inputs s and d terminates with outputs o, the part of o that was classified as static must have the value s’ and if the part of the output that was classified as dynamic has the value d’, then running r with d as input must terminate and return d’ as output.

- If running p with inputs s and d stops with a failed assertion or does not terminate, running r with d as input must do the same.

These requirements can easily be fulfilled either by the binding-time analysis classifying all inputs and outputs as dynamic and let r = p or by making the specialiser not produce any output. While we characterise such behaviours as correct, they are not desirable. But they
are not always possible to avoid: Consider a program with one input and one output. It is
undecidable if the program will terminate without failure, so if we classify the output as static
we risk nontermination or failure during specialisation. So to ensure termination, we must
reclassify the output as dynamic, which may unnecessarily postpone computations until the
residual program is executed. Analyses can determine if specialisation of a given program is
guaranteed to terminate [10, 6, 12], but since this is undecidable, such analyses must necessarily
be imprecise. We will not address this issue further in this paper but simply allow specialisation
to sometimes not terminate.

4 Polyvariant partial evaluation

The standard approach to partial evaluation of imperative languages is polyvariant partial
evaluation [5, 13, 11]. Polyvariant partial evaluation allows the same portion of the original
program to be specialised to multiple different static states. This can completely change the
structure of the program, so unless severe restrictions are imposed, it works best with programs
that use unstructured control, i.e., programs that consist of basic blocks that each start with
a label and end with a (possibly conditional) jump.

In polyvariant specialisation of basic blocks, the label of a basic block and the values of the
static variables (the static state) are combined to make a new residual label. The statements
in the basic block are then specialised with respect to this static state and a new static state
is obtained. The jump at the end of the basic block is specialised in the following way:

- An unconditional jump to \( l \) is made into a residual jump to a residual label made by
  combining \( l \) with the static state.
- A jump with a static condition is made into a residual unconditional jump to a residual
  label made by combining the selected label with the static state.
- A jump with a dynamic condition is made into a residual conditional jump by specialising
  the condition to the static state and making two residual labels by combining the original
  labels with the static state.

If there are not already specialised basic blocks for the residual labels constructed above, these
are now produced. When there are specialised basic blocks for all residual labels, the residual
program is complete. It is possible that this process will not terminate.

4.1 Translation into flowchart form

A reversible flowchart language similar to Janus is described in [22]. We will convert the body
of a Janus program and all the procedure bodies into lists of basic blocks. Each basic block
consists of three parts: An entry point, a body and a jump. An entry point can be one of the
following:

- \texttt{start}, that indicates the block where execution starts.
- A named label.
- A two-entry assertion consisting of a condition \( c \) and two named labels \( l_1 \) and \( l_2 \). This
  is written as \texttt{if } \( c \) \texttt{ from } \( l_1 \) \texttt{ l_2}. The condition \( c \) must be true if the basic block is entered
  by a jump to \( l_1 \) and false if the basic block is entered by a jump to \( l_2 \).
No label nor \texttt{start} can occur more than once in the entry points of all the basic blocks. The body of a basic block is either empty or any statement that does not contain structured control statements (conditionals and loops). The jump can be:

- \texttt{return}, that indicates the end of the program or procedure.
- An unconditional jump \texttt{goto} \texttt{l}.
- A conditional jump consisting of a condition \texttt{c} and two named labels \texttt{l}_1 and \texttt{l}_2. This is written as \texttt{if} \texttt{c goto} \texttt{l}_1 \texttt{l}_2. If \texttt{c} is true, the jump goes to \texttt{l}_1, otherwise to \texttt{l}_2.

No label nor \texttt{return} can occur more than once in the jumps of all the basic blocks. A basic block \texttt{e}: \texttt{s}; \texttt{j}, where \texttt{e} is an entry point, \texttt{s} a statement and \texttt{j} a jump is reversed into \texttt{R}((\texttt{j})): \texttt{R}((\texttt{s})): \texttt{R}((\texttt{e}))

A structured program is translated by first making the body statements of the program and procedures into single basic blocks by adding the entry point \texttt{start} and the jump \texttt{return}. These basic blocks may contain structured statements, so we translate them using the function \texttt{T} that translates a basic block that may contain structured statements into a set of basic blocks that do not:

\[
\begin{align*}
\text{T}(e: s; j) & = \{ e: s; j \} \\
& \quad \text{if } s \text{ does not contain structured statements} \\
\text{T}(e: s_1; s_2; j) & = \text{T}(e: s_1; \text{goto } l) \cup \text{T}(l: s_2 j) \\
& \quad \text{where } l \text{ is a new label} \\
\text{T}(e: \text{if } c_1 \text{ then } s_1 \text{ else } s_2 \text{ fi } c_2; j) & = \\
& \quad \{ e: \text{if } c_1 \text{ goto } l_1 \text{ } l_2 \} \\
& \quad \cup \text{T}(l_1: s_1; \text{goto } l_3) \cup \text{T}(l_2: s_2; \text{goto } l_4) \\
& \quad \cup \{ \text{if } c_2 \text{ from } l_3 \text{ } l_4; j \} \\
& \quad \text{where } l_1, l_2, l_3 \text{ and } l_4 \text{ are new labels} \\
\text{T}(e: \text{from } c_1 \text{ do } s_1 \text{ loop } s_2 \text{ until } c_2; j) & = \\
& \quad \{ e: \text{goto } l_1 \} \\
& \quad \cup \text{T}(\text{if } c_1 \text{ from } l_1 \text{ } l_2; s_1; \text{ if } c_2 \text{ goto } l_3 \text{ } l_4) \\
& \quad \cup \text{T}(l_4: s_2; \text{goto } l_2) \cup \{ l_3; j \} \\
& \quad \text{where } l_1, l_2, l_3 \text{ and } l_4 \text{ are new labels}
\end{align*}
\]

After the translation, there can be trivial basic blocks of the form (\texttt{l}_1 : \texttt{goto} \texttt{l}_2). We can eliminate such a block by making the jump to \texttt{l}_1 jump to \texttt{l}_2 instead. The program in figure 2(b) is translated into the flowchart program in figure 4(a).

\subsection*{4.2 Binding-time analysis}

We will, in this paper, not handle procedure calls, so we assume that the body of a basic block is a sequence of updates and swaps. For simplicity, we use one global binding time for each variable, so binding time analysis is fairly straightforward:
1. A statement, expression or condition that contains a dynamic variable is dynamic.

2. If an update statement is dynamic, then the variable or array element on the left-hand side is dynamic.

3. If a swap statement is dynamic, the variables or array elements on both sides are dynamic.

4. If one element of an array is dynamic, all elements of the array are dynamic.

5. An array indexed by a dynamic index expression is dynamic.

6. An if-goto or if-from with dynamic condition is dynamic.

7. A label used in a dynamic if-goto or if-from is dynamic.

8. An if-from with a dynamic label is dynamic.

9. An unconditional jump to a dynamic label is dynamic.

10. start and return are dynamic.

11. Static subexpressions of dynamic expressions or conditions are enclosed in “lift” operators that indicate that the static values will be inserted as constants during specialisation.

Note that there are three cases for arrays: A fully static array has static elements and is always indexed using static index expressions. A dynamic array has dynamic element values and is always indexed by dynamic index expressions (if not, a lift operator is used to make it so). But we may also have arrays that are statically indexed but contains dynamic element values. We explain specialisation of these in section 4.5.
We start binding-time analysis from an initial classification of the input variables as static or dynamic and everything else as static. We then iterate applying the rules above until no changes occur.

We will later need to add extra rules to ensure reversibility of residual programs, but we need to describe the specialisation process first to identify the issues.

The multiplication program shown in figure 4(a) with \( a \) classified as static and \( b \) as dynamic results in the binding-time-annotated program shown in figure 4(b). A \( \hat{\cdot} \) indicates a dynamic declaration or operation and \( \neq \) is the lift operator.

### 4.3 Specialisation of flowchart programs

As mentioned in section 4, the basic idea is to create specialised basic blocks by combining labels with static state and specialising the statements of the basic block according to the static state (and updating the static state when static variables are changed). Additionally, static jumps can be unfolded. We use the following rules for specialisation:

- Static statements are executed to update the static state.
- Dynamic statements are made into residual statements by evaluating static subexpressions and inserting their values as constants in place of the expressions.
- \( \text{start} \) is specialised to \( \text{return} \).
- An unconditional dynamic label is specialised by combining it with the static state to construct a new residual label. This is done by hashing the static state to a number and adding this number as a suffix to the label.
- A dynamic \( \text{if-from} \) is specialised into a residual \( \text{if-from} \) consisting of a residual condition and two residual labels constructed like above.
- Static labels and assertions are targets of static jumps, so we describe their treatment there.
- \( \text{return} \) is specialised to \( \text{return} \). It is verified that all static variables that are not output variables have the value zero. If not, an error message is issued.
- An unconditional dynamic jump is specialised by combining its label with the static state to construct a new residual label, as described above for entry points. The specialised label is used to make a residual unconditional jump. If there is not already a specialised basic block for the specialised label, one is made.
- A dynamic \( \text{if-goto} \) is specialised into a residual \( \text{if-goto} \) consisting of a residual condition and two residual labels constructed like above. If there are not already specialised basic blocks for the specialised labels, these are made.
- An static unconditional jump is specialised by finding the basic block that has this label in its entry point. If the target basic block has an unconditional label as entry, the jump is unfolded by specialising the body of the target basic block and adding it to the body of the specialised basic block that contains the static jump and then specialising the jump of the target basic block. If the target basic block has a two-way assertion as entry, this will be static (by rules 8 and 9 of the binding-time analysis), so its condition will be evaluated and checked. If the assertion fails, an error is reported. Otherwise, the jump is unfolded in the same way a jump to an unconditional label is unfolded.
A static if-goto is specialised by first evaluating the condition and selecting the label that corresponds to the result. It is then unfolded like an unconditional static or dynamic jump to this label, depending on whether the label is static or dynamic.

Specialisation starts by reading the values of the static input variables and setting the static state accordingly. Then the block with the start entry point is specialised with this state. This may trigger specialisation of more basic blocks with different static states. If this eventually terminates, there will be residual basic blocks for all residual jumps.

4.4 Making the residual program reversible

It is not hard to see that residual statements are reversible, but it is not clear that jumps and entry points are reversible. We will look at the requirements from section 4.1 in turn:

1. There must be exactly one entry point of the form start.
   There can be no jumps to start, so only one residual basic block can have the start entry point. So this property is preserved.

2. There must be exactly one jump of the form return.
   If the basic block that contains the return jump is specialised to two or more different static states, creating two or more residual basic blocks, there will be two or more return jumps in the residual program. So we need to remedy this.

3. Each named label must occur in exactly one entry point.
   When we make a residual jump to a specialised label, we check if a specialised basic block for this label already exists, so we will not produce multiple basic blocks with the same label. Also, if no specialised basic block exists for a residual jump, we will make one. Hence, each residual label will occur in exactly one entry point.

4. Each named label must occur in exactly one jump.
   This requirement forbids two situations: **No jumps to a label:** This may, actually happen: When we specialise a dynamic two-way assertion, we produce two residual labels even though we have seen only a residual jump to one of these. We may eventually see a jump to the other label, but there is no guarantee of this. So we may end up with a two-way assertion that has a jump to only one of its labels. **Two jumps to the same label:** This might occur if a basic block is specialised to two different static states but the updates to static variables make the static states at the end of these basic blocks identical. But since all static updates and swaps are reversible and a basic block is just a sequence of updates and swaps, this can not happen: Identical static end-states imply identical static start states.

Hence, we have two problems to fix: There may be several return jumps, and there may be a two-way assertion that has a jump to only one of its labels.

Multiple return jumps can occur only if the basic block containing the original return jump is specialised to several different static states. Since a basic block is reversible, this implies that there are several possible static states at the return jump itself, i.e., at the end of the program execution. So if we can ensure that there is only one possible static state at the end of program execution, we can avoid multiple return jumps.
All variables and array elements that are not part of the program output must, according to the Janus semantics, be 0 at the end of program execution. So for these, there is only one possible state at the end of execution. Output variables and arrays can, however, potentially have several possible values at the end program execution. If a static output variable or array can have several possible values, we get multiple specialised return jumps.

We avoid this by classifying all output variables that are modified anywhere in the program as dynamic, so no static output variables are ever updated. Static output variables will, hence, have the same value throughout execution.

It is common in partial evaluation to classify all outputs as dynamic, so even severe restrictions on static outputs is a relaxation compared to the usual case.

The issue of having a two-way entry with a jump to only one of its labels is not so easy to solve. The obvious solution would be to reduce the two-way assertion to an unconditional label, hence eliminating the label to which there is no jump. However, this will also eliminate the assertion, which may be required to preserve semantics (otherwise we might replace a failing execution by successful termination or nontermination). Another solution is to add a jump to the label that has none. This can be done in the following way: A residual basic block of the form if \( c \) from \( l_1 \) \( l_2 \): \( s \); \( j \) where there is a jump only to \( l_1 \) is replaced by the two basic blocks \( l_1 \): assert \( c \); \( s \); \( j \) and if \( c \) from \( l_3 \) \( l_2 \): \( s \); \( j \) where \( l_3 \) is a new label. The case where there is a jump only to \( l_2 \) is handled in a symmetric way.

Introducing extra jumps may make residual programs slower than the original programs, so to avoid this we extend the Janus language with statements of the form assert \( c \) (with the obvious semantics). If there is a jump only to \( l_1 \), we replace the basic block if \( c \) from \( l_1 \) \( l_2 \): \( s \); \( j \) by the basic block \( l_1 \): assert \( c \); \( s \); \( j \). If there is a jump only to \( l_2 \), we replace if \( c \) from \( l_1 \) \( l_2 \): \( s \); \( j \) with \( l_2 \): assert !\( c \); \( s \); \( j \).

The statement assert \( c \) reverses to itself and it is simple to specialise: It is classified as static if the condition is static, and a dynamic assert it is made into a residual assert by replacing the static subexpressions of \( c \) by constants.

We can eliminate unconditional jumps to unconditional labels by unfolding the jumps: The basic blocks \( e \): \( s_1 \); goto \( l \) and \( l \): \( s_2 \); \( j \) are combined to the single basic block \( e \): \( s_1 \); \( s_2 \); \( j \).

The program in figure 4(b) can be specialised to \( a=11 \) to yield the residual program shown in figure 5. Note that some two-way assertions have been converted to one-way assertion statements and unconditional jumps to unconditional labels have been eliminated.

### 4.5 Partially static arrays

We specialise a array \( a \) of size \( n \) with dynamic elements and static indices into \( n \) integer variables named \( a_0 \ldots a_m \) where \( m = n-1 \). The l-value \( a[e] \) is specialised by evaluating the static expression \( e \) to the value \( i \) and returning the residual l-value \( a_i \).

This technique is an instance of partially static data structures [17] and is well known from, e.g., C-mix as described in section 11.4.1 of [13]. It is useful for, among other things, specialising interpreters where a single array is used to hold the values of individual variables in the interpreted program. By splitting the array into scalar variables, the variables of the interpreted program become individual variables in the residual program obtained by specialising the interpreter to the interpreted program. For example, the arrays ins[i], stack[sz] and garbage[sz] in the postfix interpreter in figure 2(c) will be partially static.

12

258
b -> b prod with v 

start:
assert 0==prod; prod += b;
assert !(prod<b); v += b; b += v; v -= b/2;
assert !(0==prod); prod += b;
assert !(prod<b); v += b; b += v; v -= b/2;
assert !(0==prod);
assert prod<b; v += b; b += v; v -= b/2;
assert !(0==prod); prod += b;
assert !(prod<b)
goto f_11_92636

if prod<b+b from f_11_92636 a_11_92636:
v += b/2; b -= v; v -= b
if odd(b) goto u_11_92636 a_11_92636
u_11_92636:
return

Figure 5: Specialised multiplication program

5 Recovering structured control

The residual program shown in figure 5 is not a Janus program, as it uses unstructured control where Janus uses structured control statements. In [22] it is shown that any reversible flowchart can be translated into a program that uses only the reversible control structures shown in section 2. The translation works by first numbering all labels from 1 to n−1. A flowchart program

\[
\text{in} \rightarrow \text{outs with others; blocks}
\]

is translated into the structured program

\[
\text{in} \rightarrow \text{outs with others control;}
\text{from control==0 do } S(\text{blocks})
\text{loop skip until control==n; control -= n}
\]

where \( S \) takes a set of basic blocks and returns a statement:
As an example, the flowchart program in figure 6(a) is translated into the structured program in figure 6(b). This structure is, however, not natural and the addition of the extra control variable and the branching on this adds overhead. The flowchart program shown in figure 6(a) has a much simpler and more efficient structured equivalent shown in figure 6(c).

Ideally, we would like to have a translation that can find a structured program such that the sequences of variable updates and tests made by the structured program is the same as the sequence made by the flowchart program when both are executed with the same inputs. Intuitively, this means that no overhead is introduced by structuring the program.

There has (in the context of decompilation) been some work on recovering structured control from flowcharts [2, 21, 7, 8], but this has been done in a non-reversible setting. To our
knowledge, there is no similar work on recovering reversible control.

It has been shown [2] that general control flow can not always be translated into structured control without adding extra variable updates, but again, this result is for general, irreversible control. Since reversible flowcharts are quite restricted compared to general flowcharts, it is not obvious that the result carries over: Unrestricted flowcharts that can not be structured might not be realisable as reversible flowcharts. We will, however, below show a similar result for reversible programs.

We first define evaluation equivalence of flowchart programs.

**Definition 1** Two reversible flowchart programs are evaluation equivalent if they both execute the same sequence of tests and state modifiers when run on the same inputs. We only consider terminating executions, so the sequences are finite. A state modifier is an update or swap. A test is a condition in an assert statement, a conditional jump or a two-way entry point. If a condition \( c \) evaluates to false, it is shown as \( \neg c \) in the sequence. We consider \( c \) equivalent to \( \neg c \) and \( \neg c \) equivalent to \( c \), so it is possible to swap the two branches of a conditional jump.

A structured program is deemed to be evaluation equivalent to the flowchart program obtained by the translation shown in section 4.1 and, by transitivity, to all flowchart programs evaluation equivalent to this.

The proof in [2] that not all control flow can be made structured shows that a specific unstructured control-flow graph has no structured evaluation equivalent program (using a somewhat different notion of evaluation equivalence).

Consider the reversible flowchart in figure 7. The true exits/entries of conditional jumps and entry-points are to the left. There are three possible paths through this flowchart:

1: \( c_1, s_1, c_3, s_5, c_4 \)
2: \( c_1, s_2, c_2, s_3, c_3, s_5, c_4 \)
3: \( c_1, s_2, c_4, s_4, \neg c_4 \)

Let us see which structured programs can realise the above sequences.
Since all sequences start with $c_1$ or $\overline{c_1}$, $c_1$ must be the initial condition of an if-then-else-fi construct. An assert statement or the entry condition of a loop might have both outcomes, but would terminate execution after one of these. An if-then-else-fi construct must have a closing condition (assertion). The only condition (apart from $c_1$) that occurs in all the above sequences is $c_4$, so this must be it. So, the structured program must be of the form

$$\text{if } c_1 \text{ then } T \text{ else } E \text{ fi } c_4,$$

though with the possibility that one or both of $c_1$ and $c_4$ is negated. We can without loss of generality assume that $c_1$ is not negated (we could swap the branches if it was), so $E$ must be able to realise the rest of sequence 1. It ends in $c_4$, so the exit assertion must be $c_4$ (without negation). Sequence 2 and 3 start with $c_1$, so they both go to the false branch. They, however, end with different values for the $c_4$ condition, which contradicts the assumption that they are in the same branch of the conditional.

So if we can find actual conditions and statements such that all three sequences can be realised, we have an example of a flowchart that has no structured evaluation equivalent using the control structures of Janus. If we use the following instances of the tests and conditions:

$$
\begin{align*}
c_1 &= a = 0 & s_1 &= a \leftarrow 1 \\
c_2 &= a = 0 & s_2 &= a \leftarrow 1 \\
c_3 &= a = 1 & s_3 &= a \leftarrow 2 \\
c_4 &= a < 2 & s_4 &= a \leftarrow 2 & s_5 &= a \leftarrow 1
\end{align*}
$$

then sequence 1 is followed when $a$ is 1 initially, sequence 2 is followed when $a$ is 2 initially and sequence 3 is followed when $a$ is 3 initially. Hence, we have a flowchart that is not evaluation equivalent to any structured program.

The above is just one example of a flowchart that has no evaluation equivalent structured program.

So we may sometimes need to introduce extra state modifiers or tests when re-structuring residual programs. But we want to avoid this whenever we can.

We use a restructuring methods based on recognising subsets of basic blocks that correspond to structured statements and then replace these subsets by basic blocks that use structured statements.

The following rules do this for 17 different patterns of basic blocks. We apply these until no rule applies to the remaining set of basic blocks.

1. If the set of basic blocks contains two blocks:
   $$
   (e; s_1; \text{goto } l) \quad (l; s_2; j)
   $$
   combine these to the single basic block
   $$
   (e; s_1; s_2; j)
   $$

2. If the set of basic blocks contains four blocks:
   $$
   (e; s_1; \text{if } c_1 \text{ goto } l_1 l_2) \quad (l_1; s_2; \text{goto } l_3) \quad (l_2; s_3; \text{goto } l_4) \quad (\text{if } c_2 \text{ from } l_3 l_4; s_4; j)
   $$
   combine these into the single basic block
   $$
   (e; s_1; \text{if } c_1 \text{ then } s_2; \text{else } s_3; \text{fi } c_2; s_4; j)
   $$

3. If the set of basic blocks contains three blocks
   $$
   (e; s_1; \text{if } c_1 \text{ goto } l_1 l_2) \quad (l_1; s_2; \text{goto } l_3) \quad (\text{if } c_2 \text{ from } l_3 l_2; s_3; j)
   $$
   combine these into a single basic block
   $$
   (e; s_1; \text{if } c_1 \text{ then } s_2; \text{else skip fi } c_2; s_3; j)
   $$
4. If the set of basic blocks contains three blocks
   \( (c: s_1; \text{if } c_1 \text{ goto } l_1 \text{ l}_2) \quad (l_2: s_2; \text{ goto } l_3) \quad (\text{if } c_2 \text{ from } l_1 \text{ l}_3; s_3; j) \)
   combine these into a single basic block
   \( (c: s_1; \text{if } c_1 \text{ then skip else } s_2; \text{ fi } c_2; s_3; j) \)

5. If the set of basic blocks contains two blocks
   \( (c: s_1; \text{if } c_1 \text{ goto } l_1 \text{ l}_2) \quad (\text{if } c_2 \text{ from } l_1 \text{ l}_2; s_2; j) \)
   combine these into a single basic block
   \( (c: s_1; \text{if } c_1 \text{ then skip else skip fi } c_2; s_2; j) \)

6. If the set of basic blocks contains four blocks
   \( (c: s_1; \text{if } c_1 \text{ goto } l_1 \text{ l}_2) \quad (l_1: s_2; \text{ goto } l_3) \quad (l_2: s_3; \text{ goto } l_4) \quad (\text{if } c_2 \text{ from } l_4 \text{ l}_3; s_4; j) \)
   combine these into a single basic block
   \( (c: s_1; \text{if } c_1 \text{ then } s_2; \text{ else } s_3; \text{ fi } !c_2; s_4; j) \)

7. If the set of basic blocks contains three blocks
   \( (c: s_1; \text{if } c_1 \text{ goto } l_1 \text{ l}_2) \quad (l_1: s_2; \text{ goto } l_3) \quad (\text{if } c_2 \text{ from } l_2 \text{ l}_3; s_3; j) \)
   combine these into a single basic block
   \( (c: s_1; \text{if } c_1 \text{ then } s_2; \text{ else skip fi } !c_2; s_3; j) \)

8. If the set of basic blocks contains three blocks
   \( (c: s_1; \text{if } c_1 \text{ goto } l_1 \text{ l}_2) \quad (l_2: s_2; \text{ goto } l_3) \quad (\text{if } c_2 \text{ from } l_3 \text{ l}_1; s_3; j) \)
   combine these into a single basic block
   \( (c: s_1; \text{if } c_1 \text{ then skip else } s_2; \text{ fi } !c_2; s_3; j) \)

9. If the set of basic blocks contains two blocks
   \( (c: s_1; \text{if } c_1 \text{ goto } l_1 \text{ l}_2) \quad (\text{if } c_2 \text{ from } l_2 \text{ l}_1; s_2; j) \)
   combine these into a single basic block
   \( (c: s_1; \text{if } c_1 \text{ then skip else skip fi } !c_2; s_2; j) \)

10. If the set of basic blocks contains two blocks
    \( (\text{if } c_1 \text{ from } l_1 \text{ l}_2; s_1; \text{if } c_2 \text{ goto } l_3 \text{ l}_4) \quad (l_4: s_2; \text{ goto } l_2) \)
    combine these into a single basic block
    \( (l_1: \text{from } c_1 \text{ do } s_1 \text{ loop } s_2 \text{ until } c_2; \text{ goto } l_3) \)

11. If the set of basic blocks contains a block
    \( (\text{if } c_1 \text{ from } l_1 \text{ l}_2; s; \text{if } c_2 \text{ goto } l_3 \text{ l}_2) \)
    replace this by the basic block
    \( (l_1: \text{from } c_1 \text{ do } s \text{ loop skip until } c_2; \text{ goto } l_3) \)

12. If the set of basic blocks contains two blocks
    \( (\text{if } c_1 \text{ from } l_1 \text{ l}_2; s_1; \text{if } c_2 \text{ goto } l_4 \text{ l}_3) \quad (l_4: s_2; \text{ goto } l_2) \)
    combine these into a single basic block
    \( (l_1: \text{from } c_1 \text{ do } s_1 \text{ loop } s_2 \text{ until } !c_2; \text{ goto } l_3) \)
13. If the set of basic blocks contains a block
   (if \( c_1 \) from \( l_1 \) \( l_2 \); \( s \); if \( c_2 \) goto \( l_2 \) \( l_3 \))
   replace this by the basic block
   (\( l_1 \): from \( c_1 \) do \( s \) loop skip until \( !c_2 \); goto \( l_3 \))

14. If the set of basic blocks contains two blocks
   (if \( c_1 \) from \( l_2 \) \( l_1 \); if \( c_2 \) goto \( l_3 \) \( l_4 \))
   combine these into a single basic block
   (\( l_1 \): from \( !c_1 \) do \( s_1 \) loop \( s_2 \) until \( c_2 \); goto \( l_3 \))

15. If the set of basic blocks contains a block
   (if \( c_1 \) from \( l_2 \) \( l_1 \); if \( c_2 \) goto \( l_2 \) \( l_3 \))
   replace this by the basic block
   (\( l_1 \): from \( !c_1 \) do \( s \) loop skip until \( c_2 \); goto \( l_3 \))

16. If the set of basic blocks contains two blocks
   (if \( c_1 \) from \( l_2 \) \( l_1 \); if \( c_2 \) goto \( l_3 \) \( l_4 \))
   combine these into a single basic block
   (\( l_1 \): from \( !c_1 \) do \( s_1 \) loop \( s_2 \) until \( !c_2 \); goto \( l_3 \))

17. If the set of basic blocks contains a block
   (if \( c_1 \) from \( l_2 \) \( l_1 \); if \( c_2 \) goto \( l_2 \) \( l_3 \))
   replace this by the basic block
   (\( l_1 \): from \( !c_1 \) do \( s \) loop skip until \( !c_2 \); goto \( l_3 \))

The important rules are 1, 2 and 10, which are essentially inverses of the translation from section 4.1. The remaining rules are special cases where one branch of a conditional or part of a loop is empty or where labels in if-goto or if-from are swapped (so conditions need to be negated).

It is easy to see that these rules preserve (strong) evaluation equivalence. Since we negate some conditions, we need the equivalence of \( c \) and \( !c \) and of \( !c \) and \( c \) that allowed us in the definition of evaluation equivalence.

The reversibility requirement actually makes some things simpler than in the irreversible case, as we know that there can not be multiple jumps to the same label. In the irreversible case we would, for example, need a side condition to rule 1 saying that there are no other jumps to \( l \). Also, since there are exactly two occurrences of each label, it is easy to verify that the rules do not overlap, so they can be applied in any order.

If application of the rules reduces the set of basic blocks to a single basic block
   (start: \( s \); return), we have a single structured Janus statement \( s \). If not, we can either declare failure to structure the program or add the extra control variable as described above. Currently, we admit failure and return a partially unstructured program, as our (extended) Janus compiler allows programs to mix structured and unstructured control. This is easy enough to change if we need to use an unextended Janus compiler.

As an example, figure 8 shows a restructured version of the residual program in figure 5. Also, if we translate any of the programs in figure 2 into flowchart form and restructure the result, we get the original structure back.
b -> b prod with v;
assert 0==prod; prod += b;
assert !(0==prod); prod += b;
assert !(prod<b); v += b; b += v; v -= b/2;
assert !(0==prod); prod += b;
assert !(prod<b); v += b; b += v; v -= b/2;
assert !(0==prod);
assert prod<b; v += b; b += v; v -= b/2;
assert !(0==prod); prod += b;
assert !(prod<b);
from prod<b+b do
  v += b/2; b -= v; v -= b
loop
  skip
until odd(b)

Figure 8: Restructured specialised multiplication program

5.1 Replacing jumps by procedure calls

In [8], it is suggested that unstructured control that can not be reduced to structured control without adding variables can instead be replaced by mutually recursive procedure calls. The idea is that a tail call is very much like an unstructured goto. The method replaces every remaining basic block with a procedure and all remaining jumps by tail calls to these procedures. This works well because basic blocks in irreversible languages are headed by unconditional labels (that translate easily into procedure names) and both unconditional and conditional jumps can be translated into tail calls. In our reversible flowchart language, we have two issues not present in irreversible languages:

1. Basic blocks can be headed by two-way assertions.

2. In Janus, the branches of an if-then-else-fi are not in tail-call position, even if the whole conditional statement is. This is because the fi-condition needs to be tested after the chosen branch completes.

Two-way assertions are not difficult to handle: We just make two procedures that each test the condition (positively and negatively) and call a procedure for the common body. But we can not translate if c goto l1 l2 into if c then call p1 else call p2 fi' c' because there might be no suitable condition c', and even if there is, there is no obvious way to find it.

Hence, we believe that it is not workable to translate unstructured control flow into tail-recursive procedure calls.

6 Experiments

We have implemented (in Standard ML) a partial evaluator using the methods described in this paper.

We have used the partial evaluator to specialise a few Janus programs. For each of these, the table in figure 9 shows the number of non-blank lines in the original Janus program, the flowchart form of the program and the residual program.

fib is the program from figure 2(a). It is specialised to n=10, so the residual program is run without inputs. encrypt is a simple encryption program. The program is specialised to the key (which is used both for encryption and decryption). During specialisation, a loop is unrolled, so the residual program is quite large. postfix is the program from figure 2(c)
with the procedure calls manually unfolded (as the specialiser doesn’t handle procedure calls yet). \texttt{postfix} uses a partially static array for the input values, so the residual program has individual variables for these. The stacks are also partially static, so the stack elements become individual variables. The interpreter is specialised with respect to a postfix expression with two inputs and five operations. \texttt{control} is the program from figure 6(b). This is specialised with no static inputs, but the \texttt{control} variable is static. The residual program is identical to the program in figure 6(c). The difference in running time show the overhead of structuring a program using a \texttt{control} variable. \texttt{dfa} is an interpreter for reversible DFAs. It is specialised to a DFA that recognises bit strings that are divisible by 3. The restructurer was not able to restructure the residual program, so the numbers for the residual program are for the flowchart form.

We compile Janus programs to MIPS code that is run on the simulator MARS [20]. Figure 9 show the instruction counts of the original and residual programs. As usual with partial evaluation, the most dramatic speedups are found when specialising interpreters.

### 7 Conclusion and future work

We have made a partial evaluator for the reversible language Janus with the exception of procedure calls. It is to our knowledge the first partial evaluator for a deterministic reversible programming language.\footnote{Pure logic languages can be considered reversible and partial evaluators for such exist [15].}

Polyvariant program-point specialisation can be applied to Janus, but the reversibility requirement added some complications, which we have solved.

The residual programs produced by the specialiser use unstructured control flow where Janus uses structured control flow, so we have devised a method to restructure residual programs from flowchart form to using the reversible control structures of Janus. This is not always possible to do without introducing extra variables. Currently, the specialiser will return partially unstructured programs in such cases, but it is easy to add an extra pass to

\begin{table}[h]
\begin{tabular}{|l|c|c|c|}
\hline
Program & Source lines & Flowchart lines & Residual lines \\
\hline
fib & 9 & 12 & 33 \\
multiply & 23 & 30 & 28 \\
encrypt & 15 & 23 & 171 \\
postfix & 46 & 74 & 16 \\
control & 17 & 39 & 6 \\
dfa & 26 & 29 & 48 \\
\hline
\end{tabular}
\end{table}

\begin{table}[h]
\begin{tabular}{|l|c|c|}
\hline
Program & Original steps & Residual steps \\
\hline
fib & 147 & 95 \\
multiply & 160 & 108 \\
encrypt & 442 & 354 \\
postfix & 998 & 70 \\
control & 558 & 145 \\
dfa & 510 & 216 \\
\hline
\end{tabular}
\end{table}
structure these using a control variable. Since this adds overhead and our Janus compiler can handle unstructured programs, we have not done so.

We have in this paper not handled procedure calls. It is, as such, not difficult to specialise procedure calls: Procedures must, like the program, have a single return jump. For the program, we ensured this by disallowing modification of static output variables, so there is only one possible static state at program end (all non-output variables are zero at program end). There is no requirement that variables are zero at the end of a procedure, so to ensure that there is only one possible static state at procedure end, the equivalent solution is to disallow modification of all static variables inside a procedure. This means that a procedure call can not change static state, which makes specialisation easy. The restriction against modifying static state makes this of limited use, though. We will look at better ways of handling procedure calls in a future paper.

References


On Determination of Backward Graph Transformation
(Ongoing Work Report)

Zhenjiang Hu

National Institute of Informatics
Joint Work with BiG Team Members
January 13, 2011

BiG: NII Grand Challenge Project (2008–)

A Bidirectional Graph (Model) Transformation Framework
for Evolutinal Software Development

Bidirectional Transformation

It consists of a pair of computation forward and backward.
### Stability

No change on the target implies no change on the source.

\[
\text{put}(\text{get}(s), s) = s
\]

### Reflectivity

Permitted changes on the target should be reflected to the source.

\[
\text{get}(\text{put}(t', s)) = t'
\]

### Applications

[Diagram showing applications involving data synchronization and view updating.]
Challenge: from Trees to Graphs

We aim at a language for bidirectional model-driven software development (or roundtrip software development).

Two Approaches to Bidirectional Programming

- Design a domain-specific combinator library
  [Lens: POPL’95, POPL’98, ICFP’08, ICFP’10]
- Primitive bidirectional computing functions
- Combinators to compose bidirectional computations
- Automatic bidirectionalization of
  - A core ATL [Xiong+: ASE’07]
  - A first-order FPL [Matsuda+: ICFP’07]
  - A graph query language UnQL [Hidaka+: ICFP’10]

ASSUMPTION:
Each program has fixed computation behavior for get and put.

Not a practical assumption!

Since get is generelly non-injective, many suitable puts correspond to one get, each being useful in one context.
Consider the relation input database EMP:

\[ EMP = \{ \text{No}, \text{Name}, \text{Location}, \text{BBTeam} \} \]

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Location</th>
<th>BBTeam</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tanaka</td>
<td>Tokyo</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>Kato</td>
<td>Tohoku</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Sato</td>
<td>Tokyo</td>
<td>No</td>
</tr>
</tbody>
</table>

Consider a forward transformation defined by

```
Select *
From EMP
Where Location = "Tokyo"
```

which produces the view:

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Location</th>
<th>BBTeam</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tanaka</td>
<td>Tokyo</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Sato</td>
<td>Tokyo</td>
<td>No</td>
</tr>
</tbody>
</table>

What is a suitable backward transformation if we delete employee #1 in the view?

⇒ delete employee #1
⇒ move employee #1 from Tokyo to Kyoto

Consider another forward transformation defined by

```
Select *
From EMP
Where BBTeam = Yes
```

which produces the view:

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Location</th>
<th>BBTeam</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tanaka</td>
<td>Tokyo</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Kato</td>
<td>Tohoku</td>
<td>Yes</td>
</tr>
</tbody>
</table>

What is a suitable backward transformation if we delete employee #1 in the view?

⇒ delete employee #1?
⇒ change the BBTeam of employee #1 to No?
Rather than fixing a backward transformation, is there a way to determine a suitable backward transformation at view definition time?

From Simon Peyton Jones:

If you find a new problem, there may have been some solutions (or ideas) given by DB people.

Keller’s Dialog Approach

- **Mapping** a query (forward transformation) to the algebra consisting of selection, projection and join (Stanard).
- **Enumerating finite backward transformations** for selection, projection and join (PODS’85).
- **Dialoging** with view designers to choose a backward transformation **statically** by traversing over the syntactic tree of an algebra expression (VLDB’86).

Our Approach

Design a graph algebra such that

- it is **powerful** enough to be used as the base algebra for graph querying (transforming);
- each construct has **enumerable** choices for backward transformation.
Can we use the existing UnCAL as our graph algebra?

\[
e ::= \{ \} | \{ l : e \} | e \cup e | \text{lx} := e | \& y | \{
| e \oplus e | e \@ e | \text{cycle}(e) \quad \{ \text{constructor} \}
| \$g \quad \{ \text{graph variable} \}
| \text{if } l = l \text{ then } e \text{ else } e \quad \{ \text{conditional} \}
| \text{rec}(\lambda(\$l, \$g). e)(e) \quad \{ \text{structural recursion application} \}
\]

We can easily enumerate suitable backward transformation for all constructs except for structural recursion [ICFP 2010]

For instance, if has several possibilities for backward transformation is some modification on the view is applied.

What is the problem with structural recursion?

### Structural Recursion: Manipulating Graphs

Structural Recursion:

\[
\begin{align*}
f (\{\}) & = \{\} \\
f (\{l : g\}) & = e[l, g] \@ f(g) \\
f (g_1 \cup g_2) & = f(g_1) \cup f(g_2)
\end{align*}
\]

Or written as:

\[
\text{sfun } f (\{l : g\}) = e[l, g] \@ f(g)
\]

Or written as:

\[
f = \text{rec}(\lambda(l, g). e[l, g])
\]
**An Example**

![Diagram of a graph with nodes labeled 1 to 6 and edges labeled a, b, c, and d.]

\[
\text{sfun } a2d_{xc} \left( \{ l : g \} \right) = \begin{cases} 
\text{if } l = a \text{ then } \{ d : a2d_{xc}(g) \} \\
\text{else if } l = c \text{ then } a2d_{xc}(g) \\
\text{else } \{ l : a2d_{xc}(g) \}
\end{cases}
\]

i.e.,
\[
a2d_{xc} = \text{rec}(l, g). \begin{cases} 
\text{if } l = a \text{ then } \{ d : k \} \\
\text{else if } l = c \text{ then } k \\
\text{else } \{ l : k \}
\end{cases}
\]

---

**A structural recursion could be quite complicated**

- Possible duplicated use of \( g \):
  \[
  \text{sfun } f \left( \{ l : g \} \right) = e[l, g] \odot f(g)
  \]
  \[
  f = \text{rec}(\lambda(l, g). e[l, g])
  \]
  \( \Rightarrow \) Backward transformation may introduce side-effect

- Nested recursion:
  \[
  f = \text{rec}(\lambda(l, g). \cdots \text{rec}(\lambda(l', g'). \cdots ) \cdots )
  \]
  \( \Rightarrow \) Backward transformation needs to care about context
Nested traversals over multiple graphs:

\[
\text{rec}(\lambda(l, g) \cdot \cdots \text{rec}(\lambda(l, g) \cdot \cdots)(db_1) \cdots)(db_2)
\]

⇒ Backward transformation needs to consider data joining.

---

Refining UnCAL

Is it possible to define a graph algebra which only considers the following simple structural recursion?

\[
\text{sfun } f \{ \{ l : g \} \} = e[l] @ f(g)
\]

\[
f = \text{rec}(\lambda(l, g).e[l])
\]

The backward behavior of this simple structural recursion is uniquely determined by that of \( e[l] \).

Assumption: the unit for insertion/deletion on the view should match with \( e[l] \).

---

Simplifying Structural Recursions

Possible duplicated use of \( g \):

\[
\text{sfun } f \{ \{ l : g \} \} = e[l, g] @ f(g)
\]

\[
f = \text{rec}(\lambda(l, g).e[l, g])
\]

\[\uparrow\]

tupling \( f \) with \( id \)
Nested recursion:
\[
f = \text{rec}(\lambda(l, g). \cdots \text{rec}(\lambda(l', g'). \cdots) \cdots)
\]

Unnesting / lambda lifting
\[
\mu^f(X) = \{(v, w) \mid v \leftarrow X, w \leftarrow f(v)\}
\]

Nested traversals over multiple graphs:
\[
\text{rec}(\lambda(l, g). \cdots \text{rec}(\lambda(l, g). \cdots)(db_1) \cdots)(db_2)
\]

joining variables
\[
X \bowtie Y = \{(v, w) \mid x \leftarrow X, w \leftarrow Y\}
\]

Main Results

Theorem (Expressiveness)
Any UnQL expression can be compiled to the following graph algebra:
\[
t ::= \quad \text{any graph constructor} \quad \text{if } l = l \text{ then } t_1 \text{ else } t_2
\]

where \( f \) is a simple structural recursion.
Theorem (Enumerability of Backward Transformations)

Suitable backward transformations for each construct of the following graph algebra is enumerable.

\[ t ::= \begin{array}{l}
\text{any graph constructor} \\
g \\
\text{if } l = l \text{ then } t_1 \text{ else } t_2 \\
f \ t \\
t_1 \triangleright t_2 \\
\mu^f(t) 
\end{array} \]

where \( f \) is a simple structural recursion.

Conclusion

- We show that Keller’s dialogue approach to determining backward transformations can be generalized from relational data to graph data, by defining a new graph algebra:
  - sufficient expressive power
  - enumerable backward transformations

The new algebra can be considered as a combination of structural recursion with a general tree algebra.

More Information about BiG

The project page contains all published papers, system demo, and the source codes of the GRoundTram system.

http://www.biglab.org
Author Index

Andersen, Jesper, 71
Asada, Kazuyuki, 197
Asai, Kenichi, 10
Axelsen, Holger Bock, 33, 47
Bahr, Patrick, 141
Clementsen, Poul J., 47
Emoto, Kento, 228
Filinski, Andrzej, 54
Fischer, Sebastian, 237
Glück, Robert, 31, 33, 47
Hartmann, Lars, 3
Henglein, Fritz, 208
Henriksen, Anders Starcke, 122
Hidaka, Soichiro, 172
Hirai, Yoichi, 110
Honda, Kohei, 224
Hu, Zhenjiang, 269
Hvitved, Tom, 64, 141
Inaba, Kazuhiro, 98
Jones, Neil D., 3
Kato, Hiroyuki, 183
Klaedtke, Felix, 64
Kobayashi, Naoki, 89

Larsen, Ken Friis, 58
Liu, Yu, 156
Matsuda, Kazutaka, 80
Matsuzaki, Kiminori, 150
Mogensen, Torben Ægidius, 247
Morihata, Akimasa, 150
Nakano, Keisuke, 129
Nielsen, Lasse, 208, 224
Nielsen, Morten Ib, 141
Ong, Luke, 89
Sato, Ryosuke, 89
Simonsen, Jakob Grue, 3
Tabuchi, Naoshi, 89
Takeichi, Masato, 1
Thomsen, Mikkel Jonsson, 167
Tsukada, Takeshi, 89
Ueda, Yayoi, 10
Unno, Hiroshi, 89
Yamamoto, Kazuhiro, 110
Yokoyama, Tetsuo, 42
Yoshida, Nobuko, 224
Zălinescu, Eugen, 64
After Work
Dinner at Asakusa