The Safe λ-Calculus

William Blum

Joint work with C.-H. Luke Ong

Oxford University Computing Laboratory

BCTCS, 2–5 April 2007

Overview

- Safety: a restriction for higher-order grammars.
- Transposed to the λ-calculus, it gives rise to the Safe λ-calculus.
- Safety has nice algorithmic properties, automata-theoretic and game-semantic characterisations.

Simply Typed λ-Calculus

- Simple types $A := o \mid A \to A$.
- The order of a type is given by $\mathrm{order}(o) = 0$, $\mathrm{order}(A \to B) = \max(\mathrm{order}(A) + 1, \mathrm{order}(B))$.
- Judgements of the form $\Gamma \vdash M : T$ where Γ is the context, M is the term and T is the type:

$$(var)\ \frac{}{x : A \vdash x : A} \qquad (wk)\ \frac{\Gamma \vdash M : A}{\Delta \vdash M : A}\ \Gamma \subset \Delta$$

$$(app)\ \frac{\Gamma \vdash M : A \to B \quad \Gamma \vdash N : A}{\Gamma \vdash MN : B} \quad (abs)\ \frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x^A.M : A \to B}$$

- Example: $f : o \to o \to o, x : o \vdash (\lambda \varphi^{o \to o} x^o.\varphi\ x)(f\ x)$
- A single rule: β-reduction. e.g. $(\lambda x.M)N \to_\beta M[N/x]$

Simply Typed λ-Calculus

- Simple types $A := o \mid A \to A$.
- The order of a type is given by $\mathrm{order}(o) = 0$, $\mathrm{order}(A \to B) = \max(\mathrm{order}(A) + 1, \mathrm{order}(B))$.
- Judgements of the form $\Gamma \vdash M : T$ where Γ is the context, M is the term and T is the type:

$$(var)\ \frac{}{x : A \vdash x : A} \qquad (wk)\ \frac{\Gamma \vdash M : A}{\Delta \vdash M : A}\ \Gamma \subset \Delta$$

$$(app)\ \frac{\Gamma \vdash M : A \to B \quad \Gamma \vdash N : A}{\Gamma \vdash MN : B} \qquad (abs)\ \frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x^A.M : A \to B}$$

- Example: $f : o \to o \to o, x : o \vdash (\lambda \varphi^{o \to o} x^o.\varphi\ x)(f\ x)$
- A single rule: β-reduction. e.g. $(\lambda x.M)N \to_\beta M[N/x]$

Simply Typed λ-Calculus

- Simple types $A := o \mid A \to A$.
- The order of a type is given by $\mathrm{order}(o) = 0$, $\mathrm{order}(A \to B) = \max(\mathrm{order}(A) + 1, \mathrm{order}(B))$.
- Judgements of the form $\Gamma \vdash M : T$ where Γ is the context, M is the term and T is the type:

$$(var)\ \frac{}{x : A \vdash x : A} \qquad (wk)\ \frac{\Gamma \vdash M : A}{\Delta \vdash M : A}\ \Gamma \subset \Delta$$

$$(app)\ \frac{\Gamma \vdash M : A \to B \quad \Gamma \vdash N : A}{\Gamma \vdash MN : B} \qquad (abs)\ \frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x^A.M : A \to B}$$

- Example: $f : o \to o \to o, x : o \vdash (\lambda \varphi^{o \to o} x^o.\varphi\ x)(f\ x)$
- A single rule: β-reduction. e.g. $(\lambda x.M)N \to_\beta M[N/x]$

Simply Typed λ-Calculus

- Simple types $A := o \mid A \to A$.
- The order of a type is given by $\mathrm{order}(o) = 0$, $\mathrm{order}(A \to B) = \max(\mathrm{order}(A) + 1, \mathrm{order}(B))$.
- Judgements of the form $\Gamma \vdash M : T$ where Γ is the context, M is the term and T is the type:

$$(var)\ \frac{}{x : A \vdash x : A} \qquad (wk)\ \frac{\Gamma \vdash M : A}{\Delta \vdash M : A}\ \Gamma \subset \Delta$$

$$(app)\ \frac{\Gamma \vdash M : A \to B \quad \Gamma \vdash N : A}{\Gamma \vdash MN : B} \qquad (abs)\ \frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x^A.M : A \to B}$$

- Example: $f : o \to o \to o, x : o \vdash (\lambda\varphi^{o\to o}x^o.\varphi\ x)(f\ x)$
- A single rule: β-reduction. e.g. $(\lambda x.M)N \to_\beta M[N/x]$

Simply Typed λ-Calculus

- Simple types $A := o \mid A \to A$.
- The order of a type is given by $\mathrm{order}(o) = 0$, $\mathrm{order}(A \to B) = \max(\mathrm{order}(A) + 1, \mathrm{order}(B))$.
- Judgements of the form $\Gamma \vdash M : T$ where Γ is the context, M is the term and T is the type:

$$(var)\ \frac{}{x : A \vdash x : A} \qquad (wk)\ \frac{\Gamma \vdash M : A}{\Delta \vdash M : A}\ \Gamma \subset \Delta$$

$$(app)\ \frac{\Gamma \vdash M : A \to B \quad \Gamma \vdash N : A}{\Gamma \vdash MN : B} \qquad (abs)\ \frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x^A.M : A \to B}$$

- Example: $f : o \to o \to o, x : o \vdash (\lambda \varphi^{o \to o} x^o.\varphi\ x)(f\ x)$
- A single rule: β-reduction. e.g. $(\lambda x.M)N \to_\beta M[N/x]$

Variable Capture

The usual "problem" in λ-calculus: avoid variable capture when performing substitution: $(\lambda x.(\lambda y.x))y \rightarrow_\beta (\lambda \underline{y}.x)[\underline{y}/x] \neq \lambda y.y$

1. Standard solution: Barendregt's convention. Variables are renamed so that free variables and bound variables have different names. Eg. $(\lambda x.(\lambda y.x))y$ becomes $(\lambda x.(\lambda z.x))y$ which reduces to $(\lambda z.x)[y/x] = \lambda z.y$
   Drawback: requires to have access to an unbounded supply of names to perform a given sequence of β-reductions.
2. Another solution: switch to the λ-calculus à la de Brujin where variable binding is specified by an index instead of a name. Variable renaming then becomes unnecessary.
   Drawback: the conversion to nameless de Brujin λ-terms requires an unbounded supply of indices.

The Safety restriction avoids the need for variable renaming!

Variable Capture

The usual "problem" in λ-calculus: avoid variable capture when performing substitution: $(\lambda x.(\lambda y.x))y \rightarrow_\beta (\lambda \underline{y}.x)[\underline{y}/x] \neq \lambda y.y$

1. Standard solution: Barendregt's convention. Variables are renamed so that free variables and bound variables have different names. Eg. $(\lambda x.(\lambda y.x))y$ becomes $(\lambda x.(\lambda z.x))y$ which reduces to $(\lambda z.x)[y/x] = \lambda z.y$
   Drawback: requires to have access to an unbounded supply of names to perform a given sequence of β-reductions.
2. Another solution: switch to the λ-calculus à la de Brujin where variable binding is specified by an index instead of a name. Variable renaming then becomes unnecessary.
   Drawback: the conversion to nameless de Brujin λ-terms requires an unbounded supply of indices.

The Safety restriction avoids the need for variable renaming!

Variable Capture

The usual "problem" in λ-calculus: avoid variable capture when performing substitution: $(\lambda x.(\lambda y.x))y \rightarrow_\beta (\lambda \underline{y}.x)[\underline{y}/x] \neq \lambda y.y$

1. Standard solution: Barendregt's convention. Variables are renamed so that free variables and bound variables have different names. Eg. $(\lambda x.(\lambda y.x))y$ becomes $(\lambda x.(\lambda z.x))y$ which reduces to $(\lambda z.x)[y/x] = \lambda z.y$
   Drawback: requires to have access to an unbounded supply of names to perform a given sequence of β-reductions.
2. Another solution: switch to the λ-calculus à la de Brujin where variable binding is specified by an index instead of a name. Variable renaming then becomes unnecessary.
   Drawback: the conversion to nameless de Brujin λ-terms requires an unbounded supply of indices.

The Safety restriction avoids the need for variable renaming!

Variable Capture

The usual "problem" in λ-calculus: avoid variable capture when performing substitution: $(\lambda x.(\lambda y.x))y \rightarrow_\beta (\lambda \underline{y}.x)[\underline{y}/x] \neq \lambda y.y$

1. Standard solution: Barendregt's convention. Variables are renamed so that free variables and bound variables have different names. Eg. $(\lambda x.(\lambda y.x))y$ becomes $(\lambda x.(\lambda z.x))y$ which reduces to $(\lambda z.x)[y/x] = \lambda z.y$
   Drawback: requires to have access to an unbounded supply of names to perform a given sequence of β-reductions.
2. Another solution: switch to the λ-calculus à la de Brujin where variable binding is specified by an index instead of a name. Variable renaming then becomes unnecessary.
   Drawback: the conversion to nameless de Brujin λ-terms requires an unbounded supply of indices.

The Safety restriction avoids the need for variable renaming!

Variable Capture

The usual "problem" in λ-calculus: avoid variable capture when performing substitution: $(\lambda x.(\lambda y.x))y \rightarrow_\beta (\lambda \underline{y}.x)[\underline{y}/x] \neq \lambda y.y$

1. Standard solution: Barendregt's convention. Variables are renamed so that free variables and bound variables have different names. Eg. $(\lambda x.(\lambda y.x))y$ becomes $(\lambda x.(\lambda z.x))y$ which reduces to $(\lambda z.x)[y/x] = \lambda z.y$
   Drawback: requires to have access to an unbounded supply of names to perform a given sequence of β-reductions.
2. Another solution: switch to the λ-calculus à la de Brujin where variable binding is specified by an index instead of a name. Variable renaming then becomes unnecessary.
   Drawback: the conversion to nameless de Brujin λ-terms requires an unbounded supply of indices.

The Safety restriction avoids the need for variable renaming!

Variable Capture

The usual "problem" in λ-calculus: avoid variable capture when performing substitution: $(\lambda x.(\lambda y.x))y \to_\beta (\lambda \underline{y}.x)[\underline{y}/x] \neq \lambda y.y$

1. Standard solution: Barendregt's convention. Variables are renamed so that free variables and bound variables have different names. Eg. $(\lambda x.(\lambda y.x))y$ becomes $(\lambda x.(\lambda z.x))y$ which reduces to $(\lambda z.x)[y/x] = \lambda z.y$
   Drawback: requires to have access to an unbounded supply of names to perform a given sequence of β-reductions.
2. Another solution: switch to the λ-calculus à la de Brujin where variable binding is specified by an index instead of a name. Variable renaming then becomes unnecessary.
   Drawback: the conversion to nameless de Brujin λ-terms requires an unbounded supply of indices.

The Safety restriction avoids the need for variable renaming!

What is the Safety Restriction?

- First appeared under the name "restriction of derived types" in "IO and OI Hierarchies" by W. Damm, TCS 1982
- It is a syntactic restriction for higher-order grammars that constrains the occurrences of the variables in the grammar equations according to their orders.

Theorem (Knapik, Niwiński and Urzyczyn (2001,2002))

1. *The Monadic Second Order (MSO) model checking problem for trees generated by safe higher-order grammars of any order is decidable.*
2. *Automata-theoretic characterisation: Safe grammars of order n are as expressive as pushdown automata of order n.*

In an unpublished technical report (2004), Aehlig, de Miranda and Ong were the first to propose a notion of safety adapted to the setting of the λ-calculus.

What is the Safety Restriction?

- First appeared under the name "restriction of derived types" in "IO and OI Hierarchies" by W. Damm, TCS 1982
- It is a syntactic restriction for higher-order grammars that constrains the occurrences of the variables in the grammar equations according to their orders.

Theorem (Knapik, Niwiński and Urzyczyn (2001,2002))

1. *The Monadic Second Order (MSO) model checking problem for trees generated by safe higher-order grammars of any order is decidable.*
2. *Automata-theoretic characterisation: Safe grammars of order n are as expressive as pushdown automata of order n.*

In an unpublished technical report (2004), Aehlig, de Miranda and Ong were the first to propose a notion of safety adapted to the setting of the λ-calculus.

What is the Safety Restriction?

- First appeared under the name "restriction of derived types" in "IO and OI Hierarchies" by W. Damm, TCS 1982
- It is a syntactic restriction for higher-order grammars that constrains the occurrences of the variables in the grammar equations according to their orders.

Theorem (Knapik, Niwiński and Urzyczyn (2001,2002))

1. *The Monadic Second Order (MSO) model checking problem for trees generated by safe higher-order grammars of any order is decidable.*
2. *Automata-theoretic characterisation: Safe grammars of order n are as expressive as pushdown automata of order n.*

In an unpublished technical report (2004), Aehlig, de Miranda and Ong were the first to propose a notion of safety adapted to the setting of the λ-calculus.

The Safe λ-Calculus

The formation rules

$$(var)\ \frac{}{x : A \vdash_s x : A} \qquad (wk)\ \frac{\Gamma \vdash_s M : A}{\Delta \vdash_s M : A}\ \Gamma \subset \Delta$$

$$(app)\ \frac{\Gamma \vdash M : (A_1, \ldots, A_l, B) \quad \Gamma \vdash_s N_1 : A_1 \quad \ldots \quad \Gamma \vdash_s N_l : A_l}{\Gamma \vdash_s M N_1 \ldots N_l : B}$$

with the side-condition $\forall y \in \Gamma : \mathrm{ord}(y) \geq \mathrm{ord}(B)$

$$(abs)\ \frac{\Gamma, x_1 : A_1 \ldots x_n : A_n \vdash_s M : B}{\Gamma \vdash_s \lambda x_1 : A_1 \ldots x_n : A_n . M : A_1 \to \ldots \to A_n \to B}$$

with the side-condition $\forall y \in \Gamma : \mathrm{ord}(y) \geq \mathrm{ord}(A_1 \to \ldots \to A_n \to B)$

Property

In the Safe λ-calculus there is no need to rename variables when performing substitution.

The Safe λ-Calculus

The formation rules

$$(var)\ \frac{}{x : A \vdash_s x : A} \qquad (wk)\ \frac{\Gamma \vdash_s M : A}{\Delta \vdash_s M : A}\ \Gamma \subset \Delta$$

$$(app)\ \frac{\Gamma \vdash M : (A_1, \ldots, A_l, B) \quad \Gamma \vdash_s N_1 : A_1 \quad \ldots \quad \Gamma \vdash_s N_l : A_l}{\Gamma \vdash_s M N_1 \ldots N_l : B}$$

with the side-condition $\forall y \in \Gamma : \mathrm{ord}(y) \geq \mathrm{ord}(B)$

$$(abs)\ \frac{\Gamma, x_1 : A_1 \ldots x_n : A_n \vdash_s M : B}{\Gamma \vdash_s \lambda x_1 : A_1 \ldots x_n : A_n . M : A_1 \rightarrow \ldots \rightarrow A_n \rightarrow B}$$

with the side-condition $\forall y \in \Gamma : \mathrm{ord}(y) \geq \mathrm{ord}(A_1 \rightarrow \ldots \rightarrow A_n \rightarrow B)$

Property

In the Safe λ-calculus there is no need to rename variables when performing substitution.

Examples

- Contracting the β-redex in the following term

$$f : o \to o \to o, x : o \vdash (\lambda \varphi^{o \to o} x^o . \varphi\ x)(f\ x)$$

leads to variable capture:

$$(\lambda \varphi x . \varphi\ x)(f\ x) \not\to_\beta (\lambda x.(f\ x)x).$$

Hence the term is unsafe.
Indeed, $\mathrm{ord}(x) = 0 \leq 1 = \mathrm{ord}(f\ x)$.

- The term $(\lambda \varphi^{o \to o} x^o . \varphi\ x)(\lambda y^o . y)$ is safe.

Examples

- Contracting the β-redex in the following term

$$f : o \to o \to o, x : o \vdash (\lambda \varphi^{o \to o} x^o . \varphi\ x)(\underline{f\ x})$$

leads to variable capture:

$$(\lambda \varphi x . \varphi\ x)(f\ x) \not\to_\beta (\lambda x . (f\ x) x).$$

Hence the term is unsafe.
Indeed, $\mathrm{ord}(x) = 0 \leq 1 = \mathrm{ord}(f\ x)$.

- The term $(\lambda \varphi^{o \to o} x^o . \varphi\ x)(\lambda y^o . y)$ is safe.

Examples

- Contracting the β-redex in the following term

$$f : o \to o \to o, x : o \vdash (\lambda \varphi^{o \to o} x^{o}.\varphi\ x)(\underline{f\ x})$$

  leads to variable capture:

$$(\lambda \varphi x.\varphi\ x)(f\ x) \not\to_{\beta} (\lambda x.(f\ x)x).$$

  Hence the term is unsafe.
  Indeed, $\mathrm{ord}(x) = 0 \leq 1 = \mathrm{ord}(f\ x)$.
- The term $(\lambda \varphi^{o \to o} x^{o}.\varphi\ x)(\lambda y^{o}.y)$ is safe.

Numerical functions

Church Encoding: for $n \in \mathbb{N}$, $\overline{n} = \lambda sz.s^n z$ of type $I = (o \to o) \to o \to o$.

Theorem (Schwichtenberg 1976)

The numeric functions representable by simply-typed terms of type $I \to \ldots \to I$ are exactly the multivariate polynomials extended with the conditional function:

$$cond(t, x, y) = \begin{cases} x, & \text{if } t = 0 \\ y, & \text{if } t = n + 1 \end{cases}.$$

cond is represented by the term $C = \lambda FGH\alpha x.H(\lambda y.G\alpha x)(F\alpha x)$.

Theorem

Functions representable by safe λ-expressions of type $I \to \ldots \to I$ are exactly the multivariate polynomials.

So *cond* is not representable in the Safe λ-calculus and C is unsafe.

Numerical functions

Church Encoding: for $n \in \mathbb{N}$, $\overline{n} = \lambda sz.s^n z$ of type $I = (o \to o) \to o \to o$.

Theorem (Schwichtenberg 1976)

The numeric functions representable by simply-typed terms of type $I \to \ldots \to I$ are exactly the multivariate polynomials extended with the conditional function:

$$cond(t,x,y) = \begin{cases} x, & \text{if } t = 0 \\ y, & \text{if } t = n+1 \end{cases} .$$

cond is represented by the term $C = \lambda FGH\alpha x.H(\underline{\lambda y.G\alpha x})(F\alpha x)$.

Theorem

Functions representable by safe λ-expressions of type $I \to \ldots \to I$ are exactly the multivariate polynomials.

So *cond* is not representable in the Safe λ-calculus and C is unsafe.

Game Semantics

Let $\vdash M : T$ be a pure simply typed term.

- Game-semantics provides a model of λ-calculus. M is denoted by a strategy $[\![M]\!]$ on a 2-player game induced by T.
- A strategy is represented by a set of sequences of moves together with links: each move points to a preceding move.
- Computation tree = canonical tree representation of a term.
- Traversals $\mathcal{T}rav(M)$ = sequences of nodes with links respecting some formation rules.

The Correspondence Theorem

The game semantics of a term can be represented on the computation tree:

$$\mathcal{T}rav(M) \cong \langle\!\langle M \rangle\!\rangle$$

$$Reduction(\mathcal{T}rav(M)) \cong [\![M]\!]$$

where $\langle\!\langle M \rangle\!\rangle$ is the revealed game-semantic denotion (i.e. internal moves are uncovered).

Game Semantics

Let $\vdash M : T$ be a pure simply typed term.

- Game-semantics provides a model of λ-calculus. M is denoted by a strategy $[\![M]\!]$ on a 2-player game induced by T.
- A strategy is represented by a set of sequences of moves together with links: each move points to a preceding move.
- Computation tree = canonical tree representation of a term.
- Traversals $\mathcal{T}rav(M)$ = sequences of nodes with links respecting some formation rules.

The Correspondence Theorem

The game semantics of a term can be represented on the computation tree:

$$\mathcal{T}rav(M) \cong \langle\!\langle M \rangle\!\rangle$$

$$Reduction(\mathcal{T}rav(M)) \cong [\![M]\!]$$

where $\langle\!\langle M \rangle\!\rangle$ is the revealed game-semantic denotion (i.e. internal moves are uncovered).

Game Semantics

Let $\vdash M : T$ be a pure simply typed term.

- Game-semantics provides a model of λ-calculus. M is denoted by a strategy $[\![M]\!]$ on a 2-player game induced by T.
- A strategy is represented by a set of sequences of moves together with links: each move points to a preceding move.
- Computation tree = canonical tree representation of a term.
- Traversals $\mathcal{T}rav(M)$ = sequences of nodes with links respecting some formation rules.

The Correspondence Theorem

The game semantics of a term can be represented on the computation tree:

$$\mathcal{T}rav(M) \cong \langle\!\langle M \rangle\!\rangle$$

$$Reduction(\mathcal{T}rav(M)) \cong [\![M]\!]$$

where $\langle\!\langle M \rangle\!\rangle$ is the revealed game-semantic denotion (i.e. internal moves are uncovered).

Game-semantic Characterisation of Safety

- The computation tree of a safe term is incrementally-bound : each variable x is bound by the first λ-node occurring in the path to the root with order $> \mathrm{ord}(x)$.
- Using the Correspondence Theorem we can show:

Proposition

Safe terms are denoted by P-incrementally justified strategies: each P-move m points to the last O-move in the P-view with order $> \mathrm{ord}(m)$.

Corollary

Justification pointers attached to P-moves are redundant in the game-semantics of safe terms.

Game-semantic Characterisation of Safety

- The computation tree of a safe term is incrementally-bound : each variable x is bound by the first λ-node occurring in the path to the root with order $> \mathrm{ord}(x)$.
- Using the Correspondence Theorem we can show:

Proposition

Safe terms are denoted by P-incrementally justified strategies: each P-move m points to the last O-move in the P-view with order $> \mathrm{ord}(m)$.

Corollary

Justification pointers attached to P-moves are redundant in the game-semantics of safe terms.

Game-semantic Characterisation of Safety

- The computation tree of a safe term is incrementally-bound : each variable x is bound by the first λ-node occurring in the path to the root with order $> \mathrm{ord}(x)$.
- Using the Correspondence Theorem we can show:

Proposition

Safe terms are denoted by P-incrementally justified strategies: each P-move m points to the last O-move in the P-view with order $> \mathrm{ord}(m)$.

Corollary

Justification pointers attached to P-moves are redundant in the game-semantics of safe terms.

Conclusion and Future Works

Conclusion:

Safety is a syntactic constraint with nice algorithmic and game-semantic properties.

Future works:

- Find a categorical model of Safe PCF.
- Complexity classes characterised with the Safe λ-calculus?
- Safe Idealized Algol: is contextual equivalence decidable?

Related works:

- Jolie G. de Miranda's thesis on unsafe grammars.
- Ong introduced computation trees in LICS2006 to prove decidability of MSO theory on infinite trees generated by higher-order grammars (whether safe or not).