顕在的契約計算における代数的データ型

関山 太朗，西田 雄気，五十嵐 淳

京都大学

December 25, 2014

ソフトウェア契約

- プログラム部品に要求する性質・仕様 (本研究では)
  - 単純型よりも詳細
- 様々なプログラミング言語で利用可能
  - C 言語の assert，Eiffel の契約による設計，etc.
  - 一般にはプログラム実行時に検査

例: 割り算関数 div

```
let div x y =
  assert (y <> 0);
  ...
```

ソフトウェア契約

- プログラム部品に要求する性質・仕様 (本研究では)
  - 単純型よりも詳細
- 様々なプログラミング言語で利用可能
  - C 言語の assert，Eiffel の契約による設計，etc.
  - 一般にはプログラム実行時に検査

例: 割り算関数 `div`

```
let div x y =
  assert (y <> 0);
  ...
```

第二引数は非ゼロ

顕在的契約計算 [Flanagan 2006]

- 高階関数への契約をモデル化した計算体系
- 型に契約を記述
  - 篩型 (refinement type) $\{\mathtt{x{:}T} \mid \mathtt{e}\}$

    $\{\mathtt{x{:}int} \mid 0 < \mathtt{x}\} = \{1, 2, 3, \ldots\}$
  - 依存関数型 $\mathtt{x{:}T_1} \to \mathtt{T_2}$

    $\mathtt{x{:}int} \to \{\mathtt{y{:}int} \mid \mathtt{x} < \mathtt{y}\} = \{\lambda\, \mathtt{x}.\mathtt{x} + 1, \ldots\}$
  - 依存積型 $\mathtt{x{:}T_1} \times \mathtt{T_2}$

    $\mathtt{x{:}int} \times \{\mathtt{y{:}int} \mid \mathtt{x} < \mathtt{y}\} = \{(0,1), (1,3), \ldots\}$
- 契約をコンパイル前にも実行時にも検査

顕在的契約計算: 実行時検査

型変換 (キャスト) で実現

$$\langle \mathrm{T}_1 \Leftarrow \mathrm{T}_2 \rangle^{\ell}$$

T_2 の値が T_1 として振る舞えるか検査

$$\langle \{\mathtt{x{:}int} \,|\, 0 < \mathtt{x}\} \Leftarrow \mathtt{int} \rangle^{\ell}\, 5 \longrightarrow^{5} \quad : \quad \{\mathtt{x{:}int} \,|\, 0 < \mathtt{x}\}$$

$$\langle \{\mathtt{x{:}int} \,|\, 0 < \mathtt{x}\} \Leftarrow \mathtt{int} \rangle^{\ell}\, 0 \longrightarrow^{*} \Uparrow \ell$$

- $\langle \mathtt{x{:}int} \to \{\mathtt{y{:}int} \,|\, \mathtt{x} < \mathtt{y}\} \Leftarrow \mathtt{int} \to \mathtt{int} \rangle^{\ell}$
- $\langle \mathtt{x{:}int} \times \{\mathtt{y{:}int} \,|\, \mathtt{x} < \mathtt{y}\} \Leftarrow \mathtt{int} \times \mathtt{int} \rangle^{\ell}$

顕在的契約計算: 実行時検査

型変換 (キャスト) で実現

$$\langle \mathrm{T}_1 \Leftarrow \mathrm{T}_2 \rangle^{\ell}$$

T_2 の値が T_1 として振る舞えるか検査

$$\langle \{\mathtt{x{:}int} \,|\, 0 < \mathtt{x}\} \Leftarrow \mathtt{int} \rangle^{\ell}\, 5 \longrightarrow^{5} \quad : \quad \{\mathtt{x{:}int} \,|\, 0 < \mathtt{x}\}$$

$$\langle \{\mathtt{x{:}int} \,|\, 0 < \mathtt{x}\} \Leftarrow \mathtt{int} \rangle^{\ell}\, 0 \longrightarrow^{*} \Uparrow \ell$$

- $\langle \mathtt{x{:}int} \to \{\mathtt{y{:}int} \,|\, \mathtt{x} < \mathtt{y}\} \Leftarrow \mathtt{int} \to \mathtt{int} \rangle^{\ell}$
- $\langle \mathtt{x{:}int} \times \{\mathtt{y{:}int} \,|\, \mathtt{x} < \mathtt{y}\} \Leftarrow \mathtt{int} \times \mathtt{int} \rangle^{\ell}$

代数的データ型の導入

- 代数的データ型への契約情報の埋め込み[1]
  - 篩型をデータ構築子の型として利用
- 代数的データ型を用いた実行時検査
  - 代数的データ型間のキャストとして実現

例: 昇順リスト

```
type slist =
| SNil
| SCons of
  x : int × {xs : slist | empty xs || x ≤ head xs}
```

[1] Kawaguchi, Rondon, and Jhala 2009.

代数的データ型の導入

- 代数的データ型への契約情報の埋め込み[1]
  - 篩型をデータ構築子の型として利用
- 代数的データ型を用いた実行時検査
  - 代数的データ型間のキャストとして実現

例: 昇順リスト

```
type slist =
| SNil
| SCons of
  x : int × {xs : slist | empty xs || x ≤ head xs}
```

[1] Kawaguchi, Rondon, and Jhala 2009.

本研究の内容

- 契約付き代数的データ型を顕在的契約計算に導入
  - 契約付き代数的データ型間のキャストを導入
  - データ型が様々な契約を表現しやすいよう拡張
- その型健全性を証明
  - 特に「篩型の項の評価結果はその契約を満たす」ことを証明
- 遅延契約検査の導入
- 実装
  - OCaml への変換器を Camlp4 を用いて実装
  - 本日のポスターセッションで紹介します！

本研究の内容

- 契約付き代数的データ型を顕在的契約計算に導入
  - 契約付き代数的データ型間のキャストを導入
  - データ型が様々な契約を表現しやすいよう拡張
- その型健全性を証明
  - 特に「篩型の項の評価結果はその契約を満たす」ことを証明
- 遅延契約検査の導入
- 実装
  - OCaml への変換器を Camlp4 を用いて実装
  - 本日のポスターセッションで紹介します！

本研究の内容

- 契約付き代数的データ型を顕在的契約計算に導入
  - 契約付き代数的データ型間のキャストを導入
  - データ型が様々な契約を表現しやすいよう拡張
- その型健全性を証明
  - 特に「篩型の項の評価結果はその契約を満たす」ことを証明
- 遅延契約検査の導入
- 実装
  - OCaml への変換器を Camlp4 を用いて実装
  - 本日のポスターセッションで紹介します！

本研究の内容

- 契約付き代数的データ型を顕在的契約計算に導入
  - **契約付き代数的データ型間のキャスト**を導入
  - データ型が様々な契約を表現しやすいよう拡張
- その型健全性を証明
  - 特に「篩型の項の評価結果はその契約を満たす」ことを証明
- 遅延契約検査の導入
- 実装
  - OCaml への変換器を Camlp4 を用いて実装
  - 本日のポスターセッションで紹介します！

目次

1. イントロダクション
2. 代数的データ型による実行時検査
   - 基本戦略
   - データ構築子の選択
3. 形式化
4. 遅延契約検査
5. まとめ

目次

1. イントロダクション
2. 代数的データ型による実行時検査
   - 基本戦略
   - データ構築子の選択
3. 形式化
4. 遅延契約検査
5. まとめ

代数的データ型による実行時検査

異なるが**互換**な代数的データ型間のキャストを可能に

- 構造が似たデータ型に限りキャストを許可
  - ✓ $\langle \texttt{slist} \Leftarrow \texttt{int list} \rangle^{\ell}$
  - × $\langle \texttt{binary\_tree} \Leftarrow \texttt{int list} \rangle^{\ell}$
- 変換対象のデータ構造を見てどのように検査するかを決める

代数的データ型変換: 基本戦略

1. データ構築子の付け替え
   - 互換な (型の構造が似た) データ構築子に変換
2. 変換後のデータ構築子の型を用いて実行時検査

$$\langle \texttt{slist} \Leftarrow \texttt{int list} \rangle^{\ell}\ (\texttt{Cons}\,(1,\texttt{Nil})) \longrightarrow$$

```
type slist =
  | SNil
  | SCons of
      x : int × {xs : slist | empty xs || x ≤ head xs}
```

代数的データ型変換: 基本戦略

1. データ構築子の付け替え
   - 互換な (型の構造が似た) データ構築子に変換
2. 変換後のデータ構築子の型を用いて実行時検査

$$\langle \texttt{slist} \Leftarrow \texttt{int list} \rangle^{\ell}\ (\texttt{Cons}\,(1,\texttt{Nil})) \longrightarrow$$
$$\texttt{SCons}(\ \ldots\ \ (1,\texttt{Nil}))$$

```
type slist =
  | SNil
  | SCons of
      x : int × {xs : slist | empty xs || x ≤ head xs}
```

代数的データ型変換: 基本戦略

1. **データ構築子の付け替え**
   - **互換な (型の構造が似た) データ構築子に変換**
2. **変換後のデータ構築子の型を用いて実行時検査**

$$\langle \texttt{slist} \Leftarrow \texttt{int list} \rangle^{\ell}\ (\texttt{Cons}\,(1,\texttt{Nil})) \longrightarrow$$
$$\texttt{SCons}($$
$$\langle \texttt{x:int} \times \{\texttt{xs:slist} \mid \texttt{empty xs} \,||\, \texttt{x} \leq \texttt{head xs}\} \Leftarrow \texttt{int} \times \texttt{int list} \rangle^{\ell}$$
$$(1,\texttt{Nil}))$$

```
type slist =
  | SNil
  | SCons of
     x : int × {xs : slist | empty xs || x ≤ head xs}
```

代数的データ型変換: 基本戦略

1. **データ構築子の付け替え**
   - **互換な (型の構造が似た) データ構築子に変換**
2. **変換後のデータ構築子の型を用いて実行時検査**

$$\langle \texttt{slist} \Leftarrow \texttt{int list} \rangle^{\ell}\ (\texttt{Cons}\,(1,\texttt{Nil})) \longrightarrow$$
$$\texttt{SCons}($$
$$\langle \texttt{x:int} \times \{\texttt{xs:slist} \mid \texttt{empty xs} \,||\, \texttt{x} \leq \texttt{head xs}\} \Leftarrow \texttt{int} \times \texttt{int list} \rangle^{\ell}$$
$$(1,\texttt{Nil}))$$

```
type slist =
  | SNil
  | SCons of
      x : int × {xs : slist | empty xs || x ≤ head xs}
```

目次

1. イントロダクション
2. 代数的データ型による実行時検査
   - 基本戦略
   - データ構築子の選択
3. 形式化
4. 遅延契約検査
5. まとめ

データ型互換性の緩和

データ構築子の一対一対応は求めない

- 契約を素直に表現可能
- 不必要な実行時検査を省略

例: 整数 0 を一つ以上含むリスト

$$
\begin{array}{l}
\texttt{type list\_including}^{0} = \\
\quad \mid \texttt{ICons1 of } \{\texttt{x} : \texttt{int} \mid 0 = \texttt{x}\} \times \texttt{int list} \\
\quad \mid \texttt{ICons2 of } \{\texttt{x} : \texttt{int} \mid 0 <> \texttt{x}\} \times \texttt{list\_including0}
\end{array}
$$

- Nil に対応するデータ構築子なし
- Cons に対応するデータ構築子は二つ

データ型互換性の緩和

データ構築子の一対一対応は求めない

- 契約を素直に表現可能
- 不必要な実行時検査を省略

例: 整数 0 を一つ以上含むリスト

```
type
  | ICons  of {x: int | 0 <> x} * int list
  | ICons2 of {x: int | 0 <> x} * list_including0
```

Nil の変換は必ず失敗

- Nil に対応するデータ構築子なし
- Cons に対応するデータ構築子は二つ

データ型互換性の緩和

データ構築子の一対一対応は求めない

- **契約を素直に表現可能**
- **不必要な実行時検査を**

例: 整数 0

```
type list_inc
  | ICons1 of      t
  | ICons2 of {x:int|0      } * list_including0
```

Cons の変換にはどちらを選べばよい？

- Nil に対応するデータ構築子なし
- Cons に対応するデータ構築子は二つ

データ構築子の選択

- 形式体系
  - オラクルがデータ構築子を決定的に選ぶと仮定
  - 互換なものならどう選んでも本研究の性質は成立
- 実装
  - backtracking による虱潰し
    - 実際に実行時検査を行い，成功したものを選択
  - 詳しくはポスターで
  - (期待) うまく最適化すれば篩型による実行時検査より計算コストは高くはならない

代数的データ型の拡張: 項変数抽象化

データ型定義が項変数を束縛できるよう

- データ型，データ構築子で型パラメータを指定

例: 整数 n を少なくとも一つ含むリスト

```
type list_including (n:int) =
  | ICons1 of {x:int|n = x} × int list
  | ICons2 of {x:int|n <> x} × list_including⟨n⟩
```

- **型**: $\texttt{list\_including}\{0\} \simeq \texttt{list\_including}^{0}$
- **項**: $\texttt{ICons1}_0\,(0,\texttt{Nil}) : \texttt{list\_including}\{0\}$

目次

1. イントロダクション
2. 代数的データ型による実行時検査
   - 基本戦略
   - データ構築子の選択
3. 形式化
4. 遅延契約検査
5. まとめ

形式化

- 契約付きデータ型をもつ顕在的契約計算を形式化
  - データ型・構築子の互換性は与えられていると仮定
- 型健全性を証明

定理 (型健全性)

型 $\mathtt{T}$ **の閉じた項** $\mathtt{e}$ **について以下のいずれかが成立**

1. $\mathtt{e} \longrightarrow^* \mathtt{v}$
2. $\mathtt{e} \longrightarrow^* \Uparrow \ell$
3. $\mathtt{e}$ **の評価は停止しない**

さらに *1.* **で** $\mathtt{T} = \{\mathtt{x}{:}\mathtt{T}' \mid \mathtt{e}'\}$ **ならば** $\mathtt{e}'\{\mathtt{v}/\mathtt{x}\} \longrightarrow^* \mathtt{true}$

形式化

- 契約付きデータ型をもつ顕在的契約計算を形式化
  - データ型・構築子の互換性は与えられていると仮定
- 型健全性を証明

定理 (型健全性)

型 $\mathtt{T}$ の閉じた項 $\mathtt{e}$ について以下のいずれかが成立

1. $\mathtt{e} \longrightarrow^* \mathtt{v}$
2. $\mathtt{e} \longrightarrow^* \Uparrow \ell$
3. $\mathtt{e}$ の評価は停止しない

さらに *1.* で $\mathtt{T} = \{\mathtt{x}{:}\mathtt{T}' \mid \mathtt{e}'\}$ ならば $\mathtt{e}'\{\mathtt{v}/\mathtt{x}\} \longrightarrow^* \mathtt{true}$

目次

1. イントロダクション
2. 代数的データ型による実行時検査
   - 基本戦略
   - データ構築子の選択
3. 形式化
4. **遅延契約検査**
5. まとめ

正格な契約検査

$$\texttt{head}\ (\langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell}\ (\texttt{SCons}(1, \cdots, \texttt{SNil})))$$

正格な契約検査

$$\begin{aligned}
&\mathtt{head}\ (\langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}\ (\mathtt{SCons}(1, \cdots, \mathtt{SNil}))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\mathtt{Cons}(1, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}(\mathtt{SCons}(2, \cdots, \mathtt{SNil}))))
\end{aligned}$$

正格な契約検査

$$
\begin{aligned}
& \mathtt{head}\ (\langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}\ (\mathtt{SCons}(1, \cdots, \mathtt{SNil}))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\mathtt{Cons}(1, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}(\mathtt{SCons}(2, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots\ \mathtt{Cons}(2, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}(\mathtt{SCons}(3, \cdots, \mathtt{SNil}))))
\end{aligned}
$$

正格な契約検査

$$
\begin{aligned}
& \mathtt{head}\ (\langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}\ (\mathtt{SCons}(1, \cdots, \mathtt{SNil}))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\mathtt{Cons}(1, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(2, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(2, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(3, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(3, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(4, \cdots, \mathtt{SNil}))))
\end{aligned}
$$

正格な契約検査

$$
\begin{aligned}
& \mathtt{head}\ (\langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}\ (\mathtt{SCons}(1, \cdots, \mathtt{SNil}))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\mathtt{Cons}(1, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(2, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(2, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(3, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(3, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(4, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(4, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(5, \cdots, \mathtt{SNil}))))
\end{aligned}
$$

正格な契約検査

$$
\begin{aligned}
&\texttt{head}\ (\langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell}\ (\texttt{SCons}(1, \cdots, \texttt{SNil}))) \\
\longrightarrow^{*}\ &\texttt{head}\ (\texttt{Cons}(1, \langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell} (\texttt{SCons}(2, \cdots, \texttt{SNil})))) \\
\longrightarrow^{*}\ &\texttt{head}\ (\cdots \texttt{Cons}(2, \langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell} (\texttt{SCons}(3, \cdots, \texttt{SNil})))) \\
\longrightarrow^{*}\ &\texttt{head}\ (\cdots \texttt{Cons}(3, \langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell} (\texttt{SCons}(4, \cdots, \texttt{SNil})))) \\
\longrightarrow^{*}\ &\texttt{head}\ (\cdots \texttt{Cons}(4, \langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell} (\texttt{SCons}(5, \cdots, \texttt{SNil})))) \\
\longrightarrow^{*}\ &\texttt{head}\ (\cdots \texttt{Cons}(5, \langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell} (\texttt{SCons}(6, \cdots, \texttt{SNil}))))
\end{aligned}
$$

正格な契約検査

$$
\begin{aligned}
&\mathtt{head}\ (\langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}\ (\mathtt{SCons}(1, \cdots, \mathtt{SNil}))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\mathtt{Cons}(1, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(2, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\cdots \mathtt{Cons}(2, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(3, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\cdots \mathtt{Cons}(3, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(4, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\cdots \mathtt{Cons}(4, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(5, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\cdots \mathtt{Cons}(5, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(6, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\cdots \mathtt{Cons}(6, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(7, \cdots, \mathtt{SNil}))))
\end{aligned}
$$

正格な契約検査

$$
\begin{aligned}
&\mathtt{head}\ (\langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}\ (\mathtt{SCons}(1, \cdots, \mathtt{SNil}))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\mathtt{Cons}(1, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(2, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\cdots \mathtt{Cons}(2, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(3, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\cdots \mathtt{Cons}(3, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(4, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\cdots \mathtt{Cons}(4, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(5, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\cdots \mathtt{Cons}(5, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(6, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\cdots \mathtt{Cons}(6, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(7, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\cdots \mathtt{Cons}(7, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(8, \cdots, \mathtt{SNil}))))
\end{aligned}
$$

正格な契約検査

$$
\begin{aligned}
&\mathtt{head}\ (\langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}\ (\mathtt{SCons}(1, \cdots, \mathtt{SNil}))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\mathtt{Cons}(1, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}(\mathtt{SCons}(2, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\cdots \mathtt{Cons}(2, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}(\mathtt{SCons}(3, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\cdots \mathtt{Cons}(3, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}(\mathtt{SCons}(4, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\cdots \mathtt{Cons}(4, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}(\mathtt{SCons}(5, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\cdots \mathtt{Cons}(5, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}(\mathtt{SCons}(6, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\cdots \mathtt{Cons}(6, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}(\mathtt{SCons}(7, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ &\mathtt{head}\ (\cdots \mathtt{Cons}(7, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}(\mathtt{SCons}(8, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ &\ldots
\end{aligned}
$$

正格な契約検査

$$
\begin{aligned}
& \mathtt{head}\ (\langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}\ (\mathtt{SCons}(1, \cdots, \mathtt{SNil}))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\mathtt{Cons}(1, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}(\mathtt{SCons}(2, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(2, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}(\mathtt{SCons}(3, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(3, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}(\mathtt{SCons}(4, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(4, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}(\mathtt{SCons}(5, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(5, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}(\mathtt{SCons}(6, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(6, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}(\mathtt{SCons}(7, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(7, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}(\mathtt{SCons}(8, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \ldots \\
\longrightarrow^{*}\ & \mathtt{head}\ (\mathtt{Cons}(1, \mathtt{Cons}(2, \cdots \mathtt{Nil})))
\end{aligned}
$$

正格な契約検査

$$
\begin{aligned}
& \mathtt{head}\ (\langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}\ (\mathtt{SCons}(1, \cdots, \mathtt{SNil}))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\mathtt{Cons}(1, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(2, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(2, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(3, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(3, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(4, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(4, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(5, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(5, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(6, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(6, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(7, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(7, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(8, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \ldots \\
\longrightarrow^{*}\ & \mathtt{head}\ (\mathtt{Cons}(1, \mathtt{Cons}(2, \cdots \mathtt{Nil}))) \\
\longrightarrow^{*}\ & 1
\end{aligned}
$$

正格な契約検査

$$
\begin{aligned}
& \mathtt{head}\ (\langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}\ (\mathtt{SCons}(1, \cdots, \mathtt{SNil}))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\mathtt{Cons}(1, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(2, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(2, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(3, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(3, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(4, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(5, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(6, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(6, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(7, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \mathtt{head}\ (\cdots \mathtt{Cons}(7, \langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} (\mathtt{SCons}(8, \cdots, \mathtt{SNil})))) \\
\longrightarrow^{*}\ & \ldots \\
\longrightarrow^{*}\ & \mathtt{head}\ (\mathtt{Cons}(1, \mathtt{Cons}(2, \cdots \mathtt{Nil}))) \\
\longrightarrow^{*}\ & 1
\end{aligned}
$$

先頭要素がほしかっただけなのに...

遅延契約検査

$$\langle \mathrm{T}_1 \Leftarrow \mathrm{T}_2 \rangle^{\ell} @ \mathrm{e}$$

- 必要とされるまでデータ型キャストを遅延
  - `match` の対象となったときに型変換を実行

$$\mathtt{head}\ (\langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}\ (\mathtt{SCons}(1, \cdots, \mathtt{SNil})))$$

遅延契約検査

$$\langle \mathrm{T}_1 \Leftarrow \mathrm{T}_2 \rangle^{\ell} @ \mathrm{e}$$

- 必要とされるまでデータ型キャストを遅延
  - match の対象となったときに型変換を実行

$$\texttt{head}\ (\langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell}\ (\texttt{SCons}(1, \cdots, \texttt{SNil})))$$
$$\longrightarrow \texttt{head}\ (\langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell} @ (\texttt{SCons}(1, \cdots, \texttt{SNil})))$$

遅延契約検査

$$\langle \mathrm{T}_1 \Leftarrow \mathrm{T}_2 \rangle^{\ell} @ \mathtt{e}$$

- 必要とされるまでデータ型キャストを遅延
  - `match` の対象となったときに型変換を実行

$$\begin{aligned}
& \mathtt{head}\ (\langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell}\ (\mathtt{SCons}(1, \cdots, \mathtt{SNil}))) \\
\longrightarrow\ & \mathtt{head}\ (\langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} @ (\mathtt{SCons}(1, \cdots, \mathtt{SNil}))) \\
\longrightarrow\ & \mathtt{match}\ (\langle \mathtt{int\ list} \Leftarrow \mathtt{slist} \rangle^{\ell} @ (\mathtt{SCons}(1, \cdots, \mathtt{SNil})))\ \mathtt{with}\ \cdots
\end{aligned}$$

遅延契約検査

$$\langle \mathrm{T}_1 \Leftarrow \mathrm{T}_2 \rangle^{\ell} @ \mathrm{e}$$

- 必要とされるまでデータ型キャストを遅延
  - match の対象となったときに型変換を実行

$$\begin{aligned}
& \texttt{head}\ (\langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell}\ (\texttt{SCons}(1, \cdots, \texttt{SNil}))) \\
\longrightarrow\ & \texttt{head}\ (\langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell} @ (\texttt{SCons}(1, \cdots, \texttt{SNil}))) \\
\longrightarrow\ & \texttt{match}\ (\langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell} @ (\texttt{SCons}(1, \cdots, \texttt{SNil})))\ \texttt{with}\ \cdots \\
\longrightarrow^{*}\ & \texttt{match}\ \texttt{Cons}(1, \langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell} @ (\texttt{SCons} \cdots))\ \texttt{with}\ \cdots
\end{aligned}$$

遅延契約検査

$$\langle \mathrm{T}_1 \Leftarrow \mathrm{T}_2 \rangle^{\ell} @ \mathrm{e}$$

- 必要とされるまでデータ型キャストを遅延
  - match の対象となったときに型変換を実行

$$
\begin{aligned}
& \texttt{head}\ (\langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell}\ (\texttt{SCons}(1, \cdots, \texttt{SNil}))) \\
\longrightarrow\ & \texttt{head}\ (\langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell} @ (\texttt{SCons}(1, \cdots, \texttt{SNil}))) \\
\longrightarrow\ & \texttt{match}\ (\langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell} @ (\texttt{SCons}(1, \cdots, \texttt{SNil})))\ \texttt{with}\ \cdots \\
\longrightarrow^{*}\ & \texttt{match}\ \texttt{Cons}(1, \langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell} @ (\texttt{SCons} \cdots))\ \texttt{with}\ \cdots \\
\longrightarrow\ & 1
\end{aligned}
$$

遅延契約検査の性質

定理

1. $\mathsf{e} \longrightarrow^{*} \mathsf{c}$ **ならば** $\mathsf{e} \longrightarrow_{d}^{*} \mathsf{c}$
2. $\mathsf{e} \longrightarrow_{d}^{*} \Uparrow \ell$ **かつ** $\mathsf{e} \longrightarrow^{*} \mathsf{e}' \not\longrightarrow$ **ならば** $\mathsf{e}' = \Uparrow \ell'$

- $\longrightarrow_{d}$: **遅延契約検査の評価関係**

遅延契約検査の実用化

いくつかのデザインチョイスが考えられる

- プログラマが正格・遅延検査を選択
  - Racket などと同じ
- 成功するキャスト（アップキャスト）だけ遅延化許可
  - 「厳しい契約付きのデータ型」から「緩い契約付きのデータ型」へのキャスト
    - ✓ $\langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell}$
    - × $\langle \texttt{slist} \Leftarrow \texttt{int list} \rangle^{\ell}$

遅延契約検査の実用化

いくつかのデザインチョイスが考えられる

- **プログラマが正格・遅延検査を選択**
  - Racket **などと同じ**
- **成功するキャスト (アップキャスト) だけ遅延化許可**
  - **「厳しい契約付きのデータ型」から「緩い契約付きのデータ型」へのキャスト**
    - ✓ $\langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell}$
    - × $\langle \texttt{slist} \Leftarrow \texttt{int list} \rangle^{\ell}$

遅延契約検査の実用化

いくつかのデザインチョイスが考えられる

- プログラマが正格・遅延検査を選択
  - Racket などと同じ
- 成功するキャスト (アップキャスト) だけ遅延化許可
  - 「厳しい契約付きのデータ型」から「緩い契約付きのデータ型」へのキャスト
    - ✓ $\langle \texttt{int list} \Leftarrow \texttt{slist} \rangle^{\ell}$
    - × $\langle \texttt{slist} \Leftarrow \texttt{int list} \rangle^{\ell}$

まとめ

本研究の内容

- 契約付き代数的データ型を顕在的契約計算に導入
  - データ型による実行時検査機構の提案
- 遅延契約検査の導入
- 実装

今後の課題

- 静的契約検査との組合せ
- 篩型から代数的データ型の系統的導出
- 交差型によるデータ型の結合
- データ構築子選択機構のより実用的実装

篩型の問題

不要な実行時検査の実施

$$\texttt{let f (x:slist')} = \ldots \langle \texttt{slist'} \Leftarrow \texttt{int list} \rangle^{\ell} (\texttt{Cons(y,x)}) \ldots$$

$$\texttt{slist'} = \{\texttt{x:int list} \mid \texttt{sorted x}\}$$

- x は昇順であるにも関わらず再度実行時検査

代数的データ型による解決

不要な実行時検査の実施

```
  let f (x:slist') =
  ... ⟨slist' ⇐ int list⟩^ℓ (Cons(y,x)) ...

type slist =
  | SNil
  | SCons of
      x:int × {xs:slist | empty xs || x ≤ head xs}
```

- 次のいずれかが成り立つかだけ検査
  - x が空
  - x の先頭要素が y 以上