58 Information Systems Engineering

形式手法にもとづくソフトウェアの設計、検証、開発

情報システム工学講座
准教授 中村 正樹

研究分野

ソフトウェア工学、理論計算機科学、書き換え系

研究内容

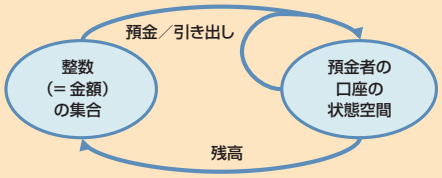
数学的に明確で厳密な意味を持つ言語を用いて、高信頼なソフトウェアを開発する技術である形式手法の研究をしています。特に、書き換えに基づく仕様実行、検証の技術に興味を持っています。

私の研究のポイント

国産の形式仕様言語である代数仕様言語CafeOBJの開発プロジェクトに参画し、特に仕様検証に適した代数仕様の作成手法についての研究成果を得ました。代数仕様の検証においては等式推論が核となります。自動化に向かない双方向性を持つ等式を，コンピュータが扱いやすい左から右へ方向付けられた書き換え規則とみなす書き換え理論を応用しました。今後はそれらの技術を実装し、仕様作成者を支援するツールの開発を目指します。

REPORT リポート

代数仕様による銀行口座の設計を考えます。預金するお金を整数の集合でモデル化し、銀行口座の状態に対して、そのときの残高確認や預金／引き出し操作を集合上の関数として定義します。



このモデルに基づきCafeOBJで仕様を記述し（左下）、書き換え理論に基づく等式推論を核に、場合分けや帰納法などの証明技術を組み合わせて検証します。右下は、連続する預金を入れ替えても残高が変わらないことの証明です。

```
mod* ACCOUNT{
  pr (INT) *     [ State ]*
 op   init   : -> State
 op balance_ : State ->          Int
 op withdraw_ _ :        Int   State -> State
...        var  S : State        var  X :    Int
   eq balance(    init    ) = 0 .
 ceq  balance (withdraw X S) =
(balance S)  - X  if balance S >= X
and X >= 0 .
  ...
}
```

```
%PROOF> eq (x >= 0) = true .
%PROOF> eq (y >= 0) = true .
%PROOF> red balance (deposit x (deposit y s)) = balance (deposit y
%PROOF> eq (x >= 0) = true .
%PROOF> eq (y >= 0) = false .
%PROOF> red balance (deposit x (deposit y s)) = balance (deposit y
%PROOF> eq (x >= 0) = false .
%PROOF> eq (y >= 0) = true .
%PROOF> red balance (deposit x (deposit y s)) = balance (deposit y
%PROOF> eq (x >= 0) = false .
%PROOF> eq (y >= 0) = false .
%PROOF> red balance (deposit x (deposit y s)) = balance (deposit y
(deposit x s)) .
(true):Bool
```