形式手法を用いたソフトウェア・プロダクトラインの研究

Software Product Line Engineering with Formal Methods

中島　震　Shin NAKAJIMA
鵜林 尚靖（九工大）　Naoyasu UBAYASHI

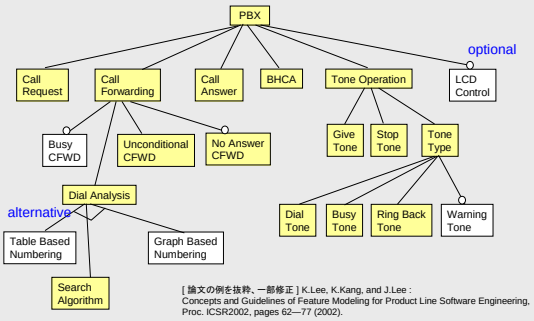
何がわかる？

「信頼できる（ディペンダブル）」とは使う側が期待する振る舞いを示すことです。ソフトウェアは稼動環境や利用者を含むオープンなシステムの一部になるため、何をどこまで期待できるかは難しい問題です。さらに、それをどのように表現し確認するかが課題です。形式手法と呼ばれる技術をどのように使えば効果的であるかをあきらかにします。

どんな研究？

形式手法は数理論理学の基礎的な裏付けがある言語を用いるため難しいと云われます。実際は、ロジックの知識は初歩で十分で、問題を整理する「モデリング」が難しさの根源です。対象の問題を吟味し、ちょっとした工夫を加えることで、形式手法がソフトウェア工学の道具として役立つことを具体例で示します。

内容



[論文の例を抜粋、一部修正] K.Lee, K.Kang, and J.Lee : Concepts and Guidelines of Feature Modeling for Product Line Software Engineering, Proc. ICSR2002, pages 62—77 (2002).

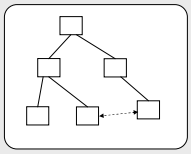
フィーチャ指向ドメイン分析 (Kang et al, 1990)

- ソフトウェアプロダクトライン工学 (SPLE) の代表的な手法
- フィーチャダイアグラム (FD) を用いた共通フィーチャと可変フィーチャの分析技法
- FD ⇒ プロダクトファミリの表現が可能（可変フィーチャの組み合わせ）

与えられたFDの整合性と妥当性を自動検査

- プリミティブ関係を命題論理で表現するとFDは論理式の集まり
- 「検査」は論理式中の命題変数の真偽値を求めること　$m \models G$

Alloy を利用する自動検査の方法



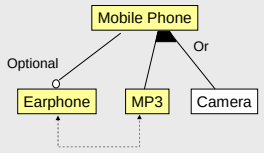
フィーチャー・ダイアグラム

⇒ 命題論理式の集まり　G

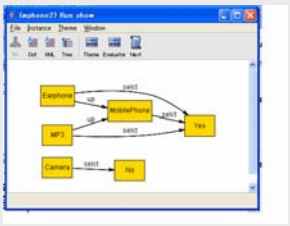
⇒ Alloy記述

```
abstract sig Feature {
  up : set Feature, selct : Selected
}
fact { no f : Feature | f in f.^up }

one sig A0 extends Feature {}{ no up }
one sig B1 extends Feature {}

fact {
  (A0.selct = Yes) => ( … ) else ( …)
  …
}

run { A0.selct = Yes }
```

Alloy自動解析 ⇒ 生成モデル　$m \in M$



Earphone ⇒ MobilePhone
MobilePhone ⇔ MP3 ∨ Camera
Earphone ⇔ MP3



FDを作成するモデリングのガイドライン

九工大大学院（修士課程）での実習経験から整理

最近の発表

研究論文

N. Ubayashi and S. Nakajima : Context-aware Feature-Oriented Modeling with an Aspect Extension of VDM, Proc. SAC'07, pages 1269—1274 (2007).
S. Nakajima and N. Ubayashi: Light-weight Formal Analysis of FODA Feature Diagrams, Proc. 4th RISE, pages 3—18 (2007).
中島震 : 代数仕様言語Maudeを用いた制約オートマトンの実現, 情報処理学会論文誌, Vol.48 No.10, pages 3341—3351 (2007).

著書

中島震 : SPINモデル検査ー検証モデリング技法, 近代科学社 (2008).

解説・セミナー講演

中島震 : ソフトウェア工学の道具としての形式手法, ソフトウェアエンジニアリング最前線2007, pages 27—48 (2007). 改訂版NII TR.
中島震 : ソフトウェア・エンジニアリングは工学か?, 茨城大学イブニングセミナー 2008年5月1日.
中島震 : 形式手法の潮流ーアーキテクチャへの関心, システム/制御/情報, 掲載予定 (2008).

関連

日本学術振興会　科学研究費補助金　基盤研究（C）「代数仕様を用いた要求モデルの自動検査に関する研究」
NII共同研究（企画型）「形式手法を用いたソフトウェア・プロダクトラインの研究」
NIIグランドチャレンジ「ソフトウェア　ー　ディペンダブルソフトウェア技術」

NII　連絡先：　中島 震（Shin　NAKAJIMA）／ 国立情報学研究所　アーキテクチャ科学研究系　教授
TEL：03-4212-2507　　FAX：03-3556-1916　　Email：nkjm@nii.ac.jp