CafeOBJ による B-抽象機械の検証法に関する研究

梅原 伸年

北陸先端科学技術大学院大学 情報科学研究科

1998 年 2 月 13 日

キーワード: B-Technology, 無矛盾性, 隠蔽代数, 段階的詳細化, 投影演算.

1 はじめに

近年コンピュータの進化によりソフトウェアの応用範囲が広がっている。ソフトウェアは大規模化し、高信頼性が求められるようになった。そこで開発の初期の段階、すなわち仕様表現の重要性がいわれるようなった。現在、信頼性を提供する手段としていくつかの形式仕様言語が提案されている。しかし形式仕様言語の開発現場での導入は進んでいない。そのなかで B-Technology(以降 B とする) を用いた開発が評価を得ている。その大きな理由として現在一般的となったオブジェクトを基にした開発アプローチのサポートがあげられる。一般にシステムの仕様を作成するとき、その振る舞いにより状態を規定することで問題を表現できる場合は多い。B は仕様作成において状態と操作からなる抽象機械を構成単位としており、これは様々な問題の仕様作成に対して B の利用が有効であるともいえる。このことから B に着目し、開発を進めるの手本とした。
本研究は CafeOBJ が基礎とする幾つかの論理のうちで特に隠蔽代数に注目し、設計が有効に行えることを示すものである。CafeOBJ の仕様を事例に基づいて記述した例は少なく、形式仕様言語として様々な事例に対応できる適応力を示すことは必要とされている。また段階的な仕様の詳細化を扱う事例は隠蔽代数を提唱した Goguen らも進めているが数は多くない。本研究で行ったモデル指向の言語を代数で記述した研究は幾つかあるが、モデル指向の言語を用いた開発手法に対する代数仕様の研究を扱う物は少ない。本研究では仕様の実行が可能であること、複数の論理を基礎としていることから代数仕様言語の中で CafeOBJ を利用する。

2　研究構成

2.1　CafeOBJ による B 抽象機械表現

モデル指向の B 抽象機械表現が 代数指向の CafeOBJ によりどのように表現することが出来るか対応を考察しテーブルを作成した。状態と操作で表現されるようなシステムの CafeOBJ の仕様を作成する指針を得るために B 抽象機械の状態への操作の記述に特に注目した。そして B 仕様に存在する個々の操作の影響範囲の把握が難しい問題を解決する必要を挙げ、解決法として内部状態を表現するソートを用い仕様を記述することを指針として与えた。

2.2　CafeOBJ による 仕様の無矛盾性の証明

B の開発手法である仕様の無矛盾性に関する考察を行った。
仕様の無矛盾性の証明は
(1) パラメタの存在可能性、
(2) 定数や集合の存在可能性、
(3) 制約を満たす変数の存在可能性、
(4) 制約を満たす初期化の実行可能性、
(5) 制約を満たす演算の実行可能性を証明している。
これらの証明が CafeOBJ 上でどのように対応するかを考察し、証明を実行可能な機能を用いて示した。

2.3　CafeOBJ による 仕様の無矛盾性の証明

また B の開発手法が定義する抽象機械の詳細化の際の無矛盾性の証明は
(1) 詳細化前仕様と詳細化仕様両方の不変条件を満たすような状態が実現可能であるか、
(2) 具体化された初期化が詳細化前仕様の制約を満たしているか、
(3) 具体的に定義された操作に対して同じ初期状態において得られる結果が等しいかどうかの証明である。
特に (3) の同じ結果が得られるかを示すことが CafeOBJ の詳細化に対する証明である。これをまた実行可能な機能を用いて証明した。

2.4　事例研究

最後に中規模の有名問題であるリフトの仕様を事例として利用し、検証に関する考察を行った。具体的に隠蔽代数を用いたシングルリフトの事例を考察した。隠蔽代数を利用す

ることで振る舞いのみに着目した詳細化前の仕様を記述し、状態遷移に関する性質が保存され詳細化後も同様に振る舞うかを検証した。また投影演算と隠蔽代数を用い振る舞いを記述したマルチリフトの事例を考察した。この事例において個々のリフトへの操作が独立に実行可能であることを検証し、振る舞い仕様で記述された仕様が検証を容易にできることを示した。

3 まとめ

B 抽象機械表現を CafeOBJ で実現できることを示すことにより CafeOBJ がシステム状態と状態の上の操作で表現されるような問題に対し十分な記述力を持つことが示せた。内部状態を変更するような操作の記述に関して新しいソートを用いる指針を与えることで、操作がもつ性質を検証する際、考慮すべき部分仕様を得るための情報を仕様から容易に得ることができた。
CafeOBJ 上で B-Method で与えられる仕様の無矛盾性の証明と詳細化の時に性質が保存されていることの検証を行うことで B がもつ開発手法が同様に CafeOBJ で実践できることを示した。このことより CafeOBJ が仕様を記述するだけでなく仕様を詳細化する段階的な開発に利用できること示した。

B の特徴である Case Study で利用される LIFT の事例を CafeOBJ で記述し実際に詳細化を行った。その際隠蔽代数を用いた仕様からの詳細化を行い、代数を用いた仕様で具体的データの詳細化が行えるだけでなくシステムの振る舞いに関する性質が保存されることを示した。
また投影演算と隠蔽代数を用いた事例により、内部システムに対する操作の並行性を検証し、性質を保存した詳細化仕様が作成できることを示すことで検証が容易にできることを示した。これにより検証を目的の抽象レベルで行い、求める性質に関与しない他の部分を隠蔽することで、大規模システムの性質の検証において問題になる状態爆発を回避できる可能性を示すことができた。