2013 年 2 月 12 日
株式会社日立製作所

社会インフラシステム向けの高信頼で高効率なソフトウェア開発技術を公開

安全性やセキュリティ確保に適した「形式手法」の適用工数を約 8 割削減

株式会社日立製作所(執行役社長:中西　宏明／以下、日立)は、スイス連邦工科大学チューリッヒ校、および Hitachi India Pvt. Ltd. (社長:飯野　一郎)と共同で、社会インフラシスシステム向けの大規模なソフトウェアに適用可能な、高い信頼性と効率を実現する形式検証支援ソフトウェアを開発しました。開発したソフトウェアには、高品質なソフトウェアを論理学や数学などに基づいて開発するために利用される「形式手法」という技法で作成されたモデルを、再利用できる技術を用いています。日立では、このソフトウェアを用いて開発を行った場合、形式モデルの開発工数を約 8 割削減できることを確認しています。日立は、実適用に向けて本技術の改良を進めるために、2013 年 2 月 12 日から本ソフトウェアをオープンソースとして公開します。

エネルギー、公共、鉄道などの社会インフラシステムでは、高いレベルの信頼性を確保しながら、システムの大規模化、複雑化に対応できる効率的なソフトウェア開発技術が必要とされています。近年では、「形式手法」という技法が、安全性やセキュリティを必要とする高品質のソフトウェア開発技術として注目され、国際標準規格において利用が推奨されています。形式手法は、ソフトウェアの設計仕様に相当する形式モデルを作成する度に検証するため、ソフトウェアの高信頼性を保つことができますが、そのために検証作業工数が多くなり、開発期間が長くなってしまうことが課題となっていました。そこで今回日立は、あるシステムに対して形式手法を用いて作成したモデルを、検証された状態を保ったままテンプレート化することで、類似する他のシステムに再利用できる技術を開発しました。これにより、検証作業に要する時間が減少し、開発期間を短縮することが可能になりました。

開発した形式検証支援ソフトウェアの特長は以下のとおりです。

(1)定理証明法を利用した形式手法 Event-B の拡張機能として開発

今回日立が開発したソフトウェアは、Event-B[*1] をベースにしています。これは、設計記述が要件を満たしていることを数学的に証明する検証法(定理証明法[*2])を利用する代表的な手法であり、大規模システムにおけるソフトウェア品質の検証を効率的行うことができます。

(2)テンプレート化された検証済み形式モデルの再利用を実現

一度設計し、数学的に品質が検証されたモデルをテンプレート化し、類似した他のシステムの開発に再利用できる技術を開発しました。これにより、モデルの検証工程を削減することができ、一からモデルを生成し、設計仕様を検証する場合に比べ、形式モデル開発に要する作業工数を約 8 割削減できました[*3]。

日立は、今回開発した形式検証支援ソフトウェアの実適用に向けた改良を進めるために、本ソフトウェアを、本日（2013 年 2 月 12 日）からオープンソースとして公開します。

今後、社会インフラを支える高信頼システムの効率的な開発に向け、形式手法適用技術の研究開発に継続的に取り組んでいきます。

■オープンソースの公開サイト

http://sourceforge.net/projects/gen-inst/

■用語等

*1 Event-B：EU プロジェクトで ETH 大他が開発した代表的な形式手法で定理証明法に基づく手法のひとつ。特にシステム開発の上流工程におけるモデリングなどに適した手法。鉄道、自動車、企業情報システムなどの開発に適用された事例も報告されている。

*2 定理証明法：形式手法の代表的な検証法の一種で、設計記述が要件を満たしていることを一階述語論理などの数学的な基盤に基づきコンピュータを使って証明する方法。証明作業の一部は、人間がおこなう必要があるが、コンピュータリソースの制約を受けず、大規模なシステムであっても検証できる。

*3 当社試算による。社内のプロジェクトを題材とした適用評価において、あらかじめ証明済みの汎化形式モデルから具体形式モデルを生成したところ、生成されたモデル上で必要な証明項目のうち約8割を再利用することができた。

■「形式検証支援ソフトウェア」の詳細

本形式検証支援ソフトウェアは、Generic Instantiation と呼ばれるモデルの再利用技術を使用しています。Generic Instantiation とは、汎化形式モデルと呼ばれるテンプレートを活用して、目的の形式モデルを生成する技術です。Generic Instantiation では、汎化形式モデルが含む特定の記号をパラメータとして扱います。このパラメータをユーザが設定した別の（より具体的な意味を持つ）記号と置き換えることで、目的のモデルを生成します。生成したモデルは、汎化形式モデルと対比して具体形式モデルと呼ばれます。今回開発した形式検証支援ソフトウェアは、上記汎化形式モデルとそのパラメータに対する設定を入力として受け付け、目的の具体形式モデルを生成する機能を備えます。このように、汎化形式モデルをテンプレートとして再利用することでモデル記述量を大幅に削減できるという利点があります。

さらに Generic Instantiation は、汎化形式モデルの正当性証明を事前に完成しておくことで、生成した具体形式モデルにおける証明の大部分を省略することができます。ただし証明の省略のためには、パラメータに設定する記号が特定の制約条件を満たす必要があります。今回、形式手法 Event-B 向けに、具体形式モデルに対する正当性証明が省略できるための制約条件を明らかにしました。開発した形式検証支援ソフトウェアは、パラメータへの設定としてユーザが入力した記号が上記制約条件を満たすかを検査する機能を備えています。そして、上記制約条件を満たす場合のみ具体モデルを生成する仕様になっています。

■照会先

株式会社日立製作所 横浜研究所 企画室 [担当:吉田]
〒244-0817 神奈川県横浜市戸塚区吉田町 292 番地
電話 045-860-3092(直通)

以上