

発表概要

契約による設計を支援する表明記述の
アスペクト指向的モジュール化方式山田 聖[†] 渡部 卓雄^{††}

契約による設計 (Design by Contract, DbC) は、ある処理の実行直前・直後で満たされるべき条件を表明として明示し、それらを処理の利用者と提供者の間の契約とすることで、責任の切り分けを明確にする。DbC に基づく表明の記述では、プログラムが大規模化するとともに、表明の数が増加し個々の表明も複雑になり、表明の整合性や表明とプログラムの一貫性を維持しつつ、それらを修正・拡張することが難しくなる。この原因は、従来の DbC に基づく表明の記述方式では、表明をプログラムに埋め込む形で記述するため、表明の記述をプログラムの構造から独立にモジュール化できないことにある。そこで我々は、DbC に基づく表明の記述をアスペクト指向的にモジュール化する方式を提案する。本発表の概要は以下のとおりである。まず背景として、Java で実装された電子メールメッセージを扱うライブラリと、その実装の JML (Java Modeling Language) による検査について説明する。JML は Java を対象とした DbC のための表明記述を可能にする言語である。次に、この検査の過程で問題となった表明記述の記述量の増加について述べるとともに、この問題に対処する、我々が提案する表明の記述をアスペクト指向的にモジュール化する方式についての説明を行う。その後、JML と本方式との比較を行い本方式の優位性を述べ、さらに今後の展開として、モジュール化された表明の記述から状態遷移モデルを生成する方式について述べる。

Aspect-oriented Modularization of DbC Assertions

KIYOSHI YAMADA[†] and TAKUO WATANABE^{††}

In Design by Contract (DbC) facility, we explicitly specify conditions as assertions for each procedures which must hold just before/after a procedure execution, and consider them to be a contract between procedures and it's users. This makes clean who is responsible for problems of a procedure execution. The more the scale of a program grows up, the more Description of assertions based on DbC complicated, because number of assertions increases and complexity of each assertions are increased. Hence it becomes difficult to modify and/or extend programs and assertions without lose consistency between them and coherence of assertions. The reason of this problem is that we cannot modularize description of assertions independent of program structure, because in the way to describe assertions based on DbC, assertions must be embedded in the programs. So we propose an aspect-oriented modularization technique for the description of assertions based on DbC. In this technique, we think of assertion as advice, location to check the assertion as join point, and the set of them as aspect. This technique makes modularization technique for the description of assertion flexible. In this presentation, we show the implementation of Maildir Folder Service Provider we developed, which manages E-mail messages in Java, and we describe a test of this implementation using Java Modeling Language (JML) which extends java to be able to describe assertions base on DbC. Next, we show the problems for increasing of description of assertions in the test process, and propose aspect-oriented modularization technique for description of assertions. And then, we compare this technique with JML and show this method is more preferable. And finally, we show a method to generate state transition models from a modularized description of assertions.

(平成 16 年 10 月 21 日発表)

[†] 北陸先端科学技術大学院大学情報科学研究科

School of Information Science, Japan Advanced Institute of Science and Technology

^{††} 東京工業大学情報理工学研究所

Graduate School of Information Science and Engineering, Tokyo Institute of Technology