Kivonat

Modellvezérelt tervezés során egy mérnöki modellből modelltranszformáció segítségével egy matematikailag precíz analízis modellt származtatunk, melyen már a fejlesztés korai szakaszában elkezdődhet a rendszer helyességellenőrzése. A gráftranszformációk paradigmája egy intuitív és egyben precíz formális módszert ad e modelltranszformációk specifikációjára. A modelltranszformációkban lévő hibák viszont érvénytelenné tehetik a matematikai modell precizitásából származó előnyöket, így a modelltranszformációk hibamentességének biztosítását célszerű formális verifikációval garantálni.

Valós informatikai rendszerek gyakran potenciálisan végtelen állapottérrel rendelkeznek, amely a formális verifikáció egyik legkomplexebb esete, hiszen a kimerítő állapottér-bejárás közvetlenül nem lehetséges. Így az ellenőrzés végrehajtásához szükséges valamilyen absztrakció alkalmazása. A forma (shape) analízis módszere egy ilyen absztrakciós technikát ad meg. Ennek során gráf alapú modelljeinket ekvivalencia osztályokba soroljuk, és ezeket címkézett gráfok speciális halmazával, formákkal ábrázoljuk. A gráftranszformációs lépések absztrakt megfelelőjét végigvezetve a formákon biztosan véges állapotteret kapunk, melynek analízisével bizonyíthatjuk a gráftranszformációs rendszer helyességét.

Dolgozatom célja, hogy egy egyesített, jól paraméterezhető, gráfelemek ekvivalencia relációján alapuló forma analízissel megteremtsem a lehetőséget arra, hogy a szakirodalomban leggyakrabban használt módszereket keverve vagy egyszerre lehessen alkalmazni, így növelhető legyen azok hatékonysága. Az eljárás egyik legfontosabb és egyben leggyakrabban használt részfeladatai a formák levezethetőségének és ellentmondásosságának felfedése, így ezek végrehajtása kutatásra érdemes terület.

Dolgozatomban megadok egy ekvivalencia relációkkal parametrizálható általános formázási módszert, amellyel figyelembe vehető a bizonyítandó követelmény specifikus tartalma. Leírok egy automatikus módszert a formákon végrehajtandó transzformációs lépés kiszámítására és a formák konzisztenciaellenőrzésére, amely gráfmintaillesztési technikák, ontológiai lekérdezések és dedikált tételbizonyítók kombinált felhasználásán alapul. Fenti módszerek implementációjára architektúrát és megvalósíthatósági tanulmányt adok, mely korszerű szoftverkomponensek (VIATRA2, Pellet és Prover9) felhasználásán alapul.

Mindezekkel egy olyan bővíthető architektúrát adok meg, amely képes létező forma analíziseket és következtető módszereket integráltan alkalmazni. Így elérhető, hogy a kombinált módszer többfajta követelmény bizonyítására legyen képes.

Abstract

In model-driven development, a mathematically precise analysis model is frequently derived from an engineering model by model transformations in order to carry out the formal verification of the system already in an early phase of design. The paradigm of graph transformations offers an intuitive yet formal technique to specify model transformations. However, model transformation errors can invalidate the results of a formal analysis of the mathematical model, so it is advantageous to guarantee the correctness of model transformations by formal verification.

As complex information systems usually have infinite state space, we need to face one of the most complex cases of formal verification since the exhaustive traversal of every possible state is impossible. To tackle this, it is necessary to apply some kind of abstraction in the verification process as provided, for instance, by shape analysis, which categorizes graph based models into a finite number of groups which are represented by a special set of labeled graphs called shapes. Applying the abstract equivalent of graph transformation rules on shapes an abstract but finite state space is obtained, on which one can reason about the correctness of graph languages.

The objective of my report is to enable the combined application of advanced techniques in the literature of shape analysis by proposing a unified, parametrizable shape analysis technique. Here, the most challenging step is to deduce derived properties from shapes and to find their inconsistencies.

In the current report, I define a general method parametrizable by equivalence relations, which is specific to the property to be verified. I propose an automated process to execute the transformation steps on shapes and check their consistency based on combined use of graph pattern matching, queries over ontologies, and dedicated theorem provers. In order to implement this process, I give an architecture and carry out a feasibility study using advanced, state-of-the-art software components (such as VIATRA2, Pellet and Prover9).

The main advantage of this framework is to provide an extensible architecture integrating and combining existing shape analysis and deductive techniques, which allows the verification of a wide range of correctness properties.