Kivonat

Modellvezérelt tervezés során az alkalmazási terület fogalmainak és összefüggéseinek leírására széles körben használnak szakterület-specifikus nyelveket (Domain-Specific Language, DSL). A DSL-ek segítségével automatikusan származtathatunk egy ellenőrzött rendszermodellből teszteseteket, vagy bizonyíthatóan helyes forráskódot. Azonban maguk a DSL nyelvek is tartalmazhatnak tervezési hibákat, melyek érvényteleníthetik a rendszermodellen végzett vizsgálatok eredményeit. A dolgozat fő célja, hogy olyan eszközt biztosítsunk, amellyel formális analízist végezhetünk szakterület-specifikus nyelveken, fényt derítve a DSL specifikációk ellentmondásaira és többértelműségére.

A szakterület-specifikus nyelvek konzisztencia-vizsgálata komoly kutatási kihívást jelent, mert (i) az összetett DSL-eken történő logikai következtetés algoritmikusan eldönthetetlen probléma, (ii) további elméleti nehézségei vannak a hozzáadott jólformáltsági kényszerek és a származtatott értékek kezelésének, és (iii) olyan eszköz fejlesztésére van szükség, amit a következtetési eljárás ismerete nélkül is használhat a nyelv tervezője.

A TDK dolgozatunkban egy egységes keretrendszert javasolunk a szakterület-specifikus nyelvek konzisztenciavizsgálatára a következő módon: (i) A jólformáltsági kényszereket és származtatott érték definícióját egységesen elsőrendű logikai kifejezésekké fordítjuk, amelyeken SMT megoldókkal végzünk következtetéseket. (ii) Approximációs technikákat alkalmazva egy hatékonyan elemezhető logikai fregmensbe képezzük az komplexebb nyelvi elemeket. (iii) A validációs eszközünket ipari modellező eszközhöz integráltuk, amely az ellentmondásokat a nyelv szabványos példánymodelljeiként állítja elő.

Módszerünk magja egy olyan leképezésen alapszik, amely egy származtatott attribútumokkal és relációkkal gazdagított EMF metamodellt, OCL vagy EMF-IncQuery nyelven definiált jólformáltsági kényszereket és egy hiányos kezdeti példánymodellt vár bemenetül. Az eszköz a kezdeti modellt kiegészíti új elemek felvételével a generált axiómák és a Z3 SMT megoldó által ismert elméletek alapján, úgy, hogy az eredmény megfeleljen a nyelv specifikációjának.

Az eszközünket két ipari követelményekkel rendelkező esettanulmányon is sikerrel alkalmaztuk. Egy brazil repülőgépgyártóval közös projektben EMF-IncQuery gráfmintákkal megfogalmazott származtatott értékekkel és jólformáltsági kényszerekkel gazdagított EMF metamodell konzisztencia vizsgálata volt a cél, hogy a fejlesztés korai szakaszában detektáljuk a nyelv hibáit. Az R3COP ARTEMIS esettanulmányban biztonságkritikus autonóm rendszerek (pl. ipari robotok) tesztelésének támogatása a cél, ahol az eszközünk feladata a konkrét tesztesetek előállítása volt az OCL kényszerekkel meghatározott absztrakt tesztleírások alapján.

Abstract

Complex design environments based on Domain-Specific Languages (DSLs) are widely used in various phases of model driven development from specification to testing in order to capture the main concepts and relations in the application domain. A precise system model captured in a DSL enables formal analysis and automated code or test generation of proven quality. Unfortunately, the specification of DSL may itself contain conceptual flaws, which invalidates the results of subsequent formal analysis of the system model. The main objective of the current report is to provide formal analysis of a DSL itself to highlight inconsistency, incompleteness or ambiguity in DSL specifications.

However, the consistency analysis of DSLs is a difficult task due to (i) decidability problems of handling complex DSLs, (ii) theoretical challenges of supporting well-formedness constraints and derived features, and (iii) the engineering problem of providing a DSL validation tool that is operable by the DSL developer without any extra validation skills.

In this report, we address these challenges by providing (i) a mapping of well-formedness rules and derived features formulated in different constraint languages into first-order logic theories processed by SMT-solvers, (ii) powerful approximations to map complex structures into an efficiently analyzable fragment of first order logic, and (iii) a DSL validation tool seamlessly integrated into industrial modeling frameworks (EMF) where inconsistencies retrieved by SMT-solvers are available as regular DSL instance models.

Our DSL validation framework is based on a mapping, which takes an EMF metamodel with derived features, a set of well-formedness constraints (captured in OCL or graph patterns of EMF-IncQuery) and a partial model as input. This partial model is completed by introducing new model elements to it which are compliant with the DSL specification using the generated axioms and underlying theories of the Z3 SMT-solver in the background.

We report on successful use of our validation framework in two complex case studies with industrial requirements. In a collaborative project with a Brazilian airframer, the consistency of EMF metamodels augmented with well-formedness constraints and derived features defined by IncQuery graph patterns is checked to detect design flaws in the early phase of the DSL development. The case study of the R3COP ARTEMIS project that aims to develop safety critical autonomous systems like industrial robots. Our validation framework supported the automatic generation of concrete test cases from abstract test properties defined in standard OCL.