Model Checking für Erlang Programme – Ein Überblick

Frank Huch
RWTH Aachen
Lehrstuhl für Informatik II

huch@i2.informatik.rwth-aachen.de

In diesem Vortrag wird ein Überblick über einen Ansatz für die formale Verifikation von Erlang Programmen mittels Model Checking und Abstraktion gegeben. Im allgemeinen ist Model Checking für interessante Logiken und Erlang Programme unentscheidbar. Es wird ein Framework für abstrakte Interpretationen von Erlang Programmen definiert, in dem es möglich ist dennoch Eigenschaften von Erlang Programmen zu beweisen. Die Abstraktion ist sicher in dem Sinne, daß alle Pfade des ursprünglichen Systems erhalten bleiben. Betrachten wir Formeln, welche auf allen Pfaden eines System gelten sollen, wie z.B. in Linear Time Logic (LTL), so gilt eine Formel, welche im Abstrakten System bewiesen ist, auch im wirklichen System. Für eine große Klasse von Erlang Programmen und Abstrakten Interpretationen mit endlichem Definitionsbereich, bildet die abstrakte operationelle Semantik ein endliches Transitionssystem. Außerdem wurde im letzten Jahr zusätzlich eine Abstraktion von nicht-endrekursiven Funktionsaufrufen vorgestellt, welche für eine größere Klasse von Erlang Programmen ein endliches Transitionssystem erzeugt. Für diese endlichen Transitionssystem kann dann automatisch mittels Model Checking entschieden werden, ob sie eine in LTL ausgedrückte Eigenschaft erfüllen.

In diesem Vortrag wird zunächst ein Überblick über den Ansatz gegeben. Anschließend werden spezielle Probleme aufgezeigt, welche sich aus der Abstraktion ergeben. Hierbei wird insbesondere auf das Beweisen der Deadlockfreiheit eines Systems und das Entscheiden von abstrakten Propositionen eingegangen. Abstrakter Propositionen, welche in konkreten Zuständen gelten, erfüllen Propositionen in den LTL-Formeln nur unter bestimmten Voraussetzungen. Speziell die Negation in den LTL Formeln muß hierbei mit Vorsicht behandelt werden.