Dirk Seifert: Automatisiertes Testen asynchroner nichtdeterministischer Systeme mit Daten

Promotion: Technische Universität Berlin
Datum der Prüfung: 20. Juli 2007
Veröffentlichung: Shaker Verlag Aachen

Erstgutachter: Prof. Dr. Stefan Jähnichen
Zweitgutachter: Prof. Dr. Ina Schieferdecker
Drittgutachter: PD Dr. Thomas Santen

Eingebettete Systeme setzen sich aus Hardware- und Softwarekomponenten zusammen, die asynchron miteinander kommunizieren und nichtdeterministisches Verhalten aufweisen können. Dies macht eine umfassende und systematische Prüfung mit manuellen Techniken nahezu unmöglich. Auch automatisierte Prüftechniken können mit Asynchronität und Nichtdeterminismus bislang nur unzureichend umgehen. Der breite Einsatz eingebetteter Systeme im täglichen Leben und das blinde Vertrauen in deren Funktionsfähigkeit erfordern jedoch eine zuverlässige und umfassende Qualitätssicherung.

Die Dissertation beschäftigt sich mit dem automatisierten Testen asynchroner nichtdeterministischer Systeme mit Daten. Zur Beschreibung des reaktiven Verhaltens von Komponenten technischer Systeme werden Zustandsmaschinen der *Unified Modeling Language* in reduzierter Form verwendet. Ausgehend von einer solchen Zustandsmaschine werden automatisiert Testfälle für einen Konformitätstest abgeleitet und gegen das zu testende System ausgeführt. Das korrekte, mögliche Verhalten wird für ausgewählte Eingaben a priori berechnet und in einem Testfall gespeichert. Der Hauptbeitrag der Arbeit liegt einerseits in der vollständigen Formalisierung der reduzierten Zustandsmaschinen, die die wesentlichen syntaktischen Ausdrucksmittel und komplex strukturierte Daten umfassen, und andererseits in der Entwicklung eines praktikablen Ansatzes zum automatisierten Testen reaktiver technischer Systeme, deren Verhalten durch solche Zustandsmaschinen beschrieben werden kann. Das Testen solcher Systeme ist aus zwei Gründen eine besondere Herausforderung. Einerseits ist die Anzahl möglicher Eingabesequenzen und damit die Anzahl der möglichen Testfälle unendlich groß. Andererseits führen die asynchrone Kommunikation und der inhärente Nichtdeterminismus in Zustandsmaschinen für jede einzelne Eingabesequenz zu einem sehr komplexen Verhalten. Die präzise und widerspruchsfreie Interpretation dieses komplexen Verhaltens ist notwendige Voraussetzung für jegliche Art von Automatisierung, erfordert jedoch einen enorm hohen Berechnungsaufwand und ist damit nicht immer praktikabel. Um die Anzahl der Testfälle sinnvoll zu beschränken werden Testspezifikationen verwendet. In Testspezifikationen werden Art und Umfang der betrachteten Eingaben festgelegt und relevante Eingabesequenzen durch Nutzungsprofile beschrieben. Einfache Nutzungsprofile erlauben die probabilistische Auswahl von Eingaben oder die Vorgabe fester Eingabesequenzen. Komplexere Nutzungsprofile beschreiben das Verhalten der Umgebung explizit in Form von Zustandsmaschinen mit probabilistischen Zustandsübergängen und ermöglichen damit eine systematische und automatisierte Auswahl relevanter Eingaben.

Die Bestimmung des möglichen korrekten Verhaltens für eine gegebene Eingabesequenz erfolgt in einer schrittweisen Ausführung der Zustandsmaschine. Da der Berechnungsaufwand mit zunehmender Länge der betrachteten Eingaben exponentiell ansteigt und deshalb eine Berechnung für typische Sequenzlängen nicht praktikabel ist, können kürzere Eingabesequenzen mehrerer Testfälle kombiniert werden. Die Einfügung von Beobachtungspunkten nach jeder Eingabesequenz führt zu einer erheblichen Reduzierung des Berechnungsaufwands für die nachfolgenden Eingaben, wobei das mögliche korrekte Verhalten approximiert wird. Der Berechnungsaufwand steigt linear mit der Anzahl der kombinierten Testfälle. Durch eine geeignete Wahl der Anzahl an Teilsequenzen, aus denen eine Eingabesequenz zusammengesetzt wird, kann hinsichtlich des Aufwands für die Testfallerzeugung und der Erkennungsrate der Testfälle ein guter Kompromiss erzielt werden.

Praktisches Ergebnis der Arbeit ist die prototypische Werkzeugumgebung TEAGER. Diese setzt sich auf der einen Seite aus einer Umgebung zur Testfallerzeugung und -ausführung und auf der anderen Seite aus einer Umgebung zur Simulation von Zustandsmaschinen zusammen. Die durchgeführten Untersuchungen zeigen, dass durch die Verhaltensapproximation mit der Komplexität und der Zustandsexplosion innerhalb von Zustandsmaschinen umgegangen, eine akzeptable Erkennungsrate erzielt und die Ablehnung korrekter Systeme vermieden werden kann.