

Formale Verifikationsmethode für reale Schaltungen und Systeme

Thesenpapier

Die Verifikation komplexer technischer Strukturen ist heute von kritischer Bedeutung. Um die Funktionalität der Systeme sicherzustellen und eine akkurate, fehlerfreie Anwendung zu gewährleisten, wird von den Hardware Designern, Entwicklern und Nutzern enormer Zeit- und Kostenaufwand sowie Rechenressourcen betrieben. Dabei unterliegt das Testen solcher realisierter Strukturen stetig steigenden Anforderungen.

Es steht nun die Behauptung im Raum, dass die funktionale Sicherheit von Schaltungen und Systemen erst durch die strukturtreue Verifikation kostengünstig durchgeführt und gleichzeitig abgesichert werden kann. Die wesentliche Schwierigkeit dabei wird in der formalen Zuordnung von virtueller Funktionalität zu realer Struktur gesehen. Es erscheint damit zwingend, die Übereinstimmung der formal hergeleiteten Funktion mit der real erzeugten Funktion sicherzustellen. Auf einen Nenner gebracht: „Die einer realen Struktur zugehörige Funktion sollte strukturtreu modelliert vorliegen. Das Ziel ist es, eine Modellierung realer Systeme mit Hilfe von genau solchen Funktionen zu erarbeiten, die mit Hilfe ihrer Verhaltensbeschreibung die Struktur bewahren können.“

In der vorliegenden Arbeit führt dies auf eine Darstellung als Signalflussgraph (SFG). Der SFG wird hier vorgestellt als die geeignete Darstellungsmöglichkeit, um strukturtreue Abbildungen verifizieren zu können. Es wird der Name und die Methode eingeführt „Strukturtreue Modellierung anhand von Signalflussgraphen“.

Flankierend dazu sollte auch der benötigte Speicherbedarf und damit eine kürzere Rechenzeit für die Testprozesse sichergestellt werden. In der vorliegenden Arbeit wird dies durch die verlustlose Datenkompaktierung für TVL-Formate als auch QVL-Formate erreicht. Zusätzlich wird ein optimales, gerichtetes Vorgehen für den Austausch von möglichen fehlerhaften Bauteilen in einem Diagnose-Flow eingeführt, und das Konzept einer selbstbestätigenden Methode namens „Fehlerbaumanalyse“ vorgeschlagen, diskutiert und überprüft.

Die Eingabe von Daten (Testergebnissen) mit hohen Dimensionen, in denen nicht wenige Elemente einer Datenmenge irrelevant oder weniger relevant als andere sind, führt meist zu sehr unübersichtlichen und schwierig zu interpretierenden Ergebnissen. Also war es sinnvoll, zusätzlich Verfahren heranzuziehen, welche die einzelnen Dimensionen der Datenmengen nach ihrer Relevanz klassifizieren und vorteilhaft reduzieren. In dieser Arbeit wird die Datenanalyse (SEDA) für eine rekursive Trennung von Daten vorgestellt.