39 Der Heilige Gral für Software

Softwarefehler können Schäden in Höhe von Hunderten Millionen Euro verursachen und sogar Menschenleben kosten. Die Mathematik hilft zu beweisen, dass die Software absolut fehlerfrei ist.

Da Computersoftware immer komplexer wird, wird es immer wichtiger, die Wahrscheinlichkeit von Fehlern so weit wie möglich zu reduzieren. Dies gilt sicherlich für lebenskritische Softwareanwendungen in Autos, Flugzeugen und Krankenhäusern, aber zunehmend auch für die Software von Unternehmen. Das niederländische Unternehmen ASML ist der weltweit größte Hersteller von Maschinen, die Computerchips auf Siliziumscheiben drucken. Große Chiphersteller wie Intel, Samsung und TSMC verwenden ASML-Maschinen, um ihre eigenen Computerchips auf Siliziumscheiben zu drucken. Diese Chips finden sich zum Beispiel in den neuesten iPhones und iPads.

Jede ASML-Maschine wird von einem kolossalen Softwareprogramm gesteuert. Die Grundlage für dieses Computerprogramm wurde vor 25 Jahren gelegt und seither kontinuierlich erweitert und verbessert. Das Programm verfügt jetzt über mehr als dreißig Millionen Codezeilen, und niemand kann alle Details übersehen. ASML beschäftigt 900 Mitarbeiter für die Wartung, Verbesserung und Erweiterung der Software. Softwarefehler können Schäden in Höhe von Hunderten Millionen Euro verursachen und sogar Menschenleben kosten. Die Mathematik hilft zu beweisen, dass ein Stück Software absolut fehlerfrei ist.

Kostspielige Fehler

Programmieren ist eine akribische Arbeit und eine goldene Regel in der Software-Welt besagt, dass im Durchschnitt 10 Fehler in 1.000 Zeilen Computercode vorkommen. Für die ASML-Maschine bedeutet dies, dass es bis zu 300.000 Fehler in der Software geben kann. In der Praxis wird ein Kunde viele dieser Fehler nicht bemerken, aber einige Fehler können das Gerät stundenlang abschalten. Die Maschine kostet 40 Millionen Euro, und für jede Stunde, in der die Maschine angehalten wird, verlieren die ASML-Kunden, die die Maschine benutzen, schnell Hunderttausende von Euro an Einnahmen.

Traditionell werden Fehler durch das Testen von Software entdeckt. Das Problem beim Testen besteht darin, dass man zwar das Vorhandensein von Fehlern nachweisen kann, nicht aber, dass es keine Fehler enthält. Weil Software-Fehler so teuer sind, verwendet ASML seit einigen Jahren mathematische Beweis-Techniken, die nachweisen können, dass Teile der Software keine Fehler enthalten.

Jedes Stück Software besteht im Wesentlichen aus einer Abfolge von Entscheidungen: wenn A wahr ist, führen Sie B aus; wenn A nicht wahr ist, führen Sie C aus. Angenommen, ein Programm enthält eine dieser Arten von Entscheidungen, dann kann es in 2 möglichen Zuständen sein. Bei 10 Entscheidungen sind dies bereits $2^{10} = 1024$ Zustände und bei 1000 sogar bis zu 2^{1000} Zustände. Wenn man garantieren will, dass

es keine Fehler in der Software gibt, dann muss man alle möglichen Kombinationen von Entscheidungen ausprobieren. Selbst mit hundert Kombinationen pro Minute ist es für ein großes System wie das von ASML nicht machbar, dies in einem vernünftigen Zeitrahmen zu erreichen.

Mathematische Tricks

Abbildung 37: Beispiel eines ASML-Lithographiegerätes. Einige große Herausforderungen für ASML-Lithographiemaschinen: sehr genaues, ultraschnelles und ultrakleines Linienschreiben auf Siliziumscheiben, die sich in Computerchips verwandeln sollen. Quelle: ASML

Der Trick besteht darin, die Anzahl der möglichen Zustände, in denen sich eine Software befinden kann, zu reduzieren. Angenommen, das Programm muss die Aufgaben A, B und C erledigen und die Reihenfolge spielt keine Rolle. So enden alle sechs Kombinationen ABC, ACB, BAC, BCA, CAB und CBA alle im gleichen Zustand Q. Beim klassischen Testen der Software müssen Sie alle sechs Kombinationen ausprobieren. Die mathematische Beweismethode sieht, dass alle Kombinationen zu Q führen. Bei dieser Beweismethode müssen Sie nur über eine viel kleinere Zahl als die Gesamtzahl der möglichen Zustände nachdenken. Dann ist es möglich, die Fehlerfreiheit in Teilen der gesamten Software nachzuweisen.

Ein weiterer Trick ist die *Symmetrie-Reduktion*. Angenommen, die ASML-Maschine kann 3 Produkte gleichzeitig verarbeiten, während sich gleichzeitig 6 Produkte in der Maschine befinden können. Die mathematische Beweismethode sieht dann sozusagen, dass die Verarbeitung von Produkt 1, 2 und 3 gleichbedeutend ist mit der Verarbeitung von Produkt 2, 3 und 4 und so weiter. Allerdings muss der Ingenieur dieses Wissen vermitteln, indem er der mathematischen Beweismethode mitteilt, dass die Produkte sauber in der Reihenfolge verarbeitet werden. Mit solchen mathematischen Tricks kann man letztlich beweisen, dass die Roboterarme, die die Siliziumscheiben bewegen, niemals kollidieren oder dass die Reihenfolge, in der man die Messungen vornimmt, immer korrekt ist.