Softwarefouten kunnen voor honderden miljoenen euro's schade veroorzaken en zelfs mensenlevens kosten. De wiskunde helpt om te bewijzen dat een stuk software absoluut foutloos is.

Heilige graal voor software:

wiskundig bewijs dat er geen fout in zit

Omdat computersoftware steeds ingewikkelder wordt, wordt het steeds belangrijker om de kans op fouten zo veel mogelijk te reduceren. Dat geldt zeker voor levenskritische softwaretoepassingen in auto's, vliegtuigen en ziekenhuizen, maar in toenemende mate ook voor de software van bedrijven. Een van de hightechbedrijven die foutloosheid van software hoog in het vaandel heeft staan, is het Nederlandse ASML. ASML is de grootste producent ter wereld van machines die computerchips op siliciumschijven printen. Grote chipfabrikanten zoals Intel, Samsung en TSMC gebruiken ASML-machines om hun eigen computerchips te fabriceren. Deze chips zitten in bijvoorbeeld de nieuwste iPhones en iPads.

Elke ASML-machine wordt bestuurd door een kolossaal softwareprogramma. De basis voor dit computerprogramma is 25 jaar geleden gelegd en sindsdien voortdurend uitgebreid en verbeterd. Inmiddels telt het meer dan dertig miljoen regels code en kan niemand meer alle details ervan overzien. ASML heeft negenhonderd mensen in dienst die zich bezig houden met het onderhoud, de verbetering en de uitbreiding van de software.

Dure fouten

Programmeren is een secuur vak, en een gouden regel in softwareland zegt dat er gemiddeld tien fouten zitten in duizend regels computercode. Voor de ASML-machine betekent dit dat er tot wel driehonderdduizend fouten in de software kunnen zitten. In de praktijk zal een klant van veel van die fouten niets merken, maar sommige fouten kunnen de machine urenlang stil leggen. De machine kost veertig miljoen euro en voor elk uur dat de machine stil staat, lopen de ASML-klanten die de machine gebruiken al snel honderdduizenden euro's aan inkomsten mis.

Traditioneel worden fouten opgespoord door software te testen. Het probleem met testen is dat je weliswaar de aanwezigheid van fouten kunt aantonen, maar niet kunt bewijzen dat er géén fouten in zitten. Software-ingenieur Sven Weber van ASML: "Omdat softwarefouten zo kostbaar zijn, gebruikt ASML sinds een paar jaar wiskundige bewijstechnieken die voor onderdelen van de software keihard kunnen bewijzen dat er geen fouten in zitten."

Elk stuk software bestaat in essentie uit een aaneenschakeling van beslissingen: als A waar is, voer dan B uit; Als A niet waar is, voer dan C uit. Stel dat een programma n van dit soort besluiten bevat, dan kan het zich in 2^n mogelijke toestanden bevinden. Met 10 besluiten loopt dit al op tot $2^{10} = 1024$ toestanden en met 1000 zelfs tot 2^{1000} toestanden. "Als we willen garanderen dat er geen fouten in de software zitten," zegt Weber, "dan moeten we alle mogelijke combinaties van beslissingen uitproberen. Zelfs met honderd combinaties per minuut is het voor een groot systeem als het onze niet haalbaar om dat in redelijke tijd te doen."

Wiskundige trucs

De truc is dan ook om het aantal mogelijke toestanden waarin een stuk software zich kan bevinden te reduceren. Stel dat het programma taken A, B en C moet doen en dat de volgorde niet uitmaakt. Dus alle zes de combinaties ABC, ACB, BAC, BCA, CAB en CBA komen allemaal in dezelfde toestand Q terecht.

Voorbeeld van een ASML-lithografiemachine. Enkele grote uitdagingen voor ASML-lithografiemachines: het zeer nauwkeurig, razendsnel en ultraklein schrijven van lijntjes op siliciumschijven, bedoeld om computerchips van te maken. Bron: ASML

Bij het klassiek testen van de software moet je alle zes de combinaties proberen. De wiskundige bewijsmethode ziet dat alle combinaties tot Q leiden. Met deze bewijsmethode hoef je dus maar over een veel kleiner aantal dan het totale aantal mogelijke toestanden te redeneren. Dan is het bewijzen van foutloosheid in delen van de totale software wel mogelijk.

Een andere truc is symmetriereductie. Stel dat de ASML-machine drie producten tegelijk kan bewerken, terwijl er zes producten tegelijk in de machine kunnen zitten. De wiskundige bewijsmethode ziet dan als het ware dat het verwerken van product 1, 2 en 3 equivalent is aan het verwerken van product 2, 3 en 4 en zo verder. Deze kennis moet de ingenieur wel aanreiken door de wiskundige bewijsmethode te vertellen dat producten netjes op volgorde verwerkt worden. "Wij gebruiken een hele reeks van dit soort wiskundige trucs", zegt Weber. "Daarmee kunnen we dan uiteindelijk bewijzen dat de robotarmen die de siliciumschijven verplaatsen nooit botsen of dat de volgorde waarin we onze metingen doen altijd correct is."