

# Bewijsassistent verbeterd

---

Het lijkt wel of tegenwoordig overal een chip en een computerprogramma in zit. Pinautomaten, magnetrons, wasmachines, horloges, scheerapparaten. Al die apparaten moet goed werken. Altijd. Je wilt bijvoorbeeld niet dat een pinautomaat teveel geld van je rekening afschrijft. Er mogen dus ook geen fouten in de computerprogramma's zitten.

Helaas. We weten maar al te goed dat er in computerprogramma's juist vrijwel altijd fouten zitten. Vastlopers van de PC zijn aan de orde van de dag, mobiele telefoons zijn inmiddels gemeengoed maar crashen voortdurend en ook auto's hebben steeds vaker last van 'softwareproblemen'. Technologische vooruitgang gaat gepaard met ongemakken.

Hoe komt dit nou? Worden de programmeurs niet goed genoeg betaald? Wordt de software niet goed uitgetest? Misschien, maar dit zijn zeker niet de enige oorzaken. Software is namelijk al snel te complex voor een mens om helemaal te begrijpen en te overzien, en het is vaak onmogelijk om alle denkbare situaties uit te testen, laat staan alle ondenkbare. Hoe kunnen we er dan ooit zeker van zijn dat het programma doet wat het moet doen?

De enige mogelijkheid om dit echt zeker te weten is door het te bewijzen. Met bewijzen wordt bedoeld dat je laat zien, volgens de regels van de logica, dat het niet anders kan zijn dan dat het programma goed werkt. Er bestaan al vrij lang computerprogramma's die hierbij kunnen helpen: de bewijsassistenten. Helaas zijn deze bewijsassistenten gericht op wiskundigen en logici, en niet op programmeurs. Men kan dingen bewijzen over een programma, maar dan wel in een andere taal dan de programmeertaal. Programmeren in het Nederlands, bewijzen in het Chinees. Geen praktische combinatie dus. Er wordt dan ook niet zo gek veel bewezen.

Om dit te verhelpen is er in Nijmegen een bewijsassistent ontwikkeld die wel een voor programmeurs bekende taal spreekt. Bijna dan. Programmeren in het Nederlands, bewijzen in het Surinaams zagezegd. Zo ontbraken er nog een aantal niet essentiële maar wel ontzettend handige eigenschappen van de programmeertaal. Één daarvan is "overloading", wat staat voor de mogelijkheid om een stuk code dat voor verschillende situaties steeds herhaald moet worden, terug te brengen tot een veel kleiner stuk voor een beperkt aantal gevallen waaruit de code voor andere gevallen automatisch gegenereerd kan worden. Het gevolg was dat de programmeur de code wel kort kon opschrijven, maar het bewijzen toch voor alle mogelijke situaties afzonderlijk moest doen. Dat kon niet de bedoeling zijn.

Goed nieuws! In dit project is dit gemis verholpen. Het bewijzen kan nu ook via de korte weg: in één keer voor alle mogelijke situaties. Dit kan zelfs zo uitgebreid worden dat de bewijzer niet eens ziet dat we hiervoor iets speciaals doen. Het bewijzen kan dan in het Vlaams in plaats van het Surinaams. Nog niet perfect, maar wel een stuk beter. De kans dat de programmeur de moeite neemt iets over zijn programma te bewijzen neemt hiermee toe. En zo komt de wereld waarin de mobiele telefoon het altijd doet, de PC nooit crasht en de wasmachine weer gewoon wast, een heel klein stukje dichterbij.