Publicatie : NRC NEXT
Datum : 20 sep 2017
cm2 : 294
Pagina : 17
Advertentiewaarde : € 10.466,00
Regio : Nederland
Frequentie : dagelijks
Oplage : 33.355

VRAAG DIE LEEFT

Hoe maakt een computer randomgetallen?

Elke week zoekt de redactie wetenschap het antwoord op **een veelgestelde vraag**. Vandaag: hoe 'bedenkt' een computer willekeurige getallen?

Dorine Schenk

Voordat je verder leest: schrijf vijf getallen op tussen de 0 en 100. Gelukt? Gefeliciteerd. Je hebt iets gedaan waar computers moeite mee hebben: willekeurige getallen bedenken. „Computers zijn deterministisch", vertelt Serge Fehr van het Centrum Wiskunde & Informatica (CWI) in Amsterdam aan de telefoon. Als je steeds hetzelfde commando geeft, zal de computer altijd hetzelfde reageren. De machine kan dus geen volledig willekeurige getallen produceren, omdat hij louter volgens voorspelbare vaste stappen en regels (algoritmes) nieuwe getallen kan bedenken.

Toch gebruiken computers randomgetallen: voor onvoorspelbaarheid in computerspellen of (online) kansspellen. Wetenschappers gebruiken ze voor simulaties. Ook om veilig websites te bezoeken en online versleuteld berichten en geld te versturen, zijn randomgetallen nodig.

Een computer kan twee soorten randomgetallen produceren: pseudorandom en 'echt' (*true*) random. Zoals de naam zegt, zijn pseudorandomgetallen niet helemaal willekeurig. Fehr: „Ze worden gemaakt door een algoritme dat zo onvoorspelbaar is, dat de getallen random lijken." Je begint hiervoor met een startwaarde. Die geeft degene die achter de computer zit of de computer kiest zelf: bijvoorbeeld het laatste getal van de digitale klok. Daarmee wordt via een formule een reeks random ogende getallen gemaakt. Een simpel voorbeeld is de *middle-square method*: kies een startwaarde (bijvoorbeeld 4455), kwadrateer die (19.847.025), neem het middelste getal van dat kwadraat (8470), enzovoort.

Dit soort rijtjes zijn niet erg random. Als je de achterliggende methode kent, kun je de volgorde voorspellen. Soms is dat geen probleem; de volgorde van de speelkaarten bij patience mag best pseudorandom zijn. Maar als je geld kunt winnen bij onlinekansspellen of als het om het beveiligen van e-mails gaat, dan is pseudorandom niet genoeg. Hiervoor bestaan 'cryptografische pseudotoevalsgetallen'. Het algoritme daarvan is zo complex dat er geen computer krachtig genoeg is om het te achterhalen.

Maar er bestaan nog willekeurigere getallen, gemaakt door *true random number generators*. „Die kijken naar fysische processen die geacht worden onvoorspelbaar te zijn", vertelt Fehr. „Zoals het exacte moment dat je toetsen op je toetsenbord indrukt." Die informatie zetten ze om in een getal. Sommige *true random number generators* gebruiken zelfs de atmosferische ruis uit de lucht om setjes toevalsgetallen te produceren.

„Ondanks dat die getallen willekeurig genoeg zijn voor alle mogelijke doeleinden, ben ik een beetje terughoudend om te zeggen dat ze echt random zijn", voegt Fehr toe. „Theoretisch is zelfs een muntworp immers voorspelbaar als je alles weet, omdat de meeste natuurkundige wetten deterministisch zijn." Behalve de quantummechanica. Fehr: „Quantummechanische processen, zoals de beweging van elektronen, zijn zelfs als je alle informatie erover hebt, niet te voorspellen." Een randomgetallengenerator die kijkt naar quantumprocessen produceert dus wel volledig toevallig getallen. Deze zijn al te koop.

Het rijtje met getallen dat je aan het begin opschreef, zal trouwens niet echt random zijn. Mensen vermijden regelmatig ogende volgordes. Waarschijnlijk was er niemand die vijf keer hetzelfde getal opschreef, terwijl dat in een 'echt' willekeurig rijtje wel kan.

Een computer kan twee soorten randomgetallen maken: 'pseudo' en 'echt'


Wetenschap
Er kan nog veel meer energie uit water worden gewonnen