‘Excel op een kwantumcomputer? Vergeet het’

We worden om de oren geslagen met jubelverhalen over de kwantumcomputer, de ‘wondermachine’ die zelfs de snelste van onze huidige gewone computers zou degraderen tot telraam. Dat is voor een deel overdreven. ‘Een kwantumcomputer rekent niet sneller, maar anders.’

Senne Starckx
is theoretisch fysicus en journalist.

Sinds bedrijven als Microsoft, Google, Intel en IBM zich op de ontwikkeling van een kwantumcomputer hebben gestort, is er een race aan de gang om als eerste een werkend prototype te bouwen. Het liefst heeft die eerste kwantumcomputer zoveel mogelijk qubits, de kwantummechanische tegenhanger van de klassieke bit. De techgiganten laten uitschijnen dat het slechts een kwestie van tijd is vooraleer ‘quantum supremacy’ wordt bereikt. Die term slaat op de mogelijkheid voor een kwantumcomputer om een probleem op te lossen dat gewone computers niet aankunnen (zie ‘Op naar de kwantumhegemonie’). Het klinkt alsof de dagen van de met bits rekenende computers, en zelfs van de krachtigste supercomputers, geteld zijn.

‘Spreek gerust van een hype’, zegt theoretisch fysicus Frank Verstraete van de Universiteit Gent. ‘De grote technologiebedrijven maken dezer dagen inderdaad veel reclame voor hun prototypes, terwijl een bedrijf als IBM al sinds de jaren 1980 onderzoek doet naar een kwantumcomputer.’

Wat wel nieuw is: door de wedijver in de kwantumrace wordt er heel veel geld in het onderzoek gepompt. Mede daardoor zijn er nu ‘kwantumsystemen’ van vijftig qubits. Verstraete: ‘Maar deze systemen zijn nog geen werkende kwantumcomputers, en je kunt ze nog altijd simuleren met een gewone computer. Voor de komende tien jaar verwacht ik niet dat een kwantumcomputer relevante problemen zal aankunnen die niet klassiek kunnen worden opgelost.’

Verstraete verdiept zich al een geruime tijd in de kwantumtheorie om kwantumfysische vraagstukken op te lossen met behulp van de computer. Als hij terugkijkt op de voorbije jaren, ziet hij geen échte doorbraak die de huidige hype kan rechtvaardigen. ‘Oké, de technologie heeft wel wat vooruitgang geboekt, maar een kwantumcomputer die zinnige dingen kan doen, is er nog lang niet.’

Zijn de kwantumsystemen van vijftig qubits waarmee Google, IBM en Intel vorig jaar groots uitpakten, dan niet bijzonder? ‘Op kwantumfysisch niveau is het natuurlijk een ongelooflijk staaltje van technisch vernuft’, zegt Verstraete. ‘Helaas zijn de huidige systemen niet foutbestendig, en daar draait het eigenlijk om. Een betrouwbare computer werkt alleen als je voldoende foutcorrectie hebt ingebouwd. Dat is bij een gewone computer niet anders. Bij een kwantumcomputer heb je daarvoor duizenden tot zelfs miljoenen extra qubits nodig (zie ‘De kat van Schrödinger bestaat echt’). Die moeten garanderen dat de samenhang tussen de basisqubits lang genoeg intact blijft. De technologie om zoveel qubits te manipuleren, staat nog maar in de kinderschoenen. Van een volwaardig kwantumcircuit, opgebouwd uit miljoenen logische kwantumpoorten, zijn we nog heel ver verwijderd.’

'Met een kwantumcomputer kun je codes kraken die nu nog waterdicht zijn, om vervolgens betere codes te ontwikkelen'

HEILIGE GRAAL

Dat de Gentse kwantumfysicus sceptisch staat tegenover de hoera-be-

richtgeving van het moment, betekent niet dat hij niet in de qubit gelooft. Integendeel, ook hij ziet een stralende toekomst voor de kwantumcomputer. Maar dan niet als een computer die haast oneindig snel kan rekenen, wel als een enorm krachtige simulator van de microwereld. Dat is de wereld waar kwantuminteracties bepalen hoe materie- en energiedeeltjes zich gedragen. 'Met rekenen heeft dat niet veel meer te maken, toch niet in de betekenis die we gewoon zijn.'

Meestal draait zo'n simulatie rond een zogenaamd veeldeeltjessysteem. Dat kan een atoomkern zijn, een molecule of zelfs een eiwit. De simulatie moet nagaan hoe dat systeem zich zal gedragen en welke eigenschappen het zal vertonen. Het is zeg maar bottom-up-deeltjesfysica, -chemie en -biologie. In de simulatie stemt elke qubit van een kwantumcomputer dan overeen met een specifieke kwantumtoestand, bijvoorbeeld de *spin* van een elektron. Kwantummechanische theorieën en methodes, waarmee bijvoorbeeld de elektronenstructuur wordt berekend van grotere moleculen, bepalen vervolgens hoe de kwantumcomputer de simulatie afhandelt.

'Nu worden veeldeeltjessystemen nog met gewone computers uitgerekend', zegt Frank Verstraete. 'Maar dat gaat zeer traag, zelfs met de krachtigste supercomputers. Een kwantumcomputer verliest geen tijd met rekenen. Je zou kunnen zeggen dat hij het systeem gewoon nabootst. Je beschikt als het ware over een artificieel lab dat buiten de tijd werkt en experimenten en klassieke computersimulaties overbodig maakt. Zo'n kwantumsimulator is voor mij de heilige graal.'

De potentiële markt voor zo'n hypersnelle systeemsimulator is natuurlijk gigantisch. Farmaceutische en chemische bedrijven stoten tegenwoordig tegen de limieten aan in hun zoektocht naar nieuwe moleculen en reacties. De labexperimenten die ze uitvoeren, worden te ingewikkeld en daardoor te duur om met gewone computers te simuleren. Verstraete: 'Het is geen toeval dat meer dan de helft van alle rekenkracht in de wereld wordt opgesoupeerd door simulaties van veeldeeltjessystemen zoals moleculen.'

Het 'simuleren van de natuur' is zeker een belangrijke toepassing van de kwantumcomputer, vindt ook Harry Buhrman, oprichter en directeur van QuSoft, een Nederlands onderzoekscentrum voor kwantumsoftware. Maar hij ziet ook andere, meer bij de wiskunde aanleunende toepassingen, zoals het ontbinden in factoren van enorm grote getallen. Deze 'factorisatie' vormt de basis onder de zogenaamde RSA-versleuteling, waarmee tal van online transacties worden beveiligd. 'Met een kwantumcomputer kun je allerlei codes die nu nog waterdicht zijn, kraken', zegt Buhrman. 'Om vervolgens betere codes te ontwikkelen.'

Het kloppende hart van de IBM Q, een prototype van een kwantumcomputer met vijftig qubits. De qubits worden gevormd door gekoelde, supergeleidende circuits.

IN HET KORT

Chemici, fysici en wiskundigen kijken uit naar een computer die hun complexe problemen veel efficiënter kan oplossen.

•

In andere domeinen is een kwantumcomputer weinig inzetbaar.

•

De machines rekenen anders, maar niet per se sneller dan bestaande systemen.

Daarnaast zoeken Buhrman en zijn collega's van QuSoft naar andere toepassingen en kwantumalgoritmes. 'Bijvoorbeeld voor optimalisatieproblemen en applicaties binnen machinaal leren', aldus Buhrman.

NICHE

Aan de Université Libre de Bruxelles werkt kwantumfysicus Jérémie Roland op de meer wiskundig geïnspireerde toepassingen van de kwantumcomputer. Hij zoekt onder andere naar kwantumalgoritmes die problemen uit de abstracte lineaire algebra kunnen (helpen) oplossen, zoals stelsels van vergelijkingen in meerdere onbekenden. 'Omdat de structuur van de kwantummechanica zélf lineair algebraïsch is, leent ze zich hier prima toe', zegt Roland. 'Je zou kunnen zeggen dat we de algebra op een kwantumcomputer simuleren.' Net zoals dat met de veeldeeltjessystemen gebeurt, dus.

Maar Roland geeft ook toe dat het zeer moeilijk is om concrete problemen te vinden die je met een kwantumcomputer kunt oplossen. 'Je probleem moet bijzonder goed gestructureerd zijn als je het wil laten oplossen door een kwantumalgoritme. Aan het algoritme van Shor (een kwantumalgoritme voor het ontbinden in priemfactoren dat in 1994 ontwikkeld werd door de Amerikaanse wiskundige Peter Shor, red.) wordt vandaag nog steeds gesleuteld, terwijl het al meer dan twintig jaar oud is.'

Een van de problemen waar een kwantumcomputer kan slagen waar een gewone computer faalt, is dat van het zogenaamde aanbevelingssysteem ('recommendation system'). Zo'n systeem verzamelt informatie over individuele aankopen of ratings door consumenten, om uiteindelijk gepersonaliseerde aanbevelingen naar diezelfde consumenten te kunnen sturen. Als je x consumenten hebt (bijvoorbeeld Netflix-abonnees of Amazon-klanten), en y producten (Netflix-series of Amazon-boeken), dan vertaalt dat zich naar een matrix met x rijen en y kolommen. 'Als je die matrix op voorhand kent, is het probleem snel opgelost', zegt Roland. 'Maar de crux zit 'm erin dat het systeem op elk moment, op basis van enkel de beschikbare informatie, een gepersonaliseerde aanbeveling moet kunnen uitsturen. Dat kun je nauwelijks efficiënt doen zónder een kwantumcomputer uitgerust met een kwantumalgoritme.'

Ook al zouden internetbedrijven veel geld kunnen verdienen met zo'n aanbevelingssysteem, toch laat dat voorbeeld ook zien dat het vooral nichevraagstukken zijn die zullen worden opgelost met kwantumcomputers. 'Het is inderdaad een grote uitdaging om relevante problemen te vinden die binnen het strikte kader passen van het kwantumalgoritme', meent Frank Verstraete. 'Theoretici breken zich al sinds begin jaren 1990 het hoofd over manieren om klassieke problemen op te lossen met kwantumalgoritmes. Met bitter weinig resultaten.'

Harry Buhrman is het daar niet helemaal mee eens. Hij ziet wél een flink aantal kwantumalgoritmes die werden ontwikkeld voor concrete toepassingen. 'Ik denk dan aan verbeterde methodes om traditionele uitdagingen binnen de informatica op te lossen, zoals zoek-, optimalisatie- en netwerkproblemen.' In dat domein gaat het er onder meer om zo snel mogelijk het juiste antwoord te vinden in een gigantische berg data.

Toch geeft ook Buhrman toe dat er wat schort aan de populaire boodschap dat een kwantumcomputer 'exponentieel' sneller kan rekenen dan een gewone computer. 'Hij rekent gewoon anders. Een gewone rekent met bits, met nullen en enen. Een kwantumcomputer met qubits, die meerdere waarden tegelijk kunnen aannemen. Daar heb je dus een heel andere computerar-

OP NAAR DE KWANTUMHEGEMONIE

In berichten over de race naar de kwantumcomputer komt vaak de term 'quantum supremacy' naar voren. Die refereert aan het moment (in de toekomst) waarop een kwantumcomputer een probleem kan oplossen dat onoplosbaar is voor gewone computers. Wanneer we dat moment kunnen verwachten, valt moeilijk te voorspellen en hangt af van de snelheid waarmee de technologie zich blijft ontwikkelen. Maar waar de 'kwantumhegemonie' zich ergens schuilhoudt, daarover bestaat min of meer een consensus. 'We vermoeden dat er zich ergens tussen vijftig en honderd qubits een drempel bevindt waarboven gewone computers voor sommige problemen niet meer kunnen concurreren met een kwantumcomputer', zegt Harry Burhman, directeur van QuSoft.

Theoretisch fysicus Frank Verstraete (UGent) zal geen gat in de lucht springen als de kwantumhegemonie straks wordt afgekondigd. 'In de race naar quantum supremacy wordt vooral gezocht naar problemen die gemakkelijk zijn voor een kwantumcomputer en moeilijk voor een gewone computer. Maar de problemen waarnaar men kijkt, doen eigenlijk wetenschappelijk niet terzake.'


ETH Zurich

Bij kwantumcomputers worden vaak neutrale atomen gebruikt als qubits. Om de atomen voldoende af te koelen (tot bij het absolute nulpunt van -273,15° C), bedienen onderzoekers zich van laserlicht uit een zogeheten magneto-optische val.

chitectuur voor nodig, én een heel andere manier van programmeren. Een klassiek algoritme zul je daarom nooit zomaar kunnen overplaatsen op een kwantumcomputer, in de hoop dat die het in geen tijd afhaspelt.' Bij QuSoft zoeken Buhrman en zijn collega's daarom naar nieuwe kwantumalgoritmes. Voorlopig doen ze dat nog met pen en papier – en soms met een gewone computer. Buhrman: 'Het zou natuurlijk wel leuk zijn als we onze algoritmes konden testen op een échte kwantumcomputer.'

TOPJE VAN DE IJSBERG

Hoe vind je een nieuw kwantumalgoritme dat een nuttige uitkomst heeft en waarmee een kwantumcomputer straks aan de slag kan? 'We hebben een aantal technieken onder de knie die kenmerkend zijn voor kwantumalgoritmes', zegt Buhrman. 'Onze zoektocht spitst zich nu toe op interessante problemen of vraagstukken waarop we die technieken kunnen loslaten. Vergelijk het met de huidige ontwikkeling van apps. Een goeie app vind je niet toevallig, maar wel door slim gebruik te maken van het nieuwste gereedschap waarover je als programmeur beschikt.'

> Het gaat om een totaal andere manier van programmeren. Een simpele tekstverwerker kun je nooit op een kwantumcomputer laten draaien

Volgens Buhrman is het huidige arsenaal aan kwantumalgoritmes slechts het topje van de ijsberg. 'In de computerwetenschap heb je drie categorieën van problemen. In de eerste zitten de problemen waarvan we nu al weten dat een kwantumcomputer ze nooit sneller zal kunnen oplossen dan een gewone computer. In de tweede zitten de problemen waarvan we weten dat dit wél mogelijk is – denk aan kwantumsimulaties, factorisaties en zogenaamde optimalisatieproblemen. De derde categorie is het onzichtbare deel van de ijsberg: we weten gewoonweg niet wat er nog allemaal kán, en niet kan.'

Als de kwantumcomputer er eenmaal is en de hardware op punt staat, moet ook de software klaar zijn. Dat was de reden waarom Buhrman drie jaar geleden QuSoft oprichtte, als de software-pendant van QuTech, het ambitieuze lab van de TU Delft en Microsoft dat een kwantumcomputer probeert te bouwen. Kwantumsoftware verschilt in alle opzichten van de programma's en apps die op onze laptops en smartphones draaien. Burhman: 'Het gaat om een compleet andere manier van programmeren. De gewone computer hoeft dus niet voor zijn voortbestaan te vrezen. Een simpele tekstverwerker zul je nooit op een kwantumcomputer kunnen laten draaien.' ■

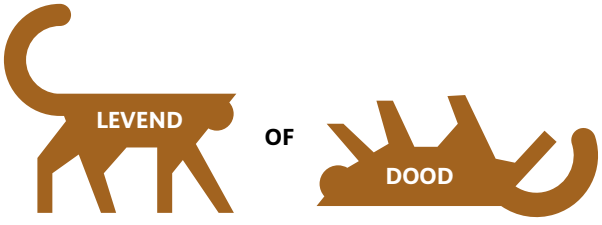
DE KAT VAN SCHRÖDINGER BESTAAT ECHT

Een kwantumcomputer met een bepaald aantal qubits werkt bij gratie van de toestand van superpositie waarbinnen het systeem zich bevindt. Superpositie wil zeggen dat een systeem zich op eenzelfde moment in meerdere kwantumtoestanden kan bevinden. Een kwantumcomputer kan daardoor meerdere berekeningen tegelijkertijd uitvoeren.

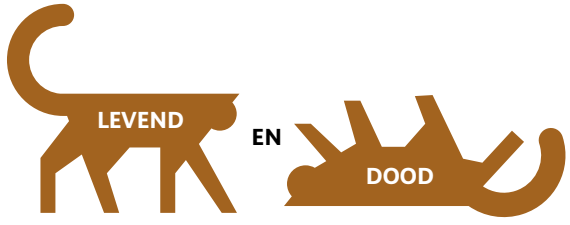
De kwantummechanica bepaalt echter dat als je een meting uitvoert op een systeem, de superpositie instort – de kwantumcomputer geeft dan een willekeurige uitkomst. Een kwantumalgoritme laat de berekeningen die een uitkomst hebben gebaard constructief op elkaar inwerken. Dat moet garanderen dat een meting op het einde van een berekening de juiste uitkomst geeft.

Om superpositie te kunnen garanderen, moeten de qubits van een kwantumcomputer dus extreem afgezonderd worden van de omgeving. Zoniet verdampt de informatie opgeslagen in het kwantumsysteem. Hoe meer qubits, hoe groter het systeem, en hoe moeilijker om het af te schermen. 'Eigenlijk zit je in een kwantumsysteem met een continuüm van fouten', zegt kwantumfysicus Frank Verstraete. 'Het zijn er oneindig veel.' En toch is dit probleem in theorie opgelost. 'Collega's van mij (onder meer Peter Shor, red.) hebben bewezen dat het mogelijk is om miljoenen qubits in superpositie met elkaar te houden. Kortom, dat een kwantumsysteem arbitrair groot kan worden gemaakt, en dat er dus geen onoverkomelijke barrière is tussen de kwantumwereld en de macrowereld.'

Dat is een spectaculair idee. In feite betekent het dat een macroscopisch kwantumsysteem kan bestaan. Dat houdt dan weer in dat een voorwerp, of zelfs een levend organisme, bijvoorbeeld op twee plaatsen tegelijk kan zijn. Of dat de kat uit het beroemde gedachte-experiment van Erwin Schrödinger, een van de grondleggers van de kwantummechanica, tegelijk zowel dood als levend kan zijn.



GEEN SUPERPOSITIE



SUPERPOSITIE