

Quantumcomputer zoekt apps

Google wist als eerste met een quantumcomputer aantoonbaar sneller te rekenen dan met de beste gewone computer. Sinds die doorbraak wordt volop gespeculeerd over **toepassingen** van de wondermachine.

Door **George van Hal**



'Voor bedrijven moet dit een waarschuwing zijn. Als je niet al nadacht over de potentie van deze technologie, dan moet je nu beginnen', schreven drie medewerkers van adviesbureau Accenture in een opiniestuk dat zij in februari publiceerden op de site van de

Amerikaanse University of Pennsylvania.

De technologie die ze in hun hyperbolisch managementjargon vervolgens bombarderen tot 'hyperdisruptief' - iets dat de normale manier van zaken doen volkomen overhoop zal gooien - is de quantumcomputer. En zij zijn niet de enigen die enthousiast zijn over die futuristische wondermachine. Dat blijkt ook wel uit de klinkende euro's, dollars en yuans die vrijwel elke techreus, van



➔ Microsoft tot IBM, en van Google tot Alibaba, steekt in de ontwikkeling ervan. Kenners dromen zelfs hardop dat quantumcomputers in de toekomst speciaal op de persoon toegepaste medicijnen gaan ontwikkelen, of nieuwe materialen gaan ontwerpen waarmee we ons energieprobleem kunnen oplossen.

Die belofte komt voort uit de fundamenteel nieuwe manier waarop deze machines rekenen: met behulp van de magische, tegendraadse wetten van de quantumfysica. Die zorgen er onder meer voor dat de rekenenheden van de quantumcomputer - zogeheten quantumbits, kortweg qubits - niet alleen '0' of '1' kunnen zijn, zoals de bits in uw computer, maar ook '0' en '1' tegelijk.

De quantumcomputer was veertig jaar lang vooral spelerei

op papier,

■ of, op z'n best, beloftevol wetenschappelijk knutselwerk in het lab. Experts knoopten handjesvol qubits aan elkaar en schreven de theoretische artike-

len die de basis legden voor het vakgebied. Dat minutieuze academische voorwerk leidde vorig jaar plotsklaps tot een doorbraak. In oktober maakte Google in vakblad *Nature* bekend dat ze met hun quantumchip in 3 minuten een berekening hadden gedaan waar zelfs de allersnelste 'gewone' supercomputer 10.000 jaar over zou doen (al beweerde concurrent IBM dat het in tweeënhalve dag ook mogelijk was).

'De prestatie van Google is vooral van belang vanwege de achterliggende technologie', zegt Vandersypen. 'Ze kregen hun chip aan de praat en hielden die lang genoeg stabiel om ermee te rekenen.' Een flinke stap voorwaarts, maar de mythische status die Google eraan vastknoopte? Quantumsuperioriteit als startschot van een wereldwijde quantumrevolutie? Nee, dat (nog) niet.

Google had daarmee, in ronkende vaktaal, 'quantumsuperioriteit' bereikt, het punt waarop een quantumcomputer in een directe wedstrijd een klassieke computer kan verslaan. Dat kreeg het voor elkaar met een chip met daarop 'slechts' 53 qubits. 'Een prestatie die ik nog niet voor mogelijk had gehouden', zegt informaticus Harry Buhrman, hoofd van quantumsoftware-instituut QuSoft in Amsterdam.

Ondertussen sorteren bedrijven alvast voor op de volgende klapper. Sla de berichten erop na, en het lijkt wel of quantumcomputers nu al de eerste nuttige programma's draaien.

'Erg bijzonder', vindt ook fysicus Lieven Vandersypen, verbonden aan het Nederlandse quantumtechnologie-instituut QuTech in Delft, maar pas wel op. Het algoritme dat op die chip draaide, was zo ontworpen dat Google zijn quantumspierballen goed kon laten rollen, maar was in praktische zin volkomen nutteloos.

'Googles quantumsuperioriteitsalgoritme heeft zijn eerste nuttige toepassing gevonden', kopte het Britse populair-wetenschappelijke weekblad *New Scientist* in december. 'IBM en Daimler gebruiken quantumcomputer om een betere batterij te ontwikkelen', schreef IBM afgelopen januari in een persbericht. En in oktober meldden verschillende media dat autofabrikant Volkswagen zijn nieuwe 'quantumnavigatie-app' zelfs al ging testen in het verkeer.

Niets van waar, of op z'n best sterk overdreven, reageren experts. Die nuttige toepassing van Google? Draait ook op gewone computers. De b-IBM? Verre toekomstmuziek, get op theoretisch onderzoek. De quantumwagen dan? Pure misleiding. De autofa samen met D-Wave, een bedrijf dat 'gel door te doen alsof het een quantumcomputer is', terwijl dat helemaal niet het geval is', zo fysicus Anton Akhmerov, hoofd van de 'tinkerers'-onderzoeksgroep aan de TU



'In persberichten wordt veel onzin verkocht over de belofte van deze technologie. De verwachtingen zijn vaak ongefundeerd en onrealistisch', zegt Vandersypen. 'Begrijp me niet verkeerd: er is wel degelijk sprake van spectaculaire vooruitgang. Dit is in ons vak een spannende tijd. We knopen voor het eerst tientallen qubits aan elkaar. Er heerst optimisme. Maar dat voedt ook de overdrijvingen.'

Het is eenvoudig, zegt Buhrman: er bestaat nog geen nuttige toepassing voor quantumcomputers. 'We weten zelfs niet wat die eerste nuttige toepassing straks zal zijn.' Daarvoor zijn de quantumchips waaraan Google en concurrenten zoals IBM werken simpelweg te ver verwijderd van de eindversie waar quantumcomputerbouwers al decennia van dromen.

'De chips van Google en IBM bestaan uit vijftig tot straks zo'n honderd niet-stabiele qubits', zegt Buhrman. Niet-stabiel betekent: qubits waarop geen foutcorrectiesoftware draait. Net als gewone bits maken ook quantumbits soms fouten. 'Gewone' computers lossen dat op door de bits uit te lezen en te controleren of alles nog wel goed gaat. Maar dat kan bij een quantumcomputer nu net niet.

Quantumcomputers zijn namelijk zo gevoelig voor verstoring van buitenaf dat een qubit zijn quantumeigenschappen verliest wanneer je hem uitleest. Wil je quantumcomputers behouden voor fouten, dan moet je dus iets anders verzinnen. Dat 'iets anders'

bestaat, maar heeft een waar oerwoud aan 'extra' qubits nodig.

Over hoeveel 'extra' qubits je nodig hebt om één qubit foutenvrij te laten rekenen, lopen de schattingen uiteen. Experts denken aan honderd tot zelfs tienduizend extra qubits per stabiele qubit. In een toekomstige computer met honderd stabiele, foutvrije qubits zijn dan als het echt tegenzit een miljoen niet-zo-stabiele qubits nodig.

Tussen dat aantal en de tientallen qubits op de huidige generatie chips zit dus op z'n zachtst gezegd nogal een gat. En dat terwijl de algoritmen die experts de afgelopen jaren ontwikkelden juist bedoeld zijn voor de verre toekomstcomputers, niet voor de kleine, foutgevoelige versies die nu plotsklaps beschikbaar zijn.

Over de vraag of we met die tussenfase überhaupt iets nuttigs kunnen, verschillen de meningen. Akhmerov noemt het onwaarschijnlijk, omdat alle bekende quantumalgoritmen hoge precisie vereisen. 'Ik zou zeggen: blijf vooral proberen, maar verwacht er niet te veel van.'

Buhrman heeft geen idee wat mogelijk is, zegt hij - niet in positieve, maar ook zeker niet in negatieve zin. 'In de berekeningen van dit soort chips sluiten onherroepelijk fouten, ruis. Omdat je niet kunt voorspellen hoe die ruis zich gedraagt, kun je ook niet voorspellen welke algoritmen wel en niet op deze chips zullen werken. Je moet elke toepassing dus eerst uitproberen. Vooraf simuleren is onmogelijk', zegt hij. Wel meent hij dat het belangrijk is om er alvast mee aan de slag te gaan. 'We hebben de kennis van dit soort instabiele systemen nodig voor een beter begrip van de stabielere systemen.'

Dat een stabiele, toekomstige quantumcomputer zich nuttig kan maken, daarover is bijna iedereen het wel eens, al houdt bijvoorbeeld Akhmerov nog een slag om de arm. 'Het is een veilige gok, maar niet honderd procent zeker', zegt hij.

Sommige algoritmen die je erop kunt draaien zijn in elk geval al jaren bekend. In 1994 bedacht de Amerikaanse wiskundige Peter Shor bijvoorbeeld een manier waarop een quantumcomputer grote getallen efficiënt kan factoriseren, zoals wiskundigen dat noemen. Je rekent '21' dan bijvoorbeeld terug naar de factoren '7' en '3', die vermenigvuldigd weer '21' opleveren.

Als quantumcomputers dat kunnen voor (veel) grotere getallen dan 21, heeft dat onder meer gevolgen voor de versleuteling van gegevens. Veel gegevens worden nu beschermd met een groot getal, terwijl de bijbehorende factoren dienen als sleutel. Als een quantumcomputer die sleutel simpelweg kan berekenen, liggen de gegevens dus voor het oprapen.

'De ontdekking van het algoritme van Shor was voor mij een reden om voor dit vakgebied te kiezen', zegt Vandersypen. In 2001 lukte het hem als promovendus al om 15 te herleiden tot 5 en 3, met een quantumcomputer met zeven qubits. Leuk, maar nog lang niet nuttig, zegt hij. 'Het wordt pas interessant wanneer je dat sneller kunt dan een klassieke computer, voor een getal dat bestaat uit een paar honderd cijfers.'

Wie een quantumcomputer wil bouwen die stabiel genoeg is om het algoritme van Shor te draaien, moet nog wel wat praktische horden nemen, benadrukt hij. Zo weet nog niemand hoe je alle draden - één per qubit - straks op een chip moet krijgen. Zeker niet als zo'n quantumchip straks honderdduizenden qubits (en dus draden) moet bevatten, terwijl de huidige computerchips er op z'n best een paar duizend kwijt kunnen.

Hoelang het nog duurt voordat zo'n computer er is, blijft door dat soort kwesties vooralsnog koffiedik kijken. Vandersypen denkt dat we, wanneer echt alles meezit, over een jaar of tien zover zijn. 'Maar in de praktijk zit eigenlijk zelden alles mee', voegt hij daar meteen aan toe.

Volgens Akhmerov is het vooral de vraag of de techniek doorontwikkelen niet te moeilijk en (daardoor) duur is. 'Het zou kunnen dat quantumcomputers net zo moeilijk zijn als kernfusie', zegt hij. Die techniek, waarbij je energie wint door atomen samen te smel-

ten, is aantoonbaar mogelijk - de zon maakt er bijvoorbeeld gebruik van - maar blijkt zo lastig uitvoerbaar dat natuurkundigen er al decennia hun tanden op stuk bijten. 'Ik heb goede hoop dat het minder moeilijk is dan fusie, maar zolang we de oplossingen voor de technologische problemen nog niet kennen, weet niemand dat zeker.'

De toekomst van technologie voorspellen blijkt sowieso altijd lastig. Vandersypen wijst als voorbeeld op de beroemd geworden misser van voormalig IBM-baas Thomas Watson, die in 1943 beweerde dat er een wereldwijde markt zou zijn voor hooguit vijf computers. 'Niemand kan de impact overzien van dit soort radicaal nieuwe technologieën', zegt hij. Betrouwbaar voorspellen welke quantumapps straks populair zijn, is daarom vrijwel onmogelijk. Net zoals computerpionier Alan Turing niet had kunnen voorzien dat we met zijn vinding nu, zeventig jaar later, foto's van eten delen op Instagram en kattenfilmpjes streamen op YouTube. ●



**Dit is in ons
vak een
spannende
tijd. Er
heerst
optimisme.
Maar dat
voedt ook de
overdrijving**

**Ik heb goede
hoop dat het
minder
moeilijk is
dan kern-
fusie, maar
dat weet
niemand
zeker**

REKENEN MET MAFFE SUPERKRACHTEN

**Anders dan een klas-
sieke bit kan een qubit,
de quantumversie, '0'
en '1' tegelijk zijn.**

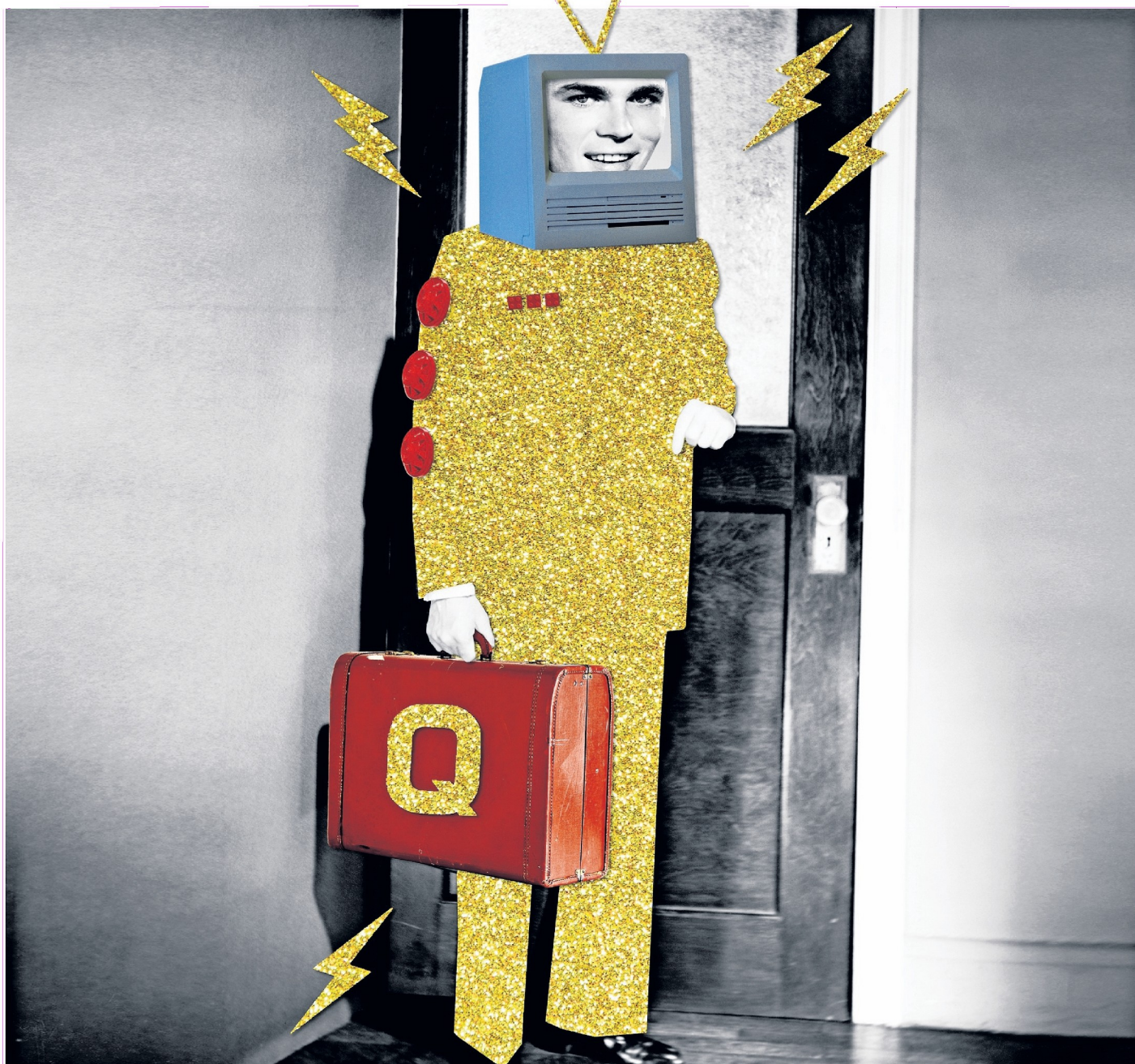
Quantumcomputers rekenen op een fundamenteel andere manier dan uw laptop of tablet. Ze maken gebruik van de tegendraadse wetten van de quantumfysica, de theorie die de natuur beschrijft op de kleinste mogelijke schaal: die van de elementaire deeltjes, de kleinste bouwstenen waaruit alles van planten tot planeten zijn opgebouwd.

Waar een mens niet tegelijk van het uitzicht kan genieten op de Eiffeltoren in Parijs en het Empire State Building in New York, kan een deeltje iets soortgelijks wel. Zo'n deeltje is dan, zeggen natuurkundigen, in 'superpositie': het bestaat op meerdere plekken tegelijk. Op dezelfde manier kan een qubit, de quantumversie van de klassieke bit, verschillende waarden tegelijk hebben. Daardoor kan een qubit niet alleen '0' of '1' zijn, maar ook '0' én '1'. En dan kunnen die qubits ook nog eens onderling zodanig verbonden

den raken – verstrengelen, zeggen experts – dat wie rekent met één qubit instantaan ook rekent met alle daarmee verbonden qubits. Combineer die twee maffe superkrachten en het resultaat is een computer die rekent als een enorme parallelle processor. Bij het zoeken van de snelste route naar een bestemming zal zo'n apparaat bijvoorbeeld niet één route per keer simuleren, maar alle routes tegelijk.

Om uiteindelijk de juiste route te vinden, moet je een algoritme bedenken waarbij de 'foute' antwoorden elkaar uitdoven. Zoals een noise cancelling-koptelefoon omgevingsgeluid verwijderd door een 'tegenovergesteld' geluidssignaal af te spelen, kan een slim algoritme alle foute antwoorden uitdoven, waarna alleen het goede antwoord resteert. 'Voor veel vraagstukken kan dat niet', benadrukt informaticus Harry Buhrman. 'Maar gelukkig zijn er ook problemen waarvoor we dat soort quantumprogramma's al geschreven hebben.'

Laurens Verhaar



Foto's **Astrid Anna van Rooij**

