Publicatie : PC-Active
Datum : 31 jul 2016
cm2 : 1.244
Pagina : 86
Advertentiewaarde : € 19.688,00
Regio : Nederland
Frequentie : 6x per jaar
Oplage : 85.000

DOOR: KOEN VERVLOESEM


# EEN QUANTUMCOMPUTER OP ELK BUREAU?

Quantumcomputers spreken al jaren tot de verbeelding, maar er is nog altijd geen bruikbare. Daar komt over enkele jaren misschien verandering in. Het Nederlandse QuTech verwacht tegen 2019 een quantumcomputer te hebben draaien.

Hoewel er elk jaar weer snellere processoren uitkomen, scherpere beeldschermen en harde schijven met meer capaciteit, is er fundamenteel al tientallen jaren niets meer aan onze computertechnologie veranderd. Maar in 1981 stelde Richard Feynman, een Amerikaanse Nobelprijswinnaar in de natuurkunde, een nieuw type computer voor: de quantumcomputer. Bij een quantumcomputer maakt men gebruik van de bijzondere eigenschappen van kleine deeltjes om quantumbits - of qubits - te creëren.

Een quantumcomputer kan door zijn bijzondere eigenschappen bepaalde berekeningen veel sneller uitvoeren dan een klassieke computer. Vooral voor wetenschappelijk onderzoek zou de quantumcomputer ons heel wat nieuwe inzichten opleveren. Aan de andere kant slagen quantumcomputers er ook in om bepaalde encryptie te kraken, zoals die wordt gebruikt voor internetbankieren. Maar dat wordt dan weer goedgemaakt door nieuwe mogelijke vormen van quantumencryptie. Kortom, de quantumcomputer biedt ons de eerste fundamen-

Publicatie : PC-Active
Datum : 31 jul 2016
cm2 : 1.244
Pagina : 86
Advertentiewaarde : € 19.688,00
Regio : Nederland
Frequentie : 6x per jaar
Oplage : 85.000

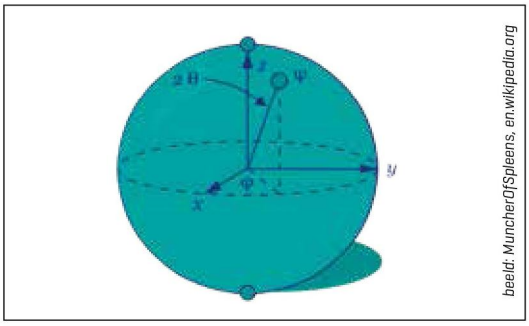
*Het Delftse onderzoekscentrum QuTech wil tegen 2019 een werkende quantumcomputer ontwikkeld hebben*

tele vernieuwing in computertechnologie in jaren. Maar waarom hebben we dan nog altijd geen quantumcomputers, terwijl Feynman al 35 jaar geleden op het idee kwam? Het grote probleem is dat de quantumeigenschappen heel onstabiel zijn. Voor quantumberekeningen die in theorie mogelijk zijn, is het een hele kunst om een quantumcomputer lang genoeg stabiel te houden om die berekeningen uit te voeren.

## WAT IS EEN QUANTUMBIT?

Naar analogie met een bit die zich in de toestand 0 of 1 kan bevinden, kan een quantumbit zich in de toestanden |0> en |1> en alle lineaire combinaties daarvan, bevinden. Zo'n lineaire combinatie noemt men een *superpositie*: a|0> + b|1>, waarbij de coëfficiënten a en b willekeurige getallen zijn. Zo zijn er toestanden mogelijk van 70% |0> en 30% |1>, of 10% |0> en 90% |1>. Men zegt wel eens dat de qubit zich dan tegelijk in toestand |0> en |1> bevindt.

Als we nu twee qubits tegelijk bekijken, dan zijn de basistoestanden |00>, |01>, |10> en |11>. Maar terwijl een klassiek koppel van twee bits zich enkel in één van zijn vier toestanden tegelijk kan bevinden, kan een koppel qubits ook bestaan in een superpositie van deze vier basistoestanden. De vier toestanden zijn dan allemaal tegelijk opgeslagen in het quantumregister van twee qubits. Meer in het algemeen kunnen we zeggen dat de hoeveelheid informatie in n qubits exponentieel met n stijgt (namelijk $2^n$), terwijl dat bij klassieke bits slechts lineair is (namelijk $n$).



beeld: Muncher0fSpleens, en.wikipedia.org

*Een qubit, de fundamentele bouwsteen van quantumcomputers, wordt voorgesteld door een blochvector in de blochbol*

En het leuke is: met het juiste algoritme voeren we in een quantumcomputer een berekening op al die verschillende toestanden tegelijk uit. Elke keer dat we een qubit toevoegen, wordt de quantumcomputer bovendien dubbel zo snel. Vandaar dus de vaak gehoorde kreet dat quantumcomputers exponentieel sneller zijn dan klassieke computers, al moet je dit wel met een korrel zout nemen: dit geldt alleen voor enkele specifieke berekeningen, zoals het factoriseren (ontbinden in factoren) van getallen - wat toevallig juist een uiterst interessante berekening is, die de veiligheid van allerlei encryptiesystemen in gevaar brengt. Veel encryptie vertrouwt immers op het feit dat het heel moeilijk is om uit een product van twee priemgetallen die priemgetallen af te leiden. Een quantumcomputer zet die veronderstelling op zijn kop.

## QUANTUMBEREKENINGEN

De moeilijkheid begint echter met het uitlezen van de toestand van een qubit (of een register van meerdere qubits). Het uitlezen verandert door de wetten van de quantumfysica immers de toestand van de qubit, waardoor hij 'ineenstort' van de superpositie tot één van de basistoestanden. De uitdaging is dus om de exponentiële kracht van een n-qubit systeem te benutten om een berekening efficiënt uit te voeren, maar toch bij het uitlezen van het register tot het gewenste resultaat te komen. Daarvoor zijn talloze slimme manieren bedacht en al even slimme algoritmes. Een goede uiteenzetting hiervan (in het Engels) is ook te vinden in het artikel Quantum Computing [1] op de Stanford Encyclopedia of Philosophy.

Abstract bekeken zien die algoritmes er als volgt uit. Na een meting wordt de toestand van het systeem door het ineenstorten geprojecteerd op één van de basistoestanden, zodat we de exponentiële informatie kwijt zijn. Om toch van deze informatie gebruik te kunnen maken, benutten we de eigenschap van *quantuminterferentie van de berekeningspaden*. Beschouw elke parallelle berekening als een 'berekeningspad'. Door quantuminterferentie kunnen deze elkaar gedeeltelijk annuleren. De kunst is nu om ervoor te zorgen dat enkel de berekeningen die ons interesseren overblijven en de rest elkaar annuleert, zodat we in staat zijn om de juiste oplossing te observeren.

Publicatie : PC-Active
Datum : 31 jul 2016
cm2 : 1.244
Pagina : 86
Advertentiewaarde : € 19.688,00
Regio : Nederland
Frequentie : 6x per jaar
Oplage : 85.000

# Quantuminterferentie

**Quantuminterferentie is kort gezegd: de eigenschap dat een elementair deeltje zich niet alleen op meer dan één plaats tegelijk kan bevinden (de superpositie, zie hiervoor), maar dat het ook zijn eigen pad kan kruisen en daardoor de richting van dat pad kan veranderen.**

Door de berekening zo op te zetten dat de coëfficiënt van de gewenste oplossing in de superpositie maximaal is en de coëfficiënt van alle andere mogelijke registerwaarden bijna nul is, geeft het uitlezen van het register met heel grote waarschijnlijkheid de juiste oplossing. Een quantumcomputer voert dus probabilistische (naar probabilisme, wat waarschijnlijkheidsleer betekent) berekeningen uit: je krijgt de uitkomst nooit met 100% zekerheid. Als we meer zekerheid willen, kunnen we achter altijd meerdere keren de berekening uitvoeren en controleren of de oplossing hetzelfde is.

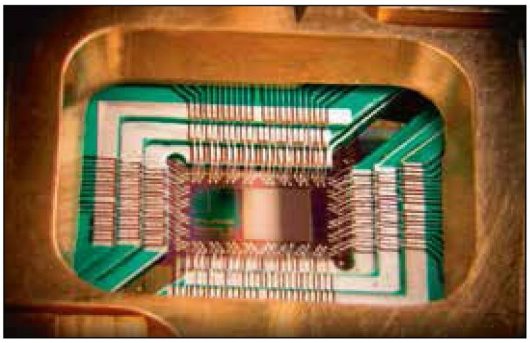
### EERSTE QUANTUMCOMPUTER IN 2019

In 2013 richtte de Nederlandse overheid het onderzoekscentrum QuTech [2] in Delft op, met de bedoeling een brug te vormen tussen het bestaande onderzoek naar quantumcomputers en de Nederlandse hightechindustrie. Tot de partners behoren onder andere TNO (Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek) en Microsoft. Aan het hoofd ervan kwam professor Leo Kouwenhoven van de TU Delft, die al heel wat baanbrekend onderzoek naar quantumcomputers heeft verricht. De ambitie is om de quantumcomputer eindelijk in realiteit te brengen.

Kouwenhoven denkt dat zijn groep binnenkort kan bewijzen dat het een quantumcomputer kan bouwen. Eerder al slaagde zijn onderzoeksgroep erin om een Majorana-quasideeltje [3] te creëren, wat een beloftevolle kandidaat is om qubits mee te bouwen. Tegen 2019 verwacht QuTech, dat intussen een honderdtal mensen tewerkstelt, een quantumcomputer te hebben draaien. Overigens beweert het Canadese bedrijf D-Wave Systems al enkele jaren een commerciële quantumcomputer te verkopen, maar wetenschappers twijfelen of het wel echt een quantumcomputer is.

Onlangs voegde Intel zich bij het project: de chipbakker gaat een tienjarige samenwerking aan met QuTech en investeert maar liefst 45 miljoen euro in het onderzoekscentrum. Intel zal de onderzoeksinspanningen van het Delftse instituut ook ondersteunen met mankracht, technische expertise en apparatuur.

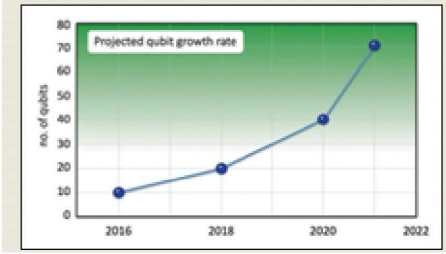
Momenteel slaagt men er bij QuTech in om een chip met 5 à 10 qubits te maken en die te programmeren. Volgens Kouwenhoven zal het nog een jaar of tien duren voor QuTech quantumchips heeft met genoeg qubits om relevante problemen te kunnen oplossen.



*Het Canadese bedrijf D-Wave Systems beweert een 128-qubit quantumcomputer te hebben*

# Hoeveel qubits?

**In 2014 creëerde een onderzoeksgroep aan UC Santa Barbara een quantumcomputer van 9 qubits. De komende jaren zijn systemen van 10 tot 20 qubits mogelijk. Tegen 2020 zouden we al quantumcomputers van 40 qubits hebben en een jaar later zouden volgens quantumcomputerspecialisten van QuSoft 70 qubits mogelijk zijn. Op dat moment zouden die computers berekeningen aankunnen die op een klassieke computer niet mogelijk zijn.**




*Het aantal qubits in quantumcomputers zal de komende jaren sterk toenemen*

Publicatie : PC-Active
Datum : 31 jul 2016
cm2 : 1.244
Pagina : 86
Advertentiewaarde : € 19.688,00
Regio : Nederland
Frequentie : 6x per jaar
Oplage : 85.000

**QUANTUMSOFTWARE**

Terwijl men zich bij QuTech op de hardwarekant van quantumcomputers focust, is in Nederland onlangs ook een onderzoeksinstituut opgericht dat zich met de softwarekant bezighoudt: QuSoft [4]. Dit is een samenwerking tussen het Centrum Wiskunde & Informatica (CWI), de Universiteit van Amsterdam (UvA) en de Vrije Universiteit Amsterdam (VU). De initiatiefnemers en wetenschappelijke directeuren van QuSoft zijn Harry Buhrman (leider van de 'Algorithms and Complexity'-groep bij CWI en hoogleraar Computerwetenschappen bij UvA) en Kareljan Schoutens (hoogleraar Theoretische Natuurkunde bij UvA). Uiteindelijk moet QuSoft doorgroeien tot een instituut met 35 tot 40 onderzoekers, zowel natuurkundigen als computerwetenschappers en wiskundigen.

QuSoft zal zich richten op de ontwikkeling van software en het vinden van toepassingen voor een toekomstige quantumcomputer. Er is tot nu toe immers vooral onderzoek verricht naar hóe we een quantumcomputer kunnen maken (de hardware). Maar stel dat we er, bijvoorbeeld door de inspanningen van het Delftse QuTech, eindelijk in slagen om een quantumcomputer met een redelijke verwerkingskracht te creëren, dan is die voorlopig maar voor een beperkt aantal soorten berekeningen in te zetten. Bij QuSoft zal men onderzoeken voor welke toepassingen we snellere quantumalgoritmes kunnen ontwikkelen.
De traditionele softwaretechnieken zijn allemaal toegespitst op klassieke computers en maken daardoor geen gebruik van optimalisaties die in quantumcomputers mogelijk zijn. Zogenaamde quantumalgoritmes vereisen fundamenteel nieuwe technieken en benaderingen om de bijzondere quantummechanische eigenschappen zoals superpositie, interferentie en verstrengeling te benutten.

Eén onderzoeksproject richt zich op de mogelijkheden van quantumcomputers met tien tot zeventig qubits. Kunnen we bestaande algoritmes voor klassieke computers daarop draaien, of moeten we ze aanpassen? Een ander onderzoeksproject zal zich richten op quantumcomputers met meer dan honderd qubits. Het kraken van encryptie is met dit aantal qubits al mogelijk. Voor quantumcomputers van deze grootte zullen nieuwe technieken nodig zijn om ze te debuggen, omdat de toestand van de computer te groot is om met klassieke debugtechnieken te controleren.

Tegelijkertijd zal een derde onderzoeksgroep werken aan de ontwikkeling van cryptografie die niet door quantumcomputers is te kraken: zogenaamde quantumencryptie. Want zodra de eerste werkende quantumcomputers beschikbaar zijn, zijn heel wat klassieke cryptografische algoritmes te kraken. We hebben dan nieuwe cryptografie nodig die bestand is tegen de slimmigheden van quantumalgoritmes.
Een laatste onderzoeksgroep bij QuSoft zal zijn aandacht besteden aan de architectuur van quantumcomputers. De software die we erop willen draaien, bepaalt immers de ideale manier om de hardware te maken. Als we dus quantumcomputers ontwerpen zonder rekening te houden met de architectuur die onze software vereist, kunnen we de mogelijkheden niet volop benutten.

Kortom, het onderzoek van QuSoft is complementair aan dat van QuTech, waardoor het onderzoek op het gebied van quantuminformatica in Nederland een breed terrein bestrijkt. Beide instituten gaan ook samenwerken aan een nationaal onderzoeksprogramma over quantuminformatie.

**EEN QUANTUMCOMPUTER OP JE BUREAU?**

Ondanks alle vooruitgang moet je niet verwachten dat we over enkele decennia allemaal een quantumcomputer hebben. Quantumcomputers zijn immers alleen bruikbaar om specifieke problemen op te lossen, zelfs als QuSoft het toepassingsgebied kan uitbreiden. Bovendien zijn het dure en grote machines. Ze zullen daarom vooral in de wereld van supercomputers verschijnen, bijvoorbeeld om nieuwe medicijnen te ontwikkelen, het weer te voorspellen en cryptografie te kraken. ■

Voor de bronnen bij dit artikel:
**WWW.HCC.NL/288-84**