

Kwantuminformatie

Kwantumcomputer als vervanger van klassieke computer

Onze wereld verandert in snel tempo, bijna met lichtsnelheid. Recent hebben enkele wetenschappers beweerd dat er deeltjes bestaan, neutrino's genoemd, die sneller zouden reizen dan het licht. Volgens de relativiteitstheorie kan dat niet. Onze digitale wereld bestaat uit enen en nullen. In de echte wereld weten we allang dat aan/uit, ja/nee en zwart/wit niet voorkomen. De werkelijkheid bestaat vooral uit vele verschillende grijsstinten. Ogenschijnlijk sneller reizen dan het licht en grijsstinten komen mooi bij elkaar in de wereld van kwantuminformatie.

Guus Pijpers

Kwantummechanica

Klassieke mechanica gaat over grote objecten, het terrein van de relativiteitstheorie. Kwantummechanica is een natuurkundige theorie die het gedrag van materie en energie op atomaire en subatomaire schaal beschrijft. De ontwikkeling startte aan het begin van de vorige eeuw. Veel wetmatigheden en nieuwe bevindingen leiden ertoe dat we nog weinig zeker weten van deze nieuwe wetenschappelijke discipline. Zo is het nagenoeg onmogelijk om op atomair niveau metingen te doen zonder het systeem te beïnvloeden of zonder meetinformatie te verliezen. Bovendien zijn de toestanden van deze atomaire deeltjes zo vluchtig dat het verval van die toestand een belangrijke factor wordt bij het goed opzetten en meten van kwantumsystemen. Elke wiskundige operatie op een kwantumsysteem is omkeerbaar, maar er zijn twee uitzonderingen. Ten eerste als het kwantumsysteem een interactie heeft gehad met de omgeving terwijl je de toestand van dat systeem niet kent. Ten tweede, logischerwijs, zoals we zullen zien, als je het kwantumsysteem gaat meten.

Een kwantumsysteem wordt beschreven met kwantuminformatie. Dat is de informatie die de verschillende toestanden van het systeem beschrijft. De belangrijkste informatie-eenheid is de kwantumbit, meestal *qubit* genoemd (afgeleid van het Engelse *quantum bit*).

Qubits

Bits zijn bekend: een bit is de kleinste eenheid van informatie. Een bit kent twee toestanden: ja/nee, kop/munt, 0/1. Kwantumbits, oftewel qubits, kunnen twee (of meer) toestanden *tegelijkertijd* aannemen. Dat wordt superpositie genoemd, een term ontleend aan de kwantummechanica. Elke toestand van een qubit is verbonden met een kans. Zo kun je 25 procent kans hebben op toestand A en 75 procent kans op toestand B. Daarbij is de totale kans van het systeem in elke toestand natuurlijk 1.

Een qubit heeft nog een apart kenmerk. Als we namelijk gaan meten in welke toestand de qubit zich bevindt, dan neemt de qubit een van de toestanden aan. Welke toestand dat is bepaalt de qubit helemaal zelf. Na de meting is een qubit met twee toestanden daardoor gewoon een bit.

Samenvatting

De kwantummechanica geeft beschrijvingen van de kleinste deeltjes in ons universum, het atomaire niveau. Deze kwantuminformatie heeft enkele unieke kenmerken die veel deskundigen nog voor raadsels en uitdagingen stellen. De inzet en het gebruik van kwantumcomputers om een kwantumsysteem te simuleren en begrijpen laten zien dat we aan het begin staan van revolutionaire ontwikkelingen en zienswijzen.

Een voorbeeld verduidelijkt dit. Stel je een gesloten doos voor waarin een munt ligt. Je rammelt met de doos. Op dat moment weet je niet welke kant boven ligt. Op de vraag wat boven ligt, antwoord je volgens de klassieke mechanica: 'Kop of munt.' Maar volgens de kwantumtheorie is het kop *noch* munt; het is kop *en* munt, omdat de toestand van de qubit een superpositie is van beide waarden. Als je de doos opent, meet je de toestand van de munt. Die geeft op dat moment de klassieke zienswijze weer.

Entanglement

Entanglement (verstrengeling) is een correlatie tussen twee kwantumdeeltjes. De waarden van de twee deeltjes zijn onverbrekelijk met elkaar verbonden. Wijziging van de waarde van het ene deeltje (bijvoorbeeld door te meten) leidt onherroepelijk en direct tot een vooraf vastgestelde waarde van het andere deeltje. Entanglement is voor ons moeilijk voor te stellen. Natuurkundigen hebben nog steeds geen verklaring hoe entanglement precies werkt. Ze zijn gedwongen te accepteren dat het werkt en dat atomaire deeltjes over grote afstanden met elkaar samenwerken. Met wiskundige modellen kun je entanglement beschrijven; verklaren doe je daarmee het verschijnsel niet. Einsteins relativiteitstheorie legt een maximum op aan de snelheid van informatie-uitwisseling. Entanglement trekt zich daar niets van aan. De verstrengelde deeltjes weten direct wat voor status het andere deeltje heeft wanneer het ene deeltje wordt gemeten. Daar komt geen (licht) snelheid aan te pas. Dat verleidde Einstein tot de uitspraak: 'Spooky action at a distance.'

Een van de manieren om entanglement voor te stellen zijn de vele etsen van Escher, of de in figuur 1 weergegeven tekening van W.E. Hill. Je kunt de tekening ophangen, maar om echt een

Het roodborstje

Het Noordoost-Europese roodborstje is een trekvogel die overwintert rond de Middellandse Zee. Met een reis van 13.000 kilometer voor de boeg trekken roodborstjes in september-november weg naar Afrika en keren in maart-april terug. Een reis zonder tomtom of andere hulpmiddelen. Er zijn aanwijzingen dat de vogels het magnetisch veld van de aarde gebruiken bij hun oriëntatie.

Recent hebben onderzoekers entanglement (verstrengeling) aangedragen als mogelijke verklaring voor deze prestatie. In een molecuul zijn twee elektronen met elkaar verstrengeld. Door de invloed van licht gedragen deze twee elektronen zich verschillend, maar ze blijven toch sterk met elkaar verbonden. Dat minieme verschil wordt vervolgens in de hersenen verwerkt tot een beeld van het magnetisch veld van de aarde. Deze kwantumeffecten zijn aangetoond in een laboratoriumomgeving. Theoretische berekeningen leveren een entanglement van ongeveer 50 microseconden op. Het verstrengelde systeem van een roodborstje laat een periode zien van zo'n 100 microseconden. Dat is voldoende tijd om die grote reis tweemaal per jaar te maken. We weten tot op heden niet hoe het roodborstje het voor elkaar krijgt om een dergelijke entanglement zo lang stand te houden.

van de twee vrouwen te zien ('te meten'), moet je een keuze maken. Op dat moment is ook de andere vrouw direct bekend. Zoals aangegeven kun je met verstrengelde deeltjes goed rekenen. De tekening kun je immers ook gewoon ophangen of verplaatsen. Een qubit kun je niet kopiëren. Dat zou immers betekenen dat je de toestand

»Een kwantumcomputer van slechts 10 qubits kan 1024 berekeningen tegelijkertijd doen«

gaat uitlezen, waardoor de qubit zijn superpositie verliest.

Om het begrip entanglement nog ingewikkelder te maken kunnen we de vergelijking maken met traditionele communicatie. Daarbij zijn altijd een zender en ontvanger te herkennen. In een kwantumomgeving met twee verstrengelde deeltjes bestaat dat onderscheid niet. Er is geen zender of ontvanger. Er bestaat zelfs geen boodschap tussen beide deeltjes. Twee kwantumdeeltjes kunnen zelfs met elkaar zijn verstrengeld *voordat* ze dat weten. Bedenk ook dat entanglement blijft bestaan zonder dat een van de twee deeltjes ooit wordt gemeten.



Figuur 1. 'Mijn vrouw en mijn schoonmoeder' – tekening van W.E. Hill (1915)

Kwantumcomputers

Een computer die gebruikmaakt van de principes en uitgangspunten van de kwantuminformatie, wordt een kwantumcomputer genoemd.

Deze computers verschillen van de bekende klassieke computers, die alle gebruikmaken van transistoren. Als de wet van Moore zich doorzet, en tot op heden geldt die nog steeds, zien we rond 2050 sowieso dat het atomaire niveau is bereikt. De verwerkingskracht moet daarna ergens anders vandaan komen. Kwantumcomputers lijken die rol te kunnen gaan vervullen. Want een kwantumcomputer van slechts 10 qubits kan 1024 berekeningen tegelijkertijd doen. Dat noemen we *massive parallelism*, naast de bij klassieke computers bekende seriële en parallelle informatieverwerking. Voor de inzet en het gebruik van kwantumcomputers moeten we wel het uitlezen van al die qubits goed onder controle krijgen.

Het snelle verval van qubits die met atomaire deeltjes moeten worden gemaakt (gesimuleerd), is de reden dat een kwantumcomputer voorlopig nog niet praktisch mogelijk is. Ook zijn er bij grotere kwantumsystemen meer manieren voor de kwantuminformatie om met de omgeving te communiceren, wat de stabiliteit niet ten goede komt. Toch hebben onderzoekers vorig jaar een record gevestigd door 14 qubits tegelijkertijd een verstrengelde status te geven. De praktische toepassingen laten nog even op zich wachten. Maar het feit dat het Amerikaanse ministerie van Defensie zeer geïnteresseerd is in de ontwikkeling van kwantumcomputers zegt genoeg. Een goede encryptie is voor dit ministerie immers essentieel.

Voorbeelden

Als je dan zo'n kwantumcomputer kunt bouwen, zijn een drietal praktische toepassingen op dit moment het meest voor de hand liggend. Ten eerste is dat factoring, ofwel het ontleden van een getal in zijn priemgetallen. In feite is dit de basis voor bijvoorbeeld encryptie. Want hoe sneller dat ontleden gaat, hoe eerder je een bepaalde encryptie kunt ontcijferen. Elke encryptie die nu in gebruik is, gaat ervan uit dat dit kraken van de code met de huidige computers te lang duurt om

Beam me up, Scotty

Een van de meest spraakmakende voorbeelden van kwantumsystemen is teleportatie. Natuurlijk is het geen echte overdracht. Bovendien wordt geen materie overgebracht maar informatie. Maar de term teleportatie is om de gegarandeerde aandacht wel goed gekozen.

Praktisch lijkt teleportatie niet te kunnen, omdat je een qubit niet kunt kopiëren. Maar we weten dat qubits op twee plaatsen tegelijkertijd kunnen bestaan, de entanglement. Twee qubits worden met elkaar verstrengeld met een afstand van een tot enkele meters tussen beide. De mogelijke afstand is afhankelijk van het atomaire deeltje dat je gebruikt om de qubit te simuleren. Vervolgens meet je de ene qubit en de kwantumstatus van de andere qubit is bekend.

Enkele jaren geleden is teleportatie over enkele honderden meters met fotonen met succes uitgevoerd. Met de meer stabielere ionen zijn nu enkele meters bereikt. Of dit de basis vormt voor een totaal nieuwe manier van communiceren zal de tijd uitwijzen.

effectief te zijn. Kwantumcomputers bestaan al sinds begin jaren tachtig, maar het eerste echte algoritme, factoring op kwantumcomputers, werd pas in 1994 geschreven.

Een tweede toepassing is simulatie. Kwantumcomputers zijn zelf ook een simulatie, want we moeten nog een qubit simuleren op een atomair deel als bijvoorbeeld een elektron of foton. Een derde toepassing is zoeken. Met zo veel informatie voorhanden is eerder het vinden van de juiste informatie het probleem dan de beschikbaarheid van informatie.

Toekomst

Kwantumsystemen staan op dit moment volop in de belangstelling. De kennis over de kleine deeltjes van ons heelal groeit razendsnel. Sommige auteurs stellen dat het universum in feite een gigantische kwantumcomputer is. Sinds het ontstaan van ons heelal, zo'n 10^{17} seconden geleden, zijn ongeveer 10^{100} bits aan informatie gegenereerd. Ons universum moet dan op een kwantumachtige manier werken, want onze

huidige computers kunnen die hoeveelheden gewoon niet aan. Dat deze auteurs op het macroniveau van het universum komen, levert alleen maar interessante zienswijzen en ideeën op over het ontstaan en de toekomst van onze wereld.

Literatuur

- Abbott, D., P.C.W. Davies & A.K. Pati (eds.) (2008). *Quantum Aspects of Life*. London: Imperial College Press.
- Baeyer, H.C. von (2003). *Information: The New Language of Science*. Cambridge, MA: Harvard Publishing Press.
- Bokulich, A. & G. Jaeger (2010). *Philosophy of Quantum Information and Entanglement*. Cambridge: Cambridge University Press.
- Chown, M. (2007). *Quantum Theory Cannot Hurt You: A Guide to the Universe*. London: Faber & Faber Limited.
- Clegg, B. (2006). *The God Effect: Quantum Entanglement, Science's Strangest Phenomenon*. New York: St. Martin's Press.
- Cox, B. & J. Forshaw (2012). *The Quantum Universe: Everything that can happen does happen*. New York: Penguin Books.
- Davies, P. & N.H. Gregersen (2010). *Information and the Nature of Reality: From Physics to Metaphysics*. Cambridge: Cambridge University Press.
- Desurvire, E. (2009). *Classic and Quantum Information Theory*. Cambridge: Cambridge University Press.
- Floridi, L. (2010). *Information: A Very Short Introduction*. Oxford: Oxford University Press.
- Hayashi, M. (2006). *Quantum Information: An Introduction*. Berlin: Springer.
- Jaeger, G. (2006). *Quantum Information: An Overview*. Berlin: Springer.
- Lloyd, S. (2006). *Programming the Universe: A Quantum Computer Scientist Takes On the Cosmos*. London: Vintage Books.
- Nielsen, M.A. & I.L. Chuang (2011). *Quantum Computation and Quantum Information: 10th Edition*. Cambridge: Cambridge University Press.
- Nixon, T. (2011). Quantum information. In: Ramage, M. & D. Chapman (eds.), *Perspectives on Information*. New York: Routledge.
- Roederer, J.G. (2005). *Information and Its Role in Nature*. Berlin: Springer.
- Seife, C. (2007). *Decoding the Universe: How the New Science of Information Is Explaining Everything in the Cosmos, from Our Brains to Black Holes*. London: Penguin.
- Vedral, V. (2010). *Decoding Reality: The Universe As Quantum Information*. Oxford: Oxford University Press.
- Vedral, V. (2011). Living in a quantum world. *Scientific American*, June, pp. 38-43.

Dr. ir. Guus Pijpers MBA

is managing director van Acuerdis. Hij helpt mensen effectief met informatie om te gaan. E-mail: ask@guuspijpers.com.