

# Een nieuwe informatica

Het realiseren van de hardware waarmee de duizelingwekkende mogelijkheden van de kwantum-ICT in de praktijk gebracht kunnen worden, is de nieuwe heilige graal van de experimentele natuurkunde. Mocht die worden gevonden, dan betekent dat het einde van heel wat gevestigde waarheden van de huidige, digitale, informatica. Er staan ons nog spannende tijden te wachten als informatie kwantum gaat, meent Sander Bais.

De gelauwerde Wet van Moore stelt dat gedurende de afgelopen zestig jaar het vermogen van computers en geheugens zich iedere achttien maanden verdubbeld heeft, dat wil zeggen exponentieel gegroeid is. Dit is het gevolg van de immense schaalverkleining van de basiscomponenten in onze computers. Als deze schaal echter die van individuele moleculen nadert, dan gelden voor die componenten niet langer de wetten van de klassieke natuurkunde, maar de kwantumwetten, en als kwantumfysica en informatica uiteindelijk samen door één deur moeten, zal dat dramatische gevolgen hebben.

In dit artikel zet ik uiteen waarom ons kwantumbesef binnen afzienbare tijd tot een essentieel andere informatica zal leiden. Informatie moet dan worden opgeslagen in kwantumtoestanden en dat heeft verstrekkende gevolgen. We gaan over van bits naar qubits of *qubits*. De onderliggende concepten van de kwantumtheorie zijn zo tegen-intuïtief dat ze tot de verbeelding spreken, ook van geleerden. Daarom dalen we in dit betoog eerst af in de krochten van de kwantumesoterie: een soort *Alice in Wonderland* voor gevorderden.

## KWANTESSENCE

Kwantesse is de kwintessence van kwantum. In het kwantumdomein heeft het doen van een waarneming onmiddellijk invloed op het waargenomen. Elke vorm van kwantumvoyeurisme laat onuitwisbare sporen na omdat er op fundamenteel niveau niet langer sprake is van een objectieve scheiding tussen object en subject. Alleen maar naar kijken is aankomen! Een kwantumtoestand wordt beschreven door een zogenaamde golf functie, ruwweg een soort kansverdeling van mogelijke uitkomsten van metingen. We zeggen dat ten gevolge van een waarneming er een instantane ineenstorting van de golf functie plaatsvindt, hetgeen betekent dat bij herhaling van precies dezelfde meting dezelfde uitkomst gevonden zou worden en dus dat die kansverdeling over mogelijke uitkomsten door die eerste meting drastisch is veranderd. Deze ineenstorting is de crux van het meetproces in de kwantumtheorie

Dan is er het onzekerheidsprincipe van Heisenberg dat impliceert dat er grootheden zijn die je niet tegelijkertijd met willekeurige precisie kunt meten. Bijvoorbeeld van zoets triviaals als een enkel deeltje, daarvan kun je niet tege-

lijkertijd de plaats en de snelheid exact bepalen. ‘Nou en?’ bent u geneigd te zeggen. Maar dit onnozele feitje levert voer – wat zeg ik – zware kost voor filosofen. Want stel dat ik de plaats van het deeltje heel nauwkeurig bepaal, dan moet de onzekerheid in de snelheid heel groot zijn en dat vertelt me dat ik dan niet weet waar dat deeltje korte tijd later zal zijn. Kortom, het klassieke determinisme gaat in rook op, want er is opeens sprake van een onontkoombaar indeterminisme op het meest fundamentele niveau.

Behalve ineenstorting en onzekerheid is er een derde eigenschap van de kwantumrealiteit die van belang is voor mijn betoog en dat is het verschijnsel van kwantumverstrengeling. Klassieke verstrengeling is een bekend verschijnsel, denk bijvoorbeeld aan het DNA van een eenelige tweeling dat honderd procent gecorreleerd is, dus als Truus in New York woont en Ans in Tokio, en we lezen de DNA-sequentie van Truus uit, dan weten we ook de uitkomst van een sequentiemeting van Ans in Tokio, omdat het DNA van de zusjes identiek is.

Laat ik nu de kwantumversie van dit verhaal beschrijven die bekendstaat als de Einstein-Po-

## Als kwantumfysica en informatica samen door één deur moeten, zal dat dramatische gevolgen hebben

dolski-Rosen (EPR)-paradox. In dit gedachte-experiment worden twee kwantumdeeltjes op een zeker tijdstip ergens simultaan gecreëerd, bijvoorbeeld boven Londen, waarna het een naar New York vliegt en het ander naar Tokio. De toestand waarin deze deeltjes zich bevinden is verstrengeld, hetgeen wederom betekent dat latere meetuitkomsten van deze kwantumzusjes in hoge mate gecorreleerd zijn. De kwantumcomplicatie is nu dat het doen van een meting aan het ene deeltje de toestand van dat deeltje kan veranderen en dat die verandering *instantaan* gevolgen kan hebben voor de toestand van het andere deeltje dat zich aan de andere kant van de wereld bevindt, en dus voor de verkregen meetuitkomsten aldaar.

De veranderingen in Tokio hangen dus af van wat de experimenterator in New York besluit te meten, en die keuze kan hij maken als beide deeltjes al lang en breed onderweg zijn. Dit verschijnsel heeft geen klassiek analogon. Ook al laat je een leger van genetisch ingenieurs zich uitleven op dat DNA van Truus, dan nog heeft dat geen gevolgen voor het DNA van Ans. Deze instantane kwantumwerking werd door Einstein ‘spooky action at a distance’ genoemd, en inderdaad: zo’n wisselwerking op zeer grote afstand suggereert dat er informatie met een snelheid groter dan die van licht kan worden uitgewisseld. Maar, als dat het geval zou zijn, zou dat in flagrante tegenspraak zijn met de postulaten van de relativiteitstheorie van niemand minder

dan diezelfde Einstein, die aanvankelijk dan ook dacht dat hij met de EPR-paradox de kwantumtheorie de genadeklap zou toedienen.

Gelukkig viel het mee, want het bleek dat in het voorgestelde experiment er niet echt informatie van New York naar Tokio wordt overgedragen: je kunt het EPR-principe niet gebruiken om informatie uit te wisselen zoals met een telefoon. Daarmee was Einsteins zielenrust tot op zekere hoogte hersteld, maar dat nam niet weg dat het effect van de verstrengeling en de instantane verandering van de toestand van een deeltje op grote afstand wel waar bleek te zijn. Dat is inmiddels – bijna een eeuw later – in vele laboratoria aangetoond. De correlaties in de veranderingen zijn zo subtiel dat je er net geen informatie mee kunt overdragen, maar het blijft zo dat de correlaties in de kwantumtheorie sterker kunnen zijn dan die in welke klassieke situatie dan ook.

Tot voor kort dachten de meeste fysici over deze esoterische kwantumverschijnselen nogal negatief en werd het tegen-intuïtieve karakter van de EPR-paradox toch vooral gezien als voor filosofen en epistemologen. De appreciatie van ingenieurs voor de verbijsterende toepassingen van dit soort esoterische kwantumeffecten op informatieopslag en -verwerking kwam inderdaad uiterst traag op gang. Maar nu, een eeuw later, heeft iedereen de mond vol van kwantuminformatie, kwantumteleportatie, kwantumcryptografie en kwantumcomputers. Het realiseren van de hardware waarmee deze prachtige mogelijkheden in de praktijk gebracht kunnen worden, is de nieuwe heilige graal van de experimentele natuurkunde. Informatie gaat kwantum!

## BANKGEHEIMEN

Even iets anders. De beveiliging van banken gaat met de RSA-sleutel, een coderingssysteem vernoemd naar Shamir, Rivest en Adleman. Waar het bij deze versleuteling in wezen om draait is dat de versleutelaar een groot getal *m* van enkele honderden cijfers maakt door twee grote priemgetallen *p* en *q* met elkaar te vermenigvuldigen. Het getal *m* is publiek, maar de factoren *p* en *q* zijn geheim. Om de code te kraken moet de ontcijferaar vervolgens gegeven *m* de getallen *p* en *q* berekenen. Dat lijkt makkelijk: als ik u het getal *m*=15 geef, dan weet u meteen dat 15 gelijk is aan 3 x 5. Einde oefening.

Er bestaan trouwens mooie computeralgoritmes om dit te doen, maar die worden zeer tijdrovend naarmate *m* groter, dit omdat de benodigde rekentijd exponentieel groeit met de lengte van het getal *m*. En dat is bij de konijnen af, want als je voor *m* in plaats van het getal 15 een getal van een paar honderd cijfers kiest, heb je al snel duizenden jaren rekentijd nodig om de code te kraken. Zo veel geduld heeft de georganiseerde misdaad doorgaans niet en dus is het veiligheidsprotocol van banken, dat gebaseerd is op een RSA-code van 768 cijfers, voornog bruikbaar.

De conclusie is niet gering, namelijk dat de



ARIKO INAOKA

Erna en Hrefna, een eenelige tweeling uit IJsland

machtigste computers dit soort sommetjes als het factoriseren van grote getallen heel erg lastig vinden; ze kunnen niet zo heel veel meer doen dan alle mogelijke gevallen een voor een uitproberen, en dat kost erg veel tijd. In de informatica worden problemen ingedeeld in complexiteitsklassen, en die exponentieel groeiende rekentijd is typisch voor problemen die tot de klasse genaamd NP behoren, terwijl bewerkingen als optellen, aftrekken, vermenigvuldigen en machtsverheffen tot de klasse P behoren, waarbij de rekentijd veel langzamer toeneemt. P staat hier voor polynomiaal (d.w.z. machtswetten) en NP staat ruwweg voor een probleem van het type ‘naald in de hooiberg’. Dat laatste vereist een zoekalgoritme dat uitputtend is en een exponentieel groeiende tijd vergt, terwijl het verifiëren van de oplossing heel makkelijk is, immers: een naald is een naald.

Opvallend is dat het factoriseren NP is, terwijl de verificatie door het vermenigvuldigen van de gevonden factoren weer P is. Dus er zijn ettelijke rechttoe rechtaan rekenproblemen die je aan een kind van tien kunt uitleggen, maar die zelfs een supersnelle teraflop-computer niet aankan. Als het probleem NP is, dan moet Meeneer van Dale een kleine eeuwigheid op antwoord wachten.

Er is een interessante kanttekening te maken bij deze computationele complexiteitsklassen. Het gaat bij de indeling natuurlijk wel om de tijdsduur voor het meest efficiënte algoritme, maar wat is het meest efficiënte algoritme? Hoe weten we nu of het best bestaande algoritme ook werkelijk het best mogelijke is? Er zou altijd nog een nerd kunnen opstaan die een algoritme presenteert waarmee het factorisatieprobleem P zou worden. Als je er zo naar kijkt, daagt wellicht het besef dat dit een zeer diep en moeilijk probleem is: *P or NP, that's the question*, want strikt genomen heeft nooit iemand bewezen dat er echt een onderscheid is tussen P en NP. Deze vraag is zelfs een van de tien grote onopgeloste millenniumproblemen die het Clay Mathematics Institute in Cambridge, Massachusetts heeft formuleerd. Een rigoureuus bewijs dat P gelijk is aan NP of juist niet, levert letterlijk een miljoen dollar op.

**INFORMATIE GAAT KWANTUM** Kwantuminformatietheorie gaat ervan uit dat informatie opgeslagen wordt, niet in bits die

nullen en enen bevatten, maar in qubits. Een qubit kun je het best opvatten als een vector (dat is een pijltje met een lengte en een richting zoals bijvoorbeeld een snelheid). De qubitvector heeft een lengte één, maar kan in elke richting in een vierdimensionale ruimte wijzen. Waar een bit slechts twee toestanden heeft, heeft de qubit een continuüm van mogelijke toestanden. Informatie wordt dus opgeslagen in een register van dit soort qubits, en informatieverwerking is niets anders dan dat deze qubits worden gemanipuleerd met bepaalde kwantumprocessen. Het effect is niet het omzetten van nullen en enen, maar het op een georkestreerde manier veranderen van de richtingen van die verzameling kwantumpijltjes.

De kwantumsetting is totaal anders en veel rijker dan de digitale, zeker als we daar de kwantumesoterie uit het begin van mijn verhaal aan toevoegen. Het zal de lezer niet verbazen dat veel gevestigde waarheden over informatie weer op losse schroeven komen te staan als ze in het kwantumperspectief geplaatst worden, zoals bijvoorbeeld de kwestie van P versus NP. Die vraag moet opnieuw geformuleerd worden en gegeneraliseerd naar kwantumcategorien QP en QNP. En dan kunt u zich voorstellen dat er iets bijzonders gebeurt, wat zeg ik, iets magisch esoterisch!

Wat dan? Wel, bijvoorbeeld dat problemen die thans tot NP behoren en dus niet in P zitten, wel in QP blijken te zitten. Dat zou impliceren dat de kwantumontcijferaar misschien in een paar uur een code kan kraken waar zijn digitale evenknie een kleine eeuwigheid voor nodig zou hebben. Voor het vinden van priemfactoren, zoals bij de gelauwerde RSA-sleutel, blijkt dat inderdaad het geval.

In 1994 zorgde Peter Shor voor enige opschudding toen hij een kwantumalgoritme publiceerde waarmee met een kwantumcomputer de priemfactoren *p* en *q* in polynomiale tijd gevonden kunnen worden. Dat zou betekenen dat wanneer de georganiseerde misdaad de beschikking krijgt over kwantumcomputers, het kraken van de huidige bankcodes die gebaseerd zijn op de factorisatie van heel grote getallen in priemfactoren, een fluitje van een cent zou worden: een uurtje stug doorrekenen.

Het verbaast dan ook niet dat de ontwikkeling van de kwantumcomputer zich in een buitenproportionele belangstelling van veilig-

heidsdiensten, banken en durfkapitalisten mag verheugen. In 2005 was ik medeorganisator van een van de eerste workshops voor de wetenschappelijke incrowd, over een nieuwe manier van het implementeren van kwantumtechnologieën. Daar ontwaarde ik tot mijn verbazing niet alleen de slonzig uitgedoste *usual suspects*, maar op de achterste rij ook een legertje van in driedelig grijs gestoken lieden. In de koffiepauze overvielen ze ons met indringende vragen nadat ze zich hadden voorgesteld als medewerker van ‘The office of sudden technological change’ of als ‘Dr X working for venture capitalist Y or Z’. Die rakkers kwamen even hun kwantumlicht opsteken.

Kwantumesoterie dwingt ons ertoe op een fundamenteel andere manier over informatie na te denken, met drastische gevolgen voor informatieverwerking en communicatie. En ik voorspel dat als onze ICT eenmaal kwantum gaat, dit nog tot vele onvoorziene en ingrijpende innovaties zal leiden.

De eerlijkheid gebiedt te zeggen dat kwantumcomputers niet alle taken exponentieel sneller kunnen doen, maar er is inmiddels een aantal kwantumalgoritmes ontwikkeld die substantiele tijdswinst boeken. Bovendien is er nog ander goed nieuws voor de gebruikers van kwantum-ICT. Dat heeft te maken met kwantumcommunicatie of kwantumteleportatie, een vorm van informatieoverdracht die intrinsiek niet af te luisteren valt. In de kwantumtheorie is het principeel onmogelijk om informatie exact te kopiëren, anders gezegd: als je een qubit kopieert, verander je per definitie de informatie van het origineel. Daar hebben de NSA en hun handlangers bij de AIVD nog niet van terug. Lang leve de privacy!

En zo neemt de harde wetenschap iedere keer de samenleving op de schop. Is het niet verbijsterend om te zien dat we door informatie systematisch te ontdoen van haar betekenis, zulke ingrijpende revoluties teweeg hebben kunnen brengen? Door de ruimte van grammatica's, metagrammatica's en ook kwantumgrammatica's diepgaand in al haar universaliteit te exploreren, zijn we op ongekende mogelijkheden gestuit. Dat heeft ons leven ingrijpend en onomkeerbaar veranderd.

