

Special

Nederlands Tijdschrift voor

# Natuurkunde

juni 2014-jaargang 80-nummer 6

Quantuminformatie  
van fundamenteel tot toepassing



Uitgave van de  
**Nederlandse Natuurkundige Vereniging**  
80<sup>e</sup> jaargang (2014), nummer 6

### NNV-bureau

lidmaatschappen en abonnementen

Nederlandse Natuurkundige Vereniging  
Noortje de Graaf (directeur), Anja Al,  
Debora van Galen Last (secretaresse)  
Postbus 41882  
1009 DB Amsterdam  
Telefoon: 020 59 222 11  
E-mail: bureau@nnv.nl  
Website: www.nnv.nl  
Leden van de NNV ontvangen maandelijks het NTvN. Opzeggen kan via  
www.nnv.nl. Opzeggingen voor het  
komende jaar dienen binnen te zijn voor 1  
december, het NNV-bureau zal de opzeg-  
ging binnen een week bevestigen.

### Redactiesecretariaat NTvN

artikelen en advertenties

Nederlands Tijdschrift voor Natuurkunde  
Esger Brunner/ Marieke de Boer  
Science Park 105, kamer N228  
Postbus 41882  
1009 DB Amsterdam  
Telefoon: 020 59 222 50  
E-mail: ntvn@ntvn.nl  
Website: www.ntvn.nl  
Twitter: NTvN\_tweets

### Redactie

Lodewijk Arntzen, TN-HH  
Rob van den Berg, Shell Amsterdam  
Claud Biemans, Amsterdam  
Erik van der Bijl, UU  
Marieke de Boer, *eindredacteur*  
Roeland Boot, Thorbecke VO en DIFFER  
Lo Bour, AMC  
Floor Broekgaarden, UvA  
Helko van den Brom, VSL  
Esger Brunner, *eindredacteur*  
Fiona van der Burgt, UU  
Edip Can, Saxon  
Menno van Dijk, Shell Amsterdam  
Eduard Driessens, CEA-Grenoble  
Richard Engeln, TUe, *hoofdredacteur*  
Aernout van Enter, RUG  
Iwan Hollerman, RUN  
Vincent Icke, UL  
Rob de Jeu, TU Delft  
Jeroen Kalkman, TU Delft  
Bart Klarenaar, TUe  
Herman de Lang, Rotterdam  
Erik Langereis, DIFFER  
Marco van Leeuwen, Nikhef en UU  
Frans van Lunteren, UL  
Tim Marcus, VUmc  
Hans Muller, Utrecht  
Gerard van Rooij, DIFFER  
Wilfried van Sark, UU  
Frans Snik, UL  
Kristiaan Temst, KU Leuven (B)  
Annemiek Vennix, TUe  
Wim Verkley, KNMI  
Bobby Vos, RUN  
Henk Vrielinck, U Gent (B)

Vormgeving Ori Ginale/Marc de Boer  
Opmaak EB/MdB  
Druk Ten Brink, Meppel  
Oplage 5000

## Quantummechanica en de publieke zaak

Enkele weken geleden las ik het boek *De terugkeer van het algemeen belang* van Roel Kuiper, voorzitter van een parlementaire onderzoekscommissie van de Eerste Kamer. Deze commissie heeft de gang van zaken onderzocht rond de privatiseringen en verzelfstandigingen van overheidsdiensten in Nederland gedurende de laatste dertig jaar. Door het boek ben ik beter gaan begrijpen waarom termen als marktwerking, kleine overheid, participatiemaatschappij enzovoorts bij mij zo veel irritatie opwekken. De boodschap van het boek is dat we, in de loop van de afgelopen decennia, de publieke zaak uit het oog hebben verloren. Tegelijk met de publieke zaak hebben we het belang van fundamenteel wetenschappelijk onderzoek uit het oog verloren. Dat is immers, zou ik zeggen, een essentieel onderdeel van de publieke zaak, net zoals onderwijs, gezondheidszorg en sociale voorzieningen. Het is een integraal onderdeel van onze culturele identiteit, een voortzetting van oude scholastieke tradities, en bepaalt daarmee onze plaats in Europa en de rest van de wereld. Het vormt bovendien de basis voor alle mogelijke technologische vernieuwingen.



## Tegelijk met de publieke zaak hebben we het belang van fundamenteel wetenschappelijk onderzoek uit het oog verloren.

De quantummechanica is een van de pijlers van de moderne natuurkunde. Het is niet nodig om te wijzen op de grote praktische betekenis die deze theorie heeft gehad in de vormgeving van ons dagelijks bestaan door de verschillende technologische ontwikkelingen die het heeft mogelijk gemaakt. Maar we lijken te zijn vergeten dat deze theorie het resultaat is van fundamenteel wetenschappelijk onderzoek in de eerste helft van de vorige eeuw. Ze werd ontwikkeld door een generatie natuurkundigen die de 'nutteloze' filosofische discussie over de interpretatie van de theorie niet uit de weg ging.

Door het pionierswerk van Bell hebben deze discussies, waarbij de toon werd gezet door Bohr en Einstein, onverwacht een nieuwe praktische dimensie gekregen. We maken nu mee hoe vruchtbaar die discussies zijn gebleken, ondanks de meewarigheid waarmee ze soms werden beschouwd in een tijdperk waarin pragmatisme en economisch belang de boventoon gingen voeren. Het bewijst de uitzonderlijke waarde van fundamenteel wetenschappelijk onderzoek en het toont aan hoe belangrijk het is dit weer te koesteren als onderdeel van de publieke zaak.

De artikelen in dit themanummer, bijeengebracht en deels geschreven door de gastredacteuren Miriam Blaauboer en Ronald Hanson van de TU Delft, laten zien hoe op basis van ogenschijnlijk nutteloze discussies over fundamentele interpretatiekwesties een geheel nieuw vakgebied tot ontwikkeling is gekomen met grote mogelijkheden om ons dagelijks bestaan diepgaand te veranderen.

Wim Verkley

## Inhoudsopgave

inleiding	176	<b>Quantumcomputers en quantuminformatie</b> Miriam Blauboer
	179	<b>Quantumcomputers: hoe en wanneer?</b> Ronald Hanson en Floris Zwanenburg
	183	<b>Quantumalgoritmes en cryptografie</b> Ronald de Wolf
	186	<b>Veilig communiceren met quantummechanica</b> Caspar van der Wal
de uitdaging	189	<b>Quantummijnenveger</b> Lodewijk Arntzen
ken uw klassieken	190	<b>Quantumverstrekking</b> Herman de Lang
ken uw klassieken	193	<b>Voor wie de klok heeft horen luiden...</b> Ad Verbruggen
loopbaan	196	<b>De quantumbeveiliger</b> Jeremy Butcher
	198	<b>Quantumzekere authenticatie</b> Boris Škorić en Pepijn Pinkse
onderwijs	201	<b>Quantumwereld in de klas</b> Lodewijk Koopman
	204	<b>Verstrengeld of niet? Bells ongelijkheid in spelvorm</b>
	206	<b>Een klassieke meting met behulp van een quantumdetector?</b> Tjerk Oosterkamp
interview	210	<b>QuTech: samen bouwen aan een quantumcomputer - interview met Leo Kouwenhoven</b> Marieke de Boer
boekbespreking	213	<b>50 inzichten quantumfysica</b> Richard Engeln
	214	<b>Magnetische roosters van koude atomen als quantumsimulatoren</b> Arthur L. La Rooij en Robert J.C. Spreeuw
cultuurkunde	217	<b>Quantumobjecten</b> Wim Verkley
	218	<b>Verstrengeling: de sleutel tot veeldeeltjesfysica?</b> Karel Van Acocleyen en Frank Verstraete
student	222	<b>Quantumstage</b> Suzanne van Dam
leukje	223	<b>De ultieme laptop</b> Herman de Lang
	224	<b>Magnetische bewustwording</b> Sander Otte
column	227	<b>Wie had dat gedacht?</b> Klaas Landsman
	228	<b>Maakt D-Wave quantumcomputers?</b> Miriam Blauboer
	230	<b>Quantumrekenen met Majoranadeeltjes</b> Carlo Beenakker
groepsportret	232	<b>Detectie van één enkel foton</b> Esger Brunner en Marieke de Boer

175

Het Nederlands Tijdschrift voor Natuurkunde is het maandelijkse tijdschrift van de Nederlandse Natuurkundige Vereniging en richt zich op de Nederlandstalige natuurkundige gemeenschap. Ingezonden artikelen, recensies, discussies en mededelingen – op het gebied van de natuurkunde in brede zin – zijn welkom. Inzendingen kunnen worden gestuurd naar het redactiesecretariaat, of naar redactieleden. Richtlijnen voor auteurs staan

op [www.ntvn.nl](http://www.ntvn.nl), of zijn op te vragen bij het redactiesecretariaat.

De redactie behoudt zich het recht voor om artikelen te weigeren, in te korten of anderszins te wijzigen zonder opgave van reden.

De auteursrechten van de artikelen in dit tijdschrift liggen bij de desbetreffende auteur(s).

Echter, artikelen kunnen geplaatst worden op de internetpagina's:

- [www.natuurkunde.nl](http://www.natuurkunde.nl)
- [www.kennislink.nl](http://www.kennislink.nl)

Niets van deze uitgave mag op welke wijze dan ook gekopieerd of verveelvuldigd worden zonder nadrukkelijke toestemming van de auteur(s).

# Quantumcomputers en quantuminformatie

**In de jaren tachtig opperde Richard Feynman het idee om quantummechanische systemen te gebruiken voor het uitvoeren van berekeningen. Inmiddels is de quantumcomputer – een computer die volgens quantummechanische principes werkt – een bekend begrip en zijn er talrijke ideeën ontstaan voor het gebruik van quantummechanica om informatie te bewerken, versturen, beveiligen enzovoort. In Nederland en Vlaanderen wordt er op dit gebied, zowel theoretisch als experimenteel, onderzoek gedaan – aanleiding voor het NTvN om dit jaar een themanummer aan quantuminformatie te wijden. Dit artikel geeft een korte inleiding over de opkomst van (quantum)computers, de basisprincipes van quantuminformatieverwerking en de inhoud van dit themanummer.** Miriam Blauboer

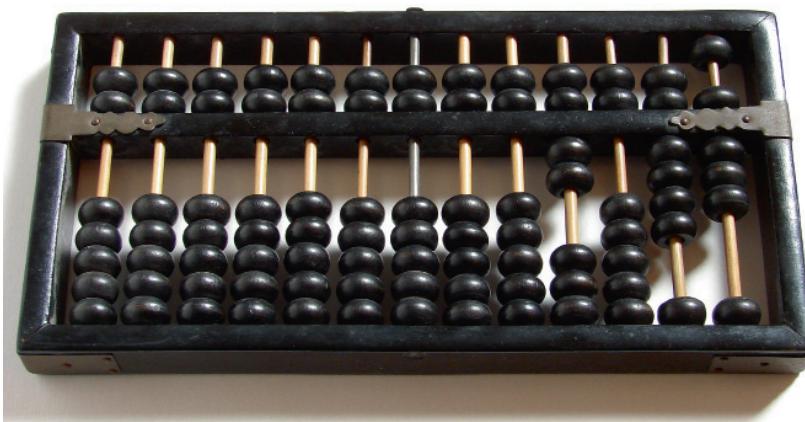
176

## Rekenapparaten door de eeuwen heen

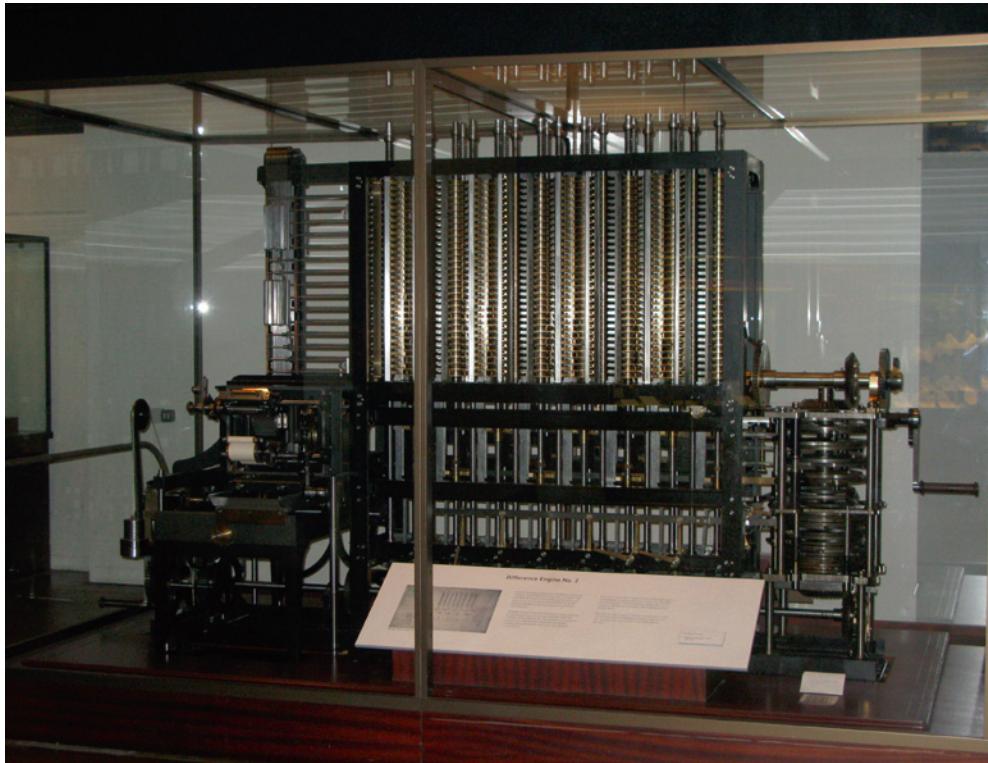
Het oudste op grote schaal in de wereld gebruikte rekenapparaat is het telraam, ook wel abacus genoemd. De eerste telramen, waarmee de gebruiker getallen kon optellen en aftrekken, dateren waarschijnlijk van rond 2500 voor Christus en kwamen uit Babylonië [1]. Geavanceerdere ver-

sies, waarmee je ook kon vermenigvuldigen, delen en worteltrekken, zijn gevonden bij opgravingen in Perzië en Griekenland en vermoedelijk afkomstig uit de vijfde eeuw voor Christus. Gedurende vele eeuwen was het telraam het belangrijkste rekenhulpmiddel – pas in de laatste 400 jaar is hier verandering in gekomen. Het begon halverwege de zeventiende eeuw toen

de Franse wis- en natuurkundige Pascal een mechanische rekenmachine, de pascaline, bouwde waarmee de basisoperaties optellen, aftrekken, vermenigvuldigen en delen uitgevoerd konden worden. Pascals uitvinding leidde tot de ontwikkeling van allerlei mechanische rekenmachines, onder andere door Leibniz en De Colmar, en wordt gezien als de vroegste voorloper van de hedendaagse computer. Ongeveer twee eeuwen later, in 1821, ontwierp de Engelsman Charles Babbage de eerste geautomatiseerde mechanische rekenmachine, de zogenaamde difference engine, die tabellen van polynomiale functies kon berekenen. Later breidde hij dit ontwerp uit tot een algemenere machine die instructies van ponskaarten kon lezen en daarmee het eerste programmeerbare rekenapparaat zou worden: de analytical engine. Op papier was deze analytische machine een gigantisch apparaat dat uit duizenden mechanische onderdelen bestond en aangedreven werd



**Figuur 1** Een eenvoudig telraam of abacus. Foto: David R. Tribble.



Figuur 2 De difference engine in het London Science Museum.

door een stoommachine. Babbage heeft door geldgebrek zijn machines nooit zelf kunnen bouwen – daardoor bleef de vraag of deze daadwerkelijk zouden werken lange tijd onbeantwoord. In de jaren tachtig van de vorige eeuw is de difference engine alsnog gebouwd in het Londen Science Museum naar het originele ontwerp van Babbage en met materialen uit zijn tijd (zie figuur 2). Het apparaat bleek foutloos te werken en is sindsdien in Londen te bezichtigen.

Een kleine eeuw na Babbage's analytische machine kwam weer een grote sprong voorwaarts, toen Alan Turing en John von Neumann onafhankelijk van elkaar een wiskundig model voor een programmeerbare computer bedachten. Nieuw aan dit idee was de universaliteit van de voorgestelde computer – in principe kon ieder programma erop uitgevoerd worden. Daarna gingen de ontwikkelingen snel. Halverwege de jaren veertig van de vorige eeuw werd de eerste elektronische digitale programmeerbare computer gebouwd (voor Britse onderzoekers die in het kader van het zogenaamde Enigma project tijdens de Tweede Wereldoorlog Duitse codes probeerden te kraken). Deze Colossus bestond uit honderden vacuümbuizen en was geschikt voor het draaien van een vast programma. In de jaren zestig verschenen de eerste supercomputers

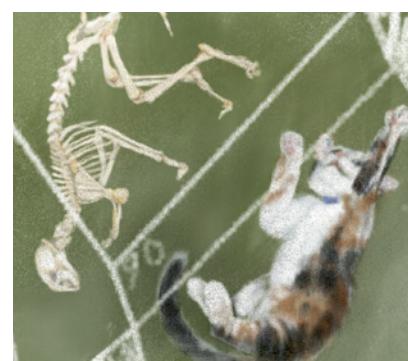
en kort daarna de eerste microprocessors, die de basis legden voor de opkomst van de pc's. Miniaturisatie van deze microprocessoren heeft er sinds de jaren tachtig van de vorige eeuw voor gezorgd dat de rekenkracht van computers voortdurend toegenomen is. In dezelfde jaren tachtig ontstond er echter ook een nieuw en geheel ander idee op het gebied van rekenapparaten: het idee voor een computer die quantummechanisch opereert, de zogenaamde quantumcomputer.

### De quantumcomputer

In een lezing in 1981 [2] stelde Richard Feynman de vraag of quantummechanische processen, zoals bijvoorbeeld de evolutie van waarschijnlijkheidsverdelingen, efficiënt gesimuleerd zouden kunnen worden op een computer die quantummechanisch opereert. Hij liet zien dat een gewone ('klassieke') computer hierbij exponentieel zou verlangzamen, terwijl zijn hypothetische universele quantumsimulator dat niet zou doen. Een paar jaar later, in 1985, bouwde David Deutsch dit idee uit tot een beschrijving van een quantum-Turing-machine, ook wel universele quantumcomputer genoemd – een abstract model voor een machine waarmee de werking van een quantumcomputer gemodelleerd kan worden. Hij stelde ook een algoritme voor dat op deze

computer gedraaid zou kunnen worden, het zogenaamde Deutsch-Jozsa-algoritme [3]. Gegeven een onbekende functie  $f: \{0,1\}^n \rightarrow \{0,1\}^n$  berekent dit algoritme met één enkele aanroep of de functie constant ( $f(0) = f(1)$ ) of gebalanceerd ( $f(0) \neq f(1)$ ) is. Een klassiek algoritme zou hier twee aanroepen voor nodig hebben.

Het concept van een quantumcomputer fascineerde zowel natuurkundigen, wiskundigen als informatici. Uit de hoek van de laatste twee disciplines kwamen al snel ontwerpen voor quantumalgoritmes die op een quantumcomputer gedraaid zouden kunnen worden en betrekking hadden op specifieke vraagstukken die een klassieke computer vermoedelijk niet in redelijke tijd op kan lossen. Bekende voorbeelden hiervan zijn de algoritmes van Peter Shor (voor het ontbinden van ge-



Figuur 3 De illustratie op de voorkant is gemaakt door Lillian Blouin.



Figuur 4 Alan Turing.



Figuur 5 Richard Feynman.



Figuur 6 David Deutsch.

hele getallen in priemfactoren) en Lov Grover (voor het zoeken naar een specifiek element in een ongesorteerde database). Daarnaast ontstonden vele nieuwe ideeën voor het gebruik van quantumsystemen in informatieverwerking. Twee voorbeelden hiervan, die elders in dit nummer uitgebreider aan bod komen, zijn transport van informatie via quantumteleportatie en het op een intrinsiek veilige manier opstellen van sleutels voor het beveiligen van informatie, de basis van de quantumcryptografie.

### Basisprincipes van quantuminformatieverwerking

Wat maakt dat quantummechanica zich leent voor het sneller uitvoeren van bepaalde berekeningen en het veilig versleutelen van informatie? Het antwoord op deze vraag is terug te voeren op twee unieke eigenschappen van quantummechanische systemen: het principe van superpositie en het fenomeen van verstrengeling. Superpositie is de eigenschap van quantummechanische golffuncties om tegelijkertijd in twee toestanden te kunnen verkeren. In de taal van bits kan een

quantumdeeltje – een quantumbit, of kortweg qubit – zich in een toestand bevinden die tegelijkertijd ‘0’ en ‘1’ is. Het is deze eigenschap, in combinatie met het golfkarakter van de quantumtoestanden, die in quantumalgoritmes gebruikt wordt om de benodigde rekentijd voor specifieke vraagstukken exponentieel te reduceren.

De tweede quantummechanische eigenschap die van belang is voor quantuminformatieverdracht is verstrengeling, de niet-lokale quantumcorrelaties die tussen quantumsystemen kunnen bestaan. Door middel van het ruimtelijk scheiden van verstrengelde deeltjes waarbij de quantumcorrelaties behouden blijven, heeft lokale wisselwerking van een van de deeltjes met andere deeltjes in zijn omgeving invloed op de toestand van het partnerdeeltje dat zich ergens anders bevindt. Hiervan maken veel quantuminformatieprotocollen, zoals teleportatie, gebruik. Verstrengeling wordt daarom ook wel de ‘brandstof’ van quantuminformatieverdracht genoemd.

### Dit themanummer

In dit themanummer komt een ver-

scheidenheid aan onderwerpen uit de quantuminformatie aan bod waaraan in Nederland en Vlaanderen gewerkt wordt. Sommige artikelen hebben met name betrekking op de fundamentele aspecten van quantuminformatieverdracht, zoals de artikelen over quantumalgoritmes en quantumcryptografie, quantummagnetisme, topologisch beschermd rekenen, quantumsimulatoren van koude atomen en quantum-correlaties in veeldeeltjessystemen. Andere artikelen besteden uitgebreid aandacht aan mogelijke (technische) toepassingen van quantummechanica en het gebruik van quantummechanische principes, zoals de artikelen over hoe je een quantumcomputer bouwt, veilig communiceren, quantumsensoren en quantumzekere authenticatie. Daarnaast vindt u een speciale geïllustreerde middenpagina, en natuurlijk de vaste rubrieken – onder meer een Leukje, een Uitdaging, een Column, een Loopbaan, en twee Ken uw klassieken, alle passend in het thema quantuminformatie. Namens alle leden van de kernredactie van dit nummer (Wim Verkley, Gerard van Rooij, Richard Engeln, Ronald Hanson en ikzelf) wens ik u veel leesplezier toe.

## Bedankt

We willen iedereen bedanken die aan dit themanummer heeft bijgedragen; alle auteurs en onze redactie. Twee mensen willen we graag bij naam noemen, te weten Miriam Blaaboe en Ronald Hanson. Zij waren voor dit nummer gastredacteur en hebben ervoor gezorgd door mee te denken over wat er in dit nummer moest komen, auteurs te vragen, artikelen te redigeren en zelf bijdragen te leveren aan het themanummer, dat dit nummer een mooi beeld geeft van onderzoek aan quantuminformatie in Nederland en Vlaanderen. Hartelijk dank daarvoor!

### Referenties

- 1 G. Ifrah, *The Universal History of Computing: From the Abacus to the Quantum Computer*, Wiley, New York (2001).
- 2 Tijdens de Physics of Computation conferentie op MIT, Boston. Transcript gepubliceerd als R.P. Feynman, *Int. J. Th. Phys.* 21, 467 (1982).
- 3 M.A. Nielsen en I.L. Chuang, *Quantum Computation and Quantum Information* Cambridge University Press, Cambridge (2010).

# Quantumcomputers:

## hoe en wanneer?

**Door gebruik te maken van superpositie en verstrekking kunnen quantumcomputers en quantumnetwerken taken verrichten die met de huidige ICT gebaseerd op ‘klassieke’ bits niet mogelijk zijn. Maar hoe maak je eigenlijk een quantumcomputer? Is er maar één manier? En wat zijn de fysische bouwstenen? In dit artikel geven we een overzicht van architectuur van een quantumcomputer en van mogelijke implementaties, beschrijven we de state-of-the-art en speculeren we wanneer de eerste quantumcomputer het licht zal zien.** Ronald Hanson en Floris Zwanenburg

**H**et centrale idee achter quantum-ICT is om gebruik te maken van quantummechanische bits, die niet alleen de klassieke bitwaarden 0 en 1 kunnen aannemen maar ook elke mogelijke superpositie van de twee. In de jaren negentig van de vorige eeuw werd dankzij belangrijke theoretische ontdekkingen duidelijk dat quantum-ICT mogelijkheden biedt die buiten het bereik liggen en altijd zullen blijven liggen van ICT met klassieke bits (zie de artikelen van Ronald de Wolf op pagina 183 en Caspar van der Wal op pagina 186). Dit inzicht was het begin van wat nu wel de tweede quantumrevolutie wordt genoemd, en luidt een nieuw tijdperk in waarin quantummechanische superposities niet slechts bestudeerd worden, maar waarin ze volledig gecontroleerd en toegepast kunnen worden. Dat vooruitzicht zette veel onderzoeks-groepen aan om te gaan kijken naar mogelijke implementaties: waarmee bouw je nou een quantumcomputer? Wat is een geschikt fysisch systeem om quantumbits mee te maken? Om dat te beantwoorden moeten we een model hebben van de quantumcomputer en begrijpen wat de eisen zijn aan de quantumbits.

### Foutencorrectie in quantumbits

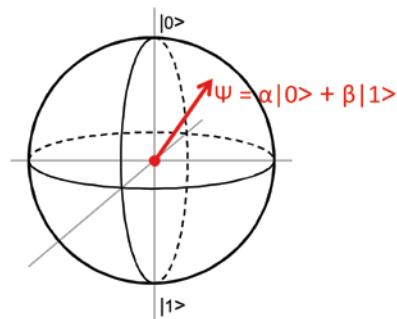
Geen enkel apparaat werkt perfect. De truc is om de kans op foutjes zo klein te maken dat we er bijna nooit last van hebben. Voor klassieke bits is het nog redelijk eenvoudig: er zijn maar twee bitwaarden die in een fysische grootheid zoals elektrische spanning geencodeerd hoeven te worden. Door de twee waarden ver van elkaar te kiezen wordt de bit robuust tegen foutjes. Bij quantumbits is dit anders: elke afwijking is meteen een fout.

Peter Shor deed in 1995 de cruciale ontdekking dat fouten in quantumbits toch gecorrigeerd kunnen worden met behulp van verstrekking [1]. Als de kans op een fout per quantumbit onder een bepaalde drempelwaarde zit (de zogeheten *fault-tolerant error threshold*) kunnen speciale algoritmes het aantal fouten verder verminderen en lange berekeningen mogelijk maken. Is de kans op een fout groter dan de drempelwaarde, dan zal toepassing van foutencorrectie de fouten alleen maar versterken. De foutendrempel is daarmee een zeer belangrijke graadmeter voor de haalbaarheid van de quantumcomputer [2].

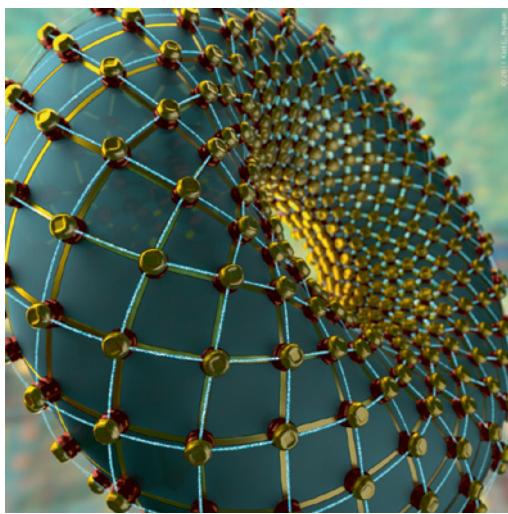
### Circuitmodel

Het eerste voorgestelde model voor

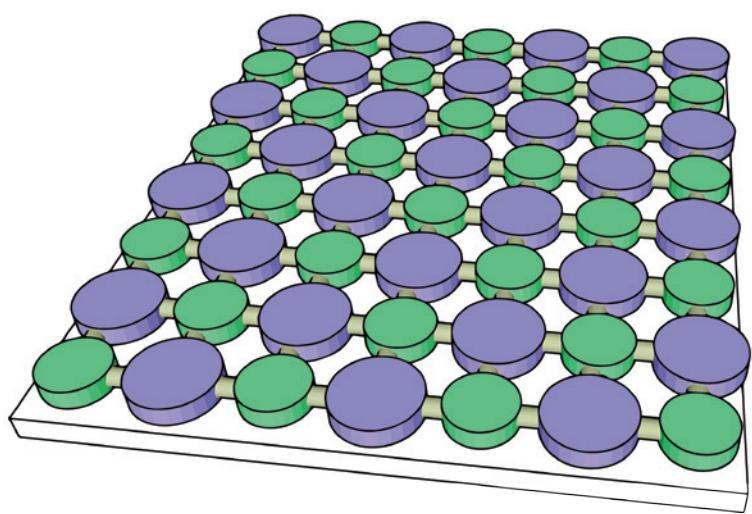
een quantumcomputer – het circuit-model – is een directe vertaling van de conventionele computer. Een computerberekening bestaat in dit model uit een reeks logische operaties (poorten) uitgevoerd op de quantumbits, die voorafgaand aan de berekening allemaal geprepareerd zijn in de toestand ‘0’. De poorten die op meerdere quantumbits tegelijk werken, worden geïmplementeerd door gebruik te maken van de wisselwerking tussen de quantumbits (bijvoorbeeld de magne-



**Figuur 1** Quantumbit gerepresenteerd als een vector op een Blochbol. De toestand  $\Psi$  van een quantumbit is in een quantummechanische superpositie van de basistoestanden  $|0\rangle$  en  $|1\rangle$ . Wiskundig schrijven we dat als  $\Psi = \alpha|0\rangle + \beta|1\rangle$ , en de meetkundige representatie van een dergelijk twee-niveausysteem tekenen we als een Blochvector.



**Figuur 2** Kitaev's torus: een topologische quantumcomputer, waarbij de quantumbits (de knooppunten) op het oppervlak van een torus zitten. Elke quantumbit kan wisselwerken met vier naburige quantumbits (de lijnen). Figuur: Karl Nyman.



**Figuur 3** Surface code: een topologische quantumcomputer, waarbij de quantumbits (de schijven) in een vlak liggen. De paarse schijven zijn quantumbits die de data encoderen en de groene schijven zijn quantumbits voor de foutencorrectie. Figuur uit [6].

tische interactie tussen spins). Tijdens de berekening ontstaan in het algemeen sterk verstrengelde toestanden van vele quantumbits. Als de berekening klaar is, kunnen de quantumbits (of een gedeelte daarvan) individueel worden uitgelezen, waarbij deze elk een '0' of een '1' opleveren. Deze 0-en en 1-en samen zijn het antwoord van de berekening. Dit circuitmodel is het meest bekend en meest toegepast tot nu toe.

Wat zijn de eisen aan quantumbits in het circuitmodel? Van conventionele computers is bekend dat alle mogelijke berekeningen terug te voeren zijn tot slechts één logische poort. Een voorbeeld van zo'n universele poort is de NAND-poort (bitwaarde aan de uitgang is 0 dan en slechts dan als beide ingangsbits de waarde 1 hebben). Ook voor de quantumcomputer blijken zulke eenvoudige universele bouwstenen te bestaan. Voor het circuitmodel is een twee-quantumbitpoort – bijvoorbeeld de quantum-exclusive OR – in combinatie met volledige controle over de enkele quantumbits genoeg om alle mogelijke quantumberekeningen uit te voeren. Het circuitmodel is populair onder fysici omdat het op een natuurlijke wijze de quantumberekening volgt. Een nadeel is echter dat de foutendrempel – voorzover nu bekend – erg scherp is: slechts één fout per grofweg 10.000 poorten is toegestaan.

## Quantumrekenen door te meten

Ondanks alle ontdekkingen in de ja-

ren negentig is het niet geheel duidelijk waarin precies de kracht van de quantumcomputers huist. Een bewijs van dit gebrek aan inzicht is misschien wel de verrassende ontdekking dat quantumberekeningen op een geheel andere manier uitgevoerd kunnen worden. Briegel en Raussendorf ontdekten begin deze eeuw measurement-based quantum computing [3]. Rekenen in dit model werkt radicaal anders dan het circuitmodel, hoewel bewezen is dat de modellen equivalent zijn aan elkaar. Voorafgaand aan de berekening worden eerst alle quantumbits met elkaar verstrengeld. Deze grote verstrengelde toestand heet een cluster state. Bepaalde cluster states zijn universeel: elke berekening kan ermee uitgevoerd worden. De berekening zelf bestaat uit het een voor een meten van de quantumbits, waarbij de meetbasis (langs welke richting het quantumbit wordt gemeten) afhangt van alle eerdere meetuitkomsten. Meetbases in één vlak zijn genoeg voor universele berekeningen. Het interessante aan dit quantumcomputermode is dat er tijdens de berekening geen wisselwerking tussen de quantumbits nodig is. Om deze reden is het een interessant model voor fotonen (die elkaar niet zien) en voor goed geïsoleerde systemen zoals enkele ionen en defecten in de vaste stof.

## Topologisch quantumrekenen en de surface code

De topologische quantumcomputer is eind vorige eeuw bedacht door Kitaev.

Zijn idee is om quantuminformatie niet-lokaal (topologisch) op te slaan, zodat lokale verstoringen geen fouten kunnen introduceren. Een voorbeeld van gebruik van topologie om stabiele quantumbits te maken is beschreven in het artikel van Carlo Beenakker over Majorana-deeltjes op pagina 230. Hoewel het originele idee van Kitaev tot een zeer gunstige foutendrempel leidde, was het niet praktisch omdat de computer op het oppervlak van een torus gebouwd moest worden [4]. Maar een paar jaar geleden ontdekten Raussendorf en anderen dat topologisch rekenen mogelijk is in twee dimensies – in één vlak dus [5]. Dit model – de zogeheten surface code – combineert elementen van topologisch rekenen en van measurement-based quantum computing. Voor veel experimenteel fysici is dit model nu het meest veelbelovend omdat het alleen wisselwerking tussen naburige quantumbits vereist en een foutendrempel heeft van ongeveer één fout op honderd poorten – in de buurt van de huidige state-of-the-art.

Naast bovenstaande modellen worden ook andere ideeën onderzocht, zoals adiabatisch quantumrekenen waarbij de hele quantumcomputer in de grondtoestand blijft. De haalbaarheid van deze modellen is op dit moment niet geheel duidelijk.

## Hoe groot moet de quantumcomputer zijn?

Uit hoeveel quantumbits een quantumcomputer moet bestaan hangt af

Qubit	Cartoon	Sterke punten	Zwakke punten
<b>Fotonen</b>  Qubit-toestanden 0 en 1: Polarisatie links- en rechtsom		<ul style="list-style-type: none"> <li>Weinig decoherentie</li> <li>Mobiel: beste kandidaat voor lange-afstand-communicatie van quantuminformatie</li> </ul>	<ul style="list-style-type: none"> <li>Zwakke interacties: twee-qubitpoorten lastig te realiseren</li> <li>Beweegt te snel op tijdschalen van controle-elektronica</li> </ul>
<b>Ingevangen atomen</b> in vacuüm, bijvoorbeeld Yb.  Qubit-toestanden 0 en 1: Hyperfijn energieniveaus binnen atomen		<ul style="list-style-type: none"> <li>Goed controleerbare qubits met lange coherentietijden (<math>&gt;1</math> s)</li> <li>Twee-qubitpoorten kunnen via fononen of fotonen</li> <li>Interface naar fotonen voor lange-afstandcommunicatie</li> </ul>	<ul style="list-style-type: none"> <li>Koppeling via fononen niet schaalbaar naar meer dan ~30 atomen</li> <li>Koppeling via fotonen nog te langzaam (~1 s)</li> </ul>
<b>Quantumdots</b> in vaste stof: Elektronspin in quantumdot  Qubit-toestanden 0 en 1: Spin omlaag en spin omhoog		<ul style="list-style-type: none"> <li>Schaling van devices op een chip in principe mogelijk</li> <li>Volledig elektrische aansturing van qubits mogelijk</li> </ul>	<ul style="list-style-type: none"> <li>Controle vooralsnog beperkt door decoherentie</li> <li>Reproduceerbaarheid: devices niet identiek</li> </ul>
<b>Doteringsatomen</b> in vaste stof:  Elektronspin gebonden aan doteringsatoom of kernspin van doteringsatoom (bijvoorbeeld: P-atoom in silicium of <b>NV center (nitrogen-vacancy)</b> in diamant)  Qubit-toestanden 0 en 1: spin omlaag en spin omhoog		<ul style="list-style-type: none"> <li>Zeer robuuste qubits: vergelijkbaar met ingevangen atomen</li> <li>Volledig elektrische aansturing van qubits soms mogelijk</li> <li>Schaling van devices op een chip in principe mogelijk</li> <li>Interface naar fotonen voor lange-afstandcommunicatie</li> </ul>	<ul style="list-style-type: none"> <li>Directe koppeling tussen atomen vereist grote nauwkeurigheid in plaatsing</li> <li>Koppeling via fotonen nog te langzaam (~100 s)</li> </ul>
<b>Supergeleidende Qubits</b> met Josephson-juncties (X in circuit)  Qubit-toestanden 0 en 1: <ul style="list-style-type: none"> <li>Ladingsqubit: Lading aan- en afwezig</li> <li>Flux qubit: Magnetische flux omhoog en omlaag</li> <li>Fase qubit: fase over junctie → spanning over junctie 0 en eindig.</li> </ul>		<ul style="list-style-type: none"> <li>Bijna macroscopische qubits: collectieve gedrag van ~10 miljard elektronen in device van ongeveer 0,1 mm</li> <li>Alle logische operaties zijn snel (<math>&lt;1</math> <math>\mu</math>s)</li> <li>Grote ontwerpervrijheid van circuitparameters</li> </ul>	<ul style="list-style-type: none"> <li>Coherentietijden nog beperkt (typisch 10 <math>\mu</math>s)</li> <li>Reproduceerbaarheid: devices niet identiek</li> <li>Schaling naar veel qubits op 1 chip lastig vanwege de grootte.</li> </ul>

**Tabel 1** Overzicht van de vijf meest prominente quantumbitsystemen: fotonen, ingevangen atomen in vacuüm, quantumdots en doteringsatomen in vaste stof en supergeleidende quantumbits (qubits).

Floris Zwanenburg (1976) studeerde technische natuurkunde aan de TU Delft. In 2008 promoveerde hij in Delft op onderzoek naar halfgeleidende nanodraden bij Leo Kouwenhoven. Na een postdoc aan UNSW in Sydney keerde hij in juni 2011 terug naar Nederland om te beginnen als assistant professor aan de Universiteit Twente, waar hij onderzoek leidt in zijn specialisatie silicium quantumelektronica.



f.a.zwanenburg@utwente.nl

van het doel. Op dit moment kunnen de beste conventionele computer-clusters een quantumcomputer van ongeveer dertig quantumbits simuleren. Een quantumcomputer van vijftig quantumbits ligt dus ver buiten bereik van klassieke simulaties, en dat zal voorlopig zo blijven. (Bedenk dat de vijftig qubits  $2^{20} \sim 10^7$  meer vrijheidsgraden hebben dan dertig qubits!). Daarmee is het maken van een processor met meer dan dertig quantumbits meteen een belangrijke mijlpaal geworden. Om simulaties te doen van andere quantumsystemen is wellicht hetzelfde aantal quantumbits al interessant (zie het artikel van Robert Spreeuw en Arthur La Rooij op pagina 214). Aan het andere eind van het spectrum staat het kraken van codes met het quantumalgoritme van Shor (zie het artikel van Ronald de Wolf op pagina 183), waarvoor een veel grotere machine nodig is. Er moet ook foutencorrectie worden ingebouwd wat leidt tot significante overhead in het aantal benodigde quantumbits. Het kraken van een code die nu ver buiten bereik ligt van conventionele computers zal met het *surface code*-model dan ook grofweg een miljard quantumbits vergen.

### Status van de experimenten

Sinds het midden van de jaren negentig zijn vele voorstellen gedaan voor het maken van quantumbits met uiteenlopende systemen. Elk van deze systemen heeft voor- en nadelen. We hebben geprobeerd de meest prominente samen te vatten in een grote tabel (zie tabel 1), maar waarschuwen explicet dat het veelal appels met peren vergelijken is. Grofweg kunnen we het veld als volgt samenvatten. Het

meest geavanceerde systeem op dit moment zijn gevangen ionen in hoog vacuüm. Dit systeem heeft bijna alle records in handen qua complexiteit van berekeningen, het aantal volledig controleerbare quantumbits in een opstelling (rond de acht) en demonstraties van foutencorrectie in handen. David Wineland (Nobelprijs 2012) is een van de pioniers in dit veld. De ionensystemen lijken echter niet schaalbaar naar meer dan honderd quantumbits binnen een ionenvak. Recent onderzoek richt zich onder meer op het ontwikkelen van modules van zo'n tien tot vijftig ionen, die dan gekoppeld kunnen worden via optische kanalen.

Een betere schaling kan wellicht verkregen worden met quantumbits in de vaste stof, analoog aan de huidige computerchips. Op dit moment zijn supergeleidende quantumbits en defecten in diamant de twee vaste-stofsystemen die het best onder controle zijn. In beide zijn universele logische poorten en simpele quantumberekeningen met drie quantumbits aangegeven. Elektronenpins in quantumdots of rond doteringsatomen zijn ook interessant omdat ze geheel elektronisch aangestuurd zouden kunnen worden, maar lopen achter wat betreft de beheersbaarheid. Verder zijn fotonen een veel gebruikt platform dat weliswaar niet schaalbaar lijkt naar een grote quantumcomputer maar waarmee wel veel pionierswerk is verricht, vooral in de richting van measurement-based quantum computing en quantumcommunicatie. Kijkend naar de tabel moge het duidelijk zijn dat op dit moment geen duidelijk beste systeem kan worden aangewezen. Dat maakt de wereldwijde wedloop naar de eerste quantumcomputer een spannende concurrentiestrijd tussen zeer uiteenlopende onderzoeksgebieden in de fysica.

### Wanneer is de quantumcomputer een feit?

We gaan ten slotte speculeren. De stap van de huidige quantumprocessoren met een handvol quantumbits naar een computer bestaande uit meer dan dertig quantumbits is conceptueel niet heel groot. Als de huidige ontwikkeling zich doorzet zal binnen vijf tot tien jaar een dergelijke computer in

Ronald Hanson (1976) is Antoni van Leeuwenhoekhoogleraar aan de TU Delft. Hij promoveerde cum laude in Delft bij Leo Kouwenhoven en had een postdocpositie aan UC Santa Barbara bij Awschalom. Sinds 2007 leidt hij onderzoek aan quantumrekenen en communicatie met diamant, ondersteund door onder andere een Vidibeurs (2007) en een ERC Starting Grant (2012). Sinds 2010 is hij lid van De Jonge Akademie van de KNAW.

R.Hanson@tudelft.nl



gebruik zijn. Daarmee kunnen dan de huidige theorieën over foutencorrectie grotendeels worden getest en zal het duidelijk worden of de computer van een miljard quantumbits realistisch is. De volgende stap van dertig naar grofweg duizend quantumbits wordt meer en meer een engineeringklus. Vele problemen die de komende jaren nog omzeild kunnen worden in de fundamentele experimenten moeten dan opgelost worden. Denk aan het parallel aansturen en uitlezen van quantumbits, snelle (klassieke) dataverwerking voor foutencorrectie en het terugdringen van de fouten tot ver onder de foutendrempel. Als dit lukt zullen we een machine bouwen met onbekende mogelijkheden: volledige controle over een enorm aantal quantummechanische vrijheidsgraden, waarmee we een wereld binnengaan die tot nu toe verborgen is gebleven achter een gordijn van omgevingsruis en complexiteit. Dit zal tot nieuwe toepassingen leiden in quantum-ICT, maar ongetwijfeld ook tot diepe nieuwe inzichten in de fundamentele wetten van de quantummechanica en tot een grote sprong voorwaarts voor de vele vakgebieden waarin klassieke computers niet krachtig genoeg zijn om de quantummechanische eigenschappen van de natuur te modelleren.

### Referenties

- 1 P. Shor, *Phys. Rev. A* **52**, R2493(R) (1995).
- 2 M.A. Nielsen en I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000).
- 3 R. Raussendorf en H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
- 4 A. Kitaev, *Ann. Phys.* **321**, 2 (2006).
- 5 R. Raussendorf en J. Harrington, *Phys. Rev. Lett.* **98**, 190504 (2007).
- 6 N. H. Nickerson, Y. Li en S. C. Benjamin, *Nature Communications* **4**, 1756 (2013)

# Quantumalgoritmes en cryptografie

**Quantumcomputers kunnen sommige problemen veel sneller oplossen dan de beste klassieke computers, bijvoorbeeld het breken van veelgebruikte computerbeveiliging. Aan de andere kant zijn er ook quantummechanische beveiligingsmethodes die zelfs niet kunnen worden gekraakt door een quantumcomputer. In dit artikel bespreken we de belangrijkste quantumalgoritmes die tot nu toe gevonden zijn en de belangrijkste gevolgen daarvan voor de cryptografie.** Ronald de Wolf

## Quantumalgoritmes: soms veel sneller, vaak ook niet

Een algoritme is een computerrecept: een serie concrete, simpele instructies die stapsgewijs de invoer omzetten in de gewenste uitvoer. Hoe minder instructies er nodig zijn, hoe sneller het algoritme is. Een klassiek algoritme voert instructies uit op bits, variabelen die 0 of 1 kunnen zijn. Een computer met  $k$  bits kan dus in  $2^k$  mogelijke basistoestanden zijn. Een computer met  $k$  quantumbits (qubits) kan in een superpositie van al deze  $2^k$  mogelijke basistoestanden zijn, waarbij elke basistoestand zijn eigen ‘amplitude’ heeft. De toestand van zo’n quantumcomputer wordt dus beschreven door

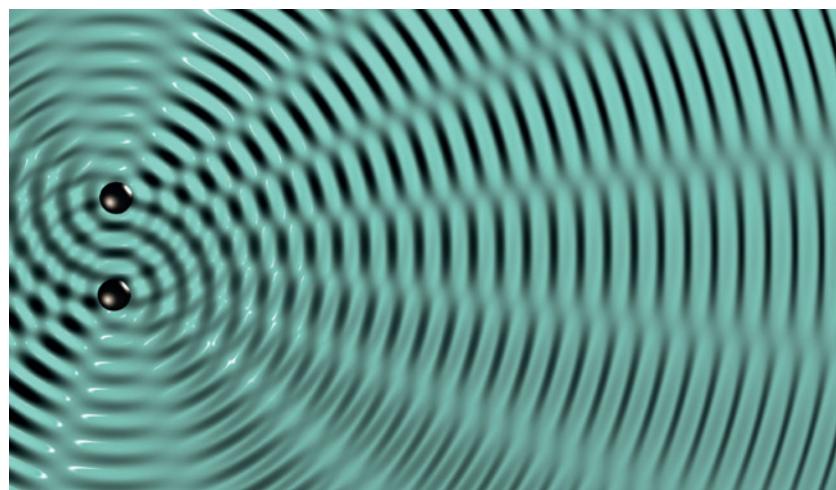
een vector van  $2^k$  amplitudes. De som van de kwadraten van die  $2^k$  amplitudes moet 1 zijn; hierdoor kunnen we de gekwadrateerde amplitude van een basistoestand interpreteren als de waarschijnlijkheid dat een meting van de quantumsuperpositie die basistoestand als uitkomst geeft. De amplitudes kunnen zowel positief als negatief zijn, wat interferentie-effecten mogelijk maakt zoals bij golven: als je positieve amplitudes bij elkaar optelt dan versterken ze elkaar en als je positieve en negatieve amplitudes bij elkaar optelt dan doven ze elkaar uit. Een quantumalgoritme heeft dankzij effecten als superpositie en interferentie meer instructies ter beschikking dan klassieke computers en dit leidt soms tot veel snellere algoritmes.

## Het factorisatiealgoritme van Shor

Een belangrijk voorbeeld is het quantumalgoritme van Peter Shor [1] waarin grote getallen in hun priemfactoren kunnen worden ontbonden. Zoals Euclides rond 300 voor Christus al wist, kan elk geheel getal op een unieke manier geschreven worden als het product van priemgetallen:  $15 = 3 \cdot 5$ ,  $91 = 7 \cdot 13$  enzovoorts. Voor kleine getallen kun je met een beetje moeite die priemfactoren nog wel vinden, maar het factoriseren van een getal van duizend cijfers ligt voor zover we weten ver buiten de mogelijkheden van klassieke computers. Het is dus erg interessant dat een quantumcomputer dit wel efficiënt kan.

De eerste stap in het algoritme van Shor definieert een periodieke functie  $f$ , gebaseerd op het te factoriseren getal  $N$ . Deze functie herhaalt zich steeds na  $r$  invoerwaarden:  $f(x) = f(x+r) = f(x+2r) = \dots$

Het blijkt dat je de priemfactoren van  $N$  kunt afleiden uit deze periode  $r$ . Het quantumdeel van het algoritme van Shor berekent  $r$ . We weten al langer dat Fouriertransformaties gebruikt kunnen worden om periodieke signalen te analyseren, bijvoorbeeld bij de opslag en analyse van muziek.



Afbeelding van interferentie. Interferentie is een van de effecten die er voor zorgen dat sommige quantumalgoritmes veel sneller zijn dan klassieke algoritmes.

Shor creëert een superpositie over alle invoerwaarden van  $f$ , en laat op dit ‘periodieke signaal’ een efficiënte quantumversie van de Fouriertransformatie los om  $r$  te vinden.

### Het zoekalgoritme van Grover

Een ander belangrijk voorbeeld is het zoekalgoritme van Lov Grover [2]. Dit lost zoekproblemen op waarbij je  $N$  ongesorteerde items hebt waarvan er maar één goed is. Stel bijvoorbeeld dat je iemands telefoonnummer weet, maar niet diens adres. Het telefoonboek is op naam gesorteerd en niet op nummer. Door alle namen in het telefoonboek af te lopen, zul je uiteindelijk het juiste telefoonnummer tegenkomen en dan kun je daar het bijbehorende adres aflezen. Als het telefoonboek  $N$  nummers bevat, dan zijn hier meestal bijna  $N$  stappen voor nodig (soms zit het gezochte nummer helemaal aan het begin van het boek, maar daar kun je niet van uitgaan). Het algoritme van Grover lost dit soort zoekproblemen op in ongeveer  $\sqrt{N}$  stappen. Het werkt als volgt. Aan het begin heeft het algoritme geen idee op welke van de  $N$  locaties het gezochte item zich bevindt, dus begint het met een uniforme superpositie waarin elke mogelijke locatie amplitude  $1/\sqrt{N}$  heeft. De truc is nu om stapsgewijs ongeveer  $1/\sqrt{N}$  extra amplitude naar de goede locatie te ‘verschuiven’. Deze extra amplitude is natuurlijk afkomstig van de andere locaties, want de som van de kwadraten van de amplitudes moet 1 blijven. Na  $\sqrt{N}$  van zulke stappen is de amplitude van de juiste locatie ongeveer 1 geworden en de amplitude van alle andere locaties ongeveer 0. Als je nu de toestand meet, dan zie je waarschijnlijk

de juiste locatie! Deze kwadratische versnelling is minder indrukwekkend dan de verbetering die Shor geeft, maar zoekproblemen komen zoveel voor dat ook zo'n kleinere verbetering heel nuttig kan zijn, bijvoorbeeld voor het vinden van de kortste weg van A naar B in navigatiesoftware.

### Waar is een quantum-computer nog meer goed voor en waarvoor niet?

Sinds de algoritmes van Shor (1994) en Grover (1996) is er nog een aantal nieuwe algoritmes gevonden, bijvoorbeeld gebaseerd op quantumversies van random walks. Een heel andere toepassing is het simuleren van grote quantumsystemen, zoals moleculen. Hierin is de farmaceutische industrie geïnteresseerd. Dit is een van de interessantste toepassingen van quantumcomputers, omdat momenteel een flink deel van de rekenkracht van klassieke supercomputers hieraan besteed wordt en omdat deze toepassing al interessant wordt wanneer we een quantumcomputer van vijftig à honderd qubits hebben.

Simulatie was de oorspronkelijke reden voor Richard Feynman om quantumcomputers te bestuderen. Hij besefte dat het voor klassieke computers onmogelijk lijkt om efficiënt quantumsystemen te simuleren, omdat het expliciet bijhouden van de  $2^k$  getallen (amplitudes) die nodig zijn om  $k$  quantumbits te beschrijven, veel te veel tijd en geheugenruimte zouden kosten. Hij concludeerde daaruit dat die quantumsystemen kennelijk een computationeel probleem oplossen dat buiten het bereik van klassieke computers ligt en dat een quantumcomputer dus krachtiger zou zijn dan

een klassieke. Verrassend genoeg blijkt het niet nodig alle amplitudes bij te houden wanneer je een quantumberekening klassiek wilt nadoen. Alles wat je kunt uitrekenen met  $k$  qubits kun je ook op een klassieke computer uitrekenen met niet veel meer dan  $k$  bits. Een quantumcomputer bespaart dus niet veel geheugenruimte, maar kan soms wel veel tijd besparen. De problemen waarbij dit het geval is (zoals factorisatie en simulatie) zijn overigens vrij zeldzaam; zo wordt er vermoed dat een quantumcomputer niet veel helpt voor zogenaamde ‘NP-complete’ pro-



Peter Shor.

blemen. Dit zijn problemen, zoals het handelsreizigersprobleem en het optimaliseren van computerchips, die behoren tot een grote klasse van praktisch-belangrijke optimalisatieproblemen die allemaal equivalent zijn, dat wil zeggen, als je er één snel zou kunnen oplossen dan kun je ze allemaal snel oplossen.

### Het breken van klassieke cryptografie

Sommige toepassingen van quantumcomputers liggen op het vlak van de cryptografie, waar methodes worden ontworpen (en soms gekraakt) om veilig te communiceren.

De efficiëntste cryptografie die we hebben heet public-key cryptografie. Dit is gebaseerd op het feit dat sommige berekeningen in de ene richting veel makkelijker zijn dan in de andere. Zo is het relatief eenvoudig om twee priemgetallen met elkaar te vermenigvuldigen, maar het kan moeilijk zijn (voor klassieke algoritmes!) om een gegeven getal weer te ontbinden in zijn priemfactoren. De veelgebruikte RSA-encryptie, genoemd naar haar uitvinders Rivest, Shamir en Adleman [3], is gebaseerd op dat idee. Stel dat Alice anderen (zoals Bob) in staat wil stellen om haar versleutelde berichten te sturen. Grof gezegd kan ze dan twee grote priemgetallen  $p$  en  $q$  als haar ‘privésleutel’ kiezen en hun product  $N = p \cdot q$  publiek maken. Er is een versleutelingsmethode die makkelijk te coderen is voor iemand die alleen de publieke sleutel heeft (Bob) en makkelijk te decoderen voor iemand die ook de privésleutel heeft (Alice). Voor

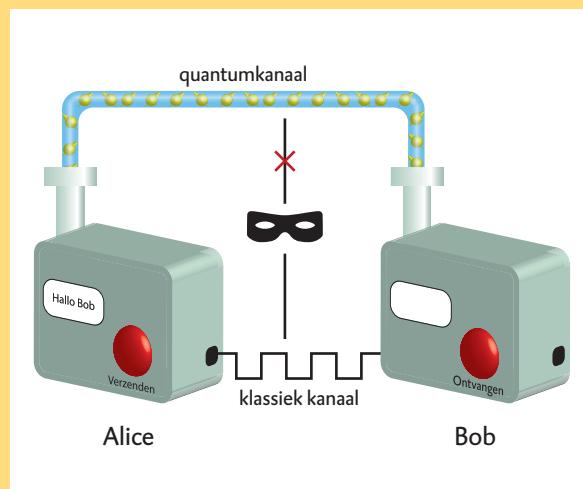
Ronald de Wolf studeerde informatica en filosofie aan de Erasmus Universiteit. In 2001 promoveerde hij in de theoretische informatica aan de Universiteit van Amsterdam, op een proefschrift over quantumcomputers. Na een jaar postdoc bij de University of California, Berkeley, werkt hij sinds 2002 bij het Centrum Wiskunde & Informatica (CWI) in Amsterdam. Sinds 2011 is hij ook deeltdhoogleraar aan de Universiteit van Amsterdam.

Ronald.de.Wolf@cwi.nl

## Het protocol van Bennett en Brassard

Als Alice een klassieke bit  $b$  naar Bob wil sturen (bijvoorbeeld een bit van de geheime sleutel), dan kan ze die bit op verschillende manieren als een qubit oversturen. Bijvoorbeeld gewoon als een  $|0\rangle$  of een  $|1\rangle$  (de ‘standaard basis’), maar ze kan 0 ook coderen als  $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ , en 1 als  $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$  (de ‘Hadamard basis’). Een spion die dit quantumkanaal aftapt weet niet welke basis Alice gebruikte en elke meting die hem informatie over  $b$  geeft, zal tegelijk de qubit verstören. Dat laatste kunnen Alice en Bob samen detecteren. Alice stuurt  $n$  bits op deze manier naar Bob, elke bit in zijn eigen random gekozen basis, en Bob meet elke qubit in zijn eigen random gekozen basis. Voor ongeveer de helft van de  $n$  qubits zullen Alice en Bob toevallig dezelfde basis gebruikt hebben en voor al die ‘goede posities’ zou de bit die Alice wilde sturen gelijk moeten zijn aan Bobs meetresultaat – tenzij er een spion op het kanaal zat. Vervolgens stuurt Alice naar Bob de informatie over de  $n$  bases die ze gebruikt heeft, zodat ze allebei weten wat de ‘goede posities’ zijn. Ze gebruiken nu de helft van de goede posities om afwijkingen te tellen. Als er hier meer afwijkingen zijn dan de natuurlijke ruis van het kanaal rechtvaardigt dan concluderen ze dat er een spion was en beginnen ze

opnieuw. Als er weinig afwijkingen waren, dan gebruiken ze de andere helft van de goede posities als een ruwe gedeelde sleutel. Omdat de spion weinig qubits verstoord heeft, heeft hij ook weinig informatie over die sleutel. Klassieke methodes kunnen dit vervolgens omzetten in een gedeelde sleutel waarover de spion nauwelijks informatie heeft.



zover we weten, kan een spion dit bericht alleen decoderen wanneer hij de priemfactoren  $p$  en  $q$  kan bepalen uit  $N$ . Dat kost hem eeuwen, zelfs met de beste algoritmes op een groot cluster van de sterkste klassieke computers. Maar wat als die spion nu een quantumcomputer heeft? We hebben gezien dat het algoritme van Shor een getal efficiënt kan ontbinden in zijn priemfactoren – maar dan kan het ook RSA-versleuteling breken! Ook de meeste andere vormen van public-key cryptografie blijken zo gebroken te kunnen worden. Dit zou de veiligheid van geldstromen tussen banken, internettransacties enzovoorts in gevaar brengen, juist nu een steeds groter deel van onze economie zich afspeelt via het internet. Niet alleen de maffia zou baat hebben bij een quantumcomputer, maar ook de veiligheidsdiensten: de Amerikanen zouden maar wat graag alle berichten van de Chinezen lezen en omgekeerd.

### Quantumcryptografie

Het breken van RSA en aanverwanten maakt de gangbare cryptografie onveilig. Wat kunnen we doen om geheime communicatie toch mogelijk te maken? Misschien zijn er vormen van public-key cryptografie die zelfs niet door quantumcomputers gebroken

kunnen worden? Hier zijn inderdaad kandidaten voor, maar ze zijn veel inefficiënter dan RSA en kunnen nog steeds gebroken worden door een spion met enorm veel rekenkracht.

Maar laten we ambitieuzer zijn: is er een vorm van cryptografie die bewijsbaar veilig is, zelfs tegen een spion met een quantumcomputer en heel veel rekentijd? Stel dat Alice en Bob allebei een kopie hadden van dezelfde geheime  $n$ -bit sleutel. Nu kan Bob een boodschap van  $n$  bits naar Alice sturen door haar de ‘som’ van zijn boodschap en van de sleutel te sturen. Alice kan het bericht decoderen met behulp van haar kopie van de sleutel, maar een meeluisterende spion zonder de sleutel krijgt geen enkele informatie over de werkelijke boodschap. Het probleem is natuurlijk hoe Alice en Bob zo’n gedeelde geheime sleutel in handen kunnen krijgen. Via communicatie over een publiek klassiek kanaal is dat onmogelijk, maar als ze kunnen communiceren over een quantumkanaal dan kan het wel! Dit quantum key distribution-protocol werd bedacht door Bennett en Brassard [4] in 1984 en is inmiddels al commercieel verkrijgbaar.

### Huidig onderzoek

Informatici richten zich vooral op

het vinden van nieuwe toepassingen van quantumcomputers, niet zoveer op het bouwen daarvan. Zo werkt de quantumcomputinggroep van Harry Buhrman op het CWI in Amsterdam (waar de auteur van dit artikel lid van is) aan het ontwikkelen van nieuwe quantumalgoritmes, bijvoorbeeld om efficiënt te testen of een gegeven functie afhangt van veel variabelen of niet, en aan nieuwe vormen van quantumcryptografie. Daarnaast hebben we de technieken die in quantumcomputing ontwikkeld zijn, kunnen gebruiken voor de oplossing van problemen in de klassieke informatica en wiskunde.

### Referenties

- Peter W. Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*, Proceedings of FOCS'94 (1994) 124–134. Ook in het vakblad SIAM Journal on Computing 26(5) (1997) 1484–1509.
- Lov K. Grover, *A Fast Quantum Mechanical Algorithm for Database Search*, Proceedings of ACM STOC'96, (1996) 212–219.
- Ronald L. Rivest, Adi Shamir en Leonard M. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM 21(2) (1978) 120–126.
- Charles H. Bennett en Gilles Brassard, *Quantum cryptography: Public key distribution and coin tossing*, In Proceedings of International Conference on Computers, Systems and Signal Processing, Bangalore, India (1984) 175–179.

# Veilig communiceren met quantummechanica

We gebruiken tegenwoordig vrijwel dagelijks het internet voor het uitwisselen van persoonlijke informatie, het uitvoeren van banktransacties en het bijhouden van medische gegevens. Het afluisteren van zulke communicatie geeft mogelijkheden tot diefstal en inbreuk op de privacy [1]. Met quantummechanica kan ongemerkt afluisteren fundamenteel onmogelijk worden gemaakt. Het vakgebied quantumcommunicatie onderzoekt hoe dit op grote schaal toepassing kan vinden.

Caspar van der Wal

## Cryptografie voor internetverkeer

Als we het internet gebruiken voor zaken die geheim moeten blijven voor buitenstaanders gebruiken we een vorm van cryptografie (ook wel encryptie genoemd). Het meest bekende voorbeeld is wellicht een webbrowser die een ‘https-protocol’ gebruikt in plaats van een gewoon ‘http-protocol’. Encryptie maakt communicatie onbegrijpelijk voor een afluisteraar door een mathematische operatie uit te voeren op de informatie (waar je over na kunt denken als een lange rij nullen en enen in digitale representatie) voor het wordt verzonden. De ontvangende partij weet dan hoe dit

kan worden terugveranderd in de originele rij nullen en enen.

Een simpel voorbeeld voor zulke encryptie gaat als volgt. Stel dat je de PIN-code van je bankpas wilt versturen aan een partij die je vertrouwt en dat je PIN-code 2360 is. Als jij en de ontvangende partij beiden eenzelfde willekeurig getal beschikbaar hebben waar niemand anders van weet (in dit voorbeeld 3567), dan kun je dit willekeurige getal bij je PIN-code optellen en de som (5927) communiceren. De ontvangende partij trekt hier gewoon 3567 van af en heeft dan de PIN-code. Informatietheoretici kunnen bewijzen dat het onmogelijk is om af te luisteren als dit getal echt willekeurig is en je het maar één keer gebruikt. Het willekeurige getal is dan de sleutel (*key*) voor deze cryptografie en alle veilige communicatieprotocollen zijn in essentie een manier om voor een zender en ontvanger een geschikte sleutel beschikbaar te maken. Dit is goed om in gedachten te houden als we hieronder een quantumversie van cryptografie bespreken: het enige wat nodig is, is dat een zender en een ontvanger op afstand van elkaar een zeer groot willekeurig getal produceren dat zij beiden kennen, terwijl niemand anders dat getal te weten kan komen.

Voor beveiligd internetverkeer ge-

bruiken onze webbrowsers nu vaak een vorm van encryptie die gebaseerd is op het RSA-algoritme voor public-key cryptografie (zie ook het artikel van Ronald de Wolf op pagina 183). De sleutel wordt hier gemaakt door in een slimme volgorde een paar getallen uit te wisselen. Dit zijn speciale getallen, die belangrijk zijn voor de wiskunde van het ontbinden van een getal in zijn priemfactoren.

De veiligheid van het algoritme is dan gebaseerd op het (sterke) wiskundige vermoeden dat  $9749 \times 7753$  (vermenigvuldigen van twee priemgetallen) een makkelijk probleem is en het vinden van deze twee priemgetallen als alleen het product gegeven is een moeilijk probleem (in dit geval 75583997 – probeer maar). In de praktijk gebruiken de algoritmen veel grotere getallen. Er is echter (nog) geen wiskundig bewijs dat het vinden van de twee priemfactoren van 75583997 daadwerkelijk veel moeilijker is dan het doen van de vermenigvuldiging  $9749 \times 7753$  en er is dus ook geen wiskundig bewijs dat de encryptiesystemen die we nu op het internet gebruiken veilig zijn. Sterker nog, er is wel geleidelijke (en voor encryptie zorgwekkende) vooruitgang onder wiskundigen die bestuderen hoe je zo efficiënt mogelijk een groot getal kan ontbinden in zijn priemfacto-

Caspar van der Wal (1971) studeerde aan de TU Delft en is daar ook gescreveerd op onderzoek aan supergeleidende quantumbits. Na een postdoc op Harvard op het gebied van quantumoptica met atoomdampen is hij sinds 2003 verbonden aan het Zernike Institute for Advanced Materials van de Rijksuniversiteit Groningen. Zijn team doet onderzoek aan quantumcoherentie in vaste-stofdevices.



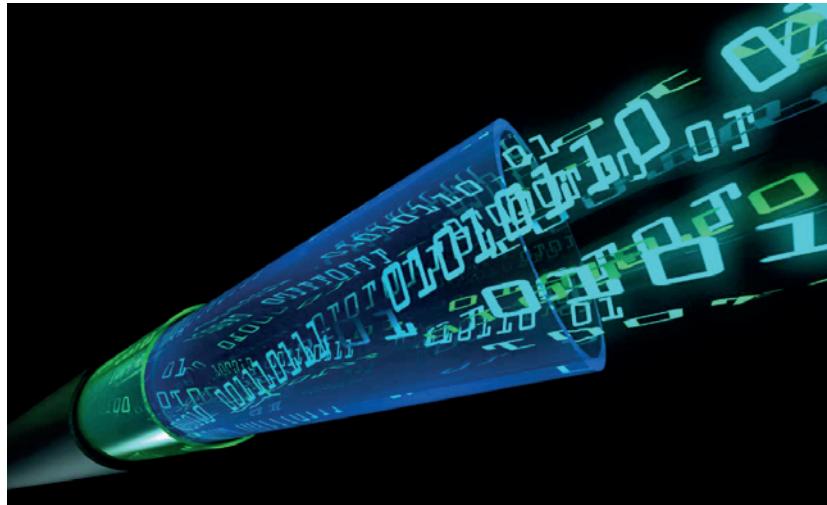
c.h.van.der.wal@rug.nl

ren (nog afgezien van het feit dat een grote quantumcomputer dit snel zou kunnen doen). Eén van de meest significante recente doorbraken was in 2006 (ook op leuke wijze gerapporteerd in het wetenschapskatern van NRC Handelsblad van 11 en 12 februari 2006). Een briljante wiskundige uit China vond toen een manier om veel gebruikte encryptiecodes te kraken in  $2^{39}$  rekenstappen (een dag rekenwerk voor een laptop) in plaats van de  $2^{64}$  rekenstappen die nodig waren voor de snelste methode die tot dan bekend was (ongeveer  $2^{25}$  dagen rekentijd als je het op een laptop wilt doen). Dit is voorlopig opgelost door simpelweg grotere priemgetallen te gebruiken voor encryptie, maar het laat zien dat er behoefte is aan een encryptieme-  
thode die veiliger is.

### Quantumcryptografie

Quantummechanica kan hier helpen [2]. Encryptie die gebruik maakt van quantumfysica kan fundamenteel veilig zijn. En terwijl de realisatie van de meeste toepassingsvoorstellingen in het vakgebied quantuminformatie nog in de laboratoriumfase zit (met experimentele groepen die misschien over tien jaar een doorbraak kunnen laten zien) werkt quantumcryptografie voor afstanden tot honderd kilometer al echt goed. De roadmap voor dit onderzoeksgebied in de Europese Unie [3] noemt ook duidelijk dat grootschalige toepassing van quantumcommunicatie een stuk dichterbij is dan quantumcomputing. Sinds het begin van deze eeuw zijn er al enkele (kleine) bedrijven die de apparatuur en diensten verkopen voor quantumcryptografie en het wordt op enkele plaatsen al toegepast voor communicatie tussen banken in financial districts. Eén van de meest bekende bedrijven in dit veld is het Zwitserse bedrijf ID Quantique. Zij hebben een interessante website over hun producten en de onderliggende natuurkunde [4].

Quantumcryptografie gebruikt enkele van de meest fundamentele aspecten van quantumfysica om afluisteren bij communicatie onmogelijk te maken. Bij deze zogenaamde quantumcommunicatie moeten de twee partijen (traditioneel Alice en Bob genoemd) quantumtoestanden naar elkaar kunnen sturen. Om dit minder abstract te maken is het goed alvast te noemen dat de fysica die hiervoor veruit het



Artistieke weergave van qubits door een glasvezelkabel.

meest geschikt is, bestaat uit optische pulsen die in glasfibers reizen. In mindere mate, maar even serieus, wordt onderzocht hoe het kan worden gerealiseerd met optische pulsen die door de lucht en de ruimte reizen voor quantumcommunicatie via satellieten [2].

Met glasfiber kun je quantumtoestanden versturen door optische pulsen te gebruiken die uit precies één foton bestaan. De quantumtoestand kan dan worden gedragen door de optische polarisatietoestand (quantum-superpositie)  $|\Psi\rangle = \alpha|H\rangle + \beta|V\rangle$  van dit foton, waarbij  $|H\rangle$  en  $|V\rangle$  de twee orthogonale lineaire polarisatietoestanden zijn, en  $\alpha$  en  $\beta$  de waarschijnlijkhedsamplitudes (dit systeem is direct geschikt voor het BB84-voorbeeld uit het artikel van Ronald de Wolf op pagina 183). Een alternatief is om optische pulsen te gebruiken waarbij de quantumtoestand wordt gedragen als een quantumsuperpositie van de toestanden  $|0_{\text{fot}}\rangle$  (geen puls) en  $|1_{\text{fot}}\rangle$  (een puls van één foton). Dat is dus een puls die tegelijkertijd uit 0 en 1 foton bestaat. In beide gevallen is er fundamentele veiligheid omdat het onmogelijk is om een onbekende quantumtoestand te meten zonder deze ook te verstören en voor pulsen met maar één enkel foton kun je maar één meetpoging doen. Hieruit is ook af te leiden dat het onmogelijk is om een kopie te maken van zo'n toestand terwijl het origineel behouden blijft (dit staat bekend als het no-cloning theorem).

Laten we communicatie met superposities van toestanden  $|0_{\text{fot}}\rangle$  en  $|1_{\text{fot}}\rangle$  verder als voorbeeld nemen. Hiervoor hebben Alice en Bob allebei een iden-

tieke quantum-twee-niveausysteem (denk aan een atoom) dat een enkel resonant foton in de toestand  $|1_{\text{fot}}\rangle$  uitzendt als het van de geëxciteerde toestand  $|e\rangle$  naar de grondtoestand  $|g\rangle$  gaat en vice versa voor absorptie van zo'n foton. Voor communicatie van een superpositietoestand begint Alice met haar systeem in  $|e\rangle$  en Bob met zijn systeem in  $|g\rangle$ . Alice moet nu haar systeem zo controleren dat de optische puls die eruit komt in gelijke mate de toestand  $|0_{\text{fot}}\rangle$  en  $|1_{\text{fot}}\rangle$  bevat (in praktijk is deze controle met lasers te realiseren door gebruik te maken van een derde niveau van het atoom). Het atoom van Alice blijft dan achter in een superpositie van  $|g\rangle$  en  $|e\rangle$ . Als deze puls door een fiber naar Bob vliegt en daar volledig wordt geabsorbeerd door het atoom, zal dit atoom daarna ook in een superpositie van  $|g\rangle$  en  $|e\rangle$  zijn. Er gelden nu quantumcorrelaties tussen de systemen van Alice en Bob – de twee systemen zijn dan verstrengeld en zitten in een gezamenlijke quantumtoestand in een vorm als  $(|e_A\rangle|g_B\rangle + |g_A\rangle|e_B\rangle)/\sqrt{2}$  (de indices geven hier Alice en Bob aan). Quantumverstrengeling is het fenomeen dat vooral bekend is van de Einstein-Podolsky-Rosenparadox (EPR). Als Alice nu meet of haar systeem in  $|g\rangle$  of  $|e\rangle$  zit, zal de uitkomst op willekeurige wijze een van de twee antwoorden zijn. Echter, als Bob daarna ook een meting doet zal hij vanwege de quantumcorrelaties met zekerheid het tegenovergestelde van Alice meten. Door dit vaak te herhalen kunnen Alice en Bob dus een lang willekeurig getal opbouwen.

Als een afluisteraar een meting doet aan zo'n optische puls zal dit de EPR-



Cryptografie is belangrijk voor een veilige overdracht van data.

correlaties tussen Alice en Bob verstoren. De afluisteraar kan proberen zijn acties onopgemerkt te houden door pulsen te meten en daarna snel pulsen door te sturen die overeenkomen met zijn meetuitkomst. Toch zal dat de correlaties verstoren, omdat meten aan een superpositietoestand geen volledig inzicht geeft in de toestand voor het meten. Alice en Bob kunnen dus merken dat er afgeluisterd wordt. Ze doen dit door na het versturen van veel toestanden op willekeurige plekken in de reeks een aantal bits aan te wijzen die ze gebruiken voor controle van de correlaties (dit kunnen ze openlijk per telefoon bespreken omdat ze deze bits niet voor de sleutel gaan gebruiken). Als dit aantal controlebits groot is (zeg een aantal  $N$ ) dan is de kans dat ze niet ontdekken dat de correlaties verstord zijn  $(1/2)^N$  en kan dus exponentieel klein worden gemaakt. Let wel, ze ontdekken dit dus terwijl ze een sleutel proberen te maken, dus voordat de echte boodschap zal worden verzonden. Het echte protocol is overigens één slag complexer dan de beschrijving hier: de veiligheid bewijzen vereist een zogenaamde Belltest van de correlaties. Dit staat bekend als het DLCZ-protocol (de afkorting verwijst naar de vier auteurs van het artikel) [2].

### Onderzoek

Quantumcryptografie is dus ideaal voor veilig communiceren. Welk onderzoek vindt nu plaats om dichter bij toepassing op grote schaal te komen? Voor het BB84-protocol zijn al systemen op de markt. Het plaatsen van zo'n systeem is echter nog om-

slachting omdat er een directe en zeer stabiele fiberconnectie nodig is zonder tussenversterkers. Door verliezen in de fiber beperkt dit in praktijk de toepassingsafstand ook tot zo'n honderd kilometer. Verder zijn de bronnen voor het maken van pulsen met precies één foton nog verre van ideaal (men gebruikt nu vaak zeer zwakke laserpulsen, er is dan altijd een kleine component met twee fotonen in de puls en de veiligheid is hierdoor niet optimaal). Een bron die gegarandeerd nooit meer dan een enkel foton afgeeft is een enkel los atoom in de geëxciteerde toestand. Echter, een los zwevend atoom laat zich moeilijk controleren en de straling die het afgeeft gaat alle kanten op en laat zich moeilijk efficiënt een fiber insturen. Onderzoek richt zich daarom op vaste-stofdevices, bijvoorbeeld optisch actieve quantumdots of defecten in kristallen. De eerste experimenten waren hier vaak op 4,2 K, maar er worden steeds meer systemen ontdekt die goed werken op kamertemperatuur [5]. Op soortgelijke wijze zijn de detectoren voor de pulsen nog verre van ideaal. De detectie-efficiëntie moet hoog zijn en het garanderen van de veiligheid gaat beter als de detector ook het verschil kan zien tussen een puls met één foton en met twee fotonen [2].

Het mooie van het DLCZ-protocol is dat het wél geschikt is voor afstanden groter dan honderd kilometer: de quantumcorrelaties van opeenvolgende segmenten van honderd kilometer kunnen worden doorgekoppeld. Het is hier echter wel nodig dat de quantumsystemen bij elk begin- en

eindpunt behoorlijk lang ongestoord in een quantumsuperpositietoestand kunnen blijven zitten (minstens  $L/c$ , waarbij  $L$  de communicatieafstand is en  $c$  de lichtsnelheid, dit is 10 ms voor  $L=3000$  km). Spintoestanden in vaste stof zijn hier het meest geschikt en recent zijn systemen ontdekt waarbij de quantumtoestanden van spins overtuigend langer leven dan 10 ms – zelfs bij kamertemperatuur [6]. Het team van Ronald Hanson in Delft heeft afgelopen jaar voor het eerst de quantumverstrengeling van spins in twee vaste-stofdevices op afstand aangetoond met defecten in diamant (zie ook NTvN, november 2013). Onderzoek in mijn eigen team richt zich erop dergelijke experimenten robuuster te maken, dat kan door met ensembles van defecten te werken in plaats van enkele defecten [7]. Dit vakgebied is dus volop in beweging om een nuttige toepassing van quantuminformatie op grote schaal beschikbaar te maken.

### Referenties

- 1 Seth Lloyd, *Privacy and the Quantum Internet*, *Scientific American* (2009) 80.
- 2 Zie bijvoorbeeld het recente overzichtsartikel van A. Ekert en R. Renner, *Nature* **507** (2014) 443.
- 3 <http://europe.eu/content/Roadmap> (Version 1.8, February 2013).
- 4 [www.idquantique.com](http://www.idquantique.com).
- 5 S. Castelletto, B. C. Johnson, V. Ivády, N. Stavrias, T. Umeda, A. Gali en T. Ohshima, *Nature Materials* **13** (2014) 151.
- 6 K. Saeedi, S. Simmons, J.Z. Salvail, P. Dluhy, H. Riemann, N.V. Abrosimov, P. Becker, H.-J. Pohl, J.J.L. Morton en M.L.W. Thewalt, *Science* **342** (2013) 830.
- 7 S. Onur en C. van der Wal, *NTvN* **78-07** (2012) 231.



# Quantummijnenveger

## De Mach-Zehnder-interferometer

De Mach-Zehnder-interferometer bestaat uit twee spiegels die 100% reflecteren en twee beamsplitters die 50% doorlaten en 50% reflecteren [1] (zie figuur 1). In deze opgave is steeds pad 1 even lang als pad 2. De faseverschuiving via pad 1 naar detector A volgt uit

$$\varphi_{1A} = \frac{2\pi t}{\lambda} + \pi + \pi + \frac{2\pi l_1}{\lambda},$$

met  $\lambda$  de golflengte,  $t$  de zogenaamde optische padlengte van de beamsplitter en  $l_1$  de doorlopen afstand. De beide reflecties onderweg leveren elk een fasesprong  $\pi$  op. Op deze manier kan voor elk mogelijk pad de faseverschuiving worden bepaald.

### 1

Laat zien dat als elke reflectie een fasesprong van  $\pi$  tot gevolg zou hebben, voor beide detectoren A en B constructieve interferentie op zou moeten treden. Leg uit waarom deze uitkomst niet mogelijk is.

De oplossing voor de paradox uit vraag 1 volgt als je je bedenkt dat er alleen een faseverschuiving van  $\pi$  optreedt als de golf op een laag reflecteert met een grotere brekingsindex. De beamsplitter is gemaakt van glas, met aan één kant een dun laagje met een lagere brekingsindex dan glas.

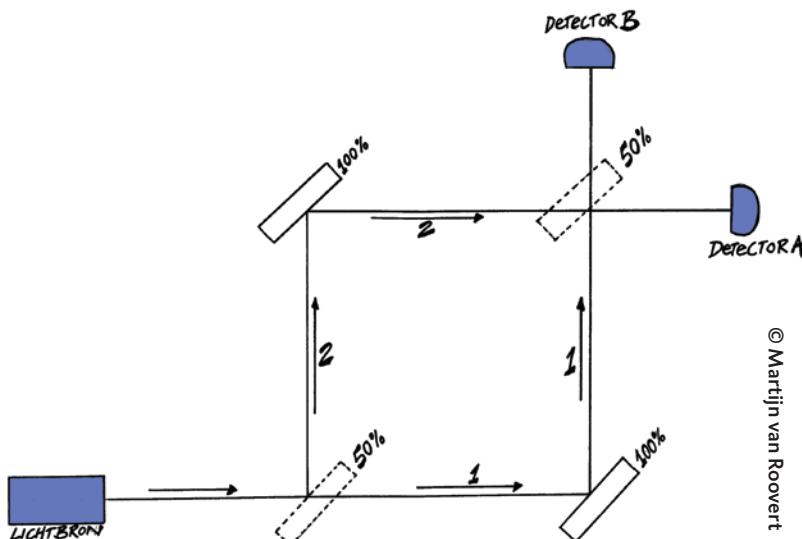
### 2

Laat zien dat het licht bij detector A nu wel constructief en bij B destructief interfereert.

## Quantummijnenveger

In het spelletje mijnenveger zoeken we mijnen door gesloten vakjes aan te klikken zonder dat ze ontploffen. Bij iedere poging krijgen we te zien hoeveel mijnen er grenzen aan het zojuist aangeklikte veld (zie figuur 2). Als deze aanwijzingen met getallen zouden ontbreken, zou elke detectie van een mijn onherroepelijk tot een ontploffing leiden. De vraag is of er toch een mogelijkheid bestaat een mijn te detecteren zonder dat hij ontploft. We doen hiervoor een gedachtenexperiment [2].

In een donkere afgesloten kamer bevindt zich een mijn. De mijn is zó ge-



Figuur 1 De Mach-Zehnder-interferometer.

voelig, dat er maar één enkel foton op hoeft te vallen om hem tot ontploffing te brengen. In de donkere kamer bevindt zich ook een Mach-Zehnder-interferometer. Verder is de kamer leeg. Als je op een knopje (dat zich buiten de kamer bevindt) drukt, verstuurdt de lichtbron slechts één enkel foton. Je drukt op het knopje. Het foton valt gelukkig niet op de mijn, maar wordt in detector A gedetecteerd.

### 3

Wat weet je nu over de positie van de mijn?

Je verplaatst de interferometer in zijn geheel en je drukt moedig nog een keer op het knopje. Het foton wordt nu in detector B gedetecteerd.

### 4

Wat weet je nu over de positie van de mijn?

### 5

Hoe groot is de kans dat de mijn ontploft als je nu nog een keer op het knopje drukt?

### 6

Kan je de uitkomsten

van het experiment nog op een klassieke manier verklaren?

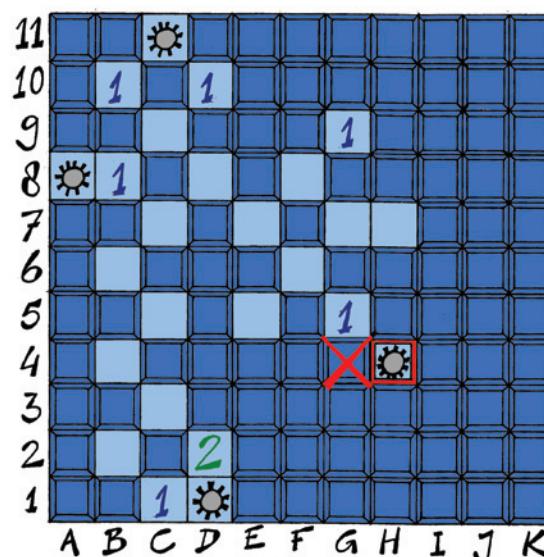
Lodewijk Arntzen

189

De antwoorden zijn te vinden op pagina 235 bij de agenda.

## Referenties

- 1 K.P. Zetie, S.F. Adams en R.M. Tocknell, How does a Mach-Zehnder interferometer work?, *Physics Education* **35**(1) (2000) 46-48.
- 2 A.C. Elitzur en L. Vaidman, Quantum Mechanical Interaction-Free Measurement, *Foundations of Physics* **23**(7), (1993) 987-997.



Figuur 2 Het klassieke spelletje Mijnenveger.



# Quantumverstengeling

A. Einstein, B. Podolsky, N. Rosen, Can quantum-mechanical description of physical reality be considered complete? *Physical Review* 47 (15 May 1935) 777 - 780.

J.S. Bell, On the Einstein Podolsky Rosen Paradox. *Physics* 1 (1964) 195 - 200. Herdrukt in J.S.Bell, *Speakable and Unspeakable in Quantum Mechanics*. Cambridge University Press 2004.

## EPR-paradox

Wat de klassieke fysica van de quantummechanica onderscheidt zijn determinisme, lokaliteit en realisme. Het determinisme zegt dat wanneer op een bepaald tijdstip de fysische toestand van een object compleet is bepaald, de toestand in verleden en toekomst daaruit ook compleet valt af te leiden. Lokaliteit wil zeggen dat de wisselwerking tussen twee objecten

afneemt met de onderlinge afstand en niet sneller kan plaatsvinden dan met de lichtsnelheid. Realisme houdt in dat het bestaan van een object los staat van de waarneming ervan. Aangezien de quantummechanica geen van die eigenschappen bezit, beschouwde Einstein de quantummechanica als een incomplete theorie. In 1935 ontwikkelde hij, tezamen met zijn medewerkers uit Princeton, Boris

Podolsky en Nathan Rosen, een beroemd geworden Gedankenexperiment, dat naar de initialen van de auteurs bekend staat als de EPR-paradox. In principe laat de paradox zich als volgt beschrijven. Een systeem in de singlettoestand dat aanvankelijk in rust is, vervalt in twee bewegende identieke deeltjes. Aangezien de totale spin van het systeem nul is, hebben de deeltjes tegengestelde spin en tegengestelde bewegingsrichtingen. Het deeltjespaar wordt beschreven door één enkele twee-deeltjesgolffunctie. Wanneer via meting blijkt dat deeltje 1 spin up heeft, dan moet deeltje 2 spin down hebben (en omgekeerd), ongeacht de afstand die hen scheidt, omdat de eindtoestand van het twee-deeltjessysteem dezelfde moet zijn als de beginstoestand, namelijk die van het enklevoudige neutrale systeem. Aldus is zonder enige verstoring (meting) de spin van deeltje 2 precies bekend, zonder dat een lokale fysische koppling met deeltje 1 bestaat.

Voor de ontstane situatie kunnen twee verklaringen gelden:

1. Deeltje 2 merkt instantaan wat de spin van deeltje 1 is en past zijn spin daaraan aan. Zo'n spookachtige werking op afstand (spukhafte Fernwirkung) achtte Einstein niet mogelijk want in strijd met de speciale relativiteitstheorie die bepaalt dat informatie niet sneller kan worden overgebracht dan de lichtsnelheid in vacuüm.
2. Het paradoxale resultaat zou met de huidige quantummechanica wellicht beschreven kunnen worden door middel van nog onbekende, verborgen parameters of variabelen (hidden variables), bijvoorbeeld via in het systeem verborgen instructies. Zulke parame-

DESCRIPTION OF PHYSICAL REALITY

777

of lanthanum is  $7/2$ , hence the nuclear magnetic moment as determined by this analysis is  $2.5$  nuclear magnetons. This is in fair agreement with the value  $2.8$  nuclear magnetons determined from La III hyperfine structures by the writer and N. S. Grace.<sup>9</sup>

<sup>9</sup> M. F. Crawford and N. S. Grace, *Phys. Rev.* 47, 536 (1935).

This investigation was carried out under the supervision of Professor G. Breit, and I wish to thank him for the invaluable advice and assistance so freely given. I also take this opportunity to acknowledge the award of a Fellowship by the Royal Society of Canada, and to thank the University of Wisconsin and the Department of Physics for the privilege of working here.

MAY 15, 1935

PHYSICAL REVIEW

VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, Institute for Advanced Study, Princeton, New Jersey  
(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

Whatever the meaning assigned to the term *complete*, the following requirement for a complete theory seems to be a necessary one: *every element of the physical reality must have a counterpart in the physical theory*. We shall call this the condition of completeness. The second question is thus easily answered, as soon as we are able to decide what are the elements of the physical reality.

The elements of the physical reality cannot be determined by *a priori* philosophical considerations, but must be found by an appeal to results of experiments and measurements. A comprehensive definition of reality is, however, unnecessary for our purpose. We shall be satisfied with the following criterion, which we regard as reasonable. *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.* It seems to us that this criterion, while far from exhausting all possible ways of recognizing a physical reality, at least provides us with one

ters moeten lokaal van aard zijn, omdat instantane werkingen op afstand niet mogelijk zijn. Maar in zijn huidige vorm, waarbij die verborgen variabelen niet bekend zijn, is de quantummechanica dus niet compleet.

In Kopenhagen sloeg EPR in als een donderslag bij heldere hemel. Iedere medewerker van het Bohr-instituut moest zijn werk laten vallen om een antwoord op EPR te formuleren. Het antwoord van Bohr kwam op 15 oktober van hetzelfde jaar, onder dezelfde titel als die van EPR, in hetzelfde tijdschrift [1] en was geheel gebaseerd op de Kopenhagense interpretatie.

Zijn antwoord was sterk filosofisch gekleurd, bevatte slechts een enkele formule en concentreerde zich op een meettechnische onmogelijkheid. Volgens Bohr kunnen uitspraken over een quantumverschijnsel pas worden gedaan op grond van een meting. Een quantumstelsel en de (klassieke) meetapparatuur vormen één geheel. Men kan niet in abstracto een uitspraak over een quantumstelsel doen. Ook al is de toestand van deeltje 1 bekend, over die van deeltje 2 weet men pas iets als dat ook is gemeten. De conclusie van Einstein over deeltje 2 is dus fysisch zonder zin. Het essentiële probleem van de niet-lokaliteit ontging Bohr geheel, althans werd nergens door hem genoemd. "Solipsistisch" noemde Einstein het verweer van Bohr – dat is bij voorbaat ongevoelig voor ieder tegenargument. Waarschijnlijk voelde ook Bohr de onbevredigdheid van zijn argument, want tot zijn dood (1962) bleef hij zich met de EPR-paradox bezighouden.

### Quantumverstrekking

De eigenschap dat een systeem van twee deeltjes die via een eerder contact



John Stewart Bell in 1988.

gecorreleerd zijn, die correlatie na separatie nog steeds behouden, ongeacht de grootte van de afstand, noemde Erwin Schrödinger *Verschränkung* (Nederlands: verstrekking, Engels: entanglement en Frans: intrication). Verstrekking is een specifiek quantumverschijnsel, waarbij de quantumtoestand van twee objecten, die tevoren deel uitmaakten van één quantumstelsel, niet onafhankelijk van elkaar beschreven kunnen worden maar nog steeds als één quantumtoestand moeten worden beschouwd. Quantumverstrekking is een product van quantumsuperpositie. Bij een tweetal verstrekkelijke objecten is de toestand van ieder van de objecten ongedefinieerd in termen van de fysische eigenschappen zoals plaats, impuls, spin, polarisatie enzovoorts. Maar zodra een meting bij de één wordt verricht (bijvoorbeeld spin up) zal de andere zich instantaan in de canoniek geconjugeerde toestand (spin down) bevinden, ongeacht de afstand die ze scheidt. Tussen verstrekkelijke deeltjes bestaat een perfecte correlatie, dat is dat de waarde van de ene grootheid die van de andere met 100% nauw-

keurigheid voorspelt. Dit is klassiek niet te verklaren. Volgens Schrödinger is verstrekking "the most characteristic trait of quantum mechanics".

### Verborgen variabelen

Aan het slot van hun artikel concludeerden Einstein, Podolsky en Rosen: "While we have thus shown that the wave function does not provide a complete description of the physical reality, we left open the question of whether or not such a description exists. We believe, however, that such a theory is possible". Einstein meende dat de incomplete quantummechanica met behulp van verborgen parameters of variabelen viel te repareren en tot een complete, dat is loka-

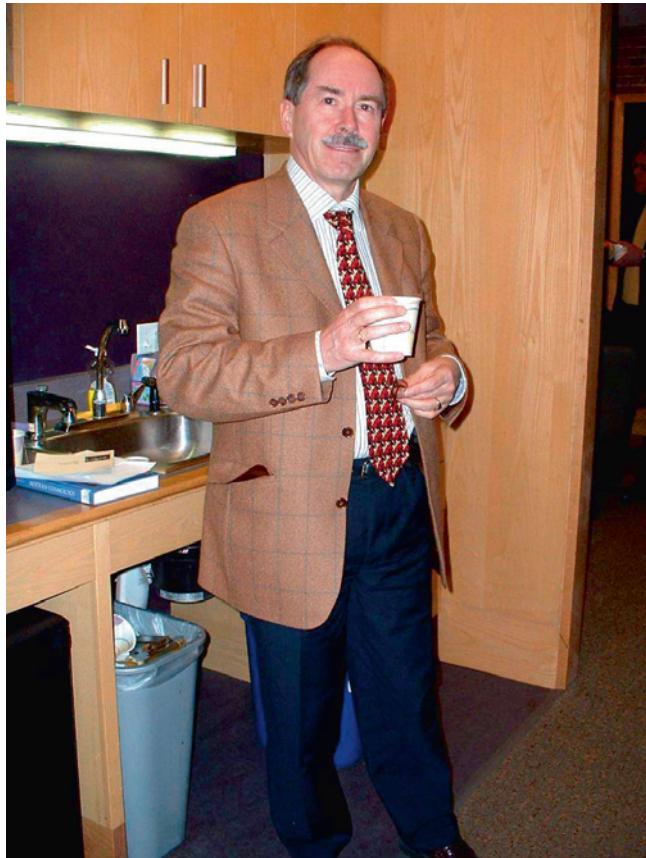
le deterministische theorie viel te maken. In 1964 ontwierp John Bell een criterium, waarmee deterministische lokale theorieën van niet-lokal theorieën konden worden onderscheiden, de zogeheten Bellongelijkheid.

### Theorema van Bell

John Stewart Bell (1928 - 1990) werd in Noord-Ierland geboren in een gezin van arme ouders, die zich echter het brood uit de mond spaarden om hem als enige en eerste van de familie naar de middelbare school te kunnen laten gaan. Via een beurs studeerde hij aan de Queen's University te Belfast waarna hij in 1956 aan de universiteit van Birmingham bij Rudolph Peierls in de theoretische fysica promoveerde. Vervolgens werkte hij aan de Atomic Energy Research Establishment te Harwell, waar hij zijn vrouw, de fysica Mary Ross ontmoette en trouwde. Enkele jaren later vertrok hij naar CERN (Genève) waar hij samenwerkte met zijn vriend en collega Martin Veltman. Bells werk lag op het gebied van de elementaire-deeltjesfysica en de versneller technologie, maar de grondslagen van de quantummechanica

beoefende hij, naar hij zei “als hobby”. In 1963 vertrokken Bell en Veltman voor een sabbatical van een jaar naar het Stanford Linear Accelerator Center (SLAC), waar Veltman zijn computerprogramma Schoonschip ontwikkelde en Bell zijn beroemd geworden Bell Inequalities ontwierp (zie het artikel van Ad Verbruggen hier-naast). Daarmee bewees Bell dat “No conceivable local reality can underlie the local quantum facts”. Dit is het befaamde theorema van Bell.

De quantumfeiten zijn altijd lokaal, maar de quantumtheorie blijkt niet-lokaal te zijn. Hoe staat het met de quantumrealiteit? Aangezien de quantumfeiten lokaal zijn, ligt het voor de hand de quantumrealiteit eveneens als lokaal te beschouwen en de niet-lokale quantumtheorie te verklaren als een heuristische afbeelding ervan, in de trant van *the map is not the territory*. Volgens de fysici uit die tijd – Bohr inclusis – zou het absurd zijn te veronderstellen dat de natuur een niet-lokale realiteit bezat, die echter uitsluitend lokale feiten opleverde. Ieder experimenteel resultaat zou derhalve verklaard moeten kunnen worden op grond van een lokale realiteit. Dit was het standpunt van Einstein, Podolsky en Rosen en van de ontwerpers van de verborgen-variabelentheorie. Met zijn theorema toonde Bell aan dat de (quantum) realiteit niet lokaal is. Ofschoon alle quantumfeiten lokaal zijn, kunnen ze niet worden gesimuleerd of verklaard vanuit een lokale theorie. Alle pogingen om via verborgen variabelen de quantummechanica tot een deterministische lokale theorie te maken, zijn door Bell als niet zinvol aangewezen. De belangrijke filosofische vraag of de realiteit als lokaal of niet-lokaal moet worden beschouwd, is daarmee fysisch opgelost. De fysicus en filosoof Abner Shimony sprak daarom van “experimentele metafysica”. Bovendien berust het bewijs voor Bells ongelijkheid niet op de details van de quantumtheorie, maar is uitslui-



Gerard 't Hooft.

tend gebaseerd op logische principes en enkele eenvoudige experimentele feiten. De fysische realiteit is niet-lokaal, ongeacht de gebruikte theorie om de feiten te verklaren. Pas in 1982 kon Alain Aspect (Orsay) het experimentele bewijs voor de Bellongelijkheid leveren. Een jaar voor zijn dood (op 1 oktober 1990 door een hersenbloeding) werd John Bell genoemd voor de Nobelprijs.

### Is complete (quantum) fysica mogelijk?

Evenals Einstein zijn er steeds fysici geweest, zoals in het verleden Louis de Broglie en David Bohm, die de compleetheid van de orthodoxe quantummechanica in twijfel trokken en het indeterminisme en de niet-lokaliteit ervan via verborgen variabelen trachten te repareren. Wat John Bell echter aantoonde was dat een mogelijke complete verborgen variabele theorie *per se* niet-lokaal moet zijn. Een modern fysicus die evenals Einstein intuïtief overtuigd blijft van de deterministische en lokale aard van de (quantum)fysica is Gerard 't Hooft. Tegenover een Duitse wetenschapsjournalist verklaarde hij: “Wir werden die lokale Natur der Gesetze der Physik nur verstehen können, wenn wir über die

Quantenphysik hinausgehen. Ich komme mehr und mehr zur Auffassung, dass die wesentlichen, lokalen Informationsträger vollständig deterministisch sind, nicht quantenphysikalisch. Aber es ist gut denkbar, dass ihre exakte Natur noch für eine lange Zeit verborgen bleibt.” Volgens 't Hooft is de quantummechanica formeel juist, maar men moet deterministische modellen vinden om achter de lokale en logische natuur van de fysische wetten te kunnen komen. In 2009 heeft hij een artikel gepubliceerd (*Entangled quantum states in a local deterministic theory*) waarin hij de Bellongelijkheid binnen een kader van een deterministisch systeem met verborgen parameters heeft ontwikkeld. “Die Beziehung zwischen Determinismus und unserem quan-

tenphysikalischen Weltbild könnte eine sehr subtile sein”, aldus 't Hooft. “Ich sehe es als meine Aufgabe herauszufinden wie eine solche Beziehung formuliert werden kann. Ich glaube fest daran, dass man die üblichen Argumente dafür, dass solche Beziehungen unmöglich sind, umgehen kann. Die Natur ist klüger als wir – bis jetzt.”

Herman de Lang

### Referentie

1 Physical Review 48 (1935) 696 - 702.



# Voor wie de klok heeft horen luiden...

## Vijftig jaar Bells ongelijkheid

J.S. Bell, On the Einstein Podolsky Rosen Paradox, Physics 1 (1964) 195, ook gepubliceerd in: J.S. Bell, Speakeable and Unspeakable in Quantum Mechanics, Cambridge University Press, Cambridge, UK (2004)

**H**et is dit jaar precies een halve eeuw geleden dat John Bell een immiddels klassiek geworden artikel publiceerde. De titel *On the Einstein Podolsky Rosen paradox* (EPR) geeft aan dat het gaat over de vraagtekens die Einstein in 1935 zette bij de interpretatie van de quantummechanica van Bohr en consorten. Einstein beargumenteerde dat de quantummechanica een niet-complete theorie is en dat de onbepaaldheid van meetuitkomsten moet worden toegeschreven aan aanvullende, verborgen variabelen. In zijn artikel gaat Bell met name in op de betekenis van de niet-lokale wisselwerking die in het EPR-gedachte-experiment naar voren was gekomen.

De vraag die Bell aan de orde stelde is: als we aannemen dat er inderdaad een diepere laag is met verborgen variabelen en we sluiten niet-lokale wisselwerkingen bij voorbaat uit, kunnen we dan toch een goede beschrijving

van het EPR-gedachte-experiment geven? Goed, in de zin dat de resultaten overeenkomen met die van de quantummechanica.

De grote verdienste van Bell is dat hij een manier heeft gevonden om een antwoord op deze vraag te geven en daarbij een weg opende om echte experimenten een rol te laten spelen. De manier waarop hij dat gedaan heeft, is heel bijzonder in de zin dat de afleiding wiskundig niet moeilijk of langdradig is. Het gaat direct om fundamentele natuurkundige vragen. Het is zelfs zo direct dat we, in dit artikel, tot in detail, de kern van Bells werk gaan bespreken. Het is vooral bedoeld voor lezers die van Bells werk hebben gehoord, maar nooit aan de bestudering van het oorspronkelijke artikel zijn toegekomen. We halen hier het oorspronkelijk werk van Bell naar voren en laten een bespreking van latere discussies en ontwikkelingen over aan anderen. Bijvoorbeeld aan Herman de

Lang die dit onderwerp in een bredere context aan bod laat komen in het artikel hiervoor.

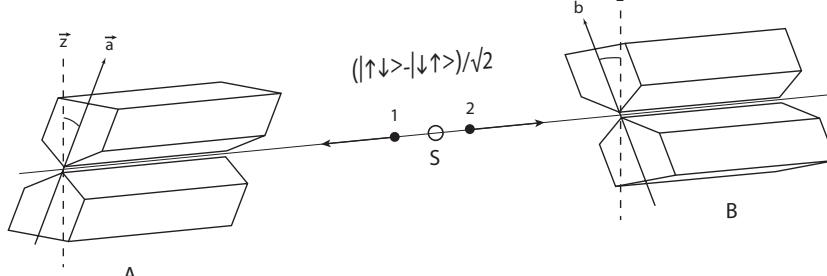
Bell haakt in op de variant die Bohm [1] ontwikkelde van het gedachte-experiment van Einstein, Podolsky en Rosen (EPRB, waarbij de B staat voor Bohm) en start met een beknopte beschrijving hiervan. Om duidelijk te maken wat we bedoelen met niet-lokaliteit, doen wij dat ook. Het vergt enige kennis van spin in de quantummechanica. Het EPRB-gedachte-experiment is weergegeven in figuur 1.

Een bron S zendt twee deeltjes met spin  $1/2$  uit in tegengestelde richting. De totale spin van het deeltjespaar is nul. De spintoestand van het paar is ook de singlettoestand:

$$\Psi_s = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) \quad (1)$$

Dit is een superpositie van de tweedeeltjestoestanden  $|\uparrow\downarrow\rangle$  en  $|\downarrow\uparrow\rangle$ . Met  $|\uparrow\downarrow\rangle$  wordt aangegeven dat één ruimtelijke component van de spin (wij nemen de  $z$ -component) van het ene deeltje  $+h/2$  ( $\uparrow$ ) is en dezelfde spincomponent van het andere deeltje  $-h/2$  ( $\downarrow$ ) ( $h$  is de gereduceerde Planck-constante). Voor  $|\downarrow\uparrow\rangle$  zijn de waarden omgekeerd.  $\Psi_s$  is een voorbeeld van een verstrengelde toestand.

Als de deeltjes uit elkaar bewegen, verandert de totale spin van het paar niet. Als de deeltjes zover uit elkaar zijn dat ze geen invloed meer op elkaar kunnen uitoefenen, meten we een component van de spin van bijvoorbeeld het deeltje dat in figuur 1 naar links



**Figuur 1** Schematische voorstelling van het EPRB-gedachte-experiment. Bron S zendt twee deeltjes in de singletspintoestand uit. Stern-Gerlach-apparaat A meet de  $\vec{a}$ -component van de spin van deeltje 1, apparaat B meet de  $\vec{b}$ -component van de spin van deeltje 2.

beweegt. We doen dit met een Stern-Gerlach-apparaat. Het magneetveld in het Stern-Gerlach-apparaat richten we zo uit dat we de  $z$ -component van de spin meten. De uitkomst van de meting is  $\hbar/2$  of  $-\hbar/2$ . De kans op een bepaalde uitkomst is 50%. Dit komt omdat de deeltjes in de toestand (1) zijn.

Het bijzondere is nu dat we na de meting van één deeltje direct weten wat de  $z$ -component van de spin van het andere deeltje is. De totale spin van het paar is immers nul. Dus de  $z$ -component van de spin van het deeltje dat naar rechts beweegt, is in dit voorbeeld  $-\hbar/2$  of  $\hbar/2$ . Er is sprake van 100% anticorrelatie. Dit kunnen we verifiëren door met het rechter Stern-Gerlach-apparaat de  $z$ -component van de spin van het rechter deeltje te meten.

Stel we draaien het magneetveld van het linker Stern-Gerlach-apparaat van de  $z$ - naar de  $\vec{a}$ -richting (zie figuur 1) en voeren een meting uit. De meetuitkomsten zijn dan nog altijd  $\hbar/2$  of  $-\hbar/2$ , maar de kans op één van die uitkomsten is nu niet meer 50%. Het is nu de  $\vec{a}$ -component van de spin die een waarde heeft gekregen. Bij de meting reduceert toestand (1) naar  $|\uparrow\downarrow\rangle$  of  $|\downarrow\uparrow\rangle$  waarbij de pijltjes nu de spincomponent in de  $\vec{a}$ -richting aanduiden. Het is dan ook de  $\vec{a}$ -component van de spin van het andere deeltje die een tegengestelde waarde krijgt ( $-\hbar/2$  of  $\hbar/2$ ). De kansen op  $\hbar/2$  of  $-\hbar/2$  zijn precies omgekeerd aan die van het linker deeltje.

We hadden al aangenomen dat de deeltjes zo ver uit elkaar zijn dat er geen sprake kan zijn van beïnvloeding op een manier die we kennen. Dit impliceert dat het rechtsgaande deeltje ook niet beïnvloed kan worden door het linker Stern-Gerlach-apparaat. Toch hadden we vastgesteld dat zodra de  $z$ -of  $\vec{a}$ -component van de spin van het linker deeltje is gemeten, wij ook die waarde van het rechter deeltje weten. Dit wekt heel sterk de suggestie dat er een soort instantane, niet-lokaal wisselwerking moet bestaan.

De kans is groot dat iemand dit moeilijk te accepteren vindt in een wereld waarin aan causaliteit en een eindige lichtsnelheid niet getwijfeld wordt. Diegene is dan in goed gezelschap, want het is de essentie van de EPR-paradox.

Einstein en consorten zagen dit pro-

bleem als een aanwijzing dat de quantummechanica geen complete theorie is. Er zouden additionele, verborgen variabelen in het spel kunnen zijn die ook verantwoordelijk zijn voor de onbepaaldheid in de quantummechanica.

Het was Bell die besloot het idee van verborgen variabelen te implementeren in het EPRB-gedachte-experiment. Als je het idee van verborgen variabelen accepteert dan is de consequentie dat je zegt dat een meetuitkomst van het EPRB-gedachte-experiment bepaald wordt door de richting  $\vec{a}$  (of  $\vec{b}$ ) van het Stern-Gerlach-apparaat en de verborgen variabele  $\lambda$ . Voor het gemak doen we net alsof er maar één verborgen variabele is. Het verhaal wordt niet anders als  $\lambda$  een verzameling of zelfs een verzameling functies voorstelt (discreet of continu). De verborgen variabelen kan men opvatten als dynamische variabelen die aan bepaalde bewegingsvergelijkingen voldoen met geschikt gekozen beginwaarden.

De meetuitkomst van het linker Stern-Gerlach-apparaat noemen we  $A \equiv A(\vec{a}, \lambda)$  en die van het rechter Stern-Gerlach-apparaat  $B \equiv B(\vec{b}, \lambda)$ . De meetuitkomsten kunnen maar twee waarden aannemen

$$A(\vec{a}, \lambda) = \pm 1 \text{ en } B(\vec{b}, \lambda) = \pm 1 \quad (2)$$

( $\pm 1$  is een afkorting voor  $\hbar/2$ ). Door de afhankelijkheden in (2) zo te kiezen is niet-lokaal gedrag uitgesloten. Het cruciale punt is dat Bell heeft gevonden dat de verwachtingswaarde van het product van de meetuitkomsten een grootheid is waarin het toevoegen van verborgen variabelen en het uitsluiten van niet-lokale invloeden tot verschillen met de oorspronkelijke quantummechanica kunnen leiden. Omdat  $\lambda$  de feitelijke uitkomst van een meting bepaalt, wordt de verwachtingswaarde beschreven door

$$E(\vec{a}, \vec{b}) = \int d\lambda \rho(\lambda) A(\vec{a}, \lambda) B(\vec{b}, \lambda) \quad (3)$$

met  $\rho(\lambda)$  de waarschijnlijkheidsverdeling van  $\lambda$  ( $\int d\lambda \rho(\lambda) = 1$ ). In het EPRB-gedachte-experiment is er sprake van perfecte anticorrelatie als beide Stern-Gerlach-apparaten precies de-

zelfde spincomponent meten, dus als  $\vec{a} = \vec{b}$ . Dit betekent  $E(\vec{a}, \vec{a}) = -1$  en voor alle  $\vec{a}$  en  $\lambda$  moet dan gelden

$$A(\vec{a}, \lambda) = -B(\vec{a}, \lambda) \quad (4)$$

Als we gebruikmaken van deze gelijkheid en van het feit  $A(\vec{b}, \lambda)A(\vec{b}, \lambda) = 1$  en bedenken dat  $|\int f(x)dx| \leq \int |f(x)|dx$ , dan is het een kwestie van invullen om te bewijzen dat als  $\vec{c}$  een andere richting van het rechter Stern-Gerlach-apparaat is, dat

$$|E(\vec{a}, \vec{b}) - E(\vec{a}, \vec{c})| \leq 1 + E(\vec{b}, \vec{c}) \quad (5)$$

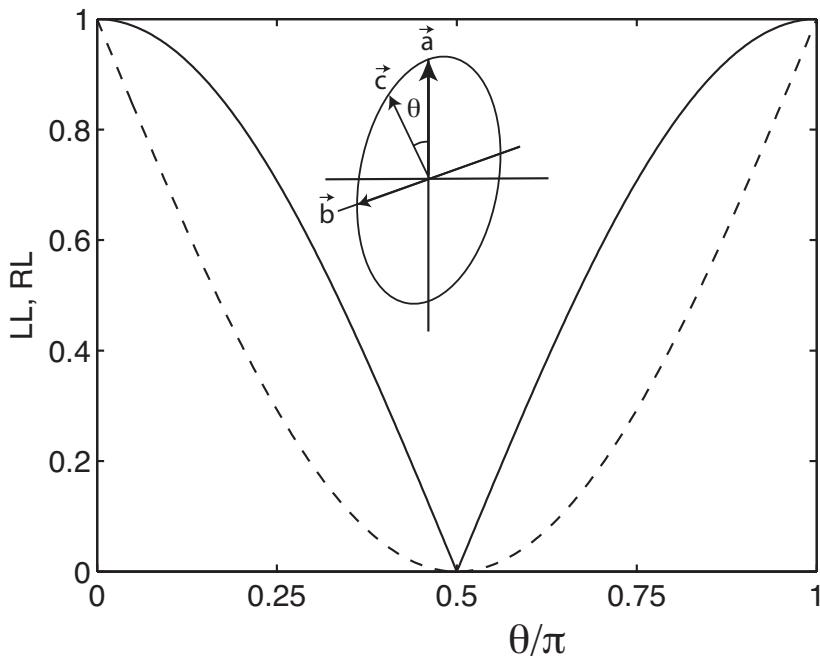
Dit is de oorspronkelijke vorm van Bells ongelijkheid. Op zich is deze uitdrukking niet iets bijzonders. In het dagelijks leven komen dergelijke uitdrukkingen vaak voor als het gaat om verdelingen van objecten met bepaalde wel/niet eigenschappen. Maar dit terzijde.

De vraag is of de ongelijkheid nu ook geldt voor de uitkomsten van de spinmetingen die op heel speciale manier met elkaar zijn gekoppeld.

Het is een opgave in veel leerboeken om met de quantummechanica een uitdrukking voor  $E(\vec{a}, \vec{b})$  af te leiden (zie bijvoorbeeld Griffiths [2]). Het resultaat is te zien in vergelijking (6) in het kader hieronder. Het gedeelte tussen de gelijktrekens is de quantummechanische verwachtingswaarde van de operator  $\sigma_a^{(1)} \sigma_b^{(2)}$  in de singlettoestand (1).  $\sigma_a^{(1)}$  en  $\sigma_b^{(2)}$  zijn de operatoren behorend bij de spincomponenten in de  $\vec{a}$ - en  $\vec{b}$ -richting van respectievelijk deeltje 1 en deeltje 2.  $\theta_{ab}$  is de hoek tussen  $\vec{a}$  en  $\vec{b}$ . We berekenen met (6) voor drie richtingen  $\vec{a}$ ,  $\vec{b}$  en  $\vec{c}$  van de Stern-Gerlach-apparaten de verwachtingswaarden  $E(\vec{a}, \vec{b})$ ,  $E(\vec{a}, \vec{c})$  en  $E(\vec{b}, \vec{c})$  en vullen de resultaten in (5) in.

Er gebeurt dan iets bijzonders. Voor willekeurige richtingen  $\vec{a}$ ,  $\vec{b}$  en  $\vec{c}$ , maar met  $\vec{b}$  en  $\vec{c}$  ongeveer in dezelfde richting, verandert het linker lid van (5) lineair met de hoek tussen  $\vec{b}$  en  $\vec{c}$ . Bovendien gaat het linker lid op discontinue wijze door nul bij  $\vec{b} = \vec{c}$ . Het rechter lid doorloopt dan kwadratisch een extreme waarde van  $1 - \cos(\theta_{bc})$ . Dat betekent dat het linker lid van (5) in dat gebied groter is dan het rechter

$$E_{QM}^{singlet}(\vec{a}, \vec{b}) = \frac{1}{2} (\langle \uparrow\downarrow | - \langle \downarrow\uparrow |) \sigma_a^{(1)} \sigma_b^{(2)} (\langle \uparrow\downarrow | - \langle \downarrow\uparrow |) = -\cos(\theta_{ab}) \quad (6)$$



**Figuur 2** Schending van Bells ongelijkheid. Het linker lid (LL, doorgetrokken lijn) en het rechter lid (RL, streeppjeslijn) van ongelijkheid (5) zijn uitgezet tegen de hoek tussen de richtingen  $\vec{a}$  en  $\vec{c}$  (zie inzet). In tegenstelling tot (5) is het rechter lid nooit groter dan het linker lid.

lid. Dat is in strijd met wat (5) aangeeft. Om dit punt iets duidelijker naar voren te brengen, kiezen we de richtingen  $\vec{a}$  en  $\vec{b}$  vast en variëren we  $\vec{c}$  zoals dat in de inzet van figuur 2 is aangegeven. Figuur 2 toont het linker lid van (5) (doorgetrokken lijn) en het rechterlid (streeppjeslijn). Het discontinue gedrag van het linkerlid bij  $\vec{b} = \vec{c}$  is duidelijk zichtbaar en we zien dat op drie punten na het linker lid groter is dan het rechter lid. We spreken van de schending van Bells ongelijkheid.

Dit betekent dat het toevoegen van verborgen variabelen en het uitsluiten van niet-locale wisselwerking tot resultaten leiden die niet in overstemming zijn met wat de quantummechanica voorspelt. Het oorspronkelijke

idee dat het instantane gedrag bij de meting van een deeltje van een verstrengeld paar ook uitsluitend met lokale interacties verklaard zou kunnen worden, pakt dus niet goed uit.

Tot nu toe zijn we ervan uitgegaan dat de voorspellingen gemaakt met behulp van de quantummechanica juist zijn. Gezien het succes van de quantummechanica is er geen reden hieraan te twijfelen. Maar het kan goed zijn dat ons blikveld te beperkt is. Een experiment is dus zeer welkom. Bell merkte al op dat er niet veel verbeeldingskracht voor nodig om je voor te stellen dat de grootheden  $E(\vec{a}, \vec{b})$ ,  $E(\vec{a}, \vec{c})$  en  $E(\vec{b}, \vec{c})$  daadwerkelijk worden gemeten in een echt EPRB-experiment. De uitkomst van zo'n experiment is natuurlijk heel belangrijk voor onze gedachten over de quantummechanica.

Een directe test van (5) is geen goed idee, omdat we in de praktijk te maken hebben met zaken als ruis en beperkte efficiëntie van de deeltjesdetectoren. Aanname (4) is in de praktijk niet te realiseren. Het waren Clauser, Horne, Shimony en Holt (CHSH) [3] die vijf jaar later, uitgaande van uitdrukking (3) Bells aanpak wisten uit te bouwen tot een haalbaar experiment.

Nu, vijftig jaar later, weten we dat hier door verschillende onderzoekers met grote toewijding aan

is gewerkt. In veel gevallen bleek de experimentele data de CHSH-versie van Bells ongelijkheid te schenden en zelfs, met inachtneming van experimentele onzekerheden, numeriek overeen te stemmen met de voorspellingen van de quantummechanica. Het besproken niet-locale gedrag is een essentieel element in recent werk aan teleportatie en quantumcryptografie en in andere quantumcomputing- en quantuminformatieprocessen. Bells werk kan gezien worden als het startpunt van deze activiteiten. Het is daarbij leuk om je nog eens te realiseren op welke wijze hij deze ontwikkelingen in werking heeft gezet.

## Referenties

- 1 D. Bohm en Y. Aharonov, *Discussion of Experimental Proof for the Paradox of Einstein, Rosen, and Podolsky*, Phys. Rev. **108** (1957) 1070.
- 2 D.J. Griffiths, *Introduction to Quantum Mechanics*, 2<sup>e</sup> ed., Pearson Prentice Hall, Upper Saddle River, NJ 07458, USA (2005).
- 3 J.F. Clauser, M.A. Horne, A. Shimony, en R.A. Holt, *Proposed experiment to test local hidden-variable theories*, Phys. Rev. Lett. **23** (1969) 880.

Ad Verbruggen  
(1953) studeerde  
natuurkunde aan  
de Vrije Universiteit  
in Amsterdam en is  
daar ook gepromo-  
veerd. Na postdoc  
periodes bij het  
IBM Thomas J. Watson Research Center  
in Yorktown Heights (VS) en het Max-  
Planck-Institute für Metallforschung in  
Stuttgart is hij sinds 1987 verbonden aan  
de Technische Universiteit Delft en is op  
dit moment staflid bij de afdeling Quantum  
Nanoscience, een onderdeel van het  
Kavli Institute of Nanoscience.



A.H.Verbruggen@tudelft.nl

**Waarom ging je natuurkunde studeren?**

Mijn ouders zijn beiden academici en ze hebben me een gezonde belangstelling meegegeven voor wetenschap en techniek. Ik kon nooit goed kiezen welk onderwerp daarbinnen me het meest trok, maar ik ben wel duidelijk een bèta. Ik vond dat je bij natuurkunde nog de meeste kanten op kon: van klein (quantumphysica) tot groot (kosmologie) en van theoretisch tot experimenteel. Vandaar.

**Wat vond je speciaal tijdens je studietijd?**

Mijn afstudeerproject heb ik uitgevoerd bij de vakgroep Quantumtransport van de faculteit Technische Natuurkunde in Delft. Daar mocht ik quantumcircuits fabriceren met vergelijkbare technieken als die in de productie van computerchips worden gebruikt. Ik vond het geweldig om te zien hoe dat proces werkt en om met de daarvoor benodigde apparatuur te werken. Het klonk in elk geval allemaal heel gaaf: elektronenbundelpatroongeneratoren, hoog-vacuümopdampers, elektronenmicroscopen. Het mooist vond ik dat je enerzijds in een clean room met hightechspullen werkt om een supergevoelig circuit te produceren, maar vervolgens met een eenvoudige weerstandsmeting bepaalt welke schakelingen op de chip goed zijn gelukt en die stukjes van de chip letterlijk afbreekt door met een stanleymesje in de wafer te krassen. Hoog technologisch, maar toch heel praktisch.

**Waarom koos je voor je eerste baan?**

Eigenlijk was dat vooral mazzel. Technische natuurkunde heet in Delft ook wel de studie van halve dagen. In mijn tweede studiejaar vond ik dat ik voldoende vrije tijd had en dat ik die toch maar met iets nuttigs moest gaan vullen. Omdat ik hoopte een leuk zak-

centje te kunnen verdienen met mijn computerhobby, heb ik me opgegeven bij een ICT-uitzendbureau voor studenten. Toen ik na mijn eerste sollicitatiegesprek in de wachtkamer zat, kwam er een telefoontje binnen van het Nederlands Forensisch Instituut (NFI). Daar werd een parttime software-ontwikkelaar gezocht om tools te ontwikkelen die de politie zouden kunnen helpen in misdaadonderzoeken. Kennelijk ging het goed met het uitzendbureau, want ik was de enige beschikbare persoon. Wie zou niet gaan voor zo'n kans?

Bij het NFI leerde ik de latere oprichters van Fox-IT kennen. Een van de dingen die onderzoekers bij het NFI vaak merkten als ze bewijsmateriaal in een strafzaak bekeken, was dat boeven doorgaans wel zo slim waren hun spullen te beveiligen. Maar ze merkten ook dat die beveiliging vaak niet heel lastig te kraken was, in elk geval in die tijd. Een van de gedachten achter de oprichting van Fox was dat dat soort beveiligstechnieken toch beter moesten kunnen – niet voor de boeven natuurlijk, maar wel voor alle andere mensen die van dergelijke beveiling gebruikmaakten. Dat leek me een leuke uitdaging en bij toeval startte er net een project toen ik mijn afstudeerproject op de TU afrondde, dus ik kon meteen aan de slag. Misschien had ik van mijn bijbaan bij het NFI ook een echte baan kunnen maken, maar op dat moment vond ik een commercieel bedrijf – zeker een start-up als Fox – ook wel spannend klinken.

**Wat zijn je belangrijkste werkzaamheden en voel je je nog natuurkundige in je huidige werk?**

Ik ben nu als director of operations bij Fox verantwoordelijk voor onze dienstverlening aan klanten in de Benelux en een

# De quantumbeveiliger

**Jeremy Butcher studeerde natuurkunde in Delft en kwam via een uitzendbedrijf terecht bij het Nederlands Forensisch Instituut om software te ontwikkelen voor het oplossen van misdaden. Momenteel werkt hij bij Fox-IT dat zich bezighoudt met cyberbeveiliging en cyberdefensie.**



Jeremy Butcher (links) aan het werk.

deel van ons internationale portfolio. Daar valt van alles onder, van het testen van de beveiliging van onze klanten en het monitoren van hun netwerken op de aanwezigheid van hackers, tot het helpen van een klant bij wie digitaal is ingebroken, tot de ontwikkeling van een cryptografische chip en afgeleide producten voor het beschermen van staatsgeheimen en de vitale infrastructuur.

Het grootste deel van de dag ben ik bezig andere Fox'ers te helpen hun werk te doen en in de gaten te houden wat er in de buitenwereld gebeurt. Ik ben mijn interesse in de techniek natuurlijk niet kwijt en ik doe mijn best om in elk geval op conceptueel niveau goed te snappen wat we bij Fox doen en waar we naartoe moeten.

Natuurkundige ben ik dus niet in het dagelijkse leven, maar op afstand volg ik wel wat er gebeurt rond quantum-

computers en quantum key distribution. Ik zou het leuk vinden als die ooit daadwerkelijk breed toegepast zouden worden voor beveiliging van systemen.

#### *Wat is fascinerend aan je huidige werk?*

Meedraaien op het allerhoogste niveau van de beveiligingswereld. Fox'ers zijn trots op hun werk: we maken producten die kerncentrales en staatsgeheimen beveiligen, we worden ingeroepen als het echt goed moet zijn (of wanneer er echt iets mis is gegaan), en we zijn vaak de eersten die incidenten signaleren bij wereldwijde spelers (recentelijk het Amerikaanse televisienetwerk NBC en Yahoo!). Je komt dus op spannende plekken waar je het verschil kunt maken en je bent continu bezig te bedenken hoe je de meest serieuze aanvallers kunt buitenhouden, vandaag, maar ook over een paar jaar.

En dan probeer je dat ook nog zo vorm te geven dat het een commercieel succes wordt.

#### *Zou je – terugkijkend – opnieuw voor dezelfde studie kiezen?*

Ik heb in elk geval nooit spijt gehad van mijn keuze voor natuurkunde. Mijn studie in Delft was een leuke tijd en ik heb er veel geleerd. Ik vind dat ik geluk heb met de plek die ik heb gevonden in de ICT. Terugkijkend denk ik dat ik dat pad kon oplopen doordat ik 's avonds nog zin had om met mijn pc te spelen. Ik denk niet dat ik dat enthousiasme zou hebben gehad als ik de hele dag al over computers had nagedacht, bijvoorbeeld door informatica te studeren. Wat dat betreft is natuurkunde mijn redding geweest ☺.



# Quantumzekere authenticatie

**Authenticatie van personen of objecten kan met behulp van ‘iets dat men weet’ of door ‘iets dat men heeft’. Nadeel van iets dat men weet, zoals een digitale code, is dat het geheim gehouden moet worden. Een traditionele sleutel, een bekend voorbeeld van iets dat men heeft, kan vaak makkelijk gekopieerd worden zonder dat het slachtoffer het opmerkt. Er bestaan fysieke onkloonbare sleutels die dit nadeel niet hebben. Een optisch voorbeeld is een stukje veelverstrooiend materiaal zoals wit keramiek, dat onder laserbelichting een uniek spikkelpatroon produceert. Emulatie van zo’n respons is echter nog steeds een gevaar als de optische eigenschappen van de sleutel bekend zijn. We introduceren een quantumfysische manier van uitlezen waardoor emulatie volledig uitgesloten kan worden. We noemen dit quantumzekere authenticatie.** Boris Škorić en Pepijn Pinkse

198

**V**eel handelingen in onze moderne maatschappij vertrouwen op foutloze authenticatie. Denk maar aan de authenticatie van stemmers in een stembureau, de authenticatie van klanten van een bank bij financiële transacties of die van reizigers op een vliegveld. Traditionele vormen van authenticatie door middel van fysieke of digitale sleutels hebben beide een groot nadeel: zulke

sleutels kunnen worden gekopieerd en de eigenaar zal in veel gevallen helemaal niet doorhebben dat zijn of haar sleutel gekopieerd is, tot het te laat is. Er is een moderne vorm van fysieke sleutels die dit nadeel niet kent: de zogenaamde ‘fysieke onkloonbare sleutel’ of in het Engels *physically unclonable function* (PUF) [1]. PUF’s zijn zeer moeilijk te kopiëren, omdat de fabricage intrinsiek een groot aantal oncontroleerbare aspecten bevat. Verder kan je een PUF onderwerpen aan een fysieke prikkel (de vraag, in cryptografentaal), die leidt tot een ingewikkelde output (de respons). De vraag- en responsruimte van een PUF zijn beide groot. Na de fabricage van een PUF wordt er een database aangelegd van vraag-responsparen; daarna wordt de PUF afgegeven aan iemand die zich wil kunnen authenticeren (typisch Bob genoemd). Iemand, laten we zeggen Alice, kan Bob later authenticeren door zijn PUF aan vragen te onderwerpen en te kijken of de responsen kloppen met de database.

Boris Škorić studeerde theoretische natuurkunde aan de Universiteit van Amsterdam. In 1999 promoveerde hij daar op een proefschrift over het quantum-Hall-effect. Daarna werkte hij als onderzoeker bij Philips Research, eerst aan display-fysica en later aan codering en cryptografie. Sinds 2008 is hij universitair docent aan de faculteit Wiskunde en Informatica van de TU Eindhoven.

b.skoric@tue.nl



## Spikkelpatroon

Wij gebruiken als PUF kleine stukjes sterk verstrooïnd materiaal zoals droge witte verf of keramiek. Het spikkelpatroon (Engels: speckle) dat ontstaat als zulk materiaal met laserlicht wordt beschouwd als uniek. Het spikkelpatroon (de respons) hangt, afgezien van de precieze belichting (de vraag), op een zeer gevoelige manier af van de positie, vorm en samenstelling van ontelbare verstrooiers op submicrometerschaal waaraan het licht veelvuldig verstrooit. Zelfs de fabrikant kan geen twee PUF’s maken met identiek gedrag, want hij zou daarvoor miljoenen verstrooiers op de juiste manier in 3D moeten kunnen assembleren met een resolutie op nanometerschaal, en dat lukt zelfs de meest geavanceerde 3D-printer bij lange na niet. Het is tevens onbegonnen werk om een ander soort object te produceren dat het gedrag van een gegeven PUF nabootst. Met moderne technieken zoals beeldvormende chips, hologrammen of nano-optische circuits kunnen weliswaar

complexe transformaties gebouwd worden, maar zijn de lichtverliezen zo groot dat het meteen opvalt.

### Emulatie

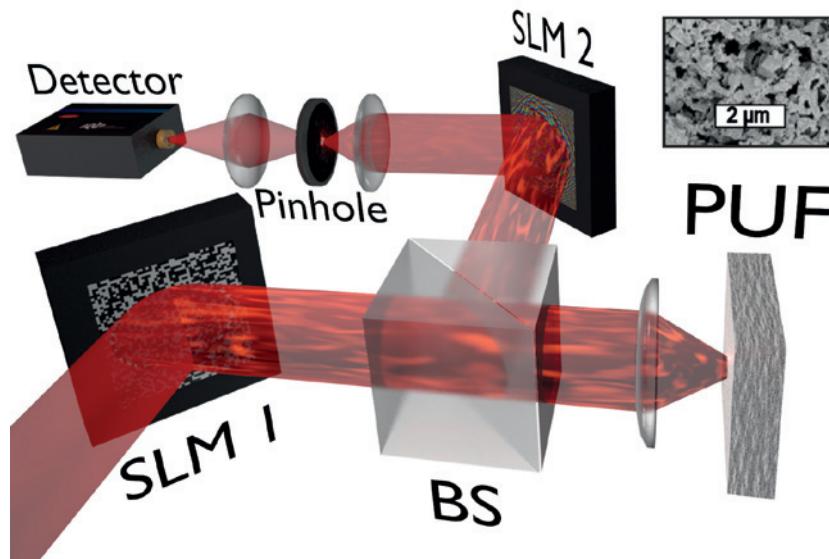
Alles dus in orde? Waarom hebben PUF's de wereld nog niet veroverd? Een van de redenen is de noodzaak om voor elke afzonderlijke PUF apart data op te slaan, wat voor logistieke overhead zorgt. Een andere reden is het probleem van emulatie. Het is niet uit te sluiten dat een aanvaller toegang verkrijgt tot Bobs PUF of zelfs tot de PUF-database. Als een aanvaller eenmaal kennis heeft van een groot aantal vraag-responsparen, dan is authenticatie problematisch geworden. De aanvaller kan zich dan namelijk voordoen als Bob: hij beantwoordt vragen door de respons op te zoeken in zijn persoonlijke database. Hier heeft hij de PUF niet voor nodig. Zo'n aanval noemen we PUF-emulatie.

Emulatie-aanvallen zijn te voorkomen door goede fysieke inspectie: je moet met zekerheid kunnen vaststellen dat je een fysiek object aan het bevrager bent en dat het object de juiste afmeting et cetera heeft. De aanvaller zou immers met zijn eigen apparatuur een fysieke respons kunnen genereren op grond van zijn database. Het bouwen versus om de tuin leiden van de inspectie is een wapenwedloop waarbij de kosten hoog oplopen en het nooit duidelijk is hoe veilig het systeem nou precies is.

Hier biedt quantumzekere authenticatie (QSA, quantum-secure authentication) [2] een uitkomst door quantumphysica in te zetten ter bescherming van de vragen. QSA is een uitleesmethode die emulatie onmogelijk maakt. Elke vraag bevat veel informatie die voor de aanvaller onvoorspelbaar is. De vraag wordt gesteld middels een klein aantal quanta (fotonen), of zelfs een enkel quantum. Vanwege de collaps van de golffunctie in geval van een meting, en vanwege het no-cloning theorem [3], bestaat er voor de aanvaller geen enkele betrouwbare manier om te leren welke informatie in de vraag verstopt zit. En als hij niet weet wat de vraag is, dan kan hij ook niet de respons opzoeken! Anderzijds is Alice wel in staat om de respons te checken, omdat zij de vraag volledig kent.

### Experiment

Ons demonstratie-experiment van



Illustratie van het demonstratie-experiment voor quantumzekere authenticatie [2]. Een zwakke laserpuls wordt door SLM1 van een complex ruimtelijk patroon voorzien en wordt daarna afgebeeld op de PUF. De PUF bestaat uit pigmentpoeder op een glasje. SLM2 is zo geprogrammeerd dat een correcte respons zal worden omgezet naar een vlakke golf (en een incorrect golffront naar een ingewikkeld spikkelpatroon). De vlakke golf wordt op een gaatje (pinhole) afgebeeld, en de detector telt hoeveel fotonen er door het diafragma passeren.  
Illustratie: T.J. Huisman.

QSA is geïllustreerd in de figuur hierboven: we belichten de PUF met een zwakke laserpuls die bijvoorbeeld maar één enkel foton bevat. Om het ruimtelijke patroon van het licht te beschrijven is echter veel informatie nodig. Het ingewikkelde golffront (de vraag) wordt gemaakt door de puls te manipuleren met een spatial light modulator (SLM), een beeldvormende chip die op programmeerbare wijze in ieder van zijn vele pixels afzonderlijk de fase van het licht kan draaien. De respons van de PUF wordt afgebeeld op een klein gaatje met behulp van faseconjugatie: middels een tweede SLM compenseren we het ruimtelijke fasepatroon van de respons zodanig dat alleen het verwachte patroon netjes afgebeeld wordt op het gaatje. Een fotonenteller achter het gaatje kijkt of er voldoende fotonen passeren. Als de respons gelijk is aan de verwachte respons, dan passeren vrijwel alle fotonen het gaatje. Een verkeerde respons wordt door SLM2 getransformeerd naar een random spikkelpatroon, waardoor het grootste deel van het licht het gaatje mist.

We hebben bewezen dat QSA veilig is tegen alle aanvallen waarbij de aanvaller probeert de vraag te meten en op grond van die meting de bijbehorende respons opzoekt [4, 5]. QSA met optische PUF's is veilig zolang het aantal fotonen in

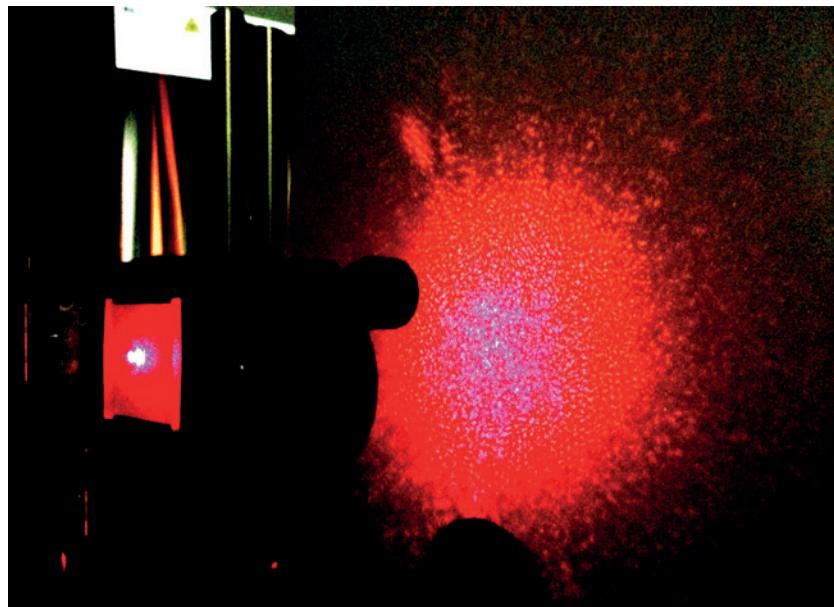
de laserpuls kleiner is dan het aantal ruimtelijke 'kanalen', wat ongeveer het aantal spikkels is. Bij QSA wordt het hele vraag-responsproces een aantal keer herhaald, waarbij natuurlijk iedere keer een nieuwe random vraag wordt gebruikt. De totale kans van slagen van de aanvaller (zijn kans om geauthenticeerd te worden ook al heeft hij de PUF niet) daalt exponentieel met het aantal herhalingen.

In het demonstratie-experiment [2] hadden we al ruim duizend kanalen, zodat een emulatiecircuit al gauw meer dan een miljoen parameters zou moeten hebben en dat gecombineerd met zeer geringe lichtverliezen als de aanvaller het volledige gedrag van de

Pepijn Pinkse studeerde natuurkunde aan de Universiteit Leiden. Hij promoveerde aan de Universiteit van Amsterdam in 1997 op onderzoek aan atomair waterstof. Hierna werkte hij elf jaar in Duitsland, voornamelijk op het Max Planck Instituut voor Quantumoptica in Garching, waar hij resonator-QED en koude atoom- en molecuulgassen onderzocht. In 2009 werd hij programma directeur nano-optica aan het MESA+ Institute for Nanotechnology van de Universiteit Twente; sinds 2014 is hij adjunct hoogleraar.



Pepijn.Pinkse@utwente.nl



Spikkelpatroon in het lab. Op de voergrond links staat een *physically unclonable function* (PUF) die – om het patroon op deze foto goed zichtbaar te maken – belicht wordt met een sterke rode laserbundel. Door veelvoudige verstrooiing in de PUF ontstaat het spikkelpatroon aan de achterkant. Dit illustreert hoe de respons van de PUF in quantumzekere authenticatie er uit ziet. De paarse kleur is in werkelijkheid intens rood.

PUF wil klonen. Dat is op zich al een schier onmogelijke opgave. Het wordt nog moeilijker als we een laser gebruiken met een korte coherentielengte: dan mag het circuit ook nog eens niet veel groter zijn dan de PUF zelf. Ons is geen technologie bekend die dat ook maar bij benadering voor elkaar kan krijgen. Men kan denken aan ander-soortige aanvallen, zoals het aanbieden van een overvloed aan licht zodat er altijd genoeg fotonen het diafragma passeren. Zulke aanvallen zijn op tri-viale wijze te herkennen, bijvoorbeeld door ook buiten het diafragma detectoren te plaatsen, of door op onvoorspelbare momenten nep-pulsen aan te bieden waarvan je juist helemaal niet verwacht dat ze tot fotondetectie leiden.

### **Veiligheid**

QSA combineert quantumfysische aspecten met elementen uit random lichtverstrooiing en cryptografie. De veiligheid van de authenticatie berust op de combinatie daarvan:

- (het fysieke gedrag van) de sleutel is niet te kopiëren omdat daartoe de technologie ontbreekt,
- emulatie middels het opzoeken van responsen is fundamenteel onmogelijk vanwege de quantummechanische onzekerheid bij meting van de zwakke vraagpuls.

Interessant is dat QSA gewoon werkt met zwak laserlicht en het niet nodig is om dure quantumlichtbronnen te

gebruiken die bijvoorbeeld precies één foton of verstrengelde fotonparen genereren. We denken daarom dan ook dat een commerciële implementatie niet duur hoeft te zijn. Bijna alle benodigde hardware is al te vinden in projector-smartphones.

Het is ook interessant om op te merken dat QSA geen geheimen nodig heeft: elke PUF kan geauthenticeerd worden op grond van publieke informatie. En als er geen geheimen zijn, kunnen die ook niet uitlekken; dat is wel zo veilig.

We verwachten dat QSA gecombineerd kan worden met quantumcryptografie om boodschappen te versturen. Voor veilige cryptografie zijn geheime digitale sleutels nodig. Er bestaan al commerciële systemen voor het uitwisselen van geheime digitale sleutels op een quantumveilige manier (*quantum key exchange*). Normaal gesproken is het daarbij vereist om naast een quantumkanaal ook een geauthenticeerd klassiek communicatiekanaal te hebben, bijvoorbeeld een telefoonlijn: Alice moet zeker weten dat ze met Bob communiceert en niet met iemand anders. De combinatie met QSA creëert een geauthenticeerd quantumkanaal, waardoor het klassieke kanaal niet langer geauthenticeerd hoeft te zijn. De praktische impact hiervan is dat het voor de partijen die samen quantumcryptografie doen niet meer nodig is om van tevoren een (korte) klassieke authenticatiesleutel

af te spreken; in plaats daarvan kan publieke informatie over de PUF gebruikt worden.

Als de Snowden-affaire ons iets geleerd heeft, is dat het belang van echt goede informatiebeveiliging. Het zou fantastisch zijn als een fundamenteel fysisch principe als quantummechanische onzekerheid en meervoudige lichtverstrooiing daartoe kunnen bijdragen.

### **Dankwoord**

We danken Jacopo Bertolotti, Klaus Boller, Geza Giedke, Jennifer Herek, Marcel Horstmann, Simon Huisman, Thomas Huisman, Bart Jacobs, Ad Lagendijk, Allard Mosk, Gerhard Rempe, Berry Schoenmakers, Willem Vos en Tom Wolterink.

### **Referenties**

- 1 R. Pappu, B. Recht, J. Taylor en N. Gershenfeld, *Physical one-way functions*, *Science* **297** (2002) 2026.
- 2 B. Goorden, M. Horstmann, A.P. Mosk, B. Škoric en P.W.H. Pinkse, *Quantum-Secure Authentication of a Classical Key*, arxiv.org/1303.0142.
- 3 W.K. Wootters en W.H. Zurek, *A Single Quantum Cannot be Cloned*, *Nature* **299** (1982) 802.
- 4 B. Škoric, A.P. Mosk en P.W.H. Pinkse, *Security of quantum-readout PUFs against quadrature-based challenge-estimation attacks*, *Int. J. Quant. Inf.* **11**, 1350041–1 – 1350041–15 (2013).
- 5 B. Škoric, *Security analysis of Quantum-Readout PUFs in the case of challenge-estimation attacks*, http://eprint.iacr.org/2013/479.



# Quantumwereld

## in de klas

**Na een lange periode van voorbereiding is in schooljaar 2013-2014 het nieuwe natuurkunde-examenprogramma NiNa van start gegaan.**

**De voorbereiding kende meerdere gevoelige punten. Eén daarvan: quantumphysica voor alle vwo-leerlingen. Enige tijd stond dit onderwerp op de rol als schoolexamendomein, maar uiteindelijk wordt het getoetst op het centraal schriftelijk examen. In 2016 zullen alle leerlingen met natuurkunde in hun pakket basale kennis moeten hebben over quantumphysica.**

Lodewijk Koopman

### Waarom quantum in het vwo?

Een van de doelstellingen van NiNa is in het schoolvak natuurkunde meer nadruk te leggen op moderne natuurkunde. In het visiedocument van de NiNa-commissie uit 2006 [1] wordt geconstateerd: "De moderne schoolnatuurkunde stopt met kernenergie en straling [...]. Veelal ontbreekt daardoor in de schoolstof de inspiratie die uitgaat van de belangrijke en nieuwe uitdagingen van het vakgebied in de 21<sup>e</sup> eeuw. Het resultaat is een groeiende spanning tussen de schoolvakken en hedendaagse natuurwetenschap zoals leerlingen die leren kennen uit hun eigen ervaring (onder andere via de media)."

Nu, bijna acht jaar na het verschijnen van het visiedocument, blijkt hoe waar deze constatering is. Met grote regelmaat verschijnen er in verschillende media berichten over technologische en wetenschappelijke doorbraken waarin quantumphysica een belangrijke rol speelt. Het is de kunst om in het onderwijs hierop aan te sluiten en te zorgen dat de kennis van leerlingen over deze nieuwe inzichten het niveau van 'knoppenbeheersing' ontstijgt.

### Het examenprogramma

Eerdere vwo-examenprogramma's toetsen ook al onderdelen van de

quantumphysica [2]. In het voorlaatste examenprogramma (geldig tot en met 2009) worden drie onderdelen genoemd: het foto-elektrisch effect, spectraallijnen (atoommodel van Bohr) en de golf-deeltjedualiteit (de Brogliegolfengte en elektronenmicroscoop).

Er is echter een belangrijk verschil met NiNa. Er bestonden toen nog twee varianten van het schoolvak: een lichte variant (natuurkunde 1) en een wat zwaardere variant (natuurkunde 1,2). De genoemde onderwerpen waren bedoeld voor natuurkunde 1,2. Niet alle leerlingen kregen dus te maken met deze quantumonderwerpen. In het laatste examenprogramma, dat dus nu vervangen wordt door NiNa, werd alleen in zeer uitgeklede vorm de golf-deeltjedualiteit genoemd en dan alleen met betrekking tot het foto-elektrisch effect.

In het nieuwe examenprogramma zit nu een eigen domein quantumwereld waarin niet alleen de 'oude' quantumonderwerpen terug te vinden zijn. Ten eerste wordt het golf-deeltjedualisme nu uitgebreider genoemd (waarschijnlijkheid, waarschijnlijkheidsverdeling). Verder zit het begrip opsluiting voor het eerst in een eindexamenprogramma: het feit dat systemen

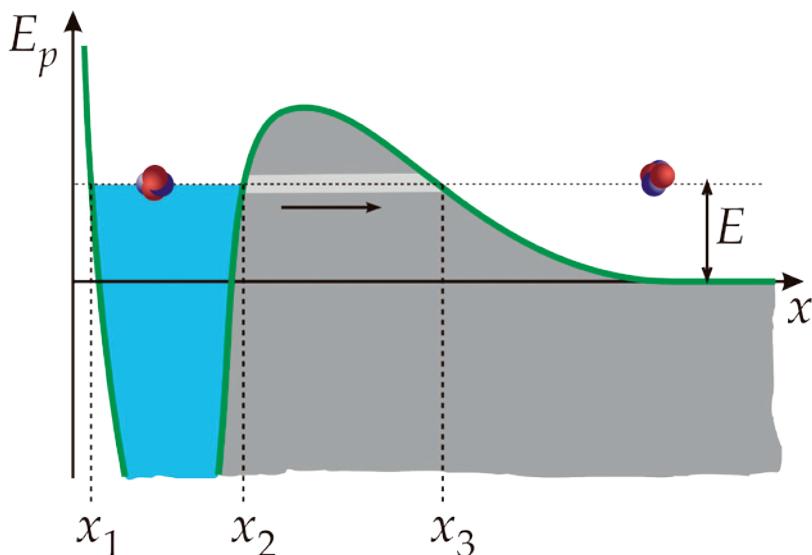
quantisatie vertonen wanneer deeltjes zich in een gebonden toestand bevinden. Belangrijke begrippen in het nieuwe programma zijn ook: onbepaaldheidsrelatie van Heisenberg en het deeltje in een doosje. Ook is er bijvoorbeeld ruimte voor het spectaculaire verschijnsel quantumtunneling. Het examenprogramma noemt als contexten waarin tunneling een rol speelt: de scanning-tunnelingmicroscoop (STM) en het model van Gamow voor alfaverval. Zoals bekend is, scant de STM op atomaire schaal met een tip een preparaat af. De ruimte tussen tip en preparaat vormt klassiek gezien voor elektronen een onoverbrugbare barrière. Dankzij tunneling kunnen elektronen deze barrière toch passeren en zo ontstaat een tun-

201

Lodewijk Koopman is docent natuurkunde aan het Scala College te Alphen aan den Rijn. In 2011 promoveerde hij aan de Universiteit van Amsterdam op een proefschrift over de didactiek van de quantumechanica. Hij is auteur van de vwo bovenbouwmethode Nova Natuurkunde.



lkoopman@dds.nl



**Figuur 1** Een alfadeeltje heeft niet genoeg energie om ‘over’ de potentiaalbarrièrē te komen, maar kan er wel ‘doorheen’ tunnelen.

nelstroom. Deze stroomsterkte is zozeer afhankelijk van de afstand tussen tip en preparaat dat de atomaire structuur van het preparaat afgestast kan worden. Voor natuurkundigen een bekend verhaal, maar voor leerlingen een buitengewoon boeiende context om quantumtunneling te leren kennen. Dit geldt ook voor het model van Gamow voor alfaverval. Dit model verklaart heel elegant waarom alfastralers enorm uiteenlopende halveringstijden hebben (van ruwweg  $10^{-6}$  seconde tot  $10^8$  jaar). In dit model wordt het alfadeeltje gezien als deeltje in een potentiaalputje dat gevormd wordt door de aantrekkende kernkracht en de afstotende Coulombkracht (zie figuur 1). De hoogte van de barrière van het putje wordt bepaald door het atoomnummer van de dochterkern, de energie van het alfadeeltje wordt gelijk gesteld aan de geobserveerde waarde. Via deze voorbeelden wordt het voor een leerling duidelijk dat we quantumphysica echt nodig hebben bij het beschrijven van de natuur.

### Nascholing

Een deel van de natuurkundedocenten is uitstekend op de hoogte van de quantumphysica en van de laatste ontwikkelingen op dit punt. Voor deze docenten zou een nascholing over de didactiek van de quantumphysica wellicht op zijn plek zijn. Een deel van de natuurkundedocenten echter heeft beperkt of zelfs geen quantumphysica onderwezen gekregen. Dit is een mogelijkheid doordat de laatste jaren op

verschillende manieren docenten zijn ingestroomd als natuurkundedocent op het vwo (denk bijvoorbeeld aan de zogenaamde zij-instromers). Hun kennis over de quantumphysica zelf zal opgefrist moeten worden. Gelukkig worden er inmiddels verspreid over Nederland door verschillende bètasteunpunten nascholingen gegeven. In opdracht van het IOBT (Innovatie van het Onderwijs in de Bèta-wetenschappen en Technologie) heeft ondergetekende samen met Hans van Bemmel een nascholingscursus ontwikkeld die inmiddels al verschillende kerken aan de TU Delft (Delft voor Docenten) en de UvA (Its Academy) is gegeven. Zonder volledig te willen zijn: er zijn nascholingen aan de Universiteit Utrecht (Bètasteunpunt Utrecht), Bèta Steunpunt Oost (samenwerking Universiteit Twente en de hogescholen Saxion en Windesheim), TU Eindhoven (binnen het programma Bèta Black Belt) en de Radboud Universiteit Nijmegen.

De opzet van deze nascholingscursussen is niet helemaal gelijk: de ene cursus richt zich meer op ‘hoe quantummechanica werkt’, de ander richt zich meer op kwalitatief begrip en vakdidactiek. Deze verscheidenheid aan aanbod is niet per se verkeerd: zoals al eerder besproken zal de behoefte bij docenten ook niet gelijk zijn.

### Didactiek

Het streven is mooi: quantumwereld op het vwo, maar hoe doe je dat? Juist omdat het huidige examenprogramma nieuw is, is er wat betreft de di-

dactiek van de quantumwereld in het voortgezet onderwijs nog veel te ontdekken. Een belangrijke uitzondering is het Project Moderne Natuurkunde (PMN) [3]. Dit project is opgezet om binnen het voorlaatste examenprogramma (natuurkunde 1,2) juist nadrukkelijker aandacht te besteden aan de moderne natuurkunde [4]. Er was zelfs een eigen eindexamen voor scholen die deelnamen aan PMN. In 2013 ontving een van de auteurs, Dick Hoekzema, mede voor dit project de Minnaertprijs.

Het unieke aan PMN is misschien wel dat het in een iteratief proces in meerdere ronden is ontwikkeld en uitgetest. Binnen PMN is er dus veel ervaring en kennis opgedaan met hoe je moderne natuurkunde in het voortgezet onderwijs kunt brengen. Toch is vakdidactisch onderzoek op dit gebied wenselijk. Ten eerste omdat PMN niet voor alle natuurkundelearlingen bestemd was, ten tweede omdat de doelstellingen van PMN en NiNa niet geheel overeenkomen. Om een paar verschillen te noemen: in PMN wordt de golffunctie nadrukkelijk gebruikt en is er aandacht voor het twee- en driedimensionale deeltje in een doosje, maar tunneling komt niet voor. Aan de universiteit Twente start in augustus een promotietraject (NWO-lerarenbeurs) over de didactiek van de quantumphysica zoals het in het nieuwe examenprogramma is opgenomen.

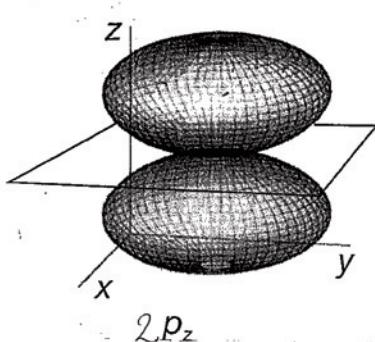
Binnen mijn promotieonderzoek heb ik vooral onderzoek gedaan naar eerstejaars vakken quantumphysica (quantummechanica voor natuurkundigen en quantumchemie voor scheikundigen) aan de universiteit [5]. Mijn interesse ging uit naar hoe aan te sluiten op het denkkader van studenten om zo toe te werken naar de quantumtheorie. Dit wordt ook wel geleid herontdekken genoemd (*guided discovery learning*). Zo blijkt het mogelijk om op basis van resultaten van experimenten (het dubbelspleetexperiment) studenten zelf fundamentele vragen te laten formuleren over hoe een quantumdeeltje (zoals een elektron) beschreven moet worden. De mogelijke misconcepties konden zo al in een vroeg stadium zichtbaar worden gemaakt.

Mijn onderzoek heeft helaas ook laten zien dat studenten die het vak met mooie cijfers hebben afgerond (rond

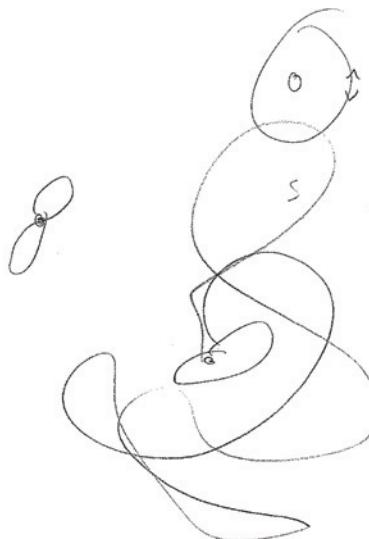
een acht of hoger) er nog steeds ‘klas-sieke’ denkbeelden op nahouden. Zo legt een student uit wat de betekenis is van een grafische weergave van een  $2p_z$ -orbitaal (figuur 2). Hij herinnert zich een plus in de ene en een min in de andere lobbe. Op mijn vraag wat die plus en min betekenen, antwoordt hij dat het te maken heeft met de la-ding van het elektron. Al pratende komen we op de betekenis van de golffunctie. Hij tekent de baantjes in figuur 3: zo beweegt volgens hem het elektron. Als ik vraag of dat altijd zo is, antwoordt hij dat elektronen soms heel vreemd doen (de wilde lijntjes rechtsonder in figuur 3).

Uit het buitenland is relevant vakdi-dactisch onderzoek beschikbaar dat naar de Nederlandse situatie vertaald kan worden. Twee onderzoeken zijn met name het vermelden waard. Het eerste gaat over het Bohrmodel van het atoom, explicet genoemd in het nieuwe examenprogramma. Er is in de literatuur een debat geweest over de vraag of dit model van de oude quantummechanica wel onderwezen moet worden. McKagan en collega’s argumenteren van wel [6]. Maar met een belangrijke bijsluiter: onderwijs het nadrukkelijk als model en plaats het naast andere modellen van het atoom. Daarbij blijkt het belangrijk om aan te geven wat de beperkingen zijn van dit model. Deze nadruk op modelleren past heel mooi bij een ander nieuw en wellicht nog niet goed opgemerkt domein binnen het nieuwe examenprogramma: natuurwetten en modellen.

Het tweede onderzoek dat ik hier wil noemen gaat over de interpretatie van de quantumphysica [7]. Al sinds de ont-staansperiode van de quantumphysica is de interpretatie van de theorie onderwerp van debat. De vraag is of je op scholen ook explicet aandacht aan interpretatie zou moeten besteden? De neiging om dit uit de weg te gaan is begrijpelijk en het kán uiteindelijk ook zonder: je hoeft je immers niet per se met interpretatie bezig te houden om toch zaken uit te kunnen rekenen. Er is echter een belangrijke didactische reden om hier toch explicet aandacht aan te besteden. Het blijkt dat, als je dat niet doet, de meeste leerlingen er aan het eind van een cursus een semi-klassiek wereldbeeld op na houden. Dit sluit aan bij wat ook uit mijn eigen onderzoek volgt.



**Figuur 2**  $2p_z$  orbitaal.



**Figuur 3** Een student tekent de ‘baan’ van een elektron in een  $2p_z$  en  $1s$  orbitaal (boven). Onder laat de student zien wat hij verstaat onder ‘onbepaaldheid’: het elektron in een  $1s$  orbitaal gedraagt zich onvoorspelbaar, maar beschrijft nog steeds een baan.

### Wat kunt u doen?

Een belangrijke verandering in het natuurkundeonderwijs is dus in gang gezet. Omdat de meeste methoden en scholen quantumwereld in 6 vwo zullen plaatsen, zal in schooljaar 2015-2016 het onderwerp echt in de klas komen. Uit de nascholingsbijeenkomsten komt naar voren dat docenten moeite hebben om voor het onderwijs geschikte contexten te vinden. Verder is er bij docenten ook vraag naar geschikte experimenten. Om aan deze vraag te voldoen wordt er onder andere door de Its Academy (regio Amsterdam) en de Universiteit Twente gewerkt aan zogenaamde leskisten met quantumexperimenten. Scholen kunnen deze leskisten huren voor bepaalde tijd. Dit bespaart scholen het aanschaffen van dure appara-tuur die slechts enkele keren wordt gebruikt.

De leskisten vormen een begin wat betreft mogelijkheden tot practica. De insteek van het nieuwe examenpro-gramma is ook aan te sluiten op de huidige onderzoekspraktijk. Hiervoor is een rol weggelegd voor veel lezers van het NTvN. Ideeën voor experi-menten, praktisch werk en contexten waarin quantumphysica nog mooier aan de orde gesteld kan worden, zijn zeer welkom. Deze ideeën zouden bij-voorbeeld beschreven kunnen worden in artikelen in het NTvN of NVOX, dat

relatief door meer natuurkundedo-centen gelezen wordt.

### Referenties

- 1 Natuurkunde Leeft – visie op het vak natuurkunde in havo en vwo, Commissie Vernieuwing Natuurkundeonderwijs havo/vwo, mei 2006.
- 2 Zie voor de huidige en oude versies van het examenprogramma: [www.examensblad.nl](http://www.examensblad.nl).
- 3 Project Moderne Natuurkunde: [www.fisme.uu.nl/mn/](http://www.fisme.uu.nl/mn/).
- 4 D.J. Hoekzema, G.J. Schooten, E. van den Berg en P.L. Lijnse, NTvN 70-5 (mei, 2004), 136.
- 5 L. Koopman, *A developmental research on introducing the quantum mechanics formalism at university level*, 2011, <http://dare.uva.nl/record/377069>.
- 6 S.B. McKagan, K.K. Perkins en C.E. Wieman (2008, March). *Why we should teach the Bohr model and how to teach it effectively*. Phys. Rev. ST Phys. Educ. Res., 4(1), 1-10.
- 7 C. Baily en N.D. Finkelstein (2010, January). *Teaching and understanding of quantum interpretations in modern physics courses*. Phys. Rev. ST Phys. Educ. Res., 6(1), 010101.

# Verstrengeld of niet? Bells

Einstein geloofde er niet in: twee deeltjes die zo verstrengeld met elkaar zijn dat ze altijd dezelfde toestand hebben, ongeacht hoe ver van elkaar verwijderd zijn. John Bells artikel uit 1964 (zie de artikelpagina) beweert dat een verstrengeling aangetoond zou kunnen worden in een experiment. Hier is een voorbeeld van hoe dat kan.



# Songelijkheid in spelvorm

zijn dat meetuitkomsten niet-klassieke correlaties vertonen, zelfs als ze van Ad Verbruggen en Herman de Lang) gaf aan hoe het bestaan van spelen we dit experiment na in een spelshow. Het verloop van het spel een score te behalen die zonder verstrengeling onmogelijk is.

## Spelregels Alles of Niets:

- HET SPEL WORDT GESPEELD IN TEAMS VAN 2 PERSONEN EN HET DOEL IS EEN ZO HOOG MOGELIJKE SCORE TE BEHALEN. HET SPEL BESTAAT UIT MEERDERE RONDES:
  - PER RONDE KRYGT IEDERE SPELER EEN EIGEN VRAAG EN GEEFT DAAROP METEEN ANTWOORD. DE SPELERS WETEN NIET WELKE VRAAG DE ANDER HEEFT GEKREGEN.
  - ER ZIJN MAAR 2 MOGELIJKE VRAGEN 'FLESJE?' EN 'GLASJE?' EN TWE MOGELIJKE ANTWOORDEN: 'ROOD' OF 'WIT'
- DE VRAGEN EN ANTWOORDEN VAN IEDERE RONDE WORDEN GENOTEERD EN AAN HET EIND VAN HET SPEL WORDT DE SCORE BEREKEND AAN DE HAND VAN DE VOLGENDE TABEL:
- De uiteindelijke score is het percentage goed beantwoorde vragen.

VRAAG AAN:	COMBINATIES VAN GOEDE ANTWOORDEN			

## Team Einstein



Team Einstein gelooft in lokaal realisme. Hun strategie is gericht op slim overleg voordat de spelshow begint. Ze stellen een lijst op met de gezamenlijke antwoorden die ze gaan geven ('verborgen variabelen'). De score die ze zo kunnen behalen is 75%. Dit betekent dat ze op 75% van de vragen de juiste combinatie van antwoorden geven. Uit de tabel is af te lezen dat ze deze score behalen als ze bijvoorbeeld afspreken altijd een verschillend antwoord te geven.

## Team Bell



Team Bell gelooft in quantummechanica. De twee spelers van Team Bell maken voor elke vragenronde twee verstrengelde quantumbits, waarvan elke speler er 1 meeneemt. Bij het antwoorden doen ze het volgende: ze meten de waarde van hun quantumbit onder een hoek die ze laten afhangen van de vraag. De verstrengeling zorgt ervoor dat hun antwoorden sterk gecorreleerd zijn. Zo halen ze een score van 85%. Flink hoger dan dat van Team Einstein!

## Team Loophole



Team Loophole gelooft niet in quantummechanica maar probeert het spel te winnen door vals te spelen. Ze hebben daarvoor twee tactieken, waarmee ze de maximale score van 100% kunnen halen.

- In sommige vragenrondes weigert een speler antwoord te geven (de 'detectie-loophole'), zodat de speler effectief bepaalt welke vragenrondes meetellen. Om dit te voorkomen, eist de presentator dat elke vraag beantwoord wordt.
- Ze gebruiken stiekem mobiele telefoons zodat ze de antwoorden kunnen afstemmen (de 'lokalisatie-loophole'). Om dit te voorkomen zet de presentator de spelers zo ver uit elkaar dat zelfs communicatie met de lichtsnelheid onmogelijk is.

Hoewel elk van deze 'loopholes' apart is uitgesloten in experimenten, is er tot nu toe geen experiment dat ze allemaal tegelijk uitsluit. Zo'n 'loophole-vrije' Bell-test kan het definitieve bewijs van het gelijk van Bell en het ongelijk van Einstein leveren.

# Een klassieke meting met behulp van een quantumdetector?

**Meten is een cruciale bezigheid in de natuurkunde. Elders in dit nummer kunt u lezen hoe het mogelijk is om, tussen de elektronen in defecten in twee verschillende diamanten, die enkele meters van elkaar verwijderd zijn, quantumverstrekking te veroorzaken door het doen van de juiste meting. Maar wat is een meting? Vragen we dit aan Niels Bohr dan krijgen we te horen hoe deze vraag in de Kopenhagense interpretatie van de quantummechanica wordt beantwoord: een meting vindt plaats door een grote detector te koppelen aan een quantumsysteem. De grote detector noemen we klassiek, ook al weten we niet hoe groot de detector daarvoor moet zijn. De kans op een bepaalde meetuitkomst  $P(x)$  wordt gegeven door het kwadraat van de golffunctie  $\psi$  die de toestand van het quantumsysteem beschrijft:  $P(x) = |\psi(x)|^2$ .** Tjerk Oosterkamp

206

In de afgelopen jaren zien we steeds meer experimentatoren die werken aan het verhogen van de gevoeligheid van mechanische resonatoren die voor verschillende doeleinden als sensor worden gebruikt. Inmiddels lukt het af en toe om deze mechanische resonatoren zo nauwkeurig te manipuleren dat ze zich zelf ook aan de wetten van de quantummechanica moeten onderwerpen. Zou een dergelijke detector twee waardes tegelijk kunnen meten, in navolging van een elektron dat op meerdere plaatsen tegelijk kan zijn? Of is dit geen zinvolle vraag?

Alvorens op die laatste kwesties in te gaan, laat ik eerst zien hoe de quantisatie van licht de nauwkeurigheid van een mechanische-krachtsensor beperkt. We bekijken een mechanische

detector, een klein duikplankje dat doorbuigt wanneer een kracht aan het vrije uiteinde van de duikplank duwt of trekt. Die doorbuiging is meetbaar op vele verschillende manieren: bijvoorbeeld door de verandering in de weerstand te meten van een rekstrookje dat op de duikplank is aangebracht of door de verandering in elektrische capaciteit te meten tussen de duikplank en een nabijgelegen elektrode. Een bijzonder nauwkeurige positiemeting is mogelijk door een laserstraal te laten weerkaatsen aan het uiteinde van de duikplank en dan de intensiteit van de laserstraal te detecteren met twee lichtgevoelige sensoren, de fotodetectoren. Het verschil tussen de hoeveelheid licht op de bovenste en op de on-

derste detector is een maat voor de doorbuiging, want als de duikplank doorbuigt, komt de laserstraal op een

Tjerk Oosterkamp is hoogleraar experimentele natuurkunde aan de Universiteit Leiden. Hij houdt zich bezig met microscopie en de grondslagen van de quantummechanica en onderzoekt of het met behulp van een gevoelige krachtsensor in de toekomst mogelijk zal zijn om een MRI-scan te maken van een eiwit in een celmembraan. Deze gevoelige krachtsensor is mogelijk ook geschikt om te onderzoeken of de quantummechanische beschrijving ophoudt te werken voor grote objecten.

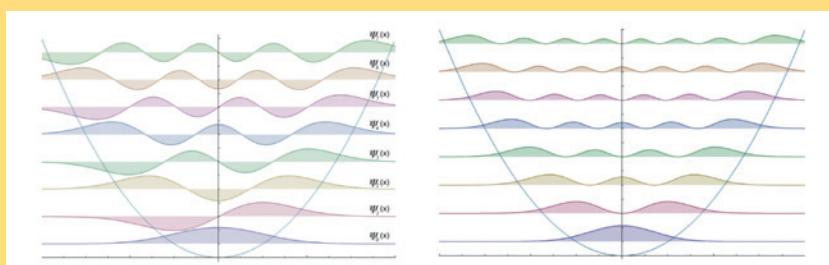


Oosterkamp@Physics.LeidenUniv.nl

# Quantisatie in een mechanische resonator?

De quantummechanica geeft een beschrijving waarin de kans om de duikplank op deze plaats of juist op een andere plaats aan te treffen, beschreven wordt door Schrödinger's golfvergelijking. Een belangrijk ingrediënt daarin is de potentiële energie die in het geval van een veer gegeven wordt door de parabol in figuur 1:  $E_{pot} = \frac{1}{2} k x^2$ . De oplossingen  $\psi_n$  van deze vergelijking worden grafisch weergegeven in de linker helft van figuur 1. In de rechter helft van figuur 1 wordt de kans om de duikplank op een zekere positie aan te treffen, weergegeven door  $P(x) = |\psi(x)|^2$ . Zo is te zien dat, wanneer de duikplank helemaal in zijn rusttoestand is en zijn positie gemeten zou worden, de duikplank dan weliswaar met enige waarschijnlijkheid op  $x=0$  zou worden aangevonden, maar dat hij ook vaak in de onmiddellijke nabijheid daarvan te vinden zal zijn. Omdat de potentiële energie daar groter is dan nul,  $E_{pot} = \frac{1}{2} k x^2$ , heeft dit tot gevolg dat de energie van de grondtoestand van de duikplank een waarde heeft die iets groter dan nul is:  $E_{min} = \frac{1}{2} h f$  en de gemiddelde uitwijking die de resonator heeft is  $x_{ZPM} = \sqrt{\hbar/(4\pi m f_{dp})}$ . Hierbij staat het subscript ZPM voor zero-point motion, oftewel nul-

puntsbeweging. De energie van de resonator neemt verder toe met stappen van  $E_{quantum} = h f$ . Dat dezelfde quantisatieregel die we zien bij de quantisatie van de energie van het foton, maar nu voor de frequentie waarmee de duikplank op en neer trilt:  $f_{dp} = 1/2 \pi \sqrt{k/m}$  waarin  $k$  en  $m$  respectievelijk de veerconstante en de massa van de duikplank zijn. De resonantiefrequentie van de duikplank zal tussen een paar kHz en een paar GHz liggen. Voor typische systemen varieert de  $x_{ZPM}$  tussen  $10^{-20}$  m en  $10^{-15}$  m. Het is daarbij van groot belang dat de fotonen die gebruikt worden voor de meting van de beweging van de sensor deze niet in beweging brengen.



**Figuur 1** Schematische weergave van de quantummechanische toestanden van een mechanische resonator. De potentiële energie van een massa veersysteem met veerconstante  $k$  wordt gegeven door  $E = \frac{1}{2} k x^2$  (de parabol in de figuur). De golffuncties  $\psi$  weer, die oplossingen zijn van de Schrödinger-golfvergelijking. De golffuncties in de rechter figuur komen overeen met het kwadraat van de golffuncties in de linkerfiguur en geven de kans weer om een mechanische resonator op een bepaalde positie aan te treffen.

andere plek op de twee fotodetectoren terecht.

Dit soort duikplanken wordt in de praktijk veelvuldig gebruikt in de atoomkrachtmicroscopie (AFM) en de doorbuiging van de duikplank maakt het mogelijk om de kracht te meten tussen een scherpe naald die aan de duikplank vast zit en een oppervlak dat in kaart gebracht moet worden. In die context is de detectievoeligheid in de afgelopen jaren geoptimaliseerd. De nauwkeurigheid waarmee de verplaatsing van de duikplank gemeten kan worden, is afhankelijk van de tijdsduur van de meting; binnen een microseconde tot op enkele picometers nauwkeurig ( $1 \text{ pm} = 10^{-12} \text{ m}$ , veel minder dan de afmeting van een atoom:  $100\text{-}200 \text{ pm}$ ) en ruim voldoende om de thermische beweging van de duikplank waar te nemen [1]. Die onnauwkeurigheid heeft een fundamentele oorzaak: omdat licht bestaat uit afzonderlijke deeltjes (lichtquanta of fotonen) varieert de intensiteit van een laserstraal voortdurend een klein beetje.

Er zijn twee dingen mogelijk om de beweging van de duikplank nog nauwkeuriger te detecteren. Allereerst kun je een krachtiger laserstraal gebruiken, maar de duikplank wordt daar al gauw te warm van en bovendien oefent die laserstraal ook een kracht uit op de resonator. En vanwege de eerder genoemde fundamentele fluctuaties in het vermogen van een laserstraal is dat een ruisoorzaak. Verstandiger is het om het experiment zo in te richten dat de laserstraal meerdere keren tussen een vaste spiegel en de duikplank heen en weer kaatst. Wanneer je de laserstraal  $F$  keer heen en weer kunt laten kaatsen zonder dat de lichtsterkte afneemt door absorptie in de spiegels kun je de positie ook een factor  $F$  nauwkeuriger waarnemen.

Daarmee komt een nieuw soort experimenten binnen bereik, dat een heel andere vraag onderzoekt: Wat gebeurt er wanneer je een mechanische sensor zo nauwkeurig kunt uitlezen dat het golfgedrag van de sensor zelf op zou kunnen gaan spelen?

In 2003 kwam Dirk Bouwmeester met

een voorstel [2] voor een concreet experiment dat voor velen geldt als de start van dit nieuwe onderzoeksgebied. Gemotiveerd door een eerder idee van Penrose [3,4], ontwierp hij een experiment waarmee het in principe mogelijk zou zijn om met de huidige technologie de beweging van een mechanische resonator tot op de nulpuntsbeweging waar te nemen en een resonator in een superpositie te brengen. Op dat moment was het niet duidelijk of een dergelijk experiment eigenlijk wel kans van slagen zou hebben. Omdat een duikplank is opgebouwd uit atomen én omdat we graag de quantummechanica serieus zouden willen blijven nemen, zou iedere duikplank ook in een superpositie moeten kunnen blijven bestaan. Maar wat zorgt er dan voor dat het klassieke meetapparaat, dat niet veel van onze duikplank verschilt, een einde maakt aan de superposities? De ervaringen in onze laboratoria en daarbuiten bieden immers weinig aanknopingspunten om te geloven in parallelle universa en ook niet in meetinstrumenten die lang

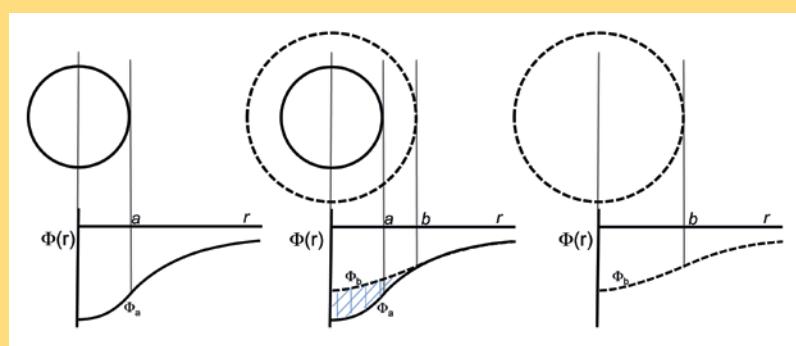
## Quantummechanica zonder eenduidige klok of assenstelsel

De Schrödinger vergelijking is een differentiaalvergelijking waarin zowel afgeleiden naar de plaats als naar de tijd voorkomen. In figuur 2 staat links een bol met een kleine straal en rechts een bol met een grote straal. Beide bollen hebben een even grote massa. In feite is de ene bol een opgerekte versie van de andere. Bij de plaatjes is de bijbehorende gravitationele potentiaal getekend. Deze potentiaal is verantwoordelijk voor de vervorming van de ruimte en zorgt er ook voor dat klokken niet overal gelijk lopen. Net zo goed als dat het effect van algemene relativiteit op klokken moet worden meegenomen om het GPS-systeem te laten functioneren, zal dit ook voor de quantummechanica gelden. Belangrijk is dat in deze situaties (de linker en de rechter bol maar ook in de GPS-satellieten rondom de aarde) de plaats en de tijd wel eenduidig gedefinieerd zijn. De quantummechanica of de quantumveldentheorie zouden op zich nog wel met een ruimte-tijd die op één manier gekromd is overweg kunnen. Maar de problemen, die wat mij betreft een nieuw regime van de quantummechanica inhouden, beginnen wanneer we een superpositie van beide bollen maken. In de middelste toestand in figuur 2 wordt een superpositie van de bol weergegeven. Welke klok en welke kromming moet dan gebruikt worden voor de golfvergelijking? En is die kromming hetzelfde als de superpositie bestaat uit 99% van de linker bol en 1% van de rechter bol, of als de superpositie uit een 50%-50% of 1%-99% verdeling bestaat? Referentie [7] probeert voor te rekenen hoe

208

groot dit probleem in de praktijk uit zou kunnen pakken. Omdat het probleem tussen quantummechanica en de algemene relativiteit op de niet-relativistische schaal van mechanische resonatoren, die immers veel langzamer bewegen dan de lichtsnelheid, niet voor zichzelf spreekt, krijg ik vaak de volgende tegenvraag. Men zegt dan: "Tjerk, we hebben toch ook geen problemen om een superpositie van twee elektrische velden te beschrijven in de quantummechanica? Je moet gewoon elk deel van de superpositie afzonderlijk bekijken. Waarom begin je niet met nadenken over twee geladen bollen die in een superpositie zijn? Als je die situatie begrijpt, dan wordt vast ook duidelijk wat je met zwaartekracht aan moet. Bovendien zijn de elektrische krachten veel groter dan de zwaartekracht en als de elektrische krachten niet tot problemen leiden dan de zwaartekracht toch ook zeker niet." Deze tegenwerping beantwoorden blijkt moeilijk omdat de constatering dat de zwaartekracht geen kracht is maar een vervorming van de ruimte, niet voldoende concreet is of voor zichzelf spreekt. Sinds kort probeer ik deze tegenwerping op een andere manier te beantwoorden. Een uniform geladen bol in een superpositie (van een toestand met grote straal en één met kleine straal) geeft inderdaad zonder enige problemen aanleiding tot een superpositie van elektrische velden buiten de bol. De problemen met de quantummechanica spelen echter ook op in het geval van de elektrisch geladen bollen, wanneer we in rekening proberen te brengen dat de energiedichtheid, die samen gaat met het elektrische veld, leidt tot een vervorming van de ruimte en de tijd.

Omdat de vervorming voor twee verschillende stralen van de geladen bol verschillend is, leidt dat tot een nieuw probleem. Tegelijk wordt ook duidelijk waarom een superpositie van een massaloze geladen bol veel minder problematisch is dan een superpositie van een massieve bol: de energiedichtheid van een massieve bol komt voort uit  $E=mc^2$  en is daarmee vele malen groter dan de energiedichtheid van een elektrisch veld.



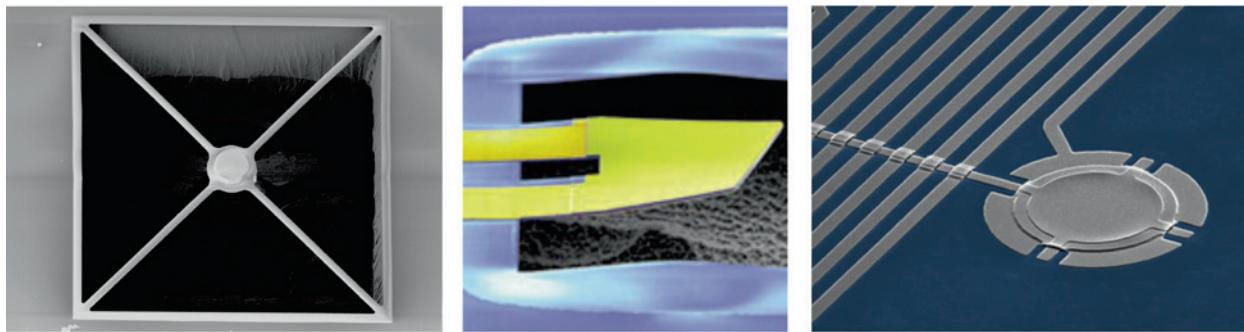
**Figuur 2** Een manier om de discrepantie tussen algemene relativiteit en de quantummechanica te illustreren. De linker en rechter bol hebben elk een eenduidige gravitationele potentiaal. Een bol in superpositie van twee toestanden met verschillende stralen heeft een gravitationele potentiaal die slecht is gedefinieerd, zoals aangegeven met de arcering. Daarmee worden plaats en tijd problematische begrippen.

in superpositie blijven. Met metingen aan mechanische resonatoren zou een lang gekoesterde wens in vervulling gaan om het grensvlak te verkennen tussen de quantumwereld van atomen en de klassieke wereld van tafels en stoelen die niet in superpositie lijken voor te komen (zie kader Quantisatie in een mechanische resonator?).

De metingen die in de afgelopen vijf

jaar uit deze tak van de natuurkunde zijn voortgekomen, laten zien dat het inderdaad technisch mogelijk is om resonatoren (al dan niet in de vorm van een duikplank, zie figuur 3) te koelen tot hun quantumgrondtoestand en vervolgens zelfs in superpositie te brengen, zoals een goed quantumssysteem betaamt [5,6]. Deze experimenten, die laten zien dat ook

dergelijke grote mechanische objecten (typisch zo'n 100 nm dik en tientallen micrometers groot) zich als quantumssystemen kunnen gedragen, zouden in de toekomst belangrijke technologische implicaties kunnen hebben. Mechanische systemen kunnen door allerlei verschillende quantumssystemen in beweging gebracht worden en dat maakt ze geschikt om



**Figuur 3** Verschillende mechanische resonatoren die gebruikt worden in quantummechanische experimenten. De foto links toont een spiegelje op een slappe mechanische resonator in de vorm van een X, zoals ze in de groep van Bouwmeester worden gebruikt. De interactie met een enkel foton moet in de toekomst voldoende zijn om deze resonator meetbaar in beweging te brengen. In het midden de piezo-elektrische resonator die door Cleland en Martinis werd gekoppeld aan een supergeleidende qubit en door manipulaties van de supergeleidende qubit gedurende enkele nanoseconden in superpositie gebracht kon worden [6]. Rechts een rond trommelvel van aluminium dat door de groep van Teufel bij NIST tot de quantumgrondtoestand gekoeld kon worden doordat het trommelvel onderdeel was een condensator. Linksboven in de foto zijn tien windingen te zien van de spiraalvormige inductor die samen met de condensator een LC-circuit vormt. Deze structuren zijn enkele tientallen micrometers groot en ongeveer 100 nm dik. Met andere woorden, meer dan 100.000 bij 100.000 atomen en ongeveer 1000 atomen dik.

quantumsystemen van verschillende soort aan elkaar te koppelen.

Nu het eenmaal gelukt is om van diverse mechanische resonatoren aan te tonen dat ze wel degelijk quantumgedrag vertonen, is het misschien ook mogelijk om experimenten te doen die licht werpen op het quantummeetprobleem: waar ligt de overgang van quantum naar klassiek, wat maakt een detector tot een klassiek systeem?

Het idee van Penrose, dat aanleiding was tot het experiment dat Bouwmeester voorstelde, is dat de quantummechanica aangepast zal moeten worden als gevolg van de kromming van de ruimte, wanneer superposities van zware objecten aan de orde zijn. Het komt voort uit het besef dat de algemene relativiteitstheorie voorzcrijft dat ruimte en tijd gekromd raken door een massa, maar dat we niet weten hoe de ruimte gekromd wordt op het moment dat er sprake is van een superpositie van een massa die zich op meerdere plaatsen tegelijk bevindt. Dat de kromming van de ruimte leidt tot problemen op de allerkleinste lengteschalen (Planckschaal) en de allerhoogste energieschalen is aanleiding voor veel studie. Op de Planckschaal kunnen elementaire deeltjes, ondanks hun geringe massa, toch zo'n grote kromming van de ruimte te weeg brengen dat ze zelf een zwart gat gaan vormen.

Penrose [3,4] maakt duidelijk dat de problemen tussen algemene relativiteit en quantummechanica ook spelen bij een superpositie van een macroscopisch object dat verre blijft van de singulariteit van een zwart gat.

Hij doet dat door een dimensionele analyse die een energiemaat oplevert die de onzekerheid beschrijft in de energie van twee verschillend gekromde ruimtes.

Recentelijk lieten Oosterkamp en Zaanen [7] zien dat een resultaat zoals gegeven wordt door de dimensionele analyse van Penrose, ook kan worden gevonden door elk atoom dat deelneemt in de superpositie een eigen klok toe te kennen, omdat de algemene relativiteit nu eenmaal de tijd op elke atomaire positie anders doet tikken (zie kader Quantummechanica zonder éénduidige klok of assenstelsel). Zij benoemen het probleem dat, voor een atoom dat deelneemt in een superpositie van een zwaar object, het niet duidelijk is welk van de twee klokken de juiste tijd aangeeft. Wanneer ervan uitgegaan mag worden dat de onzekerheden van ieder afzonderlijk atoom in zekere zin bij elkaar kunnen worden opgeteld, valt uit te rekenen na hoeveel tijd dit een serieus probleem zou kunnen gaan worden.

Hierover theoretiseren blijft op z'n zachtst gezegd problematisch, omdat een theorie ontbreekt die quantummechanica en algemene relativiteit combineert. Maar met behulp van bovenstaande redeneringen is wel af te schatten dat grote mechanische resonatoren zoals die nu in experimenten gebruikt worden, door de dubbelzinnigheid van de kromming van de ruimte-tijd, niet lang in een superpositie kunnen blijven bestaan.

Dit soort concrete voorspellingen zijn een drijfveer voor het doen van nieuwe experimenten. Mogelijk kunnen het

soort experimenten, waar Bouwmeester de aanzet toe gaf, in de toekomst een antwoord geven op de vraag of zwaartekracht verantwoordelijk kan worden gehouden voor het instorten van de golffunctie tijdens het doen van een meting.

In elk geval verwacht ik dat we in de komende jaren vaker zullen gaan horen dat niet alleen binnen hoge-energiefysica of de fysica van zwarte gaten, maar ook voor het begrijpen van experimenten met mechanische resonatoren in quantumsuperpositie, een geünificeerde theorie van algemene relativiteit en quantummechanica nodig zal zijn.

## Referenties

- 1 C. A. J. Putman, B. G. De Groot, N. F. Van Hulst en J. Greve, *A detailed analysis of the optical beam deflection technique for use in atomic force microscopy*, *J. Appl. Phys.* **72** (1), 1 July 1992, os.tnw.utwente.nl/publications/pdf/3.pdf.
- 2 W. Marshall, C. Simon, R. Penrose en D. Bouwmeester, *Towards quantum superpositions of a mirror*, *Phys. Rev. Lett.* **13401**, (2003).
- 3 R. Penrose, *Gen. Rel. Grav.* **28**, 581, (1996).
- 4 R. Penrose, *Phil. Trans. R. Soc. Lond. A* **356**, 1927, (1998).
- 5 A.D. O'Connell, M. Hofheinz, M. Ansmann, R.C. Bialczak, M. Lenander, E. Lucero, M. Neeley, D. Sank, H. Wang, M. Weides, J. Wenner, J.M. Martinis en A.N. Cleland, *Quantum ground state and single-phonon control of a mechanical resonator*, *Nature* **464**, 697-703 (2010).
- 6 J.D. Teufel, T. Donner, Dale Li, J.W. Harlow, M.S. Allman, K. Cicak, A.J. Sirois, J.D. Whittaker, K.W. Lehnert en R.W. Simmonds. *Sideband cooling of micromechanical motion to the quantum ground state*. *Nature* (2011).
- 7 T.H. Oosterkamp en J. Zaanen, arXiv:1401.0176 [quant-ph].



# QuTech: samen bouwen aan een quantumcomputer

## Interview met Leo Kouwenhoven

**Op 1 januari jongstleden opende in Delft het QuTech-instituut zijn deuren. Dit instituut houdt zich bezig met quantuminformatie en quantumcomputing. De onlangs geridderde Leo Kouwenhoven, die twee jaar geleden nog veel aandacht kreeg omdat zijn team het Majoranadeeltje vond, is de directeur van het nieuwe instituut.** Marieke de Boer

210

**D**e eerste keer dat Leo Kouwenhoven over de mogelijkheid van een quantumcomputer hoorde, was hij nog sceptisch. “Dat was in 1998. Hans Mooij, bij wie ik gepromoveerd ben, kwam destijds terug van een reis naar Santa Barbara waar hij over quantumcomputers had geleerd. Hij wilde er meteen aan gaan

werken. Ik was echter geen *early adopter*. Twee jaar later ben ik op sabbatical gegaan naar Harvard en had wat meer tijd om na te denken. Toen ik terugkwam ben ik zelf ook onderzoek op het gebied van quantumcomputers gaan doen. Sabbaticals kunnen best nuttig zijn. In 2010 heb ik een halfjaar in New York gezeten en toen ben ik in

aanraking gekomen met Majorana’s. Daarvoor wist ik er echt helemaal niets van. Nou ja, ik had er wel iets over gehoord, maar ik dacht dat het onzin was.”

In zijn kantoor in het natuurkundebouw in Delft, waar Leo Kouwenhoven hoogleraar nanofysica is, vertelt hij over het nieuwe instituut.

### Hoe is QuTech ontstaan?

“In 2012 heb ik samen met Carlo Beenakker en Lieven Vandersypen een ERC Synergy Grant gekregen voor een quantumcomputerlab (QC-lab). Bij mij leefde toen het idee ‘Is dit het of kan er meer?’ Ik ben al een jaar of vijf betrokken bij de planning van Microsoft op het gebied van quantum. Met hen heb ik gesprekken en brainstorms die best wel ver gaan; ze zijn zo concreet mogelijk. Als we het gaan doen, hoeveel kost dat dan? Toen de Synergy Grant kwam, zag ik meer mogelijkheden. Als we dit geld nou gebruiken als wetenschappelijk gedeelte voor een groter programma waarbij we ook de technologie kun-



Leo Kouwenhoven. Foto: Sam Rentmeester.



Het QC-lab in Delft. Foto: Sam Rentmeester.

nen ontwikkelen dan hebben we een heel goede basis om mensen bij elektrotechniek, TNO, wiskunde en informatica te interesseren om mee te doen. Het was voor mij zeker duidelijk dat wij het niet alleen kunnen. We hebben de expertise van de andere disciplines nodig.

Daarna hebben we het idee voor een groter iets, wat uiteindelijk QuTech is gaan heten, op een aantal plekken verteld. Denk daarbij aan het College van Bestuur van de TU Delft, Techniekstichting STW en het Ministerie van Economische Zaken. Het viel steeds erg goed, het is volgens mij ook een goed verhaal. Topwetenschap met een nieuwe manier van engineering waarbij nieuwe doorbraken te verwachten zijn. Dat daar later een nieuwe industrie uit zou kunnen ontstaan, is voor sommige mensen ook een pluspunt. En door het enthousiasme van de ontvangers zijn we steeds verder gegaan.”

#### Hoe staat het er nu voor?

“Momenteel werken we samen met de afdeling Elektrotechniek hier in Delft en met TNO. We zijn op 1 januari jongstleden begonnen en zijn nu bezig om in detail in te vullen welke thema’s (roadmaps) we willen bestrijken. Dat verdelen we in projecten waarvoor mensen ook al aan het werk zijn. Maar de nadruk ligt nu vooral op planningen maken. We willen de komende jaren nog mensen aantrekken,

in 2018 moeten we op volle sterkte zijn.”

#### Wat is het doel van QuTech?

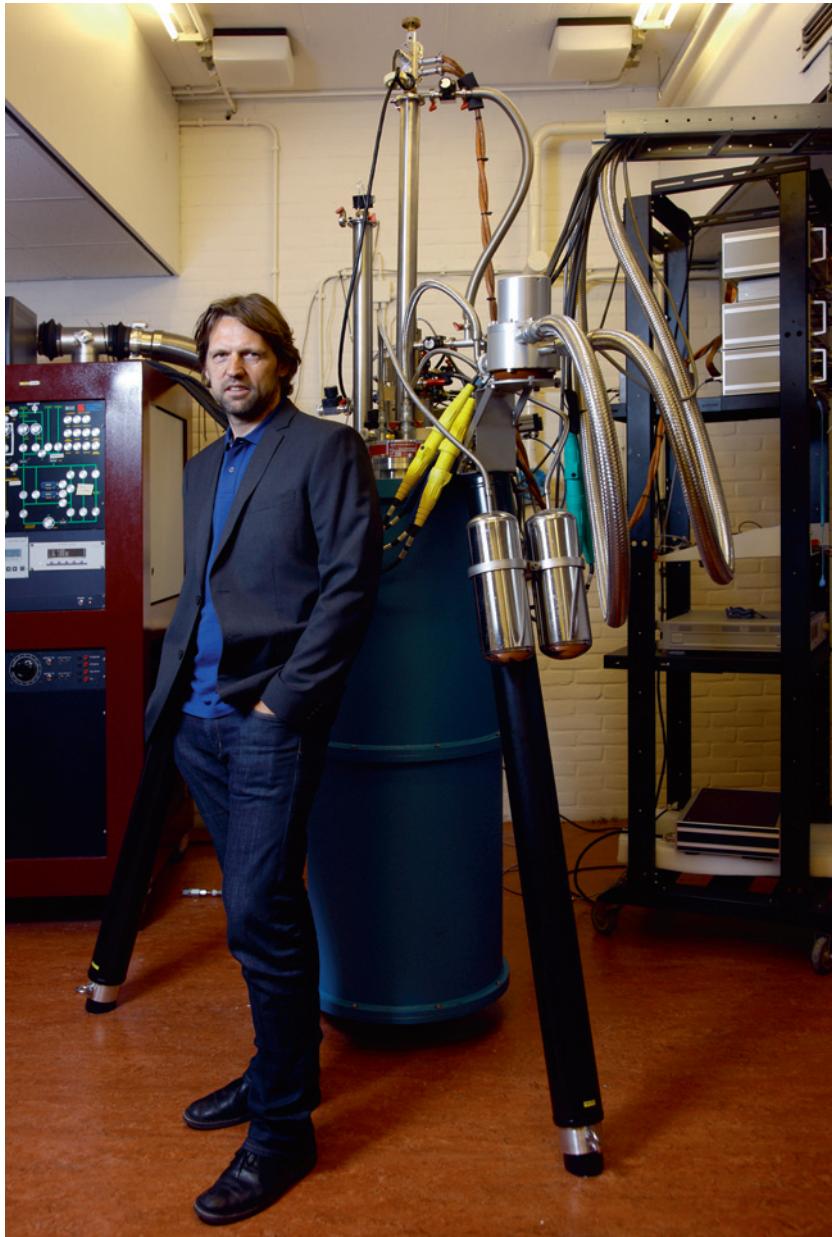
“QuTech is een mission driven instituut, net als bijvoorbeeld Nikhef. Omdat quantum een breed begrip is, hebben we het iets specifieker gemaakt, we moeten superpositie en verstrekking gebruiken. Onze drie basis roadmaps zijn quantumcomputing, topological quantumcomputing en quantuminternet. Voor quantumcomputing is ons doel om over vijf jaar 50 tot 100 qubits met elkaar te verstreken. Bij de tweede roadmap, topological quantumcomputing, maken we gebruik van topologische verschijnselen om het probleem van decoheren- tie kwijt te raken. Anders kunnen we geen grotere circuits maken. Over vijf jaar willen we die topologische qubits behandelen met een braiding gate en ervoor zorgen dat daarbij de beschermingstijd minimaal een seconde is. Quantuminternet, de derde roadmap, codeert alle informatie met verstrek- gelde fotonparen zodat er niet meer gehackt kan worden. Ons doel voor over vijf jaar is een internetsysteem tussen Delft, Leiden en Den Haag. Die afstanden kun je overbruggen met de huidige technologie. Voor nog grotere afstanden moet er eerst een quantumversterker worden uitgevonden. QuTech moet daarnaast ook gaan dienen als een centrum voor een groter ecosysteem. Het QC-lab van de ERC

Synergy is de wetenschappelijke kern, daaromheen komt QuTech met onder andere elektrotechniek en TNO en daarbuiten zit nog een schil met allerlei bedrijven zoals Microsoft en investeringsmaatschappijen. Je moet eens weten hoeveel bedrijven hier al langs zijn geweest. Bijvoorbeeld HP die zijn apparatuur hier kan testen. Bedrijven die mengkoelers maken, Atos en Fox-IT die aan beveiliging doen en het Ministerie van Defensie. Ik ben veel gebeld en gemaaid door mensen van Defensie die iets over quantum willen weten.

We willen ook wat aan educatie doen; de QuTech Academy. Het wordt een online educatiesysteem analoog aan de Khan Academy. En we willen Europa in. We gaan kijken of we internationaal met partners in een groter verband hieraan kunnen werken. QuTech is namelijk niet groot genoeg om het allemaal zelf te kunnen doen.”

#### Wat krijgen de bedrijven in ruil voor hun investering?

“Microsoft wil eigenaar worden van quantumtechnologie. Sommige kleine bedrijven maken gebruik van de fabricagefaciliteiten die wij hebben. En met Leiden Cryogenics willen we samen nieuwe mengkoelmachines ontwikkelen. Nieuwe klanten kunnen dan in Delft komen kijken. Heel wat van hun verkopen gaan via Delft. Er zijn voor alle bedrijven wel win-win-situaties te verzinnen.”



**Leo Kouwenhoven.** Foto: Sam Rentmeester.

Zijn er wereldwijd nog andere groepen die ook een quantumcomputer bouwen?

"Jazeker. In Noord-Amerika is IBM daar behoorlijk serieus mee bezig. Ze maken ook hardware, ze hebben dezelfde aanpak als wat wij voor de quantumcomputer doen. Dus dat is direct vergelijkbaar met ons werk. Dan zijn er bedrijven als Lockheed, Google en NASA. Dat zijn supergrote bedrijven die willen kijken of ze met een quantumcomputer hun problemen kunnen oplossen. Bij Lockheed bijvoorbeeld gaat het om het simuleren van nieuwe vliegtuigen en bij Google om het verwerken van big data. In Canada bij Waterloo zijn door de oprichters van Blackberry drie instituten gebouwd. Daar willen ze een soort Brainport Eindhoven of Silicon Valley-regio maken maar dan voor quantum.

In Europa wordt er in Engeland en in Zwitserland aan gewerkt. Verder heeft China een quantumsatelliet en in Rusland zijn er verschillende labs gebouwd. Daar lopen ze nog ver achter maar ze hebben er wel een hoop geld tegenaan gegooid. En dan hebben we natuurlijk nog de NSA."

Ik kan me voorstellen dat er minder dan bij ander onderzoek wordt samengewerkt omdat er bedrijven bij betrokken zijn?

"Iedereen realiseert zich nog steeds dat het nu nog heel veel wetenschap is. Het heeft nog weinig zin om veel te patenteren, want dat geeft geen winst. Tot nu toe is iedereen nog heel open, maar dat gaat een keer veranderen. Microsoft vindt het prima als er gepubliceerd wordt. Je mag ook details publiceren, als zij maar het recept in

huis hebben. Ook als je een publicatie schrijft met veel details, dan zit daar nog lang niet voldoende informatie in om het ook daadwerkelijk na te doen."

Wanneer kunnen we de eerste quantumcomputer verwachten?

"In 2025 hebben we een slechte versie, in 2030 is er een versie die dingen kan die klassieke computers echt niet meer kunnen."

Wat kunnen we met een quantumcomputer? In de media werd bij de opening van QuTech vooral benadrukt dat een quantumcomputer kan berekenen welke medicijnen een mens nodig heeft. Aan welke toepassingen denken jullie?

"De grootste uitdaging is een algoritme te verzinnen dat we nog niet kennen, waarmee je dingen kunt doen die we nu nog niet kunnen. Dat is echt voor de softwaremensen, dus ook voor Microsoft. Zij hebben het probleem in drieën gesplitst: de meer klassieke technologie, een algoritme en het derde zijn wij. Bij toepassingen kun je bijvoorbeeld denken aan cryptografie, maar voor ons is het belangrijkste het berekenen van chemische reacties en materialen. En om dat populair te maken wordt het medicijnvoorbeld gebruikt. De meeste mensen weten niet dat het lichaam een grote chemische fabriek is. Ze zijn stomverbaasd als ze horen dat er atoomkernen in je lichaam zitten."

Wat wil je de komende jaren zelf nog onderzoeken?

"Ik wil graag Majoranadeeltjes in echte quantumcircuits zien te krijgen en dan kijken hoe ze zich gedragen."

Vol trots laat Leo Kouwenhoven aan het einde van het interview het QC-lab zien. Beneden in het natuurkundengebouw van de TU Delft staat de apparatuur waarmee het onderzoek verricht wordt. Grote cryostaten zorgen ervoor dat qubits bij extreem lage temperaturen getest kunnen worden. Kabels gaan door gaten in het plafond en verbinden de apparatuur beneden met de computers boven die de analyses uitvoeren. Over een jaar of twee zal QuTech bij de renovatie van het gebouw een eigen vleugel krijgen. De nieuwe vleugel grenst aan het TNO-gebouw, dus je kunt zo door lopen. Ook elektrotechniek is op 50 meter afstand.



# 50 inzichten quantumphysica

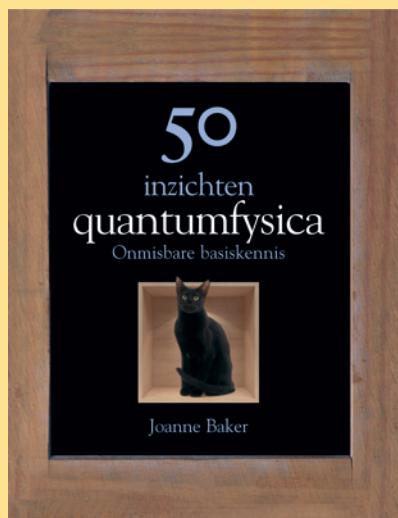
Ontdekkingen en voorspellingen kunnen op waarde geschat worden als ze bezien worden in het tijdsgewricht waarin ze gedaan werden. Het belang ervan kan worden afgemeten aan de (nieuwe) ontwikkelingen die ze in gang gezet hebben. In *50 inzichten quantumphysica*, een boek uit een serie waarin ook *50 inzichten natuurkunde*, *50 inzichten universum* en *50 inzichten aarde* zijn verschenen, worden de ontdekkingen en nieuwe ontwikkelingen in de quantumphysica besproken. In vijftig hoofdstukken worden we chronologisch geleid langs de fundamentele quantumfysische ontdekkingen, het Standaardmodel en moderne praktische toepassingen.

Eerst wordt onder andere het werk van fysici als Young, Maxwell, Michelson en Morley besproken, dat in 1901 uitmondt in de introductie van energie-quanta door Planck, die daarmee het startsein geeft voor de ontwikkeling van de quantumphysica. In de hoofdstukken die volgen komen onderwerpen zoals dualiteit, Fraunhoferlijnen, het Zeeman-effect en het uitsluitings-principe van Pauli aan bod. De hoofdstukken over Matrixmechanica, Schrödinger's golfvergelijking, het onzekerheidsprincipe van Heisenberg, de Kopenhagen-interpretatie, de kat van Schrödinger en de EPR-paradox laten een mooi beeld zien van de grote fysici van rond 1930, Einstein, Bohr, Heisenberg en Schrödinger, die in twee kampen verdeeld raakten over de grondslagen van quantumgedrag. De tien hoofdstukken die dan volgen beschrijven de ontdekkingen die leidden tot het Standaardmodel, waarbij onder andere quantumveldentheorie, quarks, quantumelektrodynamica,

quantumchromodynamica en het concept van quantumtunnelen worden besproken. Onder het kopje De quantumkosmos komen onderwerpen als het higgsdeeltje, quantumzaartekracht, Hawkingstraling en snaartheorie aan bod. Aan het eind van het boek worden meer moderne onderwerpen besproken die nauw aansluiten bij de inhoud van dit themanummer en die in het boek onder de noemer quantumtoepassingen vallen: quantumdecoherentie, qubits, quantumcryptografie en quantumdots. Het boek is geschikt voor iedereen die geïnteresseerd is in hoe de quantum-

physica zich ontwikkelt en tot welke ontdekkingen dat geleid heeft. Hier voor is basiskennis op het gebied van de quantumphysica voldoende. Om de implicaties van bepaalde ontwikkelingen goed te kunnen beoordelen, is basiskennis alleen niet meer voldoende. Achter op het boek is weliswaar geschreven: "50 inzichten quantumphysica ontdoet het meest ongrijpbare wetenschappelijke vakgebied van zijn raadselen". Dat is zeker niet gelukt in alle vijftig hoofdstukken. Hoe zou dat ook kunnen, als de auteur, Joanne Baker, redacteur bij *Nature*, vanwege het formaat maar vier pagina's per hoofdstuk ter beschikking had. Dat is voor onderwerpen zoals snaartheorie, Bellongelijkheden, quantumcryptografie en quantumbewustzijn ook (bijna?) onmogelijk. Wat haar wel goed gelukt is, is de samenhang van de verschillende ontwikkelingen en doorbraken weer te geven. Dit komt onder andere door de opbouw van ieder hoofdstuk. Zo staat er op de eerste twee pagina's van ieder hoofdstuk een tijdlijn met de meest relevante ontwikkelingen voor het betreffende onderwerp. Ook worden er markante uitspraken en een korte levensloop van de meest belangrijke hoofdrolspelers gegeven. Op die manier is het een zeer leesbaar boek geworden. De vele verschillende onderwerpen die besproken worden in dit boek, kunnen een welkomte aanvulling zijn op de onderwerpen die aan bod komen in het themanummer dat u voor u heeft.

Richard Engeln



**50 inzichten quantumphysica**

Joanne Baker

Veen Media, 2014

ISBN 9789085714439

208 bladzijden

€24,99

Heeft u ook een boek gelezen dat interessant is voor de lezers van het NTvN? En wilt u hierover een recensie schrijven? Neem dan contact op met de redactie ([ntvn@ntvn.nl](mailto:ntvn@ntvn.nl)).

# Magnetische roosters van koude atomen als quantumsimulatoren

We creëren tweedimensionale roosters van ultrakoude atomen, vastgehouden boven een chip, door patronen te etsen in een dunne laag gemagnetiseerd materiaal. Om quantumsimulatie te realiseren willen we interacties induceren door hooggeëxciteerde Rydbergniveaus aan te slaan. Anderzijds willen we ook roosters met een zodanig kleine roosterafstand realiseren dat interactie tot stand komt via sterke quantumtunneling.

Arthur L. La Rooij en Robert J.C. Spreeuw

214

## Feynmans visie

De quantummechanica lijkt in begin-sel bruikbare recepten te bieden om van een microscopisch systeem de mogelijke energietoestanden te berekenen of de evolutie in de tijd te volgen. In 1982 signaleerde Richard Feynman dat deze recepten in de praktijk toch niet zo bruikbaar zijn, met name als we te maken hebben met veeldeeltjes-systeem [1]. Hij liet onder meer zien hoeveel ruimte in het geheugen van een klassieke computer nodig is om een veeldeeltjes-quantumtoestand zelfs maar te representeren. Het probleem is dat deze benodigde ruimte exponentieel toeneemt met het aantal quantumdeel-tjes. Als het toevoegen van een enkel

deeltje bijvoorbeeld tot verdubbeling van de benodigde resources ('hulpbronnen') leidt, is zelfs de grootste super-computer al snel niet meer toereikend. Feynman stelde daarom voor om een quantum-systeem te simuleren door een ander quantum-systeem of quantumcomputer. Op het eerste gezicht lijkt het weinig zinvol om het ene quantum-systeem in te ruilen voor het andere. Toch kan dit grote winst betekenen als de simulator toegankelijk is voor metingen en parameters naar believen kunnen worden aangepast.

## Roosters van neutrale atomen

Roosters van koude, neutrale atomen lenen zich uitstekend voor de implementatie van quantum-simulatoren, van bijvoorbeeld modellen uit de vaste stof. Een doorbraak was de demonstratie van een quantumfaseovergang tussen een Mottisolator en een supergeleider [2]. Dit experiment kan worden gezien als een quantum-simulatie van het Bose-Hubbard-model (zie kader Quantumdeeltjes op een rooster).

Een andere grote klasse van modellen bestaat uit roosters van

effectieve spins, met twee toestanden ('op' en 'neer'), die op een toestandsafhankelijke manier wisselwerken met hun naaste buren. De bekendste varianten zijn de Ising- en Heisenberg-modellen. Quantum-simulatoren zouden meer licht kunnen werpen op problemen als quantum-magnetisme of hoge-T<sub>c</sub>-supergeleiding.

In de meest gangbare methode worden atomen vastgehouden in een optisch rooster, het regelmatige patroon van knopen of buiken in een interfertiepatroon van laserbundels. In Amsterdam hebben we echter een

Arthur La Rooij studeerde in 2012 af als master in de theoretische natuurkunde aan de Universiteit van Amsterdam. Sindsdien doet hij zijn promotie-onderzoek aan het Van der Waals-Zeeman Instituut voor experimentele natuurkunde, eveneens aan de Universiteit van Amsterdam.



Robert Spreeuw studeerde en promoveerde (1991) aan de Leidse Universiteit op een onderwerp in de quantum-optica. Na postdocperiodes aan NIST (Gaithersburg, VS) en in Konstanz kwam hij naar Amsterdam. Aanvankelijk met een KNAW fellowship startte hij hier onderzoek met koude atomen nabij oppervlakken en in het bijzonder op magnetische-film atoom-chips, gemotiveerd vanuit een interesse in quantum-informatie en simulatie.



R.J.C.Spreeuw@uva.nl

# Quantumdeeltjes op een rooster

Atomen in optische of magnetische roosters en elektronen in een eenvoudig kristal worden vaak beschreven met behulp van het Hubbardmodel. Voor bosonen:

$$H = -J \sum_{\langle ij \rangle} a_i^\dagger a_j + \frac{U}{2} \sum_i a_i^\dagger a_i^\dagger a_i a_i$$

In deze Hamiltoniaan beschrijft  $J$  de tunnelamplitude voor deeltjes van plek  $j$  naar plek  $i$  en is  $U$  (meestal  $U > 0$ ) de interactie-energie van deeltjes op dezelfde plek. Als  $U \gg J$  zullen deeltjes zich zoveel mogelijk verspreiden over verschillende posities en wordt tunnelbeweging onderdrukt.

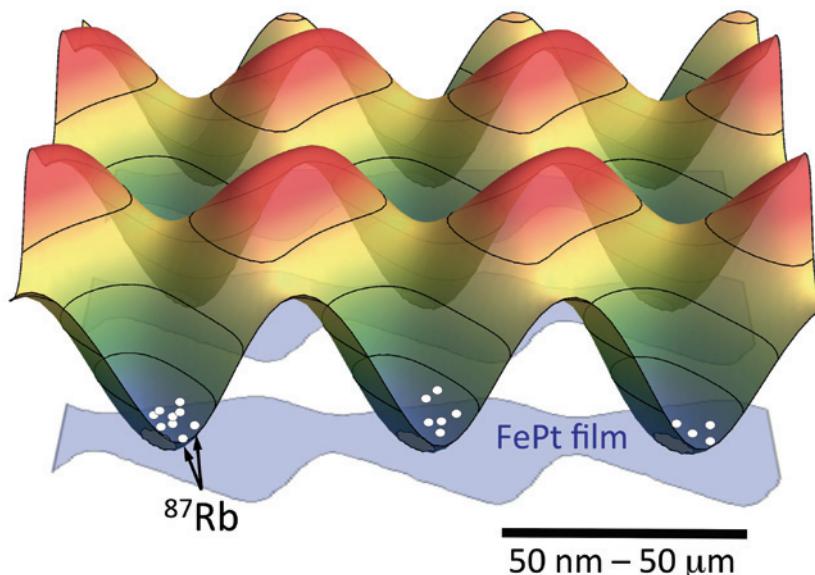
Deze toestand is analoog met een isolator waarin elektronen vast zitten op een roosterpunt omdat als ze bewegen de totale energie toeneemt. Als daarentegen  $J \gg U$  dan gaan alle deeltjes tunnelen en beschrijft het systeem een (super)fluïdum (of geleider).

Een natuurlijke energieschaal om  $J$ ,  $U$ ,  $J^2/U$  in uit te drukken is de *lattice recoil*  $E_r$ , de kinetische energie van een deeltje met een golflengte gelijk aan de roosterconstante. Deze schaalt met de roosterafstand  $d$  als  $E_r \propto 1/d^2$ . Door de roosterafstand te verkleinen kunnen we aldus de Hubbardparameters  $J$  en  $U$  groter maken.

alternatieve methode ontwikkeld om roosters van atomen te maken, die interessante nieuwe mogelijkheden biedt. Deze methode is gebaseerd op lithografisch gedefinieerde structuren op een zogenaamde atoomchip. Atomen zweven in spin-gepolariseerde toestand vlak boven het oppervlak van deze chip. Ze worden daar vastgehouden in lokale minima van een magnetisch veld die fungeren als potentiaalputjes,  $V(r) \propto |B(r)|$ . Deze putjes zijn ongeveer 0,5 mK diep. We houden hierin wolkjes atomen vast bij een temperatuur van 1-10  $\mu\text{K}$ . De chip zelf is gewoon op kamertemperatuur. Het veld wordt gegenereerd door een gemagnetiseerde film die in een speciaal ontworpen patroon is geëtst.

In figuur 1 zien we een patroon dat geoptimaliseerd is voor roosters met vierkante symmetrie, samen met het magnetische potentiaallandschap. Het ontworpen patroon wordt geëtst uit een 200 nm dikke laag van FePt. Na het etsen wordt de laag gemagnetiseerd in de richting loodrecht op het oppervlak. In figuur 2 zien we een afbeelding van enkele honderden kleine wolkjes van koude atomen die vastgehouden worden in een magnetisch rooster. In dit geval zijn een vierkant en een hexagonaal rooster gecombineerd in een interface, als demonstratie van één van de bijzondere mogelijkheden die magnetische chips bieden [3].

In eerdere experimenten hebben we al gedemonstreerd dat we een rooster van honderden wolkjes tegelijk kunnen afkoelen tot de Bose-Einstein-faseovergang. We hebben ook laten zien dat we de atomen over de chip heen en weer kunnen bewegen als in een schuifregister, door externe magnetische velden te variëren [4].



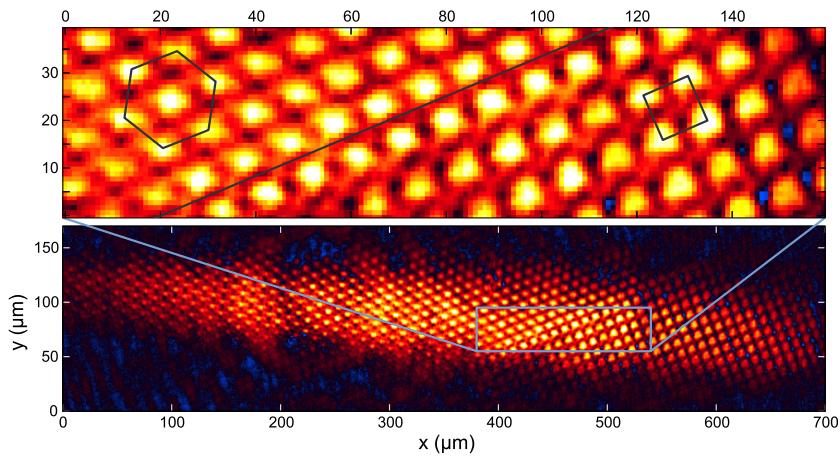
**Figuur 1** In een zig-zagvorm geëtste strips (lichtblauw) van een dunne laag FePt op een atoomchip. De laag is permanent gemagnetiseerd, loodrecht op het oppervlak. Daarboven weergegeven is het resulterende magnetische potentiaallandschap voor spin gepolariseerde atomen. De hoogte van bergen en dalen is evenredig aan de grootte van het magnetische veld  $B$ , berekend op een vaste hoogte van één roosterconstante boven het oppervlak. De witte bolletjes stellen gevangen atomen voor.

Magnetische roosters op atoomchips bieden interessante nieuwe mogelijkheden ten opzichte van optische roosters. De roosterstructuur is bijvoorbeeld zo goed als vrij te kiezen. Verschillende roostersymmetriën kunnen in één ontwerp worden gecombineerd, zoals in figuur 2, of desgewenst kan ook wanorde worden ingebouwd. De roosterconstante kan over een bereik van enkele ordegroottes worden gevarieerd.

In optische roosters is de roosterconstante meestal ongeveer 400 nm, gegeven door de halve golflengte van de gebruikte laser. Daarentegen mikken we met onze magnetische roosters op roosterconstanten die ofwel duidelijk groter, ofwel duidelijk kleiner zijn. Deze twee opties leiden ieder tot een ander type quantum simulator [5].

## Grote roosterafstand met Rydbergwisselwerking

De eerste optie gaat uit van roosters met een roosterafstand van 5-10  $\mu\text{m}$ . Op iedere roosterpositie kan nu een quantumbit (qubit) gedefinieerd worden als coherente superpositie van hyperfijn-subniveaus van de elektronische grondtoestand; voor  $^{87}\text{Rb}$  liggen deze 6,835 GHz uit elkaar. Als we de twee niveaus  $|a\rangle$  en  $|b\rangle$  noemen, wordt de toestand van het qubit dus gegeven door  $\alpha|a\rangle + \beta|b\rangle$ . Dergelijke hyperfijn-qubits in neutrale atomen zijn erg geschikt om quantuminformatie op te slaan omdat in de elektronische grondtoestand de wisselwerking met de omgeving zwak is. De coherente superpositie kan dan potentieel seconden lang in stand blijven. De qubit kan gecodeerd wor-



**Figuur 2** Absorptie-afbeelding van koude rubidiumatomen in een magnetisch rooster. We kijken hier loodrecht op het oppervlak. De atomen zweven ongeveer  $6\text{ }\mu\text{m}$  boven het chipoppervlak. De wolkjes in het centrum van de afbeelding bevatten enkele honderden atomen. In dit geval zijn twee aangrenzende roosterstructuren zichtbaar, vierkant (rechts) en hexagonaal (links).

den in een enkel atoom of ook in een wolkje van tientallen atomen. In het laatste geval wordt  $|a\rangle$  vervangen door een toestand waarbij alle atomen in het wolkje in  $|a\rangle$  zitten, en  $|b\rangle$  door een toestand waarbij precies één atoom in  $|b\rangle$  zit en de rest in  $|a\rangle$ . Dit laatste heet een collectieve excitatie. De keuze voor een roosterafstand van  $5\text{-}10\text{ }\mu\text{m}$  is een balans tussen twee vereisten. 1) De afstand is groot genoeg om naburige roosterposities (en dus qubits) in een optische afbeelding opgelost te kunnen zien. Dit is van belang voor de uitlezing van de qubits, maar ook om individuele qubits te adresseren met een gefocusseerde laserbundel. 2) De afstand is klein genoeg om naburige qubits met elkaar te laten wisselwerken door gebruik te maken van excitatie naar Rydberg niveaus: elektronisch hoog aangeslagen toestanden met hoofdquantumgetal  $50\text{-}100$ . Door hun grote dipoolmoment wisselwerken Rydbergatomen tot wel twaalf ordegroottes sterker dan atomen in de grondtoestand.

Rydbergatomen zijn echter minder geschikt om quantuminformatie te bewaren, omdat ze relatief kort leven. De beoogde oplossing is om de informatie te bewaren in de grondtoestand, maar te bewerken (met gate-operaties) tijdens een kortstondige excitatie naar de Rydbergtoestand. Voor dergelijke gate-operaties bestaan diverse theoretisch uitgewerkte voorstellen die gebaseerd zijn op het verschijnsel dipoolblokkade. Dit komt erop neer dat na laserexcitatie van een Rydbergatoom de verdere Rydbergexcitatie in de directe omgeving wordt

onderdrukt. Deze onderdrukking werkt binnen een afstand die de blokkadestraal genoemd wordt, en meestal ongeveer  $10\text{ }\mu\text{m}$  bedraagt.

Elementaire gates tussen twee individuele atomen, op basis van dipoolblokkade, zijn experimenteel gemonstreerd. Wij verwachten met onze magnetische roosters een schaallbare experimentele aanpak te kunnen ontwikkelen. Een voorstel om dit in het kader van een FOM-programma samen met onderzoekers van de TU Eindhoven aan te pakken is onlangs gehonoreerd.

### De kleinst mogelijke roosterafstand

In de tweede aanpak willen we de roosters omlaag schalen naar roosterafstanden die duidelijk kleiner zijn dan in optische roosters. Een van onze grootste uitdagingen op dit moment is het maken van een rooster met een periode van orde  $100\text{ nm}$ . Deze afstandsschaal, die goed haalbaar is met behulp van elektronenbundellithografie, opent de weg naar quantum simulatie van Hubbardachtige modellen in nieuwe fysische regimes en simulatie van andere, nieuwe systemen.

Veel experimenten die momenteel worden gedaan met optische roosters kunnen straks gedaan worden in kleinere, andere, of zelfs veranderende magnetische roosters. Overigens zijn Rydbergatomen voor dit type roosters niet meer bruikbaar omdat de atomen te dicht (eveneens ongeveer  $100\text{ nm}$ ) bij het oppervlak zitten.

Naarmate de roosterafstand kleiner wordt, zullen de atomen sneller en

verder gaan tunnelen (zie kader *Quantumdeeltjes op een rooster*). In optische roosters tunnelen atomen effectief alleen tussen direct naast elkaar liggende vallen. De dubbele afstand, rond  $800\text{ nm}$ , is te groot. Als we de roosterafstand verkleinen, worden ook hogere orde tunnелеffecten belangrijk, zoals tunnelen over twee posities (direct van  $i$  naar  $i+2$ ), tunnelen van paren (twee atomen van  $i$  naar  $i+1$ ), en superexchange (twee buuratomen wisselen van positie).

Door de afstandsschaal sterk te reduceren worden de energieschalen in het Hubbardmodel een à twee ordegroottes hoger. De thermische energie van de atomen mag dan ook navenant hoger zijn en de bijbehorende temperaturen worden dan eenvoudiger te bereiken. Zo hopen wij een quantumsimulator te bouwen die nog complexere quantumsystemen kan simuleren.

Behalve hogere energieschalen in het Hubbardmodel biedt deze aanpak nog vele andere mogelijkheden. Door zelf de magnetische patronen te schrijven kunnen wij niet alleen de roosterafstand maar ook de geometrie bepalen of deze zelfs langzaam of snel laten variëren, in de plaats (in de ontwerpfasen) of in de tijd (tijdens het experiment). Dit laatste, het dynamisch in de tijd variëren van het potentiaallandschap, kan met behulp van externe magnetvelden. Op die manier kan niet alleen de mate van tunnelbeweging worden vergroot of verkleind (via de hoogte van de tunnelbarrières), maar ook de mate van anisotropie (tunnelen in verschillende richtingen).

Samengevat, met behulp van een magnetische dunne laag vangen we ultrakoude neutrale atomen in een rooster van vallen. Dit biedt een scala aan nieuwe mogelijkheden die verder gaan dan bestaande optische roosters. We verwachten in de komende jaren quantum simulaties van interessante Hamiltonianen te doen. Stap voor stap wordt Feynmans droom werkelijkheid.

### Referenties

- 1 R. P. Feynman, *Int. J. Theor. Phys.* **21**, 467 (1982).
- 2 M. Greiner, et al., *Nature* **415**, 39 (2002).
- 3 V.Y.F. Leung, et al., arXiv:1311.4512 (2013).
- 4 S. Whitlock, R. Gerritsma, T. Fernholz en R. J. C. Spreeuw, *New J. Phys.* **11**, 023021 (2009).
- 5 V.Y.F. Leung, A. Tauschinsky, N.J. van Druten en R.J.C. Spreeuw, *Quantum Inf. Process.* **10**, 955-974 (2011).



## Quantumobjecten



*Quantum Man* van Julian Voss-Andreae.

Kunstenaars die zich laten inspireren door de wetenschap zijn zeldzaam. Een van de weinigen is de Nederlandse theater- en filmmaker Jan van den Berg die gefascineerd is geraakt door de ontdekking van het higgsdeeltje en daarover een film heeft gemaakt en theatervoorstellingen heeft gegeven [1]. Na enig zoeken [2] lukte het om ook in de beeldende kunst een voorbeeld te vinden: de uit Duitsland afkomstige beeldhouwer Julian Voss-Andreae. Een van zijn inspiratiebronnen is de quantummechanica.

Julian Voss-Andreae (1970) is geboren in Hamburg en wilde aanvankelijk schilder worden. Daartoe ging hij naar de kunstacademie in Berlijn maar besloot, na lezing van *The Emperor's New Mind* van Roger Penrose, om natuurkunde te gaan studeren aan de Vrije Universiteit aldaar. In 1999 zette hij deze studie voort aan de Universiteit van Wenen en raakte betrokken bij het werk van Anton Zeilinger aan een diffractie-experiment met  $C_{60}$ -moleculen. Dit experiment liet zien dat zelfs grote moleculen zoals buckminsterfullerenen de wetten van de quantummechanica gehoorzamen [3]. In hetzelfde jaar bezocht hij een workshop in Cortona, Italië, bedoeld voor exacte wetenschappers die geïnteresseerd zijn in de humaniora, kunst en spiritualiteit. Daar maakte hij zijn eerste beeldhouwwerk. Na zijn studie in Wenen emigreerde hij naar Portland, Oregon, in de Verenigde Staten.

In Portland vatte hij zijn oude droom weer op, hoewel hij inmiddels meer geïnteresseerd was geraakt in beeldhouwen dan in schilderen. Hij realiseerde zich dat Linus Pauling uit deze plaats kwam en besloot daarom een beeldhouwwerk te maken dat een van Paulings ontdekkingen zou uitbeelden: een spiraalvormige eiwitstructuur met de naam  $\alpha$ -helix. Dit was het begin van een lange reeks objecten die alle, op de een of andere manier, zijn geïnspireerd op de wetenschap. Bij een aantal objecten is dat de quantummechanica en een ervan heet *Quantum Man*, zie de foto's hierboven. Het object is gemaakt van dunne parallelle platen staal die een lopende man uitbeelden. Afhankelijk van hoe je er naar kijkt, zie je een solide figuur of een bijna doorzichtige schim. De kunstenaar heeft hiermee de golf-deeltjedualiteit willen uitbeelden, waarbij de parallelle platen het golfkarakter moeten voorstellen. Een kort filmpje over zijn werk en foto's van andere objecten, waaronder een *Quantum Woman* en zelfs een combinatie van een man en een vrouw die men voor Alice en Bob zou kunnen aanzien, zijn te vinden op zijn website [www.julianvossandreae.com](http://www.julianvossandreae.com).

Wim Verkley

### Referenties

- 1 M. de Boer, "Voorbij de grenzen van het blote oog en het naakte verstand" - interview met Jan van den Berg, NTvN 79-12 (2013).
- 2 Hierbij werd ik geholpen door Ferry van Geffen die me op de website van Julian Voss-Andreae heeft gewezen. De tekst is gebaseerd op een interview met de kunstenaar in Physics World, november 2006.
- 3 M. Arndt, O. Nairz, J. Voss-Andreae, C. Keller, G. van der Zouw en A. Zeilinger, Wave-particle duality of  $C_{60}$  molecules. Nature, 401, 680-682, 1999.

# Verstengeling: de sleutel tot de veeldeeltjesfysica?

**Verstengeling is de cruciale eigenschap van de quantummechanica die alle revolutionaire quantuminformaticatoepassingen mogelijk maakt. Voor ons begrip van veeldeeltjessystemen is het echter in de eerste plaats een catastrofe. Door de verstengeling explodeert de toestandsruimte voor deze systemen en elke simulatie op een klassieke computer lijkt hierdoor bij voorbaat uitgesloten. Ironisch genoeg blijkt uit recent onderzoek dat precies de verstengeling ons ook naar een oplossing voor dit probleem kan leiden.** Karel Van Acoleyen en Frank Verstraete

218

**W**at onderscheidt onze quantumwereld essentieel van de klassieke wereld zoals men die eind negentiende eeuw voor ogen had? Deze vraag wordt reeds in 1935 beantwoord door Schrödinger in een wondermooi artikel. Hij heeft het niet over het probabilistisch karakter of over de golf-deeltjedualiteit. Neen, volgens Schrödinger is entanglement, letterlijk vertaald: verstengeling, dé karakteristieke eigenschap van de quantummechanica.

In de vroege dagen van de quantummechanica blijft dit fundamentele begrip nog onder de radar, men heeft het te druk met alle succesvolle toepassingen. Dit verandert drastisch in de jaren zestig. John Bell, op dat moment werkzaam als deeltjesfysicus op

CERN, ontdekt dan dat quantumtoestanden voor meer dan één deeltje in principe correlaties kunnen vertonen die onmogelijk te vatten zijn door een klassieke theorie. Verstengeling verschijnt op het voorplan om niet meer te verdwijnen. In eerste instantie wordt het vooral gezien als het cruciale ingrediënt voor revolutionaire quantuminformaticatoepassingen zoals quantumcomputing of cryptografie. Maar gezien haar fundamentele karakter kun je verwachten dat verstengeling uiteindelijk een rol speelt bij elk systeem waar quantumeffecten in het spel zijn. Dit is precies wat de laatste jaren meer en meer duidelijk wordt. Zo is verstengeling zeer belangrijk voor het kwalitatief begrip van allerhande recent ontdekte exotische materialen. Maar even goed vormt het tegenwoordig de leidraad bij het ontrafelen van de mysteries rond zwarte gaten en bij de zoektocht naar een theorie voor quantumgravitatie. In deze bijdrage focussen we op de rol van verstengeling bij zogenoemde quantumveeldeeltjessystemen. Dit is een zeer ruim begrip: zo goed als elk systeem in de natuur valt in feite onder deze noemer. Het

kan hier gaan over een molecuul, opgebouwd uit verschillende atoomkernen en elektronen, maar ook bijvoorbeeld over een metaal met daarin opnieuw vele elektronen. Zelfs het vacuüm – de lege ruimte – is een veeldeeltjessysteem. Inderdaad, vanuit de elementaire deeltjesfysica weten we dat het vacuüm volgestouwd zit met virtuele deeltjes. Het vacuüm is de toestand met laagste energie, de eigenlijke deeltjes die we dan bijvoorbeeld in de Large Hadron Collider vinden zijn excitaties van deze vacuümtoestand. Ook voor andere quantumveeldeeltjessystemen zullen we ons concentreren op de toestanden met lage energie en in het bijzonder op de toestand met allerlaagste energie, de grondtoestand. Het zijn immers deze toestanden die

Karel Van Acoleyen is onderzoeker en docent aan de Universiteit van Gent. Hij werkt op quantumveeldeeltjesfysica, hoge-energiefysica en kosmologie.

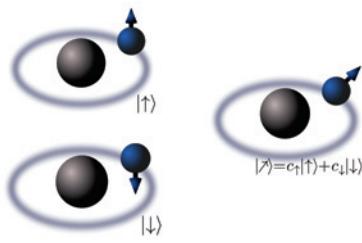
[karel.vanacoleyen@ugent.be](mailto:karel.vanacoleyen@ugent.be)



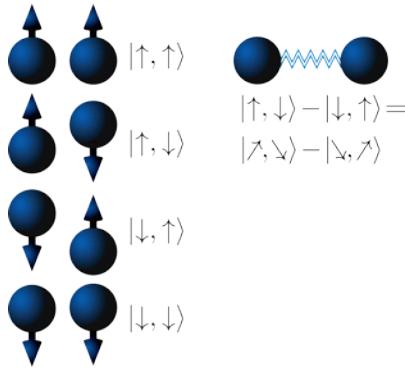
Frank Verstraete doet onderzoek in quantuminformatie en quantumveeldeeltjesfysica. Hij is professor aan de Universiteit van Gent.

[frank.verstraete@ugent.be](mailto:frank.verstraete@ugent.be)

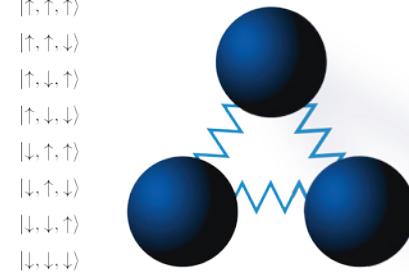




Figuur 1 Stap 1: 1 qubit, superpositie.



Figuur 2 Stap 2: 2 qubits, verstrengeling.



Figuur 3 Stap 3: 3 qubits, de monogamie van verstrengeling.

we vooral in de natuur terugvinden. De energieschaal voor elektronen in typische systemen is bijvoorbeeld vele grootteordes groter dan de energieschaal van de thermische fluctuaties bij kamertemperatuur, waardoor deze systemen voor alle praktische doeleinden door de grondtoestand beschreven worden.

Eén van de grote motivaties voor het bouwen van een quantumcomputer is het simuleren van quantumveeldeeltjessystemen. Maar tot nader order, bij gebrek aan een bruikbaar exemplaar, zijn we voor het begrijpen en simuleren van deze systemen nog aangewezen op een gewone klassieke computer. Hier speelt verstrengeling op de eerste plaats een nefaste rol. Dit is niet verwonderlijk, verstrengeling is precies de eigenschap die een quantumcomputer zijn enorm extra potentieel geeft ten opzichte van zijn klassieke tegenhanger. Maar een quantumcomputer is uiteindelijk ook een quantumveeldeeltjessysteem.

Het is dan ook te begrijpen dat het simuleren van een quantumveeldeeltjessysteem op een klassieke computer problematisch is. Zoals we meteen in de vier stappen hieronder en in de figuren 1 tot en met 4 in detail uitleggen zit de crux hem in de exponentiële groei van de toestandsruimte. Vanuit praktisch oogpunt is dit het grote probleem van de quantummechanica als voorspellende theorie. Typisch wordt bij een popularisatie van quantummechanica verwezen naar het indeterministisch karakter als het grote probleem, maar dat is uiteindelijk vooral een probleem van interpretatie. Maar laat ons nu eindelijk eens uitleggen wat verstrengeling en dus ook quantummechanica eigenlijk is.

## Quantummechanica in vier stappen (zie figuren 1-4)

**Stap 1: 1 qubit, superpositie (figuur 1)**  
We beginnen met het eenvoudigste quantumssysteem, het waterstofatoom. Dit is opgebouwd uit een proton met daaromheen een elektron. Wanneer we ons beperken tot de dynamica van het elektron bij lage energie, is de elektronspin de enige overblijvende vrijheidsgraad. Deze spin kan in elke richting staan. Tot zover kunnen we volgen met onze klassieke intuïtie, denk aan een tol waarvan de as in verschillende richtingen kan wijzen. Een eerste eigenaardig aspect van de quantummechanica is nu dat de toestand voor een bepaalde spinrichting kan worden opgeschreven als een superpositie van twee willekeurig gekozen basistoestanden. Vandaar de benaming qubit. Net als een klassieke bit kan deze de waarde nul of één aannemen, maar door zijn quantumkarakter nu ook alle mogelijke superpositions. Links schetsen we twee mogelijke basistoestanden: spin omhoog of spin omlaag. Rechts schrijven we een willekeurige andere spintoestand als een superpositie van deze eerste twee basistoestanden. Het relatieve gewicht van de coëfficiënten  $c_{\text{omhoog}}$  en  $c_{\text{omlaag}}$  staat in verband met metingen van de spin in de verticale richting. Hoe groter  $c_{\text{omhoog}}$ , hoe groter de kans om de spin omhoog te meten en analoog voor  $c_{\text{omlaag}}$ .

### Stap 2: 2 qubits, verstrengeling (figuur 2)

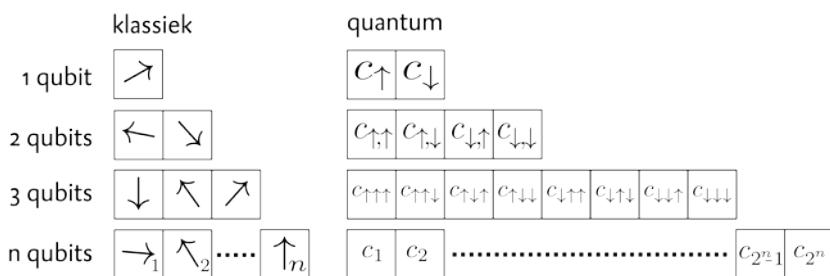
Verstrengeling ontstaat wanneer we een tweede qubit beschouwen. Dus we brengen een tweede waterstofatoom bij het eerste. Dit is trouwens ook exact wat er echt gebeurt in de natuur – twee waterstofatomen ver-

binden zich tot één waterstofmolecuul  $\text{H}_2$ .

Links in figuur 2 tonen we de vier basistoestanden voor dit twee-qubitsysteem: de spin omhoog of omlaag voor elk van de twee spins. Het blijkt nu dat de interactie tussen de twee atomen de energie minimaliseert wanneer de spins in tegengestelde richting staan. Dit leidt tot de grondtoestand (toestand met laagste energie) voor  $\text{H}_2$  die we rechts explicet opschrijven als superpositie van de basistoestanden. In deze toestand is er geen notie meer van de individuele spins – het gewicht van de coëfficiënten voor beide spinwaarden is gelijk. Elke meting van één elektronspin zal dus een compleet random uitkomst geven, en dit voor om het even welke spinrichting. De fysische eigenschap van deze maximaal verstrengelde toestand, met zijn twee spins in tegengestelde richting, manifesteert zich enkel wanneer we het gehele systeem beschouwen. Dit is de essentie van verstrengeling. Of met de woorden van Schrödinger, “the whole is more than the sum of its parts”.

### Stap 3: 3 qubits, de monogamie van verstrengeling (figuur 3)

We gaan verder en kijken wat er gebeurt wanneer we een derde qubit bij de eerste twee brengen. Links tonen we opnieuw de basistoestanden, dit zijn er nu acht. We bouwen hier niet zozeer een  $\text{H}_3$ -molecuul – deze komt niet voor in de natuur – maar wel een zogenaamde antiferromagneet, waarbij net als bij  $\text{H}_2$  de energie van naburige spins minimaal is bij een tegengestelde richting. De interactie van twee naburige qubits wil deze qubits opnieuw maximaal verstrengelen. Hier krijgen we echter te maken met de zogenaamde monogamie van verstrengeling: elke qubit heeft maar



Figuur 4 Stap 4: n qubits, de plaag van de exponentiële groei.

een bepaalde hoeveelheid verstrengeling te koop. Een qubit die maximaal verstrengeld is met een tweede qubit kan niet meer verstrengeld zijn met een derde. De grondtoestanden – het zijn er verschillende en we schrijven ze hier niet explicet uit – zijn al ietwat meer ingewikkelde superposities van de basistoestanden. We kunnen deze opvatten als een soort compromis, waarbij elke qubit een beetje verstrengeld is met zowel zijn linker- als rechterbuur.

#### Stap 4: n qubits, de plaag van de exponentiële groei (figuur 4)

Een quantumssysteem ‘leeft’ in een Hilbertruimte, dit is de ruimte van alle mogelijke toestanden. Elke toestand wordt bepaald door zijn coëfficiënten ten opzichte van de basistoestanden. Voor het één-qubitsysteem hebben we zo twee coëfficiënten, vier voor het twee-qubitsysteem en al acht voor het drie-qubitsysteem. Dit is de exponentiële groei van de Hilbertruimte: per extra qubit verdubbelt het aantal coëfficiënten dat een volledige quantumtoestand bepaalt. Het is precies de verstrengeling die verantwoordelijk is voor deze exponentiële groei. Bij een klassiek systeem, waar de quantum-mechanica en dus ook de verstrengeling te verwaarlozen is, wordt de toestand van het gehele systeem bepaald door de toestand van elk individueel deeltje. In dat geval krijgen we dus een lineaire groei van het aantal coëfficiënten. Dit contrast tussen exponentiële en lineaire groei maakt de quantumfysica zo veel moeilijker dan klassieke fysica. Met de beste supercomputers kan men bij kosmische simulaties tegenwoordig de klassieke gravitationele dynamica van vele miljarden sterrenstelsels simuleren, terwijl voor een quantumssysteem het wereldrecord ligt bij een schamele 48 qubits. Om de exponentiële groei nog even in perspectief te zetten: met de huidig beschikbare geheugencapaci-

teit van harde schijven heb je er één nodig ter grootte van het observeerbare universum om een 300-qubit toestand op te slaan.

#### De oppervlakbewet of de illusie van de monstrueuze Hilbertruimte

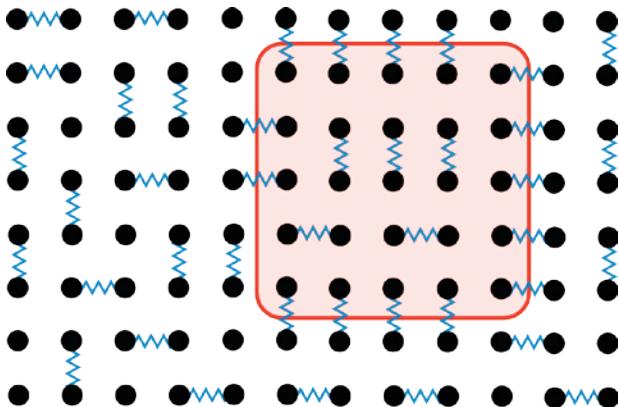
De fysica van de laatste honderd jaar heeft essentieel steeds voor twee grote uitdagingen gestaan. Enerzijds moet men voor een bepaald systeem altijd begrijpen wat de interacties tussen de deeltjes zijn. Naast de antiferromagnetische interactie van hierboven zijn er natuurlijk nog andere mogelijkheden. Maar het mooie en merkwaardige van de natuur is dat de mogelijkheden beperkt zijn. Op de eerste plaats zullen interacties steeds lokaal zijn, wat betekent dat ze enkel werkzaam zijn tussen nabijelegen deeltjes. Daarboven hebben we typisch heel wat symmetrie, wat de mogelijke interacties nog meer beperkt. Een voorbeeld is translatiesymmetrie, waaruit volgt dat de interacties op alle plaatsen gelijk zijn. Op zich zijn de interacties en bijhorende wiskundige vergelijkingen dus eenvoudig, maar – en dit is de tweede grote uitdaging – uit die vergelijkingen dient men dan nog op een of andere manier de fysisch relevante laagenergetische toestanden te puren. Hier botsen we telkens opnieuw op de exponentieel grote toestandsruimte. Inderdaad, de driehonderd qubits van de vorige paragraaf vormen een behoorlijk klein aantal wanneer we geïnteresseerd zijn in realistische materialen. Zelfs het kleinste stukje metaal bevat al snel miljarden maal miljarden elektronen en leeft dus in een monstrueus grote Hilbertruimte die nooit of te nimmer door een klassieke computer te vatten zal zijn. De grote uitdaging van de veeldeeltjesfysica bestaat uit het temmen van deze gigantische Hilbertruimte.

Traditioneel lukt dit bij relatief zwakke interacties tussen de verschillende

deeltjes. Al sinds de jaren dertig van vorige eeuw begrepen mensen als Hartree, Fock en Slater hoe de grondtoestanden er voor dergelijke systemen uitzien. Aldus identificeerden ze het fysisch relevante minuscule hoekje uit de Hilbertruimte waarop de berekeningen wel haalbaar zijn. Hun inzicht, verder op punt gezet door Feynman en co in de jaren vijftig en zestig heeft geleid tot een kwalitatief en kwantitatief begrip van talrijke systemen, gaande van metalen over halfgeleiders tot het vacuüm van de elektrozakke interactie met haar recent ontdekte higgsdeeltje.

Systemen met sterke interacties blijven echter een probleem. Een bekend voorbeeld is het tot nader order onopgeloste Hubbardmodel, dat supergeleiding bij hoge temperatuur zou beschrijven, wat het natuurlijk zeer relevant maakt voor allerhande mogelijke technologische toepassingen. Maar bijvoorbeeld ook bij de sterke kracht, die verantwoordelijk is voor 99% van alle massa op aarde, hebben we zoals de naam al weggeeft te maken met sterke interacties.

Sterke interacties tussen naburige deeltjes willen deze sterk verstrengen, maar uit de monogamie van verstrengeling (zie figuur 3) weten we dat elk deeltje maar een beperkte hoeveelheid verstrengeling toelaat. Hierdoor kan men de lokale interacties niet langer afzonderlijk beschouwen, en wordt de grondtoestand intrinsiek bepaald door al de interacties op heel het systeem samen in rekening te brengen. In principe lijkt dit dus een berekening te vragen op de volledige gigantische Hilbertruimte. Recent is echter duidelijk geworden dat een precieze karakterisering van de structuur van de verstrengeling hier een nieuwe kijk op geeft. Het is namelijk niet zo dat de verstrengeling zich random over de verschillende deeltjes zal verspreiden. De lokale interacties zorgen ervoor dat ook de verstrengeling op een of andere manier lokaal blijft. Het blijkt dat de verstrengeling tussen twee subsystemen in toestanden met lage energie vooral geconcentreerd zit aan de rand tussen die twee subsystemen, zoals geïllustreerd in figuur 5. Hierdoor schaalt de hoeveelheid verstrengeling tussen twee aangrenzende gebieden als de rand: dit is de zogeheten *area law*, oftewel: oppervlakbewet, die opduikt in heel diverse

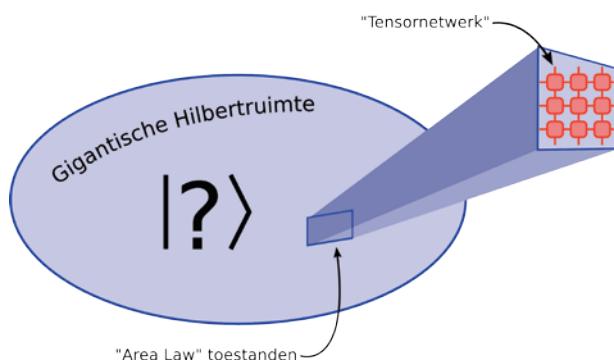


**Figuur 5** Voor laagenergetische toestanden van een veeldeeltjessysteem concentreert de verstrengeling tussen twee gebieden zich vooral aan de rand, dit maakt deze toestanden zo speciaal. Voor een willekeurige toestand zijn typisch al de deeltjes in het rode gebied, ook deze helemaal binnennin, verstrengeld met de deeltjes aan de buitenkant. Dit geeft dan een verstrengeling die schaalt als het volume.

gebieden in de fysica. In eerste instantie overigens in de context van zwarte gaten, maar dat is een ander verhaal. Quantumtoestanden die voldoen aan zo'n oppervlaktwet zijn heel speciaal, ze vertonen heel wat minder verstrengeling dan typische toestanden waarvoor de verstrengeling schaalt als het volume. Het is dus de verstrengeling die nu ook voor systemen met sterke wisselwerking het minuscule fysisch relevante hoekje uit de gigantische Hilbertruimte karakteriseert. En dit opent de deur voor een efficiënte beschrijving van alle mogelijke grondtoestanden.

Een recente doorbraak was het inzicht dat alle toestanden in dit hoekje inderdaad efficiënt geparametrisseerd kunnen worden door zogeheten tensornetwerktoestanden (zie figuur 6). De nomenclatuur ‘tensornetwerk’ is het gevolg van het feit dat de contractie van tensoren, een veralgemeening van matrixvermenigvuldigingen, een centrale rol speelt in dit formalisme. Deze tensornetwerken geven een compleet nieuw perspectief aan quantumveeldeeltjessystemen.

Essentieel komt het er op neer dat de gewone Schrödinger vergelijking van de quantummechanica met zijn exponentiële Hilbertruimte, ingewisseld wordt voor een nieuwe vergelijking op een veel kleinere ruimte die nu slechts lineair schaalt met de grootte van het systeem: zowel vanuit praktisch als vanuit conceptueel oogpunt betekent dit een enorme winst. Dit nieuwe formalisme is reeds met succes toegepast op verschillende specifieke modellen.



**Figuur 6** De fysisch relevante veeldeeltjetoestanden zitten in een minuscuul hoekje van een gigantisch grote Hilbertruimte. Deze toestanden voldoen aan de oppervlaktwet (*area law*) voor de verstrengeling en kunnen efficiënt worden beschreven door een tensornetwerk. Voor zo een tensornetwerk schaalt het aantal parameters (vervat in de rode blokjes in de tekening) slechts lineair met de grootte van het systeem.

De grote uitdaging voor het huidig onderzoek is nu de nieuwe vergelijkingen op een meer systematische manier te doorgronden. Dit zou dan uiteindelijk moeten leiden tot een algemene methode voor het oplossen van quantumveeldeeltjessystemen.

### Overall verstrengeling

Verstrengeling heeft vele gezichten en zorgt als dusdanig voor een actieve cross-over tussen verschillende onderzoeksgebieden. Het is dan ook niet verwonderlijk dat de op verstrengeling gestoelde tensornetwerken ook op andere plekken ingang vinden. Zo is verstrengeling van primordiaal belang bij de karakterisering van exotische materialen met quantumtopologische orde. Zulke systemen vallen buiten het conventionele beeld waarbij verschillende types materiaal gekarakteriseerd worden door hun lokale eigenschappen – denk bijvoorbeeld aan magnetisatie in een ferromagneet met lokaal de spins in eenzelfde richting. Materialen met topologische orde kunnen enkel onderscheiden worden van gewone types materiaal door hun speciale structuur voor de globale macroscopische verstrengeling. En ook hier blijken de tensornetwerken een nieuw perspectief te geven: de topologische orde wordt gereflecteerd in de lokale symmetrieeigenschappen van de tensoren die de grondtoestanden beschrijven.

Ook bij het onderzoek naar de aard van quantumzwaartekracht speelt verstrengeling een alsmaar belangrijker wordende rol. Volgens het beruchte holografisch principe is er een duali-

teit tussen een quantumveeldeeltjesysteem dat leeft op de rand van een ruimte en een gravitationeel systeem binnennin. Er blijkt nu een één-op-eén-verband te bestaan tussen de verstrengeling van het veeldeeltjessysteem en de geometrie van de ruimtetijd die zich binnennin bevindt. Zo komt het dan dat men tegenwoordig tensornetwerken, oorspronkelijk bedacht voor elektronen, gebruikt om de ruimtetijd zelf op quantumniveau te beschrijven. Verstrengeling is dus inderdaad overall. En het is deze veelzijdigheid die van verstrengeling zo'n boeiend onderwerp maakt.

De illustraties in dit artikel zijn gemaakt door Michaël Mariën.



# Quantumstage

**Mijn eerste kennismaking met quantuminformatie is in 2011 op de Universiteit van Cambridge in Engeland, in het Department of Applied Mathematics and Theoretical Physics. Ik volg de colleges van het vak Quantum Computation, gegeven door Richard Jozsa. Op dat moment weet ik nog niet dat hij een van de auteurs is van het artikel *Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen channels* [1]. Daarin beschrijft hij theoretisch hoe je een quantumbit (qubit) over een afstand kunt teleporteren. Precies dat ga ik een jaar later proberen tijdens mijn masterproject in Delft. Hier beschrijf ik mijn ervaringen als student in de theoretische en experimentele quantuminformatie.** Suzanne van Dam

222

Tijdens de eerste colleges in Cambridge worden tal van termen geïntroduceerd waarvan ik niet dacht dat ze in een vak zouden voorkomen waar het woord ‘quantum’ zo overheersend is in de titel. Voor een succesvolle introductie tot quantumberekeningen blijkt een heel arsenal aan computerkunde nodig, en een grote handvol wiskunde.

Ik begrijp nu ook waarom: om de quantummechanica effectief voor berekeningen in te zetten, zijn complexe algoritmes nodig. Want hoe kun je de parallelle rekencapaciteit benutten die een superpositie kan bieden als een quantummeting deze superpositie vernietigt? Om dat probleem te kunnen aanpakken gaat quantummechanica hand in hand

met informatica en wiskunde. Na de eerste theoretische kennismaking in Cambridge, ontmoet ik in februari 2013 qubits in het echt. Voor mijn afstudeerproject maak ik negen maanden lang deel uit van het team van Ronald Hanson aan de TU Delft, in de Quantum Transport-groep. Daar zie ik hoe het er in de experimentele werkelijkheid aan toe gaat.

In de colleges in Cambridge werd als uitgangspunt genomen dat er een qubit was met de mogelijkheid om hierop operaties uit te voeren. Voor deze theoretische qubit worden dan algoritmes ontwikkeld, zodat het systeem kan worden gebruikt voor berekeningen. In Delft zie ik dat het beschikken over en controleren van een qubit al een uitdaging op zich kan zijn. Daarnaast is de fysica van het gebruikte

systeem bepalend voor de quantumoperaties die mogelijk zijn en daarmee voor de algoritmes of protocollen die je kunt toepassen.

Het fysische systeem dat ik in Delft leer kennen is diamant. Toepasselijk noemt het team waarin ik afstudeer zich dan ook Team Diamond. Wij richten ons op stikstof-gat (NV) centra, onregelmatigheden in het koolstofrooster van diamant. In die centra ontbreken twee koolstofatomen waarvan er een is vervangen door een stikstofatoom en

de andere een gat achterlaat waarin zich elektronen bevinden. De totale spin van de elektronen in het gat is een van de qubits in dit systeem en wordt gecontroleerd met lichtpulsen en microgolven.

Team Diamond is het al gelukt om veel (gave!) dingen te doen met deze qubits. Toen ik mijn afstudeerproject begon, hadden wij dus de kans om het veeleisende protocol van quantumteleportatie te gaan implementeren. Daarvoor is ook andere kennis en kunde nodig dan quantuminformatietheorie alleen. Om het systeem zo goed mogelijk te benutten voor quantumprotocollen moet het goed begrepen worden. Alleen dan is duidelijk hoe het zal reageren op bijvoorbeeld de laserpulsen die wij er van buitenaf op afsturen. De implementatie van protocollen is vervolgens ook een technische uitdaging. Dit is direct te zien als je in Delft het lab in de kelder binnen gaat. De optische tafels zijn daar volgebouwd met spiegels en lenzen en de elektronica lijkt uit alle hoeken en gaten te ontspringen. En dat allemaal voor de controle over enkele qubits.

De experimentele uitdaging wordt ook duidelijk als je naar een individuele qubit gaat kijken in plaats van naar het algemene fysische systeem. Want “Qubits hebben persoonlijkheden”,

Suzanne van Dam is masterstudent Applied Physics aan de TU Delft, na afronding van een master theoretische fysica aan de Universiteit van Cambridge. Voor haar masterproject in Delft werkte ze aan quantumteleportatie in de groep van Ronald Hanson. Nu doet ze een stage bij CERN in Genève.



[suzannevandam@gmail.com](mailto:suzannevandam@gmail.com)

zoals je van veel experimentatoren hoort. Zo ook onze qubits: de precieze golflengte van het licht waar de qubits in diamant op reageren verschilt van qubit tot qubit en verandert voor elke qubit een klein beetje van minuut tot minuut. Daarom moet je de lasers tunen tijdens elke meting en elk experiment dat je doet. Voor mijn afstudeerproject heb ik hier de fijne kneepjes van geleerd: succesvol tunen vereist kennis van het fysische systeem, maar ook het aanvoelen van de individuele qubit.

Ik ben er van overtuigd dat deze arbeidsintensieve tune-methode in de loop van de tijd zal worden overgenomen door een automatische; als een van de stappen in het grootbrengen van deze onstuimige qubits. Langzaam maar zeker zullen die qubits misschien gaan lijken op de theoretische qubits uit de colleges in Cambridge.

### Referentie

- 1 C.H. Bennett et al., *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett. **70** (1993) 1895.



In de kelder van de TU Delft worden in het lab van Ronald Hanson quantumbits gecontroleerd met lasers en microgolven. Foto: Jan Jouke Harms.

223

Leukje



# De ultieme laptop

Een laptop heeft ongeveer een inhoud van 1 liter ( $1000 \text{ cm}^3$ ) en een gewicht van 1 kilogram. Wat is de maximaal mogelijke rekencapaciteit van zo'n laptop? In zijn artikel *Ultimate physical limits to computation* (Nature, **406** (2000) 1047 - 1054) heeft Seth Lloyd, hoogleraar computer science and mechanical engineering aan het Massachusetts Institute of Technology (MIT), dat uitgerekend. Computers zijn fysische systemen en dus onderhevig aan fysische wetten. De fundamentele fysische grens voor de snelheid van informatieverwerking wordt bepaald door de beschikbare energie. De hoeveelheid informatie die kan worden verwerkt wordt begrensd door het aantal beschikbare vrijheidsgraden. Volgens de wet van Moore verdubbelt het informa-

tieverwerkingsvermogen van computers iedere anderhalf tot twee jaar. Kan dat steeds doorgaan? Extrapolaties tonen aan dat de klassiek-fysische grens ongeveer tussen 2025 en 2030 zal worden bereikt. Quantumcomputers echter kunnen in principe de informatieverwerking tot aan het niveau van de individuele atomen uitbreiden. Zo'n 'Avogadro-computer', die  $10^{23}$  qubits aankan, is niet fundamenteel-fysisch onmogelijk. De maximale snelheid waarmee een elektron een 'spinflip' (tussen bit = 0 en bit = 1) kan uitvoeren, wordt bepaald door het Margolus-Levitintheorema (1998), dat de fundamentele fysische grens bepaalt voor de snelheid van toestandsverandering en daarmee ook van de rekensnelheid van iedere computer: een quantumsys-

teem van energie  $E$  heeft minstens de tijd  $t = (h/4E)$  nodig om tussen twee orthogonale vrijheidsgraden (toestanden) te wisselen ( $h = 6,626 \cdot 10^{-34} \text{ Js}$  is de constante van Planck). Als gevolg kan een systeem met gemiddelde energie  $E$ , maximaal  $4E/h$  logische ops (operations per second) verrichten. Een computer van 1 kilogram heeft een gemiddelde energie van  $E = mc^2 = 8,9874 \cdot 10^{16} \text{ J}$  om berekeningen uit te voeren. Dit staat gelijk met de energie van een waterstofbom van ongeveer 20 megaton TNT ( $1 \text{ TNT} = 4,184 \cdot 10^{12} \text{ J}$ ). De ultieme Avogadro-laptop heeft dus een verwerkingscapaciteit van maximaal  $4E/h = 5,4256 \cdot 10^{50}$  ops. Theoretisch zou de wet van Moore dus tot aan het jaar 2205 kunnen blijven gelden.

Herman de Lang

# Magnetische bewustwording

## Atoom voor atoom van spinqubit naar stabiele magneet

**De magnetisatie van een spinqubit kan tegelijkertijd omhoog en omlaag zijn. Maar bij een macroscopische magneet ligt deze vast. Hoeveel spins heb je eigenlijk nodig om een stabiele klassieke magneet te maken? Door met een tunnelmicroscoop een magneet letterlijk atoom voor atoom op te bouwen, kunnen we deze ‘magnetische bewustwording’ uitstekend in kaart brengen. Daarbij is het mogelijk de collectieve dynamische excitaties (magnonen) van in het lab ontworpen nanomagneten te zien, en deze lokaal en op atomaire schaal aan te slaan.** Sander Otte

224

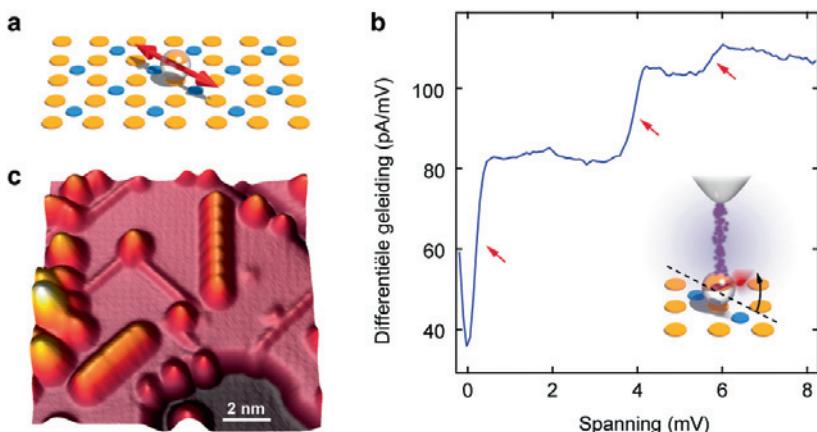
Magnetisme is een collectief fenomeen. Als heel veel magnetische atomen samen een materiaal vormen, dan kunnen die atomen besluiten om hun magnetisch moment allemaal dezelfde kant op te leggen (ferromagneet) of juist afwiss-

selend omhoog en omlaag (antiferromagneet). Neem bijvoorbeeld een bit op een harde schijf: deze bestaat uit een aantal ferromagnetische korrels waarin die momenten allemaal dezelfde kant op staan gericht.

Omvat de bit echter nog maar een

paar atomen, dan ontstaat een situatie waarbij de eigentoestanden niet meer eenvoudig omhoog en omlaag zijn, maar bijvoorbeeld 99% omhoog + 1% omlaag en 99% omlaag + 1% omhoog. Nu is er dus enige overlap tussen de twee magnetisatierichtingen. Schrijven we deze bit naar omhoog en laten we hem vervolgens aan zijn lot over, dan kan de magnetisatie op een willekeurig moment spontaan naar omlaag tunnelen. Naarmate het aantal atomen afneemt, wordt deze overlap alleen maar groter.

Bij hoeveel atomen begint dit proces? Die vraag is niet eenvoudig te beantwoorden. Ten eerste is het een geleidelijk proces. Ten tweede zijn er allerlei factoren die een rol spelen. Wat is de grootte van de spin op ieder atoom? Aan hoeveel buren is elk atoom gekoppeld en hoe sterk is die koppeling? Is er sprake van een kristalstructuur die een bepaalde voorkeursrichting oplegt? Hoe sterk is de koppeling tussen het spinmoment en het baanmoment van de elektronen? Al deze



**Figuur 1** a) Magnetische voorkeursas van een Fe-atoom op een rooster van Cu- (geel) en N- (blauw) atomen. b) Differentiële geleiding ( $dI/dV$ ) als functie van de spanning, gemeten op een enkel Fe-atoom. Spinexcitaties zijn aangegeven met rode pijlen. c) STM-topografie met daarop twee ketens van elk zeven atomen: één ferromagnetisch (linksonder) en één antiferromagnetisch (midden boven).

aspecten moeten in kaart worden gebracht voordat je kunt vaststellen hoe klein de minimale klassieke bit is, of hoe groot de maximale qubit.

## Bouwen met atomen

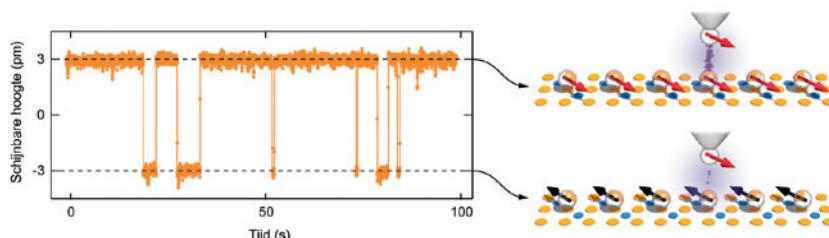
In ons lab in Delft bouwen we minuscule magneten door atomen één voor één te rangschikken met behulp van een tunnelmicroscoop, of STM (scanning tunneling microscope), waarin een scherpe naald de atomen aftast. Dit gebeurt in een ultra-hoogvacuümomgeving bij een temperatuur van minder dan één kelvin. Liggen de atomen eenmaal op hun plaats, dan kunnen ze weken blijven liggen. Zo kunnen we in alle rust de geleidelijke overgang bestuderen van één enkele quantumspin naar een klein, maar stabiel stukje magneet.

De primaire bouwstenen in veel van ons werk zijn Fe-atomen die op een kopernitride ( $\text{Cu}_2\text{N}$ ) oppervlak zijn opgedampt. Op dit oppervlak zijn de atomen covalent gebonden. Hierdoor ervaren ze een sterke voorkeur om hun spins langs de as van hun bindingen met de naburige N-atomen te leggen (figuur 1a). Dit kan nog altijd twee kanten op en voor een enkel Fe-atom is de polarisatie dan ook onbepaald: in dit geval tegelijkertijd naar links en naar rechts [1].

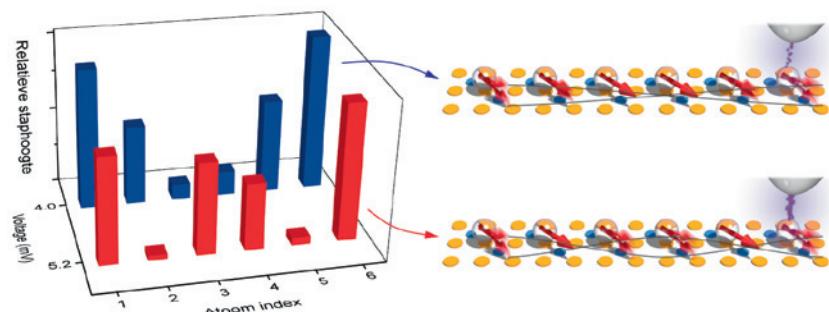
## Spinexcitaties

Andere oriëntaties van de spin zijn niet verboden, maar die kosten wat meer energie. Deze energie kunnen wij lokaal aan het atoom toedienen door middel van de tunnelstroom uit de STM-naald. Hiervoor moet er wel voldoende spanning worden aangelegd tussen de naald en het atoom. In figuur 1b staat een meting van de differentiële geleiding van het tunnelcontact als functie van deze spanning. Hierin verschijnt een aantal stappen waarvan elk correspondeert met een bepaalde discrete quantummechanische excitatie: een rotatie van de spin van de voorkeursas vandaan.

Met behulp van dit soort excitatiemetingen kunnen we veel leren over de magnetische omgeving van het atoom. Plaatsen we bijvoorbeeld een tweede atoom vlak bij het eerste, dan verschuiven de excitatie-energieën. Dankzij deze verschuivingen weten we dat de koppeling tussen de atomen, afhankelijk van hun exacte plaatsing, kan variëren tussen ferromagnetisch



**Figuur 2** Meting van de spingepolariseerde tunnelstroom (oftewel: de schijnbare hoogte van de atomen) op een keten van zes Fe-atomen als functie van de tijd, gemeten in een magnetisch veld van 100 mT. De magnetisatie van de keten klapt af en toe om van de parallelle toestand (+3 pm) naar de antiparallele toestand (-3 pm) en vice versa. Rechts is een schematische weergave van de meting in beide toestanden.



**Figuur 3** Hoogte van waargenomen stappen in de differentiële geleiding (zoals figuur 1b) voor twee opeenvolgende excitaties bij 4,0 mV en 5,2 mV op elk van de zes atomen in een ferromagnetisch gekoppelde Fe-keten. Rechts, impressies van de bijbehorende spingoltoestanden.

en antiferromagnetisch [2]. Deze eigenschap kunnen we gebruiken om spinketens te bouwen van beide soorten, zoals weergegeven in figuur 1c. Terug naar de hoofdvraag: vanaf welke lengte kiest zo'n keten voor één polarisatierichting en wordt hij klassiek magnetisch? Om dit te kunnen zien moeten we een meting doen die onderscheid maakt tussen de twee polarisaties uit figuur 1a. Dit kan met behulp van spin-gepolariseerde STM: een methode waarbij we het uiterste atoom aan het einde van de naald vervangen door een Fe-atom (figuur 2). Plaatsen we deze gemagnetiseerde naald nu boven een Fe-atom op het oppervlak, dan gedraagt het tunnelcontact zich als een magnetoweerstand: zijn de spins van de twee Fe-atomen parallel dan meten we een grotere stroom dan wanneer ze antiparallel zijn. Door dit ene atoom wordt de hele naald dus een soort minuscule versie van de leeskop in een harde schijf, waarmee we de magnetische oriëntatie van ieder atoom kunnen uitlezen.

## Omkappen

In een recent experiment hebben we met deze methode een aantal korte ferromagnetisch gekoppelde ketens onderzocht. Vanaf een leng-

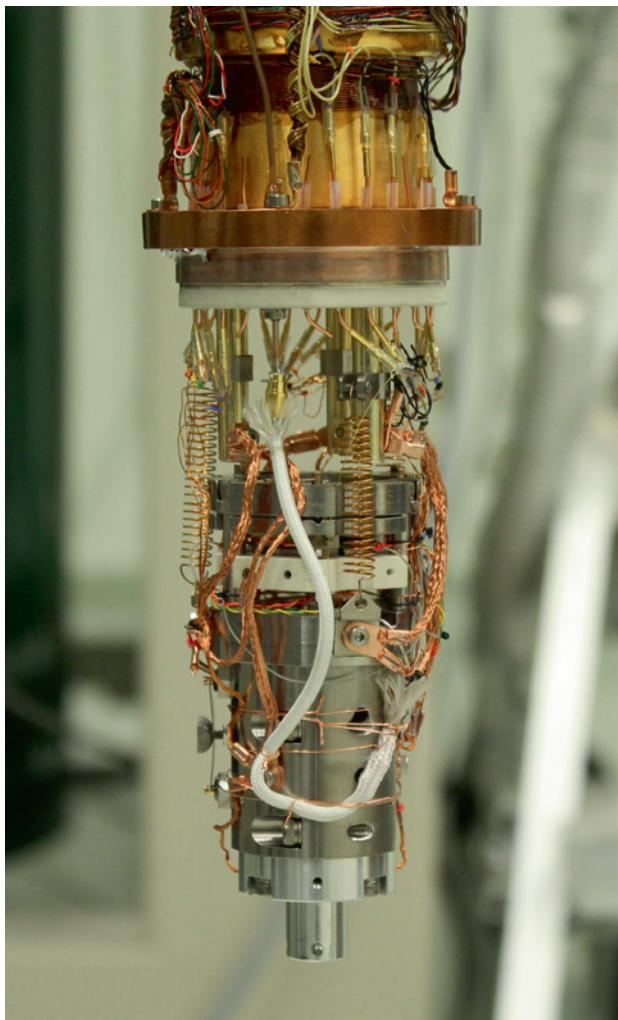
te van circa vier atomen zien we dat de tunnelstroom niet langer constant is, maar plotseling sprongen vertoont (figuur 2). Tijdens deze sprongen klapt de magnetisatie van de keten volledig om [3,4]. Voor vier atomen volgen de sprongen elkaar snel op, zodat het eigenlijk meer op een continue ruis lijkt. De tunnelkoppeling tussen de twee polarisaties is dan nog vrij sterk. Maar bij langere ketens worden de sprongen zeldzamer: bij zes atomen gaan er soms minuten voorbij zonder dat de magnetisatie verandert. Hoewel er veel tijd tussen twee omklappingen kan zitten, gaat het omklapproces zelf razendsnel: volgens onze berekeningen is het in een picoseconde gebeurd. De meetelektronica van de STM kan dit helaas bij lange na

Sander Otte promoveerde in Leiden in 2008 en werkte bij IBM Research en NIST, waar hij zich specialiseerde in lokale elektron-tunnelspectroscopie.

Sinds 2010 heeft hij een eigen onderzoeksgrond in Delft, met als focus het ontwerpen en bouwen van kunstmatige atomaire spinroosters.



A.F.Otte@tudelft.nl



**Figuur 4** Foto van de STM-module (Unisoku USM1300). Tijdens experimenten hangt deze aan drie veren (voor trillingsisolatie) in een vacuüm van  $10^{-11}$  mbar. Bovenaan (goudkleurig) de pot met vloeibaar helium-3, dat de STM afkoelt tot 330 mK. Met behulp van een supergeleidende solenoïde kunnen magneetvelden tot 9 T worden aangelegd. De STM is circa 4 cm in diameter.

niet bijhouden. Het is dus onmogelijk om rechtstreeks te zien in welke volgorde de atomen hun spin omdraaien. Toch kunnen we, met behulp van wat circumstantial evidence, wel enig inzicht krijgen in wat er nu precies gebeurt in die ene picoseconde.

Dit doen we door het omklappen zelf actief aan te drijven. Door de naald op verschillende plekken boven de keten te plaatsen en de spanning op te voeren kunnen we lokaal spinexcitatieën maken die de omklapfrequentie drastisch doen toenemen. Wat blijkt: deze toename hangt sterk af van de positie van de naald. Maken we een spinexcitatie aan een van de uiteinden van de keten dan heeft deze een veel grotere kans om tot een omklapping van alle spins te leiden dan wanneer we een excitatie met dezelfde energie aanslaan in het midden van de keten. Kennelijk hebben deze collectieve ex-

citaties dus een bepaalde niet-homogene structuur binnen de keten.

### Spingolven

Deze structuur kunnen we zichtbaar maken door spinexcitatiesspectroscopie, zoals in figuur 1b, uit te voeren op ieder atoom in de keten. We zien hierbij dat de gemeten intensiteiten (dat wil zeggen de staphoogtes in de differentiële geleiding) van bepaalde excitaties variëren over de lengte van de keten. In figuur 3 is deze variatie weergegeven voor twee opeenvolgende excitaties, bij 4,0 mV en bij 5,2 mV. Hierbij springt onmiddellijk het golfkarakter van deze toestanden in het oog: de excitaties hebben knopen en buiken waarvan de posities worden bepaald door de randvoorwaarden. Het gaat hier dan ook om spingolven, ook wel magnonen genoemd, voor het eerst waargenomen met atomaire pre-

cisie [4]. Deze magnonen spelen een hoofdrol in het omklapproces: niet alleen in deze kunstmatige atoomketens, maar ook elke keer als je op je harde schijf een bit omschrijft!

Net als bijvoorbeeld fononen, kunnen magnonen uitstekend worden beschreven als quantummechanische quasideeltjes. Uitgaande van een spin-magnitude  $S=2$  per Fe-atoom, is de grondtoestand van de keten (222222), ofwel alle spins volledig dezelfde kant op gedraaid. Met de tunnelstroom slaan we één van de spins aan, laten we zeggen naar (222221). Maar in een magnontoestand raakt deze excitatie direct gedelokaliseerd. Het magnon bij 4,0 mV, bijvoorbeeld, kan geschreven worden als:

$$33\% (122222) + 16\% (212222) \\ + 16\% (222112) + 33\% (222211).$$

Dus hoewel de stabiele grondtoestand van de keten vrijwel exact klassiek magnetisch is, zijn de dynamische aangeslagen toestanden nog altijd quantummechanisch van aard. Dit zal waarschijnlijk zo blijven zolang de keten korter is dan de vrije weglengte van de spingolf, oftewel, zolang de keten volledig defectvrij gebouwd is.

Samengevat bieden deze experimenten een unieke kijk in de prille beginfase van magnetisme. Dat is niet alleen fascinerend, maar ook technologisch waardevol. Goed begrip van welke effecten belangrijk zijn in magnetische stabilisatie kan ingenieurs helpen bij het ontwikkelen van nieuwe magnetische opslagmedia. Persoonlijk heb ik met dit onderzoek een fundamenteel doel voor ogen. Door grote atomaire spinroosters te bouwen en de koppelingen tussen de atomen nauwkeurig af te stemmen, moet het mogelijk zijn nieuwe complexe magnetische fasen te creëren die vooralsnog hoofdzakelijk op papier bestaan: spinvloeistoffen. Niemand weet hoe een materiaal zich in deze intrigerende hoedanigheid zal gedragen.

### Referenties

- 1 C. F. Hirjibehedin *et al.*, *Science* **317**, 1199 (2007).
- 2 B. Bryant *et al.*, *Phys. Rev. Lett.* **111**, 127203 (2013).
- 3 S. Loth *et al.*, *Science* **335**, 196 (2012).
- 4 A. Spinelli *et al.*, *arXiv:1403.5890* (2014).



# Wie had dat gedacht?

**A**ls Leo Kouwenhoven er inderdaad in slaagt een quantumcomputer te bouwen, dan zou dit in meerdere opzichten een fascinerende analogie met de ‘klassieke’ computer opleveren. Beide zijn gevoed door een krachtige mix van nieuwsgierigheidsgedreven en toepassingsgericht onderzoek. Ook de quantumcomputer zal de technologische infrastructuur van de samenleving ingrijpend veranderen, tenminste als de profeten van de quantuminformatietheorie gelijk krijgen. Maar de meest opmerkelijke analogie tussen de klassieke en de quantumcomputer ligt in hun totaal onverwachte oorsprong, namelijk in het grondslagenonderzoek van respectievelijk de wiskunde en de natuurkunde.

De moderne computer is uitgevonden (zowel in visionaire zin als wat betreft de daadwerkelijke bouw, onafhankelijk in het Verenigd Koninkrijk en in de Verenigde Staten) door de wiskundigen Alan Turing en John von Neumann. Zijn essentiële eigenschap is dat hij universeel is in de zin dat in principe ieder programma kan worden uitgevoerd. Dat blijkt mogelijk te zijn omdat er geen principieel verschil is

tussen programma’s en de data die ingelezen worden. Dit was een buitengewoon diep inzicht van Turing en Von Neumann, die daar nooit op zouden zijn gekomen zonder hun eerstehands kennis van eerdere ontwikkelingen in de grondslagen van de wiskunde, waarbij David Hilbert en Kurt Gödel (en in een eerder stadium ook de filosofen Gottlob Frege en Bertrand Russell) een hoofdrol speelden: de moderne computer is voortgekomen uit vragen rond formalisering, waarheid en bewijsbaarheid in de wiskunde. Quantumcomputers zijn linea recta terug te voeren op het Bohr-Einstein-debat van 1927-1949 over de grondslagen van de quantummechanica, en dan met name op het hoogtepunt daarvan, het Einstein-Podolsky-Rosen-artikel uit 1935 [1]. Vervolgens is er een duidelijke weg van het Bohr-Einsteindebat, via de mysticus David Bohm, naar John Bell (die oorspronkelijk een nauwelijks geciteerde outsider was, maar inmiddels postuum de meest vereerde grondslagenonderzoeker uit de geschiedenis van de natuurkunde lijkt), en van diens werk uit 1964 en 1966 naar de

Klaas Landsman studeerde van 1981 tot 1985 natuurkunde aan de Universiteit van Amsterdam en promoveerde aldaar in 1989 in de theoretische hoge-energiefysica. Na een verblijf van 1989 tot 1997 aan de Universiteit van Cambridge keerde hij terug naar Nederland, in eerste instantie als KNAW-Fellow aan de UvA. Hij werd in 2001 benoemd tot hoogleraar Mathematische Fysica aan de UvA, ontving in 2002 een Pioniersbeurs van NWO en is sinds 2004 verbonden aan de Radboud Universiteit. In 2005 verscheen zijn roman *Requiem voor Newton*.

landsman@math.ru.nl

227

quantuminformatietheorie. Maar ook in de jaren tachtig was het werk van Stephen Wiesner, Charles H. Bennett en Gilles Brassard, dat de quantumcryptografie inluidde, gebaseerd op het grondig doordenken van het meetprobleem van de quantummechanica en waren ook de baanbrekende artikelen van David Deutsch over quantumcomputers uiteindelijk een gevolg van zijn curieuze (*Many Worlds*) opvattingen over de interpretatie van de quantumtheorie. The rest is history.

Dit betekent dat bezinning op de grondslagen van een vakgebied niet alleen een intellectuele uitdaging biedt, maar zich ook praktisch loont. Nog meer illustreren deze twee voorbeelden nog eens hoe zinnig het niet doelgericht plannen van wetenschap en technologie is.

Klaas Landsman

## Referentie

- Zie de artikelen van Herman de Lang op pagina 190 en van Ad Verbruggen op pagina 193 en veel uitgebreider een boek als Louisa Gilder, *The Age of Entanglement: When Quantum Physics Was Reborn*, Knopf, 2008.



# Maakt D-Wave quantumcomputers?

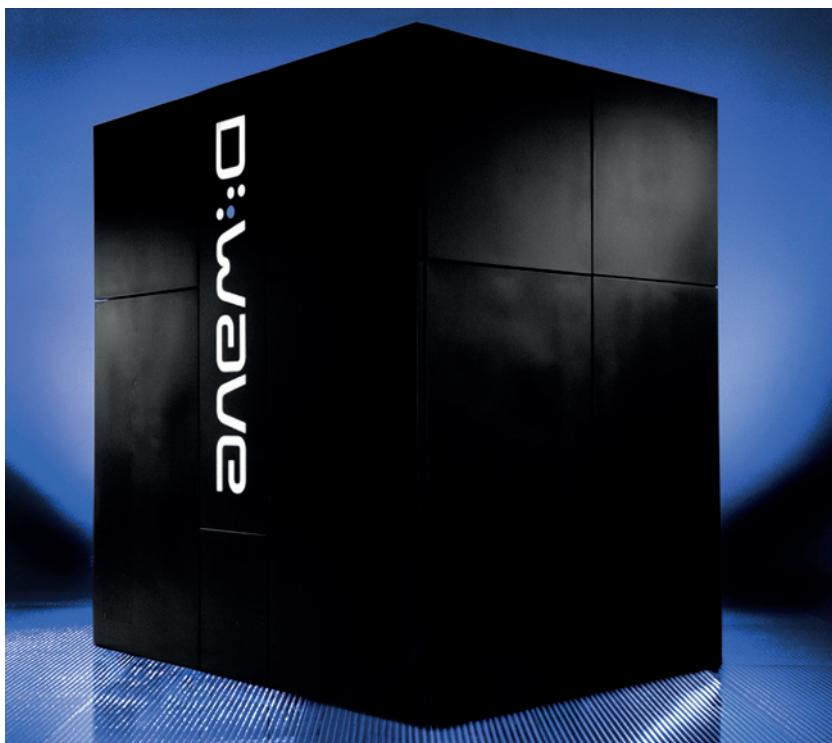
**Quantumcomputers zijn er in soorten en maten en het is niet eenvoudig om aan te tonen dat ze daadwerkelijk volledig quantummechanisch opereren. Dat zijn tot nu toe wellicht de belangrijkste conclusies die getrokken kunnen worden uit de activiteiten van het Canadese bedrijf D-Wave, fabrikant van de naar eigen zeggen eerste commercieel beschikbare quantumcomputer. Een korte inleiding over de geschiedenis van D-Wave en haar producten.** Miriam Blaauboer

In 2011 baarde het Canadese bedrijf D-Wave wereldwijd opzien met de aankondiging van een quantumprocessor die uit 128 geïntegreerde qubits bestaat. De D-Wave One, zo luidde hun claim, was de eerste commercieel beschikbare quantumcomputer ter wereld. D-Wave, gevestigd in British Columbia, is opgericht in 1999 en inmiddels uitgegroeid tot een bedrijf met meer dan honderd werknemers [1].

De D-wave One bestaat uit 128 paarsgewijs gekoppelde flux qubits, qubits waarbij de basistoestanden  $|0\rangle$  en  $|1\rangle$  uit linksom en rechtsom lopende persisterende stromen in supergeleidende juncties bestaan. De processor voert een optimalisatie-operatie uit door middel van een proces genaamd quantum annealing. Je kunt dit vergelijken met de beweging van een quantummechanische bal door een

landschap van bergen en dalen, waarbij het laagste dal het gewenste antwoord voorstelt. De bal start in alle dalen ‘tegelijkertijd’, door gebruik te maken van superpositie van qubits, en ondergaat een langzame (adiabatische) quantummechanische evolutie. Na een tijdje is de golffunctie van de bal voornamelijk in de lagere dalen geconcentreerd en uiteindelijk komt hij – via tunnelen door de bergen, die als potentiaalbarrières fungeren – in de laagste dalen terecht. De toestand van die dalen vormt het antwoord en daarmee geeft het programma een zo goed mogelijke benadering van de oplossing.

Fysisch gesproken is de D-wave One speciaal ontworpen voor specifieke problemen die beschreven kunnen worden als een klassiek tweedimensionaal Isingmodel in een magneetveld, waarbij men geïnteresseerd is in de oplossing met de laagste energie. Het is dus geen universele quantumcomputer waarop een willekeurig quantumgoritme gedraaid kan worden, maar een gespecialiseerde quantum-optimalisatiemachine. D-wave’s computer is met name geschikt voor het doorzoeken van complexe data – zoals bijvoorbeeld het debuggen van grote computerprogramma’s en het analyseren van mogelijke manieren waarop eiwitten kunnen vouwen – maar bijvoorbeeld niet voor factorisatie in priemgetallen. Voor dit laatste is een



De D-Wave One, volgens het bedrijf D-Wave's werelds eerste commercieel verkrijgbare quantumcomputer. Foto: Courtesy of D-Wave Systems Inc.

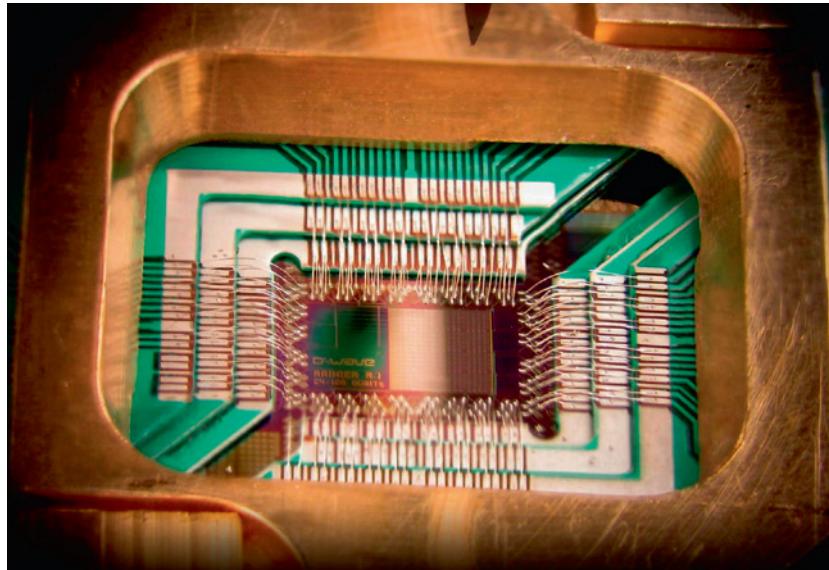
universele quantumcomputer vereist (zie de artikelen van Ronald de Wolf op pagina 183 en van Ronald Hanson en Floris Zwanenburg op pagina 179). Van begin af aan was de D-Wave One (en ook zijn opvolger de D-Wave Two, die uit 512 qubits bestaat) omstreden. Verschillende teams van universitaire onderzoekers hebben bij het analyseren en testen van door D-Wave gepubliceerde data weliswaar aanwijzingen gevonden voor quantum annealing en korte-afstandsverstrekking, maar geen tijdwinst ten opzichte van klassieke computers [2]. Ook zijn diverse vergelijkingen tussen klassieke en quantummechanische modellen enerzijds en data gegenereerd door de D-Wave Two anderzijds tot nu toe vrijwel altijd in het voordeel van een klassiek model uitgevallen. Over de vraag of D-Wave's computer intrinsiek quantummechanisch opereert is duidelijk het laatste woord nog niet gesproken.

Ondanks deze twijfels heeft D-Wave inmiddels twee grote klanten agetrokken. In 2011 heeft vliegtuigfabrikant Lockheed Martin een quantumcomputer van D-Wave aangeschaft, die gehuisvest is bij de University of Southern California. In 2013 kondigde Google aan een D-wave Two te installeren in het door hen en NASA nieuw opgerichte Quantum Artificial Intelligence-laboratorium in Californië. Met de oprichting van dit instituut beoogt Google voortgang te boeken in onder andere onderzoek naar machinaal leren, waarbij het bedrijf klassieke en quantumcomputingstijlen wil combineren.

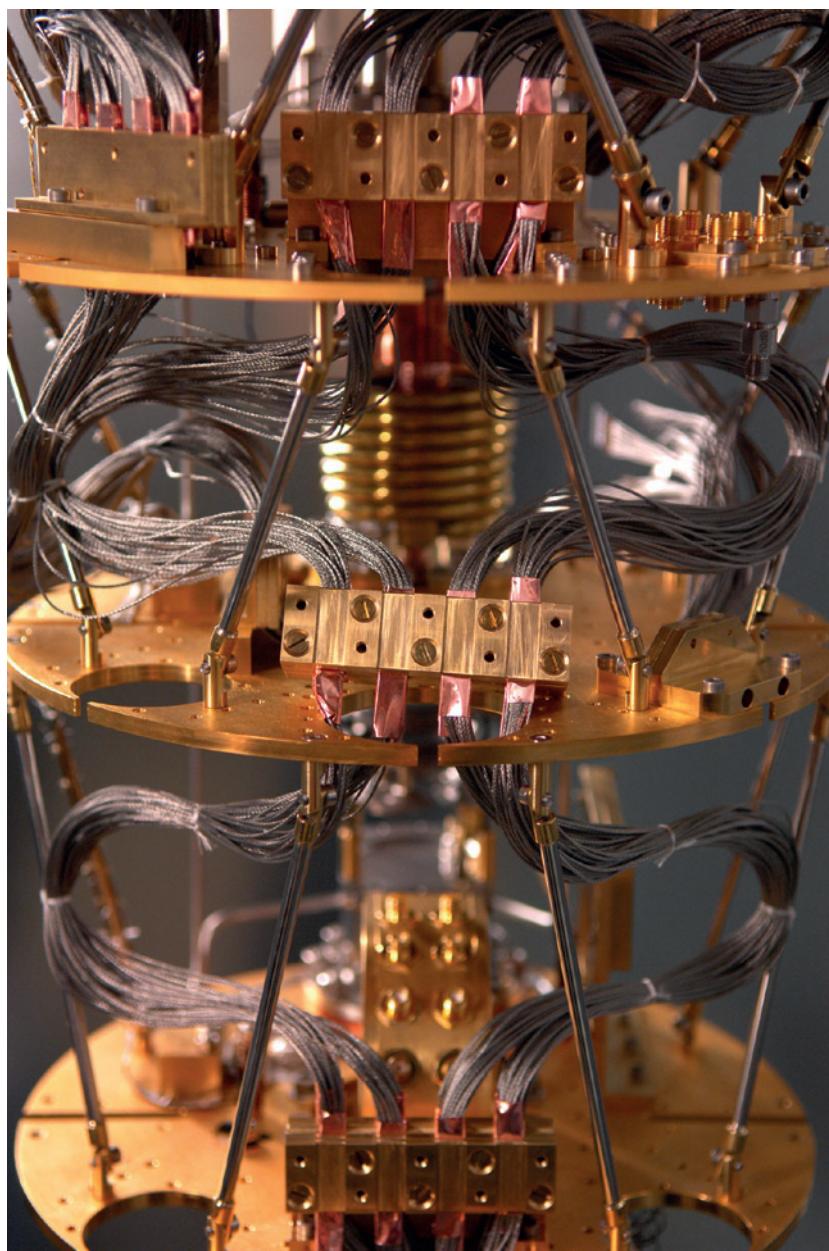
D-Wave heeft aangekondigd in 2015 een 2048-qubit quantumprocessor op de markt te willen brengen. Nader onderzoek door universiteiten en bedrijven zal in de komende jaren hopelijk meer inzicht verschaffen in het ware karakter van de computers van D-Wave – en ons op weg daarheen allerlei interessante natuurkunde op het gebied van quantuminformatie opleveren.

## Referenties:

- 1 [www.dwavesys.com](http://www.dwavesys.com).
- 2 Zie bijvoorbeeld <http://arxiv.org/abs/1401.2910>. Verder is op de blog van Scott Aaronson (MIT) veel informatie te vinden over D-wave: [www.scottaaronson.com/blog/](http://www.scottaaronson.com/blog/).



Chip uit de D-Wave One met 128 qubits. Foto: Courtesy of D-Wave Systems Inc.



De processor van de D-Wave moet afgeschermd worden tegen interferentie van buitenaf en moet tot nagenoeg het absolute nulpunt worden afgekoeld om gebruik te kunnen maken van quantumeffecten. Foto: Courtesy of D-Wave Systems Inc.

# Quantumrekenen met Majoranadeeltjes

In het onlangs geopende Quantum Computer Laboratorium (QC-lab) in Delft zullen Majoranadeeltjes worden ingezet om quantumberekeningen te beschermen tegen de verstorende invloeden van de omgeving. Deze deeltjes, die materie en antimaterie verenigen, zijn in 2012 opgedoken in supergeleidende schakelingen. Hun beschermende invloed wordt topologisch genoemd en toegeschreven aan niet-Abelse statistiek. Ik zal proberen deze wiskundige begrippen wat te verduidelijken en ons ontwerp tonen van een quantumrekenenmodule voor Majoranadeeltjes.

Carlo Beenakker

230

## Kracht en kwetsbaarheid

Quantumrekenen onderscheidt zich op twee essentiële punten van klassiek rekenen. Ten eerste kunnen de rekeneenheden verschillende waarden tegelijkertijd aannemen; in plaats van een bit die 0 óf 1 is, hebben we een qubit die 0 én 1 is. We noteren dit als  $\alpha|0\rangle + \beta|1\rangle$ . Voor een klassieke bit is een van de beide coëfficiënten  $\alpha$  en  $\beta$  altijd gelijk aan nul, dus dan heb je óf  $|0\rangle$  óf  $|1\rangle$ , en kun je de haakjes net zo goed weglaten. Voor een qubit zijn beide coëfficiënten ongelijk aan nul, we zeggen dat er een superpositie is van toestand  $|0\rangle$  met gewicht  $|\alpha|^2$  en toestand  $|1\rangle$  met gewicht  $|\beta|^2$ .

Ten tweede zijn de bewerkingen bij

quantumrekenen altijd omkeerbaar. Klassiek rekenen is niet omkeerbaar: als je alleen de som kent kun je de getallen die je hebt opgeteld niet meer reconstrueren. Qubits kun je niet zonder meer optellen, de enige toegestane bewerking is de vermenigvuldiging van de vector  $(\alpha, \beta)$  met een inverteerbare matrix (een zogenaamde unitaire operatie). Het optellen van qubits zal dan altijd samengaan met het aftrekken, en als je som en verschil kent kun je de bewerking natuurlijk wel degelijk omkeren.

Unitaire operaties op qubits zijn zowel bijzonder krachtig als buitengewoon kwetsbaar. Ze zijn krachtig omdat een enkele operatie op N qubits een superpositie van een exponentieel groot aantal (namelijk  $2^N$ ) toestanden oplevert. Ze zijn kwetsbaar omdat ze omkeerbaar zijn, invloeden van buitenaf kunnen de bewerking makkelijk verstoren.

Een quantumcomputer moet dus beschermd worden. De voor de hand liggende aanpak is volledige afzondering van de buitenwereld. Voor korte tijd is dit mogelijk, bij zeer lage temperaturen. Een alternatief voor afzondering is verhulling, de informatie is verstopt in een eigenschap van het systeem

die de buitenwereld niet kan uitlezen. In een abstracte beschrijving gaat het om een topologische eigenschap van de golffunctie van het systeem en daarom spreekt men van topologische bescherming van de verhulde informatie.

Bij de Majoranadeeltjes wordt dit allemaal wat concreter.

## Deeltje en antideeltje

Het onderscheid tussen materie en antimaterie speelt een belangrijke rol in de fysica van elementaire deeltjes: het elektron heeft als antideeltje het positron en deze twee tegengesteld geladen deeltjes zullen elkaar bij een botsing vernietigen (annihileren). Een Majoranadeeltje is zijn eigen antideeltje. Wellicht heeft het neutrino deze eigenschap, maar ook al zou het Majoranadeeltje niet bestaan als elementair deeltje, in supergeleidende metalen komt het voor als een samengesteld deeltje.

Figuur 1 legt dit uit, aan de hand van de Fermi-zee – de gevulde toestanden in de geleidingsband van een metaal. Een elektron bij positieve energie (gevulde toestand boven de ‘zeespiegel’ bij energie nul) heeft als antideeltje een gat bij negatieve energie. Het elektron annihielt het gat door de lege

Carlo Beenakker is als hoogleraar verbonden aan het Instituut-Lorentz voor theoretische natuurkunde van de Universiteit Leiden. Samen met Leo Kouwenhoven en Lieven Vandersypen van de TU Delft ontving hij vorig jaar een Europese Synergy-subsidie voor het QC-lab.

beenakker@lorentz.leidenuniv.nl



toestand op te vullen. Om hier een Majoranadeeltje van te maken moet het metaal supergeleidend worden. Dan is het mogelijk om een deeltje samen te stellen uit een elektron en een gat, en precies bij energie nul te binden aan een defect in de supergeleider (zoals het uiteinde van een draad of een magnetische wervel).

We spreken gemakshalve van Majoranadeeltje, maar het is eigenlijk slechts een half deeltje, enigszins zoals een glas dat tegelijk halfvol is en halfleeg. Omdat het totaal aantal elektronen heeltallig is, zal er altijd een even aantal Majoranadeeltjes aanwezig zijn. Zodra je twee Majoranadeeltjes bij elkaar brengt, kunnen ze annihielen, een onverstoerde Fermi-zee achterlatend. Er is een tweede mogelijkheid, een fusie van de beide halfdeeltjes kan een heel deeltje opleveren. Het is alsof het verenigen van twee halfvolle glazen resulteert in een leeg glas of een vol glas.

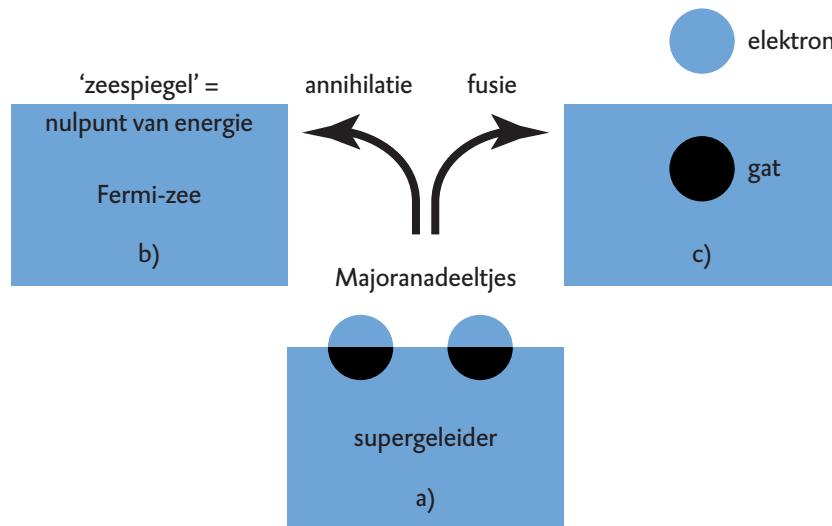
Om informatie in de Majoranadeeltjes op te slaan, definiëren we de toestand  $|1\rangle$  of  $|0\rangle$  afhankelijk van of er wel of geen deeltje overblijft als ze samengaan. Deze informatie is verhuld zolang de Majoranadeeltjes uit elkaars buurt blijven. Aan een enkel Majoranadeeltje kun je op geen enkele manier zien wat het samengaan met diens partner zal opleveren. Pas als je ze bij elkaar brengt kun je de toestand van deze qubit uitlezen. Ook voor de omgeving blijft de informatie verhuld, en dus beschermd. Dit is wat men topologische bescherming noemt.

Er is een gevaar in zicht: vrije elektronen die de supergeleider in- of uitgaan zullen de informatie verstören, omdat een  $|0\rangle$  dan een  $|1\rangle$  kan worden of omgekeerd. Er is gelukkig heel veel ervaring in de supergeleidende technologie om uitwisseling van elektronen met de omgeving te minimaliseren, zodat de bescherming intact blijft.

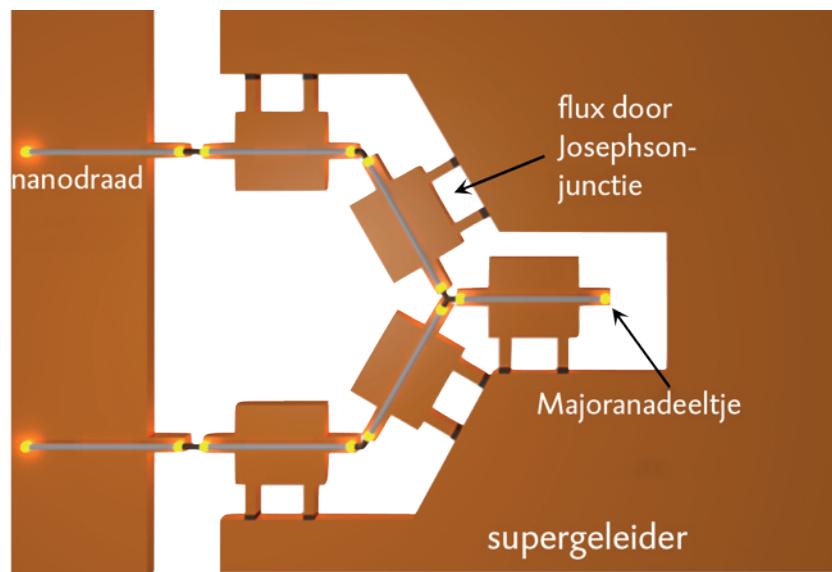
## Vlechten

Beschermde opslag van informatie door verhulling is nuttig, maar je wilt wel met die informatie kunnen rekenen – liefst zonder de verhulling op te heffen. Dit is mogelijk omdat Majoranadeeltjes die om elkaar heen bewegen een elektron uitwisselen, ook als ze voortdurend op grote afstand van elkaar blijven.

Stel je begint met twee paar Majoranadeeltjes in een supergeleider waar het



**Figuur 1** a) Schematische weergave van een tweetal Majoranadeeltjes in de Fermi-zee van een supergeleider. Samengaan van twee Majoranadeeltjes levert b) een onverstoerde Fermi-zee op, of c) een superpositie van een elektron en een gat. In het eerste geval (annihilatie) zijn alle elektronen in de Fermi-zee twee aan twee verbonden als supergeleidende Cooperparen. In het tweede geval (fusie) blijft er een enkel ongepaard elektron over.



231

**Figuur 2** Schema van een quantumrekenmodule gebaseerd op Majoranadeeltjes. De nanodraad verbindt kleine supergeleidende eilandjes, die elk door een Josephsonjunctie met een veel grotere supergeleider verbonden zijn. Ieder eiland bevat twee Majoranadeeltjes in de toestand  $|0\rangle$  of  $|1\rangle$ , afhankelijk van het aantal elektronen op het eiland even of oneven is. Door de magnetische flux in de Josephsonjuncties te variëren, kunnen elektronen tussen de eilandjes worden uitgewisseld. Zo wordt de  $\sqrt{\text{NOT}}$  operatie op de qubits uitgevoerd, zonder dat de Majoranadeeltjes verplaatst hoeven te worden.

totaal aantal elektronen oneven is. Als het eerste paar in de toestand  $|0\rangle$  is, dan is het tweede paar noodzakelijkerwijs in de toestand  $|1\rangle$ . Het omgekeerde is ook mogelijk, dus de gecombineerde toestand kunnen we schrijven als de superpositie  $\Psi = \alpha|0\rangle|1\rangle + \beta|1\rangle|0\rangle$ . Nu verwisselen we een Majoranadeeltje uit het eerste paar met een Majoranadeeltje uit het tweede paar. Het resultaat is een unitaire operatie op de toestand  $\Psi$ , waarbij de vector  $(\alpha, \beta)$  vermenigvuldigd wordt met een

matrix  $U$ . Deze wordt gegeven door  $U = \sqrt{\frac{1}{2i}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \Rightarrow U^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ , dus twee keer verwisselen van de Majoranadeeltjes verwisselt de coëfficiënten  $\alpha$  en  $\beta$  – in fysische termen komt dat neer op het uitwisselen van een elektron tussen het eerste en het tweede paar Majoranadeeltjes. De operatie  $U$  uit vergelijking (1) wordt aangeduid als  $\sqrt{\text{NOT}}$ , omdat het kwadrant ervan de NOT-operatie ( $0 \leftrightarrow 1$ )

uitvoert.

Bij het vermenigvuldigen van matrices doet de volgorde er toe,  $UV$  is niet hetzelfde als  $VU$ . Bewerkingen waar de volgorde niet uitmaakt heten in de wiskunde Abelse bewerkingen, en het verwisselen van deeltjes heet een statistische bewerking, vandaar dat men spreekt van de niet-Abelse statistiek van Majoranadeeltjes. Het verwisselen van de Majoranadeeltjes wordt wel vergeleken met het vlechten (Engels: braiding) van strengen, hetgeen ook een bewerking is waar de volgorde er toe doet.

### Vooruitzicht

De  $\sqrt{\text{NOT}}$  uitvoeren door twee Majoranadeeltjes om elkaar te laten bewegen voldoet als gedachtenexperiment, maar is niet echt praktisch omdat ze vastzitten aan de uiteinden van een draad. Er zijn wel methodes bedacht om de deeltjes langs de draad te laten

bewegen en dan bij een kruising van twee draden elkaar te laten passeren, maar het liefst zou je de deeltjes veilig op hun plaats willen laten.

Figuur 2 toont een alternatief, waarbij je de  $\sqrt{\text{NOT}}$  bewerking kunt uitvoeren zonder de Majoranadeeltjes zelf te verplaatsen. De operatie komt tot stand met behulp van een Josephson-junctie, een welbekende supergeleidende schakelaar die bediend wordt door de magnetische flux in de junc tie te variëren. De draad met Majoranadeeltjes blijft gedurende de gehele operatie onaangeroerd.

Een experiment dat een topologisch beschermd operatie realiseert zou een mijlpaal zijn in de ontwikkeling van de quantumcomputer. Wat zou het een triomf zijn als het QC-lab als eerste over de finish zou komen!

### Dankwoord

Aan het Leidse ontwerp voor een Ma-

joranaquantumrekenmodule hebben bijgedragen: Anton Akhmerov, Michele Burrello, Cosma Fulga, Fabian Hassler, Bernard van Heck en Timo Hyart, zie arXiv:1111.6001 en arXiv:1303.4379. Het onderzoek wordt vanuit Nederland gesteund door OCW/NWO/FOM en in Europees verband door de ERC.

### Referenties

- 1 A. Stern en N. H. Lindner, *Topological quantum computation – From basic concepts to first experiments*, *Science* **339** (2013) 1179.
- 2 G. P. Collins, *Computing with quantum nrots*, *Scientific American*, april 2006.
- 3 M. Leijnse en K. Flensberg, *Introduction to topological superconductivity and Majorana fermions*, *Semiconductor Science and Technology* **27** (2012) 124003 [arXiv:1206.1736].
- 4 C.W. J. Beenakker, *Search for Majorana fermions in superconductors*, *Annual Review of Condensed Matter Physics* **4** (2013) 113 [arXiv:1112.1950].

## Groepsportret



# Detectie van één enkel foton

## Single Quantum in Delft

**Single Quantum is een jong bedrijf dat detectoren maakt voor enkele fotonen. Sander Dorenbos is medeoprichter en leidt het onderzoek en de ontwikkeling binnen het bedrijf. We praten met hem en enkele medewerkers over het onderzoek dat ze doen en de producten die ze maken.** Esger Brunner en Marieke de Boer

**S**ander Dorenbos studeerde en promoveerde aan de Technische Universiteit Delft. Tijdens zijn promotie richtte hij zich op het ontwikkelen van detectoren voor enkele fotonen met behulp van supergeleidi-

dende nanodraden. Dorenbos: "Dat ging best goed en al tijdens mijn promotie vroegen mensen of we die apparaten ook verkopen." Dat was niet het geval, maar andere vakgroepen konden wel de detector in bruikleen

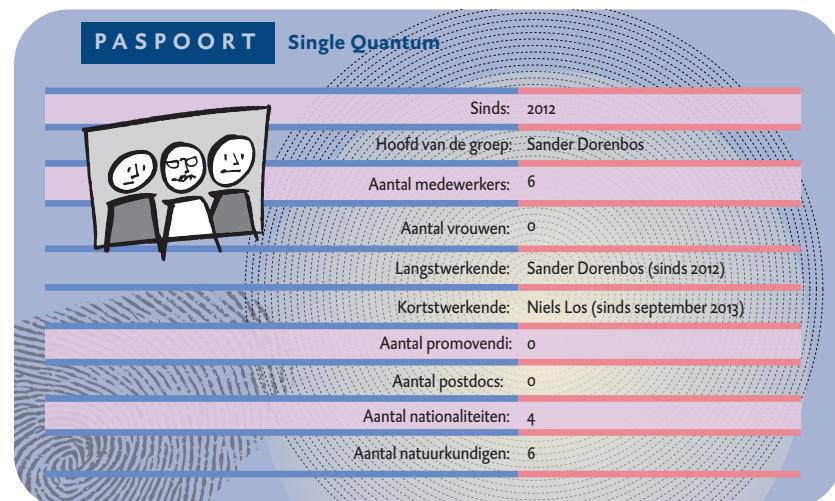
krijgen in ruil voor een mede-auteurschap op hun wetenschappelijke artikelen. Eind 2011 kwam er nog meer interesse en werd Dorenbos gevraagd een detector te bouwen. "Ik was aan het eind van mijn promotie, dus dat

kwam heel goed uit,” vertelt Dorenbos over het begin. Samen met zijn promotor Val Zwiller en zakelijk partner Floor van de Pavert richtte hij in januari 2012 Single Quantum op.

## Het product

Het bedrijf is gesitueerd in twee kamers in het natuurkundegebouw van de TU Delft en maakt detectoren voor enkele fotonen in het uv- tot nabij-infrarode gebied ( $\pm 0,3$  tot  $2 \mu\text{m}$ ). Een cirkelvormige detectiechip, die ze zelf maken in de cleanroom van de universiteit, vormt het hart van de detector. Op het oppervlak van ongeveer  $10 \mu\text{m}^2$  zigzagt een  $500 \mu\text{m}$  lange nanodraad van niobiumtitaniumnitride (NbTiN). Door de draad, die wordt gekoeld tot  $3\text{-}4\text{ K}$  om hem supergeleidend te maken, wordt een klein stroomje gestuurd. Bij absorptie van een foton, dat via een glasvezelkabel naar de detectorchip wordt geleid, warmt de draad lokaal op, waardoor hij zijn supergeleidende eigenschappen verliest. Dit wordt gedetecteerd door het voltageverschil tussen de draadeinden te meten.

De detectoren worden gebruikt in onderzoek naar nieuwe quantumtechnologieën, zoals quantumcommunicatie, medische beeldvorming en voor analyse van geïntegreerde schakelingen. De klanten bestaan nu nog alleen uit universiteiten, maar IBM heeft ook interesse getoond. Overigens duurde het wel een flinke tijd voordat Single



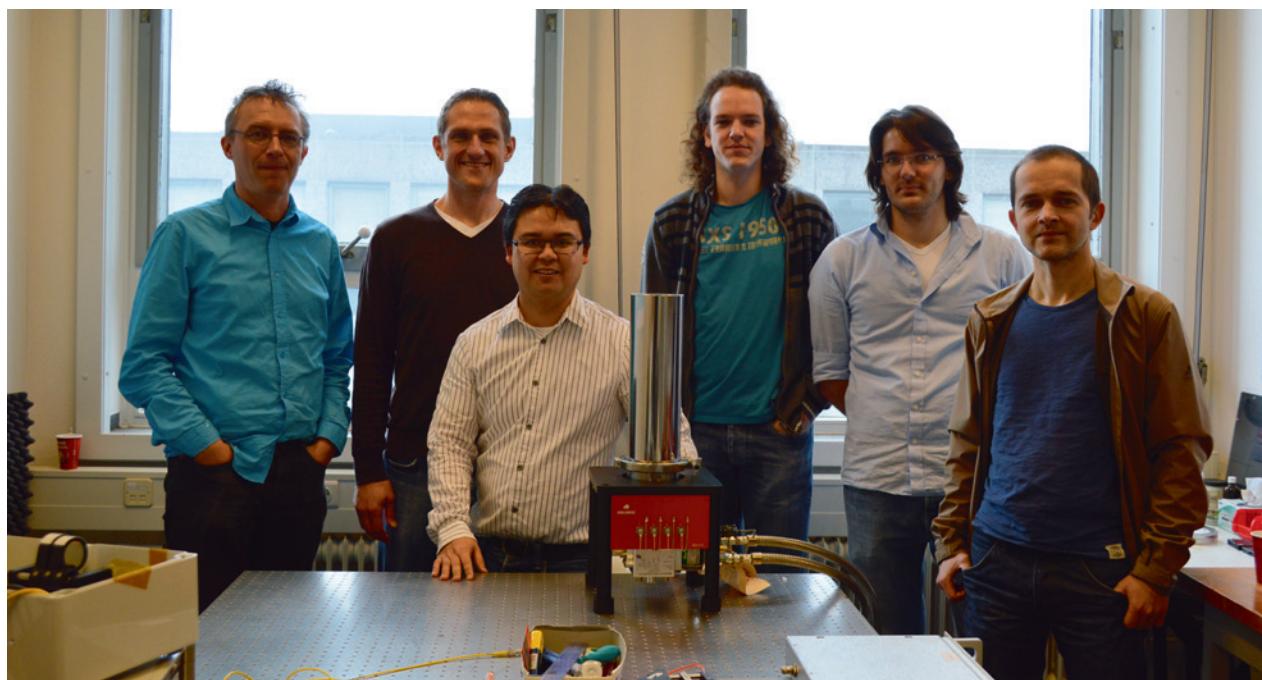
Quantum en hun detectoren voldoende naamsbekendheid hadden, ondanks de vliegende start. Dorenbos verkocht dankzij zijn en Zwillers netwerk begin 2012 twee detectoren. Daarna duurde het anderhalf jaar voor er nieuwe bestellingen binnengingen, maar sinds een paar maanden loopt het steeds beter. “De eerste vier systemen werden buiten Europa verscheept, de vijfde is onlangs naar Duitsland verzonden en er staan nog vijf of zes orders te wachten,” vertelt Dorenbos.

## Verdere ontwikkelingen

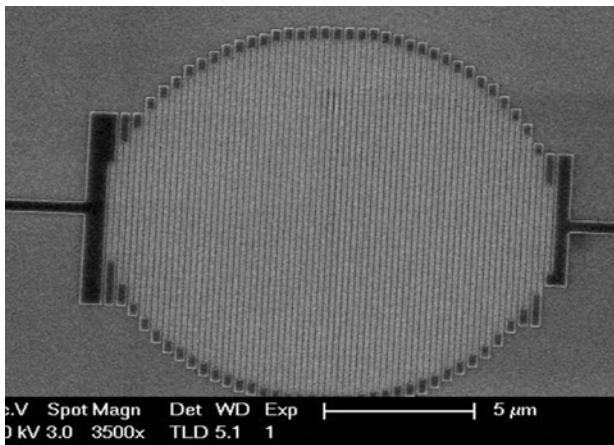
Het jonge bedrijf bestaat nu uit zes mensen. Naast het bouwen houden ze zich voornamelijk bezig met het verbeteren van hun product. “De eerste ontwikkeling is het behalen van

een nog hogere efficiëntie dan dertig procent bij de huidige golflengte. Dat betekent dat je van de tien fotonen die in de fiber zitten er ongeveer drie detecteert. Dat moet natuurlijk naar honderd procent,” legt Dorenbos uit en hij heeft goede hoop dat ze dat ook nagenoeg gaan halen. Daarnaast willen ze het detectoroppervlak vergroten. “Het bestaat nu uit slechts één pixel, het zou interessant zijn om meerdere pixels te hebben. Dan krijg je een soort camera waar je plaatjes mee kunt maken.” Toepassingen hiervoor ziet Dorenbos vooral op medisch vlak, bijvoorbeeld als vervanger van beeldvorming met röntgenstraling. “Maar dat is wel heel erg speculeren en nog ver weg”, zegt Dorenbos. Een derde ontwikkeling bij Single Quantum is het uitbreiden van de gevoelig-

233



De medewerkers van Single Quantum achter een van hun fotodetectoren (v.l.n.r.): Val Zwiller, Michael Reimer, Sander Dorenbos, Niels Los, Victor Hartong en Sergiy Dobrovolskiy. Foto: NTvN - Marieke de Boer.



Een chip uit een detector. De nanodraad gaat verticaal op en neer en is ongeveer 500 μm lang.



Het natuurkundegebouw van de TU Delft waar Single Quantum zich bevindt. Foto: NTvN - Marieke de Boer

heid bij andere golflengtes. Zo wil Dorenbos voor langere golflengtes in het infrarode gebied (2 - 10 μm) en kortere golflengtes in het ultraviolette gebied (200 - 300 nm) ook efficiënte detectie van een enkel foton ontwikkelen.

### Toekomst quantumtechnologie

In de nabije toekomst ziet Dorenbos brede inzet van technologie gebaseerd op quantummechanica in het algemeen niet gebeuren omdat de technologische ontwikkelingen langzaam gaan: "Ik denk dat het nog wel zo tot 25 jaar gaat duren en ik denk ook dat de toepassingen dan heel anders zullen zijn dan we nu voor ogen hebben." De toepassing van quantummechanica voor in het dagelijks leven zal lastig worden, alleen al vanwege praktische problemen zoals de extreem lage temperaturen die je nodig hebt voor quantummechanische effecten. "Toch hoop ik wel dat Single Quantum een rol kan spelen in de ontwikkeling van toepassingen."

### Productie

De tweede persoon die we spreken is Niels Los. Hij rondde zijn studie technische natuurkunde af in september 2013. "Toen ik klaar was, ben ik hier eigenlijk ingerold. Tijdens mijn master werkte ik al aan de detectoren. Er was hier een plek en ik ben meteen doorgegaan," vertelt Los. "Ik vind het leuk dat ik echt iets maak." Als R&D and Production Engineer is hij verantwoordelijk voor de assemblage van de detectoren, waarbij hij de verschillende onderdelen samenvoegt tot een geheel. Als dat gebeurd is, test hij of alles naar behoren functioneert. Daarnaast neemt hij praktische zaken voor zijn rekening, zoals bijvoorbeeld de

inkoop van onderdelen. "Verder zijn we bezig met wat we kunnen verbeteren," vertelt Los. Naast de eerder genoemde functionele verbeteringen, probeert Single Quantum het productieproces te verbeteren voor een hogere opbrengst. "Er is een groot verschil met de universitaire wereld. Als je onderzoek doet, hoef je maar een of twee werkende detectoren van de honderd te hebben en dan kun je daarmee je onderzoek doen en een artikel schrijven. Maar in het bedrijfsleven moet je kijken waar je dingen kunt verbeteren voor een zo hoog mogelijke opbrengst."

Waar Niels Los de assemblage op zich neemt, produceert zijn Oekraïense collega Sergiy Dobrovolskiy de detectiechips. Dobrovolskiy is via flinke wetenschappelijke omzwervingen sinds februari 2013 werkzaam voor Single Quantum. Hij studeerde theoretische natuurkunde aan Charkov National University en promoveerde er in de deeltjes- en kernfysica, waarna hij er een jaar als postdoctoraal onderzoeker werkte. "Tegelijkertijd wilde ik mijn achtergrond verbreden richting de experimentele fysica," vertelt Dobrovolskiy en eind 2002 vond hij op het FOM-Instituut AMOLF in Amsterdam een interessante positie op het gebied van dunne films. Via FOM-Rijnhuizen kwam hij op de TU Delft terecht waar hij werkte aan dunne-film silicium. In die jaren veranderde zijn interesse en wilde hij zich meer richten op de commerciële kant van natuurkunde, onderzoek en ontwikkeling. "Uiteindelijk vond ik Single Quantum, dat geïnteresseerd was in mijn ervaring met dunne films en ik was geïnteresseerd in de zakelijke

kant en ik kon mijn persoonlijke ontwikkeling doorzetten. Het is een heel nieuwe ervaring, ik leer hier nieuwe vaardigheden en methodes en werk met nieuwe machines." Daarnaast vindt Dobrovolskiy het leuk dat zijn product bijdraagt aan het genereren van wetenschappelijke resultaten in verschillende vakgebieden.

### Toepasbaar

Dobrovolskiy heeft bij diverse onderzoeksinstinten gewerkt, maar echt grote verschillen daartussen ziet hij niet. Wel merkt hij op dat er in Delft veel start-ups zijn, ontstaan uit de natuurkunde, en incubators (instituten die ondernemingen helpen op te starten) als Yes!Delft en Technopolis. "Dit zorgt voor veel uitwisseling van informatie tussen academische en commerciële groepen. Toen ik in Amsterdam werkte, telde slechts ons ene wetenschappelijke instituut. De concentratie van en interactie tussen bedrijven helpt mensen verder." Over verschillen tussen commerciële bedrijven en de universiteit is hij duidelijk: "Mijn antwoord is niet uniek. Bij bedrijven is het onderzoek doelgericht, terwijl er op een universiteit vaak langoppende onderzoeken zijn, die wellicht in de toekomst door iemand gebruikt worden. Bij een bedrijf moet het meteen toepasbaar zijn. Op dit moment vind ik dat het leukst."





## t/m 14 september 2014

Boerhaave aan de Vecht. Een wetenschapskabinet van een Heer van Stand. Aan de hand van prachtige microscopen, telescopen, mechanica modellen en elektriciteitsproeven geeft de tentoonstelling een levensechte voorstelling van een wetenschappelijk kabinet van een rijke burger uit de achttiende eeuw. In Boerhaave aan de Vecht presenteren Museum Boerhaave, Collectie Planetarium Zuylenburgh en de Collectie Van Doornen een selectie van hun mooiste voorwerpen op dit gebied, die normaal niet door publiek te bewonderen zijn.

[www.museumboerhaave.nl](http://www.museumboerhaave.nl)

[www.planetariumzuylenburgh.com](http://www.planetariumzuylenburgh.com).

## t/m 26 oktober 2014

100 jaar uitvindingen, Made by Philips Research, een tentoonstelling over het honderdjarig bestaan van Philips Research in Museum Boerhaave.  
[www.museumboerhaave.nl](http://www.museumboerhaave.nl).

## 2 - 4 juni 2014

Workshop Electron Beam Spectroscopy for Nanophotonics (EBSN), in Amsterdam.  
[www.amolf.nl/ebsn](http://www.amolf.nl/ebsn).

## 4 juni 2014

NEVAC-dag, aan vacuüm gerelateerde wetenschap en technologie. Academiegebouw Universiteit Utrecht, Domplein 29. Sprekers: Sara Bals (EMAT, Antwerp), Rafael Abela (PSI, SWISSFEL), Peter van der Straten (UU), Sense Jan van der Molen (UL), Joost W.M. Frenken (Advanced Research Center for Nanolithography, Amsterdam), Urs Wiesemann (Bruker, Germany), Inge Loes ten Kate (UU), Alexander Ako Khajetorians (Hamburg University, Germany) en NEVAC-prijs winnaar Ronald van Leeuwen (TUD).  
Aanmelding: [www.nevac.nl](http://www.nevac.nl).

## 21 - 26 juni 2014

Euroscience Open Forum, in Kopenhagen.  
<http://esof2014.org>.

## 22 juni 2014

The History and Future of Dark Matter, symposium in Amsterdam.  
<http://iop.uva.nl/>.

## 26 juni 2014

Symposium 60 jaar CERN, 1954 was

Volg het NTvN ook op Twitter via [NTvN\\_tweets!](#) Met nieuws over het NTvN, de NNV en natuurkunde in Nederland.



 tie Atomic, Molecular and Optical Physics van de NNV in congrescentrum De Werelt in Lunteren.  
[www.ru.nl/amolunteren](http://www.ru.nl/amolunteren).

## 16 - 20 november 2014

ICQNM 2014, The Eighth International Conference on Quantum, Nano/Bio, and Micro Technologies, in Lissabon.  
[www.iaria.org/conferences.html](http://www.iaria.org/conferences.html).

## 10 april 2015

 FYSICA 2015, in Eindhoven.

## 28 - 29 mei 2015

DRSTP symposium Trends in Theory 2015, 11<sup>e</sup> tweejaarlijkse symposium van de Dutch Research School of Theoretical Physics.  
<http://web.science.uu.nl/DRSTP>.

## Antwoorden



## Quantum-mijnenveger

235

### Opgave 1

Uitleg over constructieve interferentie in beide detectoren vind je op de website. De uitkomst is onmogelijk omdat die in strijd is met de wet van behoud van energie.

### Opgave 2

Zie de uitwerking op de website.

### Opgave 3

Het feit dat A het foton heeft gedetecteerd leert ons niets over de positie van de mijn.

### Opgave 4

Je weet nu dat de mijn een van de armen van de interferometer geblokkeerd moet hebben.

### Opgave 5

50%.

### Opgave 6

Nee.

De uitwerkingen zijn te vinden op onze website [www.ntvn.nl](http://www.ntvn.nl).



# Nederlandse Natuurkundige Vereniging

Tweedejaarsstudenten kunnen een jaar gratis lid worden. Alle andere studenten krijgen een flinke korting op de contributie.

## Voordelen van het NNV-lidmaatschap:

- Maandelijks het Nederlands Tijdschrift voor Natuurkunde in de bus
- Zeer aantrekkelijke ledenkorting op het jaarlijkse evenement FYSICA
- Optie op gratis lidmaatschap van de NNV-secties
- Toegang tot het complete digitale NTvN-archief
- Subsidie voor studiereizen en symposia van studieverenigingen
- Geassocieerd lidmaatschap van de European Physical Society
- Verbondenheid met de fysische gemeenschap!

De Nederlandse  
Natuurkundige  
Vereniging bestaat  
al sinds 1921 en is  
dé vereniging voor  
natuurkundigen  
in Nederland. De  
NNV is voor alle  
fysici: studenten,  
fysici werkzaam in  
het bedrijfsleven,  
onderwijs, academia...  
Immers:  
Eenmaal fysicus,  
altijd fysicus!

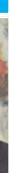
Postbus 41882, 1009 DB Amsterdam

T: 020-5922211

E: bureau@nnv.nl



Gezicht van de natuurkunde



[www.nnv.nl](http://www.nnv.nl)

