Noodzakelijke onzekerheid

Noodzakelijke onzekerheid

Rede

uitgesproken bij de aanvaarding van het ambt
van hoogleraar Quantum-kansrekening en quantum-informatietheorie
aan de Faculteit der Natuurwetenschappen, Wiskunde en Informatica
van de Universiteit van Amsterdam
op woensdag 15 januari 2014

door

Hans Maassen

Dit is oratie 489, verschenen in de oratiereeks van de Universiteit van Amsterdam.

Opmaak: JAPES, Amsterdam
Foto auteur: Jeroen Oerlemans

Mevrouw de rector magnificus,
mevrouw de dekaan,
waarde collega's, beste familie en vrienden,

1 Inleiding

Enkele jaren geleden is aan de Universiteit van Amsterdam een onderzoekszwaartepunt ingesteld met de naam 'quantum-materie en quantum-informatie'. Dit is een samenwerkingsverband van onderzoeksgroepen in de natuurkunde, in de informatica en in de wiskunde. Van de zijde van de wiskunde, het Korteweg-de Vries-Instituut, heeft men mij gevraagd de wiskundige expertise in dit zwaartepunt te komen versterken, op een leerstoel quantumkansrekening en quantum-informatietheorie.
Laat mij enkele van deze termen nader verklaren. *Quantumfysica* of *quantummechanica* is de natuurkunde van moleculen, atomen, elementaire deeltjes en licht. Deze theorie stamt uit de 20-er jaren van de vorige eeuw.
Vanaf het begin is dit een theorie die kansen berekent. Een echte *quantumkansrekening*, speciaal voor dit doel ontwikkeld, is pas zo'n 40 jaar oud. Bij de opbouw daarvan ben ik vrijwel vanaf het begin betrokken geweest.
Quantum-informatietheorie exploreert de nieuwe mogelijkheden van de quantumfysica op het gebied van informatieverwerking, -transmissie, cryptografie, en berekeningen. Deze theorie dateert uit de 80-er jaren van de vorige eeuw, en maakte zijn beginspurt door een artikel van Peter Shor in 1994 [Sh94], die liet zien hoe met quantum-middelen bepaalde algoritmen wezenlijk sneller kunnen worden uitgevoerd dan met onze huidige computers.
In deze rede wil ik kort uiteenzetten wat de genoemde kansrekening en informatietheorie bijzonder maakt. Ik zal me daarbij niet houden aan het standaardverhaal. Dit geeft mij de gelegenheid, mijn positie in het vakgebied nader te bepalen.
Naar mijn mening is een belangrijke rol weggelegd voor de wiskunde in de verheldering van het denken over de altijd wat geheimzinnige quantummechanica. Reinhard Werner, een van de coryfeeën van de wiskundige quantuminformatietheorie, schreef eens (mijn vertaling) [We08]:

> . . . oplettende studenten krijgen gemakkelijk de indruk dat quantumonzekerheid overslaat op hun docenten in de vorm van een zekere conceptuele vaagheid.

In populaire beschrijvingen van quantumfenomenen leest men verder vaak onnodig mystificerende termen en misplaatste metaforen.
De beroemde kat van Schrödinger heet vaak 'levend èn dood tegelijk'. In 'Buitenhof' van 29 december 2013 hoorde ik zelfs Robbert Dijkgraaf zijn op-

en-neer gereis tussen Princeton en Hilversum beschrijven in termen van een quantum-deeltje dat 'op twee plaatsen tegelijk kan zijn'.
Vaak wordt beweerd dat in de quantumtheorie 'alles met alles samenhangt', en dat invloeden sneller kunnen reizen dan het licht.
In spirituele kringen ziet met de quantummechanica graag als de New Age-theorie waarin de invloed van de geest op de stof eindelijk wordt erkend.
Deze voorstellingen van zaken zijn mijns inziens misleidend.
In deze rede wil ik de quantumkansrekening en quantum-informatie introduceren. Ik zal dat niet doen met de gebruikelijke Alice & Bob-verhalen, maar de nadruk leggen op de logica.

2 Logica

In zijn *Tractatus logico-philosophicus* (1918) schrijft de filosoof Ludwig Wittgenstein [Wi18]:

1. Die Welt ist alles was der Fall ist.

1.1 Die Welt ist die Gesamtheit der Tatsachen, nicht der Dinge.

Wittgenstein vervolgt met een beschrijving van de wereld, ingericht volgens de logica van de negentiende-eeuwse wiskundige George Boole. Over de wereld kan men allerlei beweringen doen, en deze kunnen waar zijn of niet. Een ware bewering noemen we een *feit*. Alle feiten samen bepalen de *toestand van de wereld*. Beweringen kunnen worden samengesteld en bewerkt met voegwoorden en bijwoorden zoals *en, of* en *niet*. Onder deze operaties vormen ze een zogenaamde Boole'se algebra, waarin bijvoorbeeld geldt:

$$A = (A \textit{ en } B) \textit{ of } (A \textit{ en niet-}B). \tag{1}$$

Een Boole'se algebra kan gemodelleerd worden met verzamelingen, door middel van de vertaalregels:

$$\begin{array}{rcl} A \textit{ en } B & \longleftrightarrow & \text{de doorsnede van } A \text{ en } B\ ; \\ A \textit{ of } B & \longleftrightarrow & \text{de vereniging van } A \text{ en } B\ ; \\ \textit{niet-}A & \longleftrightarrow & \text{het complement van } A\ . \end{array}$$

Door samenstelling van elementaire beweringen kunnen beweringen op een hoger niveau worden opgebouwd. Een bewering van heel hoog niveau is:

Amsterdam is een toeristische stad.

Een van de componenten van deze bewering is bijvoorbeeld

Mr. Brown uit Australië wandelt 's avonds over de wallen.

Een onderdeel dáárvan zou kunnen zijn

Mr. Brown ziet om elf uur een rode lamp.

Deze bewering is op zijn beurt opgebouwd uit vele kleintjes, waaronder

Tussen elf uur en 3 nanoseconden over elf uur wordt een retinacel van Mr. Brown getroffen door een foton met een golflengte tussen 600 en 605 nanometer.

Het is deze laatste, elementaire soort van beweringen, de *pixels van de werkelijkheid*, waarvan de logische structuur ons hier interesseert. De toestand van de wereld wordt vastgelegd door van al dit soort beweringen te zeggen of ze waar zijn of niet. Dat wil zeggen: door een soort *waarheidsfunctie* φ, gedefinierd door

$$\varphi(A) = \begin{cases} 1 & \text{als de uitspraak } A \text{ waar is,} \\ 0 & \text{als de uitspraak } A \text{ onwaar is.} \end{cases}$$

Door een gigantische samenstelling van elementaire pixels zou uiteindelijk ook de waarheidswaarde bepaald kunnen worden van de bewering dat Amsterdam een toeristische stad is. Wittgenstein kwam in zijn latere werk terug van deze radicale, op pure logica gebaseerde opvatting van de werkelijkheid. Toch kunnen we zijn basisgedachte voor dit verhaal goed gebruiken:

> De toestand van een natuurkundig systeem wordt bepaald door een waarheidsfunctie φ op de Boole'se algebra van de natuurkundige beweringen over dat systeem.

Dit was althans de situatie, al dan niet expliciet verwoord, tot de jaren '20, '30. Een van de grote verrassingen van de natuurkunde van de twintigste eeuw kan wiskundig zó worden geformuleerd:

> De beweringen over een natuurkundig systeem vormen geen Boole'se algebra, maar gedragen zich als deelruimten van een Hilbertruimte.

Ik zal aanstonds uitleggen wat dit betekent. De eersten die deze ontdekking formuleerden waren de wiskundigen Garrett Birkhoff en John von Neumann (1936) [BvN36]. Later is dit uitgangspunt uitgewerkt door onder anderen Mackey, [Ma63], Gleason [Gl57] Jauch en Piron. Het vormt nu het fundament van de quantum-logica en de quantum-kansrekening. De schok die deze ontdekking heeft teweeggebracht, is anno 2014 nog niet geheel verwerkt. Hieronder zal ik proberen de consequenties van deze verrassende logische structuur te schetsen.

3 Een eenvoudig voorbeeld

Laten we aan de hand van een heel eenvoudig voorbeeld bekijken wat de ontdekking van von Neumann te betekenen heeft. Stel een klassiek systeem(pje) heeft drie standen: 1, 2 en 3. We zeggen: het heeft *configuratieruimte* $\Omega = \{1, 2, 3\}$. Er zijn acht logische beweringen te bedenken over dit systeem, die volgens Boole corresponderen met de acht deelverzamelingen van Ω:

$$\begin{array}{rcl} \phi & \longleftrightarrow & \text{de onware bewering (bijvoorbeeld '}1 = 0\text{')} \\ \{1\} & \longleftrightarrow & \text{'De stand is 1.'} \\ \{2,3\} & \longleftrightarrow & \text{'De stand is niet 1.'} \\ \{1,2,3\} & \longleftrightarrow & \text{de ware bewering (bijvoorbeeld } 1+1=2\text{)} \end{array}$$

Daarnaast zijn er nog de verzamelingen $\{2\}$ en $\{3\}$ en hun complementen. Deze Boole'se algebra kan alternatief worden beschreven met de volgende set van lineaire deelruimten van een driedimesionale ruimte.

$$\begin{array}{rcl} \phi & \longleftrightarrow & \text{de oorsprong} \\ \{1\} & \longleftrightarrow & \text{de } x\text{-as} \\ \{2,3\} & \longleftrightarrow & \text{het } y\text{-}z\text{-vlak} \\ \{1,2,3\} & \longleftrightarrow & \text{de hele ruimte} \end{array}$$

Het y-z-vlak is het *orthogonaal complement* van de x-as, corresponderend met 'de stand is niet 1'. Zo zijn er ook nog: de y-as, de z-as en hun orthogonale complementen. Deze deelruimten hebben de eigenschap dat hun orthogonale projectie-operatoren met elkaar commuteren: voor elk paar projecties p en q geldt:

$$pq = qp \ .$$

In termen van deze projectie-operatoren worden de logische operaties vertaald als in tabel 1. De acht deelruimten en de acht projecties daarop vormen nog steeds een ouderwetse, Boole'se algebra.
Nu komt de quantumsprong: niet alleen deze acht, maar *alle* deelruimten, dus alle lijnen en vlakken door de oorsprong, moeten worden beschouwd als uitspraken over een nieuw, overigens nog steeds heel beperkt, quantummechanisch systeem. Veel van deze beweringen (dus deelruimten) staan scheef op elkaar. In dat geval commuteren hun projecties niet:

$$pq \neq qp \ .$$

Tabel 1: Correspondenties in quantum-logica

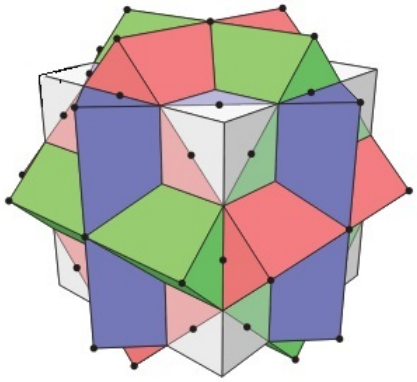
A	$\longleftrightarrow$	de lineaire deelruimte L_A	$\longleftrightarrow$	de projectie p_A;
niet-A	$\longleftrightarrow$	orthogonaal compl. van L_A	$\longleftrightarrow$	de projectie $\mathbb{1} - p_A$;
A en B	$\longleftrightarrow$	de doorsnede van L_A en L_B	$\longleftrightarrow$	het product $p_A p_B$;
A of B	$\longleftrightarrow$	het opspansel van L_A en L_B	$\longleftrightarrow$	$p_A + p_B - p_A p_B$.

Als twee projecties niet commuteren, noemen we de bijpassende beweringen *incompatibel*. Zij gaan niet samen. Het product pq is dan helemaal geen projectie, en kan dus ook niet als bewering worden opgevat. Samengestelde beweringen zoals '*A en B*' en '*A of B*' behouden hun betekenis alleen als A en B compatibel zijn. De bewering '*niet-A*' correspondeert met de lijn of het vlak loodrecht op het vlak of de lijn van A zelf. Als A en B elkaar uitsluiten, zijn ze compatibel, en staan de lijnen of vlakken loodrecht op elkaar. Onder een *waarheidsfunctie* op de beweringen (deelruimten) verstaan we een functie φ die de waarden 0 en 1 aanneemt, die 1 is op de altijd ware bewering, en die voldoet aan *additiviteit* voor elkaar uitsluitende beweringen:

$$\varphi(A \textit{ of } B) = \varphi(A) + \varphi(B).$$

Het stelsel beweringen (deelruimten van de driedimensionale ruimte) dat we zo hebben verkregen handelt over een natuurkundig systeempje dat inderdaad in het laboratorium kan worden bestudeerd: het betreft de richting van de spin van een elementair deeltje met spin 1, bijvoorbeeld een zogenaamd ρ-meson.
De meeste natuurkundige systemen zijn veel groter, en hebben nòg veel grotere, meestal oneindig-dimensionale Hilbertruimten. In het voorbeeld van Mr. Brown op de Wallen was de laatste bewering over het foton dat zijn netvlies trof een combinatie van twee enorme deelruimten van een oneindig-dimensionale Hilbertruimte, die *incompatibel* blijken te zijn: een bewering over het tijdstip van inslag van een foton gaat niet samen met een bewering over de golflengte. Het aardige van ons ρ-mesonvoorbeeld is, dat de Hilbertruimte ervan lijkt op onze vertrouwde driedimensionale ruimte. Sterker nog: in het geval van het ρ-meson mogen we de ruimtelijke richtingen van de spin direct koppelen aan de richtingen in de Hilbertruimte! (Deeltjes met spin 1 zijn het enige voorbeeld waarmee dat kan.)
Met het meson in het laboratorium kunnen we, met behulp van magnetische velden, een spelletje spelen: wij wijzen een richting aan, en vragen aan het meson: 'Heeft jouw spin waarde 0 in deze richting?'. Het meson antwoordt, door middel van zijn afbuigingsrichting, met '*ja*' of met '*nee*'. Met behulp van dit spelletje kunnen we de logica checken. Op drie onderling loodrechte

Figuur 1: De sudoku van Peres.



'vragen' moet het meson één keer '*ja*' en twee keer '*nee*' antwoorden. Dat blijkt het ρ-meson inderdaad steeds zo te doen. De gekozen logica is dus geen geloofsartikel, maar een experimenteel resultaat.
Bij dit spelletje kunnen we ons nu afvragen: 'Doet het meson maar wat, of kunnen we in principe een natuurkundige theorie bedenken die zijn gedrag precies voorspelt?' En trouwens: hoe dient een voorspelling van dit gedrag eruit te zien?
Omdat wij vrij zijn om aan het meson de vragen te stellen die we maar willen, is een voorspelling: een lijstje antwoorden '*ja*' of '*nee*', 1 of 0, op *alle mogelijke* vragen; dat wil zeggen: *een voorspelling wordt gegeven door een waarheidsfunctie.*
Hier duikt een serieus probleem op. Gleason heeft in 1957 aangetoond:

> Er bestaat geen waarheidsfunctie φ op de lijnen en vlakken in een driedimensionale ruimte.

Asher Peres [Pe91] heeft in 1991 expliciet een set van 33 ruimterichtingen aangegeven die niet met enen en nullen ingevuld kunnen worden op zo'n manier dat van drie onderling loodrechte richtingen er steeds precies één een 1, en de andere twee een 0 krijgen. Zie Figuur 1.Hierin staan vier kubussen: één witte en drie gekleurde. Door de middens van alle ribben en de hoekpunten van de gekleurde kubussen met hun tegenvoeters te verbinden, ontstaan 33 lijnen waarvan er veel onderling loodrecht staan. Dit correspondeert met 33 vragen over de spin van het meson. Deze constructie is een soort driedimensionale sudoku-puzzel die niet uitkomt. Er ìs dus niet eens een lijstje consistente antwoorden *mogelijk* op de set van 33 vragen van Peres.

Conclusie: Over de spinrichting van een ρ-meson kan geen absolute waarheid bestaan. Hiermee stort het programma van Wittgenstein in: een mate van onzekerheid is noodzakelijk.

4 Kansen

Op de beweringen in de quantumlogica bestaat dus geen waarheidsfunctie, geen additieve functie met alleen de waarden 0 en 1.Wel bestaan er additieve functies die ook waarden *tussen* 0 en 1 aannemen. Deze functies zijn, volgens dezelfde stelling van Gleason, noodzakelijk uitbreidbaar tot *affiene*, (zeg maar: lineaire) functies op alle operatoren, niet alleen de projectie-operatoren. In extreme gevallen komt er

$$\varphi(A) = ||p_A\psi||^2 \ .$$

De kans op A is gelijk aan het kwadraat van de lengte van de projectie van de *toestandsvector* ψ op de deelruimte die bij A hoort. Voor A en *niet-A* sommeren die volgens Pythagoras tot het kwadraat van de lengte van ψ, die dus 1 moet zijn. De vector ψ heet ook wel *golffunctie* van het systeem.

Wat nu te doen met waarheidsfuncties die tussen 0 en 1 in zitten? Het lijkt erop dat de natuur dit dilemma heeft opgelost door deze waarden als *kansen* te interpreteren: in het ene experiment komt er 0 uit, in het andere 1, en pas op de lange duur middelt dit uit tot $\varphi(A)$.
Dit is de gebruikelijke interpretatie van de quantummechanica, een regel die teruggaat tot een voorstel van Max Born uit 1926. Dit voorstel vond onmiddellijk ingang in de quantumfysica. Maar niet bij iedereen. In een brief aan Max Born in datzelfde jaar 1926 sprak Einstein zich uit over de nieuwe quantumtheorie met haar kansinterpretatie in de woorden:

> *Die Theorie liefert viel, aber dem Geheimnis des Alten bringt sie uns kaum näher. Jedenfalls bin ich überzeugt, daß* der *nicht würfelt.*

Einstein bleef op zoek naar een theorie waarin de antwoorden van de natuur op de experimentele vragen wél (in principe) voorspelbaar zijn. Het is niet meer na te gaan, wat hij gezegd zou hebben van de stelling van Gleason en de sudoku van Peres, die hem in grote moeilijkheden zouden hebben gebracht. Hij overleed in 1955, twee jaar voor het eerste resultaat van Gleason. Achteraf geïnterpreteerd, kwam hij echter met een vooruitziende tegenzet tegen Gleason en Peres. In zijn eigen tijd werd deze door maar weinigen op zijn waarde geschat, waaronder wel Schrödinger en Dirac.

5 Verstrengeling

In 1935, in een artikel met zijn medewerkers Podolski en Rosen, presenteerde Einstein een gedachtenexperiment [EPR35], waarmee hij de uitvinder

werd van de quantummechanische verstrengeling, en daarmee van de hele quantum-informatietheorie.
Als één quantumsysteem de Hilbertruimte $\mathcal{H}$ heeft, dan kunnen twee soortgelijke systemen beschreven worden met de grotere Hilbertruimte $\mathcal{H} \otimes \mathcal{H}$, het tensorproduct van $\mathcal{H}$ met zichzelf. Op de deelruimten hiervan bedacht Einstein een kansfunctie φ met de bijzondere eigenschap

$$\forall_p : \quad \varphi(p \otimes p^{\perp}) = 0 \; .$$

Hier staat: de kans is 0 dat beide systemen op dezelfde vraag verschillende antwoorden geven. Door dus een vraag te stellen aan het ene systeem, kan informatie gewonnen worden over het andere. Zulke systemen heten *verstrengeld*.
In de populaire literatuur wordt verstrengeling steevast voorgespiegeld als een geheimzinnige quantummechanische actie op afstand. Men plaatst in gedachten één lid van het verstrengelde paar op Jupiter, en het andere hier op aarde. Door aan het systeem op aarde een meting te doen, veranderen we de kansfunctie van het systeem op Jupiter: eerst was deze immers onzeker, nu is ze scherp bepaald. Deze invloed kan sneller gaan dan het licht.
Maar laten we wel bedenken dat verstrengeling voor ouderwetse, klassieke systemen geen verwonderlijke eigenschap is. Verstrengeling betekent gewoon dat beide systemen in dezelfde stand staan; eventueel kan deze stand onzeker zijn. In de kansrekening zegt men dat zulke systemen *gecorreleerd* zijn. Verstrengeling wordt daarom ook wel *quantumcorrelatie* genoemd. Zo'n verstrengeld klassiek paar kunnen we gemakkelijk als volgt realiseren: We nemen twee munten. We vragen een vriend een van de twee op te werpen, en de andere in dezelfde stand te leggen, (te *kopiëren* dus), zonder ons te vertellen welke stand dat is. Dan laten we, heel voorzichtig, één van de twee naar Jupiter brengen. Over de munt op aarde laten we een kapje plaatsen, zodat we hem niet kunnen zien. Op dat moment is de kans dat de munt op Jupiter op kop ligt: $\frac{1}{2}$.
Als we nu het kapje optillen, zien we de munt op aarde – bijvoorbeeld – op kop liggen. De kans dat de munt op Jupiter nu ook op kop ligt is: 1. Dus de kans φ('munt op kop op Jupiter') is versprongen van $\frac{1}{2}$ naar 1 doordat wij, ver weg op aarde, het kapje hebben opgetild.
Is hier sprake van actie op afstand, sneller dan het licht? Ik hoop dat U het met mij eens bent: Nee, natuurlijk niet. Naar mijn mening zou men dit ook een onzinnige suggestie moeten noemen in de situatie van quantum-correlatie. De logica is niet volgens Boole, maar actie op afstand is dit niet.
Voor quantumsystemen ligt de kwestie natuurlijk wèl iets subtieler. Waar de klassieke munten de waarheid over hun stand met zich mee kunnen dragen,

daar weten we inmiddels dat zo'n onderliggende *waarheid* voor mesonen niet bestaat. Ze is noodzakelijk onzeker. Verstrengeling lijkt zich daardoor slecht te verhouden met de quantummechanische onzekerheid. Dit was het punt dat Einstein in 1935 wenste te maken.

6 Quantum-informatie

Als we over twee verstrengelde mesonen beschikken, één op aarde, één op Jupiter, dan kunnen we het antwoord van het meson op Jupiter op elke gewenste vraag voorspellen, namelijk door de vraag eerst aan het meson op aarde te stellen, net als in het voorbeeld van de twee munten. Er geldt nu dus:

A. Op elke vraag is het antwoord van het Jupiter-meson op aarde te voorspellen.

B. Er bestaat geen consistente set antwoorden op alle vragen.

Dit is een aangescherpte versie van de paradox van Einstein, Podolski en Rosen.
Ik wil U uitnodigen om Einsteins zorgen te negeren, en de condities A en B hierboven als feit te accepteren: Blijkbaar bestaat er informatie, gedragen door materiële dragers, over incompatibele grootheden. Het meson op Jupiter 'kent' het antwoord *op elke* vraag die we zouden kunnen stellen, maar *niet op alle* vragen tezamen. Bij ondervraging beantwoordt het de eerste vraag correct, daarna begint het meson te fantaseren. We noemen de 'kennis' waar het dit meson over beschikt *quantum-informatie*. Voor zulke informatie is de wet (1) ongeldig. Einstein wilde de onjuistheid, of minstens de onvolledigheid van de quantummechanica aantonen, maar werd ongewild de ontdekker van één van haar grote successen: quantum-informatie.

7 De aard van quantum-informatie

Quantum-informatie is uiterst kwetsbaar. Zoals wij zullen zien, kan zij niet worden gekopiëerd.
Wanneer ik U een klassiek feit meedeel, bent U daarna op de hoogte, en ik natuurlijk ook nog. Als ik U quantum-feiten vertel, weet na afloop hoogstens één van U ervan, en ikzelf niet meer.
Als klassieke informatie uitlekt, is zij overal aanwezig. Als quantum-informatie uitlekt, is ze verdwenen.

Klassieke informatie kan over een telefoonlijn worden verzonden, quantum-informatie niet. Wel kan zulke informatie worden *geteleporteerd* over een telefoonlijn, mits zender en ontvanger tevoren over voldoende verstrengelde paren deeltjes beschikken. Het origineel wordt daarbij natuurlijk automatisch vernietigd wegens de noodzakelijke onzekerheid.
De kwetsbaarheid van quantum-informatie wordt benut in de cryptografie: het versturen van geheime boodschappen. Immers: het feit alleen dat een quantum-boodschap is overgekomen is op zich al een bewijs dat hij niet is afgeluisterd. Anders zou immers een kopie zijn gecreëerd. De Amerikaanse *National Security Agency* zou in zijn spionagepogingen machteloos staan als wij al onze emails in quantumvorm zouden versturen. Een veilige quantumlijn is al voor enkele tienduizenden Euro's te koop bij het bedrijf ID Quantique van Nicolas Gisin in Genève. Ik heb hem leren kennen op de eerste conferentie over quantum-kanstheorie in 1982, en het doet mij genoegen hem deze gratis reclame aan te bieden.

8 Quantum-computing

Quantum-informatie heeft echter niet alleen kwetsbare kanten. Een quantumsysteem bevat gelijktijdige informatie over vele incompatibele grootheden. Met slimme algoritmen blijkt het mogelijk, een quantumsysteem vele berekeningen parallel te laten uitvoeren, en daarna de resultaten in één enkel antwoord te laten concentreren. Het grote, en tot nog toe in wezen het enige, voorbeeld hiervan is het algoritme van Peter Shor uit 1994 [Sh94]. Een quantumsysteem is in staat, periodiciteiten te detecteren in de machten van quantum-operaties, en kan daarom gebruikt worden om een groot getal in factoren te ontbinden. Het aantal benodigde stappen is evenredig met een macht van het het aantal cijfers van het getal, en niet met het getal zelf. Een quantum-computer maakt het in principe doenlijk de code te kraken die banken voor beveiliging van hun gegevens gebruiken.

9 Onzekerheid

Laten we in het voorbeeld van het ρ-meson twee verschillende assenstelsels kiezen in de driedimensionale Hilbertruimte: (x, y, z) en (x', y', z'). De kansen $(\varphi(x), \varphi(y), \varphi(z))$ tellen op tot 1, evenals de kansen $(\varphi(x'), \varphi(y'), \varphi(z'))$. Deze twee kansverdelingen horen bij twee incompatibele grootheden, zeg G en G'. Volgens de wiskundige en electronisch ingenieur Claude Shannon moeten we

de onzekerheid in G zó berekenen:

$$H(G) = \varphi(x) \log \frac{1}{\varphi(x)} + \varphi(y) \log \frac{1}{\varphi(y)} + \varphi(z) \log \frac{1}{\varphi(z)} \ .$$

(Het is de gemiddelde waarde van de 'mate van verrassing', die ons te wachten staat als we de uitslag te horen krijgen.) Met Jos Uffink heb ik in 1988 bewezen [MU88] dat de som van de onzekerheden van G en van G' noodzakelijk de volgende ondergrens heeft:

$$H(G) + H(G') \geq \log \frac{1}{c^2}$$

Waarbij de constante c de cosinus is van de kleinste hoek tussen de coördinaatassen van de beide stelsels.

10 'No cloning'

Ik had U nog beloofd, uit te leggen waarom quantum-informatie niet kan worden gekopiëerd. Dit belangrijke principe gaat terug tot Wootters en Zurek [WZ82] en onafhankelijk daarvan tot Dennis Dieks [Di82] uit Utrecht, die helaas vandaag niet hier kan zijn, in samenwerking met Dick Hoekzema. Ik wil het uitleggen in de vorm van een wiskundige redenering, in de volgorde: definitie, stelling, bewijs. Ter voorbereiding zal ik zelfs eerst nog een hulpstelling bewijzen.
Het resultaat dat ik voor U wil gaan bewijzen is hetzelfde als dat van Wootters, Zurek en Dieks, maar het bewijs verloopt anders.
Laten we eerst bedenken wat het precies betekent, dat informatie, gedragen door een fysisch systeem, wordt gekopiëerd. 'Kopiëren' is een *operatie*, laten we hem C noemen, die als input het systeem heeft met zijn waarheidsfunctie of kansfunctie φ, en die als output een paar identieke systemen levert, elk apart met dezelfde kansfunctie. In eerste instantie zou je misschien geneigd zijn te definiëren:

$$C\varphi := \varphi \otimes \varphi \ .$$

Voor *extremale kansfuncties* φ blijkt dit achteraf een redelijke definitie, maar in het algemeen heeft zij ongewenste consequenties. Zo heeft een munt bijvoorbeeld kansverdeling $(\frac{1}{2}, \frac{1}{2})$, en met bovenstaande definitie levert dat twee munten op met kansverdeling

$$(\tfrac{1}{2}, \tfrac{1}{2}) \otimes (\tfrac{1}{2}, \tfrac{1}{2}) \ .$$

die kans $\frac{1}{4}$ toekent aan elk van de vier mogelijkheden (kop,kop), (kop,munt), (munt,kop) en (munt,munt). Dat is niet wat we willen. We willen dat de

kopieën *identiek* zijn, niet *onafhankelijk*! En omdat er in quantumsystemen noodzakelijk onzekerheden zitten, is dit een verkeerde definitie. De volgende definitie strookt beter met onze wensen:

Definitie We noemen C een *kopieeroperatie* als

$$\forall_\varphi \forall_p : \qquad C\varphi(\mathbb{1} \otimes p) = C\varphi(p \otimes \mathbb{1}) = \varphi(p) \ .$$

In woorden: als we na het kopiëren één kopie apart nemen, kunnen we met geen enkele statistische methode constateren of we te maken hebben met het origineel of met een kopie.

Lemma Kopieën zijn maximaal verstrengeld:

$$\forall_\varphi \forall_p : \qquad C\varphi(p \otimes p^\perp) = 0 \ .$$

Deze eigenschap volgt niet direct uit de definitie van een kopiëeroperatie, die immers alleen iets zegt over het gedrag van elke kopie op zich. 'Met kans 1 hetzelfde antwoord geven' is echter iets veel sterkers dan 'hetzelfde antwoord geven met de zelfde kans'.

Bewijs. Het is voldoende als we bewijzen dat de kans op onenigheid tussen de kopieën nul is voor de extreme gevallen $\varphi(p) = ||p\psi||^2$, met ψ een toestandsvector. Omdat onze kans een affiene functie is van φ, is is hij een (positieve) kwadratische vorm in ψ, en moet er dus uitzien als:

$$C\varphi(p \otimes p^\perp) = ||X\psi||^2 \ .$$

Maar dan moet

$$||X\psi||^2 \leq C\varphi(p \otimes \mathbb{1}) = \varphi(p) = ||p\psi||^2 \ ,$$

$$||X\psi||^2 \leq C\varphi(\mathbb{1} \otimes p^\perp) = \varphi(p^\perp) = ||p^\perp\psi||^2 \ ,$$

dus $X\psi = 0$ als ψ loodrecht staat op $p\mathcal{H}$, maar ook als ψ loodrecht staat op $p^\perp\mathcal{H}$, dat wil zeggen: in $p\mathcal{H}$ ligt. En omdat elke vector kan worden ontbonden in een gedeelte in $p\mathcal{H}$ en een gedeelte loodrecht daarop, is $X\psi$ altijd 0. Dus $X = 0$. Hiermee is het lemma bewezen.

We beargumenteren vervolgens de hoofdstelling, namelijk dat het kopiëren van de informatie in een ρ-meson onmogelijk is. Stel dat dit wel zou kunnen. Dan zouden we niet alleen twee, maar ook 16 kopien van ons meson kunnen maken, één voor elke rij en kolom van de sudoku van Peres. Aan elke kopie stellen we nu de drie vragen in onderling loodrechte richtingen, behorende bij de betreffende rij of kolom. Elke kopie antwoordt één keer '*ja*' en twee keer '*nee*'. Verschillende kopieën geven bij dezelfde richting hetzelfde antwoord, volgens het lemma. Dit leidt tot een consistente invulling van de sudoku, hetgeen onmogelijk is.

11 Macroscopische superposities

Laten we nu kijken naar de claim dat 'quantumdeeltjes op verschillende plaatsen tegelijk kunnen zijn'. Laat A en B gescheiden ruimtelijke gebieden zijn, en laten we dezelfde letters gebruiken voor de uitspraken dat het deeltje zich in deze gebieden bevindt. Delen van de Hilbertruimte behorende bij deze twee gebieden staan haaks op elkaar, zodat de uitspraken A en B elkaar eenvoudig uitsluiten. Een meting van de plaats van het deeltje zal dan ook nooit opleveren dat het in A èn in B zit. Vanwaar dan toch de bewering dat het deeltje in beide gebieden tegelijk kan zijn? Dat lijkt te komen doordat soms een derde bewering bestaat, zeg C, die incompatibel is met A zowel als B (maar niet met de bewering A *of* B). Als wij nu reden hebben te geloven dat C *waar* is, dan zijn A en B beide noodzakelijk onzeker. (Maar A *en* B blijft evengoed onwaar.)

12 Gegarandeerde onzekerheid

Tot zover is tweemaal een uitdrukking van het type

$$\varphi(p \otimes p^{\perp}) = 0$$

voorbijgekomen, één keer bij de discussie van verstrengeling, en één keer bij het definiëren van de kopieeroperatie. Maar: verstrengeling is fysisch mogelijk, en kopiëren niet. Hoe zit dit? Welnu, volledige verstrengeling is alleen mogelijk in *paren*. Met een passende term wordt dit *monogamie* genoemd. Derden komen er niet aan te pas: zij kunnen niet verstrengeld zijn, zelfs niet *correleren* met het paar. Hieruit volgt dat de random uitslagen van metingen aan het verstrengelde paar gegarandeerd onvoorspelbaar zijn.
In 2010 hebben Pironio en anderen [Pi10] volgens dit principe met 99% betrouwbaarheid 42 *echte* randomgetallen geproduceerd.
Er is een toepassing waarin onzekerheid beslist noodzakelijk is: de trekking bij een loterij.
Hier ligt een mooie toekomst voor de quantum-informatie.

13 Quantum-Markovketens

Tot zover mijn opmerkingen over de grondslagen van de quantumtheorie. Bij mijn pogingen U een indruk te geven van dit vakgebied, kom ik niet onder grondslagenvragen uit, maar mijn dagelijks werk is het niet. Ik wil nu een beschrijving geven van het lopende onderzoek, en van de uitdagingen die er

liggen voor de komende jaren. Een belangrijk onderwerp in de kansrekening is dat van de toevalsprocessen, met name Markovketens. Hierbij springt of vloeit een of ander systeem willekeurig van de ene toestand in de andere volgens een kanswet die geen geheugen kent. Voorbeelden zijn de Brownse beweging van een stuifmeelkorrel in een vloeistof, de binnenkomst van klanten in een winkel volgens een Poisson-proces, het gedrag van wachtrijen bij een server, en vele andere.
Van dit type toevalsproces bestuderen mijn collega Burkhard Kümmerer en ik de quantum-generalisatie. Die wordt verkregen door in de axioma's van de kansrekening de Boole'se algebra te vervangen door de projecties in een von Neumann-algebra. Dit roept nieuwe vragen op. Zo zijn bijvoorbeeld de observabelen op verschillende tijdstippen niet compatibel, zodat het geen zin heeft, naar de paden te vragen die het systeem in de loop van de tijd zou afleggen. Wel worden ook de quantum-Markovketens nog steeds aangedreven door ruis, quantumruis in dit geval, en daarvan zijn er veel meer dan klassiek het geval is, waar we eigenlijk alleen de genoemde Brownse beweging en het Poissonproces kennen. Zo bestaat er bijvoorbeeld vrije ruis, waarvan de verdeling niet normaal (Gaussisch) is, maar verdeeld is volgens een halve cirkel. Deze is extreem niet-commutatief. Ook bestaat er Fermi-ruis, die anticommuteert. Markovketens onder observatie leveren, via conditionering, de zogenaamde quantum-trajectoriën, waarvan we het ergodisch gedrag bestuderen. Practische voorbeelden moeten worden gezocht in de sfeer van verstrooiïngsprocessen: electronen aan een metaaloppervlak, of fotonen aan een atoom. Markovketens vormen een prachtige achtergrond om de hele quantum-kanstheorie tegen te ontvouwen, zoals wij in een Springer-leerboek aan het beschrijven zijn.

14 Verstrengelingsonderzoek

Op welke manieren materie verstrengeld kan zijn, is nog een open theoretische vraag. Met name de kwantitatieve beschrijving van de verstrengeling van meer dan twee deeltjes is tot nu toe een jungle gebleken. Veelbelovend lijkt de aanpak van de onlangs overleden Amerikaanse wiskundige William Arveson [Arv08] die raakt aan de fundamentele herformulering van de functionaalanalyse door de legendarische Alexander Grothendieck. Symmetrie lijkt verstrengeling iets te vereenvoudigen. Met hulp van de Amsterdamse expertise in representatietheorie heb ik goede hoop hier aardige resultaten te kunnen vinden.

15 Capaciteit van quantumkanalen

Een onderwerp dat mij tenslotte de laatste jaren heeft beziggehouden, is de vraag hoeveel informatie je door een kanaal, zoals een glasvezel of een radiobundel, kunt sturen. Met name de vraag, of door twee kanalen inderdaad precies de dubbele hoeveelheid kan worden verzonden, of meer wanneer je verstrengelde input gebruikt, heeft de quantum-informatie-gemeenschap een decennium lang gentrigeerd. De conclusie is, dat verstrengelde input de capaciteit inderdaad kan vergroten, maar het bewijs is hoogst niet-constructief. Men weet dat het moet kunnen, maar kan niet aangeven hoe. Als maat voor de hoeveelheid informatie wordt hierbij steeds de Shannon-entropie gebruikt. Interessante vraag: ligt het misschien aan de gekozen maat dat het antwoord zo vreemd uitpakt? Zou het kunnen zijn dat met een meer natuurlijke informatie-maat, bijvoorbeeld de Rényi-entropie bij een andere parameterwaarde, de capaciteit van quantumkanalen toch gewoon additief is? Hier proberen we in Nijmegen door een combinatie van computerberekeningen en analytische argumentatie een antwoord op te geven.

16 Dankwoord

Aan het College van Bestuur van de Universiteit van Amsterdam en de dekaan van de Faculteit van Natuurwetenschappen, Wiskunde en Informatica spreek ik mijn dank uit voor het in mij gestelde vertrouwen. Ik ben verheugd dat mij de mogelijkheid wordt geboden om op mijn geliefde onderzoeksgebied met een aantal vooraanstaande onderzoekers samen te werken. Hiervoor dank ik ook de leden van en betrokkenen bij het Zwaartepunt Quantum-Materie en Quantum-Informatie, met name Eric Opdam, Jan Wiegerinck, Harry Buhrman, Kareljan Schoutens en Bernard Nienhuis. Ook wil ik de directeuren Sijbrand de Jong en Erik Koelink van he Nijmeegse *Institute for Mathematics, Astrophysics and Particle Physics* bedanken voor hun inspanningen om deze benoeming te realiseren.
Mijn ouders ben ik dankbaar voor de brede opvoeding die ze me hebben gegeven, en ik bedank mijn vader dat hij mij de weg naar de wiskunde heeft helpen ontdekken.
Marinus Winnink en Nico Hugenholtz hebben mij de functionaalanalyse van C*-algebra's leren kennen. Daarvoor hier mijn dank.
Een belangrijke rol op cruciale momenten in mijn carrière is gespeeld door Mike Keane en door Wim Vervaat, de laatste hier vertegenwoordigd door zijn weduwe Marijke Plantema. Ik dank hen hartelijk hiervoor.
Ellen, Bas, Toon, Pieter en Inge dank ik voor het jarenlang verduren van een

vader die altijd wel een wolkje wiskunde boven zijn hoofd heeft hangen.
En tenslotte wil ik jou, Marjan, danken voor je niet-aflatende steun aan het botvieren van een toch ietwat buitenissige belangstelling.

Ik heb gezegd.

Referenties

[Arv08] William Arveson, Maximal vectors in Hilbert space and quantum entanglement, `http://arxiv.org/abs/0804.1140`, mei 2008.

[BvN36] Garrett Birkhoff, John von Neumann: The logic of quantum mechanics, *Annals of Mathematics* 37 No 4 (1936), 823–843.

[Di82] Dennis Dieks: Communication by EPR devices, *Phys. Lett.* 92A (1982), 271–272.

[EPR35] A. Einstein, B. Podolsky, en N. Rosen: Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* 47 (1935),777–780.

[Gl57] A. M. Gleason: Measures on the closed subspaces of a Hilbert space, *J. Math. Mech.* 6 (1957), 885-893.

[MU88] Hans Maassen, Jos Uffink: Generalized entropic uncertainty relations, *Physical Review Letters* 60 (1988), 1103–1106.

[Ma63] G. W. Mackey: *The mathematical foundations of quantum mechanics*, Benjamin, 1963.

[Pe91] Asher Peres: Two simple proofs of the KochenSpecker theorem, *J. Phys. A: Math. Gen.* 24 (1991), 175–I78.

[Pi10] Pironio et al.: Random numbers certified by Bell's theorem, *Nature* 464 (2010), 1021–1024.

[Sh94] Peter Shor: Algorithms for quantum computation: Discrete logarithms and factoring. *Proc. 35nd Annual Symposium on Foundations of Computer Science (Shafi Goldwasser, ed.)*, IEEE Computer Society Press (1994), 124–134.

[We08] R.F. Werner: The Uncertainty Relation for Joint Measurement of Position and Momentum, *Quantum Information & Computation* 4 Issue 6, (2004), 546–562.

[Wi18] *Tractatus Logico-Philosophicus, Logisch-Philosophische Abhandlung*, Annalen der Naturphilosophie, Oswalds 1921.

[WZ82] William Wootters, Wojciech Zurek: A Single Quantum Cannot be Cloned, *Nature* 299 (1982), 802-803.