Quantumcomputers: hoe en wanneer?

Door gebruik te maken van superpositie en verstrengeling 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 architecturen 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

Het 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 onderzoeksgroepen 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.

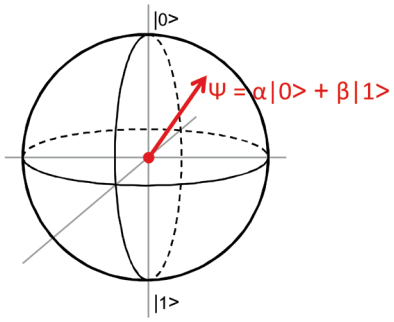
Foutencorrectie in quantumbits

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 geëncodeerd 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.

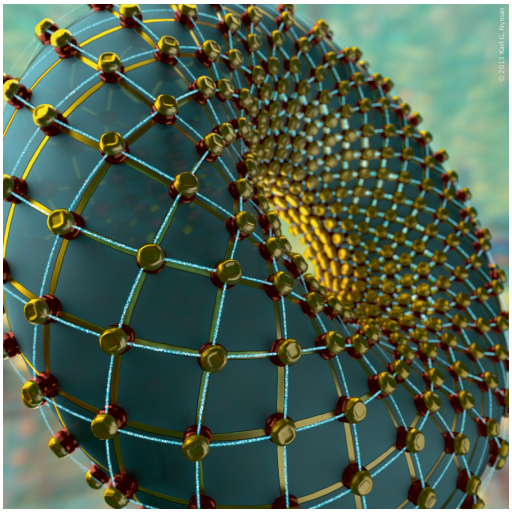
Peter Shor deed in 1995 de cruciale ontdekking dat fouten in quantumbits toch gecorrigeerd kunnen worden met behulp van verstrengeling [1]. Als de kans op een fout per quantumbit onder een bepaalde drempelwaarde zit (de zogeheten *fault-tolerant error threshold*) kunnen speciale algoritmes het aantal 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

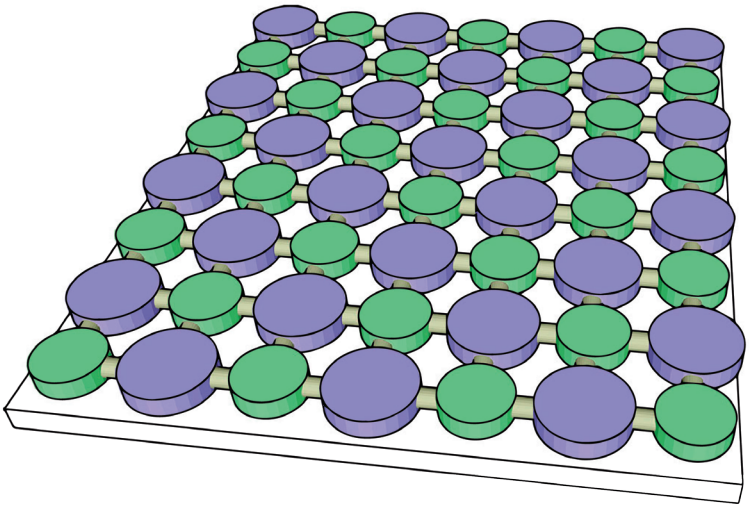
Het eerste voorgestelde model voor een quantumcomputer – het circuitmodel – is een directe vertaling van de conventionele computer. Een computerberekening bestaat in dit model uit een reeks logische operaties (poorten) uitgevoerd op de quantumbits, die voorafgaand aan de berekening allemaal geprepareerd 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 Ψ van een quantumbit is in een quantummechanische superpositie van de basistoestanden |0> en |1>. Wiskundig schrijven we dat als Ψ= α|0> + β|1>, 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 jaren 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 quantumcomputermodel 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.

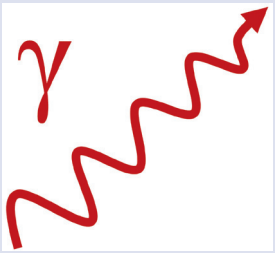
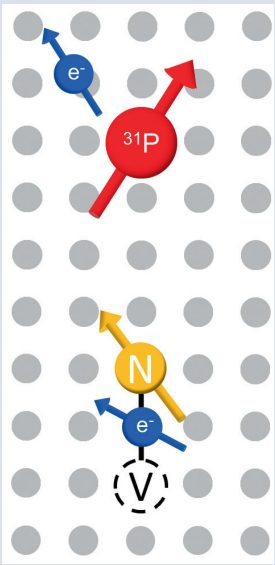
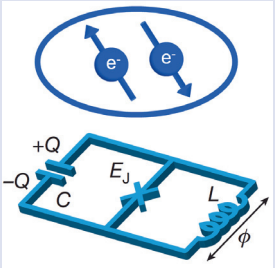
Topologisch quantumrekenen en de *surface code*

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 Majoranadeeltjes 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
Fotonen *Qubit-toestanden 0 en 1:* Polarisatie links- en rechtsom		• Weinig decoherentie • Mobiel: beste kandidaat voor lange-afstand-communicatie van quantuminformatie	• Zwakke interacties: twee-qubitpoorten lastig te realiseren • Beweegt te snel op tijdschalen van controle-elektronica
Ingevangen atomen in vacuüm, bijvoorbeeld Yb. *Qubit-toestanden 0 en 1:* Hyperfijn energieniveaus binnen atomen		• Goed controleerbare qubits met lange coherentietijden (>1 s) • Twee-qubitpoorten kunnen via fononen of fotonen • Interface naar fotonen voor lange-afstandcommunicatie	• Koppeling via fononen niet schaalbaar naar meer dan ~30 atomen • Koppeling via fotonen nog te langzaam (~1 s)
Quantumdots in vaste stof: Elektronspin in quantumdot *Qubit-toestanden 0 en 1:* Spin omlaag en spin omhoog		• Schaling van devices op een chip in principe mogelijk • Volledig elektrische aansturing van qubits mogelijk	• Controle vooralsnog beperkt door decoherentie • Reproduceerbaarheid: devices niet identiek
Doteringsatomen in vaste stof: Elektronspin gebonden aan doteringsatoom of kernspin van doteringsatoom (bijvoorbeeld: P-atoom in silicium of **NV center** (**nitrogen-vacancy**) in diamant) *Qubit-toestanden 0 en 1:* spin omlaag en spin omhoog		• Zeer robuuste qubits: vergelijkbaar met ingevangen atomen • Volledig elektrische aansturing van qubits soms mogelijk • Schaling van devices op een chip in principe mogelijk • Interface naar fotonen voor lange-afstandcommunicatie	• Directe koppeling tussen atomen vereist grote nauwkeurigheid in plaatsing • Koppeling via fotonen nog te langzaam (~100 s)
Supergeleidende Qubits met Josephson-juncties (X in circuit) *Qubit-toestanden 0 en 1:* • Ladingsqubit: Lading aan- en afwezig • Flux qubit: Magnetische flux omhoog en omlaag • Fase qubit: fase over junctie → spanning over junctie 0 en eindig.		• Bijna macroscopische qubits: collectieve gedrag van ~10 miljard elektronen in device van ongeveer 0,1 mm • Alle logische operaties zijn snel (<1 μs) • Grote ontwerpvrijheid van circuitparameters	• Coherentietijden nog beperkt (typisch 10 μs) • Reproduceerbaarheid: devices niet identiek • Schaling naar veel qubits op 1 chip lastig vanwege de grootte.

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

Ronald Hanson (1976) is Antoni van Leeuwenhoek-hoogleraar 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

van het doel. Op dit moment kunnen de beste conventionele computerclusters 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 expliciet 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 ionenval. 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 aangetoond. Elektronenspins 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 onderzoeksvelden 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 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 ongekende 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 fundamenten 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)