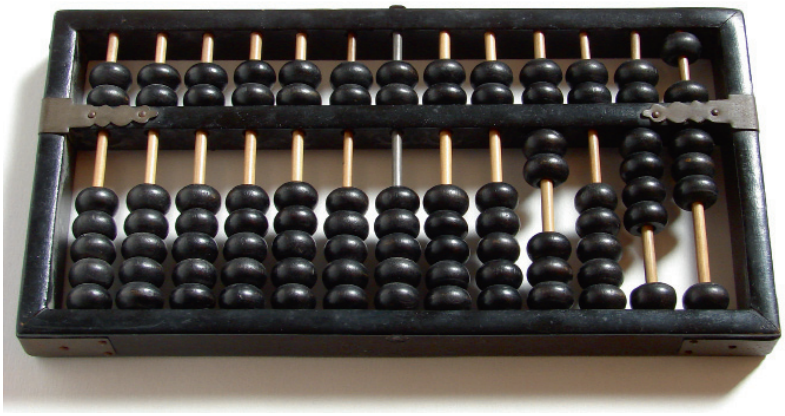
Quantumcomputers en quantuminformatie

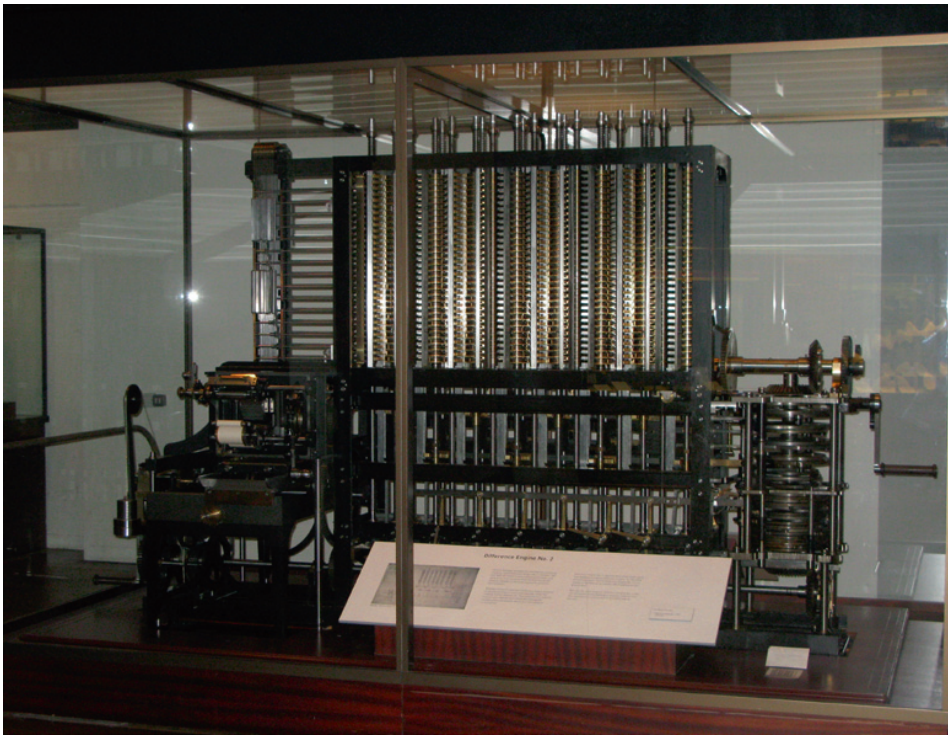
In de jaren tachtig opperde Richard Feynman het idee om quantummechanische systemen te gebruiken voor het uitvoeren van berekeningen. Inmiddels is de quantumcomputer – een computer die volgens quantummechanische principes werkt – een bekend begrip en zijn er talrijke ideeën ontstaan voor het gebruik 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 Blaauboer

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 versies, 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 microprocessoren, 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.

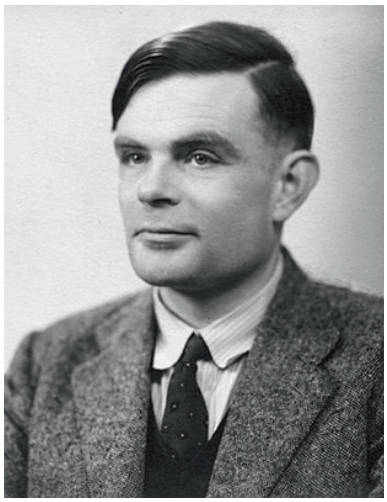
De quantumcomputer

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-Turingmachine, 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) -> (0,1) 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 quantuminformatieoverdracht 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 quantuminformatieoverdracht genoemd.

Dit themanummer

In dit themanummer komt een verscheidenheid 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 quantuminformatieoverdracht, zoals de artikelen over quantumalgoritmes en quantumcryptografie, quantummagnetisme, topologisch beschermd rekenen, quantumsimulatoren van koude atomen en quantumcorrelaties 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 Blaauboer 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, *Qantum Computation and Qantum Information* Cambridge University Press, Cambridge (2010).