

Een speld in een hooiberg

De quantumcomputer is in korte tijd uitgegroeid tot een nieuwe heilige graal van de hedendaagse natuurkunde [1]. Rekenen met behulp van quantummechanica belooft problemen te kunnen oplossen die op een klassieke computer zeer inefficiënt of zelfs praktisch onmogelijk zijn. De twee bekendste voorbeelden zijn het factorisatie-algoritme van Shor [2] en het zoekalgoritme van Grover [3]. Voor het laatste bestaat sinds kort ook een klassieke tegenhanger, zoals wij onlangs met een experiment hebben gedemonstreerd [4]. Robert

J.C. Spreeuw en Nandini Bhattacharya



spreeuw@science.uva.nl

Robert Spreeuw promoveerde in Leiden op een quantumoptisch onderwerp. Gedurende enkele jaren in de VS (NIST, Gaithersburg) en Duitsland (Konstanz) leerde hij atomen te koelen en te manipuleren met lasers. Eind 1995 startte hij als KNAW-fellow een atoomoptisch experiment in Amsterdam. Inmiddels UD aan de UvA, zint hij nu onder meer op methoden om quantum-informatie te verwerken met licht en koude atomen.



Nandini Bhattacharya promoveerde aan het Tata Institute of Fundamental Research in Mumbai, op een onderzoek aan levende ionen. Zij werkte drie jaar als postdoc in het Van der Waals-Zeeman Instituut, aanvankelijk aan de experimenten aan koude atomen. Gaandeweg raakte zij tevens geïnteresseerd in quantum-informatieverwerking. Sinds kort is zij als UD verbonden aan de optica groep van de TUD.

We kunnen ons afvragen wat nu precies de eigenschappen zijn waaraan quantumalgoritmen hun efficiëntie ontleen. Een belangrijke rol is weggelegd voor quantumsuperposities en interferentie. Afhankelijk van het algoritme spelen daarnaast ook eigenschappen als verstrengeling (entanglement) en het quantummeetproces een rol. Opmerkelijk genoeg hebben we voor het zoekalgoritme voldoende aan superposities en interferentie. Dit zijn nu juist de eigenschappen die niet exclusief zijn voor de quantumwereld, maar tevens bekend van klassieke golven. Dit suggereert dat quantum-zoeken ook gedaan kan worden met klassieke golven. Dit is precies wat wij onlangs in Amsterdam gedaan hebben [4].

TELEFOONBOEKEN EN HOOIBERGEN

Het zoekprobleem wordt vaak geïllustreerd aan de hand van een telefoonboek: je hebt iemands telefoonnummer maar je bent haar naam vergeten. Je zou kunnen opbellen maar dat leidt misschien tot een pijnlijke situatie. Een andere simpele methode zou zijn om de telefoongids van voor naar achter door te nemen tot je het gezochte nummer tegenkomt. Gemiddeld ge-

nomen kom je het nummer ergens halverwege tegen, na $N/2$ nummers te hebben doorzocht, waarbij N het totale aantal namen in de telefoongids is. Als je pech hebt, zorgt de wet van Murphy ervoor dat je het nummer pas op de allerlaatste bladzijde vindt. Hier is een taak weggelegd voor een quantumcomputer. Met behulp van het zoekalgoritme van Grover [3] kunnen we de naam bij het nummer vinden in slechts \sqrt{N} zoekstappen.

Een vereenvoudiging van het telefoonboekprobleem is het zoeken naar een speld in een hooiberg. We herformuleren het probleem als volgt: we hebben een binaire functie f , zodanig dat $f(x) = 0$ voor alle waarden van x , behalve $f(s) = 1$; gezocht is de 'speld' s tussen de 'strootjes' $x \neq s$. Merk op dat de functie f de oplossing s niet rechtstreeks levert, maar slechts herkent: als we raden naar de oplossing, vertelt f of we goed geraden hebben. De naïeve zoekmethode is om alle mogelijke argumenten te proberen: $f(0) = 0, f(1) = 0, \dots$, totdat we op $f(s) = 1$ stuiten. Dit vergt gemiddeld genomen $N/2$ evaluaties van f . Het quantum-zoekalgoritme bereikt hetzelfde met slechts \sqrt{N} functie-evaluaties.

In een quantumcomputer correspondeert met iedere waarde x een basisoestand $|x\rangle$ in de Hilbertruimte. Met de functie $f(x)$ correspondeert een unitaire operator U_O , die 'orakel' genoemd wordt:

$$U_O|x\rangle = (-1)^{f(x)}|x\rangle.$$

Merk op dat U_O de toestand $|s\rangle$ markeert met een minteken. We zouden nu één voor één alle mogelijke $|x\rangle$ kunnen proberen en kijken of ze een minteken ontvangen van U_O , maar dan hebben we nog niets gewonnen. Veel beter is het om U_O te laten werken op een superpositie van alle $|x\rangle$. Het resultaat bevat dan de waarden $f(x)$ van alle x . Dit wordt wel quantum-parallellisme

genoemd en is door Grover op slimme wijze gebruikt om het zoekproces te versnellen – zie kader. Daarbij hoeft het orakel U_O slechts \sqrt{N} maal te worden geraadpleegd.

ZOEKEN IN EEN LASERBUNDEL

In het experiment (zie figuur 1) bewerken we het transversale profiel $E(x)$ van een laserbundel. De (complexe) amplitudes $E(x)$ op verschillende posities x corresponderen met de quantum-waarschijnlijkheidsamplitudes behorende bij de basistoestanden $|x\rangle$. Het orakel is feitelijk onze database, de hooiberg met daarin de speld. We implementeren dit met een optisch fase-masker. Dat bestaat uit een glasplaatje waarop we een dun laagje SiO hebben opgedampt, met dezelfde brekingsindex als het glas. Tijdens het opdampen ontstond er in de schaduw van een dun metaaldradje een lijnvormige ‘schaduw’ in de opgedampte laag waar het plaatje ter plaatse van de schaduw dus iets minder dik is. Het plaatje vertegenwoordigt nu de hooiberg en het lijntje is de speld. De positie van de speld is onbekend, die willen we vinden. Als we licht door het plaatje laten vallen, hangt de optische weglengte, en dus de opgedane fase, nu dus af van de plaats. Idealiter wordt een vlakke lichtgolf door het orakelplaatje voorzien van een faseprofiel,

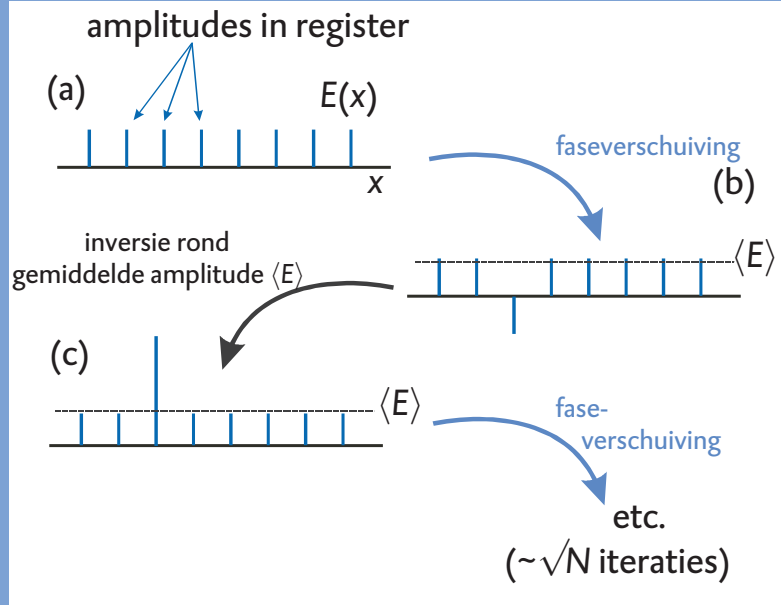
$$E(x) \rightarrow E(x)e^{i\pi f(x)} \\ = (-1)^{f(x)}E(x).$$

In het experiment wordt een faseverschuiving van 2,2 rad ($\neq \pi$) opgedaan bij een dubbele doorgang door het plaatje. Deze afwijking van π blijkt niet essentieel te zijn.

De volgende stap is deze fase-informatie om te zetten in amplitude-informatie met behulp van interferentie. Optisch gezien maken we een fasecontrast-afbeelding, zoals reeds in 1930 door Zernike uitgevonden. In termen van het zoekalgoritme noemen we deze stap

een ‘inversie rond de gemiddelde amplitude’ (*inversion about the average amplitude*, IAA). Zoals het orakel selectief de speld $|s\rangle$ van een minteken voorzagt, voorzien we nu de *gelijke superpositie van alle toestanden* van een minteken. Deze superpositietoestand is eenvoudig te onderscheiden na een Fouriertransformatie die optisch wordt uitgevoerd

met behulp van een lens. We plaatsen daarom een tweede fasemasker in het Fouriervlak van het orakelplaatje. De twee fasemaskers staan dus aan weerskanten van een lens, beide op een brandpuntsafstand. In tegenstelling tot de variabele transversale positie van de speld in het orakel, staat het lijntje op het ‘IAA-plaatje’ op een vaste posi-



Het quantum-zoekalgoritme van Grover

1. Initialisatie: prepareer een gelijke superpositie van alle basistoestanden,

$$|\psi_0\rangle = \frac{1}{\sqrt{N}}(|0\rangle + |1\rangle + \dots + |N-1\rangle) \quad (\text{figuur a})$$

2. Markeer de gezochte toestand $|s\rangle$ door middel van een unitaire ‘orakel’-operatie $U_O = \mathbf{1} - 2|s\rangle\langle s|$:

$$|\psi_1\rangle = U_O|\psi_0\rangle = \frac{1}{\sqrt{N}}(|0\rangle + |1\rangle + \dots - |s\rangle + \dots + |N-1\rangle) \quad (\text{figuur b})$$

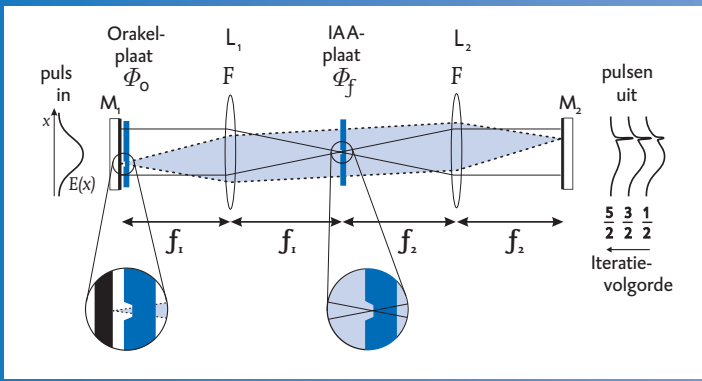
3. Inverteer alle amplitudes rond de gemiddelde amplitude, door middel van een unitaire operatie $U_{IAA} = 2|\psi_0\rangle\langle\psi_0| - \mathbf{1}$:

$$|\psi_2\rangle = U_{IAA}|\psi_1\rangle \approx \frac{1}{\sqrt{N}}(|0\rangle + |1\rangle + \dots + 3|s\rangle + \dots + |N-1\rangle) \quad (\text{figuur c})$$

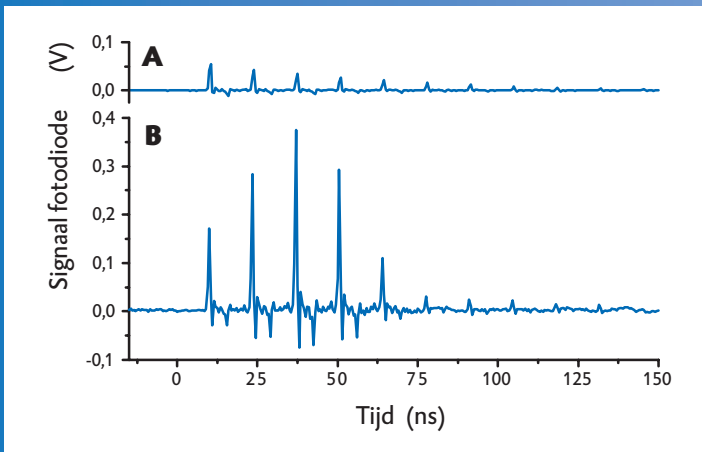
4. Itereer stappen 2. en 3; na $\sim\sqrt{N}$ iteraties is de toestand dicht bij de gezochte toestand:

$$|\psi_f\rangle = (U_{IAA}U_O)^{\sqrt{N}}|\psi_0\rangle \approx |s\rangle$$

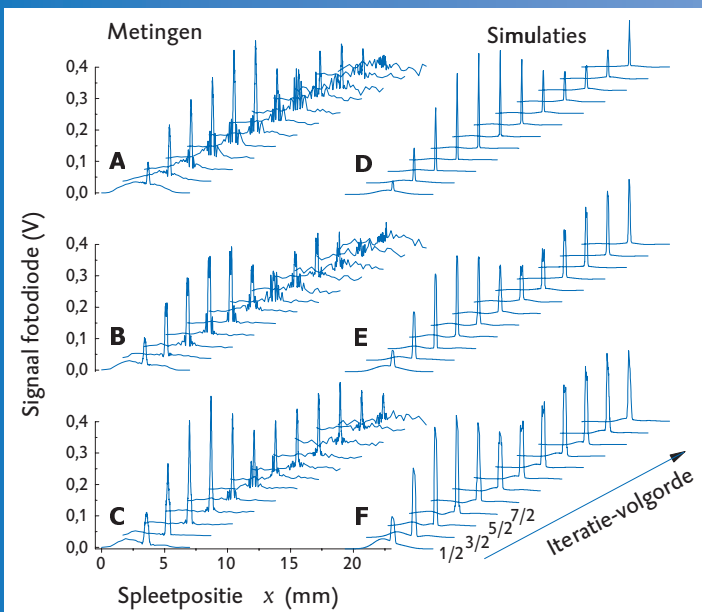
5. Verricht een meting en vind met hoge waarschijnlijkheid de gezochte toestand $|s\rangle$.



Figuur 1 Golf-optische zoekmachine. Een korte optische puls kaast heen en weer tussen twee spiegels M_1 , M_2 . Bij iedere doorgang wordt het transversale profiel bewerkt door fasemaskers en lenzen (Fouriertransformaties). Het transversale profiel dat door M_2 wordt doorgelaten vertoont een groeiende piek die de positie van de speld in het 'orakel'-fasemasker aanwijst. De profielen worden gemeten met een beweegbare spleet met daarachter een fotodiode.



Figuur 2 Amplitudeversterking, gemeten met een fotodiode.
A. Signaal zoals gemeten zonder fasemaskers in de trilhaolte. De piekhoogte neemt exponentieel af door optische verliezen.
B. Signaal gemeten achter een spleet, opgesteld in het beeld van het orakel. Ondanks optische verliezen neemt de piekhoogte aanvankelijk toe.



Figuur 3 Gemeten (links) en berekende (rechts) transversale bundelprofielen. Op een aanvankelijk Gaussvormige achtergrond zien we een piek groeien die de positie van het streepje op het orakelplaatje aanwijst. De piek bereikt een maximum na $\sim\sqrt{N}$ iteraties en neemt dan weer af. Als we de breedte van het orakelstreepje laten toenemen, neemt effectief de grootte van de database af en zijn minder iteraties nodig om het maximum te bereiken.

tie, namelijk in het focus van de ongestoorde bundel. De kleine verstoring die de speld in het orakel teweeggebracht heeft, leidt tot een verstrooide golf die ter plaatse van het IAA-plaatje niet in focus is. Het IAA-plaatje verschuift dus het faseverschil tussen de ongestoorde en de gestrooide golf. (Om precies te zijn wordt weer een faseverschuiving van $2,2$ rad verkregen na een dubbele doorgang.) In de wiskundige beschrijving van de fasecontrast-afbeelding blijken alle amplitudes behorend bij de basistoestanden $|x\rangle$ gespiegeld worden in de gemiddelde amplitude.

Om het quantumzoekalgoritme te completeren moeten nu de bewerkingen van het orakel en de inversie rond het gemiddelde geïtereerd worden. Na iedere iteratie neemt het contrast toe, totdat na $\sim\sqrt{N}$ iteraties het optimum wordt bereikt. Daarna neemt het contrast weer af en na nogmaals $\sim\sqrt{N}$ iteraties zijn we weer terug bij af. Merk op dat het hier beschreven procédé in principe met één enkel foton kan worden uitgevoerd. Na $\sim\sqrt{N}$ iteraties bevindt het foton zich dan met bijna zekerheid op de positie van de 'speld'. Ter vergelijking kunnen we ons afvragen wat er gebeurt als we het orakel zouden vervangen door een scherm met een spleet. De kans dat een foton door de spleet gaat is dan $1/N$, zodat we $\sim N$ fotonen nodig hebben om de spleet te vinden.

In het experiment worden iteraties bereikt door een lichtpulsje tussen twee spiegels M_1 , M_2 heen en weer te laten kaatsen. Om de pulsjes na opeenvolgende rondgangen te kunnen onderscheiden, is de pulsduur (300 ps) korter gekozen dan de rondlooptijd (13,5 ns). Na iedere rondgang lekt 2% door de eindspiegel heen, zodat een fotodiode een pulstreintje registreert met één pulsje per rondloop. In figuur 2A zien we zo'n serie pulsjes exponentieel zwakker worden ten gevol-

ge van optische verliezen (hier werden de fasemaskers weggelaten). Door de fotodiode achter een beweegbare spleet op te stellen, kunnen we het gehele transversale bundelprofiel af-tasten. In figuur 2B zien we de pulstrein zoals waargenomen als de spleet precies in het beeld van het orakel is opgesteld. Ondanks de optische verliezen zien we het signaal nu eerst toenemen, tot het uiteindelijk ook uitdooft. Dit wordt amplitudeversterking genoemd.

VINDEN EN WEER KWIJTRAKEN

In de linkerkolom van figuur 3 zien we de bundelprofielen na opeenvolgende iteraties, zoals ze met behulp van de beweegbare spleet zijn opgemeten. Het eerste profiel heeft een min of meer Gaussische vorm, met daarbovenop een piek die de positie van het orakel aanwijst. Opeenvolgende iteraties laten een groeiende piek zien, totdat een maximum wordt bereikt en de piek weer afneemt. We zien als het ware het vinden en weer kwijtraken van de speld.

We verwachten dus dat de maximum piek na $\sim\sqrt{N}$ iteraties wordt bereikt. Wat is nu de grootte van de hooiberg N ? Dit is het aantal verschillende posities dat mogelijk is voor het orakel, dus de verhouding D/d van de bundeldiameter D en de breedte van het orakelstreefje d . Door nu orakels te gebruiken met verschillende breedtes kunnen we de N variëren. Met een breder orakel neemt N af en gaat het zoekproces sneller. Dit is te zien door in figuur 3 de verschillende series in een kolom te vergelijken. We leiden de waarden van N af door uit de data het aantal iteraties tot de maximumpiek af te lezen. Dit levert voor N de waarden 32 (figuur 3a), 15,8 (figuur 3b) en 11,6 (figuur 3c). Deze waarden kunnen we vergelijken met de uit D en d berekende waarden voor N , namelijk 31,8, 15,7 en 10,6. We concluderen dat deze

sets goed met elkaar in overeenstemming zijn en dat onze resultaten dus de \sqrt{N} -schaling van het quantum-zoekalgoritme bevestigen.

Tenslotte hebben we de resultaten gesimuleerd met een numerieke berekening. Deze resultaten zijn te zien in de rechterkolom van figuur 3 (d, e en f) en zijn in goede overeenstemming met de gemeten data.

QUANTUM- OF GOLFCOMPUTER?

We hebben dus laten zien dat het quantum-zoekalgoritme slechts de golfverschijnselen superpositie en interferentie gebruikt. Betekent dit nu dat we een quantumcomputer kunnen bouwen op basis van klassieke golven? Het antwoord hierop luidt helaas *nee*. Een echte quantumcomputer gebruikt de ter beschikking staande middelen efficiënter dan een golfcomputer. Dat betekent dat we moeten kijken hoe op-schaalbaar het systeem is.

We kunnen vraag stellen hoeveel pixels we kunnen onderscheiden in ons transversaal laserprofiel. In het hier beschreven experiment werd met lijn-vormige pixels slechts één transversale dimensie benut. We verkrijgen meer pixels door beide transversale dimensies te benutten. Bijvoorbeeld een bundeldiameter van $D = 1$ cm en (vierkante) pixels met een breedte van $d = 10 \mu\text{m}$ krijgen we $N \sim (D/d)^2 = 10^6$. Dit is weliswaar aanzienlijk maar de schaling $N \propto D^2$ is ongunstig. De minimale grootte d van onderscheidbare pixels is beperkt door de optische diffractielimiet tot ongeveer een optische golflengte. Voor een gegeven grootte van N is dus een minimale bundeldiameter vereist. De grootte van de benodigde bundel wordt echter niet bepaald door de zoekmethode, maar door de manier waarop de informatie in de database/ hooiberg is gecodeerd. Ter vergelijking: in een quantumcomputer met n qubits schaal N exponentieel met het aantal qubits, $N = 2^n$.

Bijvoorbeeld voor $n = 200$ krijgen we $N > 10^{60}$. Om dit met klassieke golven te implementeren benadert de benodigde bundeldiameter al de diameter van ons universum ($\sim 10^{26}$ m)! Je lijkt dan dus beter af te zijn met 200 qubits. Dit is echter maar schijn, omdat de quantumcomputer dan $\sqrt{N} = 10^{30}$ iteraties nodig zou hebben om Grovers algoritme uit te voeren. Met bijvoorbeeld 10^9 iteraties per seconde duurt dat ruimschoots langer dan de leeftijd van ons universum ($\sim 10^{17}$ s). Als we de quantumcomputer 1 s willen laten rekenen, is de database dus beperkt tot $N = 10^{18}$ elementen ($n = 60$ qubits). Met klassieke lichtgolven zouden we dan een bundeldiameter van $D = 10$ km nodig hebben!

Het cruciale verschil lijkt dus niet zozeer te zitten in het zoekalgoritme zelf. Ons experiment demonstreert dat het quantum-zoekalgoritme in feite een golfalgoritme is. Het verschil zit veel eerder in de aard van de informatie en de manier waarop deze gecodeerd wordt. Om een klassieke database (zoals een telefoonboek) op te schalen, is een minimum aan resources (ruimte, papier, ...) nodig, ongeacht de methode die je gebruikt voor het doorzoeken. Het doorzoeken zelf gaat met klassieke golven even efficiënt als met quantummechanica. Wat voor soort informatie c.q. databases je met een quantumcomputer dan wel efficiënter zou kunnen coderen en doorzoeken, blijft een vraag waarover voorlopig het laatste woord nog niet gesproken is.

REFERENTIES

- 1 M.A. Nielsen en I.L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge (2000).
- 2 P. Shor, *SIAM J. Sci. Statist. Comput.* **26** (1997), 1484.
- 3 L.K. Grover, *Phys. Rev. Lett.* **79** (1997), 325.
- 4 N. Bhattacharya, H.B. van Linden van den Heuvel en R.J.C. Spreeuw, *Phys. Rev. Lett.* **88** (2002), 137901.