Koen Groenland
Centrum Wiskunde & Informatica
Amsterdam
k.l.groenland@cwi.nl

Tom Bannink
Centrum Wiskunde & Informatica
Amsterdam
tom.bannink@cwi.nl

Onderzoek

Sneller zoeken met quantum random walks

Het lijkt steeds meer een kwestie van tijd totdat werkende kwantumcomputers een feit zijn. Vooruitlopend op dit scenario zijn onderzoekers aan het Centrum voor Wiskunde & Informatica al druk bezig met het ontwerpen van *kwantumalgoritmes*, waarmee we algoritmes bedoelen die op een kwantumcomputer kunnen draaien. In dit artikel, dat geschreven is naar aanleiding van een Lorentz Center workshop, leggen Koen Groenland en Tom Bannink uit wat een *quantum random walk* is en laten zien hoe Grovers zoekalgoritme, historisch gezien een van de allereerste kwantumalgoritmes, beschreven kan worden met behulp van zo'n kwantumwandeling.

Kwantumrekenen

We zullen eerst laten zien hoe een kwantumcomputer gebruikmaakt van de wonderbaarlijke wetten van de kwantummechanica. Het geheugen van een *klassieke* computer die beschikt over n bits kan $N = 2^n$ unieke configuraties of 'toestanden' aannemen. Een *toestand* kunnen we beschrijven als een reeks van n enen en nullen, zoals '0110011'.

Een *kwantumtoestand* $|\psi\rangle$ is een vector van lengte 1 in de (complexe) vectorruimte $\mathbb{C}^N$ die wordt opgespannen door alle N klassiek toegestane toestanden. Als we elke klassieke toestand een label j geven (een geheel getal tussen 1 en N), dan kunnen we elke kwantumtoestand schrijven als lineaire combinatie van deze klassieke toestanden. Iedere kwantumtoestand $|\psi\rangle$ laat zich dus eenduidig voorstellen als

$$|\psi\rangle = \sum_{j=1}^{N} \alpha_j |j\rangle \quad \text{met normalisatie} \quad \sum_{j=1}^{N} |\alpha_j|^2 = 1. \tag{1}$$

De coëfficiënten α_j zijn complex. Hier zien we de eerste exotische eigenschap van kwantumtoestanden, namelijk dat ze een *superpositie* van klassieke toestanden zijn. Je zou kunnen zeggen dat een kwantumsysteem zich in meerdere klassieke toestanden tegelijkertijd kan bevinden! We gebruiken de notatie $|v\rangle$ om aan te duiden dat v een kwantumtoestand is. Het symbool $|\cdot\rangle$ noemen we een 'ket'. Om een complex geconjugeerde (en getransponeerde) vector weer te geven, gebruiken we de notatie $\langle v|$, die we een 'bra' noemen. De gedachte achter deze notatie wordt duidelijk wanneer we een inwendig product tussen vectoren v en w opschrijven als de zogenaamde bra(c)ket: $\langle v|w\rangle$. Evenzo kunnen we de matrix die de vector $|w\rangle$ afbeeldt op de vector $|v\rangle$ opschrijven als $|v\rangle\langle w|$. We zullen te maken krijgen met kwantumsystemen die interactie met elkaar hebben. In dat geval beschrijven we de gezamenlijke toestand als een vector in het tensorproduct van de twee afzonderlijke ruimtes. Als bijvoorbeeld de systemen A en B afzonderlijk beschreven worden met behulp van de vectorruimten $\mathbb{C}^{N_A}$ en $\mathbb{C}^{N_B}$, dan kunnen we de toestand van het gecombineerde systeem AB beschrijven met behulp van de vectorruimte $\mathbb{C}^{N_A} \otimes \mathbb{C}^{N_B}$. Als we de basisvectoren die $\mathbb{C}^{N_A}$ en $\mathbb{C}^{N_B}$ opspannen aangeven met $|j\rangle_A$ en $|k\rangle_B$, dan wordt $\mathbb{C}^{N_A} \otimes \mathbb{C}^{N_B}$ opgespannen door de (tensor) producten $|j\rangle_A |k\rangle_B$. Een toestandsvector in deze ruimte is dan te schrijven als

$$|\psi\rangle_{AB} = \sum_{j=1}^{N_A} \sum_{k=1}^{N_B} \alpha_{j,k} |j\rangle_A |k\rangle_B \quad \text{met normalisatie} \quad \sum_{j=1}^{N_A} \sum_{k=1}^{N_B} |\alpha_{j,k}|^2 = 1. \tag{2}$$

We komen nu een nieuw exotisch fenomeen tegen, de zogenaamde *verstrengeling*. Stel dat kwantumsystemen A en B beide een basis hebben bestaande uit twee toestanden (dat wil zeggen we veronderstellen dat $N_A = N_B = 2$), die we met $|0\rangle_A$ en $|1\rangle_A$, respectievelijk $|0\rangle_B$ en $|1\rangle_B$ zullen aangeven. Zulke systemen noemen we *qubits* ('kwantumbits'). We kunnen een toestand van systeem A dus schrijven in de vorm

$$|\psi\rangle_A = \alpha_0 |0\rangle_A + \alpha_1 |1\rangle_A$$

en net zo voor de toestanden van systeem B. Beschouw nu de volgende toestand van het gecombineerde systeem AB:

$$|\chi\rangle = \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B). \tag{3}$$

Hoe zou je nu de toestand van systeem A omschrijven? En van systeem B? Een (onjuiste) eerste gedachte zou kunnen zijn dat zij zich in toestand $\frac{1}{\sqrt{2}}(|0\rangle_A+|1\rangle_A)$, respectievelijk $\frac{1}{\sqrt{2}}(|0\rangle_B+|1\rangle_B)$ bevinden. Echter, de combinatie van deze twee toestanden levert iets geheel anders: door simpelweg de haakjes uit te werken vinden we immers

$$\begin{aligned}&\frac{1}{\sqrt{2}}(|0\rangle_A+|1\rangle_A)\otimes\frac{1}{\sqrt{2}}(|0\rangle_B+|1\rangle_B)\\&\quad=\frac{1}{2}(|0\rangle_A|0\rangle_B+|0\rangle_A|1\rangle_B\\&\qquad+|1\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B).\end{aligned}$$

Het blijkt zelfs zo te zijn dat $|\chi\rangle$ onmogelijk te beschrijven is als combinatie $|\chi_1\rangle_A\otimes|\chi_2\rangle_B$ van twee losse qubit-toestanden $|\chi_1\rangle_A$ en $|\chi_2\rangle_B$. Om deze reden noemen we de toestand $|\chi\rangle$ een *verstrengelde toestand*: de systemen A en B zijn als het ware met elkaar 'verstrengeld' in deze toestand. Op grond van dit verschijnsel meende Einstein dat de kwantummechanica geen complete beschrijving van de werkelijkheid kan zijn. Immers, de qubits in een verstrengelde toestand zijn van elkaar afhankelijk, zelfs wanneer zij lichtjaren van elkaar verwijderd worden [1]. Inmiddels weten we dat het kwantumformalisme wel degelijk de juiste beschrijving geeft van onze wereld. Voor een kwantumberekening zullen we de kwantumtoestanden willen manipuleren. Dit kan op twee manieren: middels zogenaamde 'gates' (schakelingen) en door het verrichten van metingen. De fysisch toegestane gates worden beschreven door unitaire matrices. Dit zijn matrices met complexe coëfficiënten die voldoen aan $U^{-1}=(U^*)^T$ (de inverse is gelijk aan de complex geconjugeerde en getransponeerde van de matrix). Deze matrices hebben de eigenschap dat ze de norm van vectoren behouden. Een gate werkt op een kwantumtoestand volgens de gebruikelijke matrix-vectorvermenigvuldiging. Een voorbeeld van een gate is bijvoorbeeld de fase-gate R_θ die de relatieve fase tussen de coëfficiënten van een qubit-toestand kan veranderen:

$$R_\theta=\begin{pmatrix}1&0\\0&e^{i\theta}\end{pmatrix}$$

oftewel

$$R_\theta(\alpha_0|0\rangle+\alpha_1|1\rangle)=\alpha_0|0\rangle+e^{i\theta}\alpha_1|1\rangle.$$

Een ander voorbeeld is de controlled-NOT-gate (CNOT-gate). Deze werkt op twee qubits als volgt. Wanneer qubit A zich in de toestand $|0\rangle$ bevindt laat CNOT de toestand van qubit B ongemoeid, en wanneer qubit A zich in de toestand $|1\rangle$ bevindt verwisselt CNOT de toestanden 0 en 1 van qubit B:

$$\mathrm{CNOT}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$$

oftewel

$$\begin{aligned}\mathrm{CNOT}\,|0\rangle_A|0\rangle_B&=|0\rangle_A|0\rangle_B,\\\mathrm{CNOT}\,|0\rangle_A|1\rangle_B&=|0\rangle_A|1\rangle_B,\\\mathrm{CNOT}\,|1\rangle_A|0\rangle_B&=|1\rangle_A|1\rangle_B,\\\mathrm{CNOT}\,|1\rangle_A|1\rangle_B&=|1\rangle_A|0\rangle_B.\end{aligned}$$

Hoewel de CNOT-gate volledig klassiek te beschrijven is, is deze in staat om kwantumverstrengeling te creëren en vormt deze de basis van veel kwantumalgoritmes. Net als bij de klassieke tegenhangers kan met een kleine set kwantumgates elke mogelijke functie f in de vorm van een 'circuit' van aaneengeschakelde kwantumgates worden gebouwd. Het bijzondere aan kwantumcircuits is dat de input kan bestaan uit een lineaire combinatie van alle mogelijke klassieke inputs. Stel bijvoorbeeld dat we een systeem A hebben met basisvectoren $|0\rangle_A,\ldots,|N\rangle_A$ dat we koppelen met een systeem B met basisvectoren $|0\rangle_B,\ldots,|M\rangle_B$. Zij voorts gegeven een functie f die $\{0,\ldots,N-1\}$ afbeeldt naar $\{0,\ldots,M-1\}$. Stel nu dat we in staat zijn een kwantumcircuit te maken dat het volgende effect heeft op de kwantumtoestand $|n\rangle_A|0\rangle_B$:

$$|n\rangle_A|0\rangle_B\mapsto|n\rangle_A|f(n)\rangle_B.$$

Met behulp van dit circuit kunnen we de functie f over *alle mogelijke inputs tegelijkertijd* uitrekenen, door simpelweg als input aan het circuit de volgende toestand te geven:

$$\frac{1}{\sqrt{N}}\sum_{n=0}^{N-1}|n\rangle_A|0\rangle_B.$$

Het circuit voert deze input over in

$$\frac{1}{\sqrt{N}}\sum_{n=0}^{N-1}|n\rangle_A|0\rangle_B=\frac{1}{\sqrt{N}}\sum_{n=0}^{N-1}|n\rangle_A|f(n)\rangle_B.\quad(4)$$

In deze toestand treden alle waarden van f op. Met andere woorden: het circuit 'berekent' alle waarden $f(n)$ in één keer. Laat u echter niet misleiden: het is niet mogelijk om al deze informatie uit de resulterende kwantumtoestand te halen. Zoals we zo dadelijk zullen beschrijven zal een meting van de kwantumtoestand (4) een van de waarden $f(n)$ geven. De enige manier om op niet-triviale wijze gebruik te maken van het 'kwantumparallellisme' inherent in (4) is door verder te rekenen met de gevonden superpositie — dit is precies wat we verderop in Grovers algoritme zullen doen.

Hoe werkt een meting dan precies? Wat er 'werkelijk' gebeurt bij een meting is nog steeds onderhevig aan meerdere interpretaties, maar voor de wiskundige beschrijving volstaat het om uit te gaan van de zogenaamde *Born-regel*. Deze zegt dat wanneer we een kwantumtoestand $|\psi\rangle=\sum_j\alpha_j|j\rangle$ meten, we met kans $|\alpha_j|^2$ de klassieke toestand $|j\rangle$ als uitkomst van onze meting zullen vinden. De normalisatie $\sum_j|\alpha_j|^2=1$ garandeert dat al deze waarschijnlijkheden optellen tot 1. Zo is de kans op het meten van een specifieke waarde $f(n)$ in de toestand van formule (4) precies $1/(N+1)$. Volgens de standaardinterpretatie van de kwantummechanica (de zogenaamde Kopenhaagse interpretatie) verandert bij een meting de toestand van het systeem instantaan als volgt: als j de uitkomst van de meting is, dan gaat het systeem van toestand $|\psi\rangle=\sum_j\alpha_j|j\rangle$ over in toestand $|\psi'\rangle=|j\rangle$. Dit wordt ook wel de 'ineenstorting' (collapse) van de kwantumtoestand genoemd. Alle verdere informatie die was opgeslagen in de waarden α_j raakt daarmee verloren. Merk op dat het verrichten van een meting de enige manier is om informatie over de qubit te winnen — er zijn geen manieren om dit te omzeilen. De enige manier om alle waarden α_j precies te achterhalen is door een qubit telkens in dezelfde toestand te prepareren en opnieuw te meten.

Ondanks deze beperkingen blijkt dat we met de spelregels van de kwantummechanica nieuwe algoritmes kunnen maken die sneller zijn dan klassiek mogelijk is. Een voorbeeld hiervan zijn de zogenaamde kwantumwandelingen.

Kwantumwandelingen

De zogeheten *quantum random walk*, of kwantumwandeling, is een model voor een kwantumdeeltje dat (vrij) kan bewegen door een systeem, meestal een graaf. Het beschrijft de positie van het deeltje als functie van de tijd. De tijd t kan hierbij een continue of discrete parameter zijn. De kwantumwandeling wordt soms gezien als de kwantumversie van de klassieke

random walk. Als men bij elke tijdstap de positie van het vrije kwantumdeeltje *meet*, dan vindt men het gedrag van een klassieke random walk terug. We zullen dit illustreren aan de hand van een simpel voorbeeld, de zogeheten 'Hadamard-wandeling'.

Hadamard-wandeling

De Hadamard-wandeling beschrijft de evolutie van een kwantumdeeltje op de discrete lijn $\mathbb{Z}$ als functie van een discrete tijd-parameter $t \in \mathbb{N}$. Het deeltje wordt op elk tijdstip beschreven door de positie en een extra interne variabele die de waarde $|\uparrow\rangle = |0\rangle$ of $|\downarrow\rangle = |1\rangle$ kan aannemen. De toestand $|x,\uparrow\rangle$ beschrijft een deeltje op positie x met interne toestand $\uparrow$. De volledige toestand van het kwantumdeeltje is een superpositie van zulke basistoestanden:

$$|\psi\rangle = \sum_{x\in\mathbb{Z}} (\alpha_{x\uparrow}\,|x,\uparrow\rangle + \alpha_{x\downarrow}\,|x,\downarrow\rangle)$$

met

$$\sum_{x\in\mathbb{Z}} (|\,\alpha_{x\uparrow}\,|^2 + |\,\alpha_{x\downarrow}\,|^2) = 1.$$

Het meten van deze toestand levert positie x op met kans $|\,\alpha_{x\uparrow}\,|^2 + |\,\alpha_{x\downarrow}\,|^2$. De evolutie van het deeltje verloopt als volgt. We passen eerst de zogeheten *Hadamard-operator* H toe op de interne toestand van het deeltje. Dit is de unitaire matrix

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

oftewel

$$H\,|\uparrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle),$$
$$H\,|\downarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\downarrow\rangle).$$

De operator H induceert een operator, die we met $\mathbb{1}\otimes H$ aangeven, op de algehele toestand van het deeltje: de identiteit $\mathbb{1}$ werkt op de positie en H op de interne toestand. Zo is bijvoorbeeld

$$(\mathbb{1}\otimes H)\,|3,\uparrow\rangle = \frac{1}{\sqrt{2}}(|3,\uparrow\rangle + |3,\downarrow\rangle).$$

Vervolgens passen we de 'shift-operator' S toe. Dit is de unitaire operator

$$S\,|x,\uparrow\rangle = |x+1,\uparrow\rangle,$$
$$S\,|x,\downarrow\rangle = |x-1,\downarrow\rangle.$$

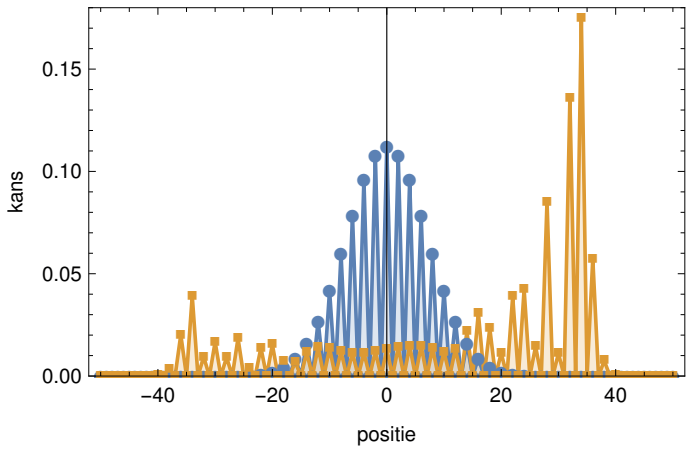
De tijdsevolutie van het deeltje bestaat uit het herhaaldelijk toepassen van de (unitaire) operator $S\circ(\mathbb{1}\otimes H)$. De operator H wordt in dit verband ook wel de *coin*-operator genoemd. De interne toestand speelt de rol van een muntje dat wordt 'opgegooid' door de coin-operator, en op basis van de uitkomst stuurt S het deeltje een stap naar links of naar rechts. We kunnen nu een begintoestand kiezen, bijvoorbeeld $|\psi\rangle_{(t=0)} = |0,\uparrow\rangle$, een deeltje dat begint in de oorsprong met interne toestand $\uparrow$. Als we de toestand van het systeem na vijftig stappen (vijftig maal de operator $S\circ(\mathbb{1}\otimes H)$ toepassen) bekijken vinden we een kansverdeling die is weergegeven in Figuur 1. Om dit resultaat te begrijpen gaan we stap voor stap kijken wat er met het systeem gebeurt. Neem aan dat het deeltje begint in de toestand $|\psi\rangle_{(t=0)} = |0,\uparrow\rangle$. We passen nu drie keer $S\circ(\mathbb{1}\otimes H)$ toe om $|\psi\rangle_{(t=3)}$ te vinden:

$$|\psi\rangle_{(t=0)} = |0,\uparrow\rangle,$$
$$|\psi\rangle_{(t=1)} = \frac{1}{\sqrt{2}}(|1,\uparrow\rangle + |-1,\downarrow\rangle),$$
$$|\psi\rangle_{(t=2)} = \frac{1}{2}(|2,\uparrow\rangle + |0,\downarrow\rangle + |0,\uparrow\rangle - |-2,\downarrow\rangle),$$
$$|\psi\rangle_{(t=3)} = \frac{1}{2\sqrt{2}}(|3,\uparrow\rangle + |1,\downarrow\rangle + 2\,|1,\uparrow\rangle - |-1,\uparrow\rangle + |-3,\downarrow\rangle).$$

Merk op dat op tijd $t=2$ de termen met positie 0 voorkomen in de specifieke combinatie $|0,\downarrow\rangle + |0,\uparrow\rangle$ (waarbij we de normalisatie even achterwege laten). Als we nu de Hadamard-operator toepassen vinden we

$$(\mathbb{1}\otimes H)(|0,\downarrow\rangle + |0,\uparrow\rangle) = \sqrt{2}\,|0,\uparrow\rangle,$$

dus de volledige operator $S\circ(\mathbb{1}\otimes H)$ stuurt de toestand $|0,\downarrow\rangle + |0,\uparrow\rangle$ naar $\sqrt{2}\,|1,\uparrow\rangle$, oftewel alleen maar naar rechts in plaats van een superpositie over links en rechts. De combinatie $|0,\downarrow\rangle - |0,\uparrow\rangle$ (met een minteken) zou echter naar $\sqrt{2}\,|-1,\downarrow\rangle$ zijn gegaan. Dit laat zien dat het resultaat erg afhankelijk is van de interne toestand van het deeltje. Dit is de reden dat het gedrag van de Hadamard-wandeling heel anders is dan dat van de klassieke random walk op $\mathbb{Z}$.

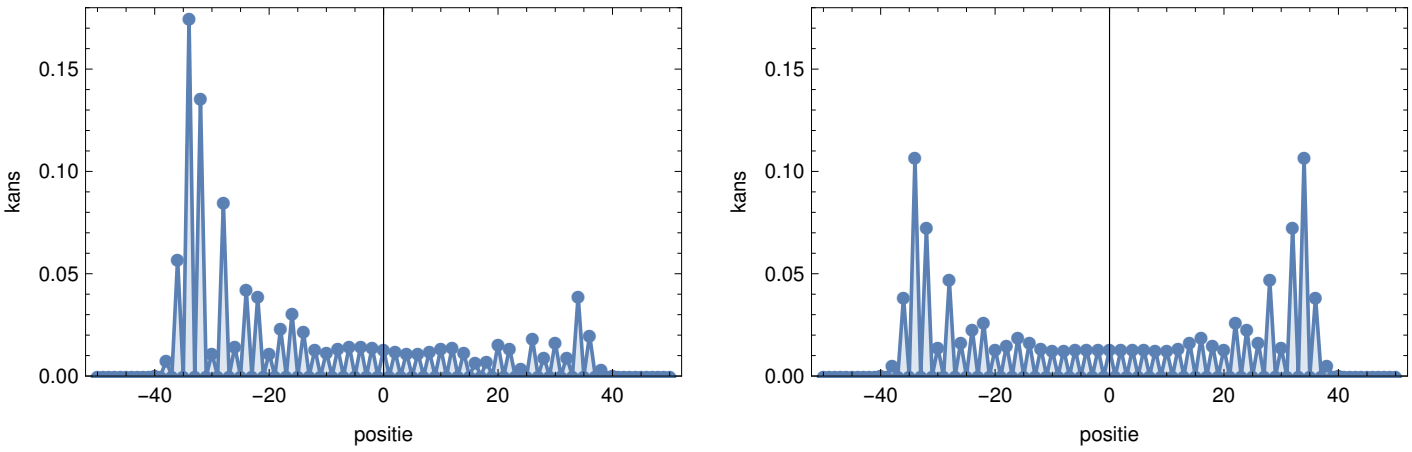


Figuur 1 De kansverdeling na vijftig stappen van een klassieke random wandeling in blauw met rondjes en de kansverdeling na vijftig stappen van de Hadamard-wandeling in oranje met vierkantjes. De begintoestand van de kwantumwandeling was $|0,\uparrow\rangle$.

Vergelijking: versus klassiek

We kunnen nu de verbinding leggen met de klassieke random walk. Als men op tijdstip $t=1$ een meting doet, wordt positie 1 of -1 gevonden met kans $1/2$. Na de meting is het systeem in de toestand $|1,\uparrow\rangle$ of $|-1,\downarrow\rangle$ en *niet* langer in een superpositie van die twee. Laten we aannemen dat het resultaat van de meting $|-1,\downarrow\rangle$ was. Als we vervolgens opnieuw een stap doen zal het systeem terechtkomen in de toestand $\frac{1}{\sqrt{2}}(|0,\uparrow\rangle - |-2,\downarrow\rangle)$. Meten we nu weer dan zullen we 0 of -2 vinden, beide met kans $1/2$. We zien dat dit precies het gedrag is van de klassieke random walk. Het kwantumgedrag komt pas voor als we de superpositie intact laten door het systeem niet tussendoor te meten, waardoor de verschillende termen kunnen 'interfereren'.

Een groot verschil is de snelheid waarmee het deeltje zich voortbeweegt, oftewel de snelheid waarmee de kansverdeling zich uitspreidt. De spreiding van de verdeling kunnen we wiskundig beschrijven met de verwachtingswaarde van het kwadraat van de positie, $\langle X_t^2\rangle$. Hier staat X_t voor de positie op tijdstip t en $\langle\cdot\rangle$ voor de verwachtingswaarde. Het getal $\langle X_t^2\rangle$ geeft intuïtief de breedte van de kansverdeling aan op tijdstip t. Men kan bewijzen dat dit getal zich bij een klassieke wandeling gedraagt als $\langle X_t^2\rangle \sim t$, terwijl voor de kwantumwandeling geldt $\langle X_t^2\rangle \sim t^2$. Het teken $\sim$ geeft



Figuur 2 De kansverdeling na vijftig stappen van de Hadamard-wandeling. Links was de begintoestand $|0,\downarrow\rangle$ en rechts was de begintoestand $\frac{1}{\sqrt{2}}|0\rangle\,(|\uparrow\rangle + i\,|\downarrow\rangle)$.

hier aan dat de linkerkant proportioneel is aan de rechterkant, met een niet nader gespecificeerde constante. In woorden betekent dit dat de Hadamard-wandeling zich kwadratisch sneller verspreidt dan de klassieke random walk.

Een ander groot verschil tussen het kwantumsysteem en het klassieke systeem is de afhankelijkheid van de tijdsevolutie van de begintoestand. In Figuur 2 wordt de kansverdeling van de Hadamard-wandeling weergegeven voor verschillende begintoestanden. Hoewel de operatoren hetzelfde blijven kan het verschil in begintoestand toch heel veel uitmaken. Als we in het voorbeeld hierboven de lijn $\mathbb{Z}$ vervangen door een eindig systeem zoals de discrete cirkel $\mathbb{Z}/N\mathbb{Z}$, dan heeft een klassieke wandeling een unieke *stationaire toestand*. Dit betekent dat hoe de begintoestand ook is, het systeem altijd zal uitkomen in deze stationaire toestand als men maar lang genoeg wacht. Op de cirkel zou dit de uniforme verdeling over alle punten zijn. De begintoestand kan bijvoorbeeld een deeltje op één punt zijn (oftewel een kansverdeling waarbij de kans 1 is op het beginpunt en 0 op alle andere punten), maar ook een kansverdeling over meerdere punten. In beide gevallen zal het systeem uiteindelijk terechtkomen in de uniforme kansverdeling. Voor de kwantumwandeling is dit echter niet het geval. Deze heeft geen stationaire toestand, en twee verschillende begintoestanden geven ook op lange termijn verschillende toestanden. Sterker nog, omdat de evolutie van een kwantumsysteem altijd unitair is zullen twee orthogonale toestanden altijd orthogonaal blijven. Een eigenschap van unitaire operatoren is namelijk dat deze het inwendig product tussen vectoren behouden, $\langle Ua, Ub\rangle = \langle a, b\rangle$ in formules. Als $|a\rangle$ en $|b\rangle$ twee begintoestanden zijn die orthogonaal zijn, zoals $|0,\uparrow\rangle$ en $|0,\downarrow\rangle$ dan zijn de resulterende toestanden na t tijdstappen nog steeds orthogonaal. Deze zullen dus nooit in dezelfde stationaire toestand terecht kunnen komen.

De Hadamard-wandeling is maar een eenvoudig voorbeeld van een kwantumwandeling. We kunnen deze wat algemener maken door in plaats van de Hadamard-operator andere 2×2 unitaire matrices toe te laten als coin-operator. Nog algemener wordt het als we een algemene graaf toelaten in plaats van de discrete lijn. Bij een graaf waarbij alle knopen d buren hebben geven we het deeltje d interne toestanden en zal de coin-operator een unitaire $d\times d$-matrix zijn. In het algemeen kan ook van elke klassieke Markov-keten (een algemeen willekeurig proces waar de random walk een voorbeeld van is) een kwantumversie worden gemaakt. Ook in dit algemene geval geldt dat de kwantumwandeling zich kwadratisch sneller uitspreidt. Er bestaat ook een versie van de kwantumwandeling met een continue tijdsparameter. In dit geval is de unitaire operator van de vorm $e^{it\mathrm{H}}$ waarbij H de zogeheten Hamiltoniaan van het systeem is (niet te verwarren met de Hadamard-operator H). De Hamiltoniaan beschrijft de energie van het deeltje. In dit artikel gaan we niet verder in op zulke systemen.

Kwantumwandelingen in algoritmen

Zoekalgoritmen. We zullen nu bekijken hoe kwantumwandelingen in kwantumalgoritmen kunnen worden gebruikt. Stel dat we een lijst van N elementen hebben, bijvoorbeeld $1,2,\ldots,N$, en we zoeken een element in de lijst dat aan een bepaalde eigenschap voldoet. Het juiste element van de lijst noemen we ook wel het *gemarkeerde element* ('marked element') van de lijst. Een simpel klassiek algoritme is om de elementen van de lijst een voor een af te gaan en bij elk te controleren of het voldoet aan de gewenste eigenschap. Als we zo'n element vinden zijn we klaar. Dit algoritme kost in het slechtste geval N stappen, aannemend dat er in ieder geval één oplossing tussen zit. Een stap betekent hier het controleren van de eigenschap voor een gegeven element. De benodigde tijd voor dit algoritme is dus van de orde $O(N)$, dat wil zeggen de tijd schaalt lineair met N. Een ander algoritme is om steeds een *willekeurig* getal te kiezen en hiervan te controleren of het gemarkeerd is (oftewel of het voldoet aan de gewenste eigenschap). Dit herhalen we net zo lang tot we een oplossing vinden, aangenomen dat die er is. Dit lijkt een onhandige methode, maar gemiddeld zal dit ook $O(N)$ stappen kosten. Het kost soms meer stappen dan in het eerste algoritme, maar het verwachte aantal benodigde stappen is nog steeds lineair in N.

Het bovenstaande willekeurige algoritme kunnen we zien als een random walk op de *complete graaf*. De getallen vormen daarbij de knopen van de graaf, en tussen *elke* twee knopen zit een lijn. Het algoritme probeert een willekeurig getal, dus bevindt zich dan op een van de knopen. Vervolgens probeert het algoritme een ander willekeurig getal en dat betekent dat het naar een van de buren van de knoop beweegt. In dit geval zijn alle knopen buren en lijkt dit geen extra inzicht te geven.

We kunnen elk element van de lijst immers los van de andere bekijken om te controleren of het gemarkeerd is.

Er zijn echter veel problemen waarbij dit niet kan. In dat geval is er ook een lijst elementen waarvan er één of meer gemarkeerd zijn, maar is het niet mogelijk om direct elk element van de lijst te controleren. Om dit duidelijk te maken kijken we naar schaken. Het mogelijke spelverloop van een potje schaken kunnen we in een graaf weergeven. Elke knoop hoort bij een configuratie van de speelstukken en daarbij de kleur van de speler die aan zet is. Er zit een lijn tussen de knopen als het toegestaan is om van de ene naar de andere configuratie te gaan met een valide zet. De beginopstelling is bijvoorbeeld een witte knoop, en alle buren van deze knoop zijn zwarte knopen met opstellingen die je kan krijgen door precies één legale zet te doen met wit. Het verloop van een schaakspel is een pad door deze graaf.

Stel dat we nu de volgende vraag willen beantwoorden: kan ik in minder dan d beurten een paard op positie C4 krijgen en een loper op positie E5? Gegeven een knoop in de graaf die we zojuist omschreven kan men meteen controleren of er een paard op positie C4 staat en een loper op positie E5. Echter, of dit ook in minder dan d beurten kan is niet meteen duidelijk. Om dit te berekenen moeten we beginnen bij de huidige opstelling en alleen via de knopen van de graaf gaan om zo bij de knoop uit te komen die we zoeken.

In het algemeen is het probleem als volgt: gegeven is een graaf met N knopen en een beginknoop, en we zoeken één of meerdere knopen die gemarkeerd zijn. Het is hierbij alleen toegestaan om knopen te controleren die buren zijn van reeds gecontroleerde knopen. We mogen dus alleen 'via de graaf' naar andere knopen toe.

Bij een klassiek algoritme kan men aan de volgende procedure denken. Begin bij de beginknoop en kies een willekeurige buur. Controleer deze en als hij niet voldoet, kies dan opnieuw een willekeurige buur. Dit is hetzelfde algoritme als hiervoor, maar nu kiezen we alleen buren van de vorige knoop in plaats van een willekeurige knoop. Dit algoritme voert een random wandeling uit op de graaf, en met kansrekening kan men uitrekenen hoe lang het gemiddeld duurt tot we bij een gemarkeerd punt aankomen. De tijd die dit kost hangt af van de graaf.

Kwantumzoekalgoritmen. We kunnen nu een kwantumversie van dit algoritme maken. Een mogelijk idee zou zijn om een kwantumwandeling te beginnen op het beginpunt, analoog aan het klassieke algoritme. Dit werkt echter niet zomaar. Merk op dat we bij het klassieke algoritme meteen klaar zijn als we eenmaal bij een gemarkeerd punt zijn aangekomen. Bij de kwantumversie werkt zo'n idee echter niet. Als je namelijk meet op welke knoop je zit, dan ondergaat de kwantumtoestand een 'collapse'. Zoals we al zagen bij de Hadamard-wandeling krijg je het klassieke gedrag terug als je na iedere stap een meting doet. Een kwantumzoekalgoritme werkt dus iets anders. Hoewel we niet steeds kunnen meten is het echter *wel* mogelijk om in superpositie te controleren of een knoop gemarkeerd is zonder een meting te doen, net zoals een functie $f(n)$ op meerdere inputs kan worden berekend zonder te meten. Dit betekent dat het is toegestaan om op de gemarkeerde knopen een andere unitaire operatie uit te voeren dan op de andere knopen. Bij de Hadamard-wandeling hierboven zou dit betekenen dat we overal de Hadamard-operator toepassen behalve op een gemarkeerde knoop, waar een andere operator naar keuze wordt toegepast. Stel bijvoorbeeld dat positie 3 gemarkeerd is. Dan zou het volgende een voorbeeld kunnen zijn van een stap uit het kwantumalgoritme:

$$\begin{aligned}&|2,\downarrow\rangle+|-4,\uparrow\rangle+|3,\uparrow\rangle+|0,\downarrow\rangle\\ &\quad\to(\mathbb{1}\otimes H)\,|2,\downarrow\rangle+(\mathbb{1}\otimes H)\,|-4,\uparrow\rangle\\ &\qquad+(\mathbb{1}\otimes A)\,|3,\uparrow\rangle+(\mathbb{1}\otimes H)\,|0,\downarrow\rangle\end{aligned}$$

waarbij A de gekozen operator is voor de gemarkeerde knoop. Dit betekent niet meteen dat na deze stap de kans heel hoog is om de gemarkeerde knoop te vinden, maar door A slim te kiezen en precies het goede aantal stappen te zetten kan het kwantumalgoritme toch werken.

Grovers algoritme. We zullen nu eerst Grovers algoritme [2] beschrijven. We moeten een gemarkeerd element vinden uit een lijst van lengte N, en we kunnen elk element direct los bekijken zoals op de complete graaf. Grovers algoritme kan ook zonder de technieken van kwantumwandelingen worden beschouwd, maar het is illustratief om het in dit formalisme te bekijken. We gaan ervan uit dat er een operator O is waarmee we kunnen controleren of een element gemarkeerd is. Deze operator is gedefinieerd als

$$O\,|i\rangle=\begin{cases}|i\rangle \text{ als } i \text{ niet gemarkeerd is,}\\ -|i\rangle \text{ als } i \text{ wel gemarkeerd is,}\end{cases}\qquad 1\le i\le N.$$

De operator O wordt ook wel het *orakel* ('oracle') genoemd, en kan bijvoorbeeld een ander algoritme zijn dat controleert of het getal i aan een vergelijking voldoet. Wat dit andere algoritme ook is, het kan vrijwel altijd in deze vorm worden geschreven en dus zullen we nu aannemen dat zo'n operator bestaat. Merk op dat O precies overeenkomt met het toepassen van de identiteitsoperator $\mathbb{1}$ op de niet-gemarkeerde knopen en de operator $-\mathbb{1}$ op de gemarkeerde knopen.

Om verder te gaan, bekijken we nu eerst de *uniforme superpositie*:

$$|U\rangle=\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle\,.$$

Deze superpositie is over alle elementen uit de lijst waarbij elk element dezelfde amplitude $1/\sqrt{N}$ heeft. Vervolgens hebben we een operator R nodig die gedefinieerd is als

$$R=2\,|U\rangle\langle U|-\mathbb{1}.$$

Dit is de *reflectie in* $|U\rangle$. Merk op dat $R\,|U\rangle=|U\rangle$, en als $|\phi\rangle$ een toestand is die loodrecht staat op $|U\rangle$, dan geldt $R\,|\phi\rangle=-|\phi\rangle$ omdat $\langle U|\phi\rangle=0$. Deze operator R speelt de rol van 'een stap zetten in de graaf'. Er geldt namelijk dat $R\,|i\rangle$ een superpositie over alle buren van knoop i is (inclusief i zelf).

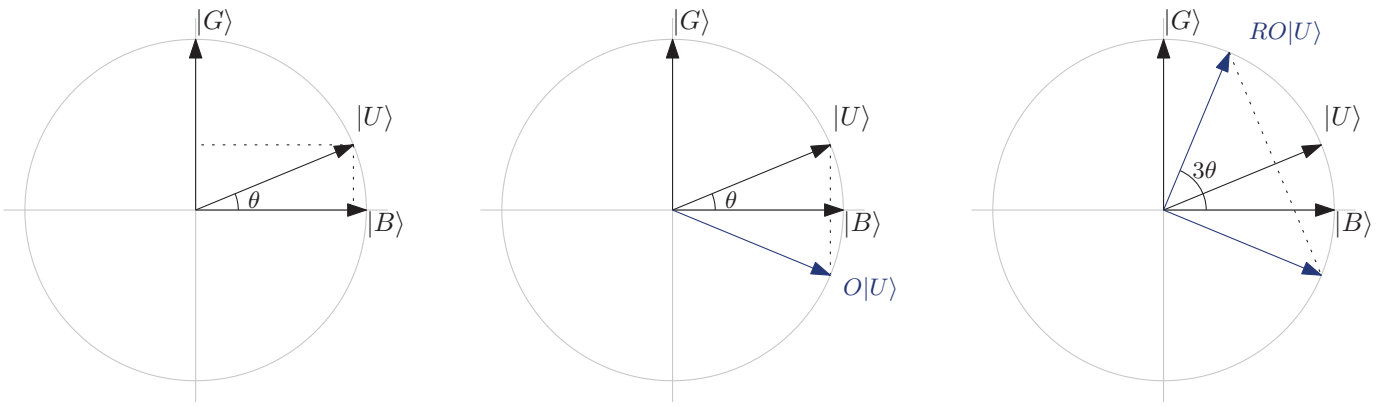
Het kwantumalgoritme van Grover is:

- maak de toestand $|\,U\,\rangle$ aan;
- pas T keer de operator $R\circ O$ toe;

waarbij we later zullen specificeren wat T is. We gaan nu kijken hoe en waarom dit werkt. Laten we aannemen dat er precies één gemarkeerd element is, dat we noteren met $|G\rangle$ ('good'). In dat geval kunnen we de som van $|U\rangle$ splitsen in $|G\rangle$ en een som zonder $|G\rangle$ die we met $|B\rangle$ ('bad') aanduiden:

$$\begin{aligned}|U\rangle&=\frac{1}{\sqrt{N}}\sum_{\substack{i=0\\ i\neq G}}^{N-1}|i\rangle+\frac{1}{\sqrt{N}}\,|G\rangle\\ &=\sqrt{\frac{N-1}{N}}\,|B\rangle+\sqrt{\frac{1}{N}}\,|G\rangle\,.\end{aligned}$$

De factor $\sqrt{(N-1)/N}$ is zo gekozen dat $|B\rangle$ genormaliseerd is. Merk op dat $|B\rangle$ en $|G\rangle$ loodrecht zijn omdat ze uit verschillende basisvectoren zijn gebouwd. Als we nu de



Figuur 3 Links: de begintoestand $|U\rangle$van Grovers algoritme. Midden: de toestand na het toepassen van de operator O. Rechts: de toestand na het toepassen van O en R.

operator O toepassen vinden we $O\,|B\rangle = |B\rangle$ en $O\,|G\rangle = -|G\rangle$, direct uit de definitie van O. We kunnen dit weergeven door $|U\rangle$ te tekenen in de $|B\rangle$-, $|G\rangle$-basis, zie het linker diagram in Figuur 3. Het systeem begint in de toestand $|U\rangle$ en na het toepassen van de operator O wordt het gespiegeld in de horizontale as, zoals weergegeven in het middelste diagram. De operator R spiegelt per definitie in de begintoestand $|U\rangle$, en het resultaat daarvan is weergegeven in het rechter diagram van Figuur 3.

In de figuur is de hoek tussen $|U\rangle$ en $|B\rangle$ aangegeven met θ. We kunnen $|U\rangle$ schrijven als

$$|U\rangle = \cos\theta\,|B\rangle + \sin\theta\,|G\rangle,$$

dus geldt $\sin\theta = 1/\sqrt{N}$ en $\cos\theta = \sqrt{(N-1)/N}$. Als N voldoende groot is, dan is $1/\sqrt{N}$ voldoende klein zodat er geldt $\sin\theta \approx \theta$, dus $\theta \approx 1/\sqrt{N}$.

De figuur laat zien dat de hoek na één toepassing van $R \circ O$ gelijk is aan 3θ. Met elke iteratie van $R \circ O$ zal de hoek met 2θ verhogen, dus na T stappen zal de hoek gelijk zijn aan $\theta + 2T\theta$. We willen uitkomen in de toestand $|G\rangle$, dus we moeten het aantal stappen T zo kiezen dat de hoek uiteindelijk gelijk is aan $\pi/2$, en dit is het geval als $T = \frac{\pi}{4\theta} - \frac{1}{2}$. De waarde van T moet een geheel getal zijn, dus voor veel waarden van θ komt dit niet meteen uit. Het heeft geen zin om langer door te gaan want dan draait het systeem te ver door en komen we uiteindelijk in $-|B\rangle$ uit. We kunnen de waarde $\frac{\pi}{4\theta} - \frac{1}{2}$ echter simpelweg afronden. Het systeem zal dan niet *exact* in $|G\rangle$ uitkomen maar wel erg dichtbij en is de kans om $|G\rangle$ te meten heel hoog. Naarmate N groter wordt, worden θ en de afrondfout kleiner.

Voor grote waarden van N geldt dus $T \approx \frac{\pi}{4}\sqrt{N}$. De tijd schaalt dus met $\sqrt{N}$ in plaats van N zoals bij een klassiek algoritme! Ongeacht hoe snel klassieke computers ook worden, een kwantumcomputer is altijd sneller, als de lengte N van de lijst groot genoeg is.

Kwantumwandeling-algoritmes. Het kwantumwandeling-zoekalgoritme op een algemene graaf begint door eerst een aantal stappen te zetten om in de *uniforme* superpositie $|U\rangle$ uit te komen zoals bij Grover. Als de zoekgraaf de complete graaf is zal dit één stap kosten, en als de graaf een lijn is zal dit N stappen kosten. In deze fase wordt nog niets speciaals met de gemarkeerde knoop gedaan. Vervolgens kan een kwantumwandeling worden uitgevoerd met verschillende operatoren op de gemarkeerde en ongemarkeerde knopen. Het hangt van de graaf af hoe snel het algoritme wordt. Voor sommige grafen is de kwantumversie niet sneller dan zijn klassieke tegenhanger.

Tot slot

We hebben laten zien hoe de kwantummechanica ons toestaat om andere algoritmes te maken die soms sneller zijn dan de klassieke algoritmes voor hetzelfde probleem. Er blijft nog veel werk te doen, want voor veel problemen is het nog niet duidelijk of een kwantumcomputer ze sneller kan doen dan een klassieke computer en zo ja, hoeveel sneller het kan. Het onderzoek is vooralsnog enkel theoretisch omdat er op dit moment nog geen kwantumcomputers zijn die goed genoeg zijn om berekeningen mee te doen. De hoop is dat dit over tien of twintig jaar wel het geval is en dat de benodigde algoritmes dan klaarliggen voor gebruik.

Referenties

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

2 L. Grover, A fast quantum mechanical algorithm for database search, *Proceedings 28th Annual ACM Symposium on the Theory of Computing* (1996).