Ronald de Wolf
CWI, Amsterdam
en ILLC, Universiteit van Amsterdam
rdewolf@cwi.nl

Onderzoek Vidi-project

Kwantumcomputers

Van december 2008 tot februari 2014 werkt Ronald de Wolf aan het Vidi-project 'Quantum computing: fault-tolerance, communication, and classical spin-offs'. Dit project gaat over het gebruik van kwantummechanische technieken in de informatica. Sinds het eerste kwart van de twintigste eeuw domineert de kwantummechanica de natuurkunde van het 'kleine': het gedrag van deeltjes als fotonen, elektronen, atomen, enzovoort. Hoewel de combinatie van de kwantummechanica met de relativiteitstheorie (die de zwaartekracht beschrijft) problematisch is, zijn tot nu toe al haar experimentele voorspellingen uitgekomen. Kwantummechanica is veel meer dan alleen esoterische theorie: volgens sommige berekeningen is een derde van ons Bruto Nationaal Product afhankelijk van onze kennis van de kwantummechanica, denk bijvoorbeeld aan elektronische apparatuur.

Kwantummechanica heeft allerlei tegen-intuïtieve effecten, zoals *superpositie* van verschillende toestanden, constructieve en destructieve *interferentie*, en *verstrengeling* tussen verschillende kwantumsystemen. Sinds het werk van Feynman [12] en Deutsch [9] in de jaren tachtig wordt er geprobeerd om dit soort vreemde effecten te gebruiken om computers te verbeteren: te versnellen, veiliger te maken, enzovoort.

Er zijn grofweg twee soorten vragen die onderzoekers zich hierover stellen: (1) kun je een grote kwantumcomputer bouwen? en (2) wat zou zo'n computer kunnen doen? De eerste vraag is voer voor experimenteel natuurkundigen. Er is gestage vooruitgang op dit gebied, hoewel de grootste kwantumcomputers die tot nu toe gerealiseerd zijn maar op een handvol kwantumbits werken. Informatici richten zich op de tweede vraag: wat zijn de potentiële toepassingen van een kwantumcomputer? Een aantal belangrijke voorbeelden zijn het algoritme van Shor [21] voor het efficiënt vinden van de priemfactoren van grote getallen (dit breekt allerlei veelgebruikte cryptografie, zoals RSA), het algoritme van Grover [15] voor het doorzoeken van grote databases, en het protocol van Bennett en Brassard [4] voor het veilig uitwisselen van geheime sleutels over een publiek kwantumcommunicatiekanaal.

In dit Vidi-project heb ik, samen met promovendus Giannicola Scarpa en postdocs Fernando de Melo en Niel de Beaudrap, geprobeerd de theorie van kwantumcomputers verder te ontwikkelen en meer toepassingen te vinden.

Het project en de resultaten

Aangezien dit project fundamenteel onderzoek is, zijn de voornaamste resultaten publicaties: dertien artikelen in tijdschriften, dertien artikelen in proceedings van conferenties, en zes preprints die naar verwachting de komende tijd ook in tijdschriften of proceedings zullen verschijnen. Daarnaast was er één proefschrift, van Giannicola Scarpa.

Hieronder zal ik de drie onderdelen van het project bespreken met een paar van de interessantste uitkomsten. Het eerste onderdeel viel een beetje tegen, de andere twee waren behoorlijk succesvol.

Fout-tolerante kwantum computers

Het eerste onderdeel van het project was gericht op technieken om kwantumcomputers te beschermen tegen ruis en kleine foutjes in de implementatie van de operaties. Zulke foutjes zijn vrijwel onvermijdelijk wanneer je een echte kwantumcomputer wilt bouwen, dus het is essentieel dat we daarvoor kunnen corrigeren. Een van de belangrijkste theoretische resultaten is de 'fault-tolerant threshold theorem' [1]. Dit zegt dat als je de fout per operatie kleiner kunt maken dan een bepaalde constante waarde p (de 'threshold'), en als de fouten op de verschillende operaties niet al te sterk gecorreleerd zijn, dan kun je je kwantumcomputer 'fault-tolerant' maken, dat wil zeggen je kunt de kans dat het eind-antwoord fout is zo klein maken als je wilt. De precieze waarde van deze p is natuurlijk erg belangrijk — het vertelt experimentalisten hoe precies ze hun operaties moeten implementeren om een werkende kwantumcomputer mogelijk te maken. Er is nog veel onzekerheid over deze waarde: p is minstens $0{,}1$ procent [2] en hoogstens ongeveer 36 procent [17]. Numerieke experimenten suggereren dat de correcte waarde boven 1 procent ligt [16].

Het voornaamste doel van dit deel van het project was om de waarde van de threshold veel preciezer te bepalen. Dit is helaas niet gelukt, we zijn er niet in geslaagd om de ondergrenzen en/of de bovengrenzen op p te verbeteren (overigens is er ook in de rest van de wereld de afgelopen vijf jaar geen vooruitgang geboekt op dit punt). Het interessantste wat wel uit dit project is gekomen is een artikel van de Melo et al. [19] dat nieuwe (maar

nog steeds niet erg precieze) boven- en ondergrenzen geeft op de waarde van de threshold wanneer zogenaamde 'Majorana Fermionen' gebruikt worden voor de kwantumbits.

Kwantumcommunicatie

Sommige van de interessantste kwantummechanische toepassingen betreffen netwerken van verschillende computers. Soms gaat het hierbij om het *beveiligen* van gegevens en communicatie (kwantumcryptografie) en soms om het *minimaliseren* van de benodigde hoeveelheid communicatie tussen de verschillende computers (kwantumcommunicatie-complexiteit). Het project leverde een aantal publicaties op over kwantumcommunicatie-complexiteit, maar het interessantste resultaat hier is waarschijnlijk een toepassing op zogenaamde *kwantum-non-lokaliteit*, die we hieronder zullen bespreken.

Stel je een spel voor met twee spelers, die we Alice en Bob zullen noemen, en die onderling niet mogen communiceren. Beide spelers krijgen een invoer, respectievelijk x en y, volgens een bepaalde waarschijnlijkheidsverdeling. Beide spelers geven daarop een uitvoer, respectievelijk a en b. De regels van het spel stipuleren dat (gegeven het invoerpaar x, y) sommige uitvoerparen het spel 'winnen' en andere uitvoerparen het spel 'verliezen.' Het doel van de spelers is om de kans om het spel te winnen te maximaliseren. Laten we de maximale winkans van spelers die de klassieke natuurkunde volgen ω noemen. Bovengrenzen op deze waarde ω staan bekend als Bell-ongelijkheden, genoemd naar Jon Bell [6]. Het blijkt nu dat als de spelers *kwantumverstrengeling* delen, dat ze hun gedrag beter kunnen coördineren en dat de winkans soms hoger wordt. Laten we de maximale winkans die mogelijk is met behulp van verstrengeling ω^* noemen. Elk spel waarbij $\omega^* > \omega$ wordt een 'schending van de Bell-ongelijkheid' genoemd. In simpele gevallen kunnen dit soort verstrengelingstrategiën in het laboratorium worden uitgevoerd, en dan blijkt de kwantumwinkans inderdaad hoger te zijn dan het maximale wat klassieke spelers kunnen bereiken. Dit soort experimenten heeft een diepere betekenis: ze laten zien dat onze wereld zich niet gedraagt volgens wat voor 'klassieke' natuurkunde dan ook. Het is interessant om spellen te ontwerpen die het verschil tussen de kwantumen de klassieke winkans (gemeten als de ratio ω^*/ω) zo groot mogelijk maken. In [7] hebben we spellen beschreven waarbij deze ratio vrijwel maximaal is (als functie van de 'hoeveelheid' verstrengeling waarmee de spelers beginnen), gebaseerd op eerdere resultaten uit de kwantumcommunicatie-complexiteit.

Een tweede hoogtepunt is het proefschrift van Giannicola Scarpa [20], wat ook over nonlokaliteit gaat. Neem als voorbeeld het volgende spel. Er is een bepaalde graaf G die bekend is gemaakt aan Alice en Bob. Alice en Bob krijgen elk een knoop van G als invoer en moeten (zonder te communiceren) een kleur als uitvoer geven met de volgende eigenschappen: als Alice en Bob dezelfde knoop als invoer krijgen dan moeten ze *dezelfde* kleur als uitvoer geven, en als hun twee invoerknopen een kant in G vormen dan moeten ze *verschillende* kleuren als uitvoer geven. Wat is het minimale aantal verschillende kleuren dat Alice en Bob moeten gebruiken om dit spel met zekerheid te kunnen winnen? Dat blijkt het chromatisch getal $\chi(G)$ van de graaf G te zijn: het minimale aantal kleuren dat je nodig hebt om de knopen van G te kleuren zodanig dat buurknopen een verschillende kleur hebben. Het blijkt dat er (voor sommige grafen) strategiën zijn die door gebruik van kwantumverstrengeling minder kleuren nodig hebben om het spel met zekerheid te kunnen winnen. Dit leidt tot een definitie van het *kwantumchromatisch getal* van de graaf G [8]. Scarpa et al. bewijzen allerlei eigenschappen van dit soort kwantumgraafparameters, en laten in het bijzonder zien dat voor sommige grafen het kwantumchromatisch getal exponentieel kleiner kan zijn dan het chromatisch getal. Scarpa et al. hebben ook voorbeelden gegeven waarbij kwantumverstrengeling de capaciteit van een klassiek communicatiekanaal flink kan verhogen.

Toepassingen op klassieke problemen

De laatste tien jaar zijn er een aantal verrassende toepassingen gevonden van *quantum computing* (beter gezegd: van de wiskundige technieken die ontwikkeld zijn in dit vakgebied) op problemen in de klassieke informatica en de wiskunde. Een van de eerste voorbeelden hiervan was een ondergrens voor bepaalde fout-corrigerende codes [18]. Dit loste een open vraag op over klassieke codes, maar het bewijs maakte essentieel gebruik van technieken uit de kwantuminformatietheorie. Dit kun je vergelijken met het bewijzen van eigenschappen van reële getallen door gebruik te maken van de complexe getallen, of met Paul Erdős' 'probabilistic method' waarin existentie-bewijzen gegeven worden met behulp van gereedschap uit de waarschijnlijkheidsrekening. Sindsdien zijn er nog een aantal andere voorbeelden van dit fenomeen gevonden, en het doel van dit deel van het project was om meer van zulke onverwachte toepassingen van het 'kwantumgereedschap' te vinden. Ik zal er hieronder twee noemen. Voor meer voorbeelden, zie het overzicht van Drucker en mijzelf [10]. Merk op dat voor dit soort toepassingen geen grote kwantumcomputer nodig is. We gebruiken hier alleen het wiskundig gereedschap dat voor de analyse van kwantumcomputers ontwikkeld is.

Polynomen

Ten eerste kunnen we gebruikmaken van een al bekende connectie tussen kwantumalgoritmes en polynomen [5]: grof gezegd kan de output van een kwantumalgoritme geschreven worden als een polynoom over de inputvariabelen. Hoe efficiënter het algoritme, hoe lager de graad van het polynoom. Dit betekent dat je soms het bestaan van lagegraadspolynomen met bepaalde gewenste eigenschappen kunt bewijzen door middel van het construeren van efficiënte kwantumalgoritmes.

Samen met Drucker heb ik dit gebruikt om een nieuw bewijs te geven van de stelling van Jackson uit de analyse [11]. Deze stelling is een kwantitatieve versterking van de beroemde stelling van Weierstrass, die zegt dat elke continue functie op een gesloten interval willekeurig goed kan worden benaderd door een polynoom. Jacksons versterking geeft aan hoe klein we de benaderingsfout kunnen maken, in termen van de 'gladheid' van de te approximeren functie, en de maximale graad die het approximerende polynoom mag hebben. Door gebruik te maken van efficiënte kwantumalgoritmes voor het tellen van het aantal enen in een gegeven binaire string, konden we een nieuw bewijs geven van deze klassieke stelling.

Een andere toepassing van deze connectie komt van Ambainis en mijzelf [3]. Met Fourieranalytische technieken konden we laten zien wat de minimale graad is van polynomen die een n-bits functie approximeren; en met behulp van efficiënte kwantumalgoritmes konden we laten zien dat er functies bestaan waarvoor onze ondergrens op de graad optimaal is.

Het handelsreizigersprobleem

Ten tweede hebben we een resultaat over kwantumcommunicatie kunnen gebruiken om te laten zien dat lineaire programma's voor

het bekende *handelsreizigersprobleem* ('traveling salesman problem') exponentieel groot moeten zijn [13–14]. Deze onverwachte connectie loste een oud open probleem op, en kreeg de 'Best Paper Award' op de STOC'12-conferentie. Dit resultaat is waarschijnlijk het interessantste dat uit dit Vidi-project is gekomen.

In het handelsreizigersprobleem moeten we, op een gegeven graaf met n knopen en gewichten op de kanten, een kortste tour vinden die precies één keer langs elke knoop gaat en die terugkeert op zijn beginpunt. Dit is een van de bekendste 'NP-harde' problemen. Waarschijnlijk (als $P \neq NP$) is er geen efficiënt algoritme voor — maar niemand weet hoe we dit kunnen bewijzen. Het handelsreizigersprobleem correspondeert met het optimaliseren van een lineaire functie (de lengte van de route) over de *polytoop* die opgespannen wordt door alle tours door de graaf. Als je deze polytoop met een klein aantal lineaire ongelijkheden zou kunnen karakteriseren, dan heb je een lineair programma waarmee je efficiënt het handelsreizigersprobleem kunt oplossen. In de jaren tachtig waren er mensen die claimden dit te kunnen [22]. Yannakakis [24] bewees al in 1987 dat de 'symmetrische' manier waarop dit gebeurde niet kon werken. Wij hebben nu laten zien dat *elke* set van ongelijkheden voor deze polytoop exponentieel groot moet zijn, zelfs wanneer je allerlei hulpvariabelen en niet-symmetrische stelsels ongelijkheden mag gebruiken. Dit bewijst dat een grote klasse van programma's niet in staat is efficiënt het handelsreizigersprobleem op te lossen.

Waar zit nu de connectie met kwantumcommunicatie? Yannakakis liet al zien dat het aantal benodigde ongelijkheden precies gelijk is aan de 'positieve rank' van de zogenaamde '*slack matrix*' die bij de polytoop hoort. Voor een ondergrens op het aantal ongelijkheden is het dus voldoende om een submatrix van de bijbehorende *slack matrix* te vinden die aantoonbaar een hoge positieve rank heeft. Nu bleek een matrix die ik tien jaar eerder gebruikt en geanalyseerd had om iets te bewijzen over kwantumcommunicatiecomplexiteit [23], hiervoor precies te passen.

Conclusie

Kwantumcomputers zijn veelbelovend, maar er moet nog veel gebeuren om die belofte uit te laten komen. Het zou mooi zijn als iemand kan aantonen dat de 'fault-tolerance threshold' redelijk hoog is. Dat zou het makkelijker maken om een grote kwantumcomputer in het lab te maken. En hopelijk worden er in de toekomst nog meer toepassingen gevonden zoals kwantumalgoritmes, communicatie-protocollen, enzovoort. Dit project heeft een aantal bijdrages geleverd aan dit laatste. Sommige van deze bijdrages zijn afhankelijk van de bouw van een grote kwantumcomputer, andere bijdrages zijn toepassingen van kwantumwiskundig gereedschap op de klassieke informatica en wiskunde, en zijn daarom vandaag al relevant. Inmiddels heeft de EU mij een ERC Consolidator Grant toegekend, waarmee ik dit onderzoek voort kan zetten.

Referenties

1 D. Aharonov en M. Ben-Or, Fault tolerant quantum computation with constant error, in *Proceedings of 29th ACM STOC*, 1997, pp. 176–188.

2 P. Aliferis, D. Gottesman en J. Preskill, Accuracy threshold for postselected quantum computation, *Quantum Information and Computation* 8 (2008), 181–244.

3 A. Ambainis en R. de Wolf, How low can approximate degree and quantum query complexity be for total boolean functions?, in *Proceedings of 28th IEEE Annual Conference on Computational Complexity (CCC'13)*, 2013, pp, 179–184.

4 C. H. Bennett en G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, 1984, pp, 175–179.

5 R. Beals, H. Buhrman, R. Cleve, M. Mosca en R. de Wolf, Quantum lower bounds by polynomials, *Journal of the ACM* 48 (2001), 778–797.

6 J. S. Bell, On the Einstein-Podolsky-Rosen paradox, *Physics* 1 (1964), 195–200.

7 H. Buhrman, O. Regev, G. Scarpa en R. de Wolf, Near-optimal and explicit Bell inequality violations, *Theory of Computing* 8 (2012), 623–645.

8 P. J. Cameron, A. Montanaro, M. W. Newman, S. Severini en A. Winter, On the quantum chromatic number of a graph, *Electronical Journal of Combinatorics* 14 (2007).

9 D. Deutsch, Quantum theory, the Church–Turing principle, and the universal quantum Turing machine, iln *Proceedings of the Royal Society of London*, Vol. A400, 1985, pp. 97–117.

10 A. Drucker en R. de Wolf, Quantum proofs for classical theorems, *Theory of Computing*, 2011, ToC Library, Graduate Surveys 2.

11 A. Drucker en R. de Wolf, Uniform approximation by (quantum) polynomials, *Quantum Information and Computation* 11 (2011), 215–225.

12 R. Feynman, Simulating physics with computers, *International Journal of Theoretical Physics* 21 (1982), 467–488.

13 S. Fiorini, S. Massar, S. Pokutta, H. R. Tiwary en R. de Wolf, Linear vs. semidefinite extended formulations: exponential separation and strong lower bounds, in *Proceedings of 44th ACM STOC*, 2012, pp 95–106.

14 S. Fiorini, S. Massar, S. Pokutta, H. R. Tiwary en R. de Wolf, Exponential lower bounds for polytopes in combinatorial optimization, te verschijnen in *Journal of the ACM*, 2014.

15 L. K. Grover, A fast quantum mechanical algorithm for database search, in *Proceedings of 28th ACM STOC*, 1996, pp. 212–219.

16 M. Knill, Quantum computing with realistically noisy devices, *Nature* 434 (2005), 39–44.

17 J. Kempe, O. Regev, F. Unger en R. de Wolf, Upper bounds on the noise threshold for fault-tolerant quantum computing, *Quantum Information and Computation* 10 (2010), 361–376.

18 I. Kerenidis en R. de Wolf, Exponential lower bound for 2-query locally decodable codes via a quantum argument, in *Proceedings of 35th ACM STOC*, 2003, pp. 106–115.

19 F. de Melo, P. Cwiklinski en B. M. Terhal, The power of noisy fermionic quantum computation, *New Journal of Physics* 15 (2013), 013015.

20 G. Scarpa, *Quantum entanglement in non-local games, graph parameters and zero- error information theory*, PhD thesis, University of Amsterdam, 2013.

21 P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Journal on Computing* 26 (1997), 1484–1509 (eerdere versie in FOCS'94).

22 T. Swart, P = NP, Technical report, University of Guelph, 1986. Revision 1987.

23 R. de Wolf, Characterization of non-deterministic quantum query and quantum communication complexity, in *Proceedings of 15th IEEE Conference on Computational Complexity*, 2000, pp. 271–278.

24 M. Yannakakis, Expressing combinatorial optimization problems by linear programs (extended abstract), in *Proceedings of 20th ACM STOC*, 1988, pp. 223–228.