Publicatie : Automatisering Gids
Datum : 22 jan 2016
cm2 : 1.305
Pagina : 16
Advertentiewaarde : € 17.850,00
Regio : Nederland
Frequentie : 1x per 2 weken_do
Oplage : 16.042

INTERVIEW

Harry Buhrman, directeur van QuSoft:

Het zou stupide zijn kwantumhardware

Terwijl de overheid miljoenen subsidie verstrekt aan R&D op het gebied van kwantumhardware, lijken weinigen zich te realiseren dat een fundamenteel anders werkende computer ook fundamenteel anders werkende software nodig zal hebben. "Laten we niet de fout maken uit de jaren vijftig."

door: ROLF ZAAL / R.ZAAL@AUTOMATISERINGGIDS.NL **beeld:** DE BEELDREDAKTIE / PETER STRELITSKI

De kwantumcomputer zou zomaar een enorme deceptie kunnen worden. Er is niet alleen weinig software voor, maar we weten ook nog nauwelijks hoe we er meer bij kunnen maken. Feitelijk kennen we ook nog maar weinig problemen waarvan duidelijk is dat die met een kwantumcomputer efficiënter zijn op te lossen dan op een 'klassieke' computer. Ondertussen raast de hardwareontwikkeling richting 50 qubit; de drempel waarbij de kwantumcomputer qua rekenvermogen de huidige supercomputers voorbijstreeft. Waarschijnlijk wordt dat punt al binnen vijf jaar bereikt. "Om dan wat betreft software niet met lege handen te staan, moet nog heel veel denkwerk worden verzet", constateert directeur Harry Buhrman van QuSoft.
QuSoft ging vorige maand van start op het Science Parc in Amsterdam Oost. De oprichtende instellingen, CWI, UvA en VU, willen met QuSoft een software-pendant creëren voor het hoofdzakelijk op hardware gerichte onderzoekcentrum QuTech in Delft. De UvA brengt mensen in van de vakgroepen Physics, Wiskunde, Informatica en Language, Logic and Computation. CWI brengt mensen in vanuit de groepen Algorithms & Complexity, Cryptology en Networks & Optimization. En de VU draagt informatici bij.

Wordt er nog samengewerkt met andere kwantumonderzoekscentra?
"Jazeker. We hebben intensief contact met QuTech in Delft, dat zich natuurlijk primair op kwantumhardware richt. Verder kom ik zeer regelmatig over de vloer bij het instituut voor quantum computing (IQC) van de Universiteit of Waterloo. Ik zit daar ook in de scientific advisory board. En ik heb uitstekende contacten met Google, dat fors in quantum computing investeert."

Google? Dan volg je, neem ik aan, ook hun experimenten met de D-Wave-computer?
"Ik heb contact met een andere groep. Ik kan dus niet veel zeggen over de D-Wave-hardware. Geweldig áls ze 1000 qubits hebben. De grote vraag is óf ze die daadwerkelijk hebben, en of ze er ook stabiel mee kunnen rekenen.
Ik las dat ze een versnelling van 10^8 zouden hebben. Maar dat is niet ten opzichte van de beste klassieke algoritme voor dat probleem. Als je het daartegen afzet levert de D-Wave-machine geen versnelling. Kortom: 'the jury is still out'.
De discussie rondom D-Wave laat overigens wel zien dat wat QuSoft doet hard nodig is. Eén van onze onderzoekslijnen stelt zich precies die vraag: Hoe weet je of een kwantumcomputer doet wat hij zou moeten

Publicatie : Automatisering Gids
Datum : 22 jan 2016
cm2 : 1.305
Pagina : 16
Advertentiewaarde : € 17.850,00
Regio : Nederland
Frequentie : 1x per 2 weken_do
Oplage : 16.042

alleen in te investeren

doen? Dat is wat nu beantwoord moet worden in het geval van D-wave. En mocht D-Wave zo'n 'test of quantumness' doorstaan, dan hebben ze duidelijk behoefte aan meer kwantumapplicaties."

Ben je nooit jaloers op de media-aandacht en de funding voor het onderzoek op het gebied van kwantumhardware?
"Niet jaloers, nee. Het is geweldig dat kwantumhardware zo'n aandacht krijgt. Maar het onderstreept wel onze uitdaging om duidelijk te maken dat kwantumsoftware zeker niet minder belangrijk is. Dat wordt nu nog onvoldoende ingezien. Wat dat betreft bevinden we ons met de kwantuminformatica in een fase die vergelijkbaar is met de situatie rond computers in de jaren vijftig. Die hardware was programmeerbaar, maar men had geen flauw idee dat die programmeerbaarheid de weg opende naar de immense verscheidenheid aan toepassingen die we nu kennen. En waarvan we nu pas beginnen te beseffen dat die ontwikkeling voorlopig nog doorgaat en tot een zodanige toename van het aantal computers leidt dat we ze eigenlijk steeds minder gaan zien. Het is de software die deze groei van het aantal toepassingen aanjaagt; en voor de kwantumcomputer zal dat niet anders zijn.
Als die prachtige, glimmende 50qubit-computer er straks staat, maar er is geen software die er spannender dingen mee kan dan razendsnel grote getallen factoriseren of grote databases doorzoeken, tja, dan is dat vanuit wetenschappelijk oogpunt natuurlijk een geweldige prestatie. Maar ik denk niet dat dat dan maatschappelijk of economisch zoden aan de dijk zal zetten. Dus laten we niet de fout maken uit de jaren vijftig. Het zou stupide zijn alleen te investeren in hardware en niet in software."

Databases doorzoeken, dat is toch een centraal thema in de informatica, dat is toch niet triviaal? En moleculaire systemen simuleren om chemische of mechanische eigenschappen te voorspellen, dat is toch ook een lang gekoesterde belofte?
"Zeker, maar de software die daarvoor nodig is kunnen we nog niet maken. Het ontbreekt ons nog aan inzicht in de architectuur die nodig is om kwantumsystemen zo in te richten dat ze programmeerbaar zijn. Zelfs bij de huidige systemen van minder dan tien qubits weten we nog niet goed hoe we dat moeten doen. Die systemen vormen nu een speeltuin om kennis op te doen die we dan kunnen toepassen op grotere systemen.
Voor real life toepassingen heb je al gauw kwantumsystemen nodig met tientallen zo niet honderden qubits. En dan komen er heel andere problemen om de hoek kijken, onder meer rond kwantumtesten, -verificatie en debugging. Of een factorisatie klopt is natuurlijk snel te controleren, maar voor vrijwel alle andere zinnige problemen waarop je een kwantumcomputer zou willen inzetten geldt dat het verdraaid lastig wordt om de uitkomsten te valideren.
Als je op een 300 qubit-systeem een complex molecule wilt nabootsen of een echt lastig databaseprobleem wilt oplossen, en het ding produceert een uitkomst, hoe beoordeel je dan of die correct is, of er niet toch geen foutje in je kwantumhardware of -software zit? De klassieke manier van debuggen, even stopzetten tussenstanden van variabelen uitlezen, dat gaat bij een kwantumcomputer niet lukken, want uitlezen bederft het hele principe waarop de kwantumcomputer is gebaseerd."

Oké, maar voor je gaat debuggen en testen, moet je wel iets te programmeren hebben. Wat zouden we op een kwantumcomputer willen kunnen maar kunnen we nog niet?
"Dat is nu net het probleem; we hebben nog nagenoeg geen zicht op de mogelijkheden. We vermoeden mogelijkheden met onder meer deep learning en met simulatie. Maar er is van maar heel weinig problemen echt duidelijk of het met een kwantumsysteem werkelijk efficiënter kan dan op een klassieke computer. Laat staan dat we er algoritmen voor hebben, afgezien van een zeer beperkt aantal successen zoals van Schor (factoriseren), Grover (databases doorzoeken, efficiënt vergelijken van agenda's) en het BB84-protocol (een door Bennet en Brassard ontwikkelde werkwijze om een cryptografische sleutel te maken die veilig over een onbeveiligde lijn kan worden doorgegeven).
Overigens zijn er andersom ook maar heel weinig problemen waarvan bewezen is dat ze met een kwantumcomputer niét sneller zijn op te lossen dan met een conventioneel systeem. Daar tussenin is een immens veld van problemen die met een kwantumcomputer misschien efficiënter zijn aan te pakken dan met een klassieke computer. Maar welke en hoe, daar hebben we nog nauwelijks zicht op."

Waar ziet QuSoft dan kansen?
"Theoretisch is simulatie van de complexe natuurlijke systemen iets waar de kwantumcomputer bij uitstek geschikt voor zou moeten zijn. Maar volgens de huidige inzichten zijn daarvoor wel enorme aantallen qubits nodig. Misschien wel een miljoen. De uitdaging is nu te kijken of er met minder, 300 of hopelijk 50, ook al zinnige simulaties denkbaar zijn. Dat weten we nog niet.
Tegelijkertijd weten we wel dat het voor onderzoekers op het gebied van hardware een extreme uitdaging is om meer qubits in één systeem te verenigen. Zowel QuTech als Google staan nu op het punt om een 10 qubit-computer te realiseren. Geweldig natuurlijk, maar niet iets waarmee je dingen kunt die in een klassiek systeem niet ook te doen zijn. Daarvoor moet je eerder aan 50 qubit denken. »

HOE WERKT EEN KWANTUMCOMPUTER?

Een kwantumcomputer werkt op basis van het slim uitbuiten van de ongerijmde mechanismen die bepalend zijn voor gebeurtenissen op subatomaire schaal. Zo wordt onder meer gebruik gemaakt van het fenomeen dat kwantumdeeltjes zich in twee ogenschijnlijk onverenigbare toestanden tegelijk kunnen bevinden. Een zeer klein deeltje (een molecuul of kleiner nog) is dan in een zogenoemde superpositie van toestanden. Veelal gaat het om de 'spin' van zo'n deeltje, dat dan op éénzelfde moment in twee tegengestelde richtingen kan tollen. De 'keuze' voor één van de twee mogelijkheden wordt pas gemaakt als de draairichting – in meer dan één betekenis van het woord – wordt 'vastgesteld'.
Bij quantum computing wordt van dat 'uitstel van bepaaldheid' gebruik gemaakt door in superpositie verkerende deeltjes in te zetten als geheugenelementen – zogeheten qubits – die gedurende de berekening gelijktijdig een 1 én een 0 representeren. Dit in tegenstelling tot conventionele bits, die slechts een 1 óf een 0 voorstellen.
Dat maakt een unieke en ongekend efficiënte vorm van 'parallel' rekenwerk mogelijk. Terwijl een klassieke computer voor de meeste problemen alle denkbare oplossingen afzonderlijk moet doorrekenen (loops doorlopen), kan één kwantumcircuit alle mogelijkheden tegelijk doorlopen. De uitdaging voor de kwantumprogrammeur is om, gebruik makend van wisselwerking tussen qubits, er voor zorgen dat gewenste mogelijkheden elkaar versterken en de niet-gewenste elkaar uitdoven. Om dat voor elkaar te krijgen is software nodig die overweg kan met de ongerijmdheden van de kwantumwereld. Waarin iets tegelijkertijd wel en niet kan zijn en waarop universeel geachte programmeerconcepten als 'IF THEN, ELSE' of andere Booleaanse expressies derhalve geen greep op bieden.

Publicatie : Automatisering Gids
Datum : 22 jan 2016
cm2 : 1.305
Pagina : 16
Advertentiewaarde : € 17.850,00
Regio : Nederland
Frequentie : 1x per 2 weken_do
Oplage : 16.042

Een van onze vier onderzoekslijnen – Few Qubit Applications – richt zich daarom op het zoeken naar zinvolle toepassingen van de vooralsnog kleine kwantumsystemen. Hoe kunnen we bestaande kwantumalgoritmen gebruiken om met bijvoorbeeld 30 qubits iets nuttigs te doen? Kunnen we die systemen wellicht gebruiken om nieuwe kwantumalgoritmen te ontwikkelen? Hoe zouden we dat willen aanpakken?
Daarnaast hebben we een onderzoekslijn die hardware-onderzoekers kan helpen om meer qubits in een systeem te verenigen. Naarmate je meer qubits bij elkaar plaatst, neemt de kans op verstoringen toe. Wij werken aan algoritmen die fouttolerant zijn of fouten corrigeren. Van centraal belang is dan natuurlijk de vraag hoe groot de kans op verstoring in één qubit hooguit mag zijn, wil er nog foutcorrectie mogelijk zijn. We noemen dat de fault tolerant treshold en dat is een waarde waarop de groepen die kwantumhardware ontwikkelen zich op richten. Waar die grens ligt, hangt af van her type operatie, maar denk ruwweg in de ordegrootte van een procent. Als je boven die threshold uitkomt dan is er, bewijsbaar, geen foutcorrectie meer mogelijk."

Zolang de hardware-onderzoekers nog niet al te veel vordering maken met het onder controle krijgen van verstoringskansen, zijn onze klassieke cryptografische systemen nog veilig?
"Ja, maar voor veel toepassingen is dat eigenlijk niet voldoende. Geheime diensten bijvoorbeeld willen dat wat ze nu versleutelen over twintig jaar ook nog veilig is. Ze moeten zich immers indekken tegen een mogelijke 'store now, decrypt later'-tactiek van de tegenstanders. Reken maar dat er van alles wordt getapt wat nu nog niet te kraken is, maar wat bewaard wordt om het alsnog te kraken zodra de technologie – klassiek of kwantum – dat mogelijk maakt. Het is nu dus al van belang gebruik te maken van klassiek toepasbare versleutelingen die ook voor een kwantumcomputer moeilijk te kraken zijn.
Om die reden doen we bij QuSoft ook onderzoek rond 'quantum safe'-cryptografie voor zowel kwantumhardware als klassieke hardware. We hebben daar wel al ideeën over, onder andere de 'latice based' methode. Het probleem is echter dat die vooralsnog te veel rekenkracht vereist om handzaam te worden verwerkt in alledaagse toepassingen zoals transactiesystemen of chip-cards. Zeker als je het vergelijkt met RSA, wat natuurlijk lekker snappy en snel is. De eerste kwantumcryptosystemen zijn trouwens al op de markt. Bijvoorbeeld van ID Quantique, waarmee we ook samenwerken."

Je wees al op de R&D-inspanningen die Google op dat gebiedt levert. We weten dat Microsoft en Intel participeren in Van Kouwenhovens QuTech. Onderzoeksresultaten zullen bedrijven mogelijk doorslaggevend concurrentievoordeel opleveren. Hoe staat QuSoft daarin? Is de kennis die QuSoft genereert publiek toegankelijk en vrij toepasbaar?
"Ja, alles is 100 procent openbaar. We publiceren alles, waar mogelijk op basis van open access. Ik vind dat ook vanzelfsprekend; ons onderzoek wordt bekostigd met belastinggeld, dus moeten de resultaten ook publiek toegankelijk zijn.
Ik geloof ook niet dat er – afgezien van het werk van geheime diensten – een redelijk belang kan zijn bij geheimhouding. Het probleem met geheimhouden en verbieden is dat het niet werkt, dat het toch gebeurt. Kijk naar illegaal downloaden via torrents; verbieden werkte niet. Het bieden van een alternatief – goedkope streaming-diensten – werkt wel. Daarom zie ik van kwantumkennis ook liever dat iedereen er toegang toe heeft, dat schept de beste mogelijkheden voor verweer tegen ongewenst gebruik."

Staat dat engagement met open access niet haaks op je wens om samen te werken met het bedrijfsleven? Dat zal toch liefst investeren in onderzoeksresultaten die niet ook voor de concurrentie toegankelijk zijn.
"Dat is waar, het zijn meestal geen filantropen. Maar ik ga er van uit dat er wel goede afspraken te maken zullen zijn."