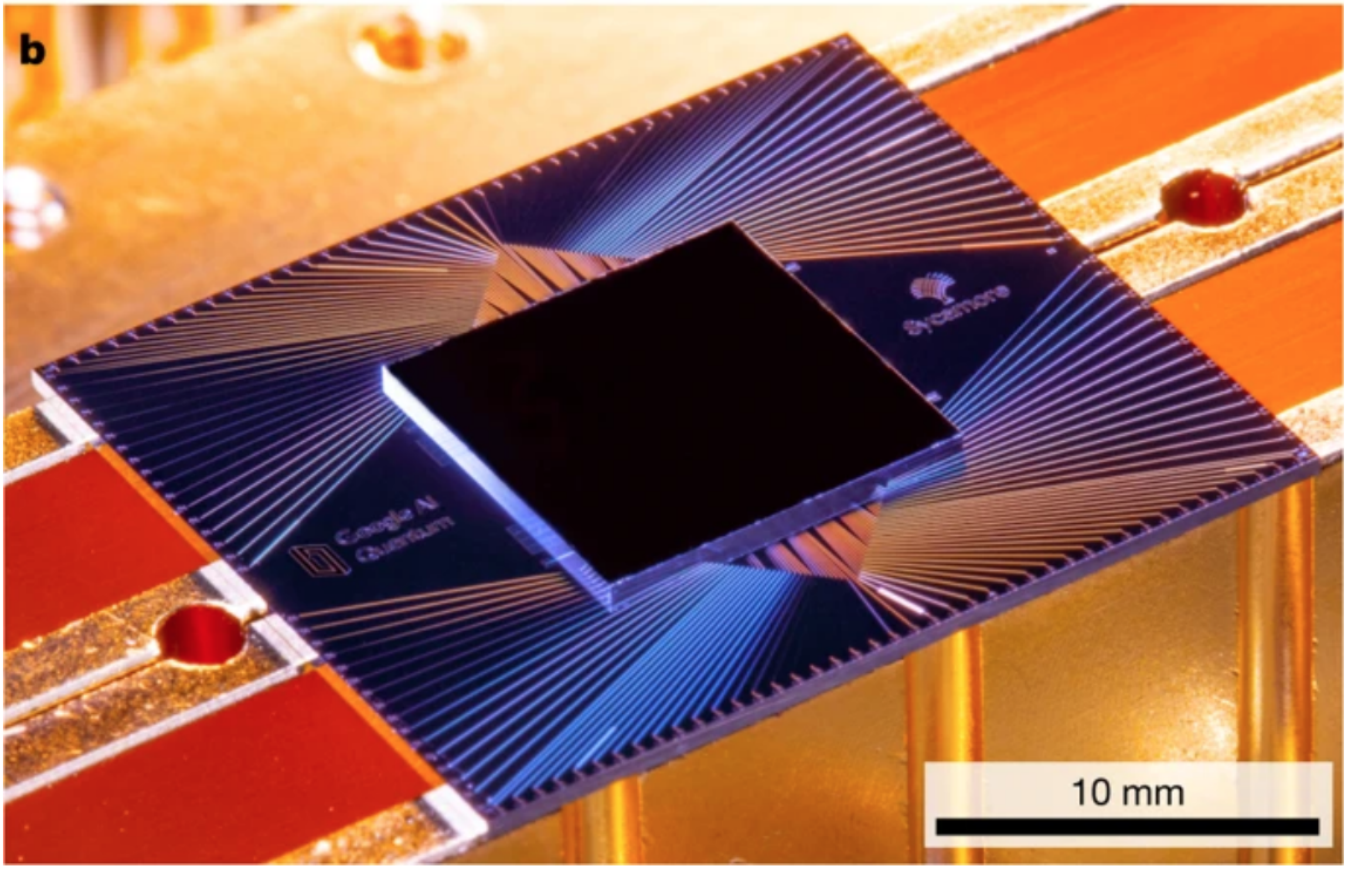
Googles "quantum supremacy"-experiment

Recent was het groot nieuws: Google claimde voor het eerst een “quantum supremacy”-berekening gedaan te hebben: een berekening op een quantumcomputer die een gewone computer niet in een normale hoeveelheid tijd zou kunnen uitvoeren. Quantum Universe vroeg Jonas Helsen, quantumcomputeronderzoeker bij het QuSoft-instituut, naar het hoe en waarom van deze claim.



Afbeelding 1. De sycamore-processor.Met deze processor met 54 qubits deed Google het quantum supremacy-experiment. Afbeelding uit het Nature-artikel over de berekening.

De wereld van quantumcomputeronderzoekers lijkt, zoals de wereld van vele

gespecialiseerde beroepen, op een dorp. En net zoals in elk ander dorp, doen er in het quantumcomputerdorp steeds geruchten de ronde. Enkele weken geleden, rond het einde van september, begon de geruchtenmolen plots op volle toeren te draaien. Het internet gonsde van commentaren en speculaties en rond koffiemachines in onderzoekslabs over de hele wereld werd druk gediscussieerd. De reden hiervoor was een gelekte draft van een artikel geschreven door het team van John Martinis, een team dat beter bekend staat als “Google Quantum Computing”.

Deze draft was blijkbaar tijdens het uitwisselen van pre-publicatiecommentaren per ongeluk op een publieke NASA-server terechtgekomen en daarna, o ironie, door Googles eigen academische zoekmachine, Google Scholar, naar de buitenwereld uitgelekt. Natuurlijk verklaart de ongebruikelijke oorsprong van de draft niet de hoeveelheid discussie die erover ontstond. Wat wel discussie, en uiteindelijk ook een grote hoeveelheid (meer of minder correcte) artikelen genereerde, was wat er in stond: Google claimde “Quantum Supremacy” bereikt te hebben.

Quantum Supremacy: Wat is dat nu eigenlijk?

Om te begrijpen waarom onderzoekers en de media zo opgewonden waren moeten we eerst begrijpen wat Quantum Supremacy nu eigenlijk inhoudt. Hiervoor kunnen we het beste luisteren naar John Preskill, professor aan CalTech en de bedenker van de term quantum supremacy. Hij zegt in een recent interview met Quanta Magazine het volgende (vrij vertaald):

> Quantum Supremacy is simpelweg het vinden van een taak die doenbaar is voor een quantumcomputer maar (quasi-) onmogelijk voor een klassieke computer, ongeacht of deze taak ergens nuttig voor is.

Dit is een ogenschijnlijk simpele wens, maar het bleek verrassend moeilijk om zo’n taak te vinden. De reden hiervoor is dat we in de praktijk erg veeleisend zijn. De quantumcomputers die we op dit moment, en in de nabije toekomst, kunnen bouwen zijn extreem klein en breekbaar. Dit betekent dat we de centrale tegenstelling van quantum supremacy maximaal moeten oprekken: we willen een taak die maximaal makkelijk is voor een quantumcomputer,

en tegelijk maximaal moeilijk voor een klassieke computer.

Daarbovenop willen we niet alleen *vermoeden* dat iets moeilijk is, maar we willen het ook kunnen *bewijzen*. Dit soort bewijzen valt onder de wiskundige noemer van “computationele complexiteitstheorie”, een deelgebied van de wiskunde dat er bekend om staat dat zelfs elementaire vraagstukken (zoals het P vs NP probleem) heel lastig te beantwoorden zijn. In de laatste paar jaar is er echter een aantal goede voorstellen voor Quantum Supremacy-taken naar voor gekomen. De belangrijkste zijn Boson Sampling (BS), Instantaneous Quantum Polynomial Computing (IQP) en Random Circuit Sampling (RCS). Het is dit deze laatste taak, RCS, die Google heeft gekozen voor hun Quantum Supremacy-experiment.

De meest willekeurige berekening

Om RCS echt te begrijpen heb je een stevige dosis wiskunde nodig, maar met wat basiskennis over quantumcomputers is het basisidee ervan best te snappen. RCS is in wezen de volgende taak. Je neemt N qubits, allemaal geïnitialiseerd in de 0 (nul) toestand. Dit betekent dat als je de qubits nu zou uitlezen, je met 100% waarschijnlijkheid het ‘woord’ 00…0 zou vinden. Vervolgens laat je je quantumcomputer een willekeurige reeks quantumoperaties op deze N qubits uitvoeren. De precieze details hiervan zijn complex, maar vanwege de structuur van quantumoperaties gaat de toestand waarin de qubits zich nu bevinden een enorme superpositie zijn van (bijna) alle binaire woorden: 00…0, 10..000,…., 11….0, enz.

Deze toestand is heel erg verstrengeld (en dus ‘heel quantum’). Als je nu meet, vind je een van de binaire woorden met een bepaalde kans. Als je dit experiment vele keren herhaalt kan je de kansverdeling berekenen die voor alle binaire woorden de kans geeft. Deze kansverdeling produceren, gegeven een willekeurig quantumcircuit, is het doel van RCS. De intuïtieve reden dat het moeilijk is om deze kansverdeling met een klassieke computer te produceren is dat je eerst een zeer verstrengelde toestand moet creëren, iets waarvan we denken dat het niet te simuleren is op een klassieke computer. Het uitvoeren van quantumcircuits (en het creeren van verstrengelde toestanden) is echt precies waar een quantumcomputer voor gemaakt is! Dit betekent dat je niet al te veel qubits nodig hebt (voor Google is N=53) om dit experiment uit te voeren op een schaal die al onmogelijk klassiek te simuleren is.

Is Google Quantum Supreme?

Een groot deel van de discussie die de afgelopen weken werd gevoerd onder academici draait rond een simpele vraag: is het Google echt gelukt? De meningen hierover lopen uiteen, maar de voorzichtige consensus lijkt te zijn dat het experiment dat Google heeft uitgevoerd in principe telt als het aantonen van Quantum Supremacy. Er kan echter een aantal kleine en grote voetnoten bij deze conclusie geplaatst worden.

Een eerste kritiek betreft de vraag of het écht onmogelijk is het experiment klassiek te simuleren. De technische appendices van Googles manuscript gaan uitgebreid in op hun pogingen om een klassieke simulatie te bewerkstelligen. Deze pogingen zijn zonder twijfel erg indrukwekkend. Ze maken gebruik van hypermoderne tensor-netwerksimulatoren die speciaal geoptimaliseerd zijn voor gebruik op supercomputers. Daarbovenop roepen ze ook nog eens de hulp in van de Summit-supercomputer, op dit moment de krachtigste supercomputer in de wereld. Zelfs met al deze hulp moeten ze concluderen dat hun experiment nabootsen op een klassieke computer volstrekt onmogelijk is. Veel onderzoekers zijn bereid hun conclusie hier te volgen.

Maar hier en daar zijn er toch tegenstemmen – bijvoorbeeld van concurrent IBM. Zo wordt bijvoorbeeld aangevoerd dat tensor-netwerken niet de enige moderne manier vormen voor de simulatie van quantumsystemen. Andere simulatiemethoden, zoals de ‘stabilisator-rang methodes’ worden niet besproken in het manuscript en critici voeren aan dat deze technieken het misschien toch mogelijk maken een klassieke simulatie uit te voeren. Dit is natuurlijk makkelijker gezegd dan gedaan, en het zou een hele klus zijn om een klassieke simulatie beter te doen dan wat Google hier presteerde.

Hoe controleer je een quantumcomputer?

Een tweede kritische noot kan gemaakt worden over hoe we de uitkomsten van het experiment moeten controleren. Quantumcomputers maken makkelijk fouten in hun berekeningen, en hoe langer en groter de berekening, hoe meer fouten er gemaakt worden. Dit betekent dat het belangrijk is om te controleren of de uitkomsten van het Google supremacy-experiment correct zijn, en geen totale nonsens. Dit is echter moeilijker dan het lijkt, want de enige gekende manier om de uitkomsten van het quantum supremacy-experiment te controleren is door een klassieke simulatie uit te voeren! Dit is echter, per

definitie van Quantum Supremacy, onmogelijk om in de praktijk te doen.

We zullen dus per definitie nooit echt weten of Google het experiment nu correct heeft uitgevoerd. Google probeert deze kritiek te beantwoorden door uitgebreide verificatiestappen uit te voeren op kleinere, eenvoudigere versies van het Quantum Supremacy-probleem. Deze versies van het probleem zijn eenvoudig genoeg om klassieke simulatie mogelijk te maken, maar dicht genoeg bij het echte probleem om de conclusie te trekken dat als de quantumcomputer het eenvoudige probleem aankan, het ook wel mogelijk is om het moeilijke probleem op te lossen op een min of meer correcte manier.

Deze laatste conclusie is echter in zekere zin een ‘leap of faith’ en er zullen zeker critici zijn die niet overtuigd zijn door dit argument. Het is in principe mogelijk om ‘verifieerbare’ versies van het Quantum Supremacy-experiment uit te voeren, maar de theorie hiervan staat nog in de kinderschoenen en alle huidige ideeën hiervoor roepen om een hoeveelheid qubits die vooralsnog volstrekt onhaalbaar is. Het zal dus nog wel even duren voor echt alle sceptici overtuigd zijn.