HO
GENT

Faculteit Bedrijf en Organisatie

De toekomst voor quantumcomputing en wanneerhedendaagse computers vervangen worden

Werner De Schryver

Scriptie voorgedragen tot het bekomen van de graad van
professionele bachelor in de toegepaste informatica

Promotor:
Antonia Pierreux
Co-promotor:

Instelling: —

Academiejaar: 2020-2021

Tweede examenperiode

Faculteit Bedrijf en Organisatie

De toekomst voor quantumcomputing en wanneerhedendaagse computers vervangen worden

Werner De Schryver

Scriptie voorgedragen tot het bekomen van de graad van
professionele bachelor in de toegepaste informatica

Promotor:
Antonia Pierreux
Co-promotor:

Instelling: —

Academiejaar: 2020-2021

Tweede examenperiode

Woord vooraf

Samenvatting

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus.

Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Inhoudsopgave

Lijst van figuren

Lijst van tabellen

1. Inleiding

De inleiding moet de lezer net genoeg informatie verschaffen om het onderwerp te begrijpen en in te zien waarom de onderzoeksvraag de moeite waard is om te onderzoeken. In de inleiding ga je literatuurverwijzingen beperken, zodat de tekst vlot leesbaar blijft. Je kan de inleiding verder onderverdelen in secties als dit de tekst verduidelijkt. Zaken die aan bod kunnen komen in de inleiding (Pollefliet, 2011):

- context, achtergrond
- afbakenen van het onderwerp
- verantwoording van het onderwerp, methodologie
- probleemstelling
- onderzoeksdoelstelling
- onderzoeksvraag
- ...

1.1 Probleemstelling

Momenteel is er nog veel onzekerheid over de evolutie van quantumcomputing op twee verschillende gebieden. Enerzijds, hoe een quantumcomputer er technisch zal uitzien. Gebruikt men best fotonen of superconductors? Anderzijds, de snelheid waarmee quantumcomputing verfijnd kan worden. Tot op de dag van vandaag zijn quantumcomputers geen rendabel alternatief voor gewone computers. In deze bachelorproef zal de focus liggen op het tweede probleem en zal er getracht worden te voorspellen wanneer quantumcomputers in de praktijk toepasbaar zullen zijn.

In theorie kunnen quantumcomputers een grote impact hebben in specifieke praktische

toepassingen, maar de praktijk is daar nog niet. Het aantal stakeholders is heel breed, van farmaceutica tot militaire doeleinden. Dit is een korte opsomming van de sectoren die de impact zullen voelen:

- Farmaceutica
- Logistiek
- Luchtvaart
- Nucleaire fusie
- Financiële modellen
- Scheikunde
- Artificiële intelligentie
- Cybersecurity
- Big Data
- Defensie

De productiviteitsverhoging voor eindgebruikers wordt geschat op $450 miljard ieder jaar, aldus Bajpai (2020).

1.2 Onderzoeksvraag

Deze bachelorproef bevat twee onderzoeksvragen, namelijk:

- Wanneer zullen de eerste quantumcomputers gebruikt worden in alledaagse toepassingen?
- Wanneer zullen quantumcomputers overal aanwezig zijn?

Voor de eerste vraag is het de bedoeling om een specifiek jaartal te bekomen waarin het gebruik van quantumcomputing 'officieel' gelanceerd zal kunnen worden voor een breed publiek. Dit zal bepaald worden door het quantumvolume.

De tweede vraag valt iets minder concreet te beantwoorden. Hiervoor zal een onderzoek moeten uitgevoerd worden naar hoe snel verschillende sectoren deze nieuwe technologie zullen adopteren. Dit zal gebaseerd zijn op verschillende factoren, namelijk het budget, hoe groot de impact weldegelijk is voor een bepaalde sector, de mate waarin deze sectoren nieuwe technologieën geadopteerd hebben in het verleden, enzovoort.

1.3 Onderzoeksdoelstelling

De doelstelling van deze bachelorproef is om een accurate grafiek te bekomen die de groei van het quantumvolume toont, samen met een tijdlijn die zowel grote als minder grote milestones bevat voor de toekomst. Deze kunnen meer zekerheid en vooruitzicht bieden aan sectoren die een grote productiviteitsverhoging kunnen verwachten van zodra deze technologie beschikbaar is voor hen. Zo kunnen deze sectoren zich hier ook op voorbereiden.

Hier mee gepaard zal ook een kleine vergelijkende studie uitgevoerd worden om de voor- en nadelen te beschrijven van de verschillende methodes van quantumcomputing, om hier ook meer duidelijkheid te scheppen.

1.4 Opzet van deze bachelorproef

De rest van deze bachelorproef is als volgt opgebouwd:

In Hoofdstuk 2 wordt een overzicht gegeven van de stand van zaken binnen het onderzoeksdomein, op basis van een literatuurstudie.

In Hoofdstuk 3 wordt de methodologie toegelicht en worden de gebruikte onderzoekstechnieken besproken om een antwoord te kunnen formuleren op de onderzoeksvragen.

In Hoofdstuk 4, tenslotte, wordt de conclusie gegeven en een antwoord geformuleerd op de onderzoeksvragen. Daarbij wordt ook een aanzet gegeven voor toekomstig onderzoek binnen dit domein.

2. Stand van zaken

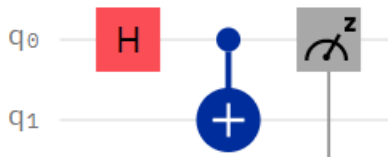
2.1 Wat is een quantumcomputer

Normale computers gebruiken bits, die een waarde 0 of 1 kunnen aannemen, om berekeningen uit te voeren. Quantumcomputers gebruiken quantum bits, of qubits. Wanneer een qubit gemeten wordt, neemt deze ook altijd een waarde 0 of 1 aan. Zolang de qubit niet geobserveerd wordt kan deze een lineaire combinate van beide zijn, dit fenomeen heet "quantum superposition". Dit betekent dat de qubit zowel 0 als 1 kan zijn, of een waarde hiertussen. De kans, of probabiliteit, om 0 of 1 te krijgen kan berekend en gemanipuleerd worden met behulp van quantum gates. Quantum gates kunnen zijn het equivalent van de logische poorten in normale computers. Deze voeren bewerkingen uit op qubits en op het einde van deze bewerkingen worden de qubits gemeten. Zoals al eerder vermeld zal deze meting altijd een waarde 0 of 1 opleveren.

De meest eenvoudige van deze quantum gates is de Hadamard (H) gate. Deze poort kan worden gebruikt om een qubit in de superposition toestand te krijgen. Na het toepassen van deze poort is de probabiliteit 0.5 voor zowel 0 als 1.

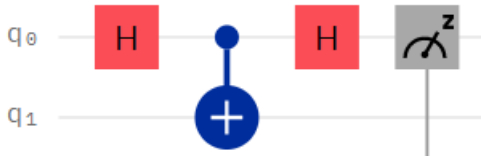
Figuur 2.1: Hadamard Gate

De CNOT gate wordt gebruikt om twee qubits in een staat van entanglement te krijgen. Dit wil zeggen dat een bewerking op één qubit ook invloed zal hebben op de andere qubit. Na het toepassen van deze gate is de probabiliteit 0.5 voor de waarden 00 en 11.



Figuur 2.2: CNOT gate

Deze twee poorten kunnen gecombineerd worden zoals op onderstaande afbeelding. De probabiliteit hier is 0.25 voor de waarden 00, 01, 10 en 11.



Figuur 2.3: H Gate en CNOT Gate

Dit zijn de basis poorten die gebruikt kunnen worden, maar er zijn uiteraard ook nog andere poorten. Al deze poorten kunnen gecombineerd worden om een quantum circuit te maken.

2.2 Gelijkaardige onderzoeken

Doorheen de jaren zijn er reeds gelijkaardige onderzoeken uitgevoerd, één hiervan is uitgevoerd door Preskill (2018). Het focust zich onder andere op de recente evolutie in quantum computing en wat hij zelf het Noisy Intermediate-Scale Quantum (NISQ) era noemt. Concreet beschrijft hij quantumcomputers met 50 tot 100 qubits, die potentieel taken kunnen uitvoeren die hedendaagse digitale computers niet kunnen uitvoeren. Het probleem in deze systemen is de 'noise' in de quantum gates. Deze 'noise' is het gevolg van de error rate van de qubits. Met de beste hardware die we vandaag beschikbaar hebben is de error rate per gate voor twee-qubit gates boven de .1%, en vaak nog veel slechter (Preskill, 2018). Preskill komt niet tot een concrete conclusie over hoe lang het nog zou duren tot quantumcomputers een impact maken in de maatschappij. Volgens hem zullen quantum computers in de 'nabije toekomst' verschijnen in praktische applicaties, maar geeft hier geen concrete tijdspanne.

Het verschil met dit onderzoek is dat hierin getracht zal worden om, aan de hand van de evolutie van quantumcomputers en de roadmap van grote technologie bedrijven zoals IBM, een voorspelling te maken over wanneer quantumcomputing toepasbaar zal zijn in onze maatschappij.

2.3 Praktische toepassingen

Zoals al eerder vermeld zijn quantumcomputers goed in bepaalde wiskundige bewerkingen, waaronder ontbinden in factoren. Dit is de basis van RSA encryptie methodes, specifiek het ontbinden in priemfactoren (from the arXiv, 2019). RSA baseert zich op de veronderstelling dat dit een onmogelijk probleem is voor normale computers. Dit duurde tot wanneer de algoritmes van Shor (1999) bewezen dat het mogelijk is om te ontbinden in priemfactoren met een polynomiale tijdscomplexiteit en een kleine kans op errors, als een quantumcomputer gebouwd kon worden.

Hoewel Shor bewezen heeft dat het mogelijk is om RSA encryptie te breken met een quantumcomputer, verwacht men niet dat quantumcomputers NP-moeilijke problemen zoals het handelsreizigersprobleem efficiënt zullen kunnen oplossen. NP-moeilijke problemen zullen allicht zowel quantum moeilijk als klassiek moeilijk blijven.

Buiten het ontbinden in priemfactoren zijn quantumcomputers ook goed in optimalisatieproblemen en het simuleren van quantum mechanica.

Dit hoofdstuk bevat je literatuurstudie. De inhoud gaat verder op de inleiding, maar zal het onderwerp van de bachelorproef *diepgaand* uitspitten. De bedoeling is dat de lezer na lezing van dit hoofdstuk helemaal op de hoogte is van de huidige stand van zaken (state-of-the-art) in het onderzoeksdomein. Iemand die niet vertrouwd is met het onderwerp, weet nu voldoende om de rest van het verhaal te kunnen volgen, zonder dat die er nog andere informatie moet over opzoeken (Pollefliet, 2011).

Je verwijst bij elke bewering die je doet, vakterm die je introduceert, enz. naar je bronnen. In LaTeX kan dat met het commando `\textcite{}` of `\autocite{}`. Als argument van het commando geef je de “sleutel” van een “record” in een bibliografische databank in het BibLaTeX-formaat (een tekstbestand). Als je expliciet naar de auteur verwijst in de zin, gebruik je `\textcite{}`. Soms wil je de auteur niet expliciet vernoemen, dan gebruik je `\autocite{}`. In de volgende paragraaf een voorbeeld van elk.

3. Methodologie

Etiam pede massa, dapibus vitae, rhoncus in, placerat posuere, odio. Vestibulum luctus commodo lacus. Morbi lacus dui, tempor sed, euismod eget, condimentum at, tortor. Phasellus aliquet odio ac lacus tempor faucibus. Praesent sed sem. Praesent iaculis. Cras rhoncus tellus sed justo ullamcorper sagittis. Donec quis orci. Sed ut tortor quis tellus euismod tincidunt. Suspendisse congue nisl eu elit. Aliquam tortor diam, tempus id, tristique eget, sodales vel, nulla. Praesent tellus mi, condimentum sed, viverra at, consectetuer quis, lectus. In auctor vehicula orci. Sed pede sapien, euismod in, suscipit in, pharetra placerat, metus. Vivamus commodo dui non odio. Donec et felis.

Etiam suscipit aliquam arcu. Aliquam sit amet est ac purus bibendum congue. Sed in eros. Morbi non orci. Pellentesque mattis lacinia elit. Fusce molestie velit in ligula. Nullam et orci vitae nibh vulputate auctor. Aliquam eget purus. Nulla auctor wisi sed ipsum. Morbi porttitor tellus ac enim. Fusce ornare. Proin ipsum enim, tincidunt in, ornare venenatis, molestie a, augue. Donec vel pede in lacus sagittis porta. Sed hendrerit ipsum quis nisl. Suspendisse quis massa ac nibh pretium cursus. Sed sodales. Nam eu neque quis pede dignissim ornare. Maecenas eu purus ac urna tincidunt congue.

Donec et nisl id sapien blandit mattis. Aenean dictum odio sit amet risus. Morbi purus. Nulla a est sit amet purus venenatis iaculis. Vivamus viverra purus vel magna. Donec in justo sed odio malesuada dapibus. Nunc ultrices aliquam nunc. Vivamus facilisis pellentesque velit. Nulla nunc velit, vulputate dapibus, vulputate id, mattis ac, justo. Nam mattis elit dapibus purus. Quisque enim risus, congue non, elementum ut, mattis quis, sem. Quisque elit.

Maecenas non massa. Vestibulum pharetra nulla at lorem. Duis quis quam id lacus dapibus interdum. Nulla lorem. Donec ut ante quis dolor bibendum condimentum. Etiam egestas

tortor vitae lacus. Praesent cursus. Mauris bibendum pede at elit. Morbi et felis a lectus interdum facilisis. Sed suscipit gravida turpis. Nulla at lectus. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Praesent nonummy luctus nibh. Proin turpis nunc, congue eu, egestas ut, fringilla at, tellus. In hac habitasse platea dictumst.

Vivamus eu tellus sed tellus consequat suscipit. Nam orci orci, malesuada id, gravida nec, ultricies vitae, erat. Donec risus turpis, luctus sit amet, interdum quis, porta sed, ipsum. Suspendisse condimentum, tortor at egestas posuere, neque metus tempor orci, et tincidunt urna nunc a purus. Sed facilisis blandit tellus. Nunc risus sem, suscipit nec, eleifend quis, cursus quis, libero. Curabitur et dolor. Sed vitae sem. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Maecenas ante. Duis ullamcorper enim. Donec tristique enim eu leo. Nullam molestie elit eu dolor. Nullam bibendum, turpis vitae tristique gravida, quam sapien tempor lectus, quis pretium tellus purus ac quam. Nulla facilisi.

4. Conclusie

Curabitur nunc magna, posuere eget, venenatis eu, vehicula ac, velit. Aenean ornare, massa a accumsan pulvinar, quam lorem laoreet purus, eu sodales magna risus molestie lorem. Nunc erat velit, hendrerit quis, malesuada ut, aliquam vitae, wisi. Sed posuere. Suspendisse ipsum arcu, scelerisque nec, aliquam eu, molestie tincidunt, justo. Phasellus iaculis. Sed posuere lorem non ipsum. Pellentesque dapibus. Suspendisse quam libero, laoreet a, tincidunt eget, consequat at, est. Nullam ut lectus non enim consequat facilisis. Mauris leo. Quisque pede ligula, auctor vel, pellentesque vel, posuere id, turpis. Cras ipsum sem, cursus et, facilisis ut, tempus euismod, quam. Suspendisse tristique dolor eu orci. Mauris mattis. Aenean semper. Vivamus tortor magna, facilisis id, varius mattis, hendrerit in, justo. Integer purus.

Vivamus adipiscing. Curabitur imperdiet tempus turpis. Vivamus sapien dolor, congue venenatis, euismod eget, porta rhoncus, magna. Proin condimentum pretium enim. Fusce fringilla, libero et venenatis facilisis, eros enim cursus arcu, vitae facilisis odio augue vitae orci. Aliquam varius nibh ut odio. Sed condimentum condimentum nunc. Pellentesque eget massa. Pellentesque quis mauris. Donec ut ligula ac pede pulvinar lobortis. Pellentesque euismod. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent elit. Ut laoreet ornare est. Phasellus gravida vulputate nulla. Donec sit amet arcu ut sem tempor malesuada. Praesent hendrerit augue in urna. Proin enim ante, ornare vel, consequat ut, blandit in, justo. Donec felis elit, dignissim sed, sagittis ut, ullamcorper a, nulla. Aenean pharetra vulputate odio.

Quisque enim. Proin velit neque, tristique eu, eleifend eget, vestibulum nec, lacus. Vivamus odio. Duis odio urna, vehicula in, elementum aliquam, aliquet laoreet, tellus. Sed velit. Sed vel mi ac elit aliquet interdum. Etiam sapien neque, convallis et, aliquet vel, auctor non, arcu. Aliquam suscipit aliquam lectus. Proin tincidunt magna sed wisi. Integer blandit

lacus ut lorem. Sed luctus justo sed enim.

Morbi malesuada hendrerit dui. Nunc mauris leo, dapibus sit amet, vestibulum et, commodo id, est. Pellentesque purus. Pellentesque tristique, nunc ac pulvinar adipiscing, justo eros consequat lectus, sit amet posuere lectus neque vel augue. Cras consectetuer libero ac eros. Ut eget massa. Fusce sit amet enim eleifend sem dictum auctor. In eget risus luctus wisi convallis pulvinar. Vivamus sapien risus, tempor in, viverra in, aliquet pellentesque, eros. Aliquam euismod libero a sem.

Nunc velit augue, scelerisque dignissim, lobortis et, aliquam in, risus. In eu eros. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Curabitur vulputate elit viverra augue. Mauris fringilla, tortor sit amet malesuada mollis, sapien mi dapibus odio, ac imperdiet ligula enim eget nisl. Quisque vitae pede a pede aliquet suscipit. Phasellus tellus pede, viverra vestibulum, gravida id, laoreet in, justo. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Integer commodo luctus lectus. Mauris justo. Duis varius eros. Sed quam. Cras lacus eros, rutrum eget, varius quis, convallis iaculis, velit. Mauris imperdiet, metus at tristique venenatis, purus neque pellentesque mauris, a ultrices elit lacus nec tortor. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent malesuada. Nam lacus lectus, auctor sit amet, malesuada vel, elementum eget, metus. Duis neque pede, facilisis eget, egestas elementum, nonummy id, neque.

A. Onderzoeksvoorstel

Het onderwerp van deze bachelorproef is gebaseerd op een onderzoeksvoorstel dat vooraf werd beoordeeld door de promotor. Dat voorstel is opgenomen in deze bijlage.

A.1 Introductie

Technologie bedrijven zoals IBM, Google en D-Wave zijn ondertussen al jaren bezig met het ontwikkelen en bouwen van quantumcomputers. Ieder jaar worden quantumcomputers krachtiger, maar wanneer zullen ze krachtig genoeg zijn om normale computers te vervangen, of om taken uit te voeren die we nog niet kunnen uitvoeren met normale computers? De manier waarop normale computers hun snelheid bleven verbeteren was door transistoren kleiner te blijven maken, zodat er meer transistoren op een chip konden. Nu komen we aan de limiet van hoe klein transistoren gemaakt kunnen worden vooraleer ze niet meer functioneren zoals het hoort. Dit is waarom experts zeggen dat Moore's Law niet langer geldig is.

Dit is waar quantumcomputers een oplossing kunnen bieden. Quantumcomputers zullen allicht normale computers niet volledig vervangen. Simpele wiskundige berekeningen zoals vermenigvuldigingen blijken vandaag de dag nog heel moeilijk voor quantumcomputers, maar ze kunnen bepaalde wiskundige problemen veel sneller oplossen dan normale computers. Specifiek het ontbinden in factoren. Dit is ook de basis van RSA encryptie en een groot veiligheidsrisico. De bijhorende onderzoeksvragen zijn als volgt:

- Wanneer zullen de eerste quantumcomputers gebruikt worden in alledaagse toepassingen?
- Wanneer zullen quantumcomputers overal aanwezig zijn?

A.2 State-of-the-art

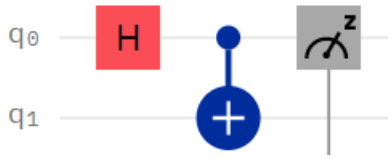
A.2.1 Wat is een quantumcomputer

Normale computers gebruiken bits, die een waarde 0 of 1 kunnen aannemen, om berekeningen uit te voeren. Quantumcomputers gebruiken quantum bits, of qubits. Wanneer een qubit gemeten wordt, neemt deze ook altijd een waarde 0 of 1 aan. Zolang de qubit niet geobserveerd wordt kan deze een lineaire combinate van beide zijn, dit fenomeen heet "quantum superposition". Dit betekent dat de qubit zowel 0 als 1 kan zijn, of een waarde hiertussen. De kans, of probabiliteit, om 0 of 1 te krijgen kan berekend en gemanipuleerd worden met behulp van quantum gates. Quantum gates kunnen zijn het equivalent van de logische poorten in normale computers. Deze voeren bewerkingen uit op qubits en op het einde van deze bewerkingen worden de qubits gemeten. Zoals al eerder vermeld zal deze meting altijd een waarde 0 of 1 opleveren.

De meest eenvoudige van deze quantum gates is de Hadamard (H) gate. Deze poort kan worden gebruikt om een qubit in de superposition toestand te krijgen. Na het toepassen van deze poort is de probabiliteit 0.5 voor zowel 0 als 1.

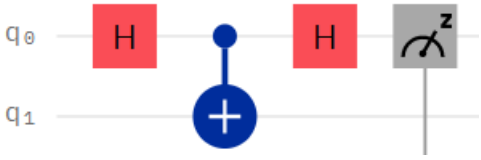
Figuur A.1: Hadamard Gate

De CNOT gate wordt gebruikt om twee qubits in een staat van entanglement te krijgen. Dit wil zeggen dat een bewerking op één qubit ook invloed zal hebben op de andere qubit. Na het toepassen van deze gate is de probabiliteit 0.5 voor de waarden 00 en 11.



Figuur A.2: CNOT gate

Deze twee poorten kunnen gecombineerd worden zoals op onderstaande afbeelding. De probabiliteit hier is 0.25 voor de waarden 00, 01, 10 en 11.



Figuur A.3: H Gate en CNOT Gate

Dit zijn de basis poorten die gebruikt kunnen worden, maar er zijn uiteraard ook nog andere poorten. Al deze poorten kunnen gecombineerd worden om een quantum circuit te maken.

A.2.2 Gelijkaardige onderzoeken

Doorheen de jaren zijn er reeds gelijkaardige onderzoeken uitgevoerd, één hiervan is uitgevoerd door Preskill (2018). Het focust zich onder andere op de recente evolutie in quantum computing en wat hij zelf het Noisy Intermediate-Scale Quantum (NISQ) era noemt. Concreet beschrijft hij quantumcomputers met 50 tot 100 qubits, die potentieel taken kunnen uitvoeren die hedendaagse digitale computers niet kunnen uitvoeren. Het probleem in deze systemen is de 'noise' in de quantum gates. Deze 'noise' is het gevolg van de error rate van de qubits. Met de beste hardware die we vandaag beschikbaar hebben is de error rate per gate voor twee-qubit gates boven de .1%, en vaak nog veel slechter (Preskill, 2018). Preskill komt niet tot een concrete conclusie over hoe lang het nog zou duren tot quantumcomputers een impact maken in de maatschappij. Volgens hem zullen quantum computers in de 'nabije toekomst' verschijnen in praktische applicaties, maar geeft hier geen concrete tijdspanne.

Het verschil met dit onderzoek is dat hierin getracht zal worden om, aan de hand van de evolutie van quantumcomputers en de roadmap van grote technologie bedrijven zoals IBM, een voorspelling te maken over wanneer quantumcomputing toepasbaar zal zijn in onze maatschappij.

A.2.3 Praktische toepassingen

Zoals al eerder vermeld zijn quantumcomputers goed in bepaalde wiskundige bewerkingen, waaronder ontbinden in factoren. Dit is de basis van RSA encryptie methodes, specifiek het ontbinden in priemfactoren (from the arXiv, 2019). RSA baseert zich op de veronderstelling dat dit een onmogelijk probleem is voor normale computers. Dit duurde tot wanneer de algoritmes van Shor (1999) bewezen dat het mogelijk is om te ontbinden in priemfactoren met een polynomiale tijdscomplexiteit en een kleine kans op errors, als een quantumcomputer gebouwd kon worden.

Hoewel Shor bewezen heeft dat het mogelijk is om RSA encryptie te breken met een quantumcomputer, verwacht men niet dat quantumcomputers NP-moeilijke problemen zoals het handelsreizigersprobleem efficiënt zullen kunnen oplossen. NP-moeilijke problemen zullen allicht zowel quantum moeilijk als klassiek moeilijk blijven.

Buiten het ontbinden in priemfactoren zijn quantumcomputers ook goed in optimalisatieproblemen en het simuleren van quantum mechanica. Dit zijn enkele sectoren waarin quantumcomputers nuttig zouden zijn:

- Scheikunde
- Materiaalwetenschappen

- Machine learning
- Optimalisatieproblemen

A.3 Methodologie

In de eerste fase zal er onderzocht worden welke manieren van quantumcomputing momenteel beschikbaar zijn of aan gewerkt worden. Bepaalde bedrijven hebben verschillende manieren van werken. IBM gebruikt bijvoorbeeld superconducters als basis voor hun quantum circuits, D-Wave maakt gebruik van een techniek genaamd quantum annealing en een onderzoeksteam van de University of Science and Technology of China maakt gebruikt van fotonen (Leprince-Ringuet, 2020). Tijdens de literatuurstudie zal ook data verzameld worden omtrent de groei van het "quantumvolume". Dit is een metriek gebaseerd op het aantal qubits in combinatie met hun fouttolerantie in een systeem.

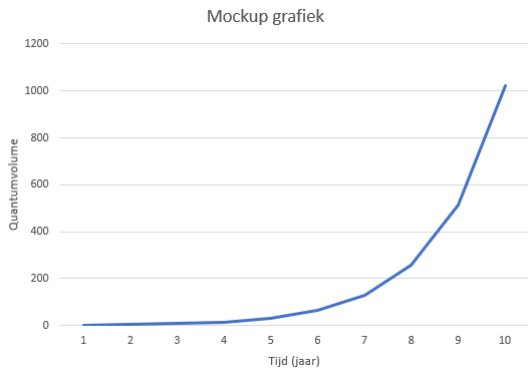
Vervolgens zal er een vergelijkende studie uitgevoerd worden tussen de verschillende methodes. Wat zijn de sterktes en zwaktes van elke methode en welke is de beste? Hier zal ook dieper worden ingegaan op welke praktische applicaties er zullen zijn binnen de genoemde sectoren.

Ten slotte zal er, op basis van data verzameld tijdens de literatuurstudie, een simulatie uitgevoerd worden om te proberen voorspellen wanneer quantumcomputers fouttolerant genoeg zullen zijn om bruikbaar te zijn in de praktijk.

A.4 Verwachte resultaten

Uit de vergelijkende studie wordt verwacht dat het gebruik van superconducters als basis voor quantum circuits het beste resultaat zal geven. Dit is namelijk waar het meeste bedrijven tot dusver in blijven investeren. Het gebruik van fotonen als alternatief zou misschien ook een goed alternatief kunnen zijn in specifieke applicaties (O'brien, 2007).

Voor de simulatie wordt verwacht dat de groei van het quantumvolume in de komende decennia er exponentieel uitziet zoals op de mockup grafiek.



A.5 Verwachte conclusies

De verwachte conclusie is dat de eerste quantumcomputers toepassingen zullen krijgen binnen de komende tien jaar en dat quantumcomputers in de komende 50 jaar overal aanwezig zullen zijn.

Bibliografie

Bajpai, P. (2020). *Quantum Computing: How To Invest In It, And Which Companies Are Leading the Way?* https://www.nasdaq.com/articles/quantum-computing%5C%3A-how-to-invest-in-it-and-which-companies-are-leading-the-way-2020-02-11

from the arXiv, E. T. (2019). *How a quantum computer could break 2048-bit RSA encryption in 8 hours*. https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hour

Leprince-Ringuet, D. (2020). *Quantum supremacy 'milestone' achieved by light-emitting quantum computer*. https://www.zdnet.com/article/quantum-supremacy-milestone-achieved-by-light-emitting-quantum-computer

O'brien, J. L. (2007). Optical quantum computing. *Science*, *318*(5856), 1567–1570.

Pollefliet, L. (2011). *Schrijven van verslag tot eindwerk: do's en don'ts*. Academia Press.

Preskill, J. (2018). Quantum Computing in the NISQ era and beyond. *Quantum*, *2*, 79.

Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, *41*(2), 303–332.