

Kansen met Quantum

Een NLT-module over Quantumcomputing

Guido Linssen
Anne-Marije Zwerver
Martin Mollema
Henk Buisman

Versie: 1.1
2023-10-13

Colofon

De lesmodule *Kansen met Quantum* is geschreven in opdracht van Vereniging NLT en is bestemd voor de lessen NLT (Natuur, Leven en Technologie). De module is op 15 oktober 2022 gecertificeerd door de Vereniging NLT, onder nummer 6140-099-E1-2F1 en is geldig tot 16 oktober 2027. De module is relevant voor de domeinen:

- VWO E1: Methoden en technieken van technologische ontwikkeling
F1: Fundamentele theorieën

versie 1.0: oktober 2022 gecertificeerd

versie 1.1: oktober 2023 update



De module is ontwikkeld door:

- **Guido Linssen** (v/h Gymnasium Feliseum, Velsen)
- **Annemarie Zwerver** (QuTech, Delft)
- **Martin Mollema** (Scala College, Alphen aan de Rijn)
- **Henk Buisman** (eindredactie, Universiteit Leiden)

Verder werkten mee:

- **Hans van Bemmel** (didactisch advies)
- **Ronald de Wolf** (wetenschappelijk advies)
- **Lianne van der Meer** (redactie)
- **Dennis Wijmer** illustraties

Versie info

Versie 1.0 (oktober 2022) NLT-Gecertificeerd.

Versie 1.1 (oktober 2023) Talloze typo's verbeterd. H2: Het meetprobleem heeft een eigen paragraaf. Het Bell experiment is herschreven. Docentenhandleiding bijgewerkt.



CC BY-NC 4.0



Copyright: Deze module is beschikbaar onder Creative Commons licentie **CC BY-NC 4.0**. Alle rechten voorbehouden.

Het gecertificeerde materiaal (voor docenten en leerlingen) vindt u op de moduledatabase van de Vereniging NLT. De geactualiseerde versie van de leerlingenhandleiding en aanvullend materiaal staan op de [website van het project](#) Quantum Rules.



website van het project

Docenten mogen deze module aanpassen voor gebruik in de les, zonder daarbij de certificering teniet te doen, onder voorwaarde dat in het colofon vermeldt staat dat het een aangepaste versie betreft.

Deze module is tot stand gekomen onder verantwoordelijkheid van de Vereniging NLT met medefinanciering van de Universiteit Leiden.

Inhoudsopgave

1 Inleiding	1
1.1 Inleiding	1
1.2 Een experiment uit de 'oertijd'	5
1.3 Leerdoelen	8
2 Waar is het qubit?	11
2.1 Van bits	11
2.2 ... naar qubits	12
2.3 Hier is het qubit	15
2.4 Het meten met verschillende bases	18
2.5 Over het meetprobleem	20
2.6 Een Bell-test	23
2.7 DiVincenzo criteria	30
2.8 Leerdoelen	32
3 Operatoren en toestandsveranderingen	33
3.1 Poorten die op één qubit werken	35
3.2 Werken met een register	48
3.3 Quantum protocollen	53
3.4 Terugblik en vooruitblik	54
3.5 Leerdoelen	55
4 Praktische opdrachten	57
4.1 Protocol: BB84	57
4.2 Eerlijk quantummuntje	61
4.3 Protocol: Superdense coding	63
4.4 Quantum en maatschappij	67
4.5 Hilbertruimtes	73
4.6 Fourieranalyse	80

5 werkbladen	87
5.1 Proef van Young 1	89
5.2 Wet van Malus	91
5.3 Proef van Young 2	93
5.4 Klassieke bits	95
5.5 Wat zie je?	99
5.6 Werken op een quantumcomputer	101
5.7 Teleportatie	103
Literatuur	109



1. Inleiding

1.1 Inleiding

Voor je ligt de NLT module Kansen met Quantum. De module behandelt de ontwikkeling van de quantumcomputing, een technologie die voortvloeit uit de quantumtheorie. Deze theorie is inmiddels meer dan 100 jaar oud, en bleek de sleutel tot het begrip van de materie op de kleinste schaal. Op die schaal zit de wereld werkelijk anders in elkaar dan onze vertrouwde, klassieke, Newtoniaanse ervaringswereld. Je hoort vaak uitspraken als 'deeltjes kunnen op twee verschillende plaatsen tegelijkertijd zijn', of 'deeltjes kunnen reizen als golf en worden weer gedetecteerd als deeltje'. De hoofdlijnen van de theorie zijn in de eerste helft van de twintigste eeuw beschreven. De theorie opende een nieuwe wereld en heeft tot veel uitvindingen geleid, zoals bijvoorbeeld de transistor. Bij het vak natuurkunde komt deze '1.0 versie' van quantumtheorie uitgebreid aan de orde.

De quantumtheorie is niet intuïtief. Zo kunnen deeltjes verdeeld zijn over meerdere toestanden. Erwin Schrödinger beschreef dit in een gedachtenexperiment met een kat. Deeltjes kunnen ook met elkaar verstengeld zijn. Op grote afstand kan een verandering in de toestand in het ene deeltje een verandering van het andere deeltje veroorzaken. Einstein [5] noemde het een paradox. Volgens hem moesten er nog onderliggende variabelen zijn om de theorie compleet te maken.

In 1982 leverde Alain Aspect een acceptabel bewijs voor het falen van Einstein's *local realism*: eigenschappen van deeltjes kunnen inderdaad over grote afstand gekoppeld zijn en je kunt geen uitspraak doen over de toestand van een deeltje als je het niet meet [10].

In de tweede helft van de twintigste eeuw groeide het besef dat ook dit deel van de quantumtheorie gebruikt zou kunnen worden voor een hele reeks van toepassingen. Een tijdlijn over de ontwikkeling

In de 'klassieke' wereld kunnen deeltjes geen eigenschappen delen op grote afstand (alleen *local*) en je kunt alleen iets zeggen over een deeltje als je het meet (*realism*). In de quantumwereld geldt deze beperking niet.

van quantumcomputing [1] zet de belangrijkste ontdekkingen vanaf 1960 op een rijtje. Vanaf de jaren 1980 is een versnelling te zien. Richard Feynman is een van de sleutelfiguren. Hij bracht naar voren dat quantumprocessen het best gesimuleerd kunnen worden op een computer waarvan de werking zelf gebaseerd is op quantumverschijnselen. Klassieke informatieverwerking is gebaseerd op bits die de waarden 0 of 1 kunnen aannemen. Quantumbits of kortweg qubits kunnen tegelijkertijd in *superpositie* van 0 en 1 zijn. En wat dat precies betekent? Ja, daar gaat deze module over.



Wat nou dood of levend Erwin? Ik ben in superpositie!

De kracht van quantumcomputers is dat ze wezenlijk andere dingen kunnen dan klassieke computers. Met de juiste voorbereiding kunnen ze bijvoorbeeld met één qubit een probleem oplossen waar een klassieke computer twee bits nodig heeft. Dit staat bekend als condensed coding of het orakel van Deutsch. Het stelt misschien nog niet veel voor maar als *proof of principle* is het een belangrijke stap. In een keuze-opdracht kun je het algoritme hiervoor ontdekken. Ook is het mogelijk (je gaat dit in deze module ontdekken) om de toestand van een qubit te teleporteren, een belangrijke stap in de ontwikkeling van quantum-beveiligde communicatie. Er is een quantumalgoritme dat het zoeken in een ongesorteerde lijst versnelt. In een ouderwets telefoonboek staan de telefoonnummers naast een alfabetisch gesorteerde lijst met namen. Het is heel makkelijk om het nummer bij een naam te vinden, maar de nummers staan in willekeurige volgorde (ongesorteerd). Als je een naam bij een nummer wilt vinden tref je het nummer nadat je gemiddeld de helft van het

boek hebt doorgeworsteld. Als het telefoonboek twee keer zo dik is duurt het zoeken ook twee keer zo lang. Het quantum-algoritme van Lov Grover (1996) versnelt deze zoekopdracht kwadratisch. Als het telefoonboek negen keer zo dik is, duurt het zoeken drie keer zo lang. Voor lange lijsten levert dat een enorm voordeel.

Een belangrijke doorbraak is de ontdekking van het factorisatie-algoritme van Peter Shor (1994). Factoriseren is het ontbinden van getallen in priemfactoren. Het coderingssysteem RSA, dat de basis vormt voor o.a. onze banktransacties is gebaseerd op de aanname dat het ontbinden in priemfactoren van een groot getal (denk aan getallen van 4000 cijfers) veel rekentijd kost. Het is niet onmogelijk, maar klassieke algoritmen doen hier veel te lang over (eeuwen of langer). Het algoritme van Peter Shor kan het ontbinden aanzienlijk versnellen als de langzaamste stap draait op een quantumcomputer. Encryptie volgens het RSA systeem is dus met quantumcomputing te kraken. Dit heeft enorme maatschappelijke gevolgen. Gelukkig geven quantumcomputers ook de oplossing: er worden nieuwe post-quantum encryptiesystemen ontwikkeld.

Peter Shor's algoritme kwam niet uit het niets. In dit [filmpje](#) (tussen ongeveer 8:50-14 minuten) vertelt hij hoe hij vanaf 1991 tot zijn ontdekkingen is gekomen. Hij noemt daarbij telkens met wie hij samenwerkt. Zo werkt wetenschap.



De opkomst van de quantumcomputer schept onrust bij banken, het verzekeringswezen en de wereld van de tech-giganten zoals Google, Amazon en IBM. Zij begrijpen dat quantumtechnologie de wereld ingrijpend kan gaan veranderen. En wie te laat komt mist de boot. Er worden nu miljarden geïnvesteerd door deze bedrijven en overheden. In Nederland is in 2019 de Nationale Agenda Quantum-technologie [2] opgesteld. Daarin wordt een flink aantal gebieden genoemd waarin de quantumtechnologie een rol kan gaan spelen. We noemen enkele voorbeelden:

- Cryptografie: behalve gevaren voor de bestaande versleutelingstechnieken biedt de quantumcomputer ook een mogelijkheid om communicatie te beveiligen. In de module behandelen we het BB84-protocol [3].
- Rekensnelheid: niet alleen bij het algoritme van Shor is de quantumcomputer superieur aan de klassieke computer. Er is in 2009 een algoritme opgesteld om een stelsel lineaire ver-

gelijkingen sneller te kunnen oplossen. Ook wordt gewerkt aan snellere algoritmes ten behoeve van optimalisatieproblemen. Als toepassing worden genoemd: klimaatvoorspellingen, doorrekenen van modellen op het gebied van waterhuishouding, modelberekeningen uit de financiële wereld, (medische) beeldvorming, proces-optimalisatie etc.

- Simulaties: De meest voor de hand liggende toepassingen liggen in het simuleren van grote moleculen zoals in de farmacie. Een ander voorbeeld is het maken van kunstmest. De grondstof voor kunstmest is ammoniak (NH_3). Dat wordt nu gemaakt volgens het Haber-Bosch proces. Dit proces vindt plaats bij hoge temperatuur en druk en kost enorm veel energie. Bacteriën in de wortels van vlinderbloemigen kunnen stikstof uit de lucht (N_2) enzymatisch, bij kamertemperatuur en druk, omzetten in ammoniak. Dit proces kost veel minder energie. Zij gebruiken hiervoor een enzym (FeMoCo) waarvan de werking nog niet begrepen is. Omdat dit een relatief klein enzym is zouden quantumcomputers al op korte termijn een bijdrage kunnen leveren aan de oplossing van het kunstmest probleem. Zonder dat er nog een quantumcomputer is hebben al veel vakgebieden nagedacht over toepassingen. Voor een overzicht zie tabel 2 in [7].

Opbouw en leerdoelen

De module bestaat uit twee delen. In het eerste deel bouwen we ons begrippenapparaat op, in het tweede deel passen we onze kennis toe in praktische opdrachten. Het eerste deel bestaat uit drie hoofdstukken, met opgaven en werkbladen. Aan het eind van ieder hoofdstuk staan de leerdoelen samengevat. In hoofdstuk 1 beginnen we met een korte inleiding op het onderwerp en maken we kennis met enkele belangrijke begrippen en fenomenen door zelf te experimenteren met licht. Om de vergelijking te maken met een quantumcomputer begint hoofdstuk 2 met een korte uitleg over hoe een klassieke computer werkt. We onderbouwen ons wiskundig begrippenapparaat met een model. Het hoofdstuk eindigt met een eisenlijst waaraan een quantumcomputer moet voldoen. In hoofdstuk 3 behandelen we de bouwblokken (poorten) van quantumcomputers. We zien dat die echt anders zijn. We combineren de poorten in een algoritme dat je echt niet op een klassieke computer kunt

uitvoeren: teleportatie. We sluiten het hoofdstuk af met een blik op de toekomst. Na dit hoofdstuk volgt een toets.

Het tweede deel (hoofdstuk 4) is een verzameling praktische keuzeopdrachten. In dit deel onderzoek je in samenwerkingsverband een aspect van quantumcomputing; je onderzoekt een algoritme, je verdiept je in wiskunde D, onderzoekt een technisch aspect of je denkt na over de maatschappelijke consequenties. Er is ook de mogelijkheid om dit deel in te vullen met een activiteit aangeboden door één van de universiteiten bij jou in de buurt. Wanneer je deze module hebt afgesloten, hopen we dat je een goed beeld hebt gevormd over wat deze technologie in de toekomst voor jou en de maatschappij kan betekenen.

1.2 Een experiment uit de 'oertijd'

We starten met een experiment dat al in 1802 door Thomas Young werd uitgevoerd. Hij liet licht door kleine spleten gaan en nam golfverschijnselen waar. In werkblad 5.1 onderzoeken we eerst hoe licht door een enkele kleine spleet gaat, en onderzoeken we hoe twee kleine spleten elkaar beïnvloeden. We gebruiken daarna polarisatie, een eigenschap van licht die aan Young nog niet bekend was, om tot moderne inzichten in het dubbelspleetexperiment te komen. De experimenten brengen ons drie belangrijke fenomenen uit de quantumwereld: *interferentie*, *superpositie* en de *waarneming*. Een vierde quantumeigenschap *verstrekking*, komt pas aan het eind van hoofdstuk 3 aan de orde.

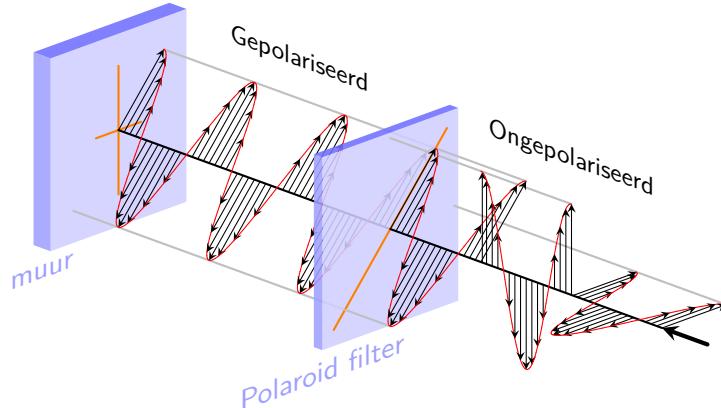
Experiment van Young 1

Voer het werkblad 5.1 uit

Polarisatie

De resultaten van het experiment van Young 5.1 zijn een tussenstap die we even moeten onthouden. We pakken ze later weer op. Voor we er mee verder gaan, hebben we een andere eigenschap van licht nodig, polarisatie. Je kunt licht voorstellen als een *transversale* golf die zich met de lichtsnelheid voortbeweegt zoals in figuur 1.1. In een transversale golf is de uitwijking van een punt in een vlak loodrecht

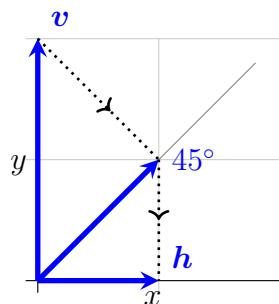
op voortgangsrichting van de golf. Lineaire polarisatiefilters laten alleen één trillingsrichting door, de rest wordt geabsorbeerd door het filter. Ze projecteren daarmee de trilling in één richting.



Figuur 1.1: Ongepolariseerde fotonen voeren een trilling uit in een willekeurige richting, die loodrecht op de voortplantingsrichting staat. Na het polarisatiefilter ligt de trillingsrichting vast. Het filter staat hier onder een hoek van 45° .

Wet van Malus

Voer werkblad 5.2 uit.



Figuur 1.2: De amplitude van verticaal gepolariseerd licht halveert als het in twee stappen over 45° horizontaal gepolariseerd wordt.

In werkblad 5.2 heb je de wet van Malus ontdekt: $I_\theta = I_0 \cos^2 \theta$. We passen de wet van Malus nu toe. Wat gebeurt er als je een derde filter onder een hoek van 45° tussen twee loodrechte polarisatiefilters plaatst? Als we twee keer achter elkaar een filter onder een hoek van 45° toepassen op licht dat aanvankelijk verticaal gepolariseerd is eindigen we ook horizontaal, maar nu houden we wél licht over. Je weet dat $\cos 45^\circ = \frac{1}{\sqrt{2}}$. Na twee filters wordt de amplitude dus gehalveerd, zie figuur 1.2. De intensiteit wordt na twee keer toepassen van de wet van Malus dus tot een vierde teruggebracht.

Bedenk telkens wat de experimenten zouden doen als ze uitgevoerd worden met enkele fotonen. Met deze kennis pakken we het dubbelspleetexperiment weer op.

Experiment van Young 2

Voer werkblad 5.3 uit



filmpje

Dit [filmpje](#) geeft een simulatie van het experiment alsof het met enkele fotonen is uitgevoerd.

De laatste vraag in het werkblad is lastig. Op de laatste stap na, kunnen we de dubbel- en enkelspleetpatronen van experiment 5.3 verklaren met klassieke interferentie. Om ook stap f. te begrijpen moeten we afdalen naar de quantumwereld. In opdracht 1.1 ontwerp je zo'n experiment.

Opdracht 1.1

Een rode laserpen van experiment 5.3 heeft een vermogen van ongeveer 1 mW. In een opstelling staat de dubbelspleet 30 cm van de sensor die enkele fotonen kan waarnemen. De hele opstelling staat in een lichtdichte doos natuurlijk. Je kunt het licht verzwakken met grijsfilters. De verzwakking van grijsfilters (neutral density, ND) geef je aan met een getal. Zo verzwakt een ND 2.0 filter het licht 100 keer, en een ND 4.0 10,000 keer. Je hebt de beschikking over een aantal ND 2.0 en ND 3.0 filters. Welke filters moet je minimaal gebruiken om gemiddeld minder dan één foton tegelijk in de lichtweg van het experiment te hebben?

Het duurt langer, maar dit *single-photon* experiment levert uiteindelijk hetzelfde interferentiepatroon als bij grote intensiteit. Het patroon kan alleen verklaard worden uit de interferentie van één foton via twee spleten. Het foton gedraagt zich alsof het door twee spleten tegelijk is gegaan. Dit is een voorbeeld van superpositie (van de plaats). Bovendien moet er een superpositie van de polarisatietoestand zijn want in het experiment (stappen d-f) konden we de polarisatietoestand beïnvloeden lang nadat het foton door de twee spleten (met loodrecht gerichte polarisatoren) is gegaan. Na een meting verdwijnt de superpositie. In ons geval lost de superpositie met een zekere kans op in één van de oplossingen. Bij ons is de meting het patroon op de muur. De intensiteit van de verschillende patronen geeft een indruk van de kans. Superpositie, interferentie, kans en meting zijn de kernbegrippen waarmee je een quantumcomputer bouwt.

Waar één foton terecht komt is niet te voorspellen, maar ze volgen wel een patroon. Zo komen er nooit fotonen aan op de donkere plekken. De kans is het grootst om in het midden aan te komen, daar is de intensiteit het hoogst. De opbouw van het patroon laat het *intrinsieke kansproces* van de quantummechanica zien. Elk fo-

Om aan het begrip superpositie te wennen hier een voorbeeldje uit de wiskunde. Als je weet dat $x^2 = 4$ dan kan $x = 2$ of $x = +2$ zijn. In de uitdrukking $x^2 = 4$ verkeert x in superpositie.

ton voldoet kennelijk aan een onderliggende kansverdeling. Die verdeling wordt duidelijk in het intensiteitspatroon als er veel fotonen door de dubbelspleet zijn gegaan.

Een enkel foton kan dus in superpositie zijn en door beide spleten tegelijkertijd gaan. Wanneer we dit beter willen bestuderen, zouden we de meting al bij de spleten kunnen doen om te kijken door welke spleet het foton nou echt gaat. Maar als we dat doen, zullen we het foton altijd slechts in één spleet meten. Door het foton te meten, gedraagt het foton zich alsof het door een enkele spleet is gegaan. Het foton volgt dan de kansverdeling van het enkelspleet patroon.

Alleen als we het experiment zeer vaak herhalen (veel fotonen) wordt de opgebouwde kansverdeling zichtbaar in het intensiteitspatroon. Dit is een aspect van *de waarneming*, een derde fundamenteel van de quantumcomputer. Het vierde fundament, *verstrekking*, behandelen we aan het eind van hoofdstuk 3. In het volgende hoofdstuk 2 bouwen we eerst het begrip twee-toestandsysteem verder op.

1.3 Leerdoelen

In dit hoofdstuk heb je kennis gemaakt met een flink aantal nieuwe begrippen. Aan het eind van ieder hoofdstuk vatten we de stof en de leerdoelen in kernwoorden samen. Controleer of je deze begrippen herkent. Het is niet erg als je moeilijke begrippen nog niet helemaal kunt plaatsen, ze komen in de volgende hoofdstukken terug.

- Deeltjes hebben golfeigenschappen en golven hebben deeltjeseigenschappen.
 - Herken de verschillen en overeenkomsten in de enkel- en dubbelspleetexperimenten.
 - Licht bestaat uit fotonen, energiepakketjes.
 - Licht heeft ook een golflengte.
 - Licht is een transversale trilling/golf die gepolariseerd kan worden.
 - Horizontale en verticale polarisatie sluiten elkaar uit: er is geen overlap.
 - Herken een twee-toestandsysteem.
 - De polarisatie-eigenschap van licht is een quantumeigenschap.
-

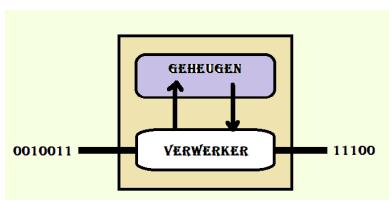
- Wet van Malus: $I_\theta = I_0 \cos^2 \theta$.
- Interferentie, superpositie, verstrengeling en waarneming zijn begrippen met een eigen betekenis in de quantumwereld.
- Een groot aantal herhalingen van een experiment levert de kansverdeling van het individueel gedrag van quantumdeeltjes, en omgekeerd:
- Quantumdeeltjes gedragen zich intrinsiek onvoorspelbaar, maar zij volgen wel een kansverdeling die duidelijk wordt als er veel waarnemingen worden gedaan.



2. Waar is het qubit?

In dit hoofdstuk gaan we op zoek naar het qubit. We onderzoeken eerst hoe een klassieke computer met bits werkt. We leren rekenen met een twee-toestandsysteem en hoe je er mee kunt rekenen op de eenheidscirkel. We leren te wisselen van basis. Deze stap hebben we nodig om het verschil tussen klassieke bits en quantum bits uit te leggen. Het hoofdstuk sluit af met een lijst met criteria waar een quantumcomputer aan moet voldoen.

2.1 Van bits ...



Figuur 2.1: Een zeer vereenvoudigde centrale verwerkingseenheid (central processing unit, CPU). Het hart van een klassieke computer.

Een klassieke computer verwerkt reeksen nullen en enen, die soms gegevens en soms instructies voorstellen. Een processor transformeert de reeks naar een andere reeks. Daarbij worden ook nullen en enen naar het geheugen geschreven en opgehaald uit het geheugen. Tot op de dag van vandaag werken bijna alle computers volgens dit systeem dat in 1945 is uitgedacht door John von Neumann [12]. In dit [filmpje](#) van 4 minuten wordt een berekening uitgevoerd die op jouw computer makkelijk binnen enkele nanoseconden wordt uitgevoerd.



filmpje

Klassieke computers beschikken over de volgende kenmerken:

- Ze werken met bits. Een bit is de elementaire informatiedrager die nul of één kan zijn. Het antwoord op een vraag die met ja of nee kan worden beantwoord bevat één bit informatie. Eén Megabit bevat dus de informatie van een miljoen ja/nee-vragen.

- Ze maken gebruik van een verwerker. Deze beschikt over logische poorten die een reeks nullen en enen kunnen veranderen in een andere reeks nullen en enen.
- Er is een set poorten waarmee je elke logische schakeling kunt maken. Een universele set is bijvoorbeeld te maken met de EN en de NOT poort en de mogelijkheid om de uitkomst van één poort naar twee of meer andere poorten door te sturen als input.
- Met de vorige eigenschap kunnen bits dus gekopieerd worden.
- Je kunt bits in een permanent geheugen bewaren.

In werkblad 5.4 leer je werken met klassieke poorten. De verwerker beschikt over logische poorten. Als je hier iets meer over wilt weten dan moet je het experiment bij werkblad 5.4 uitvoeren.

Klassieke bits

Voer werkblad 5.4 uit.

De quantumcomputer verschilt van de klassieke computer:

- Een quantumcomputer werkt niet met bits maar met qubits. In dit hoofdstuk gaan we verkennen wat daar de eigenschappen van zijn.
- De quantumcomputer kent wel poorten, maar die zien er heel anders uit. In hoofdstuk 3 zullen we die verkennen.
- Kopiëren van een qubit is niet mogelijk, dus een quantumpoort kan maar aan één poort informatie doorgeven.

Kortom, klassieke computers kunnen dingen die quantumcomputers niet kunnen. Quantumcomputers zullen klassieke computers niet vervangen. Maar die quantumcomputers kunnen dingen die klassieke computers niet kunnen...

2.2 ... naar qubits

Quantumcomputers hebben hun eigen elementaire informatiedragers, het quantumbit ofwel qubit. Ook het qubit kent twee basistoestanden. In werkblad 5.3 maakten we al kennis met de superpositie van fotonen die in het dubbelspleetexperiment zowel horizontaal als verticaal gepolariseerd waren. Om een idee te krijgen wat dit be-

tekent kijken we naar een model voor superpositie uit de klassieke wereld. Bekijk figuur 2.2.



Figuur 2.2: Wat is hier afgebeeld?)

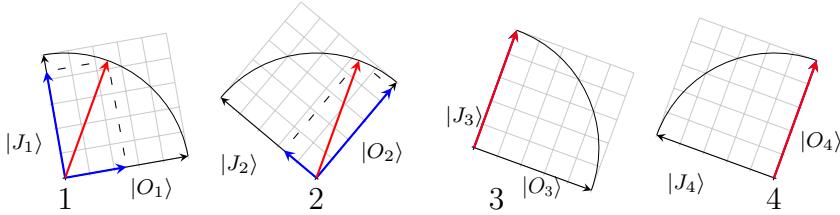
De afbeelding heette in 1915 "My Wife and My Mother-in-Law" [8] naar een Duitse ansichtkaart uit 1888. De tekening zou men kunnen beschouwen als een superpositie van de afbeeldingen van een jonge vrouw en van een oude vrouw. Maar als je gaat kijken, en dus een meting doet, dan zie je slechts één van de twee. Onze hersenen kunnen kennelijk maar één van de twee beelden tegelijk verwerken.

Oude vrouw Jonge vrouw

Voer het eerste deel van werkblad 5.5 uit.

Het plaatje is een objectief gegeven. De tekenaar heeft zijn best gedaan de oude en de jonge vrouw allebei tot uiting te laten komen. We kunnen de inhoud 'oud en jong' in het plaatje als een vector voorstellen in een willekeurige maar vaste richting. In figuur 2.3 is dat met een rode pijl weergegeven.

Waarnemers scoren verschillende percentages oude of jonge vrouw. Hoe waarnemers het plaatje interpreteren is het resultaat van de test: het percentage 'oud' en 'jong'.



Figuur 2.3: Resultaten van vier waarnemers van “oude vrouw/jonge vrouw”. Het object (rode pijl) is voor alle waarnemers gelijk. Bij elke waarnemer hoort een eigen assenstelsel.

In figuur 2.3 hebben vier waarnemers (W) een tijdje naar hetzelfde plaatje gekeken. W_1 ziet vaker een jonge vrouw en W_2 heeft een grote kans om een oude vrouw te zien. W_3 ziet met zekerheid een jonge vrouw. En W_4 ziet met zekerheid een oude vrouw.

Het nut van deze abstracte voorstelling is dat deze gebruik maakt van dezelfde wiskundige taal als de quantumtheorie. Het assenstelsel is dan karakteristiek voor de waarnemer.

De notatie $|0\rangle$ en $|1\rangle$ lijkt op de pijl van een vector. Dit is de *braket* notatie van Paul Dirac, een Brits natuurkundige en een pionier in de quantumtheorie.

De twee toestanden ‘oud’ en ‘jong’ zouden we als klassieke bits kunnen opvatten. Hier gebruikt de waarnemer een vectorruimte om verschillende toestanden ten opzichte van elkaar vast te leggen. Die vectorruimte wordt opgespannen met twee basisvectoren die elkaar uitsluiten. Voor de eerste waarnemer zijn dat $|J_1\rangle$ en $|O_1\rangle$. Op basis van figuur 2.3 geldt blijkbaar (meet de relatieve amplitudes maar na):

De coëfficiënten noem je *amplitudes*, hun kwadranten geven de *kans*.

$$|\Psi_{JO}\rangle = 0,87|J_1\rangle + 0,5|O_1\rangle$$

De Griekse letter Ψ (spreek uit: psi) wordt in de quantumwereld vaak gebruikt om een toestand uit te drukken. Herken je de vectoroptelling die je ook gebruikt als je bijvoorbeeld krachten optelt? De coëfficiënten geven de lengtes aan van de projecties op de assen. De toestandsvectoren hebben altijd een lengte 1. De stelling van Pythagoras leert:

$$0,87^2 + 0,5^2 = 0,75 + 0,25 = 1$$

Bedenk dat de waarnemer ófwel een jonge vrouw ófwel een oude vrouw ziet. Er geldt dus dat (kans op een oude vrouw) + (kans op een jonge vrouw) = 100 %. In dit voorbeeld geldt blijkbaar dat

waarnemer 1 een kans van 75% heeft om een jonge vrouw te zien en een kans van 25% om een oude vrouw te zien.

Pas op! De afbeelding van figuur 2.2 is geen qubit. Het is geen quantumobject.

Opdracht 2.1

Hoeveel machten van tien zouden we moeten inzoomen om van het plaatje tot in de quantumwereld te komen?

Het model lijkt een superpositie van twee toestanden te dragen. Bij een waarneming zie je maar één van de twee. We kunnen de kans en amplitude beschrijven en weergeven in een vectorvoorstelling zoals in het tweede deel van experiment 5.5.

Oude vrouw Jonge vrouw

Voer het tweede deel van werkblad 5.5 uit.

Maar het blijft een metafoor, we hebben nog geen stap in de quantumwereld gezet. Het wordt tijd om te kijken naar een echt qubit.

2.3 Hier is het qubit

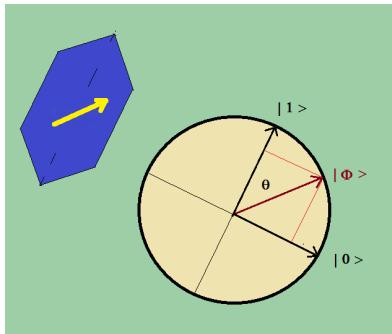
We zetten even op een rijtje wat onze verkenningen tot nu toe hebben opgeleverd.

- In hoofdstuk 1 hebben we *interferentie* gevonden bij het enkel-en dubbelspleetexperiment, een bewijs voor het golfkarakter van licht.
- We gebruikten Einsteins bevinding dat licht opgebouwd is uit deeltjes (energiepakketjes) die we nu fotonen noemen. In een simulatie zagen we dat het gedrag van individuele fotonen niet voorspelbaar is, maar dat zij wel een kansverdeling volgen. Als je heel veel fotonen projecteert wordt deze kansverdeling in het intensiteitspatroon zichtbaar.
- We onderzochten polarisatie, een eigenschap die alleen bij transversale golven kan optreden. Als ongepolariseerd licht door een polarisatiefilter gaat, wordt de helft tegengehouden

en de helft die doorgelaten wordt krijgt de polarisatierichting van het filter. Alle doorgelaten fotonen hebben nu dezelfde polarisatierichting. De bundel is *geprepareerd*. In figuur 2.4 valt een bundel licht die gepolariseerd is in de richting van de pijl op een polarisatiefilter. De doorlaatrichting van het filter is de lange as, die een hoek θ maakt met de lichtbundel. De kans om doorgelaten te worden is evenredig met $\cos^2 \theta$. We toonden dit aan in werkblad 5.2 door gepolariseerd licht van een computerscherm te gebruiken.

De wet van Malus:

$$I = I_0 \cos^2 \theta$$



Figuur 2.4: De polarisatierichting is in de lengterichting van het blauwe kristal. Een foton in de toestand $|1\rangle$ zal het filter passeren. Een foton in de toestand $|0\rangle$ wordt tegengehouden. Het foton in de afbeelding heeft een kans van $\cos^2 \theta$ om te worden doorgelaten.

Aan het tweede filter kunnen we nu een coördinatenstelsel toewijzen (zie figuur 2.4). Toestand $|1\rangle$ wordt zeker doorgelaten, en toestand $|0\rangle$ wordt zeker geblokkeerd. Aan elke toestand wijzen we nu een vector toe met lengte 1 en een richting die overeenkomt met de polarisatierichting van die toestand. In de vierde klas heb je geleerd dat in figuur 2.4 moet gelden:

$$|\Psi\rangle = \sin \theta |0\rangle + \cos \theta |1\rangle$$

In een andere notatie, als we voor $\sin \theta = \alpha$ en $\cos \theta = \beta$ invullen, en de basisvectoren schrijven als $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ en $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, schrijven we ook wel:

$$\begin{aligned} |\Psi\rangle &= \alpha |0\rangle + \beta |1\rangle \\ |\Psi\rangle &= \begin{pmatrix} \sin \theta \\ \cos \theta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \end{aligned}$$

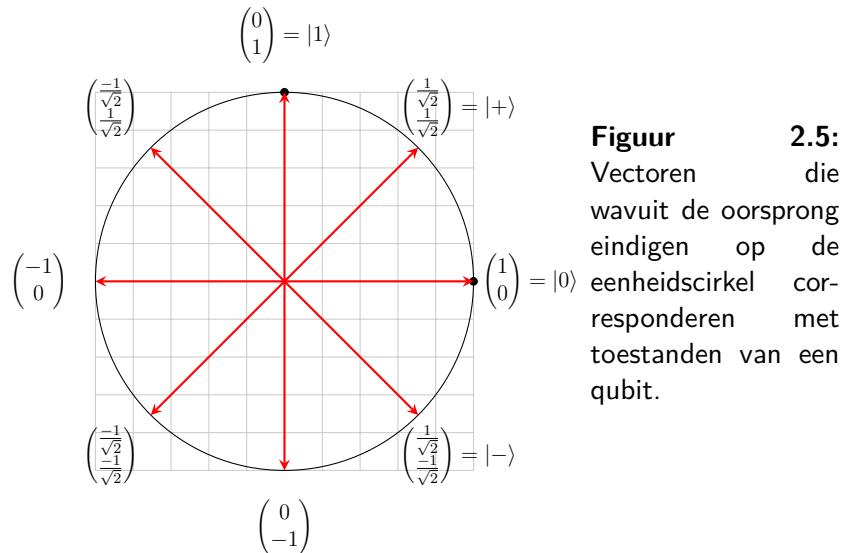
We kunnen de toestand van het foton dus opvatten als een superpositie van de basistoestanden. 'Het foton is als het ware in twee toestanden tegelijkertijd'. Dit is een eigenschap die een klassiek bit niet heeft, dat is immers altijd 0 of 1. De kans dat het foton

wordt doorgelaten is dan blijkbaar gelijk aan β^2 . Er is natuurlijk ook een kans dat het foton door het tweede filter juist wordt tegengehouden. De beide kansen samen moeten optellen tot 1. De kans op tegenhouden moet dan wel gelijk zijn aan het kwadraat van de coëfficiënt van de toestand $|0\rangle$. Er geldt immers

$$\cos^2 \theta + \sin^2 \theta = 1, \quad \alpha^2 + \beta^2 = 1$$

Elke toestand kan als een vector op de eenheidscirkel worden geschreven. In figuur 2.4 zagen we dat al.

In figuur 2.5 is de eenheidscirkel nogmaals getekend. Elk punt op de eenheidscirkel correspondeert met een toestand. Er zijn oneindig veel toestanden want er zijn oneindig veel punten op een cirkel. Van acht toestanden is de bijbehorende vector getekend.



Figuur 2.5:
Vectoren die wauit de oorsprong eindigen op de eenheidscirkel corresponderen met toestanden van een qubit.

Stel nu dat we een foton hebben met een onbekende toestand $|\Psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$. Kunnen we door middel van metingen vaststellen wat de toestandscoëfficiënten α en β zijn?

De procedure is als volgt. Het filter staat klaar en achter het filter is een fotodetector geplaatst die een klik geeft als er één foton opvalt. Het foton valt op het filter. Er is nu een kans dat hij er door gaat en dan hoor je een klik. Maar als hij wordt tegengehouden hoor je niets. Dat is alles. Klik of geen klik. Het experiment overdoen kan niet. Het foton is weg, en daarmee de informatie over zijn polarisatietoestand.

De enige manier om de toestand van het foton te achterhalen is door het experiment te herhalen met een groot aantal fotonen die allemaal in dezelfde toestand verkeren. Met behulp van de klikfrequenties kan nu statistiek worden bedreven. Daarover gaat opdracht [2.2](#).

Opdracht 2.2

Een polarisatiefilter staat verticaal opgesteld. Achter het filter staat een fotodetector die een klik geeft als er een foton opvalt. Men laat 1000 fotonen op het filter vallen die allemaal op dezelfde wijze zijn geprepareerd. De toestand van de fotonen wordt beschreven met de formule

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Er wordt 750 keer een klik vastgesteld.

- a. Bereken de coëfficiënten α en β .
- b. Bereken de hoek tussen de polarisatierichting van de fotonen en de doorlaatrichting van het filter.

2.4 Het meten met verschillende bases

In het voorgaande zagen we dat de toestand van een qubit kan worden beschreven met behulp van een toestandsvector. Om de toestand te leren kennen zal er gemeten moeten worden. Maar met het meetapparaat komt een meetbasis. Zo'n meetbasis bestaat uit twee toestanden waarvan de bijbehorende toestandsvectoren loodrecht op elkaar staan. De onderzoeker noemt die twee toestanden doorgaans $|0\rangle$ en $|1\rangle$. Men spreekt in dat geval van de standaardbasis. Die basis is een vrije keuze. Als er dus twee onderzoekers zijn, die elk hun eigen basis kiezen is het handig om de twee bases te onderscheiden met een subscript, bijvoorbeeld $|0\rangle_A$ en $|1\rangle_A$ voor de één en $|0\rangle_B$ en $|1\rangle_B$ voor de ander.

Voor onderzoeker A is de toestand van het qubit gelijk aan

$$|\Psi\rangle = \alpha|0\rangle_A + \beta|1\rangle_A$$

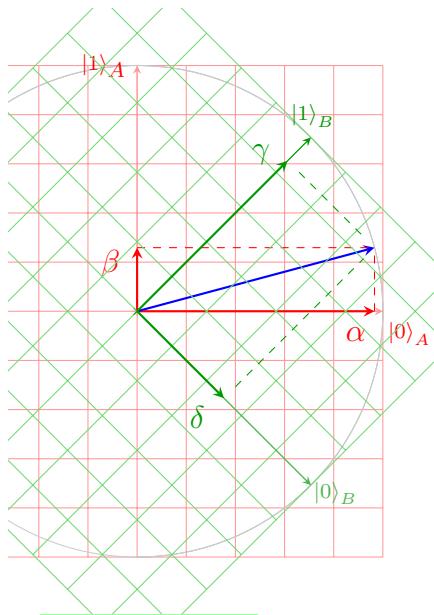
Voor onderzoeker B is de toestand van het qubit gelijk aan

$$|\Psi\rangle = \gamma |0\rangle_B + \delta |1\rangle_B$$

Het verwisselen van bases is een belangrijk instrument in quantumalgoritmes. Naast de standaardbasis wordt vaak de diagonale basis gebruikt die in figuur 2.6 is afgebeeld. Voor de diagonale basis gebruiken we meestal $|+\rangle$ en $|-\rangle$:

$$|+\rangle = |1\rangle_B = |1\rangle_{45^\circ}$$

$$|-\rangle = |0\rangle_B = |0\rangle_{45^\circ}$$



Figuur 2.6: De blauwe toestandsvector wordt in de standaardbasis (rood) genoteerd als $|\Psi\rangle = \alpha |0\rangle_A + \beta |1\rangle_A$ en in de diagonale basis (groen) als $|\Psi\rangle = \gamma |0\rangle_B + \delta |1\rangle_B$

Opdracht 2.3

Een onderzoeker beschikt over een qubit in de toestand $|\Psi\rangle = \frac{1}{2} |0\rangle + \frac{1}{2}\sqrt{3} |1\rangle$. Hij gaat over van de standaardbasis $|0\rangle$ en $|1\rangle$ naar de diagonale basis $|+\rangle$ en $|-\rangle$. De toestand wordt dan beschreven door $|\Psi\rangle = \gamma |+\rangle + \delta |-\rangle$

- a. Bereken de coëfficiënten γ en δ
- b. Bereken de kans op een $|0\rangle$ in de standaardbasis.
- c. Bereken de kans op een $|+\rangle$ in de diagonale basis.

2.5 Over het meetprobleem

In hoofdstuk 1 is het tweespleten-experiment ter sprake gekomen. Op een scherm werd daar een interferentiepatroon zichtbaar van invallend licht. Interferentie is een golfverschijnsel. Een golf valt op twee spleten en het deel dat door de ene spleet gaat interfeert met het deel dat door de andere spleet gaat. Voor deeltjes is een dergelijke uitleg niet mogelijk. Maar een interferentiepatroon ontstaat ook als de fotonen één voor één op het scherm terecht komen. Wat interfereert nu met wat? Het interferentie-experiment maakt duidelijk dat je niet mag stellen dat een foton door één van de spleten gaat. Maar wat dan wel?

Het scherm denken we opgedeeld in plaatsen waar de fotonen het scherm kunnen treffen. De toestand van de fotonen vlak voor ze het scherm gaan treffen kan worden beschreven als een superpositie van de verschillende mogelijkheden:

$$|\Psi\rangle = c_1 |P_1\rangle + c_2 |P_2\rangle + c_3 |P_3\rangle + c_4 |P_4\rangle + c_5 |P_5\rangle + c_6 |P_6\rangle + \dots$$

Maar op het moment dat het foton het scherm treft, bijvoorbeeld op plaats 5, geldt ineens: $|\Psi\rangle = |P_5\rangle$. In een klap is er sprake van één foton en het is ook duidelijk waar het is. Maar vlak voor de inslag was er niet sprake van een foton dichtbij plaats P_5 . Deze vreemde gang van zaken dwong natuurkundigen na te denken over de vraag wat hun kennis eigenlijk inhield.



Erwin, ik heb een probleem

Voor Niels Bohr (1885-1962), de grote Deense natuurkundige uit Kopenhagen, was dit aanleiding om aan te nemen dat eigenschappen pas ontstaan op het moment van de wisselwerking, nodig voor de waarneming. Vóór de meting zijn er alleen maar mogelijkheden. Deze opvatting die bekend zou worden als de Kopenhaagse interpretatie wordt ook van toepassing geacht bij het uitlezen van een qubit. Stel een qubit bevindt zich in een toestand van superpositie.

Dus:

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

Bij uitlezing verandert de toestand van het qubit. Het wordt $|0\rangle$ of $|1\rangle$. Dat is een irreversibel proces. De oorspronkelijke toestand is verloren gegaan. Volgens de Kopenhaagse interpretatie is de superpositie alleen maar een optelsom van mogelijkheden. Er bestaat geen onderliggende realiteit. Voor een man als Einstein was het ontbreken van quantumrealiteit onaanvaardbaar. En in 1935 bedacht hij met zijn medewerkers Nathan Rosen en Boris Podolsky [5] een gedachte-experiment. De publicatie was bedoeld om het model om zeep te helpen dat eigenschappen pas ontstaan op het moment van de wisselwerking bij waarneming. De publicatie is bekend geworden als de EPR-paradox. Om de gedachten achter de publicatie te verduidelijken maken we gebruik van een voorbeeld waarin twee elektronen worden uitgezonden in tegengestelde richting.

Elektronen hebben spin. Over die eigenschap valt alleen maar te zeggen dat er een richting bij hoort. Vergelijk het met de richting waarin de punt van een spijker wijst als een spijker door de lucht vliegt. Een elektron met spin is een voorbeeld van een qubit. Een meetapparaat kan maar twee toestanden vastleggen die bij spin *up* $|\uparrow\rangle$ en *down* $|\downarrow\rangle$ worden genoemd. In de toestand $|\uparrow\rangle$ heeft het elektron een klein beetje meer energie dan in de toestand $|\downarrow\rangle$. Om verwarring te voorkomen houden we de notatie aan die we bij polarisatie van fotonen en oudevrouw/jongevrouw hebben gebruikt. We zullen de benaming $|0\rangle$ voor de lagere energietoestand gebruiken en $|1\rangle$ voor de andere toestand.

Het experiment begint met twee elektronen die tegengestelde spinrichting hebben. Als de één in de toestand $|1\rangle$ zit, verkeert de andere in de toestand $|0\rangle$ en omgekeerd. Om bij het beeld van de spijkers te blijven: ze blijven parallel gericht maar wel tegengesteld. De ene spijker vliegt de ene kant op en de andere de andere kant. Als de beide elektronen op grote afstand van elkaar zijn wordt hun spin gemeten met een meetapparaat. En dat geeft dan een meetuitkomst: '0 of 1' .

Alice bevindt zich met een meetapparaat op de ene plaats. Bob bevindt zich op de andere plaats. Zijn meetapparaat is identiek aan dat van Alice en ze meten beide in dezelfde basis. De elektronenbron zit precies tussen hen in. Dus de beide elektronen van één paar komen gelijktijdig aan bij Alice en Bob.

Het is hoog tijd om twee trouwe virtuele helpertjes voor te stellen: Alice en Bob. Zij helpen graag als een quantum-situatie verduidelijkt moet worden. Later zullen we ook Eve ontmoeten (van eavesdropping, afluisteren). Zij probeert tegen te werken.

De redenering van EPR was nu als volgt: als Alice haar qubit uitleest en ze vindt een 1, en Bob beschikt over eenzelfde meetapparaat met dezelfde meetinstelling (zelfde basis), dan krijgt Bob de meetuitkomst 0. Niet vreemd volgens de opvatting van EPR want die eigenschap hebben de elektronen van meet af aan meegekregen bij de creatie! Maar aldus EPR: de Kopenhaagse opvatting is wel vreemd. Want volgens deze opvatting ontstaat de eigenschap $|0\rangle$ pas op het moment van de meting door Alice! En dan zou dus ook pas op dat moment de eigenschap $|1\rangle$ ontstaan bij het elektron van Bob! Maar de beide elektronen bevinden zich op grote onderlinge afstand! Dat was onmogelijk volgens Einstein en zijn medewerkers. Een handeling van Alice zou instantaan (=onmiddelijk) gevolgen hebben voor een ver-verwijderd object. Volgens Einstein was er een onderliggende realiteit die door de quantummechanica niet werd beschreven. De quantummechanica was volgens hem daarom een onvolledige theorie.



Het verweer van Niels Bohr was dat de beide elektronen een geheel vormden. Tegenwoordig zouden we zeggen: ze zijn maximaal *verstrengeld*. Maar die opvatting was voor Einstein weinig bevredigend. De opvattingen van de twee partijen in het quantumdebat bleven lijnrecht tegenover elkaar staan. Het debat werd beschouwd als een filosofisch debat. In de decennia daarop volgend gingen natuurkundigen de kwestie uit de weg omdat er van uit werd gegaan dat het meningsverschil niet middels het experiment kon worden beslecht.

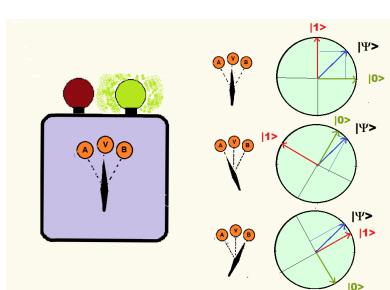
Maar in 1964 kwam daarin verandering. Een Ierse onderzoeker, John Bell, liet zien dat er een manier bestond om de Kopenhaagse opvatting aan een empirische toets te onderwerpen. Hij voorspelde dat als de Kopenhaagse opvatting juist zou zijn dat er dan bij het door hem bedachte experiment een meetuitkomst zou optreden die onmogelijk gerealiseerd zou kunnen worden als Einstein en de zijnen gelijk zouden hebben. Sinds die tijd zijn er vele Belltesten uitgevoerd. Bij al die testen bleek steeds weer dat de grenzen van de klassieke natuurkunde werden overschreden. Het standpunt van

Einstein was redelijk, en volledig geworteld in de bestaande natuurkunde. In feite ging het hier dus om een controversie tussen twee denkwerelden. John Bell zelf geloofde eigenlijk ook dat Einstein het gelijk aan zijn zijde had. Maar in de fysische wereld is het niet de redelijkheid die de doorslag geeft, maar de empirische bevinding. En die bleek uit te vallen ten gunste van de Kopenhaagse opvatting. Einstein had ongelijk!

De Bell-test toont voor alle gevallen van verstrengelde paren aan dat de natuur niet-lokaal en niet-reeël is. In de volgende paragraaf (2.6) laten we in een hypothetisch experiment voor één geval zien dat de klassieke en de quantumredenering verschillende resultaten opleveren. Dit experiment is diverse malen uitgevoerd en in 2022 mochten Alain Aspect, John Clauser en Anton Zeilinger hiervoor de nobelprijs natuurkunde delen.

2.6 Een Bell-test

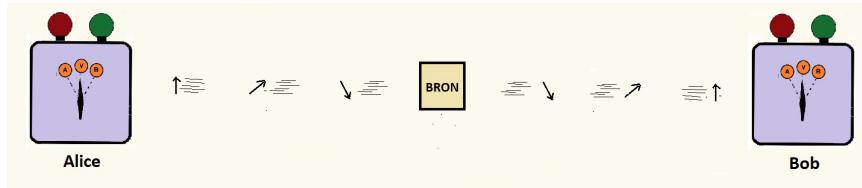
Hoe ziet zo'n Belltest er uit? Hieronder wordt een bepaalde Bell-test besproken. Alice en Bob bevinden zich op grote onderlinge afstand. Ze hebben allebei een meetapparaat om de spin te bepalen van een binnenvkomend elektron. Het meetapparaat kan in verschillende bases meten. In figuur 2.7 is het meetapparaat weergegeven waarover Alice en Bob beschikken. Het meetapparaat is zo ontworpen dat bij een elektron in de toestand $|0\rangle$ de groene lamp gaat branden en bij de toestand $|1\rangle$ een rode lamp.



Figuur 2.7: Een meetapparaat dat in drie verschillende bases kan meten. In dit geval wordt er blijkbaar een toestand $|0\rangle_V$ gemeten omdat de groene lamp brandt terwijl het apparaat meet in de verticale basis.

De drie bases zijn als volgt gekozen: V is de standaardbasis. A is een basis die verkregen wordt door een rotatie van 60° op de eenheidscirkel tegen de klok in. B is een basis die verkregen wordt door een rotatie van 60° op de eenheidscirkel met de klok mee.

Zowel Alice als Bob ontvangen elektronen waarvan ze de spinrichting kunnen bepalen. De binnenkomende elektronen hebben een willekeurige spinrichting, maar de spin van het ene elektron is wel identiek aan die van het andere elektron. Zowel Alice als Bob kiezen bij elke meting willekeurig in welke basis zij meten. Figuur 2.8 geeft weer wat er gebeurt in een klassieke gedachtegang.



Figuur 2.8: Een klassieke voorstelling. In het centrum worden elektronenparen gecreëerd die met identieke maar willekeurige spinrichting vanuit het centrum naar Alice en Bob worden gestuurd. Zij meten de spin waarbij ze kunnen kiezen tussen drie meetbases.

In het centrum worden elektronenparen met willekeurige spinrichtingen gecreëerd. Omdat de gekozen basis doorgaans niet overeenkomt met de spinrichting van het binnenkomend elektron is er sprake van een kansproces. In figuur 2.9 staat een tabel met denkbeeldige meetresultaten.

	Alice			Bob		
	A	V	B	A	V	B
meting 1	○	●	○	○	●	○
meting 2	●	○	○	○	○	●
meting 3	○	○	●	●	○	○
meting 4	●	○	○	○	○	●
meting 5	○	●	○	●	○	○
meting 6	○	●	○	○	●	○
meting 7	●	○	○	○	○	●
meting 8	●	○	○	●	○	○
meting 9	○	○	●	○	●	○

Figuur 2.9: De resultaten van negen metingen. Bij de tweede meting heeft Alice blijkbaar gebruik gemaakt van de basis A en registreerde zij de toestand $|1\rangle$ (rood) terwijl Bob de basis V gebruikte en daarbij een toestand $|0\rangle$ (groen) vaststelde.

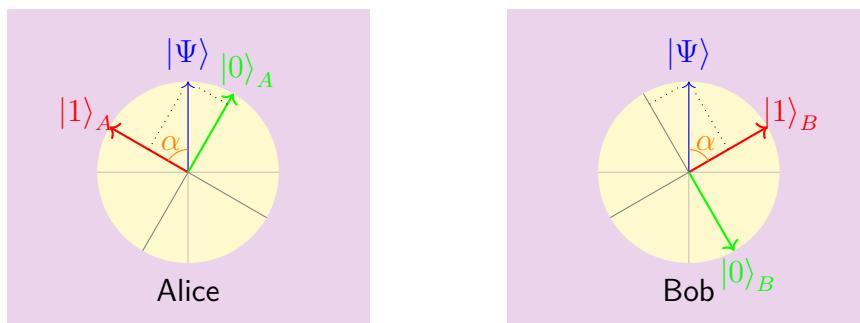
Bij deze Bell-test gaat het om de kans op een meetuitkomst waarbij een rode lamp en een groene lamp oplicht. In bovenstaande figuur zijn dat dus de metingen 1,2, 6 en 9.

De klassieke gedachtegang voorspelt nu dat de kans op kleurenverschil in ieder geval kleiner moet zijn dan $\frac{1}{2}$. Niet zo vreemd als bedacht wordt dat de twee elektronen van een paar dezelfde spinrichting hebben. De quantumtheorie voorspelt dat bij deze gekozen bases de kans dat de oplichtende lampen verschillende kleur hebben $\frac{1}{2}$ is. Waar komt dat verschil vandaan? Je kunt dit in zijn

algemeenheid bewijzen. In de volgende paragraaf laten we met één voorbeeld zien dat de klassieke en quantumwereld tot verschillende resultaten leiden. Dat is voldoende bewijs.

Kansen volgens EPR (klassiek)

We onderzoeken een voorbeeld met slechts één elektronenpaar. Bekijk figuur 2.8. In het centrum wordt een elektronenpaar gecreëerd met verticale spin. Eén elektron gaat naar Alice, het andere naar Bob. Alice meet in basis A. Bob heeft zijn schakelaar in de stand B staan. Wat is in een Einsteiniaanse (klassieke) gedachtekang de kans dat dit elektronenpaar zowel groen licht als rood licht oplevert? In deze gedachtekang wordt de spinrichting vastgelegd in het centrum. Om eerlijk te kunnen vergelijken met de Kopenhaagse versie moeten up en down beide kunnen voorkomen. In ons voorbeeld krijgen Alice en Bob daarom allebei een elektron in gelijke toestand. Die kan echter up of down zijn. Dus als Alice een toestand $|1\rangle_V$ krijgt, krijgt Bob die ook, en als Alice een $|0\rangle_V$ krijgt, krijgt Bob ook een $|0\rangle_V$. Voor het eerste geval (beiden een $|1\rangle_V$) werken we kansen op gelijke en ongelijke kleur uit. In opgave 2.4 kun je zelf uitrekenen dat deze kansen als beiden een $|0\rangle_V$ ontvangen gelijk blijven. De meting van Bob is volledig onafhankelijk van die van Alice. De kansen op rood of groen kunnen met vectordiagrammetjes in de eenheidscirkel worden bepaald op dezelfde manier als in het voorbeeld van jongevrouw/oudervrouw. Kijk maar eens naar figuur 2.10.



Figuur 2.10: Alice meet een qubit in de toestand $|1\rangle_V$ in de basis A. Bob meet $|1\rangle_V$ in basis B. Uit het diagram is te halen dat voor Alice de kans op groen licht $\frac{3}{4}$ is en de kans op rood licht $\frac{1}{4}$. Voor Bob geldt ook een kans van $\frac{3}{4}$ op groen en $\frac{1}{4}$ op rood.

In figuur 2.10 zien we dat Alice een kans van $\frac{1}{4}$ heeft op rood licht en van $\frac{3}{4}$ op groen licht. Voor Bob geldt hetzelfde! De kans op groen bij Alice en rood bij Bob kunnen we weergeven als $P(GR)$. Het gaat hier om onafhankelijke kansen, de kans op een combinatie van gebeurtenissen is het product van de kans op elk van die gebeurtenissen. In de tabel staan alle combinaties uitgerekend.

Klassieke kansen voor Alice en Bob: P_{AB}
$P_{GG} = \frac{3}{4} * \frac{3}{4} = \frac{9}{16}$
$P_{GR} = \frac{3}{4} * \frac{1}{4} = \frac{3}{16}$
$P_{RG} = \frac{1}{4} * \frac{3}{4} = \frac{3}{16}$
$P_{RR} = \frac{1}{4} * \frac{1}{4} = \frac{1}{16}$

In onze Bell-test zoeken we de kans op een rode en een groene lamp. De volgorde is daarbij niet van belang. De kans op een rode en groene lamp halen we uit de tabel:

$$P(GR \text{ of } RG) = P(GR) + P(RG) = \frac{3}{16} + \frac{3}{16} = \frac{3}{8}$$

De tabel geldt voor de situatie dat Alice en Bob beiden een elektron in de toestand $|0\rangle_V$ kregen. In dat geval is de kans op ongelijke kleur gelijk aan $\frac{3}{8}$ en dus de kans op gelijke kleur $\frac{5}{8}$. Als ze een elektron in de toestand $|1\rangle_V$ binnenkrijgen komt er een andere tabel maar de kans op ongelijke kleur blijft $\frac{3}{8}$ en die op gelijke kleur blijft ook $\frac{5}{8}$. Dit kun je zelf bewijzen in opgave 2.4.

Kopenhaagse kansen (quantum)

In de Kopenhaagse opvatting mag niet worden aangenomen dat het elektron dat bij Alice arriveert in een bepaalde toestand verkeert. Figuur 2.8 geeft dan ook geen goed beeld van het experiment. De spinrichting ligt immers nog niet vast bij aankomst van het elektron bij het meetapparaat! In plaats daarvan moeten we kijken naar het elektronenpaar. De beide qubits zijn verstengeld zoals dat heet. De toestand van zo'n verstengeld elektronenpaar kan worden beschreven met

$$\frac{1}{\sqrt{2}} |0\rangle_V |0\rangle_V + \frac{1}{\sqrt{2}} |1\rangle_V |1\rangle_V$$

In hoofdstuk 3 komt verstrengeling uitgebreid aan de orde, maar de formule laat zich toch wel “lezen”. Hier staat een superpositie (optelling) van twee mogelijkheden: de eerste mogelijkheid is dat Alice een qubit krijgt in toestand $|0\rangle_V$, en dan heeft Bob automatisch een qubit in toestand $|0\rangle_V$. Als Alice een $|1\rangle_V$ meet, dan heeft Bob ook een $|1\rangle_V$.

Alice maakt de keuze om te meten in de basis A en Bob besluit om in B te meten. Omdat Alice niet in basis V meet maar in basis A moeten de kets $|0\rangle_V$ en $|1\rangle_V$ vervangen worden door de kets $|0\rangle_A$ en $|1\rangle_A$. Dat is een hele klus, maar je bent het al eerder tegengekomen in opdracht 2.3. Voor $|0\rangle_V$ en $|1\rangle_V$ geldt bijvoorbeeld:

$$|0\rangle_V = \cos \alpha |0\rangle_A - \sin \alpha |1\rangle_A$$

$$|1\rangle_V = \sin \alpha |0\rangle_A + \cos \alpha |1\rangle_A$$

Deze vergelijkingen kun je afleiden met behulp van de eenheidscirkel van figuur 2.10. Met deze twee uitdrukkingen voor de basistoestanden kunnen we elke toestand van de verticale basis uitdrukken in basis A. We werken de verstrengelde toestand

$$\Psi = \frac{1}{\sqrt{2}} |0\rangle_V |0\rangle_V + \frac{1}{\sqrt{2}} |1\rangle_V |1\rangle_V$$

om naar basis A. Om het overzicht te houden berekenen we de twee termen apart.

$$|0\rangle_V |0\rangle_V = (\cos \alpha |0\rangle_A - \sin \alpha |1\rangle_A) (\cos \alpha |0\rangle_A - \sin \alpha |1\rangle_A)$$

$$|1\rangle_V |1\rangle_V = (\sin \alpha |0\rangle_A + \cos \alpha |1\rangle_A) (\sin \alpha |0\rangle_A + \cos \alpha |1\rangle_A)$$

$$|0\rangle_V |0\rangle_V = \cos^2 \alpha |0\rangle_A |0\rangle_A + \sin^2 \alpha |1\rangle_A |1\rangle_A - \cos \alpha \sin \alpha |1\rangle_A |0\rangle_A - \cos \alpha \sin \alpha |0\rangle_A |1\rangle_A$$

$$|1\rangle_V |1\rangle_V = \sin^2 \alpha |0\rangle_A |0\rangle_A + \cos^2 \alpha |1\rangle_A |1\rangle_A + \cos \alpha \sin \alpha |1\rangle_A |0\rangle_A + \cos \alpha \sin \alpha |0\rangle_A |1\rangle_A$$

Als je deze termen optelt en gebruikt dat $\sin^2 \alpha + \cos^2 \alpha = 1$ wordt de toestand:

$$\Psi = \frac{1}{\sqrt{2}} |0\rangle_V |0\rangle_V + \frac{1}{\sqrt{2}} |1\rangle_V |1\rangle_V = \frac{1}{\sqrt{2}} |0\rangle_A |0\rangle_A + \frac{1}{\sqrt{2}} |1\rangle_A |1\rangle_A$$

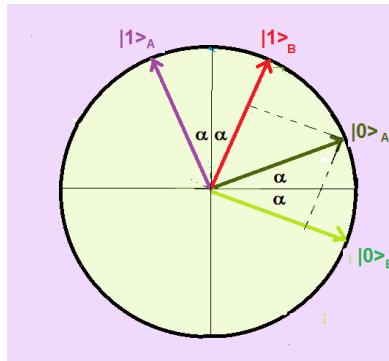
Dat is heel prettig en scheelt een hoop werk! Nu gaat Alice meten en ze zal dus vinden dat de toestand van haar qubit gelijk is aan

$|0\rangle_A$ of $|1\rangle_A$. De kans op elk van die twee gebeurtenissen is $\frac{1}{2}$. Dus de kans hier op een groene lamp is $\frac{1}{2}$. Dat is al het eerste verschil met de opvatting volgens EPR. Daar vond Alice een kans van $\frac{1}{4}$ op rood en $\frac{3}{4}$ op groen!

In ons voorbeeld meet Alice een 1. Bij haar gaat dus de rode lamp branden. Maar haar meting heeft in de Kopenhaagse opvatting grote consequenties voor de toestand van het elektronenpaar: de tweede mogelijkheid in de superpositie verdwijnt.

$$\cancel{\frac{1}{\sqrt{2}}|0\rangle_A|0\rangle_A} + \cancel{\frac{1}{\sqrt{2}}|1\rangle_A|1\rangle_A}$$

Nu één van de twee mogelijkheden is verdwenen blijft de andere over met een kans van één. En Bob heeft nu plotseling een qubit in een toestand $|1\rangle_A$. Volgens de EPR opvatting was zoets nooit mogelijk geweest. Hier heeft een quantum sprong plaatsgevonden! Bob meet in basis B. Hoe groot is nu de kans dat bij hem een groene lamp oplicht? Bekijk het diagrammetje van figuur 2.11. De bases A en B kiezen we iets anders omwille van de duidelijkheid van de tekening. Maar wel krijgen we de basis A weer door over een hoek α linksom te draaien vanaf de verticale basis en de basis B door over een hoek α rechtsom te draaien.



Figuur 2.11: De basisvectoren van basis A en B in één figuur. De basisvectoren $|0\rangle_A$ en $|1\rangle_A$ kunnen worden uitgedrukt in de basisvectoren van basis B.

De basisvectoren van basis A kunnen uitgedrukt worden in basis B:

$$|0\rangle_A = \cos 2\alpha |0\rangle_B + \sin 2\alpha |1\rangle_B$$

$$|1\rangle_A = -\sin 2\alpha |0\rangle_B + \cos 2\alpha |1\rangle_B$$

De kans op een rode lamp bij Bob ($|1\rangle_B$) is dan $\cos^2 2\alpha$. De kans dat bij Bob de groene lamp oplicht ($|0\rangle_B$) is gelijk aan $\sin^2 2\alpha$. We zagen eerder dat bij Alice de kans op een rode lamp gelijk is aan de kans op een groene lamp $P_{rood \ bij \ Alice} = P_{groen \ bij \ Alice} = \frac{1}{2}$. Voor

een hoek $\alpha = 60^\circ$ is de kans op de combinatie van rood bij Alice en groen bij Bob kan nu eenvoudig te berekenen:

Quantumkansen voor Alice en Bob: $P_{AB}, \alpha = 60^\circ$

$$P_{GG} = \frac{1}{2}\cos^2 2\alpha = \frac{1}{8}$$

$$P_{RG} = \frac{1}{2}\cos^2 2\alpha = \frac{1}{8}$$

$$P_{GR} = \frac{1}{2}\sin^2 2\alpha = \frac{3}{8}$$

$$P_{RR} = \frac{1}{2}\sin^2 2\alpha = \frac{3}{8}$$

De tabel omvat alle mogelijke uitkomsten en die tellen op tot 1. De kans dat de beide kleuren oplichten is de som van P_{RG} en P_{GR} . Dus uiteindelijk is de kans op kleurverschil gelijk aan $\frac{1}{8} + \frac{3}{8} = \frac{4}{8} = \frac{1}{2}$! $P(RG) + P(GR)$ is ook voor andere hoeken dan 60° gelijk aan $1/2$. Kijk maar eens naar de tabel en bedenk dat $\sin^2 + \cos^2 = 1$. We hebben het eerst aannemelijk gemaakt met een getallen voorbeeld voor $\alpha = 60^\circ$, we bewezen dat het onafhankelijk is van de hoek waarover we de bases draaien.

Samenvattend: De Kopenhagense theorie en de opvatting volgens EPR voorspellen verschillende uitkomsten bij een experiment zoals dat van figuur 2.8. EPR: kans op kleurverschil is kleiner dan $\frac{1}{2}$ en de kans op gelijke kleuren is groter dan $\frac{1}{2}$. Copenhagen:kans op kleurverschil is $\frac{1}{2}$.

Het Bell-test experiment leverde de beslissende slag en toonde aan dat Einstein ongelijk had.

Het experiment om deze theoriën te testen heet de Bell-test. Dit bleek moeilijk te voeren, maar zou beslissend zijn in de theorie. Het werk van Alain Aspect, Anton Zeilinger en John Clauser toonde aan dat EPR moest worden verworpen. Het leverde hen de Nobelprijs van natuurkunde in 2022 op.

Opdracht 2.4

Bij het experiment van fig. 2.8 ontvangen Alice en Bob elk een elektron met dezelfde oriëntatie. In de vorige paragraaf is voorgerekend dat in de toestand $|1\rangle_V$ de kans op gelijke kleur gelijk is aan $\frac{5}{8}$. Nu onderzoeken we hoe dat zit als beiden een elektron ontvangen in de toestand $|0\rangle_V$. Alice meet in basis A en Bob meet in basis B. Alice en Bob krijgen een elektron met dezelfde verticale oriëntatie maar met 50% kans op een up en 50% kans op een down.

- a. Bereken de klassieke (EPR) kansen in de tabel voor Alice en Bob: $P_{AB}, \alpha = 60^\circ$

$$P_{GG} = \dots$$

$$P_{RG} = \dots$$

$$P_{GR} = \dots$$

$$P_{RR} = \dots$$

Bij de Kopenhaagse interpretatie zijn we er bij het voorbeeld van uitgegaan dat Alice als eerste meet. Bij de volgende berekening gaan Bob als eerste meten.

- b. Stel de tabel weer op maar nu met quantum (Kopenhaagse)kansen:

$$P_{GG} = \dots$$

$$P_{RG} = \dots$$

$$P_{GR} = \dots$$

$$P_{RR} = \dots$$

2.7 DiVincenzo criteria

Om een betrouwbare quantumcomputer te kunnen bouwen, moet de 'hardware', oftewel het materiaal waarvan qubits worden gemaakt, aan een aantal voorwaarden voldoen. David DiVincenzo heeft in het jaar 2000 vijf criteria opgesteld waar de hardware noodzakelijk aan moet voldoen om een quantumcomputer te kunnen bouwen [4]. De criteria zijn de volgende:

Spin is een quantumeigenschap van elektronen. De spintoestand kan in superpositie zijn, maar als je de spin meet kan het alleen 'up' of 'down' opleveren.

Criterium 1 Het klinkt misschien voor de hand liggend, maar een belangrijke randvoorwaarde aan een qubit systeem is dat de toestanden $|0\rangle$ en $|1\rangle$ duidelijk te onderscheiden zijn. Daarnaast moet het qubit natuurlijk in een superpositie van $|0\rangle$ en $|1\rangle$ kunnen zijn. Dit zou bijvoorbeeld een elektron in de spintoestand 'up' of 'down' kunnen zijn, of de polarisatietoestand van een foton. Maar uiteindelijk heb je voor een werkende quantumcomputer natuurlijk veel qubits nodig die met elkaar interacties kunnen aangaan. Daarom is het ook heel belangrijk dat het qubit systeem schaalbaar is en de qubits met elkaar kunnen interacteren.

Criterium 2 Om een berekening te kunnen uitvoeren is het belangrijk dat je aan het begin van de berekening de toestand van al je qubits kent, zodat je vanuit die toestand de quantumpoorten kunt uitvoeren en de berekening kunt doen. Zo'n begintoestand kan bijvoorbeeld de grondtoestand zijn. Dit is de laagste energietoestand waarin het systeem kan verkeren.

Criterium 3 Een toestand waarin een qubit zich bevindt, is vaak niet stabiel. Zo kan een systeem terugvallen naar zijn grondtoestand, of kan een qubit quantuminformatie verliezen door energie uit omgevingswarmte, of door omgevingsruis. We noemen dit *decoherentie*. Om een betrouwbare berekening te kunnen doen, willen we veel quantumbewerkingen kunnen uitvoeren voordat er decoherentie optreedt in het systeem. Daarom willen we lange decoherentietaijden en snelle qubit poorten in ons systeem. Alles is overigens relatief: qubits leven over het algemeen enkele microseconden tot milliseconden. Maar met nog veel snellere qubit poorten (nanoseconden), is dat geen probleem.

Criterium 4 Om alle mogelijke toestanden te kunnen maken en alle mogelijke berekeningen te kunnen uitvoeren met een quantumcomputer, moet er een universele set van quantumpoorten zijn die je met de quantumcomputer kunt uitvoeren. Dit betekent dat er een set met een aantal quantumpoorten is die je op het systeem kunt uitvoeren, waarmee je alle mogelijke toestanden kunt maken en berekeningen kunt doen. Een voorbeeld van zo'n universele set zijn: de Hadamard, de CNOT en de $\pi/8$ -faseflip. De eerste twee behandelen we in hoofdstuk 3. In onze module beperken we ons tot reële getallen. De $\pi/8$ -fase flip brengt ons in de wereld van de complexe getallen en die behandelen we niet. Onze module werkt dus met een incomplete set. We kunnen maar een deel van de mogelijkheden van quantumcomputers laten zien.

Criterium 5 Het systeem moet in staat zijn om na afloop van de berekening de toestand van een qubit te kunnen uitlezen. Bij een meting zal de toestand van het qubit vanuit superpositie vervallen naar een toestand in de meetbasis. Je kunt een superpositie niet als meetuitkomst krijgen. Toch is het heel belangrijk om een qubit uit te kunnen lezen. In de praktijk blijkt dit niet altijd eenvoudig. Hoe kun je meten of een qubit toestand $|0\rangle$ of $|1\rangle$ is?

2.8 Leerdoelen

In dit hoofdstuk heb je het volgende geleerd:

- Een qubit is een elementaire informatiedrager die bij uitlezing één van twee toestanden als uitkomst kan geven. Deze toestanden zullen we $|0\rangle$ of $|1\rangle$ noemen.
- Een toestand kan worden voorgesteld door een vector met lengte één.
- De toestanden $|0\rangle$ en $|1\rangle$ vormen de standaard basis.
- Elke waarnemer hanteert zijn eigen standaard basis, die wordt opgelegd door zijn meetinstrument.
- Het qubit verkeert voorafgaand aan de uitlezing in een toestand $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- Het is heel handig om toestanden van een qubit te visualiseren met de eenheidscirkel.
- De coëfficiënten α en β worden amplitudes genoemd. Ze geven weer wat de *overlap* is van de toestand $|\Psi\rangle$ met de basistoestanden $|0\rangle$ en $|1\rangle$.
- De kans dat uitlezing van toestand $|\Psi\rangle$ de toestand $|0\rangle$ oplevert is gelijk aan α^2 en de kans dat het $|1\rangle$ oplevert is β^2 .
- Voor de coëfficiënten α en β geldt de betrekking: $\alpha^2 + \beta^2 = 1$
- Bij uitlezing is de oorspronkelijke toestand $|\Psi\rangle$ overgegaan in de nieuwe toestand: de meetuitkomst.
- Uitlezing is een *irreversibel* proces. Je kunt het niet ongedaan maken.
- De DiVincenzo criteria zijn ontwerpeisen voor een quantumcomputer.
 - Qubits moeten goed gedefinieerd kunnen worden in een $|0\rangle$ en een $|1\rangle$ toestand en het systeem moet schaalbaar zijn.
 - Qubits moeten in een duidelijke begintoestand kunnen worden gebracht.
 - Berekeningen moeten veel sneller kunnen worden uitgevoerd dan de tijd waarin het systeem onbetrouwbaar wordt.
 - Er moet een universele set van quantumpoorten mogelijk zijn.
 - De output moet gemeten kunnen worden.

3. Operatoren en toestandsveranderingen

In het vorige hoofdstuk zagen we hoe klassieke computers poorten gebruiken om bits te manipuleren. Deze bits kunnen twee toestanden aannemen. We hebben ook gezien hoe qubits in superpositie kunnen verkeren, maar dat een meting een basistoestand oplevert.

In dit hoofdstuk onderzoeken we hoe we met poorten op een quantumcomputer qubits kunnen manipuleren. We onderzoeken eerst poorten die op één enkele qubit werken. We onderzoeken de working van meerdere poorten na elkaar en programmeren een quantumcomputer. We beschrijven daarna een poort die op twee qubits werkt. Hiermee kunnen we qubits *verstrengelen*, een begrip dat we uitgebreid behandelen. We sluiten dit hoofdstuk af met een toepassing waarin we al onze eigenschappen van een quantumcomputer gebruiken: we schrijven een protocol voor het teleporteren van een qubit. Teleporteren is met een klassieke computer niet mogelijk.

De toestand van een qubit kan worden weergegeven als

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Hierin vormen $|0\rangle$ en $|1\rangle$ een set van twee basistoestanden. De twee basisvectoren staan loodrecht op elkaar. Ze hebben geen overlap.

Zoals je de toestand van bits kunt manipuleren met klassieke poorten, zo kun je de toestand van qubits veranderen met quantumpoorten. Zo'n doelbewuste verandering is een operatie. Alle operaties op een quantumcomputer voldoen aan de eis van *lineariteit*.



Lineariteit: Quantumpoorten zijn lineaire operatoren. Dit is een eigenschap waarbij aan twee regels wordt voldaan. Een afbeelding is lineair als

$$\begin{aligned}\mathbf{A}(\lambda x) &= \lambda \mathbf{A}(x) \\ \mathbf{A}(x_1 + x_2) &= \mathbf{A}(x_1) + \mathbf{A}(x_2)\end{aligned}$$

We zien in opgave 3.1 dat dat een heel alledaagse eigenschap is.

Opdracht 3.1

Eigenschap 1: haakjes.

Eerst de algebra: De lijn $y = \mathbf{a}x$ gaat door de oorsprong, en heeft richtingscoëfficiënt \mathbf{a} . Voor twee punten geldt:

$$\begin{aligned}y &= \mathbf{a}(x_1 + x_2) \\ &= \mathbf{a}x_1 + \mathbf{a}x_2\end{aligned}$$

We nemen een voorbeeld met literen en Engelse pints. Als \mathbf{a} het omzetten van literen naar pints voorstelt, x een hoeveelheid in literen en y een hoeveelheid in pints:

Één emmer van elf liter melk levert net zoveel pints als één emmer van vijf liter en één emmer van zes liter melk samen (en omgekeerd).

Eigenschap 2: Schaalbaarheid. Eerst de algebra:

$$\begin{aligned}y &= \mathbf{a}(bx_1) \\ &= b\mathbf{a}x_1\end{aligned}$$

In het voorbeeld: Één pak van vier liter levert net zoveel pints als vier pakken van één liter (en omgekeerd).

- a. Ga met een getallen voorbeeld na dat deze twee regels gelden. (Kies bijvoorbeeld $a = 3, b = 4, x_1 = 5, x_2 = 6$)
- b. Een '='-teken werkt twee kanten op. Formuleer in woorden de omgekeerde weg.

Stel we hebben een poort \mathbf{F} die werkt op de willekeurige toestand $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Dit levert een nieuwe toestand van het qubit, stel $|\Phi\rangle$. Er geldt dus

$$|\Phi\rangle = F |\Psi\rangle$$

We kunnen de twee regels in één keer toepassen op de basisvectoren:

$$F |\Psi\rangle = F(\alpha |0\rangle + \beta |1\rangle) = \alpha F |0\rangle + \beta F |1\rangle$$

Als je weet wat de poort doet met de basistoestanden dan weet je ook wat de poort doet met iedere andere toestand. Daar zullen we veel gebruik van maken.

3.1 Poorten die op één qubit werken

In deze paragraaf beschrijven we enkele operaties (poorten) die op qubits werken. We beschrijven ook de regels waar quantumpoorten aan moeten voldoen. Omdat de operaties *lineair* zijn, is het voldoende om de actie van de poorten op de basisvectoren te beschrijven. We behandelen ook één poort die op twee qubits werkt. Met deze kennis kunnen we vervolgens quantum-algoritmen schrijven.

De I -poort

Met de identiteit houden we het qubit in dezelfde toestand. Het is de simpelste operatie: niets doen. De identiteitspoort lijkt niet zo interessant, maar kan soms erg nuttig zijn. Lees hiernaast maar wat Nobelprijswinnaar Richard Feynman erover zegt.

De actie van de I -poort en alle andere poorten geven we in twee notaties weer. Links de afbeelding van de basisvectoren, en rechts de afbeelding van een willekeurige vector $(\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix})$. Bij de hierna volgende poorten geven we ook een toestandsdiagram. Voor de identiteit is die te simpel.

Figuur 3.1 geeft aan hoe je de poort als bouwblokje in een circuit opneemt. Dit blokje is te lezen als een onderdeel van een tijdlijn. Handig als je meerdere operaties achter elkaar uitvoert. We zullen het bij het programmeren tegenkomen. De I -poort laat de basisvectoren onveranderd. Het zal je niet verbazen dat de I -poort een willekeurige toestand $|\Psi\rangle = (\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix})$ op zichzelf afbeeldt. Voor de volgende poorten werken we dit uitgebreider uit.

Richard Feynman: "And then there's the identity, I , which we always have to put in there to complete our mathematics – it doesn't do a damn thing!"[6, p.476]

$$(\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}) \xrightarrow{I} (\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix})$$

Figuur 3.1: De I -poort doet niks.

De X -poort

Deze poort verwisselt de basisvectoren. Dus $|0\rangle$ wordt $|1\rangle$ en $|1\rangle$ wordt $|0\rangle$. De X -poort wordt ook wel de *bitflip* genoemd.

Wat doet de poort met een willekeurige toestand $|\Psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$? We gebruiken lineariteit om dit op te lossen:

$$\begin{aligned} X(\alpha|0\rangle + \beta|1\rangle) &= \\ X\alpha|0\rangle + X\beta|1\rangle &= \\ \alpha X|0\rangle + \beta X|1\rangle \end{aligned}$$

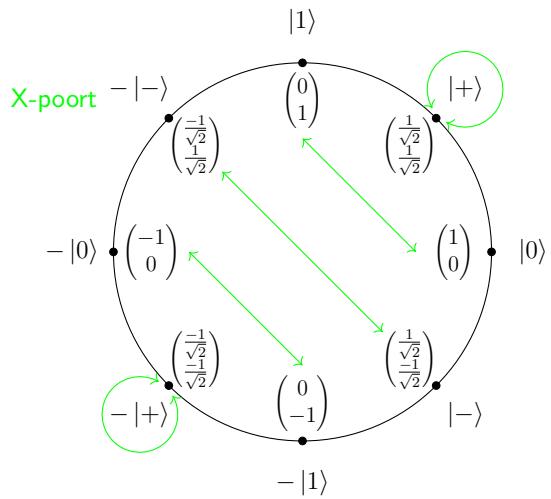
maar we weten dat $X|0\rangle = |1\rangle$ en $X|1\rangle = |0\rangle$. Daarmee wordt de nieuwe toestand (vul maar in):

$$\begin{aligned} \alpha|1\rangle + \beta|0\rangle &= \\ (\alpha \quad -X \quad \beta) \quad - \boxed{X} \quad - \quad (\alpha \quad \beta) &= \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \end{aligned}$$

Figuur 3.2: De X -poort ofwel bit-flip.

In figuur 3.2 staat het bouwblok van de X -poort.

We geven nog een manier om actie van de poorten weer te geven. Soms is het handig om toestandsdiagrammen te gebruiken. Zo'n diagram geeft aan hoe je van de ene toestand in de andere komt. In figuur 3.3 is een diagram voor de X -poort afgebeeld. Kun je in het diagram aangeven wat er met een willekeurige toestand gebeurt als de X -poort er op werkt? In quantumcomputing kan de werking van een poort altijd ongedaan gemaakt worden. De oorspronkelijke toestand kun je dus herstellen. Dit noemen we reversibel. Is dat hier het geval?

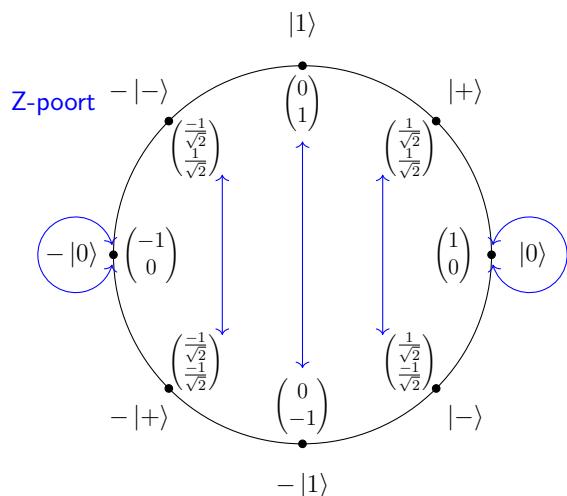


Figuur 3.3:
Toestandsdiagram voor **X-poort**.

De **Z-poort**

Deze poort laat de toestand $|0\rangle$ altijd onveranderd en wisselt de amplitude van toestand $|1\rangle$ van teken. Dus $Z(\begin{smallmatrix} \alpha & \\ \beta & \end{smallmatrix}) = (\begin{smallmatrix} \alpha & \\ -\beta & \end{smallmatrix})$. In figuur 3.4 staat de poort weergegeven. In figuur 3.5 vind je het toestandsdiagram.

In het toestandsdiagram van figuur 3.5 staan de overgangen van de **Z-poort** grafisch weergegeven.



Figuur 3.5:
Toestandsdiagram voor de **Z-poort**.

$$\left(\begin{smallmatrix} \alpha & \\ \beta & \end{smallmatrix} \right) \xrightarrow{\text{Z}} \left(\begin{smallmatrix} \alpha & \\ -\beta & \end{smallmatrix} \right)$$

Figuur 3.4: De **Z-poort**.

Opdracht 3.2

Oefen met lineariteit door stap voor stap de werking van de Z -poort op te schrijven zoals we dat ook bij de X -poort hebben gedaan. $Z\left(\begin{array}{c} \alpha \\ \beta \end{array}\right) = \dots = \left(\begin{array}{c} \alpha \\ -\beta \end{array}\right)$.

De Hadamard-poort

We gebruiken weer de regels voor lineariteit om de afbeelding $H\left(\begin{array}{c} \alpha \\ \beta \end{array}\right)$ van een willekeurige vector te berekenen.

$$\left(\begin{array}{c} \alpha \\ \beta \end{array}\right) \xrightarrow{H} \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix}$$

Figuur 3.6: De H -poort.

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

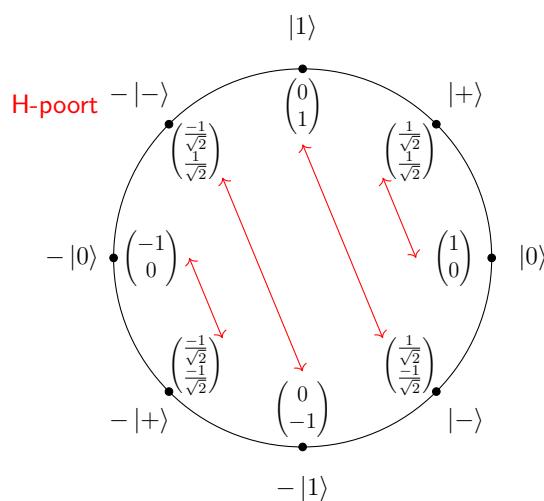
$$H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$$H\left(\begin{array}{c} \alpha \\ \beta \end{array}\right) = H(\alpha|0\rangle + \beta|1\rangle) = \alpha H|0\rangle + \beta H|1\rangle$$

We kennen de werking van H op de standaardbasis. Daarmee wordt de nieuwe toestand:

$$\begin{aligned} \frac{\alpha}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{\beta}{\sqrt{2}}(|0\rangle - |1\rangle) = \\ \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle \end{aligned}$$

Ook voor een Hadamard gate kun je een toestandsdiagram maken (figuur 3.7).



Figuur 3.7: Toestandsdiagram voor de H -poort.

Een voorbeeld: Wat doet de H-poort met een qubit in de toestand $|\Psi\rangle = \frac{2}{\sqrt{5}}|0\rangle + \frac{1}{\sqrt{5}}|1\rangle$? We passen de eigenschappen van lineariteit toe.

$$\begin{aligned}\mathbf{H}\Psi &= \mathbf{H} \left(\frac{2}{\sqrt{5}}|0\rangle + \frac{1}{\sqrt{5}}|1\rangle \right) \\ &= \frac{2}{\sqrt{5}}\mathbf{H}|0\rangle + \frac{1}{\sqrt{5}}\mathbf{H}|1\rangle \\ &= \frac{2}{\sqrt{5}}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{5}}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{2}{\sqrt{10}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{10}}(|0\rangle - |1\rangle) \\ &= \frac{3}{\sqrt{10}}|0\rangle + \frac{1}{\sqrt{10}}|1\rangle\end{aligned}$$

Ga na dat de lengte van $|\Psi\rangle$ ($=\|\Psi\|$) voor en na de operatie gelijk blijft ($= 1$).

Opdracht 3.3

Een qubit bevindt zich in toestand $|\Psi\rangle = \frac{1}{2} \begin{pmatrix} 1 \\ \sqrt{3} \end{pmatrix}$.

- a. Teken de eenheidscirkel en teken de bovengenoemde toestand in op de cirkel.
- b. Hoe groot is de hoek tussen de vectoren van de toestand $|\Psi\rangle$ en de toestand $|0\rangle$?
- c. Bereken de toestand $H|\Psi\rangle$.
- d. Hoe lang is deze vector?

De Hadamard-poort (**H**-poort) transformeert de standaard basis van en naar de diagonale basis (zie figuur 3.6). De basisvectoren van de diagonale basis geven we ook wel weer met $|+\rangle$ en $|-\rangle$:

$$\begin{aligned}|+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\end{aligned}$$

Opdracht 3.4

In de tekst staat hoe de basisvectoren van de diagonale basis uitgedrukt worden in de basisvectoren van de standaardbasis.

- a. Druk de basisvectoren van de standaard basis uit in $|+\rangle$ en $|-\rangle$. Dus:

$$|0\rangle = \dots$$

$$|1\rangle = \dots$$

- b. Bereken $H |+\rangle$.

Meerdere poorten

Op de nieuwe toestand kun je weer een poort laten werken. Bijvoorbeeld $ZH |\Psi\rangle$. De haakjes worden daarbij weggelaten. Let op, deze algebraïsche notatie ontwikkelt van rechts naar links. Eerst bereken je de H -poort op $|\Psi\rangle$, daarna de Z -poort op het resultaat. We kunnen de poorten ook in een tijdlijn weergeven. Je plaatst dan de poorten achter elkaar van links naar rechts. We bouwen zo een quantumcircuit op.

wiskundig:

niet commutatief:

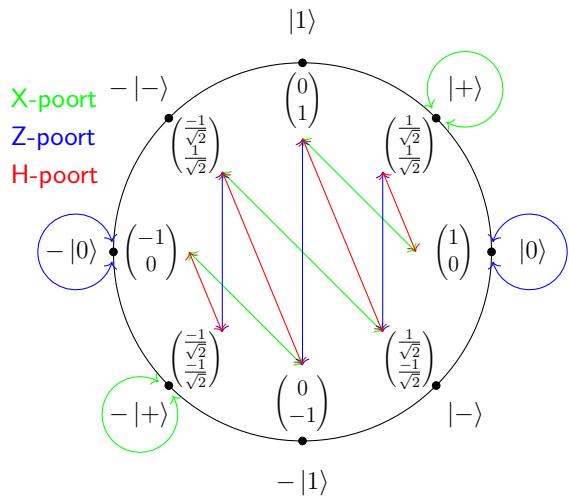
$$AB |\Psi\rangle \neq BA |\Psi\rangle$$

wel associatief

$$A(B |\Psi\rangle) = (AB) |\Psi\rangle$$

$$ZH |\Psi\rangle \quad \equiv \quad |\Psi\rangle - [H] - [Z] -$$

Toestandsdiagrammen geven een derde manier om zo'n combinatie door te rekenen. Met een aantal keer zigzaggen kom je op het antwoord. In figuur 3.8 staan de overgangen van de X -, Z - en H -poort weergegeven.



Figuur 3.8:
Toestandsovergangen voor X -, Z -, en H -poorten in een figuur.

Rekenvoorbeeld

Bereken $|\Psi\rangle = XHZX|0\rangle$.

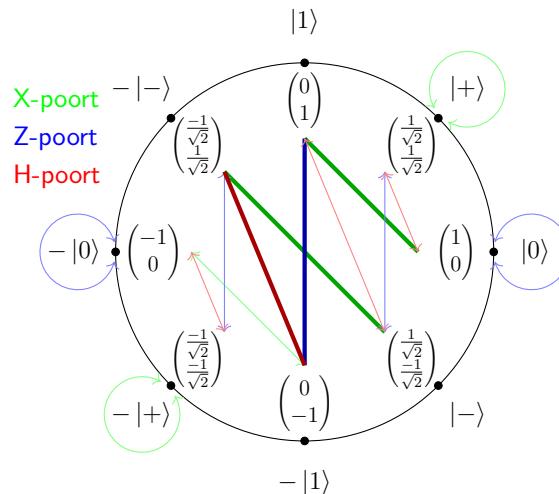
Omgezet naar een tijdlijn (register) lezen we van links naar rechts:

$$|0\rangle \xrightarrow{[X]} \xrightarrow{[Z]} \xrightarrow{[H]} \xrightarrow{[X]} |\Psi\rangle$$

De X eerst evalueren, dan de rest afknabbelen. Telkens passen we de rekenregels van lineariteit toe:

$$\begin{aligned}
 XHZX|0\rangle &= XHZ|1\rangle \\
 &= XH(-|1\rangle) \\
 &= -XH|1\rangle \\
 &= -X\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \\
 &= -\frac{1}{\sqrt{2}}X(|0\rangle - |1\rangle) \\
 &= -\frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) \\
 &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
 |\Psi\rangle &= |- \rangle
 \end{aligned}$$

Een antwoord vinden we snel met een toestandsdiagram (figuur 3.9).



Figuur 3.9: Als je wilt weten wat de uitkomst is van $XHZX|0\rangle$ kun je met de eenheidscirkel snel afleiden dat dat de toestand $|-\rangle$ moet zijn. Bij uitlezing heb je dan 50% kans op een 0 en 50% kans op een 1 als uitkomst.

We hebben nu voldoende kennis om op een echte quantumcomputer te werken.

Quantum Inspire

Voer het werkblad Werken op een quantumcomputer [5.6](#) uit

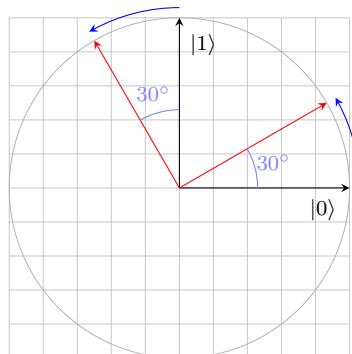
Kop of munt

Speel het spel Kop of munt (instructies krijg je van je docent)

De toestandsdiagrammen van de **X**-, **Z**-, en **H**-poort zijn in onze eenheidscirkel spiegelingen. Zij laten de lengte onveranderd.

De R_y -poort

In figuur 3.10 wordt een voorbeeld weergegeven waarbij wordt gedraaid over een hoek van 30° .



Figuur 3.10: Werking van de rotatieoperator $R_y 30$. Alle vectoren worden gedraaid over een hoek van 30° .

Voor toestandsveranderingen van qubits moet gelden dat lengtes en hoeken niet veranderen. Als twee vectoren loodrecht op elkaar staan dan doen hun beelden dat ook. Zowel spiegelingen als rotaties voldoen aan deze eis.

De rotatiepoort wordt R_y -poort genoemd. We nemen als voorbeeld de werking van de $R_y 30$ -poort op de toestand $|0\rangle$ en de toestand $|1\rangle$. Eenvoudige regels voor vectoren toepassen geeft de nieuwe toestanden die in figuur 3.10 in rood zijn getekend.

Er bestaan ook R_x en R_z -poorten maar hun werking valt buiten het vlak van de eenheidscirkel. Zij introduceren complexe getallen.

$$\begin{aligned} R_y 30 |0\rangle &= \frac{1}{2}\sqrt{3}|0\rangle + \frac{1}{2}|1\rangle \\ R_y 30 |1\rangle &= -\frac{1}{2}|0\rangle + \frac{1}{2}\sqrt{3}|1\rangle \end{aligned}$$

Opdracht 3.5

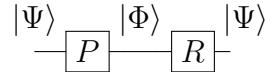
Anders dan bij spiegelingen geldt hier *niet* dat bij twee keer toepassen de oorspronkelijke toestand ontstaat. We kunnen dit voorbeeld doen voor de toestand $|0\rangle$.

- a. Bereken $R_y 30 (R_y 30(|0\rangle))$

Reversibiliteit

Quantumpoorten moeten reversibel zijn. Dat betekent dat de werking van een poort P ongedaan moet kunnen worden gemaakt door een andere poort, R . In het schema van figuur 3.11:

Blijkbaar geldt $PR|\Psi\rangle = |\Psi\rangle$. De PR operatie is dus gelijk aan de identiteit. In zo'n geval wordt R dan de inverse van P genoemd. De vier behandelde poorten I , X , Z en H moeten zo'n inverse hebben. Het blijkt dat deze poorten hun eigen inverse zijn. Twee keer toepassen levert de originele toestand op. Voor I , X en Z is dat onmiddellijk duidelijk. Voor de H -poort heb je dat zelf al afgeleid in opdracht 3.4. De R_y -poort is niet zelfreversibel, maar het is niet moeilijk in te zien hoe de inverse van de R_y -poort er uit ziet. Een R_y -poort is een rotatie. Dus je moet gewoon terug draaien. Zo is de inverse van $R_y 30$ de R_y^{-30} .



Figuur 3.11: De R -poort moet de P -poort ongedaan maken.

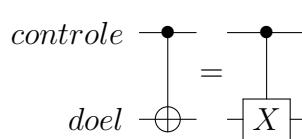
De CNOT-poort

CNOT conditional not
(speak uit si-not)

De **X**-, **Z**- en **H**-poort werken op één qubit. Er zijn ook poorten die op meerdere qubits tegelijkertijd werken. De **CNOT**-poort is de simpelste poort waarmee we qubits kunnen verstrengelen. Verstrengeling is misschien wel de meest bijzondere eigenschaap die een quantumcomputer onderscheidt van een klassieke computer. We zijn het begrip verstrengeling tegengekomen in [2.6](#) en komen het weer tegen aan het einde van deze paragraaf.

De **CNOT**-poort is een conditionele **X**-poort. Eén van de qubits werkt als controle-qubit. Dit geef je aan met een dicht bolletje (\bullet). Het andere qubit (doel-qubit)flipoft als het controle-qubit in de toestand $|1\rangle$ is. Als het control-bit in de toestand $|0\rangle$ is gebeurt er niets. Het doel-qubit (\oplus) werkt als een **X**-poort als het controle-qubit in de toestand $|1\rangle$ is en werkt als identiteit als op de controle een $|0\rangle$ staat. Het schema van de **CNOT**-poort is in figuur [3.12](#) te zien. In de ket-notatie schrijven we het bovenste register meest links: $|Controle, Doel\rangle$.

input $ CD\rangle$	output $ CD\rangle$
$ 00\rangle$	$ 00\rangle$
$ 01\rangle$	$ 01\rangle$
$ 10\rangle$	$ 11\rangle$
$ 11\rangle$	$ 10\rangle$



Figuur 3.12: De **CNOT**-poort. Het register met het zwarte bolletje (\bullet) is de controle. Het doel wordt weergegeven met een \oplus of met een **X**-poort.



Figuur 3.13: Het icoon voor een meting.

De meting

Een quantumcircuit eindigt met een meting. De meting is een heikel punt in de quantummechanica. De verschillende interpretaties van de quantummechanica geven een andere uitleg van wat er tijdens en na de meting gebeurt. Net als in sectie [2.5](#) houden we de Kopenhaagse interpretatie aan. Volgens deze interpretatie treedt je na een meting uit de quantumwereld. Daarbij reduceert de quantumtoestand tot een reëel getal. In een circuit is het icoon voor een meting een metertje met een wijzer (zie fig. [3.13](#)).

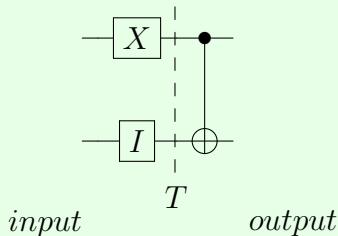
Opdracht 3.6

We onderzoeken de werking van het circuit hieronder voor alle mogelijke combinaties van basisvectoren. Het circuit bestaat uit twee delen. Eerst wordt elk register door een poort gevoerd.

- a. Bereken de tussenstand in T voor de vier mogelijke inputs.

Vervolgens voeren we een **CNOT**-operatie uit.

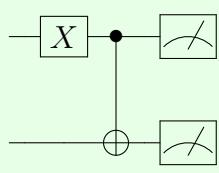
- b. Gebruik je antwoord uit T om de tabel verder in te vullen.



input	T	output
$ 00\rangle$		
$ 01\rangle$		
$ 10\rangle$		
$ 11\rangle$		

Opdracht 3.7

Bekijk onderstaand circuit.



input	output
	$ 00\rangle$
	$ 01\rangle$
	$ 10\rangle$
	$ 11\rangle$

- a. Welke input levert als resultaat $|00\rangle$?
 - b. Bereken ook de input voor de drie andere combinaties in de tabel.

De CNOT-poort en superpositie

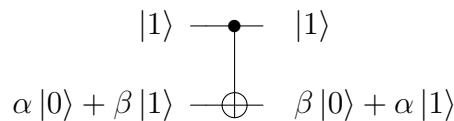
In plaats van basistoestanden ($|0\rangle$ of $|1\rangle$) zoals hierboven kunnen we ook superposities aan de **CNOT** aanbieden. We zetten eerst een superpositie $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ op het doel-qubit. Dus wat is de uitkomst van:

$$\begin{aligned}\mathbf{CNOT}(|1\Psi\rangle) = \\ \mathbf{CNOT}(|1\rangle, \alpha|0\rangle + \beta|1\rangle)\end{aligned}$$

Het controlebit is $|1\rangle$ dus wordt het doel geflipped. We gebruiken weer de twee eigenschappen van lineaire operatoren:

$$\begin{aligned}\mathbf{CNOT}(|1\rangle, \alpha|0\rangle + \beta|1\rangle) = \\ \mathbf{CNOT}(|1\rangle, \alpha|0\rangle) + \mathbf{CNOT}(|1\rangle, \beta|1\rangle) = \\ \alpha\mathbf{CNOT}(|1\rangle|0\rangle) + \beta\mathbf{CNOT}(|1\rangle|1\rangle) = \\ \beta|10\rangle + \alpha|11\rangle\end{aligned}$$

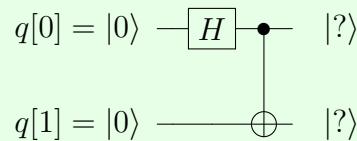
In het eerste register vinden we nog steeds de controle $|1\rangle$. Het tweede register geeft een superpositie maar met een omkering van de coëfficiënten. Als je wilt weten wat de **CNOT** doet met een superpositie hoef je dus alleen maar te weten wat de **CNOT** doet met de basistoestanden. En dat is vastgelegd in figuur 3.12.



Als we een superpositie op het controlebit aanbieden is het resultaat verrassend. We ontdekken dat in opdracht 3.8.

Opdracht 3.8

Alice wil weten wat er gebeurt als je een **H**-poort en een **CNOT**-poort combineert. Ze maakt het volgende circuit:



Zij heeft twee qubits in toestand $|0\rangle$. Ze noteert de begin-toestand $|00\rangle$. Zij voert een **H**-poort op haar eerste bit ($q[0]$) uit.

- a. Schrijf de toestand die Alice nu heeft als lineaire combinatie van $|00\rangle, |01\rangle, |10\rangle$ en $|11\rangle$.

Daarna voert ze een **CNOT**-poort uit met $q[0]$ als controle en $q[1]$ als doel.

- b. Schrijf de toestand die Alice nu heeft als lineaire combinatie van $|00\rangle, |01\rangle, |10\rangle$ en $|11\rangle$.
 c. Kun je de toestanden nog schrijven als aparte qubit toestanden?

De toestand die Alice heeft gemaakt, wordt een Bell-toestand genoemd. Er zijn vier Bell-toestanden:

- I. $\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$
- II. $\frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)$
- III. $\frac{1}{\sqrt{2}} (|01\rangle + |10\rangle)$
- IV. $\frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$

- d. Geef aan welke Bell-toestand Alice heeft gemaakt.
 e. Met welke begintoestanden kun je de andere Bell-toestanden creëren?

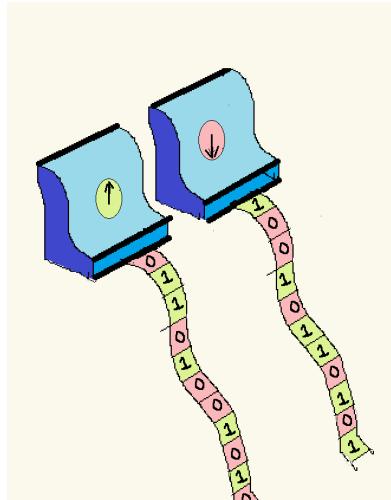
In opgave 3.8 heb je ontdekt dat je de toestand $\alpha |01\rangle + \beta |10\rangle$ niet kunt ontbinden in de toestanden van de twee qubits apart (tenzij $\alpha = 0$ of $\beta = 0$). Maar hoe zit dat dan? Met een controle-qubit in de toestand $|1\rangle$ óf $|0\rangle$ is duidelijk wat de output is. Maar wat als het controle-qubit in een toestand $|1\rangle$ én $|0\rangle$ zit? We krijgen het antwoord door de werking van de **CNOT** (zie fig. 3.12) en de eigenschappen van lineariteit toe te passen:

$$\begin{aligned}\mathbf{CNOT}(\alpha |0\rangle + \beta |1\rangle, |1\rangle) &= \\ \alpha \mathbf{CNOT} |01\rangle + \beta \mathbf{CNOT} |11\rangle &= \\ \alpha |01\rangle + \beta |10\rangle\end{aligned}$$

Elk bit wordt uitgelezen door zijn eigen meetapparaat. Maar wat lezen de meetinstrumenten nu uit? We lezen met kans α^2 de toestand $|01\rangle$ uit, en met kans β^2 lezen we $|10\rangle$ uit. Andere mogelijkheden zijn er niet. Als één van de twee meetapparaten een 0 als output geeft, geeft de andere een 1 en omgekeerd. Het experiment moet vele malen worden herhaald om de amplitudes α en β te kunnen bepalen. In figuur 3.14 staat het uitgebeeld. De rechter geeft de uitlezing van de lijn van het controle-qubit en de linker zit op de onderste lijn, die van het doelqubit. Als je bij het controle-qubit

een toestand $|1\rangle$ uitleest, lees je bij het doelqubit toestand $|0\rangle$ uit. De beide qubits zijn niet onafhankelijk meer maar zijn verstrend.

NB. Met dit experiment kun je de absolute waarden van α en β benaderen, maar niet hun tekens.



Figuur 3.14: Resultaat van de uitlezing van een register in een Bell-toestand.

3.2 Werken met een register

In paragraaf 3.1 ben je de **CNOT**-poort tegengekomen die werkt op twee qubits. Bij twee of meer qubits spreek je van een register. Eén qubit heeft twee basistoestanden $|0\rangle$ en $|1\rangle$. Bij een register met twee qubits zijn er dan vier mogelijke combinaties van de basisstoestanden: $|00\rangle$, $|01\rangle$, $|10\rangle$ en $|11\rangle$. In de vorige paragraaf zijn we ze al tegengekomen. Om de toestanden van een register te bepalen aan de hand van de toestanden van de afzonderlijke qubits maken we gebruik van wat het tensorproduct wordt genoemd. Stel je hebt twee qubits in een toestand van superpositie:

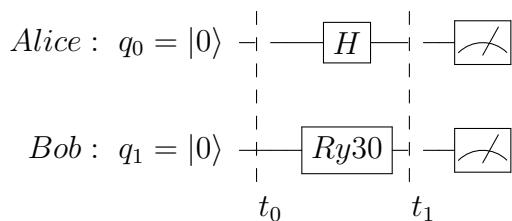
$$\begin{aligned} |\Psi\rangle &= \alpha|0\rangle + \beta|1\rangle \\ |\Phi\rangle &= \gamma|0\rangle + \delta|1\rangle \end{aligned}$$

Voor het tensorproduct \otimes geldt dan:

$$\begin{aligned}
 |\Psi\rangle \otimes |\Phi\rangle &= \\
 &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) \\
 &= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle
 \end{aligned}$$

papegaaienbekken:
 $(a+b)(c+d) =$

Om meer zicht te krijgen op het werken met een register kijken we naar het volgende circuit.

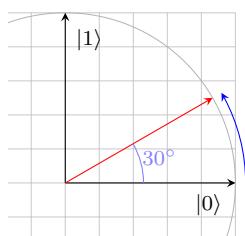


Figuur 3.15: Het tweetal qubits ondergaat een verandering en wordt daarna uitgelezen.

Wat kunnen we bij uitlezing verwachten?

Op t_0 bevindt het register zich in een toestand $|0\rangle \otimes |0\rangle$. We geven dat ook wel weer als $|0\rangle|0\rangle$ of kortweg $|00\rangle$. Let er op: de eerste toestand in dit rijtje heeft betrekking op de bovenste in de figuur. De volgorde is dus van belang! Tussen t_0 en t_1 vindt er een bewerking van de qubits plaats. Op het eerste qubit werkt een Hadamard poort. De toestand van dat qubit wordt nu $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

Bij het tweede wordt de toestandsvector over 30° geroteerd. In figuur 3.16 is dat weergegeven. De toestand van dit qubit wordt nu $\frac{1}{2}\sqrt{3}|0\rangle + \frac{1}{2}|1\rangle$



Figuur 3.16: Rotatie van een toestandsvector over 30° .

Op t_1 heeft het register dan de volgende toestand :

$$\left(\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \right) \otimes \left(\frac{1}{2}\sqrt{3}|0\rangle + \frac{1}{2}|1\rangle \right) = \\ \frac{1}{\sqrt{2}} \frac{\sqrt{3}}{2} |00\rangle + \frac{1}{\sqrt{2}} \frac{1}{2} |01\rangle + \frac{1}{\sqrt{2}} \frac{\sqrt{3}}{2} |10\rangle + \frac{1}{\sqrt{2}} \frac{1}{2} |11\rangle = \\ \sqrt{\frac{3}{8}} |00\rangle + \sqrt{\frac{1}{8}} |01\rangle + \sqrt{\frac{3}{8}} |10\rangle + \sqrt{\frac{1}{8}} |11\rangle$$

Dit is dus de toestand van het register op t_1 .

Stel dat het eerste qubit wordt uitgelezen door Alice en het tweede door Bob. Stel dat bij uitslag '0' een groene lamp gaat branden en bij uitslag '1' een rode lamp. Dan is de kans op groen bij Alice en Bob dus $\frac{3}{8}$! En de kans dat bij beide de rode lamp gaan branden is dan $\frac{1}{8}$!

Opdracht 3.9

Het hele experiment van 3.15 kan worden herhaald, maar nu wordt het circuit uitgebreid met een **CNOT**-poort die na het tijdstip t_1 wordt toegepast. Daardoor bevindt het register zich op tijdstip t_2 in een nieuwe toestand.

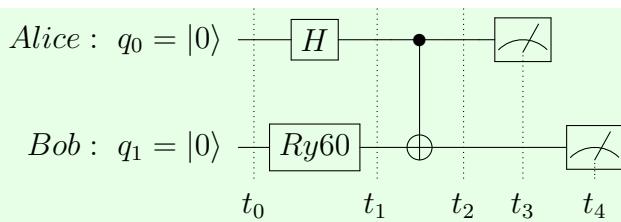
- a. Teken het nieuwe circuit.
- b. Bepaal de toestand van het register op t_2 .

Er wordt uitgelezen door Alice en Bob. Bij een '0' brandt een groene lamp. Bij een '1' brandt een rode lamp.

- c. Bereken de kans dat er twee verschillende kleuren te zien zijn.

Opdracht 3.10

In het volgende circuit:



hebben Alice en Bob op t_0 elk een qubit in toestand $|0\rangle$. Op t_1 hebben zij hun qubits bewerkt met respectievelijk een **H**- en een **Ry60**-poort. Vervolgens verstrekken zij hun bits met een **CNOT**-poort.

Op t_2 scheiden zich hun wegen. Ze nemen elk hun qubit mee.

- a. Laat zien dat op t_1 hun toestand gelijk is aan

$$\sqrt{\frac{1}{8}}|00\rangle + \sqrt{\frac{3}{8}}|01\rangle + \sqrt{\frac{1}{8}}|10\rangle + \sqrt{\frac{3}{8}}|11\rangle$$

- b. Bereken de toestand op t_2 .
- c. Op t_3 leest Alice haar qubit uit en meet een 0. Hoe ziet het register er uit op t_3 ?
- d. Bob leest zijn qubit uit. Hoe groot is de kans dat hij een 0 meet?
- e. Maak een kansentabel voor het geval dat Alice als eerste uitleest.
- f. Bob is Alice te snel af en leest als eerste uit. Beantwoord voor dat geval vragen c., d. en e..

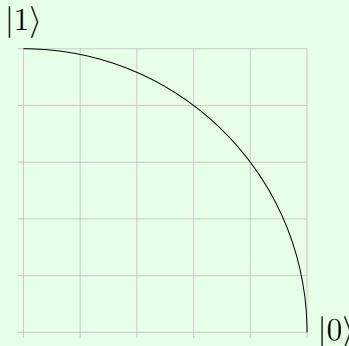
	B_0	B_1
A_0		
A_1		

Opdracht 3.11

Bob heeft de stand van de **Ry**-poort niet goed opgeschreven. Het circuit wordt nog een flink aantal keer gerund op de quantumcomputer van Quantum Inspire en geeft de volgende uitslag:



Figuur 3.17: Het resultaat van 1024 runs op Quantum Inspire van het schema uit opgave 3.10.



- Noteer je resultaten in een kruistabel en bepaal hiermee de amplitudes α en β (Ga uit van positieve oplossingen).
- Teken de toestandsvector q_1 in de figuur zoals hiernaast.
- Bepaal de hoek van q_1 met de x-as.

Quantum Inspire gebruikt een ander coördinatenstelsel. Om daar te testen moet je de hoek die je vond onder **c.** met 2 vermenigvuldigen.

- Welke **Ry**-poort wordt er gebruikt?
- Controleer je antwoord bij **c.** met behulp van de quantumcomputer in Delft.

Opdracht 3.12

Het is niet mogelijk een qubit te kopiëren. Dit staat bekend als het 'no-cloning theorema'. We geven een bewijs uit het ongerijmde. In zo'n bewijs ga je eerst uit van de juistheid van een stelling, totdat dit tot een tegenspraak leidt. Je moet dan concluderen dat de stelling ongeldig is.

We zetten de twee qubits in één ket. De **U**-poort zou het linker qubit kopiëren en de waarde in het rechter qubit opslaan.

$$\mathbf{U}|00\rangle = |00\rangle \quad \text{en} \quad \mathbf{U}|10\rangle = |11\rangle$$

We stellen de operatie op die een toestand $|\Psi\rangle$ kopieert. De twee operaties mogen we samenvoegen (in superpositie brennen). We passen daarbij de regels van lineariteit toe (zie **3**):

$$\begin{aligned}\mathbf{U}\Psi &= \mathbf{U}\left(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right) = \\ &\frac{1}{\sqrt{2}}(\mathbf{U}|00\rangle + \mathbf{U}|10\rangle) = \\ &\frac{1}{\sqrt{2}}((|00\rangle + |11\rangle)\end{aligned}$$

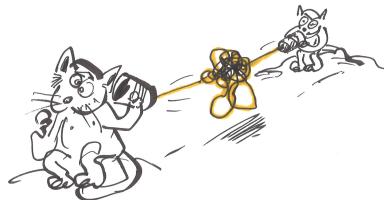
Je moet tot hetzelfde resultaat komen als je $|0\rangle$ in de begin-toestand buiten haakjes haalt, en **U** vervolgens het eerste deel (Ψ) kopieert op de plek van $|0\rangle$:

$$\begin{aligned} \mathbf{U}\left(\frac{|00\rangle + |10\rangle}{\sqrt{2}}\right) &= \mathbf{U}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}|0\rangle\right) = \\ \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ &\neq \frac{1}{\sqrt{2}}((|00\rangle + |11\rangle)) \end{aligned}$$

- a. Geef het no-cloning bewijs met $|1\rangle$ in plaats van $|0\rangle$ 'opslag'-qubit.
- b. Waarom geldt het no-cloning theorema voor een willekeurige toestand $|\Psi\rangle$?

3.3 Quantum protocollen

We hebben nu alle eigenschappen ontdekt die een quantumcomputer speciaal maken. We hebben het nog niet toegepast. In de opdrachten van het tweede deel van de cursus kun je deze toepassingen verder onderzoeken. Met onze kennis kunnen we als voorbeeld eerst het teleportatieprotocol helemaal doorrekenen.



Teleportatie: een quantumprotocol

Teleportatie

Voer werkblad Teleportatie uit ([5.7](#)).

Het teleportatie-protocol is een van de eenvoudigste algoritmen van een quantumcomputer. We hebben er mee aangetoond dat een quantumcomputer iets kan dat een klassieke computer niet kan: de toestand van een qubit teleporeren. Misschien is dit flauw, een klassieke computer heeft nu eenmaal geen qubits. Toch is het een wonder. Aanvankelijk delen Alice en Bob verstrelende qubits in de vorm van een Bell-toestand (zie opg. [3.8](#)), iedere ket met amplitude $\frac{1}{\sqrt{2}}$. Dit worden ook wel EPR paren genoemd. Het te teleporteren

qubit $\Psi = \alpha |0\rangle + \beta |1\rangle$ heeft (mogelijk complexe) amplitudes α en β die in principe onbegrensd nauwkeurig kunnen zijn. Dit qubit wordt in al zijn precisie geteleporteerd terwijl er via klassieke de kanalen maar twee klassieke bits gecommuniceerd zijn. Als het mogelijk zou zijn om EPR paren langere tijd in een koelkast te bewaren en te vervoeren, zou dit een mogelijkheid opleveren voor Alice en Bob om met klassieke bits quantuminformatie over te dragen.

3.4 Terugblik en vooruitblik

Deze eerste drie hoofdstukken hebben we gebruikt om uit te leggen dat een quantumcomputer wezenlijk anders is dan een klassieke computer.

We startten met een combinatie van het splettenexperiment van Young en polarisatie in hoofdstuk 1. We maakten kennis met drie van de vier bouwstenen van een quantumcomputer: *superpositie*, *interferentie* en de *meting*. We zagen dat de uitkomst van een meting door een onderliggend kansproces werd bepaald, en dat een groot aantal herhalingen van een experiment dit kansproces zichtbaar maakte. In hoofdstuk 2 keken we eerst naar klassieke bits en gingen we op zoek naar qubits. We maakten de stap naar de wiskunde met de metafoor 'oudervrouw/jongevrouw'. Een quantumcomputer rekent in amplitudes, maar geeft het antwoord met een bepaalde kans. Het hoofdstuk sluit af met de ontwerpeisen van een quantumcomputer. In hoofdstuk 3 bouwden we de quantumcomputer verder op. We beschreven enkele quantumpoorten en we maakten kennis met de laatste en meest bijzondere eigenschap: *verstrengeling*. We bespraken een algoritme dat zeker niet op een klassieke computer kan worden uitgevoerd: teleportatie. Geven de investeerders daar nu hun miljarden voor uit? Nee, het teleportatie protocol is een *proof of principle*. Misschien neem je hiermee genoeg en accepteer je dat er nog wel andere problemen op te lossen zijn. Je kunt dan verder gaan met de opdracht Quantum en maatschappij 4.4. Een encryptiemodel vind je in de opdracht BB84 4.1. In de opdrachten Deutsch-Josza 4.3 en superdense coding 4.3 ontdek je andere toepassingen van simpele algoritmen.

We hebben lang niet alle aspecten van quantumcomputing kunnen behandelen. Vele toepassingen zoals quantumsimulatie, optimali-

sering zoekstrategiën, quantuminternet en quantumsensoren zijn wellicht mooie onderwerpen voor je profielwerkstuk.

3.5 Leerdoelen

In dit hoofdstuk heb je het volgende geleerd:

- Qubits kunnen worden geprepareerd. Dat wil zeggen je kunt dezelfde qubit telkens weer in eenzelfde gewenste toestand brengen.
- De geprepareerde toestand kan worden bewerkt met poorten die zorgen voor een welbepaalde overgang naar een andere toestand.
- Als je weet wat een poort met de twee basistoestanden doet, dan weet je wat de poort doet met elke willekeurige toestand.
- De werking van de **I**-, **X**-, **Z**-, **H**, en **Ry**-poort op een willekeurige toestand kan worden uitgelegd door te laten zien wat deze poorten doen met de toestanden $|0\rangle$ en $|1\rangle$.
- Met een toestandsdiagram kun je de werking van poorten op enkele qubits weergeven.
- Clonen van qubits is niet mogelijk.
- Uitlezen van de toestand van een qubit is alleen zinnig als je de uitlezing vaak kunt herhalen en je dus statistiek kunt bedrijven.
- Uitlezen is irreversibel. De toestand van het qubit verandert daardoor en de uitlezing kan niet ongedaan worden gemaakt.
- De werking van de **Ry**-poort kan worden geïllustreerd met behulp van de eenheidscirkel.
- Werken met de quantumcomputer.
- Een quantumregister beschrijft het verloop van qubits in de tijd.
- Je kunt het tensorproduct, \otimes , berekenen van twee qubittoestanden.
- Uitlezing van een systeem met N qubits levert een verdeling op over 2^N mogelijke toestanden.
- De werking van de CNOT-poort is uitgelegd door te laten zien wat de CNOT-poort doet met de vier basistoestanden: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.
- Bij verstrekking is ontbinding in basistoestanden niet mogelijk.

- Het teleportatieprotocol kan de toestand van een qubit teleporteren door twee klassieke bits te communiceren.
- Informatie-overdracht gaat niet sneller dan het licht.

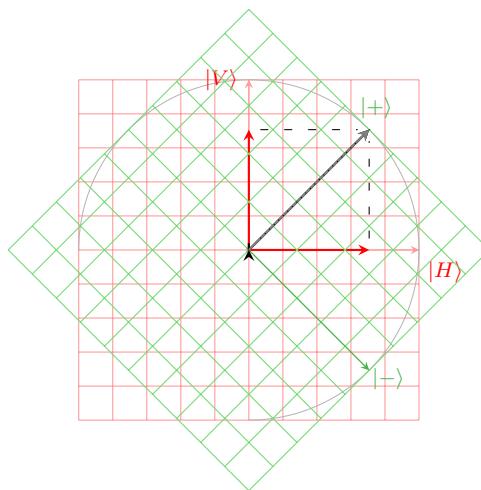
4. Praktische opdrachten

De kennis van de vorige hoofdstukken kunnen we nu toepassen. Net als in het theoriegedeelte beperken we ons in dit hoofdstuk tot gebruik van reële getallen. Alleen in de wiskunde verdieping gaan we verder. We zullen zien dat je met quantumcomputing heel andere dingen kunt doen dan met klassieke computers. Ook kun je de ontwikkelingen en de maatschappelijke implicaties verkennen.

4.1 Protocol: BB84

In hoofdstuk 1 hebben we met experimenten 5.1 en 5.3 de eigenschappen van gepolariseerd licht gebruikt om superpositie te introduceren. In hoofdstuk 2 en werkblad 5.5 'Wat zie je' hebben we gezien hoe een waarnemer in een andere basis, andere coördinaten aan dezelfde vector geeft. In dit werkblad werken we met die kennis een quantumcryptieprotocol uit. Dit protocol is in 1984 door Charles Bennet en Giles Brassard [3] gepresenteerd en geldt als eerste voorbeeld van onkraakbare code. Het staat bekend als BB84 en als quantum key distribution (QKD).





$$\begin{aligned}|+\rangle &= \frac{1}{2}\sqrt{2}|H\rangle + \frac{1}{2}\sqrt{2}|V\rangle \\|-\rangle &= \frac{1}{2}\sqrt{2}|H\rangle - \frac{1}{2}\sqrt{2}|V\rangle \\|H\rangle &= \frac{1}{2}\sqrt{2}|+\rangle + \frac{1}{2}\sqrt{2}|-\rangle \\|V\rangle &= \frac{1}{2}\sqrt{2}|+\rangle - \frac{1}{2}\sqrt{2}|-\rangle\end{aligned}$$

Figuur 4.1: In de standaardbasis (rood) wordt de zwarte vector met gelijke kans als $|H\rangle$ of $|V\rangle$ waargenomen. In de diagonale basis (groen) wordt de vector met zekerheid als $|+\rangle$ waargenomen.

We gebruiken twee twee bases: de standaard basis en de diagonale basis. We weten hoe de Hadamard poort de standaardbasis op de diagonale basis afbeeldt én andersom. Het toestandsdiagram voor de **H**-poort en de vergelijkingen daarbij vind je bij fig. 3.7.

$$\begin{aligned}|0\rangle &\equiv |H\rangle \\|1\rangle &\equiv |V\rangle \\|+\rangle &\equiv |D\rangle \\|-\rangle &\equiv |A\rangle\end{aligned}$$

Fotonen zijn quantumdeeltjes die bij uitstek geschikt zijn voor het quantuminternet. Polarisatie blijft goed behouden over zeer lange lange afstanden, en fotonen reizen lekker snel, met de lichtsnelheid. Je kunt gepolariseerde fotonen versturen onder elke gewenste polarisatierichting.

In deze communicatie zijn er twee partijen, Alice en Bob die op grote afstand van elkaar mogen staan. Ze gebruiken een quantumkanaal voor het verzenden van fotonen (glasvezelkabel), en een klassiek kanaal, een afluisterbare telefoon. Het quantumkanaal is éénrichting. Alice zendt een stroom fotonen naar Bob (één richting), ieder foton in een door haar geprepareerde polarisatie. Ze noteert precies wat ze doet. Bij ontvangst meet Bob de fotonen via een polarisatiefilter dat hij willekeurig standaard of diagonaal zet. Ook hij houdt nauwkeurig bij wat hij doet. Ze verbreken de quantumverbinding en bellen elkaar. Via dit klassieke kanaal spreken ze met elkaar (bidirectioneel) het vervolg af. We werken deze stappen verder uit.

We weten uit hoofstuk 1 dat als we een foton bijvoorbeeld verticaal polariseren en het vervolgens door een verticaal filter laten gaan, het foton met *zekerheid* doorgelaten wordt, en dat het met

zekerheid geblokkeerd wordt als er een horizontaal filter volgt. Het gedrag is volledig voorspelbaar, *deterministisch*. Als een verticaal gepolariseerd foton door een filter gaat dat onder 45° (of -45°) staat, is er 50% kans dat het er doorheen gaat.

Alice wil uiteindelijk een boodschap als een reeks klassieke bits naar Bob sturen. Klassieke bits hebben de waarde 0_b of 1_b . Ze houdt de volgende conventie aan:

bit	basis	pol
logisch 0_b	\oplus	H \leftrightarrow
logisch 0_b	\otimes	- \nwarrow
logisch 1_b	\oplus	V \updownarrow
logisch 1_b	\otimes	+ \nearrow

Alice heeft dus twee mogelijkheden om een 0_b te sturen en twee mogelijkheden voor een 1_b . Als ze in de juiste basis worden waargenomen is het antwoord deterministisch. De informatie over haar eigen basiskeuze houdt Alice echter geheim. Alice heeft een string random bits gekozen en verzendt die ieder met een random basis.

Bob kan niet beter doen dan de binnengekomende fotonen meten volgens twee bases standaard (recht) en diagonaal. Bob kiest voor ieder foton een basis, en houdt nauwkeurig zowel de basiskeuze als het resultaat bij. Bob heeft geen idee of de basis waarmee hij meet dezelfde is als waarmee ze verzonken zijn. Ze verbreken daarna hun quantumverbinding. Hier onder een uitgewerkt voorbeeld;

Alice' random bits	0	1	1	0	0	1	1	1	0	0
Alice' basis	\otimes	\oplus	\otimes	\oplus	\oplus	\oplus	\otimes	\otimes	\oplus	\oplus
Alice verzendt	\nwarrow	\updownarrow	\nearrow	\leftrightarrow	\leftrightarrow	\uparrow	\nearrow	\nearrow	\leftrightarrow	\leftrightarrow
Bob's basis	\oplus	\oplus	\otimes	\oplus	\otimes	\otimes	\otimes	\oplus	\otimes	\oplus
Bob's meting	0	1	1	0	0	0	1	1	1	0

De rest van het protocol handelen ze af ze via de telefoon: Alice en Bob melden eerst hoeveel en welke bits bij Bob zijn overgekomen. Voor het gemak hier alle tien! Bob meldt Alice in welke basis hij heeft gemeten. Alleen als hun bases overeenkomen levert het zinnige informatie. De rest gooien ze weg.

Vraag: Hoeveel procent overeenkomst kun je verwachten als er een groot aantal bits verstuurd wordt?

Ze weten nu over welke bits zij overeenstemming hebben zonder dat de data zelf is gecommuniceerd. Zij weten beiden bijvoorbeeld of een foton in de standaard basis horizontaal of verticaal was. Elk van de overgebleven fotonen bevat één bit informatie uit Alice' random bit string.

Bob's basis	\oplus	\otimes	\oplus		\otimes		\oplus
Bob's meting	1	1	0		1		0

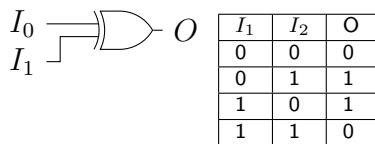
Afgeluisterd? Alice en Bob kunnen zijn afgeluisterd door Eve. Zij zou een foton door een filter kunnen leiden. Daarbij verliest het foton zijn eerdere informatie. Fotonen hebben geen geheugen. Ze kan het nooit meer terugzetten. Zij zou kunnen proberen een foton te versterken en dan een kopie uitlezen en het origineel doorsturen. Ook deze operatie is in tegenstrijd met de fundamentele principes van quantumtheorie [13]. Alice en Bob testen of zij zijn afgeluisterd met een aantal goedgekeurde qubits (bijvoorbeeld een kwart van het totaal). Deze qubits kunnen ze verder niet gebruiken want ze zijn openbaar gemaakt.

Bob's publiceert		1			1		
Alice bevestigt:		OK			OK		

Ze kunnen concluderen dat hun transmissie niet ernstig is afgeluisterd, anders konden ze opnieuw beginnen. De overgebleven bits kunnen worden gebruikt voor een **one-time pad**. Dit is een sleutel voor de enig bewezen methode die onbreekbare versleuteling mogelijk maakt. Daarvoor moet de code nog wel aan extra eisen voldoen. Kijk op de bron welke vier eisen daar genoemd worden.



Met het verkrijgen van de sleutel houdt het BB84 gedeelte van de encryptie op. De boodschap is een binaire reeks. De sleutel is precies even lang als de boodschap. De **XOR**-poort is een logische poort (zie par. 5.4) met de volgende waarheidstabell (zie fig. 4.2).

**Figuur 4.2:** XOR-poort met waarheidstabel.

Alice **XOR**-t haar boodschap met de sleutel en zendt deze data over.

Bob **XOR**-t de boodschap met de sleutel. Wat is het resultaat?

Voorbeeld:

Alice' boodschap	1	0	0	1	0	1	0	0
Alice' sleutel	1	1	0	0	0	1	1	0
Alice verzendt	0	1	0	1	0	0	1	0
	:			:				
Bob ontvangt	0	1	0	1	0	0	1	0
Bob's sleutel	1	1	0	0	0	1	1	0
Bob leest	1	0	0	1	0	1	0	0

Hoeveel fotonen moet Alice minimaal versturen als zij de boodschap "Heb je vanavond wat te doen?" wil overzenden zonder dat het afgeluisterd kan worden? Om een letterteken over te zenden zijn acht bits nodig. De zwakke quantumverbinding verliest 20% van de qubits.

4.2 Eerlijk quantummuntje

Een andere toepassing van het BB84 protocol is deze quantumtoss. Alice en Bob hebben ruzie. Ze willen elkaar even niet zien. Wie mag met de auto weg? Ze bellen elkaar op. Bob ziet het al voor zich: Alice daagt uit tot een kop of munt spelletje over de telefoon. Zij vraagt kop of munt? Wat ik ook kies, zeg zegt gewoon wat haar uit komt. Ze liegt. Dat deed ze vorige keer ook. Ze vertrouwen elkaar even niet.

(De telefoon gaat). Bob: Ja?

(Alice): Alice hier. Kan ik de auto vanmiddag ...

(Bob): Nee

(Alice): Het is ook mijn auto! Laten we er om loten?

(Bob): Ok?

(Alice): Ik gooi een muntje op. Kop of munt?

(Bob): Ja zeg, net als vorige keer zeker.

(Alice): Vertrouw je me niet?

(Bob): Nee!

(Alice): Tsss

(Bob zucht): Ok, we doen het zo. We gebruiken een quantumbasis 'R' of 'D' in plaats van kop of munt.

Alice: Hmm, ok dan.

Alice kiest een reeks random bits (bv 1kbit) en één willekeurige basis, bijvoorbeeld "R". Ze kiest een codering ($H = 1_b$, $V = 0_b$).

Alice stuurt haar reeks van gepolariseerde fotonen.

Bob kiest voor ieder foton dat hij ontvangt een basis, onafhankelijk en willekeurig voor elk foton.

Niet alle fotonen komen over, er zijn gaten in de ontvangstabel.

Na ontvangst belt hij Alice en zegt welke basis zij heeft gekozen.

Als hij goed geraden heeft wint hij, anders verliest hij.

Alice meldt of Bob gewonnen of verloren heeft en zendt ter controle nogmaals de reeks random bits waar zij mee begon.

Bob controleert de reeks tegen zijn tabellen. Er moet een perfecte match zijn met de kolommen in Alice' basis, en een random relatie bij de andere kolommen.

4.3 Protocol: Superdense coding

In deze opdracht ga je onderzoeken hoe je door gebruik te maken van qubits, boodschappen kunt communiceren. Je kunt twee klassieke bits vervangen door één qubit. Dit heet *superdense coding*. De opdracht bestaat uit drie delen. Eerst zullen we superdense coding bekijken en is er een aantal opgaven. Daarna ga je zelf een klein quantum communicatiesysteem ontwerpen en programmeer je dit systeem in Quantum Inspire. Aan het eind van de opdracht presenteert je je bevindingen.

Communiceren op een eiland

Alice woont alleen op een eiland. Ze heeft met niemand contact, behalve met Bob, die op het vasteland woont en die ze berichten kan sturen als er dingen op het eiland misgaan. In eerste instantie kan Alice alleen klassieke bits met Bob uitwisselen. Ze hebben de volgende codering afgesproken:

- 00 – SOS!
- 01 – Nieuw materiaal voor huis nodig
- 10 – Er is droogte/geen water op het eiland
- 11 – Er is geen voedsel op het eiland

Alice stuurt de bits altijd één voor één naar Bob; eerst het bit dat achteraan staat en dan het voorste bit. Ze begint altijd met beide bits in 0 (00). Wanneer ze nieuw materiaal nodig heeft voor haar huisje, zal ze dus haar achterste bit eerst moeten flippen alvorens haar boodschap naar Bob te sturen. En als Alice voedsel nodig heeft, moet ze beide bits flippen. Alleen als Bob een volledige code ontvangt, kan hij Alice helpen. Immers, als Bob enkel een 0 ontvangt en het tweede bit ontbreekt, kan dat ofwel 'SOS', ofwel 'water nodig' betekenen. Om een boodschap over te laten komen, moet Alice dus twee bits versturen.

Dan hoort Bob over qubits en verstrekking van Julia. Alice en Bob besluiten daarom over te stappen op quantumcommunicatie. Om dit mogelijk te maken, delen ze twee volledig verstrekkelde qubits in een van de Bell-toestanden. De Bell-toestanden zijn:

$$G: \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$$

$$H: \frac{1}{\sqrt{2}} |00\rangle - \frac{1}{\sqrt{2}} |11\rangle$$

$$J: \frac{1}{\sqrt{2}} |10\rangle + \frac{1}{\sqrt{2}} |01\rangle$$

$$K: \frac{1}{\sqrt{2}} |10\rangle - \frac{1}{\sqrt{2}} |01\rangle$$

Alice en Bob delen de eerste Bell toestand G: $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$. Alice krijgt de eerste (**rode**) qubit, Bob houdt de tweede (**blauwe**) qubit. Door poorten op haar qubit toe te passen, kan Alice van toestand G in een van de andere Bell-toestanden komen. Als Alice bijvoorbeeld een X-poort op haar qubit toepast, delen Bob en zij toestand J, zonder dat Bob iets met zijn qubit heeft gedaan. En om toestand H te krijgen, hoeft Alice alleen een Z-poort op haar qubit toe te passen. Alice en Bob zouden nu hun vier verschillende boodschappen aan de Bell-toestanden kunnen hangen (maakt Alice de toestand G, dan betekent dat 'SOS', etc.) Door haar qubit te roteren, kan Alice elke Bell-toestand maken die ze wil. Vervolgens stuurt Alice haar qubit naar Bob. Bob meet het verstrengelde paar en weet welke boodschap Alice wilde overbrengen. Het bijzondere hieraan is dat Alice in dit geval slechts één qubit hoeft te versturen om dezelfde boodschap over te brengen waarvoor ze met klassieke communicatie twee bits nodig had. Vandaar de naam voor dit protocol!

Opdracht 4.1

- a. Laat zien dat toestand G inderdaad verstrengeld is.
- b. Teken het schema om van twee losse qubits in de toestand $|0\rangle$ in verstrengelde toestand (G) te komen.
- c. Welke quantumpoort(en) moet Alice op haar qubit toe passen om de toestand K te krijgen?
- d. Kan één qubit nu twee bits aan informatie opslaan?
- e. Zou dit schema ook werken als Alice en Bob twee qubits hadden die niet verstrengeld waren? Waarom wel/niet?
- f. In het teleportatieprotocol van hoofdstuk drie heb je gezien dat er een klassiek kanaal nodig is om een quantum-toestand (quantumboodschap) over te brengen. Wat voor kanaal (klassiek/quantum) wordt er bij superdense coding gebruikt en wat voor boodschap (klassiek/quantum)?

- g. Bob zou de qubits kunnen meten in een speciale Bellbasis, maar hij besluit de qubits te meten in de $|0\rangle/|1\rangle$ -basis. Hiertoe moet hij de verstrengelde toestand terugbrengen tot twee losse qubits. Het protocol om dit te doen is precies tegenovergesteld aan het protocol om twee qubits te verstrengelen. Teken het schema en laat zien dat Bob op deze manier inderdaad de qubits kan decoderen en de boodschap kan ontcijferen. Welke boodschap hoort dus bij welke Bell-toestand?

Uitgebreidere communicatie

Alice vindt haar communicatiemogelijkheden met Bob maar gelimiteerd. Ze wil graag meer boodschappen kunnen overbrengen. Ze stelt daarom aan Bob voor om drie verstrengelde qubits te delen (dit heet een GHZ toestand):

$$M : \alpha |000\rangle + \beta |111\rangle$$

Hier kan Alice 8 boodschappen mee versturen ($2^3 = 8$). Bedenk nu zelf een schema waarbij Alice deze acht boodschappen kan versturen. Denk hierbij aan het volgende:

- Schrijf de acht GHZ toestanden uit die gemaakt kunnen worden.
- Teken het schema om drie qubits die beginnen in de toestand $|0\rangle$ in de GHZ-toestand M te krijgen.
- Teken het schema om drie qubits die beginnen in de toestand $|0\rangle$ in een willekeurige andere GHZ-toestand te krijgen.
- Hoeveel van deze GHZ-toestanden kan Alice maken als ze zelf de eerste qubit heeft en Bob de laatste twee?
- Hoeveel van deze GHZ-toestanden kan Alice maken als ze zelf de eerste twee qubits heeft en Bob de laatste?
- Als Alice zelf twee qubits heeft, welke poorten moet zij dan toepassen op toestand M om naar de andere GHZ toestanden te komen?
- Beschrijf hoe het protocol werkt als Alice twee qubits heeft en Bob één. Teken het schema, inclusief het maken van de GHZ-toestand en het decoderen en uitlezen ervan door Bob.

Opdracht 4.2

We gaan nu kijken of alle voorspellingen kloppen door het protocol te bouwen op Quantum Inspire. Open hiertoe Quantum Inspire en voer de volgende opdrachten uit:

- Bouw het protocol waarbij Alice en Bob een Bell-toestand delen (je kunt hiervoor zelf kiezen welke van de twee quantumchips je gebruikt). Bouw het hele protocol, begin met twee qubits in $|0\rangle$, maak hiervan een verstengeld paar, verzin welke boodschap je wilt versturen, voer Alice's handelingen uit en decodeer de toestand alvorens je deze meet. Doe dit voor alle vier de boodschappen. Zijn de uitkomsten zoals je verwachtte?
- Bouw het protocol waarbij Alice en Bob een GHZ-toestand delen, waarbij Alice begint met 2 qubits en Bob met 1 qubit. Je kunt dus 8 boodschappen versturen (je moet hiervoor de quantumchip met 5 qubits gebruiken). Bouw het hele protocol; verstengel de drie qubits, codeer een boodschap, decodeer de boodschap en meet de qubits. Doe dit voor alle acht de boodschappen. Zijn de uitkomsten zoals je verwachtte?
- Bouw een protocol waarbij Alice en Bob twee Bell-toestanden delen. Van beide toestanden heeft Alice de eerste qubit en Bob de tweede qubit (je moet hiervoor de quantumchip met 5 qubits gebruiken). Bouw opnieuw het hele protocol, van het verstengelen van beide paren en het coderen van de boodschap tot het decoderen van de boodschap en het meten van de qubits. Hoeveel boodschappen kan Alice nu versturen en hoeveel qubits heeft ze naar Bob gestuurd?
- Vind je het efficiënter als Alice en Bob een GHZ-toestand delen, of twee verstengelde paren?

4.4 Quantum en maatschappij

Quantumtechnologie is een sleuteltechnologie die radicaal nieuwe producten en diensten mogelijk maakt. Quantumcomputers, quantumsimulators, quantumnetwerken en quantumSENSoren kunnen straks dingen die 'klassieke' apparaten niet kunnen. [...] We staan daarmee aan het begin van een technologierevolutie die verwacht wordt een grote bijdrage te leveren aan het oplossen van maatschappelijke uitdagingen op het gebied van bijvoorbeeld energie, voedsel en zorg. Nederland doet mee in de wetenschappelijke en technologische voorhoede van de ontwikkelingen en wereldwijd wordt er door overheden en bedrijven fors geïnvesteerd in quantumonderzoek en -innovatie.

Zo begint het rapport van de Nationale Agenda Quantumtechnologie, opgesteld in september 2019 in opdracht van het Ministerie van Economische Zaken en Klimaat. Het duidelijk: de quantumcomputer komt er aan. In een opdracht over de maatschappelijke impact van deze tweede quantumgolf (de eerste vond plaats in het begin van de twintigste eeuw) mag een gedachtewisseling over deze ontwikkelingen niet ontbreken. In opdracht 4.3 lezen we de Nationale Agenda door.

Opdracht 4.3

Voor deze opdracht moet je gebruik maken van internet. Je doet de opdracht met zijn tweeën.

- a. Download de [Nationale Agenda](#)
- b. De Nationale Agenda noemt behalve de quantumcomputer nog drie andere toepassingen van quantumtechnologie in bovenstaand citaat. Zoek in de brochure op wat deze technologieën inhouden.

In **hoofdstuk 1** vind je een overzicht van de inhoud van de brochure.

- c. Geef in trefwoorden de inhoud van de brochure van de verschillende hoofdstukken.



Hoofdstuk 2 geeft de vier belangrijkste toepassingsgebieden die ook voor het Europese Quantum Flagship van belang zijn. Bij de beschrijving van deze vier toepassingsgebieden worden belangrijke details vermeld.

- d. Wat is het verschil tussen universele quantumcomputers en quantumsimulatoren?
- e. Wat is een hybride quantumsimulator?
- f. Wat zijn de voordelen van quantumcommunicatie op wereldschaal?
- g. Welke domeinen kunnen profiteren van quantumsensing?

Hoofdstuk 3 gaat over de relatie tussen quantumtechnologie en maatschappij. In figuur 7 van de module is die relatie in kaart gebracht.

- h. Geef aan op welke maatschappelijke terreinen quantumtechnologie een rol gaat spelen. Geef voor elk terrein een voorbeeld van een toepassing.

Hoofdstuk 4 brengt de positie van Nederland op quantumgebied in kaart. Daarbij wordt ook aandacht gegeven aan Nederlandse kennisinstellingen en universiteiten.

- i. Geef bij figuur 7 voor elk van de maatschappelijke terreinen één universiteit/kennisinstelling aan die op dat terrein actief is.

Hoofdstuk 5 beschrijft vier lijnen waarop moet worden geacteerd en drie katalysator-programma's.

- j. Noem de vier lijnen en beschrijf de drie programma's.

Hoofdstuk 6 gaat over de Nederlandse overheid.

- k. Geef met twee werkwoorden aan wat de Nederlandse overheid volgens de brochure moet doen.

Wat gaan de gemiddelde burger merken van de quantumcomputer?

De quantumcomputer zal de gewone PC niet gaan vervangen. De digitalisering die overal om ons heen plaats vindt gaat gewoon door. En daarbij wordt gebruik gemaakt van bits en niet van qubits. Niettemin is uit het voorgaande ook op te maken dat de wereld om ons

heen gaat veranderen door de komst van de quantumcomputer. Er wordt zelfs gesproken van een nieuwe technologische revolutie. In opgave 4.4 doe je een poging om in kaart te brengen hoe die revolutie er uit gaat zien.

Opdracht 4.4

Maak aan de hand van de teksten en interviews in het voorstaande een overzicht van alle mogelijke ontwikkelingen op het gebied van de quantumtechnologie.

- a. Begin met de Nationale Agenda, hoofdstuk 3, figuur 7. Denk na over de wijze waarop je de ontwikkelingen in kaart brengt. Maak eventueel gebruik van een matrix om overzicht te krijgen.
- b. Loop de andere bronnen langs om te kijken of er nog waardevolle aanvullingen zijn.

De Nationale Agenda voor Quantumtechnologie is zelfverzekerd; de quantumcomputer gaat er komen. Dat verwacht je ook van zo'n rapport. Er is inmiddels ook al 615 miljoen Euro uitgetrokken voor een **nationaal groefonds**. Het rapport besteedt ook aandacht aan maatschappelijke aspecten. Aan onderzoek wordt de eis gesteld dat het ethisch getoetst is, en een gebrek aan maatschappelijk draagvlak kan een spaak in het wiel steken.



nationaal groefonds

In opdracht 4.5 onderzoeken we of deze nieuwe sleuteltechnologie de mensheid tot dienst zal zijn.

Opdracht 4.5

Is de komst van de quantumtechnologie wenselijk of niet? De bedoeling is om je eerste gedachten hierover op te schrijven op een half A4-tje. De bedoeling is dat je dit in je eentje doet. Het papier blijft verder ook in jouw bezit en wordt niet openbaar gemaakt.

- a. Geef een voorlopig antwoord op de vraag.
- b. Zet puntsgewijs je argumenten pro of con op papier.
- c. Zet ook je twijfels op papier.

In zijn boek "The Wizard and the Prophet"^[9] beschrijft Charles Mann het debat over de uitdagingen waar de mensheid voor staat:

voedsel, water energie en klimaatverandering. Hij maakt een indeling in tovenaars en profeten.

De *tovenaars* wijzen op onze vindingrijkheid. Het is werkelijk ongelooflijk waartoe de mens in staat is.

De *profeeten* wijzen erop dat er natuurlijke grenzen zijn aan de aarde die we niet kunnen en mogen overschrijden.

Het onderscheid tussen tovenaars en profeten vinden we ook in andere technologische revoluties terug. Er is een discussie tussen twee kampen. Het ene kamp (de profeten) wil de mens beschermen tegen de techniek en vreest dat de techniek een bedreiging vormt voor de autonomie van de mens. Profeten zijn bang dat de techniek de menselijke maat overstijgt en zo de menselijke soevereiniteit ondervindt. Ze zullen wijzen op de afhankelijkheid van de mens van bijvoorbeeld de digitale hulpmiddelen. Het andere kamp (de tovenaars) wijst veel sneller naar het nut van de techniek. Voor de tovenaars zijn technische middelen alleen maar mogelijkheden die het menselijk bestaan vergemakkelijken. De autonomie van de mens wordt dus vergroot want hij krijgt meer tijd voor andere dingen.

Filosofie over techniek en maatschappij

Je zult je zelf meestal niet als 100% tovenaar of profeet zien. Het zal niet voor elke technologie hetzelfde zijn, en je beeld verandert in de tijd. Weinig mensen zullen zich als profeet zien waar het de boekdrukkunst betreft. (Dat lag destijds overigens wel even anders!). En weinig mensen zullen zich als tovenaar zien bij het idee van Elon Musk om een searchchip in het brein te implanteren om daarmee het zoeken op internet te vergemakkelijken ([neuralink](#)). Maar toch: dit soort technologie kan heel belangrijk zijn voor mensen met een totale verlamming en die alleen via dit soort technologie kunnen communiceren. De indeling profeet/tovenaar is bij één technologie kennelijk al niet ondubbelzinnig. Het is een graduele schaal. de methode van opgave [4.6](#) geeft meer inzicht.



Opdracht 4.6

Bij deze opdracht ga je bij een groot aantal technologische oplossingen voor een welomschreven behoefte jezelf indelen in de categorie profeet of tovenaar.

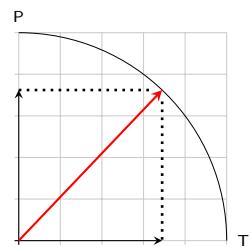
- a. Zelf bedenk je één zo'n case. Het moet gaan om een moderne technologie (dus geen boekdrukkunst!). De technologie moet ergens beschreven staan samen met een mogelijke toepassing. (De implantchip voor communicatie voor patiënten met verlamming is een kandidaat, maar de chip voor Googlesearch is wel een andere!).
- b. Stel samen met de cases van andere leerlingen een lijst op.

Ten behoeve van de indeling is een demarcatielijn nodig. Kies hier: bij ernstige niet-technologische twijfel aan de voorgestelde oplossing ben je profeet anders tovenaar. Het gaat dus niet om de technische realiseerbaarheid maar om de wenselijkheid van de technologie.

- c. Deel jezelf volgens bovenstaand criterium in bij elk van de cases uit de lijst .
- d. Verzamel de resultaten. Hoe vaak was je tovenaar? Hoe vaak profeet?

net als in hoofdstuk 2 van de module kun je je eigen toestand weergeven met een vector. Dat betekent natuurlijk niet dat het hier over quantum gaat!

- e. Stel het diagram op.
- f. Ben je meer tovenaar of toch meer profeet?
- g. Is het onderscheid tovenaar/profeet zinvol?



Het voorgaande heeft hopelijk duidelijk gemaakt dat in ieder mens zowel een profeet als een tovenaar schuilt. Een genuanceerde mening biedt plaats voor beide en er is sprake van een spectrum. Dat maakt het moeilijker maar ook uitdagender.

Gesprek over quantum

De quantumtechnologie gaat er komen. Welke gevaren brengt quantumtechnologie met zich mee? Welke eisen stelt de komst van quantumtechnologie aan de maatschappij? Kan deze technologische ontwikkeling worden gestuurd? Om antwoord op dat soort

vragen te vinden moet er gepraat worden. Maar het debat is daarvoor niet het geschikte instrument. Bij het debat heb je kampen. Er wordt strijd gevoerd. Je moet partij kiezen. Het debat met als enige uitkomst: voor (tovenaars) of tegen (profeten) heeft een verlammende werking. Een veel betere aanpak is het socratisch gesprek. Hierbij gaat het niet om je gelijk te halen of om een overwinning te boeken. Hierin draait het om nieuwsgierigheid naar de opvattingen van de ander. Zijn er verschillen of overeenkomsten met je eigen opvattingen? Het onderscheid tovenaar-profeet is dan geschikt om een zaak van twee kanten te bekijken. Een socratisch gesprek over quantumtechnologie vormt het doel van opgave 4.7.

Opdracht 4.7

Bestudeer je notities die je gemaakt hebt over jouw opvattingen over quantumtechnologie in opdrachten 4.3, 4.4 en 4.5. Ben je meer profeet of meer tovenaar? Vorm een gespreksgroep van 3 tot 5 personen. Zoek een samenstelling met zowel profeten als tovenaars. Ga het gesprek aan over de wenselijkheid van quantumcomputing. Voer het gesprek in drie fasen:

- a. Bespreek eerst de voordelen van quantumcomputing: vergeet vooral niet door te vragen. Is de QC sneller? Is dat belangrijk? Waarom... etc.
- b. Bespreek de nadelen van quantumcomputing.
- c. Bespreek welke eisen de komst van quantumcomputing stelt aan de maatschappij.

Een socratisch gesprek kent geen beslissingen. Meningsverschillen worden niet beslecht. Maar dat betekent niet dat er niet een gemeenschappelijke afsluiting mogelijk is. Daarvoor dient opgave 4.8.

Opdracht 4.8

Bereid met je gespreksgroep een presentatie voor met als doelstelling de uitdaging van het quantumtijdperk in beeld te brengen. De presentatie kan bestaan uit een poster, een verslag, een filmpje of ieder andere creatieve uiting.

4.5 Hilbertruimtes

Aan het einde van de negentiende eeuw en in het begin van de twintigste eeuw werd er veel wiskundig onderzoek gedaan naar abstracte vectorruimtes. Een van de mensen die dit onderzocht was David Hilbert (1862-1943), hij was zeer geïnteresseerd in zogenoemde L^p -ruimtes. Later heeft John von Neumann (1903-1957) zijn werk veralgemeiniseerd naar abstracte vectorruimtes en heeft de Hilbertruimtes naar hem vernoemd.

Hilbertruimtes zijn belangrijk voor het begrijpen van quantumtheorie. Ze bieden een manier om over dingen te denken met behulp van vectoren. Zo kun je ze gebruiken om de "lengte" van een functie te berekenen of zelfs de stelling van Pythagoras te gebruiken voor functies.

Het standaard inproduct

We beginnen met een korte herhaling van het al bekende inproduct. Voor twee vectoren in het vlak $x = (x_1, x_2)$ en $y = (y_1, y_2)$ is het standaard inproduct

$$x \cdot y = x_1y_1 + x_2y_2$$

Op dezelfde manier kun je het inproduct nemen van twee n -dimensionale vectoren.

$$x \cdot y = x_1y_1 + x_2y_2 + \dots + x_ny_n$$

Als twee vectoren loodrecht op elkaar staan dan is het inproduct 0. We zeggen dan dat de vectoren orthogonaal op elkaar staan.

Je kunt de lengte van vector x berekenen met het inproduct door $\|x\| = \sqrt{x \cdot x}$.

Opdracht 4.9

a. Laat $x = \begin{pmatrix} -1 \\ 4 \\ 0 \\ 2 \end{pmatrix}$ en $y = \begin{pmatrix} 0 \\ 1 \\ -3 \\ 2 \end{pmatrix}$. Bereken $x \cdot y$.

b. Ga na dat $(x + z) \cdot y = x \cdot y + z \cdot y$.

c. Vind twee vectoren die orthogonaal staan op $x = \begin{pmatrix} 5 \\ -8 \\ 0 \end{pmatrix}$.

Het complexe geval

Voor complexe vectoren kun je proberen het standaard inproduct op dezelfde manier te definiëren. Dit gaat mis omdat je lengtes krijgt die complex zijn. Kijk bijvoorbeeld naar de vector $x = (i)$ dan zou $\sqrt{i^2} = i$ de lengte van x zijn, maar voor lengte willen we een reëel getal hebben.

Om wel van lengtes te kunnen spreken is het standaard complex inproduct als volgt gedefinieerd:

$$\langle x, y \rangle = x_1\bar{y}_1 + x_2\bar{y}_2 + \dots + x_n\bar{y}_n$$

waarin \bar{y}_1 de complex geconjugeerde is van y_1 . Ga na dat:

Def.: De complex ge-

conjugeerde van $a+ib$:

$$\overline{a+ib} = a - ib$$

$\|i\| = \sqrt{\langle i, i \rangle} = 1$.

$$y = \begin{pmatrix} -7i \\ 4+3i \end{pmatrix}$$

Als voorbeeld berekenen we het inproduct van $x = \begin{pmatrix} 1+5i \\ -2+i \end{pmatrix}$ en

$$\langle x, y \rangle = (1+5i)(7i) + (-2+i)(4-3i) = -40 + 17i$$

Net als bij reële vectoren kunnen we ook van complexe getallen (niet de nulvector) zeggen of ze orthogonaal op elkaar staan. Maar pas op: Het is heel moeilijk, zo niet onmogelijk, om complexe vectoren te visualiseren.

Opdracht 4.10

a. Bereken $\langle x, y \rangle$ in:

$$\begin{array}{ll} a. x = \begin{pmatrix} i \\ -i \end{pmatrix}, y = \begin{pmatrix} 1 \\ -1 \end{pmatrix} & c. x = \begin{pmatrix} 1-3i \\ 5+i \end{pmatrix}, y = \begin{pmatrix} 3 \\ 4+2i \end{pmatrix} \\ b. x = \begin{pmatrix} 2i \\ 4 \end{pmatrix}, y = \begin{pmatrix} -3i \\ i \end{pmatrix} & d. x = \begin{pmatrix} 4+7i \\ 5-4i \end{pmatrix}, y = \begin{pmatrix} 6-3i \\ 1+8i \end{pmatrix} \end{array}$$

b. Bereken de lengte van x in:

$$\begin{array}{ll} a. x = \begin{pmatrix} 5 \\ 2 \end{pmatrix} & c. x = \begin{pmatrix} 2-i \\ 1+3i \end{pmatrix} \\ b. x = \begin{pmatrix} -i \\ 3i \end{pmatrix} & d. x = \begin{pmatrix} 3-7i \\ -2+6i \end{pmatrix} \end{array}$$

c. Ga na dat $x = \begin{pmatrix} 2 \\ -i \\ 1+i \end{pmatrix}$ en $y = \begin{pmatrix} 2+i \\ 2+4i \\ 0 \end{pmatrix}$ orthogonaal op elkaar staan.

d. Laat zien als $x = \begin{pmatrix} i \\ 3-i \end{pmatrix}$ en $y = \begin{pmatrix} 1+2i \\ 4 \end{pmatrix}$ dat $\langle x, y \rangle$ niet gelijk is aan $\langle y, x \rangle$ maar aan $\overline{\langle y, x \rangle}$.

Hilbertruimtes

Vectoren worden vaak gezien als (eindige) rijtjes getallen, maar er zijn veel meer dingen die zich hetzelfde gedragen. Een voorbeeld hiervan zijn (reële) functies. Net als normale vectoren kan je functies optellen en met een getal vermenigvuldigen (vaak aangegeven met λ) om een nieuwe functie te krijgen. Ook heb je de functie $f(x) = 0$, de nulfunctie, die net als de nulvector niks doet bij optelling. De (reële) functies vormen een zogenoemde (reële) vectorruimte.

Een Hilbertruimte is een (volledige) complexe vectorruimte met een gedefinieerd inproduct zodat:

- $\langle x, y \rangle = \overline{\langle y, x \rangle}$ (de complex geconjugeerde van $\langle y, x \rangle$),
- $\langle \lambda_1 x + \lambda_2 y, z \rangle = \lambda_1 \langle x, z \rangle + \lambda_2 \langle y, z \rangle$ (λ_1, λ_2 zijn complexe getallen),
- $\langle x, x \rangle$ is een reëel getal en $\langle x, x \rangle \geq 0$,
- Als $\langle x, x \rangle = 0$ dan $x = 0$.

Deze eigenschappen zijn makkelijk af te leiden aan de hand van het inproduct van de vorige paragraaf en vormen een basis voor inproducten van vector ruimtes. Zo kun je dus functies met elkaar "vermenigvuldigen" zodat er een getal uit komt. **Voorbeeld:** Als we kijken naar continue functies met als inproduct

$$\langle f, g \rangle = \int_{-1}^1 f(x) \overline{g(x)} dx$$

waarin $\overline{g(x)}$ de complex geconjugeerde is van $g(x)$, bijvoorbeeld $\overline{e^{ix}} = e^{-ix}$.

Als $f(x) = e^x$ en $g(x) = xe^{-x}$ (dus $\overline{g(x)} = g(x)$), dan geldt

$$\begin{aligned} \langle f, g \rangle &= \int_{-1}^1 f(x) \overline{g(x)} dx \\ &= \int_{-1}^1 x dx \\ &= \left[\frac{1}{2}x^2 \right]_{-1}^1 = 0 \end{aligned}$$



Figuur 4.3: groen: $f(x)$, blauw: $g(x)$, rood: $\langle f, g \rangle$

We zeggen dat x, y orthogonaal op elkaar staan (in een Hilbertruimte) als $\langle x, y \rangle = 0$. De twee functies in het voorbeeld staan dus orthogonaal op elkaar. Functies die orthogonaal op elkaar staan hoeven elkaar dus niet loodrecht te snijden (zie figuur 4.3).

In een Hilbertruimte wordt de lengte van x gegeven door $\|x\| = \sqrt{\langle x, x \rangle}$.

Voorbeeld: De lengte van $f(x) = -3ix^4 + 5x^2 + 10i$ is $\sqrt{\langle f, f \rangle}$.

$$\begin{aligned}\langle f, f \rangle &= \int_{-1}^1 f(x) \overline{f(x)} dx \\ &= \int_{-1}^1 (-3ix^4 + 5x^2 + 10i)(3ix^4 + 5x^2 - 10i) dx \\ &= \int_{-1}^1 9x^8 + 35x^4 + 100 dx \\ &= [x^9 + 7x^5 + 100x]_{-1}^1 = 216\end{aligned}$$

Dus $\|f\| = \sqrt{216}$.

Opdracht 4.11

Laat het inproduct voor continue functies (die een reëel getal sturen naar een complex getal, bijvoorbeeld e^{ix}) gegeven zijn door

$$\langle f, g \rangle = \int_{-1}^1 f(x) \overline{g(x)} dx.$$

met $\overline{g(x)}$ de complex geconjugeerde van $g(x)$, bijvoorbeeld $\overline{e^{ix}} = e^{-ix}$.

a. Bereken $\langle f, g \rangle$ voor:

- a. $f(x) = x + 4, g(x) = x^2 + 7$
- b. $f(x) = x^5 + ix + 7, g(x) = 3x^3 + 2ix$
- c. $f(x) = \cos(x), g(x) = \tan(x)$
- d. $f(x) = e^{2\pi ix}, g(x) = e^{4\pi ix}$

b. Gebruik hetzelfde inproduct als in de vorige opgave. Bereken $\|f\|$ voor:

- a. $f(x) = 5x + 1$
- c. $f(x) = 6e^x$
- b. $f(x) = 2ix^3 + 4x + 1$
- d. $f(x) = e^{2\pi ix}$

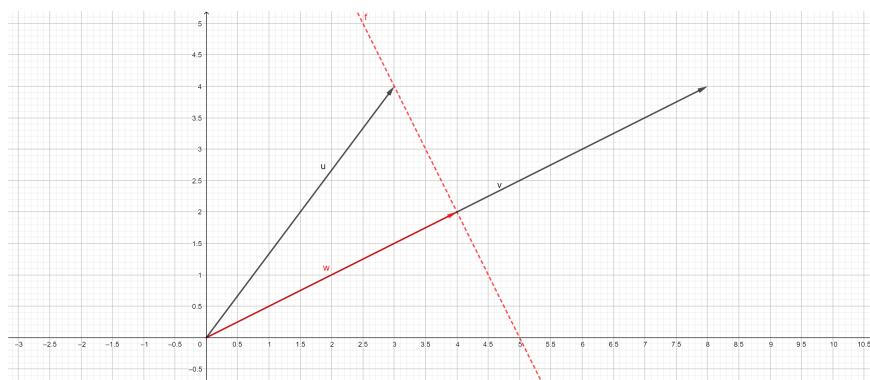
Opdracht 4.12

Laat het inproduct voor 2-dimensionale reële vectoren gegeven zijn door

$$\langle x, y \rangle = x_1 y_1 + (x_2 - x_1)(y_2 - y_1).$$

- a. Wanneer geldt $x_1 y_1 + (x_2 - x_1)(y_2 - y_1) = x_1 y_1 + x_2 y_2$? (geef een voorbeeld).
- b. Bereken $\langle x, y \rangle$ voor $x = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$ en $y = \begin{pmatrix} -1 \\ -3 \end{pmatrix}$, en concluder dat ze orthogonaal op elkaar staan.
- c. Laat zien dat x en y niet loodrecht op elkaar staan (hoek van 90°).

Projectie: In een Hilbertruimte wordt de projectie van x op y (allebei niet nul) gegeven door $\frac{\langle x, y \rangle}{\langle y, y \rangle} y$.



Figuur 4.4: w is de projectie van u op v (met behulp van een loodlijn).

Dus de projectie van x op y is altijd in de vorm $\lambda \cdot y$ met λ een getal.

Opdracht 4.13

- a. Bereken de projectie (met het standaard inproduct) van $x = \begin{pmatrix} 5 \\ 2 \end{pmatrix}$ op $y = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ (dit is de projectie van x op de y -as).

- b. Laat het inproduct voor reële functies:

$$\langle f, g \rangle = \int_1^2 f(x)g(x)dx$$

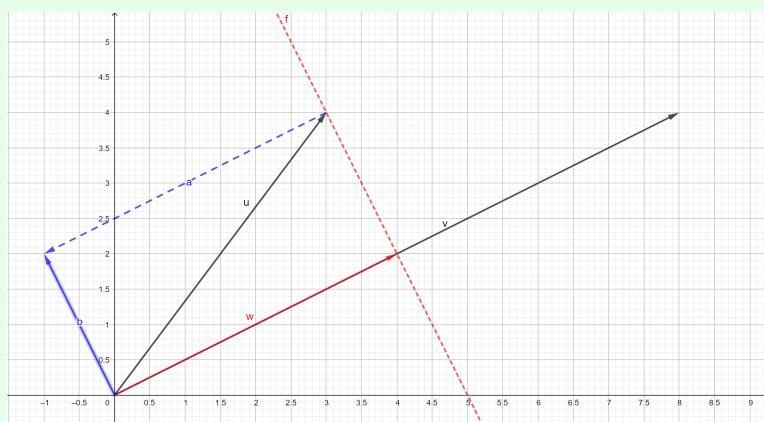
Laat $f(x) = \frac{e^x}{x}$, $g(x) = x^3 + 4x^2$ en $h(x) = x$. Bereken de projectie van $f(x)$ op $h(x)$, en bereken de projectie van $g(x)$ op $h(x)$

- c. Schets de functies gevonden bij b..

- d. Laat zien dat de projectie van x op x gelijk is aan x .

Opdracht 4.14

Stel je hebt x en y (met x niet een veelvoud van y), dan kun je z vinden zodat z en y orthogonaal op elkaar staan. Een manier om dit te doen is de projectie van x op y uitrekenen en die van x aftrekken. Dit geeft de formule $z = x - \frac{\langle x, y \rangle}{\langle y, y \rangle}y$.



Figuur 4.5: $b = u - w$ en inderdaad: b staat loodrecht op v .

- a. Gebruik deze methode (met het standaard inproduct) om een orthogonaal element te vinden van $y = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$ met behulp van $x = \begin{pmatrix} 7 \\ 2 \end{pmatrix}$. Ga na of de gevonden vector ook echt orthogonaal staat op y .
- b. Laat het inproduct en de functies hetzelfde zijn als bij b. van opdracht 4.13. Vind twee functies die orthogonaal staan op h .
- c. Schets de functies gevonden bij b..

Opdracht 4.15

Pythagoras: We gaan in deze opgave laten zien dat de stelling van Pythagoras geldt in elke Hilbertruimte.

- a. Laat zien dat voor elk inproduct geldt $\langle x, \lambda_1 y + \lambda_2 z \rangle = \overline{\lambda_1} \langle x, y \rangle + \overline{\lambda_2} \langle x, z \rangle$ met λ_1, λ_2 complexe getallen. (hint: $\overline{a+b} = \overline{a} + \overline{b}$)
- b. Schrijf $\|x+y\|^2$ uit en concludeer $\|x+y\|^2 = \langle x, x \rangle + \langle x, y \rangle + \langle y, x \rangle + \langle y, y \rangle$
- c. Laat zien dat als $\langle x, y \rangle = \langle y, x \rangle = 0$ (dus x en y orthogonaal op elkaar staan), dat dan $\|x+y\|^2 = \|x\|^2 + \|y\|^2$ (de stelling van Pythagoras).

Hilbert ruimten en Fourier analyse zijn twee van de vele wiskundige pijlers waarop de wiskunde van quantumcomputing is gebouwd.

4.6 Fourieranalyse

In de quantumtheorie spelen golven een belangrijke rol. Fourieranalyse probeert functies te koppelen aan golven. Voor de sinus is dat natuurlijk niet moeilijk want dat is al een golf, maar met Fourieranalyse kun je bijna alle functies zien als de som van golven, zelf functies zoals $\frac{1}{2}x$ kun je door maar een paar sinusoïdes bij elkaar optellen erg goed benaderen. Ter voorbereiding hiervan zullen we eerst kijken naar een simpelere benaderingsmethode.

Taylorreeksen

Zoals eerder gezegd kun je functies zien als vectoren (rijtjes getallen). In deze paragraaf laten we zien waarom dit zo is. We gaan proberen elke functie als een polynoom (bijvoorbeeld $x^4 + 3x^2 + 17$) te schrijven. Een voordeel hiervan is dat je door de eerste paar termen van het polynoom uit te rekenen al een zeer goede benadering krijgt van de functie (die ook nog makkelijk integreerbaar is). Voor een functie als $f(x) = x^9 + 5x^4 + 7$ is dat zeer makkelijk want dat is al een polynoom. We gaan nu proberen $f(x) = e^x$ te schrijven als het polynoom

$$g(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots$$

Omdat $f(x) = g(x)$ en $f(0) = 1$ geldt $g(0) = a_0 = 1$. Om a_1 uit te rekenen is het niet handig om een ander punt in te vullen want

$$g(1) = a_0 + a_1 + a_2 + \dots$$

dit geeft geen makkelijke manier om a_1 uit te rekenen. Daarom gebruiken we de afgeleide $f'(x) = e^x$ dus $f'(0) = 1$, maar

$$g'(x) = a_1 + 2a_2x + 3a_3x^2 + 4a_4x^3$$

dus $g'(0) = a_1 = 1$. Op dezelfde manier kun je door de afgeleide van $f'(x)$ (dus $f''(x)$) gebruiken om $a_2 = \frac{1}{2}$ te vinden. Als je de eerste zes termen uitrekent krijg je:

$$g(x) = 1 + x + \frac{1}{2}x^2 + \frac{1}{6}x^3 + \frac{1}{24}x^4 + \frac{1}{120}x^5$$

Je ziet rond 0 dat g een goede benadering is van f . Als je meer termen toevoegt zal de benadering steeds beter worden en als je oneindig veel termen hebt zijn g en f gelijk.

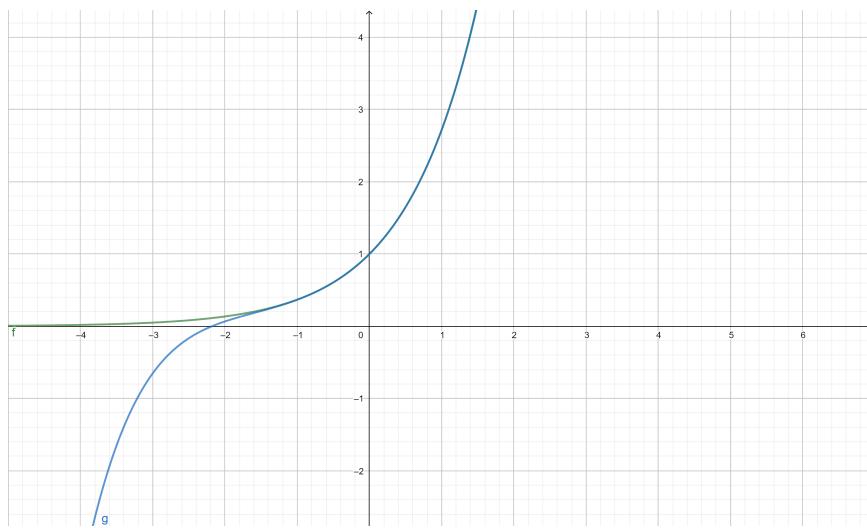
De algemene formule van een Taylorreeks (rond 0) voor een functie f is

$$g(x) = f(0) + f^{(1)}(0)x + \frac{f^{(2)}(0)}{2!}x^2 + \frac{f^{(3)}(0)}{3!}x^3 + \frac{f^{(4)}(0)}{4!}x^4 + \dots$$

Hierbij is $f^{(n)}(0)$ de n -de afgeleide in 0 dus $f^{(2)}(0) = f''(0)$ en $n! = 1 \cdot 2 \cdot 3 \cdots n$ dus $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$ ($0! = 1$).

We bekijken weer $f(x) = e^x$ omdat ook $f'(x) = e^x$. Er geldt $f^{(n)}(0) = e^0 = 1$ dus

$$g(x) = 1 + x + \frac{1}{2!}x^2 + \frac{1}{3!}x^3 + \frac{1}{4!}x^4 + \dots$$



Je kunt e^x dus zien als de rij getallen $(1, \frac{1}{2!}, \frac{1}{3!}, \frac{1}{4!}, \dots)$.

Opdracht 4.16

- a. Bereken de eerste 4 termen van de Taylorreeks van de volgende functies en plot f en g

Als je een Taylorreeks probeert te maken van $f(x) = \frac{1}{x}$ heb je een probleem want $f(0)$ is niet gedefinieerd.

- b. Vervang x door $x = y + 1$ en bereken $f^{(1)}(y)$, $f^{(2)}(y)$ en $f^{(3)}(y)$.
 - c. Bepaal de eerste 4 termen van de Taylorreeks van $f(y)$.
 - d. Substitueer $y = x - 1$ in de Taylorreeks en plot f en g .
 - e. Gebruik dezelfde truc om een benadering te maken (4 termen) van $f(x) = \ln(x)$.

Fourierreeksen

In deze paragraaf gaan we een andere benadering vinden van (periodeke) functies aan de hand van sinusoïde. Hiervoor gebruiken we het volgende inproduct:

$$\langle f, g \rangle = \frac{1}{2\pi} \int_0^{2\pi} f(x)g(x)dx.$$

Als benadering voor de functie f gebruiken we nu de volgende functie

$$\begin{aligned} g(x) &= a \\ &+ b_1 \sin(x) + b_2 \sin(2x) + b_3 \sin(3x) + \dots \\ &+ c_1 \cos(x) + c_2 \cos(2x) + c_3 \cos(3x) + \dots \end{aligned}$$

Als we proberen a uit te rekenen (op dezelfde manier zoals bij Taylorreeksen) komen we in de problemen, want als $\sin(x) = 0$ dan $\cos(x) \neq 0$. Daarom gebruiken we dat als $f = g$ dat dan de projectie P op $h(x) = 1$ voor f en g hetzelfde zijn.

$$\begin{aligned} P(x) &= \frac{\langle g, h \rangle}{\langle h, h \rangle} h \\ &= \langle a, h \rangle + \langle b_1 \sin(x), h \rangle + \langle c_1 \cos(x), h \rangle + \dots \end{aligned}$$

maar omdat $h(x) = \cos(0x)$ is h een sinusoïde dus staat h orthogonaal op alle andere sinusoïde. Dus

$$\begin{aligned} P(x) &= \langle a, h \rangle \\ &= \frac{1}{2\pi} \int_0^{2\pi} a dx = a \end{aligned}$$

Ook geldt

$$\begin{aligned} P(x) &= \frac{\langle f, h \rangle}{\langle h, h \rangle} h \\ &= \frac{1}{2\pi} \int_0^{2\pi} f(x)dx \end{aligned}$$

Dus

$$a = \frac{1}{2\pi} \int_0^{2\pi} f(x)dx = \langle f, 1 \rangle$$

Op dezelfde manier geldt

$$b_n = \frac{1}{2\pi} \int_0^{2\pi} f(x) \sin(nx) dx = \langle f, \sin(nx) \rangle$$

$$c_n = \frac{1}{2\pi} \int_0^{2\pi} f(x) \cos(nx) dx = \langle f, \cos(nx) \rangle.$$

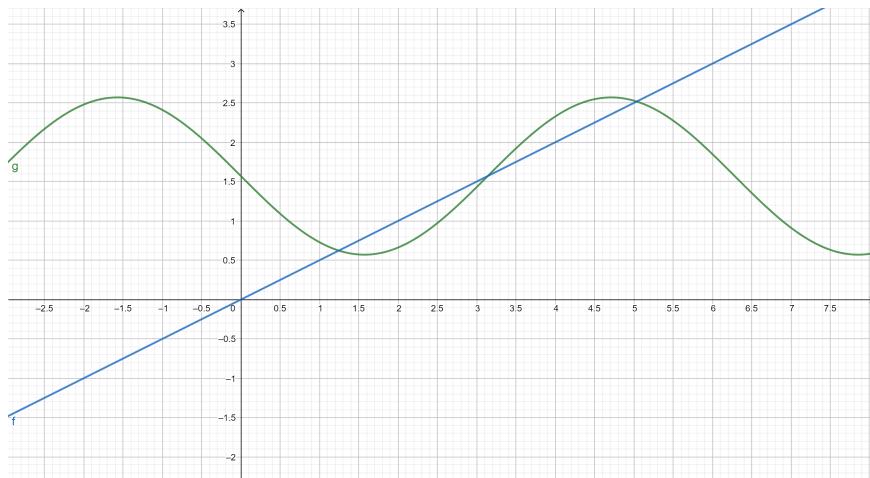
Als voorbeeld bekijken we $f(x) = \frac{1}{2}x$ waarvoor dan geldt

$$a = \frac{1}{2\pi} \int_0^{2\pi} \frac{1}{2}x dx = \frac{1}{2\pi} \left[\frac{1}{4}x^2 \right]_0^{2\pi} = \frac{\pi}{2}$$

$$b_1 = \frac{1}{\pi} \int_0^{2\pi} \frac{1}{2}x \sin(x) dx = \frac{1}{\pi} \left[\frac{1}{2} \sin(x) - \frac{1}{2}x \cos(x) \right]_0^{2\pi} = -1$$

$$c_1 = \frac{1}{\pi} \int_0^{2\pi} \frac{1}{2}x \cos(x) dx = \frac{1}{\pi} \left[\frac{1}{2}x \sin(x) + \frac{1}{2} \cos(x) \right]_0^{2\pi} = 0$$

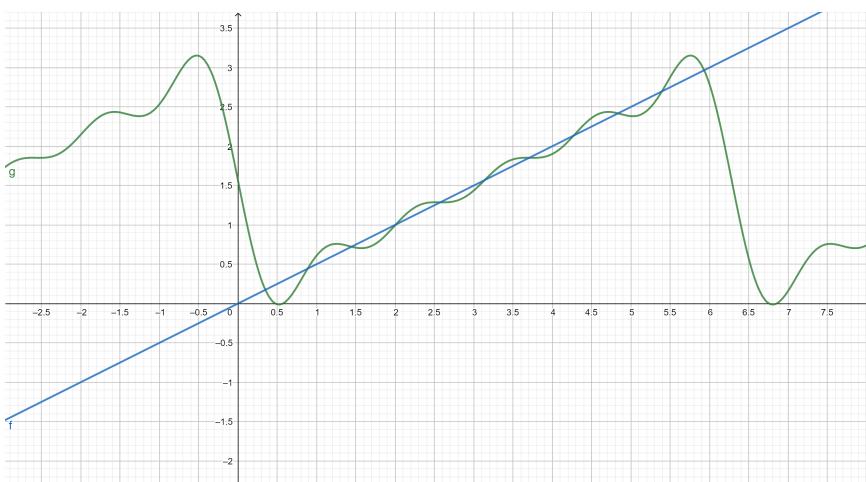
Dus we krijgen als benadering $g(x) = \frac{\pi}{2} - \sin(x)$.



Zoals je ziet is het nog niet zo 'n goede benadering. Als je b_2 tot en met b_5 en c_2 tot en met c_5 uitrekent krijg je:

$$g(x) = \frac{\pi}{2} - \sin(x) - \frac{1}{2} \sin(2x) - \frac{1}{3} \sin(3x) - \frac{1}{4} \sin(4x) - \frac{1}{5} \sin(5x)$$

Dit is al een veel betere benadering, maar alleen in het interval $(0, 2\pi)$ daarna herhaalt de grafiek zich. Dit blijft het geval hoeveel termen je ook uitrekent daarom is deze manier juist geschikt voor periodieke functies.



Opdracht 4.17

- a. Laat zien dat $\int \sin(2x) \cos(x) dx = -\frac{2}{3} \cos^3(x)$.
- b. Laat zien dat $\sin(2x)$ en $\cos(x)$ orthogonaal op elkaar staan (met het hierboven genoemde inproduct).
- c. Bereken a, b_1, b_2, c_1 en c_2 van de Fourierreeks van de volgende functies (met behulp van je GR) en plot f en g .
 - a. $f(x) = x^2 - x - 1$
 - c. $f(x) = e^x$
 - b. $f(x) = \tan\left(\frac{x - \pi}{2}\right)$
 - d. $f(x) = \frac{1}{x + 1}$

We kunnen ook een ander inproduct nemen voor een Fourierreeks. Beschouw

$$\langle f, g \rangle = \frac{1}{4\pi} \int_{-2\pi}^{2\pi} f(x)g(x)dx$$

Net als hiervoor zoeken we een benadering voor een functie f en die benadering is nog steeds

$$\begin{aligned}g(x) = & a \\& + b_1 \sin(x) + b_2 \sin(2x) + b_3 \sin(3x) + \dots \\& + c_1 \cos(x) + c_2 \cos(2x) + c_3 \cos(3x) + \dots\end{aligned}$$

d. Laat zien met behulp van projectie dat $a = \langle f, 1 \rangle$.

Er geldt $b_n = \langle f, \sin(nx) \rangle$ en $c_n = \langle f, \cos(nx) \rangle$.

e. Bereken a, b_1, b_2, c_1 en c_2 van de Fourierreeks van de volgende functies (met behulp van je GR) en vergelijk met de antwoorden gevonden bij opgave 2.

- a. $f(x) = x^2 - x - 1$.
- b. $f(x) = e^x$.

Fouriertransformaties hebben tal van toepassingen in het dagelijks computerleven. Bijvoorbeeld in geluids- en beeldverwerking. Quantum Fouriertransformaties zijn ook een essentiële stap in het algoritme van Shor, waarmee grote getallen kunnen worden ontbonden in priemfactoren. Je begrijpt dat de bancaire sector en internet giganten in dit vakgebied belangrijke spelers zijn.

5. werkbladen

5.1 Proef van Young 1

De opstelling wordt gebouwd op een T-vormig plankje. Aan de achterkant wordt een rode laserpen gemonteerd. Aan de voorkant kan een visitekaartje in een sleuf heen en weer geschoven worden. In het visitekaartje zitten drie spleetpatronen. De spleten hebben telkens dezelfde breedte (0,1 mm), maar staan op verschillende afstand. Het linker patroon is een enkele spleet, in het midden een dubbelspleet (hartafstand 0,3 mm). Het rechter patroon heeft een heel kleine afstand tussen de spleten. We gebruiken het rechter patroon niet in deze experimenten. De laser geeft voldoende licht om het experiment in een enigszins verduisterde ruimte uit te voeren.

- a. Schuif de visitekaart in de gleuf en belicht de enkelspleet. Het enkelspleetpatroon is zo'n 10 cm breed op 3 m afstand. Hang dit werkblad aan de muur en trek het intensiteitspatroon over. Er staat een hulplijntje voor de symmetrieas van het patroon.
- b. Meet de afstand tussen muur en spleetpatroon en noteer die in het vakje hiernaast. Verander de afstand niet meer.
- c. Belicht de dubbelspleet. Controleer of beide spleten evenveel licht doorlaten door een papiertje vlak achter de spleten te houden. Projecteer het dubbelspleetpatroon in het midden van het volgende vak van het werkblad. Trek het intensiteitspatroon weer over.

naam:

klas:

datum:

afstand tussen muur
en spleet:

enkelspleet

dubbelspleet

We hebben het enkel- en dubbelspleetexperiment uitgevoerd met telkens dezelfde spleetbreedte (0,1 mm). Om experimenten te vergelijken moet je beseffen welke onderdelen hetzelfde zijn gebleven en welke zijn veranderd.

- d. Wat zijn de overeenkomsten en verschillen in de opzet van de twee experimenten? Hoe vind je die terug in de resultaten, de patronen op de muur?

- e. Wat gebeurt er met het dubbelspleetpatroon als je één van de spleten afdekt?

- f. Waar op de muur moet ik twee lichtsensors plaatsen waarmee ik kan waarnemen of ik met een enkel- of met een dubbel-spleetexperiment te maken hebt?

- g. Teken in de intensiteitspatronen van het enkel- en dubbelspleetexperiment honderd (nu ja) losse fotonen die zouden bijdragen aan de opbouw van het patroon. Waar komen de meeste fotonen terecht, waar komen ze zeker niet?

5.2 Wet van Malus

Voor dit experiment [11] heb je nodig: een computer met een LCD scherm, een smartphone, een stukje polaroidfilter (2x4cm) en een oude sok of wat haarbandjes.

naam:

klas:

datum:

voorbereiding

- Installeer de app *physics toolbox Sensor Suite* op je telefoon (freeware versie).
- Zet een laptop scherm (geen touch-screen!) verticaal. Maak een wit scherm door bijvoorbeeld een tekstverwerker te openen met een blanco pagina.
- Kijk door het polaroidfilter naar het scherm en draai het filter rond. Je ziet het lichter en donkerder worden terwijl je draait.
- Zet in de app de lichtsensor even aan en vind uit waar de lichtsensor op je telefoon zit. Plak het polaroidfilter verticaal over de lichtsensor met een stukje plakband en zorg dat het filter een stukje uitsteekt. Je kunt dan tijdens de meting met het blote oog zien dat de polarisator zijn werk doet.

In physics toolbox moeten wat instellingen aangepast worden:



Physics Toolbox Sensor
suite

- Ga naar instellingen en selecteer 'langzaam bemonsteren' anders worden de files erg groot.
- In het sensormenu: kies voor 'multi'-opname en selecteer 'Intensiteit' en 'helling'. Helling levert drie meetwaarden (Aziëtum, Pitch en Roll). In het databestand bestaat elke regel uit een tijdstempel, intensiteit, en driemaal een hoek in graden. (Pitch = stampen in de NL versie).

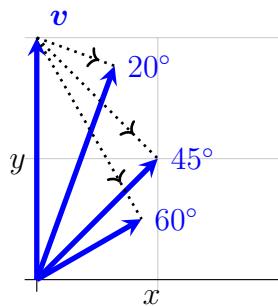
Uitvoering Doe een paar haarbandjes of een sok om de telefoon zodat de schermen niet krassen. Start de meting. Hou de telefoon tegen het scherm en draai deze langzaam volledig rond. Stop de meting en stuur het CSV bestand naar je computer.

Uitwerking Open het bestand in Excel. Bekijk de ruwe data. Zet in een grafiek de intensiteit tegen de tijd uit en selecteer het

geldige gebied voor de meting. (Je meet twee keer een maximum in de energie in één rondje.)

Voeg bovenaan een regel toe met in vakje A1 0 of 90 ingevuld, om te compenseren voor de polarisatierichting van het scherm (sommige schermen zijn horizontaal, andere juist verticaal gepolariseerd).

Voeg een berekende kolom toe waarin $\cos^2(pi()*(pitch+\$A\$1)/180)$ berekend wordt. Excel rekent in radialen dus dat moet je omzetten. Dat is in de formule al gebeurd. Maak een grafiek van de Intensiteit (y-as) tegen de berekende kolom (x-as). Varieer de parameter in A1 ook in kleine stapjes. De juiste waarde van A1 levert je een rechte lijn door de oorsprong. Maak de grafiek netjes op en sla het resultaat op als .xlsx bestand.



Figuur 5.1: Projectie van de lichtvector op een draaiend polarisatie-filter. De amplitude van verticaal gepolariseerd licht neemt af met de cosinus van de hoek tussen de filters.

Interpretatie De lichtvector uit het scherm van de computer wordt geprojecteerd op de richting van het filter (zie fig. 5.1). Hier geldt een cosinus verband. Bij polarisatie wordt de *amplitude* van de lichtvector geprojecteerd op de richting van het filter. Licht is een trilling, en de energie van een trilling is evenredig met het kwadraat van de uitwijking. Vandaar de evenredigheid met $\cos^2(\theta)$:

$$I_\theta = I_0 \cos^2 \theta$$

Dit is de wet van Malus.

We weten dat licht is opgebouwd uit enkele fotonen. Wat betekent het voor één enkel verticaal gepolariseerd foton als het een filter nadert dat op 45° staat?

5.3 Proef van Young 2

We gebruiken weer de opstelling met het T-vormige plankje waarop de laser gemonteerd is. Licht van laserpennen is enigszins gepolariseerd. Bij de opstelling is een schuifje met twee loodrecht gemonteerde polarisatoren. Zet een van de filters in de bundel en draai de laser zo ver rond dat de afgebeelde lichtvlek het donkerst is. Draai de laser nu 45° . Controleer dat beide filters in het schuifje evenveel licht doorlaten. De laser staat nu goed afgesteld. Markeer de bovenkant van de laser.

naam:

klas:

datum:

- a. Leg het schuifje even opzij en stel de dubbelspleet in zoals je in experiment 5.1 hebt gedaan. Als het goed is kun je het patroon van de dubbelspleet reproduceren.
- b. Schuif het plaatje met de twee loodrechte polarisatieplaatjes ná de dubbelspleet. De fotonen gaan dus eerst door de dubbelspleet, en daarna door het filter. Het schuifje kun je heen en weer bewegen terwijl het visitekaartje op zijn plaats blijft. Dat wordt op zijn plaats gehouden door een stukje rubber. Plaats het schuifje zó, dat elk van de filters één spleet afdekt.
- c. Hang dit werkblad op dezelfde afstand als in experiment 5.1. Teken het intensiteitspatroon hieronder.

Dubbelspleet met gekruiste polarisatoren

Het patroon komt overeen met een enkelspleet patroon. Kun je deze waarneming verklaren met klassieke theorie (intensiteit van de bundels) en vanuit het gedrag van enkele fotonen?

- d. Neem nu een los vel polaroid en hou dat ergens tussen het apparaat en de afbeelding. Draai het rond. Bij 45° zie je het dubbelspleetpatroon herstellen. Trek het patroon over op het werkblad.

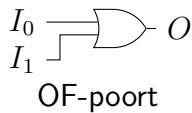
met extra polarisator op 45°

- e. Kun je dit verklaren met klassieke theorie (intensiteit van doorgelaten bundels)?

- f. Neem de stappen van het experiment door alsof het met één foton tegelijk wordt uitgevoerd. Waar komt de interferentie dan vandaan?

5.4 Klassieke bits

Informatie verwerk je met logische poorten. Enkele zijn hieronder weergegeven met hun waarheidstabellen:



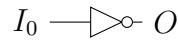
OF-poort

I_1	I_2	O
0	0	0
0	1	1
1	0	1
1	1	1



EN-poort

I_1	I_2	O
0	0	0
0	1	0
1	0	0
1	1	1



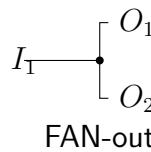
NOT-poort

I_0	O
0	1
1	0

naam:

klas:

datum:

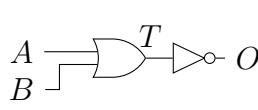


FAN-out

I_0	O_1	O_2
0	0	0
1	1	1

Figuur 5.2: logische poorten en fan-out.

De fan-out wordt doorgaans niet expliciet vermeld. In feite gaat het hier om het kopiëren van een bit. Hier ligt een belangrijk verschil liget tussen klassieke en quantumcomputers. Bij quantumcomputing is kopiëren niet mogelijk. De fan-out maakt het mogelijk ingewikkelde uitdrukkingen maken door poorten te verbinden. Een simpele uitbreiding zie je in figuur 5.3.



A	B	T	O
0	0	0	1
0	1	1	0
1	0	1	0
1	1	1	0

Figuur 5.3: Een OF-poort en een NOT-poort levert een NEN (niet-en) poort. In de notatie geeft een klein bolletje een NOT poort aan.

Als het ingewikkeld wordt kun je voor tussenstappen een waarheidstabellen opzetten. Zo is het resultaat van de OF-poort in stap

T weergegeven. Op T is een NOT toegepast. Het resultaat is in kolom O weergegeven.

De vier getekende poorten in figuur 5.2 vormen een **universele set**. Dat wil zeggen dat alle andere denkbare logische uitdrukkingen gesimuleerd kunnen worden met behulp van deze vier poorten.



universele set

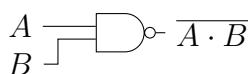
algebra In een algebraïsche notatie schrijven we ‘·’ voor EN, en ‘+’ voor OF. De NOT operatie geef je aan met een streep boven het deel van de uitdrukking dat ontkent moet worden.

Er geldt:

$$\overline{A \cdot B} = \overline{A} + \overline{B}$$

en

$$\overline{A + B} = \overline{A} \cdot \overline{B}$$



Figuur 5.4: Een NEN-poort is samentrekking van een EN en een NOT poort.

Deze uitdrukkingen staan bekend als de stellingen van DeMorgan. Aan de linkerkant van de eerste uitdrukking staat een uitdrukking voor een NEN-poort. Met NOT poorten kunnen we hiermee OF en EN poorten in elkaar overzetten.

- a. Controleer de eerste stelling van DeMorgan met een waarheidstabell en teken hiervan een schema.

We kunnen een complete set maken met alleen NEN-poorten (of alleen NOF-poorten). Omdat we maar één poort gebruiken heet deze set een minimale universele set. Kun je een reden bedenken waarom een chipfabrikant slechts één poort wil gebruiken in een ontwerp?



uitleg

Als we bewijzen dat we de bewerkingen NOT, EN, en OF kunnen realiseren met enkel NEN-poorten, dan hebben we aangetoond dat NEN poorten een minimale universele set vormen. We gebruiken wel de fan-out. Hier een **uitleg** op video. In de opdrachten ga jij aantonen dat ook NOF poorten een minimale universele set vormen.

De NOT operatie: $NOT(A) \rightarrow \overline{A}$

We kopiëren A en zetten die op beide ingangen van een NEN poort:

$$\overline{A} = \overline{A \cdot A}$$

De EN operatie: $EN(A, B) \rightarrow A \cdot B$

$$A \cdot B = \overline{\overline{A} \cdot \overline{B}} = \overline{\overline{A} \cdot \overline{B} \cdot \overline{A} \cdot \overline{B}}$$

De OF operatie: $OR(A, B) \rightarrow A + B$

$$A + B = \overline{\overline{A}} + \overline{\overline{B}} = \overline{\overline{A} \cdot \overline{B}}$$

b. Teken de schema's van deze uitdrukkingen.

Ook de NOF-poort is een minimale universele set.

c. Druk de NOT, OF en EN poort uit in alleen NOF-poorten.

5.5 Wat zie je?



naam:

klas:

datum:

Figuur 5.5: Oude vrouw jonge vrouw.

eerste deel Zorg dat je een notitieblaadje hebt en een pen in de aanslag. Kijk naar de afbeelding in figuur 5.5. Je ziet af en toe een jonge vrouw, en af en toe een oude vrouw. Wen er even aan.

Je gaat gedurende 60 s het wisselen waarnemen. Als je docent 'nu' zegt turf je een 'J' of een 'O', afhankelijk welk beeld je op dat moment ziet.

Noteer in de eerste regel in de tabel hieronder het aantal keren dat je 'jonge vrouw' en 'oude vrouw' geturf'd hebt in de tabel.

Iemand verzamelt de gegevens van alle leerlingen in een spreadsheet tabel en telt de totalen op. In het tweede deel verwerk je de data op dit blad, maar eerst bestuderen we de rest van paragraaf 2.2.

	jong	oud		jong	oud
jouw waarnemingen			klas (totaal)		
kans			kans		
amplitude			amplitude		

tweede deel Nu je de gegevens hebt verzameld en kansen en amplitudes hebt berekeend (tabel) kunnen we met onze persoonlijke resultaten onze eigen toestandsvector $|\Psi\rangle$ tekenen. Daarin stel je

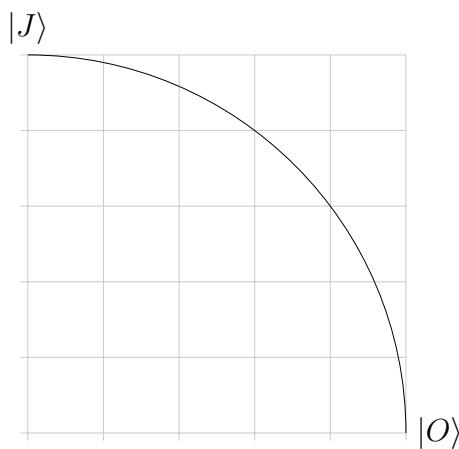
de coëfficiënten op van de toestand

$$|waarneming\rangle = a|O\rangle + b|J\rangle$$

uit je eigen meting.

In figuur 5.6 vind je een diagram waarin je kunt aangeven hoeveel oude en hoeveel jonge vrouw je hebt waargenomen.

Bereken de coördinaten van jouw waargenomen 'toestandsvector' (W) en die van het klassengemiddelde (K) en teken beide in het diagram.



Figuur 5.6: Teken hier je eigen toestandvectoren van jouw (W) en het klassengemiddelde (K).

Noem enkele redenen waarom dit experiment een model voor quantum kan zijn. Noem ook enkele manco's. Denk aan de experimenten in hoofdstuk 1.

5.6 Werken op een quantumcomputer

We rekenen het voorbeeld 3.1 uit op de quantum computer Quantum Inspire in Delft. Wat is de uitkomst van $\mathbf{XHZX}|0\rangle$?

In deze opdracht ga je zelf een quantumcomputer programmeren. We maken gebruik van de quantumcomputer van Delft: Quantum Inspire. Nu ja, als gast gebruik je gebruik je een simulatieprogramma. Wil je echt op de quantumcomputer dan kun je een account aanmaken. Voor deze opdracht is dat niet nodig. In figuur 5.7 is een screenshot te zien van het programma voor je eerste opdracht.

```

1 version 1.0
2 qubits 1
3
4 {prep_x q[0] }
5
6 X q[0]
7 Z q[0]
8 H q[0]
9 X q[0]
10
11 measure q[0]

```

Figuur 5.7: De editor van de quantum-computer van Delft. Een programma kun je "runnen"(laten lopen). Daarna wordt je gevraagd om het aantal shots te kiezen.

- a. Ga naar de website van [Quantum Inspire](#). Je krijgt een scherm met oranje-rode kleuren.
- b. Klik rechtsboven de Knowledge base aan.
- c. Links vind je de quick guide met het onderdeel *working with the editor* : klik aan.
- d. Even scrollen en je ziet een voorbeeld met rechtsboven open the editor: klik aan. [via deze link](#)
- e. Je bent nu in de editor met een programma dat al werkt.
- f. Pas het programma aan zodat het overeenkomt met figuur 5.7.
- g. Run het en zorg voor 1000 shots,
- h. Bekijk de resultaten: voldoen ze aan je verwachting?
- i. Herhaal de hele procedure voor een andere reeks poorten, bijvoorbeeld $\mathbf{XHXHX}|0\rangle$

5.7 Teleportatie

In science fiction komt teleportatie veelvuldig voor. Veelal wordt er een machine gebruikt die een persoon ergens laat verdwijnen en vervolgens op een totaal andere locatie laat verschijnen. Bij quantum teleportatie worden geen voorwerpen geteleporteerd, maar de informatie van een qubit; door slim gebruik te maken van verstrekking, wordt bij teleportatie een qubit op plek A gemeten, verdwijnt de informatie en wordt het qubit op plaats B gereconstrueerd, zonder het qubit daadwerkelijk naar plaats B te sturen.

- a. Als je een qubit meet die in de toestand $\alpha|0\rangle + \beta|1\rangle$ is, wat is dan de uitkomst van de meting?
 - A 0
 - B 1
 - C 0 met kans $|\alpha|^2$ en 1 met kans $|\beta|^2$
 - D 0 met kans $\sqrt{\alpha}$ en 1 met kans $\sqrt{\beta}$.
- b. Wat gebeurt er als je een verstrekkelde qubit uit de toestand $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ meet?
 - A De uitkomst van de qubits is altijd tegengesteld: als jij $|0\rangle$ meet, zal de andere qubit altijd $|1\rangle$ zijn.
 - B De uitkomst van de qubits is altijd gelijk als jij $|0\rangle$ meet, zal de andere qubit altijd $|0\rangle$ zijn.
 - C Je meet altijd $|00\rangle$
 - D Je meet altijd $|11\rangle$
- c. Kun je van een onbekende toestand $\alpha|0\rangle + \beta|1\rangle$ met een enkele meting de exacte toestand leren kennen (dus α en β bepalen)? Waarom wel/niet?
- d. Wanneer dit niet kan, kun je dan een manier bedenken om de toestand te bepalen?

naam:

klas:

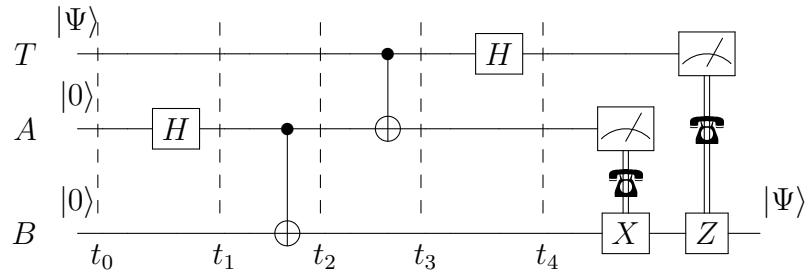
datum:

Quantum teleportatie is een techniek om een *onbekende* qubit toestand van A naar B te verplaatsen, zonder het qubit zelf te verplaatsen. Omdat qubits niet gekopieerd kunnen worden, zal het qubit informatie op plaats A verdwijnen. Het qubit zelf is er natuurlijk nog wel, maar zal in een andere toestand zijn.

Voor het teleportatieprotocol heb je drie qubits nodig: het qubit waarvan je de toestand wilt teleporteren, laten we deze qubit T noemen en twee qubits die worden verstrekeld.

Alice wil graag een boodschap overbrengen aan Bob, die ver weg zit, zonder fysiek iets te versturen. Alice en Bob gaan eerst samen

twee qubits verstrekken. Met A en B geven we aan welk qubit van Alice en welk van Bob is. Daarna gaat Bob op reis en neemt zijn helft van het verstrekkelde qubitpaar mee. Alice heeft informatie verstoopt in de toestand van een qubit; T . T kan elke willekeurige toestand zijn, laten we zeggen $T = \alpha |0\rangle + \beta |1\rangle$. We bekijken stap voor stap hoe Alice de toestand van T kan overbrengen zonder het qubit daadwerkelijk te versturen. We gebruiken daarvoor het schema in figuur 5.8.



Figuur 5.8: Quantumcircuit voor teleportatie. Er zijn drie qubits, in registers $|TAB\rangle$. Aan het eind meet Alice qubits $|T\rangle$ en $|A\rangle$, zij geeft de uitkomst met een klassieke telefoonlijn (dubbele lijn) door aan Bob, die al dan niet een **X** en een **Z**-poort toepast.

Let op, je mag kets binnen en buiten haakjes halen, maar je mag **nooit** de volgorde veranderen.

t=t₀: We beginnen met een qubit $T = \alpha |0\rangle + \beta |1\rangle$, en Alice en Bob hebben allebei een qubit in toestand $|0\rangle$. Met het tensorproduct kunnen we ze schrijven als

$$|T\rangle \otimes |A\rangle \otimes |B\rangle = |TAB\rangle = (\alpha |0\rangle + \beta |1\rangle) |00\rangle = \alpha |000\rangle + \beta |100\rangle$$

papegaaienbekken:

$$(a+b)(c+d) = ac + ad + bc + bd$$

t=t₁: Als eerste gaat qubit A door een **H**-poort:

$$\begin{aligned} T \otimes \mathbf{H} |A\rangle |0_B\rangle &= \\ T \otimes \frac{|0_A\rangle + |1_A\rangle}{\sqrt{2}} |0_B\rangle &= \\ (\alpha |0_T\rangle + \beta |1_T\rangle) \otimes \left(\frac{1}{\sqrt{2}} |0_A0_B\rangle + \frac{1}{\sqrt{2}} |1_A0_B\rangle \right) \end{aligned}$$

Nu zelf aan de slag: Werk de haakjes weg (papegaaienbekken). Dit levert vier termen met kets die elk een T, een A en een B component bevatten. Zorg dat de volgorde van de qubits in de termen telkens

T,A,B blijft. De termen staan er al. Schrijf de factoren op de plaats van de puntjes.

$$\dots |0_T 0_A 0_B\rangle + \dots |0_T 1_A 0_B\rangle + \dots |1_T 0_A 0_B\rangle + \dots |1_T 1_A 0_B\rangle$$

t=t₂ Alice past een **CNOT**-poort toe op A en B. A is hierbij het controlebit en B het doel. Een CNOT laat het doel onveranderd als het controlebit 0 is, en flippt het doel als het controlebit 1 is. De qubits A en B zijn nu verstrengeld. Bob gaat op reis en neemt zijn register mee. Bereken de toestandt op t₂:

t=t₃: Alice past een **CNOT**-poort toe op haar twee qubits. T is hierbij het controlebit en A het doel. Bereken de toestandt op t₃:

t=t₄: Daarna haalt Alice qubit T door een Hadamard poort. Pas werking van de H-poort: de **H**-poort toe op het eerste qubit bij alle vier de termen. De $\mathbf{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ eerste rekenen we voor. Werk zelf de andere drie uit: $\frac{\alpha}{2}(|0_T\rangle + \mathbf{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|1_T\rangle)|0_A 0_B\rangle \dots$

Als we de haakjes wegwerken ontstaan er acht ket-termen met drie qubits. We geven de eerste twee: $\frac{\alpha}{2} |0_T 0_A 0_B\rangle + \frac{\alpha}{2} |1_T 0_A 0_B\rangle \dots$

Wanneer we Alice's qubits apart opschrijven van Bobs qubits, krijgen we de toestand die begint met $\frac{\alpha}{2} |0_T 0_A\rangle |0_B\rangle + \frac{\alpha}{2} |1_T 0_A\rangle |0_B\rangle \dots$:

En door nu termen buiten haakjes te halen, krijgen we:

Alice	Bob
meet	heeft
$ 00\rangle$	$\alpha 0\rangle + \beta 1\rangle$
$ 01\rangle$	$\alpha 1\rangle + \beta 0\rangle$
$ 10\rangle$	$\alpha 0\rangle - \beta 1\rangle$
$ 11\rangle$	$\alpha 1\rangle - \beta 0\rangle$

$$\frac{1}{2} |0_T 0_A\rangle (\alpha |0_B\rangle + \beta |1_B\rangle) + \frac{1}{2} |1_T 0_A\rangle (\alpha |0_B\rangle - \beta |1_B\rangle) +$$

$$\frac{1}{2} |0_T 1_A\rangle (\alpha |1_B\rangle + \beta |0_B\rangle) + \frac{1}{2} |1_T 1_A\rangle (\alpha |1_B\rangle - \beta |0_B\rangle)$$

Klopt dit met jouw tussenberekeningen?

Nu meet Alice haar beide qubits. Er zijn vier mogelijke uitkomsten ($|0_T 0_A\rangle$, $|0_T 1_A\rangle$, $|1_T 0_A\rangle$ en $|1_T 1_A\rangle$) die elk overeenkomen met een unieke toestand van Bob's qubit. Die toestand is een simpele transformatie van het originele qubit T. De mogelijke toestanden staan in tabel 5.9.

Figuur 5.9: Alice' metingen en de toestand van Bob's ontvangen qubit T.

Als Alice $|00\rangle$ meet heeft Bob gelijk de goede qubit te pakken. Als Alice een andere combinatie meet, dan moet Bob nog een of twee rotaties op zijn qubit uitvoeren. Met welke operaties (gebruik **X**, **H** en **Z**) kan Bob zijn ontvangen qubit terugbrengen tot de toestand $\Psi = \alpha|0\rangle + \beta|1\rangle$? Schrijf je antwoord in de register notatie als Alice de volgende toestanden meet:

- e. $|00\rangle$ -I-
- f. $|01\rangle$ _____
- g. $|10\rangle$ _____
- h. $|11\rangle$ _____

Bob is inmiddels ver weg. Zijn register bevat qubit T, maar in een versleutelde vorm. Hij weet natuurlijk niet wat Alice gemeten heeft. Alice moet Bob op de hoogte brengen van haar bevindingen. Dit kan via een klassiek kanaal, bijvoorbeeld per mail, of via de telefoon. Dit betekent dat Alice en Bob geen toestand kunnen teleporteren zonder contact met elkaar te hebben. De wet dat niets sneller kan gaan dan het licht, is dus niet verbroken.

De kern van het teleportatieprotocol is dat Alice de toestand T niet hoeft te kennen (zelfs niet mag kennen!) om deze te teleporteren naar Bob. Bovendien kan Alice een qubit toestand naar Bob versturen zonder gebruik te maken van een quantum kanaal. De enige communicatie die Alice en Bob gebruiken is de telefoon (of mail) en dus klassiek!

- i. Waarom zou iemand kunnen denken dat je sneller dan de lichtsnelheid kunt teleporteren? Leg uit waarom dit hier niet het geval is.
- j. Denk je dat je een fysiek object, zoals een lamp, of een persoon kunt teleporteren? Waarom wel/niet?
- k. Stel nou dat Alice en Bob niet de verstrengelde toestand $\frac{|0_A0_B\rangle+|1_A1_B\rangle}{\sqrt{2}}$ delen, maar in plaats daarvan de toestand $\frac{|0_A1_B\rangle+|1_A0_B\rangle}{\sqrt{2}}$. Hoe werkt het teleportatie protocol dan? Schrijf het protocol voor jezelf uit. Werk systematisch analoog aan het protocol van dit werkblad.

Literatuur

- [1] URL: https://en.wikipedia.org/wiki/Timeline_of_quantum_computing_and_communication.
- [2] URL: <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/brochures/2020/02/17/nationale-agenda-quantumtechnologie/Nationale+Agenda+Quantumtechnologie.pdf>.
- [3] Charles H. Bennett en Gilles Brassard. „Quantum cryptography: Public key distribution and coin tossing”. In: *Theoretical Computer Science* 560 (2014). Theoretical Aspects of Quantum Cryptography - celebrating 30 years of BB84, p. 7–11. ISSN: 0304-3975. DOI: <https://doi.org/10.1016/j.tcs.2014.05.025>. URL: <http://www.sciencedirect.com/science/article/pii/S0304397514004241>.
- [4] David P DiVincenzo. „The physical implementation of quantum computation”. In: *Fortschritte der Physik: Progress of Physics* 48.9-11 (2000), p. 771–783.
- [5] A. Einstein, B. Podolsky en N. Rosen. „Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?” In: *Phys. Rev.* 47 (10 mei 1935), p. 777–780. DOI: [10.1103/PhysRev.47.777](https://doi.org/10.1103/PhysRev.47.777). URL: <https://link.aps.org/doi/10.1103/PhysRev.47.777>.
- [6] Richard P Feynman. „Simulating physics with computers”. In: *Int. J. Theor. Phys.* 21.6/7 (1982).
- [7] I. M. Georgescu, S. Ashhab en Franco Nori. „Quantum simulation”. In: *Reviews of Modern Physics* 86.1 (mrt 2014), p. 153–185. ISSN: 1539-0756. DOI: [10.1103/revmodphys.86.153](https://doi.org/10.1103/revmodphys.86.153). URL: <http://dx.doi.org/10.1103/RevModPhys.86.153>.

- [8] W. E. Hill. *My wife and my mother-in-law*. 1915. URL: [https://commons.wikimedia.org/wiki/File:My_Wife_and_My_Mother-In-Law_\(Hill\).png](https://commons.wikimedia.org/wiki/File:My_Wife_and_My_Mother-In-Law_(Hill).png).
- [9] Charles C Mann. *The wizard and the prophet: Two groundbreaking scientists and their conflicting visions of the future of our planet*. Picador, 2018.
- [10] N David Mermin. „Is the moon there when nobody looks? Reality and the quantum theory”. In: *Physics today* 38.4 (1985), p. 38–47.
- [11] Martín Monteiro e.a. „The polarization of light and Malus' law using smartphones”. In: *The Physics Teacher* 55.5 (2017), p. 264–266.
- [12] John von Neumann. 2021. URL: https://nl.wikipedia.org/wiki/Von_Neumann-architectuur.
- [13] William K Wootters en Wojciech H Zurek. „A single quantum cannot be cloned”. In: *Nature* 299.5886 (1982), p. 802–803.