Pieter Naaijkens
IMAPP
Radboud Universiteit Nijmegen
Postbus 9010
6500 GL Nijmegen
p.naaijkens@math.ru.nl

Onderzoek

Topologische kwantumcomputers: rekenen met vlechten

Topologische kwantumcomputers bieden een alternatief voor meer gebruikelijke modellen van kwantumcomputers, die in de praktijk met grote technische moeilijkheden kampen. Topologische kwantumcomputers gebruiken topologische eigenschappen van bepaalde kwantumsystemen om berekeningen te doen. Pieter Naaijkens, promovendus in Nijmegen, laat zien dat zulke systemen op een elegante manier kunnen worden beschreven door modulaire categorieën.

Kwantumcomputers gebruiken de wetten van de kwantummechanica om berekeningen te doen. Het idee van een kwantumcomputer gaat terug tot begin jaren '80. De wiskundige Manin [16] (pp. 69–79) en de fysicus Feynman [5] vroegen zich onafhankelijk van elkaar af of het mogelijk was om de wetten van de kwantummechanica te gebruiken om kwantumsystemen te simuleren. Dit soort simulaties zijn op een gewone computer niet te doen vanwege de computationele complexiteit. Een natuurlijke vraag is dan of omgekeerd kwantummechanica gebruikt kan worden om grote berekeningen te doen. Dit is precies wat een kwantumcomputer doet. Er wordt gebruik gemaakt van kwantummechanische effecten om operaties uit te voeren die in een gewone computer niet mogelijk zijn, zoals het rekenen met superposities van toestanden.

David Deutsch gaf in 1985 een meer concrete vorm aan het idee van een kwantumcomputer [4]. Hij introduceerde een model voor kwantumcomputers en beschreef een 'universele kwantumcomputer', een computer waarop in principe elk kwantumalgoritme uitgevoerd kan worden. De interesse kwam echter pas goed op gang toen Shor een algoritme voor een kwantumcomputer publiceerde waarmee getallen gefactoriseerd kunnen worden [28]. Dit algoritme is veel efficiënter, in termen van het aantal benodigde operaties, dan de bekende 'klassieke' algoritmes.

In de praktijk is het nog niet mogelijk gebleken om iets anders dan de simpelste kwantumcomputers, bijvoorbeeld eentje die het getal 15 kan factoriseren [30], te bouwen. Een groot probleem bij het realiseren van ingewikkeldere kwantumcomputers is dat de systemen erg gevoelig zijn voor interactie met de omgeving, hetgeen leidt tot *decoherentie*. Een van de voorstellen om dit probleem aan te pakken is om *topologische* eigenschappen van een systeem te gebruiken. Op deze manier hoopt men het systeem beter te kunnen beschermen tegen decoherentie. Dit kan gezien worden als een vorm van *hardware* foutcorrectie.

Veel van de literatuur over dit onderwerp is gericht op fysici. Hier richten we ons op de essentie van de achterliggende wiskunde. Eerst bekijken we de wiskundige formulering van een kwantumcomputer. In de volgende secties behandelen we zogenaamde *anyonen*, en hoe hiermee een kwantumberekening kan worden gedaan. Daarna wordt beschreven hoe de algebraïsche eigenschappen van anyonen gegeven worden door middel van een *modulaire tensorcategorie*. Tenslotte komt een eenvoudig model, dat van Fibonacci anyonen, aan bod.

De literatuur over kwantumcomputers is inmiddels erg uitgebreid. Voor de geïnteresseerde lezer geven we daarom aan het eind van het artikel een selectie uit de literatuur die als startpunt kan worden gebruikt voor meer informatie. Resultaten in dit artikel die zonder referentie worden vermeld, zijn terug te vinden in één van deze referenties.

Kwantumcomputers

De toestandsruimte van een kwantummechanisch systeem wordt beschreven door een (complexe) Hilbertruimte $\mathcal{H}$. Voor toepassingen op kwantumcomputers is het voldoende om te kijken naar het geval waar $\mathcal{H} = \mathbf{C}^2 \otimes \cdots \otimes \mathbf{C}^2 \cong \mathbf{C}^{2^n}$, voor zekere n. We zien elke tensorfactor $\mathbf{C}^2$ als een *qubit*, het kwantumanalogon van een bit. Om aan te sluiten bij de fysische literatuur, gebruiken we de Dirac notatie $|\psi\rangle$ voor een vector in $\mathcal{H}$. Een basis van de qubit wordt als $|0\rangle, |1\rangle$ genoteerd, om de analogie met bits te benadrukken. Een *toestand* in het systeem is dan een eenheidsvector (modulo fase) in $\mathcal{H}$, of equivalent, een projectie van rang 1. De basisvectoren $|0\rangle$ en $|1\rangle$ zijn doorgaans eigentoestanden van een vooraf gekozen observabele (zoals hieronder

beschreven), bijvoorbeeld de spin van een deeltje in de z-richting. De toestand van het systeem is in het algemeen een lineaire combinatie van deze basisvectoren. Dit is in feite wat kwantumcomputers zo krachtig maakt, omdat in een klassieke computer dit niet mogelijk is.

We kunnen informatie over de toestand verkrijgen door het meten van *observabelen*. Een observabele komt overeen met een zelfgeadjungeerde matrix werkend op de toestandsruimte. In de kwantummechanica is het, anders dan in de klassieke fysica, niet mogelijk om door metingen de oorspronkelijke toestand precies te achterhalen. Een meting zorgt ervoor dat het systeem instantaan in een *eigentoestand* van de gemeten observabele komt. Als $|\psi\rangle$ de toestand van het systeem is, en $|\chi\rangle$ een eigentoestand van de te meten observabele, bijvoorbeeld $|\chi\rangle = |0\rangle \otimes \cdots \otimes |0\rangle$, dan is de kans dat het systeem na meting naar de toestand $|\chi\rangle$ overgaat volgens de wetten van de kwantummechanica gelijk aan $|\langle\chi|\psi\rangle|^2$. Hier is $\langle\chi|\psi\rangle$ het inproduct van de twee toestandsvectoren in de Hilbertruimte [33]. Zoals eerder vermeld zijn de vectoren $|0\rangle$ en $|1\rangle$ over het algemeen eigenvectoren van een zekere observabele S. Een meting van deze observabele wordt ook wel een *meting in de computationele basis* genoemd. Als de toestand gegeven wordt door $|\psi\rangle = a|0\rangle + b|1\rangle$, met $|a|^2 + |b|^2 = 1$, levert zo'n meting 0 op met kans $|a|^2$ en 1 met kans $|b|^2$.

De uitkomst van een algoritme kan worden bepaald door een meting in de computationele basis van de toestand. De uitkomst van een algoritme is dus *probabilistisch*. De meeste algoritmes, zoals het factoriseren van getallen, geven het correcte antwoord met een bepaalde kans p. Door het algoritme een aantal keren te herhalen, kan het antwoord met grotere zekerheid vastgesteld worden. Zelfs als dit in ogenschouw wordt genomen, blijven sommige kwantumalgoritmes, zoals het ontbinden in priemfactoren, veel efficiënter dan hun klassieke tegenhangers.

Het systeem kan van een toestand $|\psi\rangle$ in een andere toestand $|\psi'\rangle$ overgaan door middel van *unitaire evolutie*. Dat betekent dat er een unitaire matrix U is [34], zodat

$$|\psi'\rangle = U|\psi\rangle.$$

We zullen de werking van een unitaire matrix op een vector ook wel een *unitaire operatie* noemen. Een unitaire operatie behoudt het inproduct op de Hilbertruimte, en in het bijzonder dus de norm van een vector.

Een *kwantumpoort* is nu een unitaire operatie werkend op één of twee qubits. Een belangrijke kwantumpoort is de *Hadamardpoort*. De bijbehorende unitaire matrix is

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Deze poort maakt het mogelijk om superposities van de basistoestanden te verkrijgen, bijvoorbeeld $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Bij een meting in de computationele basis is de kans op 0 als uitkomst gelijk aan de kans op 1 als uitkomst, namelijk $\frac{1}{2}$.

Een berekening op een kwantumcomputer bestaat uit drie stappen:

1. *Initialisatie*: breng het systeem in een bekende toestand, bijvoorbeeld $|\psi\rangle = |0\rangle \otimes \cdots \otimes |0\rangle$.
2. *Berekening*: het algoritme wordt uitgevoerd door het toepassen van unitaire operaties op de qubits.
3. *Meting*: bepaal de uitkomst door een meting te doen.

Hoe elke stap in de praktijk uitgevoerd kan worden, hangt af van het specifieke kwantumsysteem, en valt buiten het bereik van dit artikel.

Het belangrijkste voordeel van kwantumcomputers is *kwantumparallellisme*. Willen we op een klassieke computer een eigenschap van de grafiek van een functie weten, dan rest ons niets anders dan eerst elke waarde uit te rekenen. Op een kwantumcomputer kan dit in één stap. We laten dit zien in het eenvoudigste geval. Stel dat $f : \{0,1\} \to \{0,1\}$. Dan is het mogelijk om een unitaire operator U_f op $\mathcal{H} = \mathbf{C}^2 \otimes \mathbf{C}^2$ te vinden, zodat $U_f(|x\rangle \otimes |0\rangle) = |x\rangle \otimes |f(x)\rangle$, waarbij $x = 0, 1$. Met behulp van U_f is het dus mogelijk om de grafiek van f te bepalen. Maar we kunnen deze operator ook op een *superpositie* van de toestanden toepassen, bijvoorbeeld op $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$. Deze toestand kan met de Hadamardpoort verkregen worden. We vinden nu

$$U_f \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle \otimes |f(0)\rangle + |1\rangle \otimes |f(1)\rangle\right).$$

Met één operatie hebben we nu informatie over de grafiek van f gevonden.

In een algoritme voor een kwantumcomputer is in principe *elke* unitaire operatie toegestaan. Dit is in de praktijk niet realiseerbaar. Het blijkt echter voldoende te zijn om een manier te hebben om een willekeurige unitaire operatie te benaderen. Stel dat we een *eindige* verzameling $\mathcal{U}$ kwantumpoorten hebben. Zo'n verzameling heet *universeel*, als voor elke poort $U \in \mathcal{U}$, zijn inverse $U^* \in \mathcal{U}$, en de groep voortgebracht door deze poorten *dicht* ligt in $SU(2^n)$, de groep van complexe $2^n \times 2^n$ matrices met determinant 1 [35]. Deze conditie geeft aan dat we een operatie uit $SU(2^n)$ willekeurig dicht kunnen benaderen. Met deze voorwaarden geldt de volgende stelling:

Stelling 1 (Solovay-Kitaev). *Zij $\varepsilon > 0$ gegeven. Zij $\mathcal{U}$ een universele verzameling kwantumpoorten. Dan is er een c, zodanig dat er voor elke $V \in SU(d)$ een ε-benadering U, bestaande uit $O(\log^c(1/\varepsilon)$ poorten uit $\mathcal{U}$, is.*

De constante c kan op 4 geschat worden, maar verbeteringen hierop zijn mogelijk. De stelling geeft ook een algoritme om voor een willekeurige unitaire operatie V zo'n ε-benadering te vinden. Een toegankelijk bewijs en beschrijving van het algoritme is te vinden in [3]. In het algemeen is het erg lastig om te bewijzen dat een bepaalde verzameling universeel is. Desondanks zijn er wel enkele voorbeelden, bijvoorbeeld door de Hadamard-, de $\pi/8$- en de CNOT-poort te nemen. De $\pi/8$ poort [36] stuurt $|0\rangle$ naar $|0\rangle$ en $|1\rangle$ naar $e^{i\pi/4}|1\rangle$. De CNOT-poort U werkt op twee qubits: $U(|i\rangle \otimes |j\rangle) = |i\rangle \otimes |i \oplus j\rangle$, waar $i, j = 0, 1$ en $\oplus$ is optelling modulo 2.

Het is echter niet genoeg om een willekeurige unitaire operatie te kunnen benaderen. In de praktijk is het vaak onmogelijk om een universele poort $U \in \mathcal{U}$ exact uit te voeren. Dit introduceert nieuwe fouten in de berekening. Verder speelt het probleem van *decoherentie*. Interacties met de omgeving zorgen ervoor dat de toestand van het systeem verandert, zelfs als we geen operaties uitvoeren. In analogie met klassieke computers zijn er foutcorrectieprotocollen ontwikkeld die deze problemen ondervangen. Met behulp van deze methodes is het mogelijk om *fout-tolerante kwantumberekingen* te doen. Dit wil zeggen dat we elk algoritme willekeurig precies kunnen uitvoeren.

Stelling 2 (Drempelstelling). *Stel dat we een universele verzameling kwantumpoorten $\mathcal{U}$ hebben, zó dat de kans p dat een poort $U \in \mathcal{U}$ niet exact wordt uitgevoerd voldoet aan $p < p_{th}$. Dan zijn fout-tolerante kwantumberekeningen mogelijk.*

De meest optimistische schatting voor p_{th} is 10^{-3}, dit is echter in de praktijk nog verre van haalbaar. Het is mogelijk om een boven-

grens te geven voor het aantal kwantumpoorten dat in de fout-tolerante implementatie van het algoritme nodig is. Voor een kwantumcircuit bestaande uit $p(n)$ poorten en kans op fout $\varepsilon > 0$ wordt de bovengrens gegeven door

$$O(\text{poly}(\log p(n)/\varepsilon)p(n)),$$

waar poly een polynoom van vaste graad is. Dus het aantal poorten in een fout-tolerant kwantumcircuit hangt poly-logaritmisch af van het aantal poorten in het oorspronkelijke circuit.

Anyonen

Beschouw een kwantummechanisch systeem met n deeltjes. In ruimtedimensie 3 en groter gedragen deeltjes zich óf symmetrisch (*bosonen*) óf anti-symmetrisch (*fermionen*) onder verwisseling. In de beschrijving van hierboven betekent dat dat de toestand (een eenheidsvector) gelijk blijft, respectievelijk met -1 wordt vermenigvuldigd als we twee deeltjes omwisselen.

In 1971 toonden Laidlaw en Morette DeWitt aan dat het aantal mogelijkheden afhangt van de topologie van de klassieke configuratieruimte van ononderscheidbare deeltjes [13]. Deze topologische ruimte beschrijft de posities van de deeltjes, waarbij twee deeltjes niet op dezelfde plek kunnen zijn en de klassieke toestand niet verandert onder permutatie van de deeltjes. Leinaas en Myrheim bekeken in 1977 de situatie in *twee* ruimtedimensies [14]. In plaats van alleen een plus- of minteken, wordt de toestand dan met een willekeurige fasefactor $e^{i\theta}$ vermenigvuldigd. Wilczek gaf in 1982 de naam *anyon* (omdat 'elke waarde' is toegestaan) aan zulke deeltjes [32]. In plaats van een fasefactor kan ook een meer algemene unitaire transformatie mogelijk zijn. In dit geval kan het uitmaken in welke volgorde anyonen worden verwisseld. Men spreekt dan van *niet-abelse anyonen*.

De reden dat er in twee ruimtedimensies meer mogelijkheden zijn, is topologisch van aard. Beschouw, om dit in te zien, een aantal deeltjes in het vlak (Figuur 1). De posities van de anyonen vormen een pad in de ruimte-tijd, de zogeheten *wereldlijnen*. In de figuur zijn de wereldlijnen van de deeltjes getekend: bovenaan de positie van de deeltjes op $t = 0$, en onderaan op $t = 1$. Ze vormen zo een *vlecht*. Het punt is nu dat er twee *verschillende* manieren zijn om twee deeltjes om te wisselen. De vlecht links in de figuur is topologisch anders dan de vlecht in het midden. Als we van de ene vlecht naar de andere willen, zullen de wereldlijnen op een zeker punt moeten kruisen. Dit betekent echter dat de deeltjes botsen, wat niet is toegestaan. In meer ruimtedimensies is dit niet meer het geval [37]. Twee keer deeltje 1 en 2 omwisselen (of equivalent: het ene deeltje rondom het andere deeltje bewegen), moet dan gelijk zijn aan de identieke operatie. Hieruit volgt het onderscheid in bosonen en fermionen.

In twee dimensies zijn er dus a priori meer mogelijkheden. Het verwisselen van twee anyonen heeft als effect dat de toestand vermenigvuldigd wordt met een fasefactor $e^{i\theta}$, of algemener, de toestand gaat met een unitaire transformatie over in een nieuwe toestand. Stel dat het systeem in een toestand $|\psi\rangle$ is. Schrijf σ_1 voor het verwisselen van de anyonen op positie 1 en 2, en σ_2 voor het verwisselen van de anyonen op positie 2 en 3, et cetera. Bij elke σ_i, hoort dan een unitaire operatie $\pi(\sigma_i) = U_i$, zodat het systeem van toestand $|\psi\rangle$ naar $U_i|\psi\rangle$ overgaat. Schrijf $\sigma_2\sigma_1$ voor het eerst uitvoeren van σ_1 en dan σ_2. Het is dan duidelijk dat moet gelden

$$\pi(\sigma_2\sigma_1)|\psi\rangle = U_2U_1|\psi\rangle = \pi(\sigma_2)\pi(\sigma_1)|\psi\rangle.$$

Dit levert een *unitaire representatie van de vlechtgroep* op. De vlechtgroep B_n wordt voortgebracht door voortbrengers $\sigma_1, \dots \sigma_{n-1}$ en de Artin relaties: $\sigma_i\sigma_j = \sigma_j\sigma_i$ als $|i-j| \geq 2$, en $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$. Als de representatie abels is, spreken we van *abelse anyonen*.

De uiteindelijke toestand hangt alleen van de vlecht en de begintoestand af. Dit is de reden dat topologische kwantumcomputers beter beschermd zijn tegen invloeden van buitenaf. Een kleine verstoring in het systeem kan er voor zorgen dat de anyonen een iets ander pad volgen, maar de vlecht blijft topologisch hetzelfde. Het probleem dat poorten met een kans p niet exact worden uitgevoerd kan hiermee worden ondervangen. Men kan dan de vervlechtingsoperaties gebruiken als (deel van) de verzameling kwantumpoorten $\mathcal{U}$.

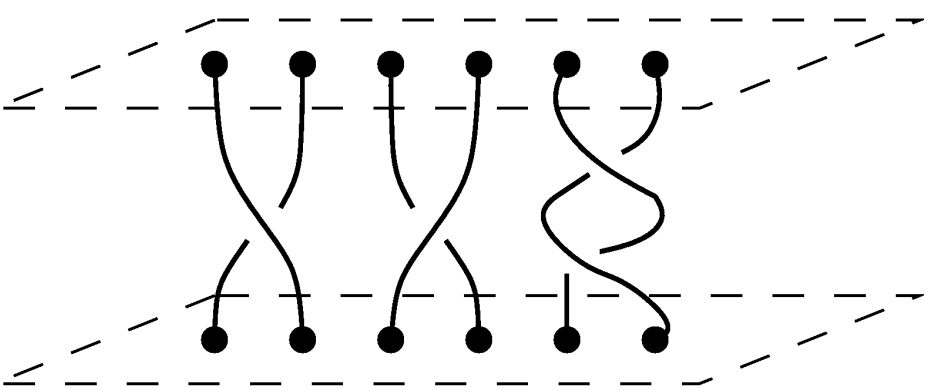
Een topologische kwantumcomputer

Het idee van een topologische kwantumcomputer gaat terug naar Freedman [6] en Kitaev [12]. De aanpak van Freedman gaat via topologische kwantumveldentheorie, zie [7] voor een introductie. Kitaevs aanpak gebruikt de eigenschappen van systemen met anyonen. Hij betoogt ook dat de topologische aard van anyonen zorgt voor goede eigenschappen met betrekking tot foutvrije berekeningen. De twee aanpakken liggen dichter bij elkaar dan op het eerste gezicht lijkt, zie bijvoorbeeld [27]. In beide gevallen zijn modulaire categorieën, zoals hieronder beschreven, belangrijk.

De gedachte is dan om een systeem met anyonen te gebruiken om berekeningen mee te doen. Volgens de beschrijving hierboven zijn er drie stappen noodzakelijk. Het moet mogelijk zijn om het systeem in een bekende begintoestand te brengen, we moeten door middel van unitaire operaties de toestand kunnen veranderen, en tenslotte moet er een manier zijn om het resultaat uit te lezen door middel van een meting.

Ten eerste de belangrijkste stap: het uitvoeren van kwantumalgoritmes. Het cruciale punt is dat door het vervlechten van anyonen de toestand van het systeem door middel van een unitaire transformatie overgaat in een nieuwe toestand. Stap 2 uit de beschrijving van een kwantumcomputer hierboven kan dus uitgevoerd worden door het vervlechten van anyonen.

Om weer elk kwantumalgoritme te kunnen implementeren, moet elke unitaire operatie op de toestandsruimte willekeurig goed benaderd kunnen worden. Er zijn in dit geval twee verschillende aanpakken. In de ene gebruikt men systemen waar de vervlechtingen elke unitaire operatie kunnen benaderen. Wiskun-



Figuur 1 Een vervlechting van 6 anyonen. Dit is de vlecht $\sigma_1\sigma_3^{-1}\sigma_5^2$, waarbij $\sigma_i, i = 1 \dots 5$ de generatoren van de vlechtgroep B_6 zijn.

dig gezien betekent dit dat representatie dicht ligt in $U(d)$, waarbij d de dimensie is van de toestandsruimte. In specifieke modellen is dit vaak erg lastig om te bewijzen, desalniettemin zijn er wel enkele resultaten in die richting. Freedman, Larsen en Wang bijvoorbeeld hebben dit aangetoond voor bepaalde representaties die voorkomen in de topologische Chern-Simons theorie [8]. Als eenmaal bewezen is dat de representatie dicht ligt, kunnen we met behulp van de Solovay-Kitaev stelling bij een unitaire operatie de bijbehorende vervlechting vinden die deze operatie benadert.

Als de representatie van de vlechtgroep niet dicht ligt, zal een aantal operaties moeten worden toegevoegd, die samen met de vervlechtingen dicht liggen in de unitaire groep. Een voorbeeld hiervan zijn modellen gebaseerd op de kwantumdubbel $D(G)$ van bepaalde eindige groepen [17]. Deze aanpak sluit aan bij de oorspronkelijke aanpak van Kitaev.

Om de initialisatie en uitlezing van een topologische kwantumcomputer te beschrijven, is het noodzakelijk om te weten hoe we informatie kunnen opslaan in een systeem met anyonen. Met andere woorden, wat is het analogon van een qubit? Abstract gezien verandert er weinig: de toestandsruimte is weer een Hilbertruimte, waarin we een geschikte basis kunnen kiezen. We kunnen echter wat concreter zijn door het begrip *fusie* te introduceren.

Als we twee anyonen bij elkaar brengen, kunnen deze fuseren. De *fusieregels* geven aan welke mogelijkheden er zijn. Door twee deeltjes te laten fuseren, en het resultaat te meten, kunnen we informatie krijgen over de berekening. We gaan hier later iets dieper op in.

Samenvattend kan gesteld worden dat het mogelijk is om kwantumberekeningen te doen met behulp van topologische eigenschappen van een systeem. Om aan te geven wat de voordelen zijn ten opzichte van de 'conventionele' kwantumcomputers, komen we terug op het probleem van decoherentie. In een topologische kwantumcomputer worden kwantumpoorten uitgevoerd door het vervlechten van anyonen, een operatie die alleen van de topologie van de vlecht afhangt. Een kleine verstoring levert (topologisch gezien) dezelfde vlecht op, en dus dezelfde operatie. Stel dat één van de operaties het roteren van een basisvector over 90° is. In tegenstelling tot in een 'conventionele' kwantumcomputer, is het hier niet mogelijk dat we iets te ver door roteren.

Er zijn nog andere factoren van belang, behalve het uitvoeren van de kwantumpoorten. Door thermische fluctuaties bijvoorbeeld, kunnen anyon-antianyon paren ontstaan, die de berekening beïnvloeden. Ook hiervoor kan beargumenteerd worden dat onder gunstige omstandigheden, deze invloeden miniem zijn [12].

Modulaire tensorcategorieën

De structuur van anyonen kan puur algebraïsch beschreven worden door een *modulaire tensorcategorie* (MTC) [1, 9, 29]. Dit is in essentie de structuur die er achter topologische kwantumcomputers verborgen zit. Aan de andere kant komen MTC's ook in andere gebieden van de wiskunde voor, bijvoorbeeld bij representaties van kwantumgroepen, invarianten van 3-variëteiten en topologische kwantumveldentheorie [9, 29]. Dit leidt tot interessante verbanden tussen op het oog zeer verschillende vakgebieden. Aan de andere kant zijn er systemen die een onderliggende structuur van een MTC hebben. Deze leveren mogelijk nieuwe kandidaten op voor topologische kwantumcomputers. Voor de duidelijkheid geven we niet de meest algemene definitie van een MTC, en laten we compatibiliteitseisen tussen de verschillende eigenschappen achterwege. De originele motivatie van Turaev, die als eerste een MTC definieerde, kwam uit de conforme veldentheorie.

Een categorie $\mathcal{C}$ bestaat uit een klasse *objecten*, en voor elk paar objecten X, Y een verzameling *morfismes* van X naar Y, $\mathrm{Hom}(X, Y)$. Als $f : X \to Y$ en $g : Y \to Z$ twee morfismes zijn, dan is er een samenstelling $g \circ f : X \to Z$. Deze samenstellingsoperatie is associatief. Verder is er voor elk object X een identiteitsmorfisme $\mathrm{id}_X \in \mathrm{Hom}(X, X)$.

Het standaardvoorbeeld is de categorie **Set**, met als objecten verzamelingen, en als morfismes functies tussen verzamelingen.

Als we $\mathcal{C}$ noteren voor de categorie die de anyonen gaat beschrijven, kunnen we intuïtief de objecten van $\mathcal{C}$ zien als verschillende configuraties van anyonen. De morfismen tussen twee objecten zijn dan de wereldlijnen van de anyonen, als de ene configuratie in de andere wordt overgebracht.

Behalve de basisstructuur van een categorie, is in een MTC een *tensorproduct* gedefinieerd. Dit is een zogeheten *bifunctor*: voor elk tweetal objecten X, Y is er een object $X \otimes Y$, evenzo is er een tensorproduct voor morfismen. Het tensorproduct voldoet aan een aantal eisen, zoals associativiteit [38]: $(X \otimes Y) \otimes Z = X \otimes (Y \otimes Z)$, voor alle X, Y, Z. Verder is er een eenheid $\mathbf{1}$, zodat $X \otimes \mathbf{1} = \mathbf{1} \otimes X = X$. In een *gevlochten* tensorcategorie is er voor elk paar objecten X, Y een isomorfisme $\varepsilon_{X,Y} \in \mathrm{Hom}(X \otimes Y, Y \otimes X)$. Zo'n vervlechting geeft aan wat er gebeurt als je twee objecten 'omwisselt'.

Definitie 3. *Zij $\mathcal{C}$ een gevlochten tensorcategorie. Het* centrum $\mathcal{Z}_2(\mathcal{C})$ *is de volle deelcategorie met objecten X [39], waarvoor geldt dat $\varepsilon_{X,Y} \circ \varepsilon_{Y,X} = \mathrm{id}_{Y \otimes X}$ voor alle objecten Y van $\mathcal{C}$.*

Een gevlochten tensorcategorie heet *symmetrisch* als $\mathcal{Z}_2(\mathcal{C}) = \mathcal{C}$. Het centrum is een maat voor hoe 'triviaal' de vervlechting is.

Een andere eigenschap is *rigiditeit*. Voor elk object X, is er een *duaal* object $\overline{X}$ [40], samen met morfismes $\mathbf{1} \to X \otimes \overline{X}$ en $\overline{X} \otimes X \to \mathbf{1}$. Het is mogelijk dat een object gelijk is aan zijn duale, in het bijzonder geldt $\overline{\mathbf{1}} \cong \mathbf{1}$. We eisen ook dat de categorie een *twist* heeft: voor elk object X een isomorfisme $\Theta_X \in \mathrm{End}(X) := \mathrm{Hom}(X, X)$. Deze twist maakt het mogelijk om X met zijn dubbele duale $\overline{\overline{X}}$ te identificeren. Fysisch komt de twist neer op rotatie van een aantal anyonen om een centrale as.

Definitie 4. *Een (strikte) rigide tensorcategorie met een twist heet een* lintcategorie *(Engels: ribbon category).*

Een belangrijke eigenschap van lintcategorieën is dat het mogelijk is om het spoor van een morfisme en de dimensie van een object in de categorie te definiëren. In de categorie van eindigdimensionale vectorruimtes, die een lintcategorie is, komen deze begrippen overeen met het spoor van een lineaire afbeelding, en de dimensie van een vectorruimte.

In de context van anyonen heeft de duale van een object een fysische interpretatie als het antideeltje van X. Het morfisme $\mathbf{1} \to X \otimes \overline{X}$ valt dan te interpreteren als het creëren van een deeltje/antideeltje paar uit het vacuüm. Het bijbehorende morfisme $\overline{X} \otimes X \to \mathbf{1}$ is dan niets anders dan het annihileren van het paar.

Tenslotte is er nog de lineaire structuur, in dit geval over het lichaam $\mathbf{C}$. Voor elk paar objecten X, Y is $\mathrm{Hom}(X, Y)$ een vectorruimte over $\mathbf{C}$. Verder eisen we dat samenstelling van morfismen bilineair is, evenals het tensorproduct. Het is ook mogelijk om *directe sommen* van objecten en morfismes te nemen, precies zoals we directe sommen van bijvoorbeeld Hilbertruimtes kunnen nemen. Dus, voor elk tweetal objecten X, Y is er een directe som $X \oplus Y$, met een overeenkomende operatie om de directe som van morfismes te nemen. In een tensorcategorie moet de tensoroperatie compatibel zijn met het nemen van directe sommen,

$$(X \oplus Y) \otimes Z \cong X \otimes Z \oplus Y \otimes Z.$$

In de categorie van anyonen beschrijft een directe som een samengesteld object opgebouwd uit eenvoudigere objecten.

Een object heet *irreducibel*, of *enkelvoudig*, als het niet op een niet-triviale manier te schrijven is als directe som van objecten. In de huidige situatie geldt een variant op Schurs Lemma: een object X is irreducibel, dan en slechts dan als $\mathrm{End}(X) \cong \mathbf{C}$. We eisen dat de eenheid $\mathbf{1}$ voor de tensoroperatie *irreducibel* is.

Een categorie heet *half-enkelvoudig*, ruwweg, als deze directe sommen heeft en elk object te schrijven is als een directe som van enkelvoudige objecten. Kiezen we voor elke equivalentieklasse van irreducibele objecten een representant X_k, dan geldt in een half-enkelvoudige tensorcategorie in het bijzonder

$$X_i \otimes X_j \cong \bigoplus_k N_{ij}^k X_k.$$

Hier zijn de N_{ij}^k positieve gehele getallen. Informeel geeft dit aan hoe vaak het object X_k voorkomt in het tensorproduct $X_i \otimes X_j$. Een bekend geval van deze situatie is de categorie van eindig-dimensionale unitaire representaties van een compacte groep G, $\mathbf{Rep}_f\, G$. Deze categorie is half-enkelvoudig: elke eindigdimensionale unitaire representatie kan als een directe som van irreducibele representaties geschreven worden.

Definitie 5. *Een* fusiecategorie *is een half-enkelvoudige, $\mathbf{C}$-lineaire categorie met eindigdimensionale* Hom*-sets, eindig veel, tot op isomorfisme, irreducibele objecten en irreducibele tensoreenheid $\mathbf{1}$. Tenslotte moet de categorie ook dualen hebben.*

Een fusiecategorie is dan een modulaire categorie, als de vervlechting *niet gedegenereerd* is. Dit houdt in dat het centrum $\mathcal{Z}_2(\mathcal{C})$ triviaal is.

Definitie 6. *Een* modulaire tensorcategorie *is een fusiecategorie die tevens een lintcategorie is, waarvoor geldt dat $\mathcal{Z}_2(\mathcal{C})$ triviaal is: de enige objecten in $\mathcal{Z}_2(\mathcal{C})$ zijn van de vorm $\mathbf{1} \oplus \ldots \oplus \mathbf{1}$.*

De term *modulair* komt van het feit dat het in een modulaire categorie mogelijk is om twee matrices S en T te definiëren die een eindigdimensionale projectieve representatie van de modulaire groep $SL(2, \mathbf{Z})$ definiëren [29, 31]. De modulariteitseis wordt vaak in termen van deze matrix S gegeven. De conditie is dan dat S inverterbaar is. Dit is equivalent aan de definitie hier [26].

Merk op dat de vervlechting $\varepsilon_{\rho,\sigma} \circ \varepsilon_{\sigma,\rho}$ kan worden geïnterpreteerd als het deeltje ρ eenmaal om σ winden. De modulariteitseis maakt het mogelijk om verschillende soorten anyonen te onderscheiden van elkaar, door ze te omwinden met bekende testdeeltjes.

Tenslotte is er nog een generalisatie van Hermitische conjugatie: de $*$-operatie. De $*$-operatie is een contravariante functor, wat inhoudt dat $(f \circ g)^* = g^* \circ f^*$, die involutief is: $(f^*)^* = f$. De $*$-operatie heet *positief*, als $f^* \circ f = 0$ impliceert $f = 0$. Een categorie met een positieve $*$-operatie heet *unitair*.

In een modulaire tensorcategorie is het mogelijk om op een canonieke manier representaties van de vlechtgroep B_n te construeren. Neem een object X. Dan is $\mathrm{End}(X^{\otimes n})$ een eindigdimensionale vectorruimte. Hier is $X^{\otimes n} = X \otimes \cdots \otimes X$, het tensorproduct van n kopieën. Definieer een representatie π_X^n van $\mathcal{B}_n$ door

$$\pi_X^n(\sigma_i) f := (\mathrm{id}_X^{\otimes(i-1)} \otimes \varepsilon_{X,X} \otimes \mathrm{id}_X^{\otimes(n-i-1)}) \circ f,$$

met $f \in \mathrm{End}(X^{\otimes n})$. In een unitaire modulaire categorie kan $\mathrm{End}(X^{\otimes n})$ van een inproduct worden voorzien, zodat het een Hilbertruimte wordt. De representatie is dan unitair. De studie van deze representatie is interessant voor de toepassing op topologische kwantumcomputers. Als de representatie dicht ligt in $U(\mathrm{End}(X^{\otimes n}))$, of in ieder geval dicht in de unitaire groep van een deelruimte die qubits kan beschrijven, is universele kwantumberekening mogelijk. Is dit niet het geval, dan zullen de vervlechtingen aangevuld moeten worden met andere operaties.

Fibonacci anyonen

Het eenvoudigste voorbeeld van een universele topologische kwantumcomputer is dat van de zogeheten Fibonacci anyonen [24]. De enkelvoudige objecten zijn het vacuüm $\mathbf{1}$ en een anyon τ. De enige niet-triviale fusieregel is

$$\tau \otimes \tau = \mathbf{1} \oplus \tau.$$

Verder geldt $\overline{\tau} = \tau$. We beschrijven hoe we een qubit kunnen zien in dit model, en hoe we kwantumpoorten kunnen benaderen door vervlechtingen.

Er zijn drie anyonen nodig om een qubit te beschrijven. Nemen we drie anyonen met label τ, dan geven de fusieregels

$$(\tau \otimes \tau) \otimes \tau = (\mathbf{1} \oplus \tau) \otimes \tau = \tau \oplus \tau \oplus \mathbf{1}.$$

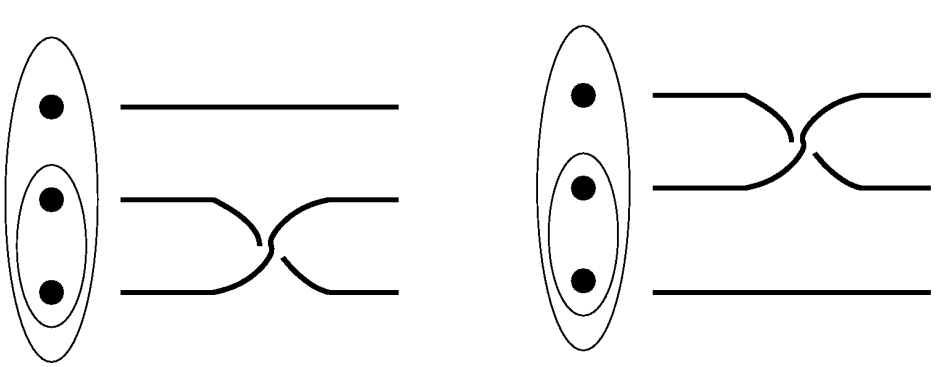
Dit is als volgt te interpreteren. Stel dat we drie τ-anyonen hebben, als in Figuur 2, en we fuseren eerst de onderste twee anyonen met elkaar, en dan het resultaat met de overgebleven anyon, dan kunnen we een τ-anyon overhouden op twee verschillende manieren, of $\mathbf{1}$ op één manier. De toestandsruimte is dus driedimensionaal. In het algemeen geldt in dit model: de toestandsruimte van n τ-deeltjes, heeft dimensie $\mathrm{Fib}(n+1)$, het $n+1$-ste Fibonacci getal. Het idee is om een qubit te beschrijven door een basis van twee van deze drie toestanden. Door vervlechting van de *drie* anyonen kunnen we unitaire transformaties op de *tweedimensionale* qubit bewerkstelligen.

Uit de axioma's voor een MTC, en door te gebruiken dat $\mathbf{1}$ en τ irreducibel zijn, volgt

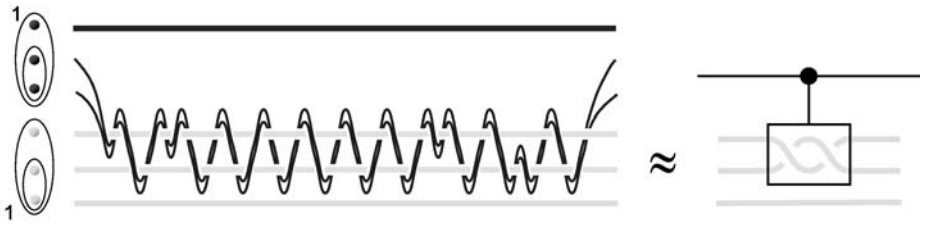
$$\mathrm{Hom}((\tau \otimes \tau) \otimes \tau, \tau) \cong \mathbf{C}^2,$$
$$\mathrm{Hom}((\tau \otimes \tau) \otimes \tau, \mathbf{1},) \cong \mathbf{C},$$

als vectorruimtes. Deze vectorruimtes heten *fusieruimtes*, ze beschrijven hoe de anyonen kunnen fuseren. De fusieruimte van $(\tau \otimes \tau) \otimes \tau$ is de directe som van de fusieruimtes, dus isomorf aan $\mathbf{C}^2 \oplus \mathbf{C}$. Het centrale idee is om deze structuur te gebruiken om de qubit te beschrijven.

In deze vectorruimte kiezen we een basis.



Figuur 2 Een qubit in het Fibonacci model, samen met de twee vervlechtingsoperaties op de qubit. Deze operaties, samen met de inverses, kunnen elke unitaire operatie op de qubit willekeurig dicht benaderen.



Figuur 3 Een benadering van een *gecontroleerde vervlechting*. De vervlechting van de anyonen uit de onderste qubit wordt alleen uitgevoerd, als de bovenste qubit in de toestand $|1\rangle$ is. De nauwkeurigheid is hier $\varepsilon = 2,3 \times 10^{-3}$. Figuur uit Bonesteel et al. [2].

Met $|((\bullet,\bullet)_\tau,\bullet)_\tau\rangle$ geven we de toestand aan waarbij de twee onderste anyonen tot τ fuseren, en een fusie met het overgebleven anyon weer τ oplevert. Definieer met deze notatie de basis $|0\rangle = |((\bullet,\bullet)_{\mathbf{1}},\bullet)_\tau\rangle$, $|1\rangle = |((\bullet,\bullet)_\tau,\bullet)_\tau\rangle$ en $|NC\rangle = |((\bullet,\bullet)_\tau,\bullet)_{\mathbf{1}}\rangle$. De eerste twee vectoren vormen de qubit, de laatste is voor de berekening niet belangrijk. Merk op dat wel van belang is dat de deelruimte opgespannen door de vectoren $|0\rangle$ en $|1\rangle$ in zichzelf wordt afgebeeld door de operaties op de anyonen. Uit de beschrijving volgt dat we de qubit kunnen meten door de onderste twee qubits te fuseren, en te bepalen of er een $\mathbf{1}$ of τ overblijft.

De categorie die we bekijken is in dit geval niet strikt: $(\tau\otimes\tau)\otimes\tau$ is bijvoorbeeld slechts isomorf aan $\tau\otimes(\tau\otimes\tau)$, in plaats van identiek. Om het model volledig vast te leggen, moet nog vastgelegd worden hoe associativiteit en vervlechting effect hebben op de toestanden. In dit specifieke model wordt dit door de axioma's van een gevlochten tensorcategorie en compatibiliteit met de fusieregels in essentie uniek bepaald. Een gevolg van deze eisen is bijvoorbeeld dat er een unitaire transformatie moet zijn tussen $\mathrm{Hom}((\tau\otimes\tau)\otimes\tau,\tau)$ en $\mathrm{Hom}(\tau\otimes(\tau\otimes\tau),\tau)$. De eisen leveren een stelsel polynoomvergelijkingen op, die in dit geval een unieke oplossing hebben.

Voor wat betreft de vervlechtingsoperatie kan een soortgelijke procedure worden gevolgd. Opnieuw leveren compatibiliteitseisen een unieke oplossing op. Het vervlechten van anyonen induceert een unitaire operatie op de fusieruimte. In de basis $|0\rangle, |1\rangle, |NC\rangle$ die we hierboven hebben gekozen, wordt de vervlechting van de bovenste twee anyonen, zoals in Figuur 2 rechts, gegeven door de matrix [2]

$$\begin{pmatrix} -\eta e^{-i\pi/5} & -i\sqrt{\eta}e^{-i\pi/10} & 0 \\ -i\sqrt{\eta}e^{-i\pi/10} & -\eta & 0 \\ 0 & 0 & -e^{-i2\pi/5} \end{pmatrix},$$

met $\eta = (\sqrt{5}-1)/2$, de inverse van de gulden snede. Merk op dat de vervlechting de qubit in zichzelf overvoert.

Bonesteel et al. laten zien hoe door vervlechten een willekeurige unitaire operatie op de qubit benaderd kan worden. De auteurs gebruiken een brute force methode, maar door gebruik te maken van de Solovay-Kitaev stelling kan een willekeurige nauwkeurigheid bereikt worden [2]. Dit is nog niet genoeg voor universele kwantumberekening. Daarom construeren Bonesteel et al. ook bepaalde kwantumpoorten die op twee qubits (in dit model dus voorgesteld door 6 anyonen) werken. Ook hier wordt de Solovay-Kitaev stelling gebruikt om de gewenste nauwkeurigheid te bereiken. Zie Figuur 3 voor een voorbeeld. Deze kwantumpoorten samen zijn universeel, elk kwantumalgoritme kan met behulp van deze poorten worden opgebouwd.

Conclusies

Topologische kwantumcomputers lijken een aantrekkelijk alternatief voor, of aanvulling op, de bestaande methodes voor kwantumberekeningen. Het is aan de fysici om daadwerkelijk, in een laboratorium, een systeem met anyonen te maken. Er zijn wat resultaten in die richting (zie [21]), maar die zijn nog lang niet voldoende voor topologische kwantumcomputers. Het is bijvoorbeeld nodig om de individuele anyonen te kunnen manipuleren, om de vervlechting uit te voeren.

Een interessant vraagstuk voor de mathematische fysica is systemen te beschrijven die aanleiding geven tot een modulaire tensorcategorie. Dit soort systemen kunnen uiteindelijk wellicht nieuwe aanknopingspunten geven voor de zoektocht naar een topologische kwantumcomputer in de praktijk. In het raamwerk van de algebraïsche kwantumveldentheorie is er een aantal voorbeelden hiervan bekend [11, 18, 25].

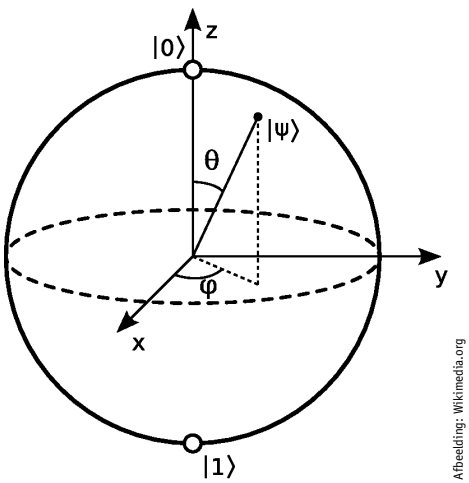
Vanuit een wiskundig oogpunt is de abstracte beschrijving in termen van een modulaire categorie interessant. Deze categorieën komen ook in andere onderzoeksgebieden voor. Voor een kort overzicht van de verbanden, en toepassingen op kwantumcomputers, zie [27]. Men kan zich afvragen wat voor representaties van de vlechtgroep we in een bepaalde categorie krijgen, en of deze representatie voldoende is om een universele kwantumcomputer te beschrijven. De theorie van vlechtgroepen en hun representaties is ook erg uitgebreid. In tegenstelling tot de representatietheorie van S_n, is die van B_n echter nog niet volledig begrepen [10].

Als een representatie van de vlechtgroep niet universeel is, kan niet elk kwantumalgoritme uitgevoerd worden door het vervlechten van anyonen. In plaats van het toevoegen van nieuwe operaties zodat *wel* een universele verzameling kwantumpoorten beschikbaar is, kan ook gekeken worden welke algoritmes nog wel uit te voeren zijn. Zie [27] voor een overzicht.

Tenslotte kan men denken aan een classificatie van modulaire categorieën, en bijvoorbeeld methodes om van een gevlochten, maar niet modulaire, categorie een modulaire categorie te krijgen. Zie bijvoorbeeld [19], en voor een iets recenter overzicht, de lecture notes van Müger [20].

Aanvullende literatuur

Het standaardwerk over kwantumberekening en kwantuminformatie is het boek van Nielsen en Chuang [22]. De lecture notes van Preskill geven een introductie tot *topologische* kwantumcomputers [24]. Het overzichtsartikel van Nayak et al. [21] geeft een overzicht van de huidige stand van zaken, en behandelt enkele systemen die mogelijk in een laboratorium gerealiseerd kunnen worden. In het artikel van Panangaden en Paquette ligt de nadruk op het verband met modulaire tensorcategorieën; het voorbeeld van de Fibonacci anyonen wordt ook behandeld [23]. Deze laatste referentie is het meest toegankelijk voor lezers zonder achtergrond in de fysica.



Afbeelding: Wikimedia.org

Figuur 4 De mogelijke toestanden van een qubit kunnen inzichtelijk worden gemaakt door middel van de Bloch sfeer. Elk punt op het boloppervlak komt overeen met een eenheidsvector in $\mathbf{C}^2$.

Referenties

1 B. Bakalov en A. Kirillov, Jr. *Lectures on tensor categories and modular functors*, American Mathematical Society, Providence, RI, 2001.

2 N.E. Bonesteel, L. Hormozi, G. Zikos en S.H. Simon, 'Braid Topologies for Quantum Computation', *Phys. Rev. Lett.*, **95**(14):140503, 2005

3 C.M. Dawson en M.A. Nielsen, 'The Solovay-Kitaev theorem', *Quantum Inf. Comput.*, **6**(1):81–95, 2006.

4 D. Deutsch, 'Quantum theory, the Church-Turing principle and the universal quantum computer', *Proc. Roy. Soc. London Ser. A*, **400**(1818):97–117, 1985.

5 R.P. Feynman, 'Simulating physics with computers', *Internat. J. Theoret. Phys.*, **21**(6–7):467–488, 1982.

6 M.H. Freedman, 'P/NP, and the quantum field computer', *Proc. Natl. Acad. Sci. USA*, **95**(1):98–101, 1998.

7 M.H. Freedman, A. Kitaev, M.J. Larsen en Z. Wang, 'Topological quantum computation', *Bull. Amer. Math. Soc. (N.S.)*, **40**(1):31–38, 2003.

8 M.H. Freedman, M.J. Larsen en Z. Wang, 'A modular functor which is universal for quantum computation', *Comm. Math. Phys.*, **227**(3):605–622, 2002.

9 C. Kassel, M. Rosso en V. Turaev, *Quantum groups and knot invariants*, Société Mathématique de France, Parijs, 1997

10 C. Kassel en V. Turaev, *Braid groups*, Springer, New York, 2008.

11 Y. Kawahigashi, R. Longo en M. Müger, 'Multi-interval subfactors and modularity of representations in conformal field theory', *Comm. Math. Phys*, **219**(3):631–669, 2001.

12 A. Kitaev, 'Fault-tolerant quantum computation by anyons', *Ann. Physics*, **303**:2–30, 2003.

13 G.M.M. Laidlaw en C. Morette DeWitt, 'Feynman Functional Integrals for Systems of Indistinguishable Particles', *Phys. Rev. D*, **3**(6):1375–1378, 1971.

14 J.M. Leinaas en J. Myrheim, 'On the theory of identical particles', *Il Nuovo Cimento B*, **37**(1):1–23, 1977.

15 S. Mac Lane. *Categories for the working mathematician*, Springer-Verlag, New York, second edition, 1998.

16 Y.I. Manin, *Mathematics as metaphor*, American Mathematical Society, Providence, RI, 2007.

17 C. Mochon, 'Anyon computers with smaller groups', *Phys. Rev. A*, **69** 032306, 2004.

18 M. Müger, 'On charged fields with group symmetry with degeneracies of Verlinde's matrix S', *Ann. Inst. H. Poincaré Phys. Théor.*, **71**(4):359–394, 1999.

19 M. Müger, 'On the structure of modular categories', *Proc. London Math. Soc. (3)*, **87**(2):291–308, 2003.

20 M. Müger, *Tensor categories: A selective guided tour*, arXiv:0804.3587.

21 C. Nayak, S.H. Simon, A. Stern, M. Freedman en S. Das Sarma, 'Non-abelian anyons and topological quantum computation', *Rev. Mod. Phys.*, **80**(3):1083–1159, 2008.

22 M.A. Nielsen en I.L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.

23 P. Panangaden en É.O. Paquette, 'A categorical presentation of quantum computation with anyons', in B. Coecke (red.): *New structures for Physics*, 2010.

24 J. Preskill, *Lecture notes in quantum computation*, www.theory.caltech.edu/people/preskill/ph229/#lecture.

25 K.-H. Rehren, 'Markov traces as characters for local algebras', *Nucl. Phys. B Proc. Suppl.*, **18B**:259–268, 1990.

26 K.-H. Rehren, 'Braid group statistics and their superselection rules', in D. Kastler (red.): *The algebraic theory of superselection sectors*, 1990.

27 E.C. Rowell, 'Two paradigms for topological quantum computation', *Contemp. Math,* **482**:165–178, 2009.

28 P.W. Shor, 'Algorithms for quantum computation: discrete logarithms and factoring'. In *Proceedings, 35^{th} Annual Symposium on Foundations of Computer Science*, pp. 56–65, IEEE Press, Los Alamitos, CA, 1994.

29 V.G. Turaev, *Quantum invariants of knots and 3-manifolds*, Walter de Gruyter, Berlijn, 1994

30 L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, I.L. Chuang, 'Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance', *Nature*, **414**(6866):883–887, 2001

31 E. Verlinde, 'Fusion rules and modular transformations in 2D conformal field theory', *Nuclear Phys. B*, **300**(3):360–376, 1988.

32 F. Wilczek, 'Quantum mechanics of fractional-spin particles', *Phys. Rev. Lett.*, **49**(14):957–959, 1982.

33 Stel A is de observabele die we willen meten. Dan is er een *spectrale decompositie*, $A = \lambda_1 P_1 + \ldots + \lambda_n P_n$. Hier zijn λ_i de eigenwaarden van A, en P_i de bijbehorende projectie op de eigenruimte. Een meting van een systeem in toestand $|\psi\rangle$, levert dan een eigenwaarde λ_i op, met kans $\langle\psi|P_i|\psi\rangle$. Dit is *Borns regel*.

34 Een matrix waarvoor geldt $U^*U = UU^* = I$, met $*$ Hermitische conjugatie en I de eenheidsmatrix.

35 Preciezer: voor elke $\varepsilon > 0$ zijn er $S_i \in \mathcal{U}$, $i = 1, \ldots, n$, zodanig dat $||S_1 \cdots S_n - U|| < \varepsilon$, waarbij $||A|| = \sup_{||\xi||=1} ||A\xi||$ met $\xi \in \mathbf{C}^{2^n}$.

36 Deze poort heet de $\pi/8$ poort om historische redenen. De poort is (op een irrelevante fasefactor na) gelijk aan de poort met $e^{\pm i\pi/8}$ op de diagonaal.

37 Het argument komt er op neer dat de fundamentaalgroep van de configuratieruimte van n deeltjes in $\mathbf{R}^2$ gelijk is aan de vlechtgroep. In hogere dimensies is de fundamentaalgroep triviaal.

38 De gelijkheid geldt in het geval van een *strikte* tensorcategorie. In het algemene geval geldt de gelijkheid slechts tot op isomorfisme. Echter, men kan aantonen dat elke tensorcategorie equivalent is aan een *strikte* tensorcategorie [15].

39 Een deelcategorie $\mathcal{C}$ van $\mathcal{D}$ heet *vol*, als $\mathrm{Hom}_{\mathcal{C}}(X, Y) = \mathrm{Hom}_{\mathcal{D}}(X, Y)$, voor alle objecten X, Y van $\mathcal{C}$.

40 Algemener kan men spreken over een links- respectievelijk rechtsduale. In een unitaire $*$-categorie zijn deze twee a priori verschillende objecten automatisch isomorf. Het is dan mogelijk om een symmetrische definitie van een duale te geven. De definitie hier heeft als voordeel dat in de huidige context er een duidelijke fysische interpretatie is.