Leibniz Universität Hannover
Institut für Theoretische Informatik

Berechnungsmodelle der Quanteninformation

Bachelorarbeit

Vanessa Werth
Matrikelnummer: 2723840

03. September 2018

Prüfer: Prof. Dr. Heribert Vollmer
Dr. Arne Meier

Inhaltsverzeichnis

1 Einleitung

Die erste Idee für einen Quantencomputer formulierte Feynman im Jahre 1982 [1]. Seit dem wurde theoretisch als auch experimentell viel in diesem Gebiet erreicht. Es besteht die Hoffnung, dass Quantencomputer in der Lage sind Probleme generell schneller lösen zu können, als klassische Computer. Mit dem Shor-Algorithmus zur Faktorisierung einer Zahl ist ein erstes Problem gefunden worden, dass auf einem Quantencomputer schneller skaliert als mit jedem bisher bekannten Algorithmus auf einem klassischen Computer [2]. Leider ist dies nur ein erstes Indiz, dass Quantencomputer den klassischen Computern überlegen sind. Es lässt sich aus diesem Beispiel noch keine verallgemeinerte Aussage ableiten.

Um die Laufzeit eines Quantencomputers für einen Algorithmus bestimmen zu können, werden Modelle benötigt, wie sie für klassische Computer bekannt sind. Diese Modelle müssen dann auf die Besonderheiten der Quantenwelt angepasst werden. Zwei der bekanntesten klassischen Modelle zur Laufzeitanalyse sind Turingmaschinen und Schaltkreise. Übertragen auf die Quantenwelt geben diese Berechnungsmodelle die Möglichkeit die Laufzeit eines für Quantencomputer entworfenen Algorithmus zu analysieren und zu vergleichen.

In dieser Arbeit sollen die Modelle des Quantenschaltkreises und der Quantenturingmaschine vorgestellt werden, um dem Leser das Werkzeug mitzugeben Algorithmen in diesen Modellen formulieren zu können. Des Weiteren kann der Leser mithilfe dieser Darstellung von Algorithmen eine Laufzeitanalyse durchgeführen. In der vorliegenden Arbeit wird sich weiterhin damit beschäftigt, ob eine Quantenturingmaschine auch als Quantenschaltkreis formuliert werden kann. Diese Frage wird am Ende der Arbeit mithilfe eines mathematischen Beweises beantwortet. Bis dahin werden in dieser Arbeit alle notwendigen Grundlagen gelegt, die für das Verständnis des Beweises notwendig sind.

2 Theoretische Grundlagen

In diesem Kapitel soll dem Leser eine kurze theoretische Einführung in das Thema geboten werden. Dazu wird ein kurzer Überblick über die Quantenmechanik gegeben, wobei der Inhalte dieses Abschnitts auf den Büchern von I. Levine [3] und C. Cohen-Tannoudji *et al.* [4] basiert. Im nächsten Abschnitt werden kurz die wichtigsten mathematischen Definitionen und Grundlagen zusammengefasst, die für das Verständnis der Arbeit notwendig sind. Die letzten beiden Abschnitte befassen sich mit Qubits und Operationen auf Qubits und basieren zum größten Teil auf dem Buch von M. A. Nielsen und I. L. Chuang [5] und dem Buch von E. Rieffel und W. Polak [6].

2.1 Quantenmechanik

Die Theorie der Quantenmechanik kam um 1900 auf, als Folge von Plancks Untersuchung des sogenannten schwarzen Strahlers im niedrigen Frequenzbereich [3]. Der schwarze Strahler absorbiert und emittiert Licht aller Wellenlängen. Die Intensität und spektrale Verteilung der emittierten Strahlung hängen von der Temperatur des schwarzen Strahlers ab. Die erste theoretische Behandlung des Problems lieferte keine ausreichende Beschreibung der Intensität in Abhängigkeit von der Frequenz und der Temperatur des schwarzen Strahlers im Bereich niedriger Frequenzen. Für die Herleitung einer angepassten Gleichung machte Planck die Annahme, dass die Absorber/Emitter des schwarzen Strahlers harmonisch oszillierende elektrische Ladungen sind, deren Energien ein Vielfaches von $h\nu$ betragen. Die Energie der elektrischen Ladungen ist quantisiert, kann also nur diskrete Werte annehmen.

Die Quantisierung der Energie lässt sich nicht aus den Gesetzen der klassischen Mechanik herleiten und scheint deswegen zunächst im Widerspruch zur klassischen Mechanik zu stehen. Die Quantenmechanik beschreibt physikalische Phänomene für kleine Teilchen (atomare oder subatomare Größe) und für große Teilchen gehen die Gesetze der Quantenmechanik in die klassische Mechanik über. Die Quantisierung der Energie ist eines der Postulate der Quantenmechanik, weitere Postulate sind der Welle-Teilchen-Dualismus und die Schrödinger-Gleichung.

Die Theorie der Quantenmechanik ist zum Teil schwer nachzuvollziehen, da Beobachtungen von Einflüssen der Quantenmechanik nicht zu unserem alltäglichen Leben gehören. Einfacher lässt sich mit der Quantenmechanik arbeiten, wenn sie als eine rein mathematische Beschreibung angesehen wird, da hierfür die Kenntnisse der linearen Algebra ausreichend sind. Ein anschauliches Beispiel für diese Problematik ist die Wellenfunktion $\psi(x)$. Im einfachsten Fall

beschreibt die Wellenfunktion den Zustand eines Teilchens in einer Dimension. Alle im Folgenden gemachten Beobachtungen lassen sich aber auch auf höher-dimensionale Wellenfunktion übertragen.

Die Wellenfunktion enthält alle nötigen Informationen, um das System zu beschreiben, allerdings sind diese Informationen nicht direkt zugänglich. Aus $\psi(x)$ kann beispielsweise die Aufenthaltswahrscheinlichkeit des Teilchens erhalten werden, das durch $\psi(x)$ beschrieben wird. Das Integral

$$\int_{x_1}^{x_2} |\psi(x)|^2 \mathrm{d}x \tag{2.1}$$

beschreibt die Wahrscheinlichkeit dafür, dass das Teilchen im Intervall $[x_1, x_2]$ zu finden ist. $\psi(x)$ wird aus diesem Grund auch als Wahrscheinlichkeitsverteilungsfunktion bezeichnet. Es gilt $\int |\psi(x)|^2 \mathrm{d}x = 1$, da sich das Teilchen irgendwo im Raum befinden muss. Der Funktionsraum solcher normierten und quadratisch integrierbaren Funktionen wird mit L^2 bezeichnet und hat die Eigenschaften eines Hilbertraums.

Eine abzählbare Menge von Funktionen $u_i(x) \in L^2$ heißt orthonormale Basis, wenn sich jede Funktion $\psi(x) \in L^2$ darstellen lässt als

$$\psi(x) = \sum_{i=1}^{n} c_i u_i(x) \tag{2.2}$$

mit $c_i \in \mathbb{C}$ und $i \in \mathbb{N}$ und weiterhin gilt

$$\int u_i^*(x) u_j(x) \mathrm{d}x = \kappa_{ij} \tag{2.3}$$

wobei $u_i^*(x)$ das komplex Konjugierte von $u_i(x)$ ist. Die Funktion κ_{ij}, die den Wert 1 annimmt, wenn $i = j$ und ansonsten den Wert 0 annimmt, wird als Kronecker-Delta bezeichnet. Der Zustand eines Teilchens lässt sich also nicht nur durch die Wellenfunktion $\psi(x)$ beschreiben, sondern auch durch die Koeffizienten c_i in der orthonormalen Basis $u_i(x)$. Anders gesagt, jeder Zustand eines Teilchens lässt sich in der Basis $u_i(x)$ durch einen Zustandsvektor $\mathbf{c} \in \mathbb{C}^n$ ausdrücken. Interessant zu beobachten ist, dass

$$\begin{aligned} \int |\psi(x)|^2 \mathrm{d}x &= \int \left| \sum_{i=1}^{n} c_i u_i(x) \right|^2 \mathrm{d}x = \int \left(\sum_{i=1}^{n} c_i^* u_i^*(x) \right) \cdot \left(\sum_{i=1}^{n} c_i u_i(x) \right) \mathrm{d}x \\ &= \sum_{i=1}^{n} c_i^* \cdot c_i = \sum_{i=1}^{n} |c_i|^2, \end{aligned} \tag{2.4}$$

was in der linearen Algebra dem Skalarprodukt $(\mathbf{c}, \mathbf{c})$ entspricht. Diese Analogien zwischen der funktionalen Betrachtung und der linearen Algebra sind ein wichtiger Bestandteil der mathematischen Beschreibung der Quantenmechanik.

Bei Verwendung der sogenannten Dirac-Notation muss keine explizite Darstellungsweise angegeben werden. Die Dirac-Notation führt die Bra- und Ket-Vektoren ein, die sowohl eine Entsprechung in der funktionalen Betrachtung als auch in der linearen Algebra finden. Es gilt dann

$$\langle\psi|\psi\rangle = \int |\psi(x)|^2 \mathrm{d}x = (\mathbf{c}, \mathbf{c}). \tag{2.5}$$

Des Weiteren spielen Operatoren in der Beschreibung der Quantenmechanik eine entscheidende Rolle. Mit ihrer Hilfe können weitere Informationen (Observablen) aus der Wellenfunktion gewonnen werden. Auch für die Operatoren kann die Dirac-Notation verwendet werden. Einer der wichtigsten Operatoren ist der Hamiltonoperator, der häufig auch als Energieoperator bezeichnet wird, mithilfe dessen die Energieniveaus eines Systems bestimmt werden können. Für den Hamiltonoperator $\hat{H}$ im eindimensionalen Fall gilt

$$\hat{H} = -\frac{\hbar}{2m}\frac{\mathrm{d}^2}{\mathrm{d}x^2} + V(x). \tag{2.6}$$

Die Anwendung von $\hat{H}$ auf die Wellenfunktion $\psi(x)$ ist äquivalent zu der Multiplikation einer Matrix H mit dem Zustandsvektor $\mathbf{c}$. In der Dirac-Notation wird dies als $H\,|\psi\rangle$ dargestellt.

2.2 Mathematische Grundlagen

Allgemeine Definitionen

Definition 1. $\mathbf{I}_n$ *bezeichne die* $(n \times n)$*-Matrix, für deren Matrixeinträge* $a_{ij} = \kappa_{ij}$ *gilt.*

Definition 2. *Eine Matrix* A *wird als unitär bezeichnet, wenn* $A^\dagger \cdot A = \mathbf{I}_{\dim(A)}$ *gilt.*

Die unitäre Eigenschaft bei der Multiplikation zweier unitärer Matrizen bleibt erhalten.

Definition 3. *Eine unitäre* $(n \times n)$ *Matrix mit der Eigenschaft, dass nur die Einträge* a_{ii}*,* a_{jj}*,* a_{ij} *und* a_{ji} *mit* $i, j \in \{\, 1, 2, \ldots, n \,\}$ *ungleich den Einträgen einer Einheitsmatrix sein dürfen, wird als 2-Level-Matrix bezeichnet.*

Definition 4. *Eine kontrollierte* $(n \times n)$*-Matrix* V_C *mit den Matrixeinträgen* $a_{11}, \ldots, a_{nn}$ *ist durch folgende Bedingungen definiert:*

1. *Die Einträge* $a_{ij} = \kappa_{ij}$ *für alle* $i, j \in Set1, 2, \ldots, n-2$*.*
2. *Die Untermatrix* V *der letzten beiden Zeilen und Spalten ist unitär.*

Definition 5. *Die lineare Hülle* span$A$ *einer Vektormenge* A *ist die Menge aller Linearkombinationen von Elementen aus* A*.*

Tensorprodukt

Definition 6. *Das Tensorprodukt $\otimes$ bildet die Vektoren $[v_1, \ldots, v_n]^\intercal$ und $[w_1, \ldots, w_m]^\intercal$ aus den Vektorräumen V und W auf den Vektor $[v_1 \cdot w_1, \ldots, v_1 \cdot w_m, \ldots, v_n \cdot w_1, \ldots v_n \cdot w_m]^\intercal$ ab, wobei der resultierende Vektorraum $V \otimes W$ die Dimension $\dim(V) \cdot \dim(W)$ besitzt.*

Die Tensorprodukte aller Elemente zweier orthonormalen Basen in den Vektorräumen V und W ergibt eine orthonormale Basis im Vektorraum $V \otimes W$. Das Tensorprodukt kann auch auf Matrizen angewandt werden.

Definition 7. *Das Tensorprodukt $\otimes$ bildet die $(m \times n)$-Matrix A und die $(j \times k)$-Matrix B ab auf die $(m \cdot j \times n \cdot k)$-Matrix*

$$\begin{bmatrix} a_{11} \cdot B & \ldots & a_{1n} \cdot B \\ \vdots & \ddots & \vdots \\ a_{m1} \cdot B & \ldots & a_{mn} \cdot B \end{bmatrix}.$$

Die unitäre Eigenschaft wird bei der Bildung eines Tensorprodukts erhalten, wenn beide Matrizen unitär sind.

Lemma 8. *Für die Vektoren v und w und Matrizen A und B gilt $(Av) \otimes (Bw) = (A \otimes B)(v \otimes w)$.*

Adjungierte Vektoren und Matrizen

Das Adjungierte eines Vektors v bzw. einer Matrix A wird durch $v^\dagger$ bzw. $A^\dagger$ gekennzeichnet. Es handelt sich bei dem Adjungierten um das Transponierte ($^\intercal$) und komplex Konjugierte (*) des ursprünglichen Elements. Es gelten die folgenden Rechenregeln:

1. $(A + B)^\dagger = A^\dagger + B^\dagger$
2. $(A \cdot B)^\dagger = B^\dagger \cdot A^\dagger$
3. $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$

Dirac-Notation

Die von Dirac eingeführte Bra-Ket-Schreibweise ermöglicht eine einfachere Handhabung von Vektoren im Hilbertraum. Es lassen sich mit ihrer Hilfe Vektoren in einer Schreibweise darstellen, die unabhängig von der gewählten Basis des Vektorraums ist. Dies sei an folgendem Beispiel illustriert:

Die Zahlen 0 bis 3 sollen in einem Vektorraum kodiert werden. Des Weiteren soll es sich dabei um orthonormale Vektoren handeln. Hierzu kann bspw. die Standardbasis gewählt werden und es entspricht die Zahl 0 dem Vektor $[1, 0, 0, 0]^\intercal$ usw. Es kann notwendig sein, die Basis zu ändern und dann müssen die Vektoren zunächst in die neue Basis transformiert werden. Diese Änderung der Basis hat hier aber nur zur Folge, dass die Vektoren anders geschrieben werden,

nicht aber auf ihre orthonormale Eigenschaft. In der Dirac-Notation lassen sich die kodierten Vektoren schreiben als $|0\rangle$, $|1\rangle$, $|2\rangle$ und $|3\rangle$. Der Ket-Vektor $|0\rangle$ entspricht dann dem Spaltenvektor $[1, 0, 0, 0]^\intercal$. Allerdings kann der Vektor $|0\rangle$ auch einem beliebigen anderem Spaltenvektor entsprechen, wenn eine andere Basis gewählt wird.

Viele in der linearen Algebra bekannten Operationen haben eine Darstellung in der Bra-Ket-Schreibweise. Es entspreche $|\psi\rangle$ dem Vektor $[\psi_1, \ldots, \psi_n]^\intercal$ und $|\phi\rangle$ dem Vektor $[\phi_1, \ldots, \phi_n]^\intercal$.

1. Es ist $|\psi\rangle^\dagger = \langle\psi|$. Es entspricht $\langle\psi|$ dem Vektor $[\psi_1^*, \ldots, \psi_n^*]$.
2. Das Skalarprodukt der Vektoren ψ und ϕ ist $\langle\phi|\psi\rangle$ und entspricht $\sum_{i=1}^{n} \phi_i^* \cdot \psi_i$.
3. Das äußere Produkt zweier Vektoren ψ und ϕ ist $|\phi\rangle\langle\psi|$ und dies entspricht der Matrix

$$\begin{bmatrix} \phi_1 \cdot \psi_1^* & \cdots & \phi_1 \cdot \psi_n^* \\ \vdots & \ddots & \vdots \\ \phi_n \cdot \psi_1^* & \cdots & \phi_n \cdot \psi_n^* \end{bmatrix}.$$

4. Die Multiplikation des Vektors $|\psi\rangle$ mit einer Matrix A wird geschrieben als $A|\psi\rangle$.

2.3 Qubits

Beim klassischen Computer werden die Informationen mithilfe von Bits gespeichert. Diese können die Werte 0 oder 1 annehmen. Beim Quantencomputer werden die Informationen mithilfe von Qubits (Kurzform für Quantenbits) gespeichert. Diese können ebenfalls die Werte 0 oder 1 annehmen, allerdings können sie auch beide Werte gleichzeitig annehmen.

Ein Qubit ist ein normierter Vektor aus $\mathbb{C}^2$ mit der orthonormalen Basis $|0\rangle$ und $|1\rangle$. Ein Qubit befindet sich im Zustand $|\psi\rangle$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.7}$$

mit $\alpha, \beta \in \mathbb{C}$ und $|\alpha|^2 + |\beta|^2 = 1$. Die Koeffizienten α und β werden auch als Amplituden bezeichnet. Eine solche Darstellung, die auch schon im Abschnitt 2.1 angesprochen wurde, wird als Superposition bezeichnet, wenn $\alpha \neq 0$ und $\beta \neq 0$ gilt.

Die Anzahl an Superpositionen, in denen sich ein Qubit befinden kann, sind unendlich, da nur die Normierungsbedingung erfüllt sein muss. Insgesamt gibt es 6 prominente Zustände:

$$|1\rangle = 0 \cdot |0\rangle + 1 \cdot |1\rangle, \; |0\rangle = 1 \cdot |0\rangle + 0 \cdot |1\rangle, \tag{2.8}$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \; |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{2.9}$$

$$|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \mathrm{i}|1\rangle), \; |-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - \mathrm{i}|1\rangle). \tag{2.10}$$

Die Zustände aus Gleichung 2.9 finden sich in der Literatur häufig unter der Bezeichnung Hadamard-Basis wieder.

Interaktion mehrerer Qubits

Ein n-Qubitsystem wird durch einen normierter Vektor aus $\mathbb{C}^{2^n}$ beschrieben mit den orthonormalen Basisvektoren $|x\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$ mit $x \in \{0, 1\}^n$ [7]. Für ein 2-Qubitsystem wird die orthonormale Basis demnach wie folgt erhalten:

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \; |01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix},$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \; |11\rangle = |1\rangle \otimes |1\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}.$$

Der Zustand $|\psi\rangle$ ist

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle \tag{2.11}$$

beschrieben, mit den Amplituden α_x mit $x \in \{\,0,\,1\,\}^2$ und $\sum_{x\in\{\,0,\,1\,\}^2}|\alpha_x|^2 = 1$. Für n-Qubits werden 2^n Basisvektoren und Amplituden erhalten.

2.3.1 Projektive Messung

Die Superposition, also die Koeffizienten α und β, eines Qubits lassen sich nicht direkt bestimmen. Wird der Wert eines Qubits ausgelesen, so wird mit einer Wahrscheinlichkeit von $|\alpha|^2$ der Zustand $|0\rangle$ und mit einer Wahrscheinlichkeit von $|\beta|^2$ der Zustand $|1\rangle$ bei einem Qubit beobachtet. Das Auslesen eines Qubits wird mathematisch über eine projektive Messung in der Standardbasis beschrieben.

Definition 9. *Sei $\mathcal{P} = \{P_0, \ldots, P_m\}$ mit $m \leq 2^n - 1$ eine beliebige Menge von Projektionsoperatoren, d. h. es gilt $P_i^2 = P_i$, auf dem n-Qubitzustand $|\psi\rangle$ mit $\sum_{i=0}^{m} P_i = \mathbf{I}_{2^n}$.*

Der Zustand nach einer Messung

$$|\psi_{\mathrm{M}}\rangle = \frac{P_i\,|\psi\rangle}{\sqrt{\langle\psi|P_i|\psi\rangle}} \tag{2.12}$$

wird mit einer Wahrscheinlichkeit von $\langle\psi|P_i|\psi\rangle$ gemessen. Durch die Anwendung der projektiven Messung wird der Zustand möglicherweise verändert. Wird bspw. bei einem 2-Qubitzustand

das erste der beiden Qubits in der Standardbasis gemessen und als Ergebnis der Messung $|0\rangle$ erhalten, so ist

$$|\psi_{\mathrm{M}}\rangle = \frac{\alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}, \tag{2.13}$$

der Zustand des Systems nach der Messung.

2.4 Operationen auf Qubits

Die Veränderung des Zustands eines n-Qubitsystems geschieht aus rein mathematischer Sicht über die Multiplikation mit einer Matrix. Diese Matrix M muss aufgrund der physikalischen Gesetzmäßigkeiten bestimmte Bedingungen erfüllen. Durch die Multiplikation muss die Normalisierungsbedingung weiterhin erfüllt sein. Des Weiteren können alle physikalischen Operationen auf Zustandsvektoren durch reversible Operationen auf einem größeren Raum von Zustandsvektoren dargestellt werden. Aus diesem Grund werden im Folgenden nur reversible Operationen betrachtet. Damit die Normalisierungsbedingung und die Reversibilität gilt, muss die Matrix M unitär sein. Alle unitären Matrizen sind demnach valide Operationen auf Qubits.

2.4.1 Operationen auf einzelnen Qubits

Beim klassischen Computer existiert nur der Inverter, welcher nur mit einem einzelnen Eingangsbit arbeitet. Liegt am Eingang eine 0 an, wird als Ergebnis eine 1 erhalten und umgekehrt. Eine solche Invertierung ist auch bei einem Qubit möglich, unterscheidet sich aber aufgrund der unterschiedlichen Beschaffenheit von Bit und Qubit.

Um den Zustandsvektor $|0\rangle$ bzw. $|1\rangle$ eines Qubits zu invertieren, wird mit

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{2.14}$$

multipliziert. Der erhaltene Zustand bei Anwendung auf die Wellenfunktion $|psi\rangle$ ist

$$X\,|\psi\rangle = X(\alpha\,|0\rangle + \beta\,|1\rangle) = \beta\,|0\rangle + \alpha\,|1\rangle\,. \tag{2.15}$$

Bei der Invertierung einer Superposition werden also die Amplituden der Zustände $|0\rangle$ und $|1\rangle$ vertauscht.

Neben der Invertierung gibt es für die Anwendung auf einzelne Qubits aber noch weitere Operatoren. Die sogenannten Paulimatrizen

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{2.16}$$

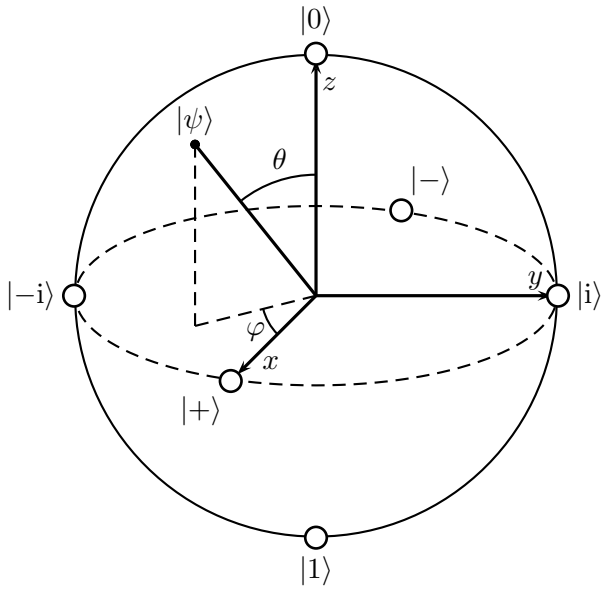

Abbildung 2.1: Darstellung der Superposition von $|\psi\rangle$ in der Blochsphäre.

sind nur einige Beispiele für solche Operatoren. Weitere wichtige Vertreter sind die Hadamardmatrix H, die Phasenmatrix S und der $\pi/8$-Operator T:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \; S = \begin{bmatrix} 1 & 0 \\ 0 & -\mathrm{i} \end{bmatrix}, \; T = \exp(\mathrm{i}\pi/8) \begin{bmatrix} \exp(-\mathrm{i}\pi/8) & 0 \\ 0 & \exp(\mathrm{i}\pi/8) \end{bmatrix}. \tag{2.17}$$

Die Anwendung eines Operators auf ein Qubit kann verstanden werden, als die Rotation und Reflektion in einer Blochsphäre. Die Darstellung eines 1-Qubitzustands $|\psi\rangle$ in der Blochsphäre ist in Abbildung 2.4.1 gezeigt. Die Rotation um die Achsen x, y und z jeweils um den Winkel θ wird durch folgende Matrizen beschrieben

$$R_x(\theta) = \begin{bmatrix} \cos\theta/2 & -\mathrm{i}\sin\theta/2 \\ -\mathrm{i}\sin\theta/2 & \cos\theta/2 \end{bmatrix}, \tag{2.18}$$

$$R_y(\theta) = \begin{bmatrix} \cos\theta/2 & -\sin\theta/2 \\ \sin\theta/2 & \cos\theta/2 \end{bmatrix}, \tag{2.19}$$

$$R_z(\theta) = \begin{bmatrix} \exp(-\mathrm{i}\theta/2) & 0 \\ 0 & \exp(\mathrm{i}\theta/2) \end{bmatrix}. \tag{2.20}$$

2.4.2 Operationen auf mehreren Qubits

Die Gatter, die auf zwei Signalen agieren, sind beim klassischen Computer AND, OR und XOR, sowie ihre invertierten Gegenstücke NAND, NOR und NXOR. Für diese klassischen Gatter gibt es keine analogen Quantenoperationen, da alle diese Operationen nicht reversible sind.

Die wichtigste Operation für zwei Qubits ist das kontrollierte NOT-Gatter, welches als CNOT-Gatter bezeichnet wird. Das CNOT-Gatter kann als Verallgemeinerung des klasssichen XOR-Gatters angesehen werden. Die Funktionsweise vom CNOT-Operator wird über

$$U_{\text{CNOT}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{2.21}$$

beschrieben. Angewandt auf den Zustandsvektor $[\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11}]^\intercal$ ergibt sich eine Vertauschung der Amplituden α_{10} und α_{11}. Diese Vertauschung macht sich aber nur bemerkbar, wenn bei der Messung des ersten Qubits eine 1 erhalten wird, denn dann ist

$$|\psi'\rangle = \frac{\alpha_{11}\,|10\rangle + \alpha_{10}\,|11\rangle}{\sqrt{\alpha_{10}^2 + \alpha_{11}^2}}. \tag{2.22}$$

Häufig begegnet einem die Schreibweise $|A,\, B\rangle \to |A,\, B \oplus A\rangle$ für die Anwendung der CNOT-Operation auf die Zustände $|A\rangle$ und $|B\rangle$ der beiden Qubits.

Die wichtigste Operation auf einem 3-Qubitsystem ist die Toffoli-Matrix, die der CNOT-Operation sehr ähnlich ist. Durch die Anwendung der Toffoli-Matrix wird der Zustand $|A,\, B,\, C\rangle$ in den Zustand $|A,\, B,\, C \oplus AB\rangle$ überführt. Bei der Betrachtungsweise über die Amplituden wird durch die Anwendung der Toffoli-Matrix die Amplituden α_{110} und α_{111} miteinander vertauscht.

Mithilfe der Toffoli-Operation lässt sich jede klassische Logik simulieren. Für klassische Schaltkreise sind die benötigten Komponenten das NAND-Gatter und ein sogennanter FANOUT, der das Bit repliziert. Das Klonen einer Superposition ist nicht möglich. Für die Simumaltion eines klassischen Systems wird keine Superposition eines Qubits benötigt. Wird sich darauf beschränkt, dass der Zustand eines Qubits nur $|0\rangle$ oder $|1\rangle$ sein kann, dann lässt sich auch ein FANOUT realisieren. Die NAND-Logik wird durch die Eingabe $|A,\, B,\, 1\rangle$ erhalten die durch die Toffoli-Operation abgebildet wird auf $|A,\, B,\, 1 \oplus AB\rangle = |A,\, B,\, \neg(AB)\rangle$. Ein FANOUT lässt sich durch die Eingabe $|1,\, A,\, 0\rangle$ realisieren, denn hier wird durch Anwendung der Toffoli-Operation die Ausgabe $|1,\, A,\, 0 \oplus 1A\rangle = |1,\, A,\, A\rangle$.

3 Quantenschaltkreis

In diesem Kapitel wollen wir zunächst den Begriff des Quantenschaltkreises einführen. Anschließend wird skizziert, welche elementaren Operationen für die Darstellung eines Quantenschaltkreises benötigt werden. Wir werden sehen, dass zwar alle unitären Transformationen prinzipiell als Gatter verwendet werden können, aber einige ausgewählte ausreichen um alle unitären Transformationen approximativ darzustellen. Abschließend wird der Begriff der Quantenschaltkreisfamilie eingeführt, der die Umsetzung von Algorithmen mithilfe von Quantenschaltkreisen ermöglicht.

3.1 Definition des Quantenschaltkreises

Der Begriff des Quantenschaltkreises ist wie folgt definiert [7, 8].

Definition 10. *Ein Quantenschaltkreis $C = (n, (U_1, U_2, \ldots, U_L))$ ist eine Reihe von unitären Transformationen, auch Gatter genannt, die auf dem Hilbertraum der n-Qubits wirken. Die Transformationen $U_1, U_2, \ldots, U_L$ sind aus einer definierten Gattermenge $\mathcal{G}$. L wird als Länge des Quantenschaltkreises bezeichnet.*

Die in der Gattermenge G enthaltenen Gatter können auf beliebige Qubits angewandt werden. Beispiele für Gattermengen $\mathcal{G}$ werden im nächsten Abschnitt betrachtet.

Ein Quantenschaltkreis C kann als Funktion verstanden werden, die jeden n-Qubitzustandsvektor $|\psi\rangle$ auf $U_L \cdots U_2 \cdot U_1 |\psi\rangle$ abbildet. Der Quantenschaltkreises $C = (1, (U))$ entspricht demnach der Anwendung eines einzelnen Gatters auf den Quantenzustand $|\psi\rangle$, der am Eingang des Quantenschaltkreises anliegt. Ein Beispiel für die Visualisierung eines Quantenschaltkreis ist in Abbildung 3.1 dargestellt. Die zeitliche Reihenfolge wird von links nach rechts gelesen. Gleichzeitig stattfindende Transformationen werden durch das Tensorprodukt miteinander kombiniert. Laut Definition 10 ist der Quantenschaltkreis aus Abbildung 3.1 beschrieben durch $(3, (U_1 \otimes U_2, \mathbf{I}_2 \otimes U_3 \otimes \mathbf{I}_2))$. Das Ergebnis der Abbildung des klassischen Eingangssignals $|\psi_1, \psi_2, \psi_3\rangle$ ist $(\mathbf{I}_2 \otimes U_3 \otimes \mathbf{I}_2) \cdot (U_1 \otimes U_2) |\psi_1, \psi_2, \psi_3\rangle$.

3.2 n-Qubitgatter

Solange Transformationen unitär sind, sind sie als Gatter in einem Quantenschaltkreis zulässig. Wird sich aber nicht auf eine festgelegte Gattermenge geeinigt, ist die Vergleichbarkeit

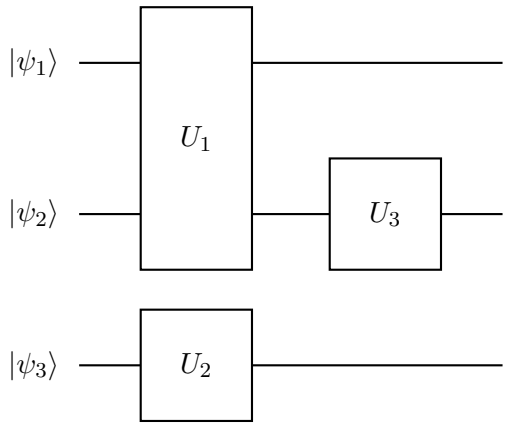

Abbildung 3.1: Beispielhafter Quantenschaltkreis auf 3 Qubits, die als klassische Eingabe konfiguriert sind.

der Länge L eines Quantenschaltkreises nicht gewährleistet An dieser Stelle soll aus diesem Grund skizziert werden, wie sich die Menge unitärer Transformationen einschränken lassen. Der vollständige Beweis findet sich in der Literatur wieder, bspw. in dem Buch von Nielsen und Chuang [5], sowie in dem wissenschaftlichem Artikel von Barenco [9]. Der folgende Satz ist zu zeigen:

Satz 11. *Jedes n-Qubitgatter kann durch die Kombination aus CNOT-Transformationen und 1-Qubitgattern dargestellt werden.*

Beweisskizze Satz 11

Um diesen Satz zu zeigen, ist es hilfreich zunächst die folgende Aussage zu zeigen.

Lemma 12. *Jede unitäre* 3×3 *Matrix* U *lässt sich in drei unitäre, 2-Level Matrizen* U_1*,* U_2*,* U_3 *zerlegen.*

Beweisskizze Lemma 12

Die Matrix U sei von folgender Form

$$U = \begin{bmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{bmatrix}. \tag{3.1}$$

Nun soll U so in die unitären 2-Level-Matrizen U_1, U_2, U_3 zerlegt werden, dass $U_3U_2U_1U = \mathbf{I}_3$ gilt. Für die Matrizen U_1, U_2, U_3 gilt

$$U_1 = \begin{bmatrix} b_{11} & b_{12} & 0 \\ b_{21} & b_{22} & 0 \\ 0 & 0 & 1 \end{bmatrix}, U_2 = \begin{bmatrix} c_{11} & 0 & c_{12} \\ 0 & 1 & 0 \\ c_{21} & 0 & c_{22} \end{bmatrix}, U_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & d_{11} & d_{12} \\ 0 & d_{21} & d_{22} \end{bmatrix}. \tag{3.2}$$

Es kann gezeigt werden, dass eine solche Zerlegung gefunden werden kann. Das Ziel ist es U_1 und U_2 so zu konstruieren, dass die erste Spalte der Matrix U_2U_1U den Wert (1, 0, 0) annimmt. Wir wählen U_1 so, dass die Matrix U_1U folgende Form annimmt:

$$U_1U = \begin{bmatrix} a'_{11} & a'_{21} & a'_{31} \\ 0 & a'_{22} & a'_{32} \\ a'_{13} & a'_{23} & a'_{33} \end{bmatrix}. \tag{3.3}$$

Dann wird U_2 so gewählt, dass

$$U_2U_1U = \begin{bmatrix} 1 & a''_{21} & a''_{31} \\ 0 & a''_{22} & a''_{32} \\ 0 & a''_{23} & a''_{33} \end{bmatrix}. \tag{3.4}$$

Aufgrund der unitären Eigenschaft von U, U_1 und U_2 muss auch das Ergebnis der Multiplikation eine unitäre Matrix sein. Dadurch muss $a''_{21} = 0$ und $a''_{31} = 0$ gelten. Bei U_3 und U_2U_1U handelt es sich um unitäre, 2-Level-Matrizen und U_2U_1U hat dieselbe Form wie U_3. Die Matrix U_3 wird dann so gewählt, dass die Einträge d_{11} bis d_{22} jeweils das komplex Konjugierte und Normierte der Einträge a''_{22} bis a''_{33} sind. Durch Multiplikation von U_3 mit U_2U_1U wird dann die Einheitsmatrix $\mathbf{I}_3$ erhalten und dadurch ist gezeigt, dass

$$U = U_1^\dagger U_2^\dagger U_3^\dagger \tag{3.5}$$

gilt. □

Allgemein lässt sich dieses Vorgehen auf unitäre $(d \times d)$-Matrizen übertragen. Um jede Spalte so zu transformieren, dass am Ende die Einheitsmatrix erhalten wird, werden für die k-te Spalte jeweils $(d - k)$ unitäre 2-Level-Matrizen benötigt. Es lässt sich daraus das folgende Korollar ableiten.

Korollar 13. *Jede unitäre d-dimensionale Matrix lässt sich in k unitäre 2-Level-Matrizen zerlegen mit* $k \leq {}^{(d-1)(d-2)}/_{2}$.

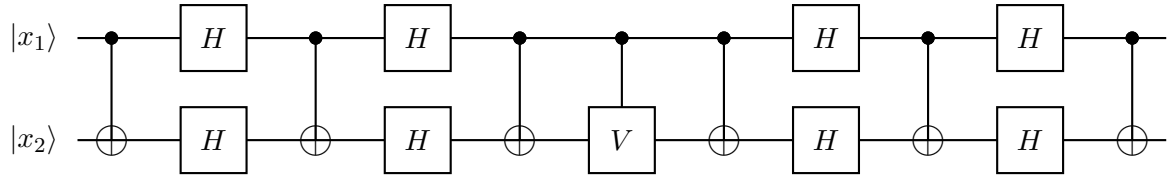

Abbildung 3.2: Umsetzung der Transformation aus Gleichung 3.6 mithilfe von CNOT- und Hadamardgattern sowie dem Gatter aus Gleichung 3.8

Jetzt muss nur noch gezeigt werden, dass mithilfe von CNOT und 1-Qubitgattern alle unitären, 2-Level-Matrizen dargestellt werden können. Wie das funktioniert soll an einem kurzen Beispiel gezeigt werden. Gegeben sei die folgende unitäre Matrix

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & c & 0 & d \end{bmatrix}. \tag{3.6}$$

Es ist schnell zu erkennen, dass ein 1-Qubitgatter der Form

$$V = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \tag{3.7}$$

benötigt wird, welches auf die Amplituden der Zustände $|01\rangle$ und $|11\rangle$ wirkt. Werden die Amplituden α_{01} und α_{10} miteinander vertauscht, lässt sich V als kontrollierte Matrix V_{C} darstellen, wobei das erste Qubit als Kontrollqubit und das zweite Qubit als Zielqubit dient. Es ist V_{C} von folgender Form:

$$V_{\mathrm{C}} = \begin{bmatrix} \mathbf{I}_2 & 0 \\ 0 & V \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{bmatrix}. \tag{3.8}$$

Um diese Vertauschung realisieren zu können, benötigen wir sowohl das CNOT-, als auch das Hadamard-Gatter. In Abbildung 3.2 ist gezeigt wie mithilfe dieser Gatter die Amplituden α_{01} und α_{10} vertauscht werden können. Anschließend kann die kontrollierte Transformation V_{C}

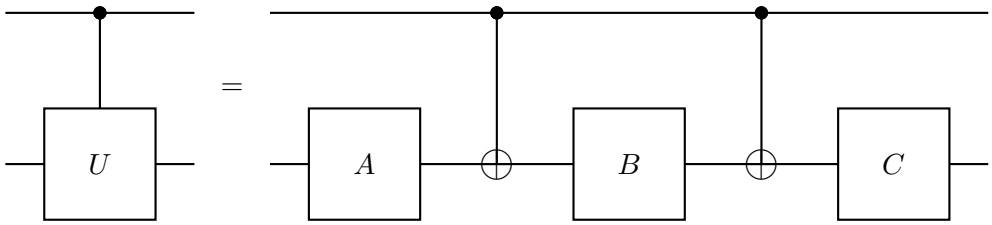

Abbildung 3.3: Die Zerlegung einer kontrollierten (4×4)-Matrix in CNOT- und 1-Qubitgatter.

angewandt und schlussendlich können die Amplituden wieder zurückgetauscht werden. Mit $H_2 = (H \otimes H)$ ergibt sich für die Transformationsmatrix des Quantenschaltkreises

$$\begin{aligned} U &= U_{\text{CNOT}} \cdot H_2 \cdot U_{\text{CNOT}} \cdot H_2 \cdot U_{\text{CNOT}} \cdot V_{\text{C}} \cdot U_{\text{CNOT}} \cdot H_2 \cdot U_{\text{CNOT}} \cdot H_2 \cdot U_{\text{CNOT}} \\ &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & c & 0 & d \end{bmatrix}. \end{aligned} \tag{3.9}$$

Dieses Vorgehen funktioniert für beliebig große n-Qubitsysteme und skaliert mit $\mathcal{O}(n)$. Bei größeren n-Qubitsystemen als in dem gewählten Beispiel treten kontrollierte Matrizen mit mehr Kontrollqubits auf. Diese gilt es noch in (4×4)-Matrizen zu zerlegen. Ebenso muss eine Zerlegung für die kontrollierten (4×4)-Matrizen in CNOT- und 1-Qubitgatter gefunden werden.

Lemma 14. *Sei U_{C} eine kontrollierte (4×4)-Matrix mit der (2×2)-Untermatrix U. Es existieren unitäre Matrizen A, B, C mit $ABC = \mathbf{I}_2$ und $AXBXC = U$, sodass gilt*

$$U_{\text{C}} = (\mathbf{I}_2 \otimes A) \cdot U_{\text{CNOT}} \cdot (\mathbf{I}_2 \otimes B) \cdot U_{\text{CNOT}} \cdot (\mathbf{I}_2 \otimes C). \tag{3.10}$$

Diese Zerlegung ist in Abbildung 3.3 visualisiert. Ist das erste Qubit im Zustand $|1\rangle$, so wird die Matrix U auf das zweite Qubit angewandt. Wenn sich das erste Qubit im Zustand $|0\rangle$ befindet, wird $ABC = \mathbf{I}_2$ auf das zweite Qubit angewandt. Diese Zerlegung ist von konstanter Größe und skaliert somit nicht mit der Anzahl an Qubits.

Größere kontrollierte Matrizen müssen zunächst erst in kontrollierte (4×4)-Matrizen zerlegt werden. Insgesamt werden $\mathcal{O}(n)$ Matrizen benötigt, um eine 2-Level-Matrix in kontrollierte 2-Qubittransformationen und CNOT-Gatter zu zerlegen.

Fassen wir die Ergebnisse der vorangegangenen Beweisskizze zusammen, so kommen wir zu folgendem Schluss. Jede $(2^n \times 2^n)$-Transformation auf n-Qubits kann in 2-Level-Matrizen zerlegt werden. Hierfür werden $\mathcal{O}\left((2^n)^2\right) = \mathcal{O}(4^n)$ 2-Level-Matrizen benötigt. Diese 2-Level-Matrizen können mithilfe von Hadamard- und CNOT-Gattern in die Form von mehrfach kon-

trollierten n-Qubitgatter gebracht werden. Für jede 2-Level-Matrix werden dafür $\mathcal{O}(n)$ Transformationen benötigt. Die kontrollierten n-Qubitgatter können wiederrum in kontrollierte 2-Qubittransformationen und CNOT-Gatter zerlegt werden. Hierfür werden jeweils $\mathcal{O}(n)$ kontrollierte 2-Qubittransformationen und CNOT-Gatter benötigt. Die Zerlegung der kontrollierten 2-Qubittransformationen in 1-Qubitgatter und CNOT-Gatter benötigt $\mathcal{O}(1)$ viele Gatter. Insgesamt ergibt werden $\mathcal{O}(n^2 4^n)$ 1-Qubitgatter und CNOT-Gatter benötigt um jede beliebige n-Qubittransformation zu zerlegen. □

Aus obiger Beweisskizze ergibt sich das folgende Korollar.

Korollar 15. *Es sei die Gattermenge* $\mathcal{G} = \{ U_{\text{CNOT}} \} \cup \left\{ U \;\middle|\; U \in \mathbb{C}^{2\times 2} \right\}$. *Jede beliebige n-Qubittransformation K lässt sich in $\mathcal{O}(n^2 4^n)$ Gatter V zerlegen mit $V \in \mathcal{G}$.*

Eine weitere Einschränkung der Gattermenge lässt sich vornehmen, wodurch alle unitären Transformationen approximativ dargestellt werden können.

Satz 16. *Mithilfe des Hadamard-Gatters H, dem $\pi/8$-Gatter und dem CNOT-Gattern lassen sich alle unitären Transformationen näherungsweise darstellen. Die Anzahl der verwendeten Gatter bestimmt dabei die Genauigkeit mit der diese Transformationen dargestellt werden können.*

3.3 Quantenschaltkreisfamilie

Zunächst soll die Definition der Turingmaschine rekapituliert werden, da diese einen wichtigen Bestandteil der Quantenschaltkreisfamilie darstellt.

Definition 17. *Eine Turingmaschine (TM) ist definiert als das Tupel* $(\Sigma, Q, q_0, q_{\text{E}}, \delta)$. *Es ist*

- Σ *das Alphabet, auf dem die TM agiert,*
- Q *die endliche Menge aller Zustände, die die TM annehmen kann mit*
- q_0 *dem Startzustand und*
- q_{E} *dem Endzustand sowie*
- $\delta\colon Q \times (\Sigma \cup \{ \square \}) \to Q \times (\Sigma \cup \{ \square \}) \times \{ \text{L}, \text{N}, \text{R} \}$ *die Übergangsfunktion, die beschreibt, wie sich die TM abhängig vom Zustand und eingelesenen Zeichen des Alphabets verhält.*

Eine Turingmaschine besitzt ein unendliches Speicherband, dessen Zellen mit den Zahlen aus $\mathbb{Z}$ nummeriert sind und einen Lese-/Schreibkopf, der sich entlang des Speicherbandes bewegen kann. Dieses Speicherband wird mit einer Eingabe $x \in \Sigma^n$ der Länge n an den Positionen 0 bis $n-1$ initialisiert und enthält in allen anderen Zellen das Leersymbol $\square$. Die TM startet im Zustand q_0 mit dem Lese-/Schreibkopf an der Position 0 des Speicherbandes. Das Verhalten

der Turingmaschine ist definiert durch die Übergangsfunktion δ. Diese beschreibt, wie sich der Lese-/Schreibkopf abhängig vom Zustand q und gelesenem Zeichen σ verhält. Pro Übergang kann der Lese-/Schreibkopf nur in der gelesenen Speicherzelle das Zeichen ersetzen, einen neuen Zustand annehmen und sich auf dem Speicherband eine Zelle nach links oder rechts bewegen, oder an der aktuellen Position verweilen. Eine TM hält, wenn sie sich im Zustand q_{E} befindet. Der Inhalt des Speicherbandes, nachdem die TM in den Zustand q_{E} übergegangen ist, wird als Ausgabe der TM bezeichnet. Die Anzahl der Übergänge, die die TM benötigt, um in den akzeptierenden Zustand zu wechseln, wird als Laufzeit t bezeichnet.

Eine Quantenschaltkreisfamilie ist wie folgt definiert.

Definition 18. *Es sei Σ eine endliche Menge an Zeichen. Eine Quantenschaltkreisfamilie $\mathcal{C} = \{C_x\}_{x\in\Sigma^*}$ wird beschrieben durch eine Turingmaschine, die für jede Eingabe $x \in \Sigma^*$ die Beschreibung eines Quantenschaltkreises C_x ausgibt, der auf einem Quantenzustand $|0^k\rangle$ wirkt. Wir bezeichnen die Laufzeit der Turingmaschine auch als Laufzeit der Quantenschaltkreisfamilie.*

Wir sagen, eine Quantenschaltkreisfamilie $\mathcal{C}$ basiert auf einer Gattermenge $\mathcal{G}$, wenn jeder Quantenschaltkreis C_x auf der Gattermenge $\mathcal{G}$ basiert.

Mithilfe der Quantenschaltkreisfamilie ist es nun möglich Algorithmen als Quantenschaltkreise zu implementieren, da durch die Turingmaschine für unterschiedliche Eingaben der für den Algorithmus notwendige Quantenschaltkreis konstruiert wird. Die Turingmaschine erhält als Eingabe $x \in \Sigma^*$ und gibt den Quantenschaltkreis C_x aus, der den Algorithmus für die Eingabe x umsetzt. Zu diesem Zweck bestimmt die TM zunächst die Anzahl der benötigten Qubits k. Diese entsprechen mindestens der Länge der Eingabe x, es können aber auch mehr Qubits benötigt werden. Dies ist beispielsweise dann der Fall, wenn die Eingabe x nicht im Binäralphabet, sondern in einem beliebigen Alphabet dargestellt wird. Das Alphabet muss binär kodiert werden und dadurch werden mehr Qubits benötigt.

Anschließend muss der Eingabezustand $|0^k\rangle$ des Quantenschaltkreises initialisiert werden. Dies kann mithilfe des Pauli-Gatters X realisiert werden, da dieses für einzelne Qubits die Amplituden von 0 und 1 vertauscht. So kann $\left|0^k\right\rangle$ in die eigentliche Eingabe $|x\rangle$ umgewandelt werden. Die Turingmaschine bestimmt zunächst auf welche Qubits das X-Gatter angewandt werden muss. Das Qubit, auf welches das X-Gatter wirkt, sowie die vier Einträge der Transformation werden auf das Speicherband geschrieben und durch ein beliebiges Trennzeichen von der vorherigen und nächsten Eingabe abgetrennt.

Nachdem die Initialisierung im Quantenschaltkreis abgeschlossen ist, wirken die eigentlich Transformationen, die den Algorithmus umsetzen. Diese müssen ebenfalls von der Turingmaschine bestimmt und mit der Angabe auf welches Qubit sie wirken, auf das Speicherband geschrieben werden. Wie die Turingmaschine dabei vorgeht ist für jede Quantenschaltkreisfamilie in der Übergangsfunktion δ festgelegt.

4 Quantenturingmaschine

Nachdem sich in dieser Arbeit zunächst dem Quantenschaltkreis als Berechnungsmodell der Quanteninformation gewidmet wurde, wird im Folgenden die Quantenturingmaschine (QTM) betrachtet. Die Quantenturingmaschine wurde zuerst in der Arbeit von D. Deutsch im Jahre 1985 definiert [10]. Aufbauend auf dieser Arbeit veröffentlichten E. Bernstein und U. Vazirani 1993 eine Arbeit, in der die QTM von Deutsch aus komplexitätstheoretischer Sicht kritisiert wurde. Des Weiteren geben sie in dieser Veröffentlichung eine veränderte Definition der QTM an, mit der sie ihre Kritikpunkte berücksichtigen. In dieser Arbeit zeigten die Autoren, dass basierend auf ihrer Definition eine universelle QTM entworfen werden kann, die jede QTM mit einer Genauigkeit ϵ simulieren kann und dabei nur einen polynomiellen Mehraufwand betreibt [11]. Noch im gleichen Jahr veröffentlichte A. Yao eine Arbeit, in der er zeigte, dass eine QTM effizient durch eine Quantenschaltkreisfamilie simuliert werden kann [12]. Im Jahr 1999 folgte eine Arbeit von H. Nishimura und M. Ozawa, in der die Autoren die Komplexität von Quantenturingmaschinen und Quantenschaltkreisfamilien für spezielle Fälle verglichen haben [13]. Von den gleichen Autoren gibt es weitere wissenschaftliche Artikel, die sich diesem Themengebiet widmen [14, 15, 16, 17, 18]. Im Jahr 2002 veröffentlichte U. Vazirani einen Übersichtsartikel, in dem er sich mit verschiedenen Aspekten der Quantenturingmaschine und der Quantenschaltkreise auseinandersetzt [19]. Im Jahr 2005 wurde zum Thema Quantenturingmaschine eine Masterarbeit von C. Westergaard verfasst, die die Arbeiten von H. Nishimura und M. Ozawa zusammenfasst und diese in einer einheitlichen Notation präsentiert [20]. Die in den Abschnitten 4.1 und 4.2 verwendeten Defintionen, Beweise und Erläuterungen basieren zum Großteil auf den Arbeiten von Bernstein und Vazirani [11], Yao [12], Nishimura und Ozawa [13] und dem Übersichtsartikel von Vazirani [19].

Ziel dieses Abschnitts ist es dem Leser das Berechnungsmodell der Quantenturingmaschine näher zu bringen und die polynomielle Äquivalenz von Quantenturingmaschine und Quantenschaltkreisfamilien zu zeigen. Dazu wird zunächst die Quantenturingmaschine ähnlich zur klassischen Turingmaschine definiert. Im Anschluss wird präzisiert, welche Einschränkungen es für die Übergangsfunktion δ geben muss, da diese auf der Quantenebene agiert. Am Ende des Kapitels wird gezeigt, wie Quantenturingmaschine und Quantenschaltkreisfamilie ineinander überführt werden können. Die Länge L der Quantenschaltkreisfamilie ist dabei polynomiell abhängig von der Laufzeit t, der Zustandsmengengröße $|Q|$ und der Alphabetsgröße $|\Sigma|$ der Quantenturingmaschine. Des Weiteren ist der Konstruktionsalgorithmus selbst effizient in der Laufzeit t, Zustandsmengengröße $|Q|$ und der Alphabetsgröße $|\Sigma|$.

4.1 Definition der Quantenturingmaschine

Für die Definition der Quantenturingmaschine wird zunächst folgende Definition benötigt, die in Analogie zu der Definition der effizient berechenbaren reellen Zahlen von Ko und Friedman [21] formuliert ist.

Definition 19. *Es sei $\widetilde{\mathbb{C}}$ die Menge der effizient berechenbaren, komplexen Zahlen. Für alle $x + \mathrm{i}y \in \widetilde{\mathbb{C}}$ gilt, dass jeweils das j-te Bit von x und y durch eine Turingmaschine in polynomieller Zeit in j berechnet werden kann.*

Der Hauptunterschied zur klassischen Turingmaschine liegt in der Übergangsfunktion δ. Die Übergangsfunktion ist durch den Schrittoperator $\mathcal{S}$ festgelegt. Ähnlich zur klassischen Turingmaschine ist die Quantenturingmaschine wie folgt definiert.

Definition 20. *Eine Quantenturingmaschine (QTM) ist definiert als das Tupel $(\Sigma, Q, q_0, q_\mathrm{E}, \mathcal{S})$. Es ist*

- *Σ das Alphabet, auf dem die QTM agiert,*
- *Q die endliche Menge aller Zustände, die die QTM annehmen kann mit*
- *dem Startzustand q_0 und*
- *dem Endzustand q_E sowie*
- *dem unitäre Schrittoperator $\mathcal{S}$ aus dem Hilbertraum $\mathcal{H}_\mathbb{Z} \otimes \mathcal{H}_Q \otimes \left(\bigotimes_{i=-\infty}^{\infty} \mathcal{H}_{\Sigma\cup\{\,\square\,\}}\right)$ mit*

$$\begin{aligned}
\mathcal{H}_\mathbb{Z} &= \operatorname{span}\{\, |m\rangle \;\mid\; m \in \mathbb{Z} \,\}, \\
\mathcal{H}_Q &= \operatorname{span}\{\, |q\rangle \;\mid\; q \in Q \,\}, \\
\mathcal{H}_{\Sigma\cup\{\,\square\,\}} &= \operatorname{span}\{\, |\sigma\rangle \;\mid\; \sigma \in \Sigma \cup \{\,\square\,\} \,\},
\end{aligned}$$

der definiert ist als

$$\begin{aligned}
\mathcal{S} = \sum_{m=-\infty}^{\infty} & |m-1\rangle\langle m| \otimes (A_\mathrm{L})_m \otimes \mathbf{I}_\infty \\
& + |m\rangle\langle m| \otimes (A_\mathrm{N})_m \otimes \mathbf{I}_\infty \\
& + |m+1\rangle\langle m| \otimes (A_\mathrm{R})_m \otimes \mathbf{I}_\infty .
\end{aligned} \tag{4.1}$$

$(A_{\mathrm{L}})_m$, $(A_{\mathrm{N}})_m$ *und* $(A_{\mathrm{R}})_m$ *sind aus dem Hilbertraum* $\mathcal{H}_Q \otimes \mathcal{H}_{\Sigma \cup \{\,\square\,\}}$ *und es gilt*

$$\left\langle q',\, \sigma' \right| A_{\mathrm{L}} \left| q,\, \sigma \right\rangle = \delta(q,\, \sigma,\, \mathrm{L},\, q',\, \sigma') \tag{4.2}$$

$$\left\langle q',\, \sigma' \right| A_{\mathrm{N}} \left| q,\, \sigma \right\rangle = \delta(q,\, \sigma,\, \mathrm{N},\, q',\, \sigma') \tag{4.3}$$

$$\left\langle q',\, \sigma' \right| A_{\mathrm{R}} \left| q,\, \sigma \right\rangle = \delta(q,\, \sigma,\, \mathrm{R},\, q',\, \sigma') \tag{4.4}$$

mit $\sigma \in \Sigma \cup \{\,\square\,\}$ *dem Bandinhalt der Speicherzelle* m *und der Übergangsfunktion* $\delta\colon Q \times (\Sigma \cup \{\,\square\,\}) \times \{\,\mathrm{L},\, \mathrm{N},\, \mathrm{R}\,\} \times Q \times (\Sigma \cup \{\,\square\,\}) \to \widetilde{\mathbb{C}}$.

Der Initialzustand einer Quantenturingmaschine ist

$$|0\rangle \otimes |q_0\rangle \otimes \left(\bigotimes_{i=-\infty}^{-1} |\square\rangle \right) \otimes \left(\bigotimes_{i=0}^{n-1} |\sigma_i\rangle \right) \otimes \left(\bigotimes_{i=n}^{\infty} |\square\rangle \right), \tag{4.5}$$

wobei sich ähnlich wie bei einer klassischen Turingmaschine aus rein technischer Sicht kein unendliches Speicherband realisieren lässt. Der Lese-/Schreibkopf befindet sich an der Position 0, die Turingmaschine im Zustand q_0 und die Zellen auf dem Speicherband links und rechts von der Eingabe sind mit $|\square\rangle$ initialisiert. Die Zellen 0 bis $n-1$ sind mit der Eingabe $x = (\sigma_0,\, \sigma_1,\, \ldots,\, \sigma_{n-1})$ der Länge n initialisiert. Nach jedem Schritt der QTM, wird der Zustand Q in der Basis $(|q_{\mathrm{E}}\rangle \langle q_{\mathrm{E}}|\,,\, \mathbf{I} - |q_{\mathrm{E}}\rangle \langle q_{\mathrm{E}}|)$ gemessen. Wir sagen die QTM hält, wenn sie im Zustand q_{E} gemessen wird. Die Haltebedingung ist somit probabilistisch. Selbiges gilt auch für die Ausgabe einer QTM. Die Anzahl der durchgeführten Schritte, bis die QTM hält, wird als Laufzeit t bezeichnet.

Gleichung 4.1 entspricht nicht der bisher eingehaltenen Konvention bezüglich der Reihenfolge des Tensorprodukts. Es lassen sich jedoch nur auf diese Weise der Schrittoperator $\mathcal{S}$ und die Matrizen $(A_{\mathrm{L}})_m$, $(A_{\mathrm{N}})_m$ und $(A_{\mathrm{R}})_m$ verständlich darstellen. Die Matrizen $(A_{\mathrm{L}})_m$, $(A_{\mathrm{N}})_m$ und $(A_{\mathrm{R}})_m$ wirken auf den aktuellen Zustand q der QTM und den Inhalt der m-ten Speicherzelle σ. Auf dem Rest des unendlichen Speicherbandes wirkt die Einheitsmatrix $\mathbf{I}_\infty$. Die Übergangsfunktionstransformationen A_{L}, A_{N} und A_{R} lassen sich in Matrixschreibweise ausdrücken als

$$A_d = \begin{bmatrix} \delta_{1,1,d,1,1} & \cdots & \delta_{1,|\Sigma|+1,d,1,1} & \delta_{2,1,d,1,1} & \cdots & \delta_{|Q|,|\Sigma|+1,d,1,1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \delta_{1,1,d,1,|\Sigma|+1} & \cdots & \delta_{1,|\Sigma|+1,d,1,|\Sigma|+1} & \delta_{2,1,d,1,|\Sigma|+1} & \cdots & \delta_{|Q|,|\Sigma|+1,d,1,|\Sigma|+1} \\ \delta_{1,1,d,2,1} & \cdots & \delta_{1,|\Sigma|+1,d,2,1} & \delta_{2,1,d,2,1} & \cdots & \delta_{|Q|,|\Sigma|+1,d,2,1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \delta_{1,1,d,|Q|,|\Sigma|+1} & \cdots & \delta_{1,|\Sigma|+1,d,|Q|,|\Sigma|+1} & \delta_{2,1,d,|Q|,|\Sigma|+1} & \cdots & \delta_{|Q|,|\Sigma|+1,d,|Q|,|\Sigma|+1} \end{bmatrix},$$

wobei $\delta_{i,\,j,\,d,\,k,\,l} = \delta(q_i,\, \sigma_j,\, d,\, q_k,\, \sigma_l)$ mit $q_i,\, q_k \in Q$, $\sigma_j,\, \sigma_l \in \Sigma \cup \{\,\square\,\}$ und $d \in \{\,\mathrm{L},\, \mathrm{N},\, \mathrm{R}\,\}$.

Die Übergangsfunktion δ gibt die Amplitude zurück, mit der eine QTM, die sich im Zustand q befindet und das Zeichen σ liest, das Zeichen σ' schreibt, in einen Zustand q' übergeht und

sich in Richtung d bewegt. Welchen Einschränkungen die Übergangsfunktion δ unterliegt, wird durch die unitäre Einschränkung des Schrittoperators $\mathcal{S}$ bestimmt.

Lemma 21. *Die Übergansgfunktion* $\delta\colon Q \times (\Sigma \cup \{ \square \}) \times \{ \mathrm{L}, \mathrm{N}, \mathrm{R} \} \times Q \times (\Sigma \cup \{ \square \}) \to \widetilde{\mathbb{C}}$ *unterliegt folgenden Einschränkungen:*

1. *Für beliebige* $(q, \sigma) \in Q \times \Sigma$ *muss gelten:*

$$\sum_{\substack{p \in Q,\, \tau \in \Sigma, \\ d \in \{\mathrm{L}, \mathrm{N}, \mathrm{R}\}}} |\delta(q, \sigma, d, p, \tau)|^2 = 1 \tag{4.6}$$

2. *Für beliebige* $(q, \sigma), (q', \sigma') \in Q \times \Sigma$ *mit* $(q, \sigma) \neq (q', \sigma')$ *muss gelten:*

$$\sum_{\substack{p \in Q,\, \tau \in \Sigma, \\ d \in \{\mathrm{L}, \mathrm{N}, \mathrm{R}\}}} \delta(q', \sigma', d, p, \tau)^* \cdot \delta(q, \sigma, d, p, \tau) = 0 \tag{4.7}$$

3. *Für alle* $(q, \sigma, \sigma'), (q', \tau, \tau') \in Q \times \Sigma \times \Sigma$ *muss gelten:*

$$\begin{aligned} &\sum_{p \in Q} \delta(q, \sigma, \mathrm{N}, p, \sigma')^* \cdot \delta(q', \tau, \mathrm{L}, p, \tau') \\ &\quad + \delta(q, \sigma, \mathrm{R}, p, \sigma')^* \cdot \delta(q', \tau, \mathrm{N}, p, \tau') = 0 \end{aligned} \tag{4.8}$$

4. *Für alle* $(q, \sigma, \sigma'), (q', \tau, \tau') \in Q \times \Sigma \times \Sigma$ *muss gelten:*

$$\sum_{p \in Q} \delta(q, \sigma, \mathrm{L}, p, \sigma')^* \cdot \delta(q', \tau', \mathrm{R}, p, \tau) = 0 \tag{4.9}$$

Im Anhang A wird gezeigt, wie diese Eigenschaften aus der Unitarität des Schrittoperators $\mathcal{S}$ hergeleitet werden können.

4.2 Simulation einer Quantenturingmaschine durch eine Quantenschaltkreisfamilie

Um die Messung nach jeder Durchführung des Schrittoperators nicht im Quantenschaltkreis berücksichtigen zu müssen, wird die Quantenturingmaschine ohne wiederholte Zustandsmessung definiert.

Definition 22. *Eine Quantenturingmaschine ohne wiederholte Zustandsmessung ist eine Quantenturingmaschine nach Definition 20, bei der nicht nach jeder Ausführung des Schrittoperators gemessen wird. Stattdessen wird nur nach einer gegebenen Laufzeit* t *durch eine finale Messung geprüft, ob die QTM gehalten hat.*

Das die Quantenturingmaschine ohne wiederholte Zustandsmessung äquivalent zu der vorher definierten Quantenturingmaschine ist, wird in folgendem Satz festgehalten.

Satz 23. *Eine QTM M ohne wiederholte Zustandsmessung befindet sich nach der vorgegebenen Laufzeit t und finaler Messung im gleichen Quantenzustand wie eine QTM M', bei der nach jedem Schritt der Zustand gemessen wird. Des Weiteren halten beide Quantenturingmaschinen M und M' mit den gleichen Wahrscheinlichkeit p_x in derselben Ausgabe x.*

Beweis

Sei $M' = (\Sigma, Q, q_0, q_\mathrm{E}, \mathcal{S})$ eine QTM mit Zustandsmessung P nach jeder Ausführung des Schrittoperators $\mathcal{S}$ mit Ausgabemenge $A \subseteq \mathbb{Z} \times \Sigma^*$. Es sei $|\psi_t\rangle$ der Zustand der QTM M' nach der Ausführung des t-ten Schrittoperators, $|\psi'_t\rangle$ der Zustand nach der t-ten Zustandsmessung P und $|\psi_0\rangle$ der Initialzustand der QTM. Es soll $\delta(q_\mathrm{E}, \sigma, \mathrm{N}, q_\mathrm{E}, \sigma) = 1$ für beliebige $\sigma \in \Sigma$ gelten.

Mit $p_{x,t}$ bezeichnen wir die Wahrscheinlichkeit dafür, dass die QTM M' in der Ausgabe x nach einer beliebigen Laufzeit t hält. Die Ausgabe x enthält neben dem Inhalt der Bandzellen noch die Bandposition m auf der sich der Lese-/Schreibkopf der QTM befindet. Mit p_t wird die Wahrscheinlichkeit bezeichnet, dass die QTM M' nach einer beliebigen Laufzeit t noch nicht gehalten hat. Es ist

$$p_t = 1 - \sum_{T=1}^{t} \sum_{x \in A} p_{x,T}.$$

Der Quantenzustand $|\psi_t\rangle$ setzt sich wie folgt zusammen.

$$|\psi_t\rangle = \frac{1}{\sqrt{p_{t-1}}} \left(\sum_{x \in A} \sqrt{p_{x,t}} \, |q_\mathrm{E}\rangle \otimes |x\rangle + \sqrt{p_t} \, |\psi'_t\rangle \right) \tag{4.10}$$

$$= \sum_{T=1}^{t} \sum_{x \in A} \sqrt{p_{x,T}} \, |q_\mathrm{E}\rangle \otimes |x\rangle + \sqrt{p_t} \, |\psi'_t\rangle \tag{4.11}$$

Der Zustand $|\psi_t\rangle$ setzt sich demnach zusammen aus dem Zustand $|q_\mathrm{E}\rangle \otimes |x\rangle$, also dem Zustand, wenn die QTM gehalten hat sowie dem Zustand $|\psi'_t\rangle$, der nach der Projektion P übrig bleibt.

Es sei $M = M'$ mit dem Unterschied, dass nur eine Zustandsmessung P nach einer vorgegebenen Laufzeit durchgeführt wird. Es ist $|\phi_0\rangle = |\psi_0\rangle$ der Initialzustand der QTM M, $|\phi_t\rangle$ der Zustand nach der Ausführung des t-ten Schrittoperators und $|\phi'_t\rangle$ der Zustand nach der Ausführung der finalen Zustandsmessung nach t Schritten. Zu zeigen ist, dass die QTM M nach Laufzeit t und einer finalen Zustandsmessung P sich in dem gleichen Zustand befindet wie die QTM M'.

Induktionsanfang (IA) $t = 1$: Es ist

$$|\phi_1\rangle = \mathcal{S} \, |\phi_0\rangle = \mathcal{S} \, |\psi_0\rangle = |\psi_1\rangle$$

Da $|\phi_1\rangle = |\psi_1\rangle$ gilt, sind auch die Zustände nach der Ausführung der Zustandsmessung P gleich.
Induktionsvoraussetzung (IV): Es gilt $|\phi_t\rangle = |\psi_t\rangle$ für ein $t \in \mathbb{N}$.
Induktionsschritt (IS) $t \to t+1$: Es ist

$$\begin{aligned}
|\phi_{t+1}\rangle = \mathcal{S}\,|\phi_t\rangle = \mathcal{S}\,|\psi_t\rangle &= \mathcal{S} \sum_{T=1}^{t} \sum_{x \in A} \sqrt{p_{x,\,T}}\,|q_e\rangle \otimes |x\rangle + \sqrt{p_t}\,\left|\psi'_t\right\rangle \\
&= \sum_{T=1}^{t} \sum_{x \in A} \sqrt{p_{x,\,T}}\,|q_e\rangle \otimes |x\rangle + \sqrt{p_t}\,|\psi_{t+1}\rangle \\
&= \sum_{T=1}^{t} \sum_{x \in A} \sqrt{p_{x,\,T}}\,|q_e\rangle \otimes |x\rangle + \sum_{x \in A} \sqrt{p_{x,\,t+1}}\,|q_e\rangle \otimes |x\rangle + \sqrt{p_{t+1}}\,\left|\psi'_{t+1}\right\rangle \\
&= \sum_{T=1}^{t+1} \sum_{x \in A} \sqrt{p_{x,\,T}}\,|q_e\rangle \otimes |x\rangle + \sqrt{p_{t+1}}\,\left|\psi'_{t+1}\right\rangle = |\psi_{t+1}\rangle
\end{aligned}$$

□

Damit ist gezeigt, dass es für den resultierenden Zustand nach Laufzeit t keine Auswirkung hat, ob eine Projektionsmessung nach jeder Ausführung des Schrittoperators $\mathcal{S}$ oder einmalig nach vorgegebener Laufzeit t durchgeführt wird.

Definition 24. *Es sei*

$$\eta_t \colon \mathbb{Z} \times Q \times (\Sigma \cup \{\,\square\,\})^{2t+1} \to (\{\,0,\,1\,\} \times (Q \cup \{\,\emptyset\,\}) \times (\Sigma \cup \{\,\square\,\}))^{2t+1}$$

die bijektive Funktion, die das Wort $mq\sigma_{-t}\cdots\sigma_t$ auf das Wort $s_{-t}q_{-t}\sigma_{-t}\cdots s_tq_t\sigma_t$ abbildet. Es ist

$$s_i = \begin{cases} 1 & \textit{für } i = m \\ 0 & \textit{sonst} \end{cases} \text{ und } q_i = \begin{cases} q & \textit{für } i = m \\ \emptyset & \textit{sonst} \end{cases}.$$

Es sei $|x\rangle$ die Eingabe der QTM M der Länge n und t die Laufzeit. Es ist

$$M(|x\rangle\,,\,t) = \sum_{y \in \mathbb{Z} \times Q \times \Sigma^{2t+1}} \alpha_y\,|y\rangle \tag{4.12}$$

der Quantenzustand nach t Schritten der QTM M für die Eingabe $|x\rangle$. Eine Quantenschaltkreisfamilie $\mathcal{C}$ simuliert eine QTM M mit Eingabe $|x\rangle$ der Länge n und Laufzeit t, wenn gilt $\sum_y \alpha_y\,|\eta_t(y)\rangle = C_x\,|0^{(2t+1)\ell}\rangle$ mit $\ell = 2 + \lceil\log_2(|\Sigma|+1)\rceil + \lceil\log_2(|Q|+1)\rceil$. Folgende Aussage soll in diesem Abschnitt gezeigt werden:

Satz 25. *Es sei M eine Quantenturingmaschine ohne wiederholte Zustandsmessung mit Laufzeit t. Dann existiert eine Quantenschaltkreisfamilie $\mathcal{C}$ mit Laufzeit* $\mathrm{poly}(t)$*, die die Quantenturingmaschine M simuliert.*

Zu zeigen ist, dass für jede QTM M ohne wiederholte Zustandsmessung mit Eingabe $|x\rangle$ und Laufzeit t eine Quantenschaltkreisfamilie $\mathcal{C}$ mit Laufzeit $\text{poly}(t)$ und Länge $\text{poly}(t)$ existiert, die die QTM M simuliert. Der Beweise wird auf Basis der QTM ohne wiederholter Zustandsmessung durchgeführt, da dann die Projektionsmessung im Quantenschaltkreis nicht explizit berücksichtigt werden muss. Die abschließende Projektionsmessung der QTM und des Quantenschaltkreises muss ebenfalls nicht berücksichtigt werden, da diese das gleiche Ergebnis liefert, wenn der Quantenschaltkreis die QTM simuliert.

Der Beweis von Satz 25 lässt sich in zwei Abschnitte aufteilen. Zunächst muss gezeigt werden, dass eine solche Quantenschaltkreisfamilie $\mathcal{C}$ konstruiert werden kann. Im zweiten Schritt muss dann bewiesen werden, dass der resultierende Quantenzustand der Quantenschaltkreisfamilie $\mathcal{C}$ mit dem der QTM M äquivalent ist.

4.2.1 Konstruktionsidee der Quantenschaltkreisfamilie $\mathcal{C}$

Bevor der konkrete Beweis angebracht wird, soll dem Leser die Idee hinter der Konstruktion des Quantenschaltkreises für eine beliebige Laufzeit t und Eingabelänge n näher gebracht werden. In Abbildung 4.1 ist der Quantenschaltkreis dargestellt, der die QTM M simulieren soll. Das Ziel der Konstruktion ist es, dass der Quantenschaltkreis C und die QTM M nach t Schritten die gleiche Verteilungsfunktion besitzen. Das t-malige Anwenden der Übergangsfunktion δ entspricht der t-maligen Anwendung einer Transformationsmatrix K im Quantenschaltkreis C. Die Transformationsmatrix K lässt sich wiederrum zerlegen in $2t-1$ Transformationen G und eine Matrix T. Dies ist ebenfalls in Abbildung 4.1 visualisiert.

Der Quantenschaltkreis besitzt $2t+1$ Register, wobei jedes Register einen Speicher für ein Zeichen $\sigma \in \Sigma \cup \{\square\}$, für einen Zustand $q \in Q \cup \{\emptyset\}$ und den Aktivitätszustand des Lese-/Schreibkopfes $s \in \{0, 1, 2, 3\}$ besitzt. Die Anzahl der benötigten Qubits hängt von der Laufzeit t, der Größe des Alphabets Σ und der Größe der Zustandsmenge Q der QTM M ab. Um ein Zeichen $\sigma \in \Sigma \cup \{\square\}$ zu kodieren, werden $\lceil \log_2(|\Sigma|+1) \rceil$ Qubits benötigt. Für die Kodierung eines Zustands $q \in Q \cup \{\emptyset\}$ werden $\lceil \log_2(|Q|+1) \rceil$ Qubits benötigt. Der Aktivitätszustand des Lese-/Schreibkopfes s zeigt an, ob sich der Lese-/Schreibkopf der simulierten QTM gerade auf diesem Register befindet. Um diesen zu kodieren, werden 2 Qubits benötigt. Der Initialzustand des Quantenschaltkreises hängt von der gegebenen Laufzeit t ab und ist $\left|0^{(2t+1)\ell}\right\rangle$ mit $\ell = 2 + \lceil \log_2(|\Sigma|+1) \rceil + \lceil \log_2(|Q|+1) \rceil$. Der Eingabezustand des Quantenschaltkreises muss zunächst mithilfe des Pauli-Gatters X initialisiert werden, sodass er der Binärkodierung von $|\eta_t(x)\rangle$ entspricht, wobei $|x\rangle$ die Eingabe der QTM M ist. Die Register 0 bis $t-1$ sind dann in dem Zustand $|0, \emptyset, \square\rangle$ initialisiert. Das Register t ist mit dem Zustand $|1, q_0, \sigma_0\rangle$ initialisiert und die Register $t+1$ bis $\min(t+n-1, 2t)$ jeweils mit $|0, \emptyset, \sigma_i\rangle$ mit $1 \leq i \leq \min(n-1, t)$. Gilt $2t > t+n-1$ dann sind die verbleibenden Register mit dem Quantenzustand $|0, \emptyset, \square\rangle$ initialisiert. Der Zustand q wird also nicht global im Quantenschaltkreis C gespeichert, sondern

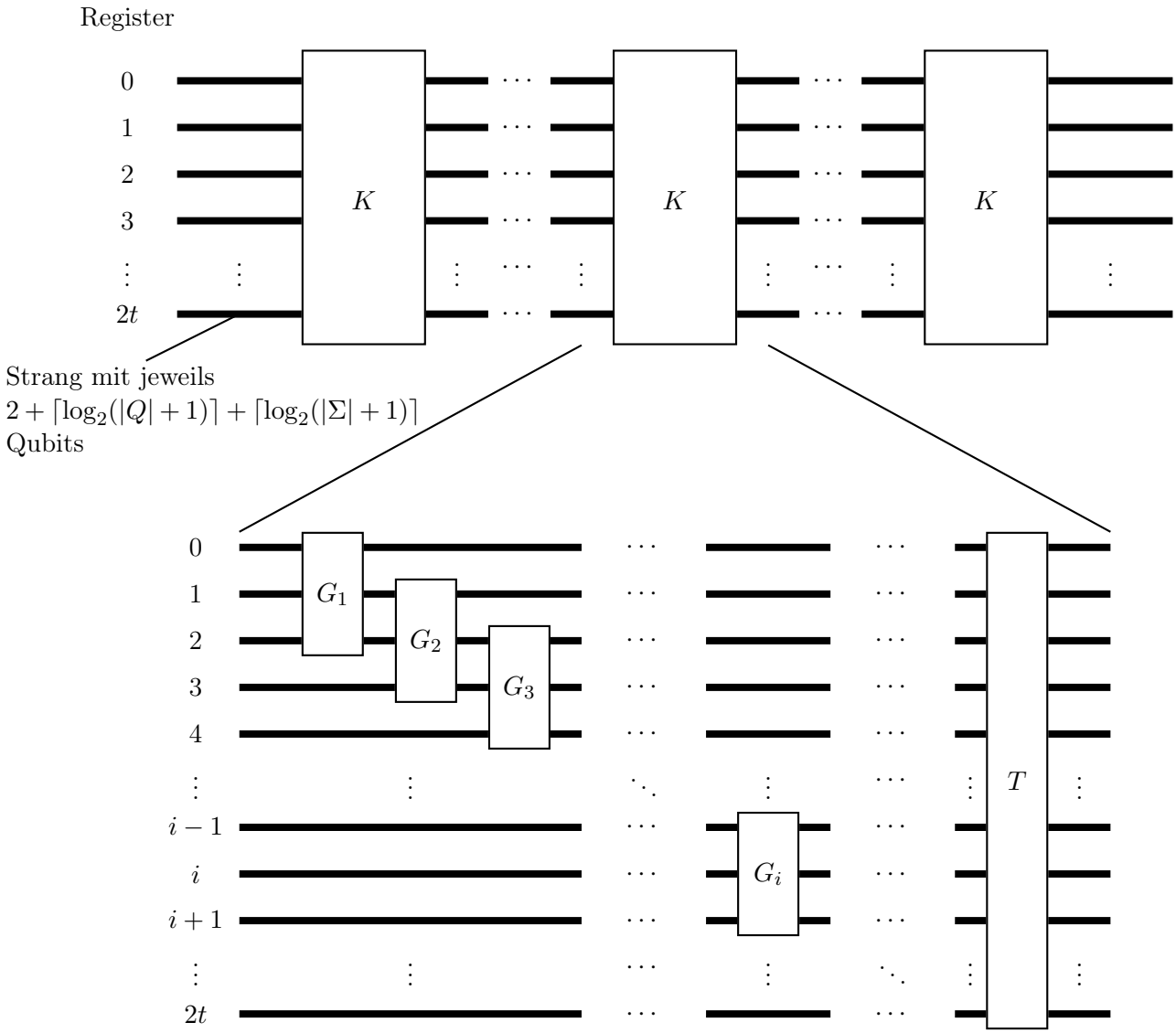

Abbildung 4.1: Idee zur Konstruktion eines Quantenschaltkreises aus einer Quantenturingmaschine. Die Matrix K spiegelt das Verhalten der Übergangsfunktion δ wieder und kann in $2t$ Matrizen zerlegt werden. Diese Matrizen G_i mit $i = 1, 2, \ldots, 2t - 1$ wirken nur auf jeweils drei Registern, die die Bandzellen $i - 1$, i und $i + 1$ der QTM M repräsentieren. Die Matrix T wirkt abschließend auf den gesamten Quantenzustand. Jeder Strang, der ein Register repräsentiert, besteht aus $2 + \lceil \log_2(|Q| + 1) \rceil + \lceil \log_2(|\Sigma| + 1) \rceil$ Qubits.

nur in dem Register, welches einen Aktivitätszustand des Lese-/Schreibkopfes von 1 oder 2 hat. In den anderen Fällen wird der Zustand mit $\emptyset$ kodiert.

Die Transformationsmatrix K ist zusammengesetzt aus $2t-1$ Transformationen G und einer Matrix T. Jede der Matrizen G_i mit $i = 1, 2, \ldots, 2t-1$ wirkt auf genau drei Register $i-1$, i und $i+1$, die die Bandzellen $i-1$ bis $i+1$ der QTM M repräsentieren. Diese Matrizen G_i sind alle gleich, der Index macht nur deutlich, auf welchen Registern die jeweilige Transformation G wirkt.

Pro Anwendung der Transformationsmatrix K ändert jedoch nur eine der Transformationen G_i den Quantenzustand. Welches G_i das ist, entscheidet die Position des Lese-/Schreibkopfs. Analog entscheidet bei einer QTM die Position des Lese-/Schreibkopf, welche Bandzelle geändert wird. Die Position des Lese-/Schreibkopfes wird beim Quantenschaltkreis durch den Aktivitätszustand des Lese-/Schreibkopfes s angezeigt. Die Kodierungen von s haben folgende Bedeutung: Ist $s = 0$, so bleibt die Zelle durch die Transformation G_i unverändert. Für $s = 1$ wird der Inhalt der Zelle bei Multiplikation mit G_i geändert. Ist $s = 2$, so wurde der Inhalt der Zelle durch die Transformation G_i bereits verändert. Auch $s = 3$ ist eine mögliche Kodierung, wird aber nicht benötigt. Die Unterscheidung zwischen den Zuständen für $s_i = 1$ und $s_i = 2$ ist notwendig, da sonst mehrere Schritte der Übergangsfunktion durch eine Transformation K simuliert werden könnten. Dadurch kann nicht mehr sichergestellt werden, dass die QTM M und der Quantenschaltkreis C nach t Schritten die gleiche Verteilungsfunktion besitzen. Die Transformation T sorgt abschließend dafür, dass vor der nächsten Ausführung der Transformation K die Amplituden der Quantenzustände für $s = 2$ mit $s = 1$ vertauscht werden, denn nur dann verändert die Matrix G den Quantenzustand.

4.2.2 Konstruktion der Quantenschaltkreisfamilie $\mathcal{C}$

Nachdem die Idee hinter der Konstruktion des Quantenschaltkreises erläutert ist, befasst sich dieser Abschnitt mit der ersten Hälfte des Beweises von Satz 25. Es ist zu zeigen, dass die im vorherigen Abschnitt erörterte Transformation K konstruiert werden kann. Insbesondere muss gezeigt werden, dass die Transformation unitär ist. Des Weiteren muss die Transformation K in der Elementargatterdarstellung die Länge $\text{poly}(t)$ haben.

Es sei M eine QTM mit dem Alphabet Σ, der Zustandsmenge Q und der Übergangsfunktion $\delta(q, \sigma, d, q', \sigma')$ mit den Kopfbewegungsmöglichkeiten $d \in \{ \text{L}, \text{N}, \text{R} \}$. Wie bereits im vorherigen Abschnitt erwähnt, kann die Übergangsfunktion δ als die Amplitude dafür verstanden werden, dass sich M im Zustand q befindet, das Zeichen σ liest und anschließend in den Zustand q' übergeht, das Zeichen σ' schreibt und sich der Lese-/Schreibkopf in Richtung d entlang des Speicherbandes bewegt. Wir bezeichnen im Folgenden diese Amplituden auch als Übergangsfunktionskoeffizienten.

Die Quantenschaltkreisfamilie $\mathcal{C}$ wird so konstruiert, dass sie aus t identischen Gattern K besteht. Ein Gatter K führt einen Schritt der Übergangsfunktion δ der QTM M aus. Für jede der

$2t+1$ Bandzellen der QTM M werden zur Kodierung der $2t+1$ Register der Quantenschaltkreisfamilie $\mathcal{C}$ jeweils $\ell = 2 + \lceil \log_2(|Q|+1) \rceil + \lceil \log_2(|\Sigma|+1) \rceil$ Qubits benötigt. Die Kodierung des Registers i der Quantenschaltkreisfamilie $\mathcal{C}$ ist durch den Zustandsvektor $|s_i, q_i, \sigma_i\rangle$ gegeben, wobei $s_i \in \{0, 1, 2, 3\}$, $q_i \in Q \cup \{\emptyset\}$ und $\sigma_i \in \Sigma \cup \{\square\}$ ist.

Die Transformation K lässt sich aufteilen in $2t-1$ kleinere Gatter G_i, welche jeweils nur auf die Zellen $i-1$, i und $i+1$ wirken. Zusätzlich wirkt eine Matrix T nach der Durchführung aller G_i. Die Matrix K wird durch die Kaskadierung von $2t-1$ Matrizen G_i konstruiert, wobei jedes G_i den Quantenzustand der zwei Ausgangsregister der vorherigen Transformation G_{i-1} betrachtet und den Quantenzustand des darauffolgenden Registers $i+1$ mit einbezieht. Der Index i dient nur der Unterscheidung, auf welche Zellen die Matrix G wirkt. Für jedes i sind die Matrizen G_i gleich.

Wir definieren uns zunächst einen Unterraum H wie folgt

Definition 26. *Es sei H der Unterraum von $\widetilde{\mathbb{C}}^{2^{3\ell}}$ der aufgespannt wird durch die Vektoren*

1. $|s_{i-1}, q_{i-1}, \sigma_{i-1}, s_i, q_i, \sigma_i, s_{i+1}, q_{i+1}, \sigma_{i+1}\rangle$ *mit* $s_{i-1}, s_i \neq 1$ *und* $s_{i-1}, s_i, s_{i+1} \neq 2$

2. $\left|v_{q_{i-1}, \sigma_{i-1}, \sigma_i, \sigma_{i+1}}\right\rangle$ *für beliebige* $(q_{i-1}, \sigma_{i-1}, \sigma_i, \sigma_{i+1}) \in Q \times \Sigma \times \Sigma \times \Sigma$ *mit*

$$\begin{aligned}\left|v_{q_{i-1}, \sigma_{i-1}, \sigma_i, \sigma_{i+1}}\right\rangle = &\sum_{\substack{q' \in Q, \\ \sigma' \in \Sigma}} \delta(q_{i-1}, \sigma_{i-1}, \mathrm{N}, q', \sigma') \, |2, q', \sigma', 0, \emptyset, \sigma_i, 0, \emptyset, \sigma_{i+1}\rangle \\ &+ \sum_{\substack{q' \in Q, \\ \sigma' \in \Sigma}} \delta(q_{i-1}, \sigma_{i-1}, \mathrm{R}, q', \sigma') \left|0, \emptyset, \sigma', 2, q', \sigma_i, 0, \emptyset, \sigma_{i+1}\right\rangle,\end{aligned} \tag{4.13}$$

3. $\left|u_{q_{i-2}, \sigma_{i-2}, \sigma', \sigma_{i-1}, \sigma_i, \sigma_{i+1}}\right\rangle$ *für beliebige* $(q_{i-2}, \sigma_{i-2}, \sigma', \sigma_{i-1}, \sigma_i, \sigma_{i+1}) \in Q \times \Sigma \times \Sigma \times \Sigma \times \Sigma \times \Sigma$ *mit*

$$\left|u_{q_{i-2}, \sigma_{i-2}, \sigma', \sigma_{i-1}, \sigma_i, \sigma_{i+1}}\right\rangle = \sum_{q' \in Q} \delta(q_{i-2}, \sigma_{i-2}, \mathrm{R}, q', \sigma') \left|2, q', \sigma_{i-1}, 0, \emptyset, \sigma_i, 0, \emptyset, \sigma_{i+1}\right\rangle \tag{4.14}$$

Es handelt sich bei den Vektoren des Unterraums H um einen Ausschnitt von Quantenzuständen dreier aufeinanderfolgendender Register des gesamten Quantenzustands. Die Vektoren des Unterraums H sind diejenigen Quantenzustände, die während der Simulation als Eingabe in G auftreten können, ohne diejenigen Quantenzustände dessen Aktivitätszustand des Lese-/Schreibkopfes s_i 1 ist. Der Quantenzustand $\left|v_{q_{i-1}, \sigma_{i-1}, \sigma_i, \sigma_{i+1}}\right\rangle$ tritt auf, wenn $s_{i-1} = 1$ vor der Ausführung von G_{i-1} galt und sich der Lese-/Schreibkopf in Richtung N oder R bewegt hat. Der Summand für die Bewegung des Lese-/Schreibkopfs nach L ist durch die erste Art von Vektoren des Unterraums H abgedeckt. Der Quantenzustand $\left|u_{q_{i-2}, \sigma_{i-2}, \sigma', \sigma_{i-1}, \sigma_i, \sigma_{i+1}}\right\rangle$ tritt auf, wenn $s_{i-2} = 1$ vor der Ausführung von G_{i-2} galt und sich der Lese-/Schreibkopf

in Richtung R bewegt hat. Für die Vektoren des 1. Typ aus dem Unterraum H befindet sich der Lese-/Schreibkopf weder am Register i noch am Register $i-1$. Nur der Fall $s_{i+1} = 1$ ist erlaubt. Die Varianten mit $s_{i-1} = 1$ und $s_{i+1} = 2$ sind Eingaben, die nicht auftreten können, und können deshalb aus dem Unterraum H ausgeschlossen werden.

Lemma 27. *Für beliebige* $(\sigma_{i-1},\, q_i,\, \sigma_i,\, \sigma_{i+1}) \in \Sigma\times Q\times\Sigma\times\Sigma$ *sind die Vektoren* $|w_{\sigma_{i-1},\, q_i,\, \sigma_i,\, \sigma_{i+1}}\rangle$ *mit*

$$\begin{aligned} |w_{\sigma_{i-1},\, q_i,\, \sigma_i,\, \sigma_{i+1}}\rangle = &\sum_{\substack{q'\in Q,\\ \sigma'\in\Sigma}} \delta(q_i,\, \sigma_i,\, \mathrm{L},\, q',\, \sigma')\, |2,\, q',\, \sigma_{i-1},\, 0,\, \emptyset,\, \sigma',\, 0,\, \emptyset,\, \sigma_{i+1}\rangle \\ &+ \sum_{\substack{q'\in Q,\\ \sigma'\in\Sigma}} \delta(q_i,\, \sigma_i,\, \mathrm{N},\, q',\, \sigma')\, |0,\, \emptyset,\, \sigma_{i-1},\, 2,\, q',\, \sigma',\, 0,\, \emptyset,\, \sigma_{i+1}\rangle \\ &+ \sum_{\substack{q'\in Q,\\ \sigma'\in\Sigma}} \delta(q_i,\, \sigma_i,\, \mathrm{R},\, q',\, \sigma')\, |0,\, \emptyset,\, \sigma_{i-1},\, 0,\, \emptyset,\, \sigma',\, 2,\, q',\, \sigma_{i+1}\rangle \end{aligned} \tag{4.15}$$

zueinander orthonormale Einheitsvektoren. Ebenso sind sie orthonormal zum Unterraum H*.*

Um dieses Lemma zu beweisen, muss die Orthogonalität für alle Kombinationen geprüft werden. Der Beweis zu diesem Lemma ist im Anhang B ausgeführt, um den Lesefluss des eigentlichen Beweises nicht zu unterbrechen.

Satz 28. *Es gibt eine unitäre Transformationsmatrix* $G \in \widetilde{\mathbb{C}}^{2^{3\ell}} \times \widetilde{\mathbb{C}}^{2^{3\ell}}$*, die die folgenden Bedingungen erfüllt.*

1. *Für alle Zustandsvektoren* $|v\rangle \in H$ *gilt* $G\,|v\rangle = |v\rangle$*.*
2. *Für beliebige* $(\sigma_{i-1},\, q_i,\, \sigma_i,\, \sigma_{i+1}) \in \Sigma \times Q \times \Sigma \times \Sigma$ *mit* $i \in \mathbb{N}_{\leq 2t-1}$ *gilt*

$$G\,|0,\, \emptyset,\, \sigma_{i-1},\, 1,\, q_i,\, \sigma_i,\, 0,\, \emptyset,\, \sigma_{i+1}\rangle = |w_{\sigma_{i-1},\, q_i,\, \sigma_i,\, \sigma_{i+1}}\rangle \tag{4.16}$$

Des Weiteren sind die Matrixeinträge von G *Quotienten von Polynomen von Übergangsfunktionskoeffizienten der Übergangsfunktion* δ *der simulierten Quantenturingmaschine* M*.*

Beweis

Damit die Matrix G unitär ist, muss es sich um eine Basistransformationsmatrix handeln. Sind die Spalten- und Zeilenvektoren der Matrix G orthonormal, dann ist G auch eine unitäre Matrix. Zu diesem Zweck wird aus den Vektoren des Unterraums H zunächst mit dem Gram-Schmidt-Verfahren eine Orthonormalbasis konstruiert. Dieser Vektorraum $V = \{\, |v_1\rangle, \ldots, |v_j\rangle \,\}$ mit $j < 2^{3\ell}$ ist nach Lemma 27 orthonormal zu $\left|w_{\sigma_{i-1},\, q_i,\, \sigma_i,\, \sigma_{i+1}}\right\rangle$. Ebenso sind all diese Vektoren orthonormal zu dem Quantenzustand $|0,\, \emptyset,\, \sigma_{i-1},\, 1,\, q_i,\, \sigma_i,\, 0,\, \emptyset,\, \sigma_{i+1}\rangle$. Um eine vollständige

Basis zu erhalten, muss aus der ursprünglichen Basis unter Verwendung der bereits konstruierten orthonormalen Vektoren das Gram-Schmidt-Orthonormalisierungsverfahren durchgeführt werden. Der dadurch erhaltene Vektorraum $W = \{ |w_1\rangle, \ldots, |w_k\rangle \}$ spannt zusammen mit dem Vektorraum V und den Vektoren $\left|w_{\sigma_{i-1}, q_i, \sigma_i, \sigma_{i+1}}\right\rangle$ und $|0, \emptyset, \sigma_{i-1}, 1, q_i, \sigma_i, 0, \emptyset, \sigma_{i+1}\rangle$ den Hilbertraum $\widetilde{\mathbb{C}}^{2^{3\ell}}$ auf.

Es sei G' die Matrix, deren Einträge in der konstruierten Basis geschrieben sind. Daurch sind die Matrixeinträge von G' aus der Menge $\{ 0, 1 \}$. Alle Vektoren aus V und W werden auf sich selbst abgebildet und die Vektoren $|0, \emptyset, \sigma_{i-1}, 1, q_i, \sigma_i, 0, \emptyset\, \sigma_{i+1}\rangle$ werden auf $\left|w_{\sigma_{i-1}, q_i, \sigma_i, \sigma_{i+1}}\right\rangle$ abgebildet und umgekehrt. Dadurch handelte es sich bei G' um eine Basistransformationsmatrix. Um G zu erhalten, muss $UG'U^\dagger$ berechnet werden. Die Matrix U enthält als Zeilen die Vektoren der konstruierten Basis, dargestellt in der ursprünglichen Basis. □

Nachdem bisher nur die Transformation G betrachtet wurde, muss sich auch den anderen beiden benötigten Transformationen T und K, welche aus G und T konstruiert wird, gewidmet werden. Die beiden Transformationen sind wie folgt definiert.

Definition 29. *Es ist*

$$T = \bigotimes_{i=0}^{2t} \left(\left(|0\rangle\langle 0| + |1\rangle\langle 2| + |2\rangle\langle 1| + |3\rangle\langle 3| \right) \otimes \mathbf{I}_{2^{\ell-2}} \right) \tag{4.17}$$

und

$$K = \prod_{i=1}^{2t-1} \left(\mathbf{I}_{2^{(1+i)\ell}} \otimes G \otimes \mathbf{I}_{2^{(2t-i)\ell}} \right) \cdot T. \tag{4.18}$$

Die Transformation T vertauscht die Amplituden für $s_i = 2$ mit $s_i = 1$ für alle $2t + 1$ Register, damit alle Quantenzustände mit Amplituden ungleich 0 als Eingabe in die nächste Matrix K nur Werte von 0 oder 1 für s besitzen. Die Matrix K beinhaltet die Kaskadierung der Matrix G und die abschließende Tauschtransformation T. Damit es sich bei der Transformation K um eine gültige Transformation der Quantenschaltkreisfamilie $\mathcal{C}$ handelt, muss K unitär sein.

Lemma 30. *Die Transformationsmatrix K kann als unitäre Transformation konstruiert werden.*

Beweis

Um zeigen zu können, dass K unitär ist, reicht es zu zeigen, dass die Matrizen G und T unitär sind. Für die Transformation G wurde dies bereits gezeigt. Zur Prüfung der unitären

Eigenschaft von T muss nur gezeigt werden, dass die Matrix $|0\rangle\langle 0| + |1\rangle\langle 2| + |2\rangle\langle 1| + |3\rangle\langle 3|$ unitär ist. Es ist

$$\begin{aligned}
&\big(\,|0\rangle\langle 0| + |1\rangle\langle 2| + |2\rangle\langle 1| + |3\rangle\langle 3|\,\big)^\dagger \cdot \big(\,|0\rangle\langle 0| + |1\rangle\langle 2| + |2\rangle\langle 1| + |3\rangle\langle 3|\,\big) \\
&\quad = \big(\,|0\rangle\langle 0| + |2\rangle\langle 1| + |1\rangle\langle 2| + |3\rangle\langle 3|\,\big) \cdot \big(\,|0\rangle\langle 0| + |1\rangle\langle 2| + |2\rangle\langle 1| + |3\rangle\langle 3|\,\big) \\
&\quad = |0\rangle\langle 0| \cdot |0\rangle\langle 0| + |2\rangle\langle 1| \cdot |1\rangle\langle 2| + |1\rangle\langle 2| \cdot |2\rangle\langle 1| + |3\rangle\langle 3| \cdot |3\rangle\langle 3| \\
&\quad = |0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2| + |3\rangle\langle 3| \\
&\quad = \mathbf{I}
\end{aligned}$$

Hierbei wurden die Terme, deren innere Produkte sich zu 0 ergeben, in der dritten Zeile weggelassen, die durch das Ausmultiplizieren der beiden Klammern entstehen. Dabei handelt beispielsweise um den Term $|0\rangle\langle 0| \cdot |1\rangle\langle 2|$, dessen inneres Produkt $\langle 0| \cdot |1\rangle$ Null ergibt. Es handelt sich bei T also um eine unitäre Transformation. Es ist also auch die Matrix K unitär. □

Es bleibt noch zu zeigen, dass die Quantenschaltkreisfamilie effizient in Abhängigkeit von der vorgegebenen Laufzeit t ist. Hierbei wird sich auf die Gattermenge beschränkt, die das CNOT-Gatter und alle 1-Qubittransformationen enthält, um die Transformation K exakt darstellen zu können.

Lemma 31. *Die Transformationsmatrix K lässt sich aus* $\mathrm{poly}(t)$*-vielen 1-Qubittransformationen und CNOT-Gattern konstruieren.*

Beweis

Die Transformation T lässt sich aus $\mathcal{O}(t)$ Elementargattern konstruieren. Wie aus Abschnitt 3.2 bekannt ist, lässt sich der Tausch zweier Amplituden mithilfe von CNOT- und Hadamard-Gattern realisieren. Es ist

$$|0\rangle\langle 0| + |1\rangle\langle 2| + |2\rangle\langle 1| + |3\rangle\langle 3| = U_{\mathrm{CNOT}} \cdot (H \otimes H) \cdot U_{\mathrm{CNOT}} \cdot (H \otimes H) \cdot U_{\mathrm{CNOT}}. \tag{4.19}$$

Für jede Zelle muss die Vertauschung der Amplituden einmal realisiert werden, was genau $(2t+1) \cdot 7$ Elementargattern entspricht.

Die Transformation G muss $(2t-1)$-mal für jede Transformation K implementiert werden. Aus Kapitel 3 ist bekannt, dass jede Transformation auf n Qubits durch $\mathcal{O}(n^2 \cdot 4^n)$ Gatter realisiert werden kann. Für die Implementierung einer Transformation G werden demnach $\mathcal{O}((3\ell)^2 \cdot 4^{3\ell})$ Gatter benötigt. Da ℓ aber nur logarithmisch von der Größe der Zustandsmenge und der Größe des Alphabets abhängt, handelt es sich bei $(3\ell)^2 \cdot 4^{3\ell}$ um eine Konstante, dessen Größe polynomiell von der Größe der Zustandsmenge und des Alphabtes abhängt. So lässt sich eine Transformation K mit insgesamt $\mathcal{O}\left((2t-1) \cdot \mathrm{poly}(|Q| + |\Sigma|)\right) = \mathcal{O}(t)$ Gattern implementieren. Die Transformation K wird insgesamt t-mal benötigt, also lässt sich die Quantenschaltkreisfamilie aus $\mathcal{O}(t^2)$ Elementargattern konstruieren. □

Dass ein Quantenschaltkreis C_x in der in Abschnitt 4.2.1 beschriebenen Form konstruiert werden kann, konnte bis hierhin gezeigt werden. Wie genau ein Quantenschaltkreis C_x für eine bestimmte QTM M mit Laufzeit t und Eingabe $|x\rangle$ jeweils aussieht, muss zunächst von einer klassischen Turingmaschine bestimmt werden.

Lemma 32. *Es sei $|x\rangle$ die Eingabe der QTM $M = (\Sigma, Q, q_0, q_\mathrm{E}, \mathcal{S})$ und t ihre Laufzeit. Es existiert eine Turingmaschine M_D die als Eingabe die QTM M und die Eingabe x erhält und in Laufzeit $\mathrm{poly}(t)$ den obigen Quantenschaltkreis C_x konstruiert.*

Beweis

An dieser Stelle sei zunächst die Church-Turing-These erwähnt, die besagt, dass ein effizient berechenbarer Algorithmus auf einer Rechenmaschine R_1 auch effizient auf einer anderen Rechenmaschine R_2 berechnet werden kann. Wird im Folgenden also ein effizienter Algorithmus beschrieben, lässt sich dieser auch effizient auf einer Turingmaschine umsetzen.

In Abschnitt 3.3 wurde bereits erläutert, wie die Ausgabe einer solchen Turingmaschine aussehen kann. Zunächst wird die Anzahl an benötigten Qubits kodiert. Zu diesem Zweck muss die TM $(2t+1)(2+\lceil\log_2(|\Sigma|+1)\rceil+\lceil\log_2(|Q|+1)\rceil)$ berechnen. Dazu muss die Mächtigkeit von Σ und von Q bestimmt werden, was sich jeweils in Zeit $\mathcal{O}(|\Sigma|)$ bzw. in $\mathcal{O}(|Q|)$ erledigen lässt. Anschließendes addieren einer Eins und berechnen der Vorkommastellen von $\log_2(|\Sigma|+1)$ und $\log_2(|Q|+1)$, ist somit in konstanter Zeit möglich. Die Anzahl der benötigten Qubits zum Kodieren des Aktivitätszustands des Lese-/Schreibkopfes s muss anschließend noch addiert werden. Abschließend muss mit dem Faktor $2t+1$ multipliziert werden. Nur die Multiplikation mit t lässt sich nicht in konstanter Zeit berechnen. Insgesamt lässt sich die Anzahl an benötigten Qubits in Zeit $\mathcal{O}(t^2)$ berechnen.

Im nächsten Schritt müssen die Gatter zur Initialisierung des Eingabezustands ausgegeben werden. Der Eingabezustand für den Quantenschaltkreis ist $\left|0^{(2t+1)\ell}\right\rangle$, allerdings muss der Quantenzustand vor der ersten Transformation $K\,|\eta_t(x)\rangle$ entsprechen. Diese Übersetzung von $\left|0^{(2t+1)\ell}\right\rangle$ zu $|\eta_t(x)\rangle$ kann durch ein Pauli-Gatter X realisiert werden. Mithilfe dieser lassen sich einzelne Qubits flippen, sodass die Eingabe $|\eta_t(x)\rangle$ binärkodiert dargestellt werden kann. Insgesamt werden maximal $(2t+1)\ell$ X-Gatter benötigt, deren Position und Matrixeinträge auf das Ergebnisband der Turingmaschine M_D geschrieben werden müssen. Für jedes einzelne Qubit muss berechnet werden, ob es geflippt werden muss oder nicht. Für ein einzelnes Qubit hängt die benötigte Zeit dafür von $|Q|$ und $|\Sigma|$ ab. Für alle Qubits ist Zeit $\mathcal{O}(t)$ dafür notwendig. Das Aufschreiben der Position auf das Ergebnisband ist in Zeit $\mathcal{O}(\log_2(t))$ für jedes Qubit möglich.

Abschließend muss die Transformation K in Elementargatter zerlegt und auf das Band geschrieben werden. Dafür muss die Transformation G berechnet werden. Ein lineares Gleichungssystem der Größe $n \times n$ mit dem Gauß-Algorithmus kann in polynomieller Zeit der Eingabegröße gelöst werden [22]. Die Größe des hier zu lösenden linearen Gleichungssystems beträgt $2^{3\ell} \times 2^{3\ell}$, was einer konstanten Laufzeit entspricht. Das lineare Gleichungssystem kann also in

Zeit $\mathcal{O}(\text{poly}(|Q| \cdot |\Sigma|))$ gelöst werden. Auch die Berechnung der Zerlegung in Elementargatter ist nur abhängig von der Größe der Matrix und ist somit in konstanter Laufzeit möglich. Die Matrix G muss in Elementargatterzerlegung insgesamt $(2t-1)$-mal zusammen mit der Position, auf denen die Gatter wirken, auf das Band geschrieben werden. Zusätzlich muss auch T in Elementargatterzerlegung auf das Band geschrieben werden. Dafür wird insgesamt eine Laufzeit $\mathcal{O}(\log_2(t) \cdot t)$ benötigt. Insgesamt muss die Transformation K t-mal auf das Ergebnisband geschrieben werden, was insgesamt Zeit $\mathcal{O}(\log_2(t) \cdot t^2)$ entspricht. Die Turingmaschine M_D kann also in Zeit $\text{poly}(t)$ die Konstruktion des Quantenschaltkreises berechnen. □

Wird eine QTM M ohne wiederholte Zustandsmessung, eine klassische Eingabe $|x\rangle$ und eine Laufzeit t vorgegeben, lässt sich ein passender Quantenschaltkreis konstruieren, der die QTM M simulieren soll. Der Beweis, dass die QTM M durch den Quantenschaltkreis C_x korrekt simuliert wird, steht noch aus.

Satz 33. *Die QTM M ohne wiederholte Zustandsmessung mit der klassischen Eingabe $|x\rangle$ und der Laufzeit t wird durch den von der Turingmaschine M_D ausgegebenen Quantenschaltkreis C_x simuliert.*

Beweis

Um Satz 33 zu zeigen, reicht es zu zeigen, dass eine Anwendung der Transformation K einen Schritt der QTM M korrekt simuliert. Wir erinnern uns, dass für eine klassische Konfiguration $|x\rangle$ der QTM M mit $|\eta_t(x)\rangle$ der Zustandsvektor des Quantenschaltkreises

$$|s_0,\, z_0,\, a_0,\, s_1,\, z_1,\, a_1,\, \ldots,\, s_{2t+1},\, z_{2t+1},\, a_{2t+1}\rangle$$

bezeichnet wird. Es sei $|x_0\rangle$ eine klassische Konfiguration der QTM M für eine beliebige Lese-/Schreibkopfposition $1 \leq i \leq 2t-1$ und $\sum_x \alpha_x |x\rangle$ der Zustand nach der einmaligen Ausführung der Übergangsfunktion δ der QTM M. Zu zeigen ist, dass für die Eingabe $|\eta_t(x_0)\rangle$ die einmalige Ausführung der Transformation K das Ergebnis $\sum_x \alpha_x |\eta_t(x)\rangle$ liefert.

Es sei $|\eta_t(x_0)\rangle = |k_0\rangle$ die Eingabe in die Transformation K und $|k_1\rangle, \ldots, |k_{2t-1}\rangle$ jeweils der Quantenzustand nach der Ausführung von G_i. Der Quantenzustand $|k_{2t}\rangle$ ist der Quantenzustand nach der Ausführung aller G_i und der Transformation T. Es ist zu zeigen, dass gilt $|k_{2t}\rangle = \sum_x \alpha_x |\eta_t(x)\rangle$.

Es sei $s_i = 1$ für ein $1 \leq i \leq 2t-1$ mit $i \in \mathbb{N}$. Für $1 \leq j \leq i-1$ mit $j \in \mathbb{N}$ liegt die Eingabe von G_j in dem Unterraum H. Da $G|v\rangle = |v\rangle$ für $|v\rangle \in H$ gelten muss, gilt $|k_j\rangle = |k_0\rangle$ für alle $1 \leq j \leq i-1$. Ist $j = i$, so wird der Quantenzustand $|k_i\rangle$ abgebildet auf $\sum_{k_i} \alpha_{k_i} |k_i\rangle$. An dieser Stelle gilt noch $|k_i\rangle \neq |\eta_t(x)\rangle$, allerdings nur, weil $s_i = 2$ gilt.

Der Quantenzustand $|k_i\rangle$ lässt sich in die Summe $|k_i'\rangle + |k_i''\rangle$ zerlegen. Dabei sei $|k_i'\rangle$ der Teil des Quantenzustands, in dem sich der Lese-/Schreibkopf durch eine Linksbewegung an der Position $i-1$ befindet. Mit $|k_i''\rangle$ wird der Rest des Zustands bezeichnet. Der Lese-/Schreibkopf

befindet sich nach einer Neutralbewegung an der Position i bzw. durch eine Rechtsbewegung an der Position $i+1$. Für die Transformation G_{i+1} lässt sich $|k_{i+1}\rangle$ wie folgt berechnen.

$$|k_i'\rangle = \sum_{\substack{q'\in Q,\\ \sigma'\in\Sigma}} \delta(q_i,\, \sigma_i,\, \mathrm{L},\, q',\, \sigma')\,|0,\, \emptyset,\, \sigma_1,\, \ldots,\, 2,\, q',\, \sigma_{i-1},\, \underline{0,\, \emptyset,\, \sigma',\, 0,\, \emptyset,\, \sigma_{i+1},\, 0,\, \emptyset,\, \sigma_{i+2}},\, \ldots\rangle \tag{4.20}$$

$$\begin{aligned}|k_i''\rangle = &\sum_{\substack{q'\in Q,\\ \sigma'\in\Sigma}} \delta(q_i,\, \sigma_i,\, \mathrm{N},\, q',\, \sigma')\,|0,\, \emptyset,\, \sigma_1,\, \ldots,\, 0,\, \emptyset,\, \sigma_{i-1},\, \underline{2,\, q',\, \sigma',\, 0,\, \emptyset,\, \sigma_{i+1},\, 0,\, \emptyset,\, \sigma_{i+2}},\, \ldots\rangle \\ &+ \sum_{\substack{q'\in Q,\\ \sigma'\in\Sigma}} \delta(q_i,\, \sigma_i,\, \mathrm{R},\, q',\, \sigma')\,|0,\, \emptyset,\, \sigma_1,\, \ldots,\, 0,\, \emptyset,\, \sigma_{i-1},\, \underline{0,\, \emptyset,\, \sigma',\, 2,\, q',\, \sigma_{i+1},\, 0,\, \emptyset,\, \sigma_{i+2}},\, \ldots\rangle\end{aligned} \tag{4.21}$$

G_{i+1} wirkt jeweils auf dem unterstrichenem Ausschnitt der Zustandsvektoren der Gleichungen 4.20 und 4.21. Für $|k_i'\rangle$ entspricht dies einer Linearkombination von Vektoren aus dem Unterraum H. $|k_i''\rangle$ ist ebenfalls ein Vektor aus dem Unterraum H. Beide Quantenzustände werden durch die Transformation G_{i+1} nicht verändert. Es gilt $|k_i\rangle = |k_{i+1}\rangle$. Zusätzlich muss noch die Transformation G_{i+2} betrachtet werden. Hier lässt sich $|k_{i+1}\rangle$ wie folgt in die zwei Quantenzustände $|k_{i+1}'\rangle$ und $|k_{i+1}''\rangle$ aufteilen.

$$\begin{aligned}|k_{i+1}'\rangle = &\sum_{\substack{q'\in Q,\\ \sigma'\in\Sigma}} \delta(q_i,\, \sigma_i,\, \mathrm{L},\, q',\, \sigma')\,|\ldots,\, 2,\, q',\, \sigma_{i-1},\, 0,\, \emptyset,\, \sigma',\, \underline{0,\, \emptyset,\, \sigma_{i+1},\, 0,\, \emptyset,\, \sigma_{i+2},\, 0,\, \emptyset,\, \sigma_{i+3}},\, \ldots\rangle \\ &+ \sum_{\substack{q'\in Q,\\ \sigma'\in\Sigma}} \delta(q_i,\, \sigma_i,\, \mathrm{N},\, q',\, \sigma')\,|\ldots,\, 0,\, \emptyset,\, \sigma_{i-1},\, 2,\, q',\, \sigma',\, \underline{0,\, \emptyset,\, \sigma_{i+1},\, 0,\, \emptyset,\, \sigma_{i+2},\, 0,\, \emptyset,\, \sigma_{i+3}},\, \ldots\rangle\end{aligned} \tag{4.22}$$

$$|k_{i+1}''\rangle = \sum_{\substack{q'\in Q,\\ \sigma'\in\Sigma}} \delta(q_i,\, \sigma_i,\, \mathrm{R},\, q',\sigma')\,|\ldots,\, 0,\, \emptyset,\, \sigma_{i-1},\, 0,\, \emptyset,\, \sigma',\, \underline{2,\, q',\, \sigma_{i+1},\, 0,\, \emptyset,\, \sigma_{i+2},\, 0,\, \emptyset,\, \sigma_{i+3}},\, \ldots\rangle \tag{4.23}$$

In Gleichung 4.22 handelt es sich bei dem unterstrichenem Ausschnitt des Quantenzustands um die Summe von Quantenzuständen, für die der Aktivitätszustand des Lese-/Schreibkopfes für alle Register 0 ist. Jeder dieser Quantenzustände bleibt durch die Transformation G_{i+2} unverändert, da diese Quantenzustände im Unterraum H liegen. Bei Gleichung 4.22 handelt es sich bei dem Ausschnitt des Quantenzustands, auf den die Transformation G_{i+2} wirkt, ebenfalls um einen Quantenzustand aus dem Unterraum H. Er hat die selbe Form wie die Quantenzustände in Gleichung 4.14. Für alle weiteren Transformationen G handelt es sich bei der Eingabe um die Summe von Quantenzuständen, deren Aktivitätszustand des Lese-/Schreibkopfes für alle Register 0 ist. Jeder einzelne Quantenzustand liegt als im Unterraum H. Es ist also $|k_i\rangle = |k_{i+1}\rangle = |k_{i+2}\rangle = \cdots = |k_{2t-1}\rangle$. Die Ausführung der Transformation T ändert

$|k_{2t-1}\rangle$ insofern, dass die Amplituden der Quantenzustände von $s_i = 2$ mit $s_i = 1$ vertauscht werden. Nun gilt

$$|k_{2t}\rangle = \sum_{x \in \Sigma^*} \alpha_x \, |\eta_t(x)\rangle \, . \tag{4.24}$$

□

Damit konnte Satz 25 vollständig bewiesen werden. Aus der Konstruktion der Quantenschaltkreisfamilie lässt sich folgendes Korollar ableiten.

Korollar 34. *Es sei M eine QTM ohne wiederholte Zustandsmessung mit Zustandsmenge Q und Alphabet Σ und einer vorgegebenen Laufzeit $t(n) \geq n$. Es gibt eine in Laufzeit* $\mathrm{poly}(|Q|, |\Sigma|, t)$ *berechenbare Funktion, die M auf eine Quantenschaltkreisfamilie $\mathcal{C}$ abbildet, die sich aus $\ell = (2t+1)(2 + \log_2(|Q|+1) + \log_2(|\Sigma|+1))$ Qubits und $\mathcal{O}(\mathrm{poly}(|Q| \cdot |\Sigma|) \cdot t^2)$ Elementargatter mit Matrixelementen aus $\widetilde{\mathbb{C}}$ zusammensetzt, sodass die Endkonfiguration von M auf Eingabe x und der Zustand $\mathcal{C}(|0^\ell\rangle)$ gemäß der Äquivalenzfunktion η_t äquivalent sind.*

5 Zusammenfassung

In der vorliegenden Arbeit wurde der Beweis aufgearbeitet, dass eine Quantenturingmaschine in einen Quantenschaltkreis überführt werden kann. Dieser Beweis wurde zuerst von A. Yao im Jahre 1993 veröffentlicht [12]. Es konnte gezeigt werden, dass der dabei entstehende Mehraufwand polynomiell von der Laufzeit, der Größe des Alphabets und der Zustandsmenge der Quantenturingmaschine abhängt. Auch die Darstellung eines Quantenschaltkreis als Quantenturingmaschine kann durch einen polynomiellen Mehraufwand gewährleistet werden [11].

Neben der Quantenturingmaschine und dem Quantenschaltkreis gibt es noch weitere Berechnungsmodelle. Quantenschaltkreise sind gebräuchlicher, weil sich mit ihrer Hilfe Algorithmen leichter beschreiben lassen. Näher an der physikalischen Implementierung sind sogenannte adiabatische und messungsbasierte Beschreibungen eines Quantencomputers [7, 23]. Die Quantenturingmaschine selber ist hauptsächlich aufgrund der Äquivalenz zum klassischen Modell entstanden und war neben den Quantenschaltkreisen eines der ersten Berechnungsmodelle.

A Beweis Lemma 21

Die in Lemma 21 beschriebenen Eigenschaften der Übergangsfunktion δ lassen sich aus der Unitarität Schrittoperator $\mathcal{S}$ herleiten. Aufgrund der Unitarität muss $\mathbf{I} = \mathcal{S}^\dagger \mathcal{S}$ gelten. Es ist also

$$
\begin{aligned}
\mathbf{I} = \Bigg(& \sum_{m=-\infty}^{\infty} |m\rangle\langle m-1| \otimes \left(A_{\mathrm{L}}^\dagger\right)_m \otimes \mathbf{I}_\infty + |m\rangle\langle m| \otimes \left(A_{\mathrm{N}}^\dagger\right)_m \otimes \mathbf{I}_\infty \\
& + |m\rangle\langle m+1| \otimes \left(A_{\mathrm{R}}^\dagger\right)_m \otimes \mathbf{I}_\infty \Bigg) \cdot \Bigg(\sum_{m'=-\infty}^{\infty} \left|m'-1\right\rangle\left\langle m'\right| \otimes \left(A_{\mathrm{L}}\right)_{m'} \otimes \mathbf{I}_\infty \\
& + \left|m'\right\rangle\left\langle m'\right| \otimes \left(A_{\mathrm{N}}\right)_{m'} \otimes \mathbf{I}_\infty + \left|m'+1\right\rangle\left\langle m'\right| \otimes \left(A_{\mathrm{R}}\right)_{m'} \otimes \mathbf{I}_\infty \Bigg) \\
= & \sum_{m=-\infty}^{\infty} \sum_{m'=-\infty}^{\infty} \Bigg(|m\rangle\langle m-1| \cdot \left|m'-1\right\rangle\left\langle m'\right| \otimes \left(A_{\mathrm{L}}^\dagger\right)_m \left(A_{\mathrm{L}}\right)_{m'} \otimes \mathbf{I}_\infty \\
& + |m\rangle\langle m-1| \cdot \left|m'\right\rangle\left\langle m'\right| \otimes \left(A_{\mathrm{L}}^\dagger\right)_m \left(A_{\mathrm{N}}\right)_{m'} \otimes \mathbf{I}_\infty \\
& + |m\rangle\langle m-1| \cdot \left|m'+1\right\rangle\left\langle m'\right| \otimes \left(A_{\mathrm{L}}^\dagger\right)_m \left(A_{\mathrm{R}}\right)_{m'} \otimes \mathbf{I}_\infty \\
& + |m\rangle\langle m| \cdot \left|m'-1\right\rangle\left\langle m'\right| \otimes \left(A_{\mathrm{N}}^\dagger\right)_m \left(A_{\mathrm{L}}\right)_{m'} \otimes \mathbf{I}_\infty \\
& + |m\rangle\langle m| \cdot \left|m'\right\rangle\left\langle m'\right| \otimes \left(A_{\mathrm{N}}^\dagger\right)_m \left(A_{\mathrm{N}}\right)_{m'} \otimes \mathbf{I}_\infty \\
& + |m\rangle\langle m| \cdot \left|m'+1\right\rangle\left\langle m'\right| \otimes \left(A_{\mathrm{N}}^\dagger\right)_m \left(A_{\mathrm{R}}\right)_{m'} \otimes \mathbf{I}_\infty \\
& + |m\rangle\langle m+1| \cdot \left|m'-1\right\rangle\left\langle m'\right| \otimes \left(A_{\mathrm{R}}^\dagger\right)_m \left(A_{\mathrm{L}}\right)_{m'} \otimes \mathbf{I}_\infty \\
& + |m\rangle\langle m+1| \cdot \left|m'\right\rangle\left\langle m'\right| \otimes \left(A_{\mathrm{R}}^\dagger\right)_m \left(A_{\mathrm{N}}\right)_{m'} \otimes \mathbf{I}_\infty \\
& |m\rangle\langle m+1| \cdot \left|m'+1\right\rangle\left\langle m'\right| \otimes \left(A_{\mathrm{R}}^\dagger\right)_m \left(A_{\mathrm{R}}\right)_{m'} \otimes \mathbf{I}_\infty \Bigg)
\end{aligned}
$$

Die einzelnen Summanden ergeben sich zu 0, wenn das innere Produkt 0 ergibt. Es bleiben nur die Summanden übrig, dessen inneres Produkt sich zu 1 ergibt. Dies ist der Fall, wenn $m' = m$, $m' = m-1$, $m' = m-2$, $m' = m+1$ bzw. $m' = m+2$, wobei die notwendige Bedingung vom

Bra-Vektor des inneren Produkts abhängig ist. Die Summe über m' fällt dadurch weg und es ergibt sich

$$
\begin{aligned}
\mathbf{I} = \sum_{m=-\infty}^{\infty} \Bigg(& |m\rangle\langle m| \otimes \left(A_{\mathrm{L}}^{\dagger}\right)_m \cdot \left(A_{\mathrm{L}}\right)_m \otimes \mathbf{I}_{\infty} \\
& + |m\rangle\langle m-1| \otimes \left(\mathbf{I}_{\dim(A)} \otimes \left(A_{\mathrm{L}}^{\dagger}\right)_m\right) \cdot \left(\left(A_{\mathrm{N}}\right)_{m-1} \otimes \mathbf{I}_{\dim(A)}\right) \otimes \mathbf{I}_{\infty} \\
& + |m\rangle\langle m-2| \otimes \left(\mathbf{I}_{\dim(A)} \otimes \left(A_{\mathrm{L}}^{\dagger}\right)_m\right) \cdot \left(\left(A_{\mathrm{R}}\right)_{m-2} \otimes \mathbf{I}_{\dim(A)}\right) \otimes \mathbf{I}_{\infty} \\
& + |m\rangle\langle m+1| \otimes \left(\left(A_{\mathrm{N}}^{\dagger}\right)_m \otimes \mathbf{I}_{\dim(A)}\right) \cdot \left(\mathbf{I}_{\dim(A)} \otimes \left(A_{\mathrm{L}}\right)_{m+1}\right) \otimes \mathbf{I}_{\infty} \\
& + |m\rangle\langle m| \otimes \left(A_{\mathrm{N}}^{\dagger}\right)_m \cdot \left(A_{\mathrm{N}}\right)_m \otimes \mathbf{I}_{\infty} \\
& + |m\rangle\langle m-1| \otimes \left(\mathbf{I}_{\dim(A)} \otimes \left(A_{\mathrm{N}}^{\dagger}\right)_m\right) \cdot \left(\left(A_{\mathrm{R}}\right)_{m-1} \otimes \mathbf{I}_{\dim(A)}\right) \otimes \mathbf{I}_{\infty} \\
& + |m\rangle\langle m+2| \otimes \left(\left(A_{\mathrm{R}}^{\dagger}\right)_m \otimes \mathbf{I}_{\dim(A)}\right) \cdot \left(\mathbf{I}_{\dim(A)} \otimes \left(A_{\mathrm{L}}\right)_{m+2}\right) \otimes \mathbf{I}_{\infty} \\
& + |m\rangle\langle m+1| \otimes \left(\left(A_{\mathrm{R}}^{\dagger}\right)_m \otimes \mathbf{I}_{\dim(A)}\right) \cdot \left(\mathbf{I}_{\dim(A)} \otimes \left(A_{\mathrm{N}}\right)_{m+1}\right) \otimes \mathbf{I}_{\infty} \\
& + |m\rangle\langle m| \otimes \left(A_{\mathrm{R}}^{\dagger}\right)_m \cdot \left(A_{\mathrm{R}}\right)_m \otimes \mathbf{I}_{\infty} \Bigg).
\end{aligned}
$$

Es sei $\mathbf{0}$ die Matrix deren Einträge alle 0 sind. Es lassen sich die folgenden Bedingungen an die Übgergangsfunktionstransformationen formulieren.

$$A_{\mathrm{L}}^{\dagger}A_{\mathrm{L}} + A_{\mathrm{N}}^{\dagger}A_{\mathrm{N}} + A_{\mathrm{R}}^{\dagger}A_{\mathrm{R}} = \mathbf{I} \tag{A.1}$$

$$\left(A_{\mathrm{N}}^{\dagger} \otimes \mathbf{I}_{\dim(A)}\right) \cdot \left(\mathbf{I}_{\dim(A)} \otimes A_{\mathrm{L}}\right) + \left(A_{\mathrm{R}}^{\dagger} \otimes \mathbf{I}_{\dim(A)}\right) \cdot \left(\mathbf{I}_{\dim(A)} \otimes A_{\mathrm{N}}\right) = \mathbf{0} \tag{A.2}$$

$$\left(\mathbf{I}_{\dim(A)} \otimes A_{\mathrm{L}}^{\dagger}\right) \cdot \left(A_{\mathrm{N}} \otimes \mathbf{I}_{\dim(A)}\right) + \left(\mathbf{I}_{\dim(A)} \otimes A_{\mathrm{N}}^{\dagger}\right) \cdot \left(A_{\mathrm{R}} \otimes \mathbf{I}_{\dim(A)}\right) = \mathbf{0} \tag{A.3}$$

$$\left(\mathbf{I}_{\dim(A)} \otimes A_{\mathrm{L}}^{\dagger}\right) \cdot \left(A_{\mathrm{R}} \otimes \mathbf{I}_{\dim(A)}\right) = \mathbf{0} \tag{A.4}$$

$$\left(A_{\mathrm{R}}^{\dagger} \otimes \mathbf{I}_{\dim(A)}\right) \cdot \left(\mathbf{I}_{\dim(A)} \otimes A_{\mathrm{L}}\right) = \mathbf{0} \tag{A.5}$$

Dabei ist es egal, an welcher Position m sich der Lese-/Schreibkopf genau befindet. Entscheidend ist, dass zwei unterschiedliche Zeichen gelesen werden, wenn der positionanzeigende Index der Matrizen nicht gleich ist. Dies wird aber durch das Tensorprodukt mit einer Einheitsmatrix verdeutlicht, die dieselbe Dimension haben wie die Matrizen A_d.

Gleichung A.2 und Gleichung A.3 führen zu der selben Einschränkung der Übergangsfunktion, da sie sich durch Adjunktion ineinander überführen lassen. Selbiges gilt auch für Gleichung A.4 und Gleichung A.5. Aus den Gleichung A.1, Gleichung A.2 und Gleichung A.4 lassen sich vier Einschränkungen an die Übergangsfunktion δ formulieren.

1. Aus Gleichung A.1 lässt sich die erste Bedingung herleiten. Die Summe der drei Matrizen $A_{\mathrm{L}}^{\dagger}A_{\mathrm{L}}$, $A_{\mathrm{N}}^{\dagger}A_{\mathrm{N}}$ und $A_{\mathrm{R}}^{\dagger}A_{\mathrm{R}}$ muss auf den Diagonaleinträgen 1 ergeben. Aus der Matrixmultiplikation ergibt sich für die Diagonaleinträge $a_{(ij)(ij)}$ von $A_{\mathrm{L}}^{\dagger}A_{\mathrm{L}}$:

$$a_{(ij)(ij)} = \sum_{p \in Q,\, \tau \in \Sigma} \left|\delta(q_i,\, \sigma_j,\, \mathrm{L},\, p,\, \tau)\right|^2 . \tag{A.6}$$

   Analog lassen sich die Matrixeinträge für $A_{\mathrm{N}}^{\dagger}A_{\mathrm{N}}$ und $A_{\mathrm{R}}^{\dagger}A_{\mathrm{R}}$ konstruieren. Diese unterscheiden sich ausschließlich in der Kopfbewegungsrichtung. Mit Gleichung A.6 ergibt sich, dass für beliebige $(q,\, \sigma) \in Q \times \Sigma$ gelten muss:

$$\sum_{\substack{p \in Q,\, \tau \in \Sigma,\\ d \in \{\mathrm{L},\, \mathrm{N},\, \mathrm{R}\}}} \left|\delta(q,\, \sigma,\, d,\, p,\, \tau)\right|^2 = 1. \tag{A.7}$$

2. Auch die zweite Bedingung lässt sich aus Gleichung A.1 herleiten. Hierfür müssen die Elemente betrachtet werden, die nicht auf der Diagonalen liegen. Diese müssen für alle drei Matrizen $A_{\mathrm{L}}^{\dagger}A_{\mathrm{L}}$, $A_{\mathrm{N}}^{\dagger}A_{\mathrm{N}}$ und $A_{\mathrm{R}}^{\dagger}A_{\mathrm{R}}$ aufsummiert 0 ergeben. Aus der Matrixmultiplikation ergibt sich für die Einträge $a_{(ik)(jl)}$ der Transformation $A_{\mathrm{L}}^{\dagger}A_{\mathrm{L}}$ mit $(i,\, k) \neq (j,\, l)$

$$a_{(ik)(jl)} = \sum_{p \in Q,\, \tau \in \Sigma} \delta(q_i,\, \sigma_k,\, \mathrm{L},\, p,\, \tau)^* \cdot \delta(q_j,\, \sigma_l,\, \mathrm{L},\, p,\, \tau).$$

   Analog lassen sich die Matrixeinträge für $A_{\mathrm{N}}^{\dagger}A_{\mathrm{N}}$ und $A_{\mathrm{R}}^{\dagger}A_{\mathrm{R}}$ konstruieren. Es ergibt sich, dass für beliebige $(q,\, \sigma)$, $(q',\, \sigma') \in Q \times \Sigma$ mit $(q,\, \sigma) \neq (q',\, \sigma')$ gilt

$$\sum_{\substack{p \in Q,\, \tau \in \Sigma,\\ d \in \{\mathrm{L},\, \mathrm{N},\, \mathrm{R}\}}} \delta(q',\, \sigma',\, d,\, p,\, \tau)^* \cdot \delta(q,\, \sigma,\, d,\, p,\, \tau) = 0. \tag{A.8}$$

3. Die dritte Bedingung lässt sich aus Gleichung A.2 herleiten. Für alle $(q,\, \sigma,\, \tau)$, $(q',\, \sigma',\, \tau') \in Q \times \Sigma \times \Sigma$ muss gelten

$$\begin{aligned} \Big\langle q,\, \sigma,\, \tau \Big| \Big(A_{\mathrm{N}}^{\dagger} \otimes \mathbf{I}_{\dim(A)}\Big) \cdot \Big(\mathbf{I}_{\dim(A)} \otimes A_{\mathrm{L}}\Big) \\ + \Big(A_{\mathrm{R}}^{\dagger} \otimes \mathbf{I}_{\dim(A)}\Big) \cdot \Big(\mathbf{I}_{\dim(A)} \otimes A_{\mathrm{N}}\Big) \Big| q',\, \sigma',\, \tau' \Big\rangle = 0 \end{aligned} \tag{A.9}$$

wobei σ, bzw. σ' und τ bzw. τ' die Zeichen zweier verschiedener Bandzellen sind. Es ergibt sich aus Gleichung A.9

$$0 = \left(\sum_{\substack{q'' \in Q, \\ \sigma'' \in \Sigma}} \delta(q,\, \sigma,\, \mathrm{N},\, q'',\, \sigma'')^* \cdot \left\langle q'',\, \sigma'',\, \tau \right| \right) \cdot \left(\sum_{\substack{q''' \in Q, \\ \tau'' \in \Sigma}} \delta(q',\, \tau',\, \mathrm{L},\, q''',\, \tau'') \cdot \left| q''',\, \sigma',\, \tau'' \right\rangle \right)$$
$$+ \left(\sum_{\substack{q'' \in Q, \\ \sigma'' \in \Sigma}} \delta(q,\, \sigma,\, \mathrm{R},\, q'',\, \sigma'')^* \cdot \left\langle q'',\, \sigma'',\, \tau \right| \right) \cdot \left(\sum_{\substack{q''' \in Q, \\ \tau'' \in \Sigma}} \delta(q',\, \tau',\, \mathrm{N},\, q''',\, \tau'') \cdot \left| q''',\, \sigma',\, \tau'' \right\rangle \right).$$

Gilt $q'' = q'''$ und $\sigma' = \sigma''$ sowie $\tau = \tau''$, ist das Ergebnis der obigen inneren Produkte 1, sonst 0. Die Übergangsfunktion muss nur für den Fall eingeschränkt werden, indem sich das innere Produkt zu 1 ergibt. Somit lässt sich die folgende Beschränkung der Übergangsfunktion formulieren.

Für alle $(q,\, \sigma,\, \sigma')$, $(q',\, \tau',\, \tau) \in Q \times \Sigma \times \Sigma$ muss gelten

$$\begin{aligned} 0 = \sum_{q'' \in Q} & \delta(q,\, \sigma,\, \mathrm{N},\, q'',\, \sigma')^* \cdot \delta(q',\, \tau',\, \mathrm{L},\, q'',\, \tau) \\ & + \delta(q,\, \sigma,\, \mathrm{R},\, q'',\, \sigma')^* \cdot \delta(q',\, \tau',\, \mathrm{N},\, q'',\, \tau). \end{aligned} \tag{A.10}$$

4. Die vierte und letzte Bedingung lässt sich aus Gleichung A.4 herleiten. Für alle $(q,\, \sigma,\, \tau)$, $(q',\, \sigma',\, \tau') \in Q \times \Sigma \times \Sigma$ muss gelten

$$\left\langle q,\, \sigma,\, \tau \right| \left(\mathbf{I}_{\dim(A)} \otimes A_{\mathrm{L}}^{\dagger} \right) \cdot \left(A_{\mathrm{R}} \otimes \mathbf{I}_{\dim(A)} \right) \left| q',\, \sigma',\, \tau' \right\rangle = 0, \tag{A.11}$$

wobei σ, bzw. σ' und τ, bzw. τ' die Zeichen zweier unterschiedlicher Bandzellen sind. Es ergibt sich aus Gleichung A.11

$$0 = \left(\sum_{\substack{q'' \in Q, \\ \tau'' \in \Sigma}} \delta(q,\, \tau,\, \mathrm{L},\, q'',\, \tau'')^* \cdot \left\langle q'',\, \sigma,\, \tau'' \right| \right) \cdot \left(\sum_{\substack{q''' \in Q, \\ \sigma'' \in \Sigma}} \delta(q',\, \sigma',\, \mathrm{L},\, q''',\, \sigma'') \cdot \left| q''',\, \sigma'',\, \tau' \right\rangle \right).$$

Mit $q'' = q'''$, $\sigma = \sigma''$ und $\tau' = \tau''$ ergibt sich die Bedingung an die Übergangsfunktion zu

$$0 = \sum_{q'' \in Q} \delta(q,\, \tau,\, \mathrm{L},\, q'',\, \tau')^* \cdot \delta(q',\, \sigma',\, \mathrm{R},\, q'',\, \sigma). \tag{A.12}$$

Obige Bedingung muss für alle $(q,\, \tau,\, \tau')$, $(q',\, \sigma',\, \sigma) \in Q \times \Sigma \times \Sigma$ gelten. □

B Beweis Lemma 27

Um Lemma 27 zu zeigen, muss nur die Orthogonalität für die verschiedenen Vektorpaare geprüft werden. Zu zeigen ist, dass für beliebige $(\tau_{i-1},\, p_i,\, \tau_i,\, \tau_{i+1}) \in \Sigma \times Q \times \Sigma \times \Sigma$ der Quantenzustand

$$\begin{aligned}\left|w_{\tau_{i-1},\, q_i,\, \tau_i,\, \tau_{i+1}}\right\rangle = &\sum_{q' \in Q,\, \tau' \in \Sigma} \delta(q_i,\, \tau_i,\, \mathrm{L},\, q',\, \tau') \left|2,\, q',\, \tau_{i-1},\, 0,\, \emptyset,\, \tau',\, 0,\, \emptyset,\, \tau_{i+1}\right\rangle \\ &+ \sum_{q' \in Q,\, \tau' \in \Sigma} \delta(q_i,\, \tau_i,\, \mathrm{N},\, q',\, \tau') \left|0,\, \emptyset,\, \tau_{i-1},\, 2,\, q',\, \tau',\, 0,\, \emptyset,\, \tau_{i+1}\right\rangle \\ &+ \sum_{q' \in Q,\, \tau' \in \Sigma} \delta(q_i,\, \tau_i,\, \mathrm{R},\, q',\, \tau') \left|0,\, \emptyset,\, \tau_{i-1},\, 0,\, \emptyset,\, \tau',\, 2,\, q',\, \tau_{i+1}\right\rangle\end{aligned}$$

orthonormal zu sich selbst ist für $(\sigma_{i-1},\, q_i,\, \sigma_i,\, \sigma_{i+1}) \in \Sigma \times Q \times \Sigma \times \Sigma$ und orthonormal ist zu

1. $\left|s_{i-1},\, q_{i-1},\, \sigma_{i-1},\, s_i,\, q_i,\, \sigma_i,\, s_{i+1},\, q_{i+1},\, \sigma_{i+1}\right\rangle$ mit $s_{i-1},\, s_i \neq 1$ und $s_{i-1},\, s_i,\, s_{i+1} \neq 2$,
2. $\left|v_{q_{i-1},\, \sigma_{i-1},\, \sigma_i,\, \sigma_{i+1}}\right\rangle$ für beliebige $(q_{i-1},\, \sigma_{i-1},\, \sigma_i,\, \sigma_{i+1}) \in Q \times \Sigma \times \Sigma \times \Sigma$

$$\begin{aligned}\left|v_{q_{i-1},\, \sigma_{i-1},\, \sigma_i,\, \sigma_{i+1}}\right\rangle = &\sum_{q' \in Q,\, \sigma' \in \Sigma} \delta(q_{i-1},\, \sigma_{i-1},\, \mathrm{N},\, q',\, \sigma') \left|2,\, q',\, \sigma',\, 0,\, \emptyset,\, \sigma_i,\, 0,\, \emptyset,\, \sigma_{i+1}\right\rangle \\ &+ \sum_{q' \in Q,\, \sigma' \in \Sigma} \delta(q_{i-1},\, \sigma_{i-1},\, \mathrm{R},\, q',\, \sigma') \left|0,\, \emptyset,\, \sigma',\, 2,\, q',\, \sigma_i,\, 0,\, \emptyset,\, \sigma_{i+1}\right\rangle,\end{aligned}$$

3. $\left|u_{q_{i-2},\, \sigma_{i-2},\, \sigma',\, \sigma_{i-1},\, \sigma_i,\, \sigma_{i+1}}\right\rangle$ für beliebige $(q_{i-2},\, \sigma_{i-2},\, \sigma',\, \sigma_{i-1},\, \sigma_i,\, \sigma_{i+1}) \in Q \times \Sigma \times \Sigma \times \Sigma \times \Sigma \times \Sigma$ mit

$$\left|u_{q_{i-2},\, \sigma_{i-2},\, \sigma',\, \sigma_{i-1},\, \sigma_i,\, \sigma_{i+1}}\right\rangle = \sum_{q' \in Q} \delta(q_{i-2},\, \sigma_{i-2},\, \mathrm{R},\, q',\, \sigma') \left|2,\, q',\, \sigma_{i-1},\, 0,\, \emptyset,\, \sigma_i,\, 0,\, \emptyset,\, \sigma_{i+1}\right\rangle$$

ist.

1. Die Orthogonalität zu der ersten Art der Quantenzustände aus dem Unterraum H muss für $s_{i-1},\, s_i,\, s_{i+1} = 0$ sowie $s_{i-1},\, s_i = 0$ und $s_{i+1} = 1$ gezeigt werden. Die resultierenden Quantenzustände, für die die Orthogonalität gezeigt werden muss, sind $|0,\, \emptyset,\, \sigma_{i-1},\, 0,\, \emptyset,\, \sigma_i,\, 0,\, \emptyset,\, \sigma_{i+1}\rangle$ und $|0,\, \emptyset,\, \sigma_{i-1},\, 0,\, \emptyset,\, \sigma_i,\, 1,\, q_{i+1},\, \sigma_{i+1}\rangle$ für $(\sigma_{i-1},\, \sigma_i,\, \sigma_{i+1},\, q_{i+1}) \in \Sigma \times \Sigma \times \Sigma \times Q$.

$$\begin{aligned}&\left\langle w_{\tau_{i-1},\, p_i,\, \tau_i,\, \tau_{i+1}} \,\middle|\, 0,\, \emptyset,\, \sigma_{i-1},\, 0,\, \emptyset,\, \sigma_i,\, 0,\, \emptyset,\, \sigma_{i+1}\right\rangle \\ &= \sum_{p' \in Q,\, \tau' \in \Sigma} \delta(p_i,\, \tau_i,\, \mathrm{L},\, p',\, \tau')^* \left\langle 2,\, p',\, \tau_{i-1},\, 0,\, \emptyset,\, \tau',\, 0,\, \emptyset,\, \tau_{i+1} \,\middle|\, 0,\, \emptyset,\, \sigma_{i-1},\, 0,\, \emptyset,\, \sigma_i,\, 0,\, \emptyset,\, \sigma_{i+1}\right\rangle \\ &\quad + \sum_{p' \in Q,\, \tau' \in \Sigma} \delta(p_i,\, \tau_i,\, \mathrm{N},\, p',\, \tau')^* \left\langle 0,\, \emptyset,\, \tau_{i-1},\, 2,\, p',\, \tau',\, 0,\, \emptyset,\, \tau_{i+1} \,\middle|\, 0,\, \emptyset,\, \sigma_{i-1},\, 0,\, \emptyset,\, \sigma_i,\, 0,\, \emptyset,\, \sigma_{i+1}\right\rangle \\ &\quad + \sum_{p' \in Q,\, \tau' \in \Sigma} \delta(p_i,\, \tau_i,\, \mathrm{R},\, p',\, \tau')^* \left\langle 0,\, \emptyset,\, \tau_{i-1},\, 0,\, \emptyset,\, \tau',\, 2,\, p',\, \tau_{i+1} \,\middle|\, 0,\, \emptyset,\, \sigma_{i-1},\, 0,\, \emptyset,\, \sigma_i,\, 0,\, \emptyset,\, \sigma_{i+1}\right\rangle\end{aligned}$$

$$
\begin{aligned}
&= \sum_{p' \in Q,\, \tau' \in \Sigma} \delta(p_i,\, \tau_i,\, \mathrm{L},\, p',\, \tau')^* \, \langle 2 \,|\, 0 \rangle \, \langle p' \,|\, \emptyset \rangle \, \langle \tau_{i-1} \,|\, \sigma_{i-1} \rangle \, \langle 0 \,|\, 0 \rangle \, \langle \emptyset \,|\, \emptyset \rangle \, \langle \tau' \,|\, \sigma_i \rangle \, \langle 0 \,|\, 0 \rangle \, \langle \emptyset \,|\, \emptyset \rangle \, \langle \tau_{i+1} \,|\, \sigma_{i+1} \rangle \\
&\quad + \sum_{p' \in Q,\, \tau' \in \Sigma} \delta(p_i,\, \tau_i,\, \mathrm{N},\, p',\, \tau')^* \, \langle 0 \,|\, 0 \rangle \, \langle \emptyset \,|\, \emptyset \rangle \, \langle \tau_{i-1} \,|\, \sigma_{i-1} \rangle \, \langle 2 \,|\, 0 \rangle \, \langle p' \,|\, \emptyset \rangle \, \langle \tau' \,|\, \sigma_i \rangle \, \langle 0 \,|\, 0 \rangle \, \langle \emptyset \,|\, \emptyset \rangle \, \langle \tau_{i+1} \,|\, \sigma_{i+1} \rangle \\
&\quad + \sum_{p' \in Q,\, \tau' \in \Sigma} \delta(p_i,\, \tau_i,\, \mathrm{R},\, p',\, \tau')^* \, \langle 0 \,|\, 0 \rangle \, \langle \emptyset \,|\, \emptyset \rangle \, \langle \tau_{i-1} \,|\, \sigma_{i-1} \rangle \, \langle 0 \,|\, 0 \rangle \, \langle \emptyset \,|\, \emptyset \rangle \, \langle \tau' \,|\, \sigma_i \rangle \, \langle 2 \,|\, 0 \rangle \, \langle p' \,|\, \emptyset \rangle \, \langle \tau_{i-1} \,|\, \sigma_{i-1} \rangle
\end{aligned}
$$

Alle Quantenzustände sind zueinander orthonormale Eigenvektoren. Es gilt beispielsweise $\langle 2 \,|\, 0 \rangle = 0$, aber $\langle 0 \,|\, 0 \rangle = 1$. Für alle drei Summanden ist mindestens einer der Faktoren 0, wodurch die Summe insgesamt 0 ergibt. Selbiges gilt auch für den Quantenzustand $|0,\, \emptyset,\, \sigma_{i-1},\, 0,\, \emptyset,\, \sigma_i,\, 1,\, q_{i+1},\, \sigma_{i+1}\rangle$. Somit ist die Orthogonalität für den ersten Vektor des Unterraumes H gezeigt.

2. Als nächstes ist zu zeigen, dass $\left| v_{q_{i-1},\, \sigma_{i-1},\, \sigma_i,\, \sigma_{i+1}} \right\rangle$ orthogonal zu $\left| w_{\tau_{i-1},\, p_i,\, \tau_i,\, \tau_{i+1}} \right\rangle$ ist.

$$
\begin{aligned}
&\left\langle w_{\tau_{i-1},\, p_i,\, \tau_i,\, \tau_{i+1}} \,\middle|\, v_{q_{i-1},\, \sigma_{i-1},\, \sigma_i,\, \sigma_{i+1}} \right\rangle \\
&= \sum_{\substack{p' \in Q,\, \tau' \in \Sigma \\ q' \in Q,\, \sigma' \in \Sigma}} \delta(p_i, \tau_i, \mathrm{L}, p', \tau')^* \delta(q_{i-1}, \sigma_{i-1}, \mathrm{N}, q', \sigma') \left\langle 2, p', \tau_{i-1}, 0, \emptyset, \tau', 0, \emptyset, \tau_{i+1} \,\middle|\, 2, q', \sigma', 0, \emptyset, \sigma_i, 0, \emptyset, \sigma_{i+1} \right\rangle \\
&\quad + \sum_{\substack{p' \in Q,\, \tau' \in \Sigma \\ q' \in Q,\, \sigma' \in \Sigma}} \delta(p_i, \tau_i, \mathrm{L}, p', \tau')^* \delta(q_{i-1}, \sigma_{i-1}, \mathrm{R}, q', \sigma') \left\langle 2, p', \tau_{i-1}, 0, \emptyset, \tau', 0, \emptyset, \tau_{i+1} \,\middle|\, 0, \emptyset, \sigma', 2, q', \sigma_i, 0, \emptyset, \sigma_{i+1} \right\rangle \\
&\quad + \sum_{\substack{p' \in Q,\, \tau' \in \Sigma \\ q' \in Q,\, \sigma' \in \Sigma}} \delta(p_i, \tau_i, \mathrm{N}, p', \tau')^* \delta(q_{i-1}, \sigma_{i-1}, \mathrm{N}, q', \sigma') \left\langle 0, \emptyset, \tau_{i-1}, 2, p', \tau', 0, \emptyset, \tau_{i+1} \,\middle|\, 2, q', \sigma', 0, \emptyset, \sigma_i, 0, \emptyset, \sigma_{i+1} \right\rangle \\
&\quad + \sum_{\substack{p' \in Q,\, \tau' \in \Sigma \\ q' \in Q,\, \sigma' \in \Sigma}} \delta(p_i, \tau_i, \mathrm{N}, p', \tau')^* \delta(q_{i-1}, \sigma_{i-1}, \mathrm{R}, q', \sigma') \left\langle 0, \emptyset, \tau_{i-1}, 2, p', \tau', 0, \emptyset, \tau_{i+1} \,\middle|\, 0, \emptyset, \sigma', 2, q', \sigma_i, 0, \emptyset, \sigma_{i+1} \right\rangle \\
&\quad + \sum_{\substack{p' \in Q,\, \tau' \in \Sigma \\ q' \in Q,\, \sigma' \in \Sigma}} \delta(p_i, \tau_i, \mathrm{R}, p', \tau')^* \delta(q_{i-1}, \sigma_{i-1}, \mathrm{N}, q', \sigma') \left\langle 0, \emptyset, \tau_{i-1}, 0, \emptyset, \tau', 2, p', \tau_{i+1} \,\middle|\, 2, q', \sigma', 0, \emptyset, \sigma_i, 0, \emptyset, \sigma_{i+1} \right\rangle \\
&\quad + \sum_{\substack{p' \in Q,\, \tau' \in \Sigma \\ q' \in Q,\, \sigma' \in \Sigma}} \delta(p_i, \tau_i, \mathrm{R}, p', \tau')^* \delta(q_{i-1}, \sigma_{i-1}, \mathrm{R}, q', \sigma') \left\langle 0, \emptyset, \tau_{i-1}, 0, \emptyset, \tau', 2, p', \tau_{i+1} \,\middle|\, 0, \emptyset, \sigma', 2, q', \sigma_i, 0, \emptyset, \sigma_{i+1} \right\rangle
\end{aligned}
$$

Bis auf den erste und vierten Summanden ist bei allen anderen Summanden der Bra-Ket-Vektor 0 und somit auch der Summand 0. Für den ersten und vierten Summanden ergibt sich für den Bra-Ket-Vektor 1, wenn $p' = q'$, $\sigma' = \tau_{i-1}$ und $\tau' = \sigma_i$ sowie $\tau_{i+1} = \sigma_{i+1}$ gilt. Für alle $(p_i,\, \tau_i,\, \sigma_i)$ und $(q_{i-1},\, \sigma_{i-1},\, \tau_{i-1}) \in Q \times \Sigma \times \Sigma$ ergibt sich

$$
\begin{aligned}
&\left\langle w_{\tau_{i-1},\, p_i,\, \tau_i,\, \tau_{i+1}} \,\middle|\, v_{q_{i-1},\, \sigma_{i-1},\, \sigma_i,\, \sigma_{i+1}} \right\rangle \\
&\qquad = \sum_{p' \in Q} \delta(p_i, \tau_i, \mathrm{L}, p', \sigma_i)^* \delta(q_{i-1}, \sigma_{i-1}, \mathrm{N}, p', \tau_{i-1}) + \delta(p_i, \tau_i, \mathrm{N}, p', \sigma_i)^* \delta(q_{i-1}, \sigma_{i-1}, \mathrm{R}, p', \tau_{i-1}).
\end{aligned}
$$

Diese Form entspricht der in Gleichung 4.8 beschriebenen Form. Somit ist

$$
\left\langle w_{\tau_{i-1},\, p_i,\, \tau_i,\, \tau_{i+1}} \,\middle|\, v_{q_{i-1},\, \sigma_{i-1},\, \sigma_i,\, \sigma_{i+1}} \right\rangle = 0.
$$

3. Es ist noch zu zeigen, dass auch die Quantenzustände $\left|w_{\tau_{i-1},\,p_i,\,\tau_i,\,\tau_{i+1}}\right\rangle$ und $\left|u_{q_{i-2},\,\sigma_{i-2},\,\sigma',\,\sigma_{i-1},\,\sigma_i}\right\rangle$ orthogonal zueinander sind.

$$
\begin{aligned}
&\left\langle w_{\tau_{i-1},\,p_i,\,\tau_i,\,\tau_{i+1}} \,\middle|\, u_{q_{i-2},\,\sigma_{i-2},\,\sigma',\,\sigma_{i-1},\,\sigma_i} \right\rangle \\
&= \sum_{\substack{p'\in Q,\\ \tau'\in\Sigma}} \sum_{q'\in Q} \delta(p_i,\tau_i,\mathrm{L},p',\tau')^*\delta(q_{i-2},\sigma_{i-2},\mathrm{R},q',\sigma') \left\langle 2,p',\tau_{i-1},0,\emptyset,\tau',0,\emptyset,\tau_{i+1} \,\middle|\, 2,q',\sigma_{i-1},0,\emptyset,\sigma_i,0,\emptyset,\sigma_{i+1}\right\rangle \\
&\quad + \sum_{\substack{p'\in Q,\\ \tau'\in\Sigma}} \sum_{q'\in Q} \delta(p_i,\tau_i,\mathrm{N},p',\tau')^*\delta(q_{i-2},\sigma_{i-2},\mathrm{R},q',\sigma') \left\langle 0,\emptyset,\tau_{i-1},2,p',\tau',0,\emptyset,\tau_{i+1} \,\middle|\, 2,q',\sigma_{i-1},0,\emptyset,\sigma_i,0,\emptyset,\sigma_{i+1}\right\rangle \\
&\quad + \sum_{\substack{p'\in Q,\\ \tau'\in\Sigma}} \sum_{q'\in Q} \delta(p_i,\tau_i,\mathrm{R},p',\tau')^*\delta(q_{i-2},\sigma_{i-2},\mathrm{R},q',\sigma') \left\langle 0,\emptyset,\tau_{i-1},0,\emptyset,\tau',2,p',\tau_{i+1} \,\middle|\, 2,q',\sigma_{i-1},0,\emptyset,\sigma_i,0,\emptyset,\sigma_{i+1}\right\rangle
\end{aligned}
$$

In diesem Fall sind die Bra-Ket-Vektoren der letzten beiden Summanden 0. Der Bra-Ket-Vektor des ersten Summanden ist 1, wenn $p' = q'$, $\tau' = \sigma_i$ und $\tau_{i-1} = \sigma_{i-1}$ sowie $\tau_{i+1} = \sigma_{i+1}$ gilt. Es ergibt sich somit für alle $(p_i,\, \tau_i,\, \sigma_i)$ und $(q_{i-2},\, \sigma_{i-2},\, \sigma') \in Q \times \Sigma \times \Sigma$

$$\left\langle w_{\tau_{i-1},\,p_i,\,\tau_i,\,\tau_{i+1}} \,\middle|\, u_{q_{i-2},\,\sigma_{i-2},\,\sigma',\,\sigma_{i-1},\,\sigma_i} \right\rangle = \sum_{p'\in Q} \delta(p_i,\,\tau_i,\,\mathrm{L},\,p',\,\sigma_i)^*\delta(q_{i-2},\,\sigma_{i-2},\,\mathrm{R},\,p',\,\sigma').$$

Dies entspricht Gleichung 4.9. Somit ist

$$\left\langle w_{\tau_{i-1},\,p_i,\,\tau_i,\,\tau_{i+1}} \,\middle|\, u_{q_{i-2},\,\sigma_{i-2},\,\sigma',\,\sigma_{i-1},\,\sigma_i} \right\rangle = 0$$

und die beiden Quantenzustände sind orthogonal zueinander.

4. Zuletzt ist noch zu zeigen, dass für $(\tau_{i-1},\, p_i,\, \tau_i,\, \tau_{i+1})$, $(\sigma_{i-1},\, q_i,\, \sigma_i,\, \sigma_{i+1}) \in \Sigma \times Q \times \Sigma \times \Sigma$ mit gilt $(\tau_{i-1},\, p_i,\, \tau_i,\, \tau_{i+1}) \neq (\sigma_{i-1},\, q_i,\, \sigma_i,\, \sigma_{i+1})$

$$\left\langle w_{\tau_{i-1},\,p_i,\,\tau_i,\,\tau_{i+1}} \,\middle|\, w_{\sigma_{i-1},\,q_i,\,\sigma_i,\,\sigma_{i+1}} \right\rangle = 0.$$

Desweiteren muss für $(\tau_{i-1},\, p_i,\, \tau_i,\, \tau_{i+1}) = (\sigma_{i-1},\, q_i,\, \sigma_i,\, \sigma_{i+1})$

$$\left\langle w_{\tau_{i-1},\,p_i,\,\tau_i,\,\tau_{i+1}} \,\middle|\, w_{\sigma_{i-1},\,q_i,\,\sigma_i,\,\sigma_{i+1}} \right\rangle = 1$$

gelten.

Es ergibt sich

$$
\begin{aligned}
&\left\langle w_{\tau_{i-1},\,p_i,\,\tau_i,\,\tau_{i+1}} \,\middle|\, w_{\sigma_{i-1},\,q_i,\,\sigma_i,\,\sigma_{i+1}} \right\rangle \\
&\quad = \sum_{\substack{p'\in Q,\\ \tau'\in\Sigma}} \sum_{\substack{q'\in Q,\\ \sigma'\in\Sigma}} \delta(p_i,\tau_i,\mathrm{L},p',\tau')^*\delta(q_i,\sigma_i,\mathrm{L},q',\sigma') \left\langle 2,p',\tau_{i-1},0,\emptyset,\tau',0,\emptyset,\tau_{i+1} \,\middle|\, 2,q',\sigma_{i-1},0,\emptyset,\sigma',0,\emptyset,\sigma_{i+1}\right\rangle \\
&\qquad + \sum_{\substack{p'\in Q,\\ \tau'\in\Sigma}} \sum_{\substack{q'\in Q,\\ \sigma'\in\Sigma}} \delta(p_i,\tau_i,\mathrm{L},p',\tau')^*\delta(q_i,\sigma_i,\mathrm{N},q',\sigma') \left\langle 2,p',\tau_{i-1},0,\emptyset,\tau',0,\emptyset,\tau_{i+1} \,\middle|\, 0,\emptyset,\sigma_{i-1},2,q',\sigma',0,\emptyset,\sigma_{i+1}\right\rangle
\end{aligned}
$$

$$
\begin{aligned}
&+ \sum_{\substack{p'\in Q,\\ \tau'\in\Sigma}} \sum_{\substack{q'\in Q,\\ \sigma'\in\Sigma}} \delta(p_i,\tau_i,\mathrm{L},p',\tau')^*\delta(q_i,\sigma_i,\mathrm{R},q',\sigma') \left\langle 2,p',\tau_{i-1},0,\emptyset,\tau',0,\emptyset,\tau_{i+1} \,\middle|\, 0,\emptyset,\sigma_{i-1},0,\emptyset,\sigma',2,q',\sigma_{i+1}\right\rangle \\
&+ \sum_{\substack{p'\in Q,\\ \tau'\in\Sigma}} \sum_{\substack{q'\in Q,\\ \sigma'\in\Sigma}} \delta(p_i,\tau_i,\mathrm{N},p',\tau')^*\delta(q_i,\sigma_i,\mathrm{L},q',\sigma') \left\langle 0,\emptyset,\tau_{i-1},2,p',\tau',0,\emptyset,\tau_{i+1} \,\middle|\, 2,q',\sigma_{i-1},0,\emptyset,\sigma',0,\emptyset,\sigma_{i+1}\right\rangle \\
&+ \sum_{\substack{p'\in Q,\\ \tau'\in\Sigma}} \sum_{\substack{q'\in Q,\\ \sigma'\in\Sigma}} \delta(p_i,\tau_i,\mathrm{N},p',\tau')^*\delta(q_i,\sigma_i,\mathrm{N},q',\sigma') \left\langle 0,\emptyset,\tau_{i-1},2,p',\tau',0,\emptyset,\tau_{i+1} \,\middle|\, 0,\emptyset,\sigma_{i-1},2,q',\sigma',0,\emptyset,\sigma_{i+1}\right\rangle \\
&+ \sum_{\substack{p'\in Q,\\ \tau'\in\Sigma}} \sum_{\substack{q'\in Q,\\ \sigma'\in\Sigma}} \delta(p_i,\tau_i,\mathrm{N},p',\tau')^*\delta(q_i,\sigma_i,\mathrm{R},q',\sigma') \left\langle 0,\emptyset,\tau_{i-1},2,p',\tau',0,\emptyset,\tau_{i+1} \,\middle|\, 0,\emptyset,\sigma_{i-1},0,\emptyset,\sigma',2,q',\sigma_{i+1}\right\rangle \\
&+ \sum_{\substack{p'\in Q,\\ \tau'\in\Sigma}} \sum_{\substack{q'\in Q,\\ \sigma'\in\Sigma}} \delta(p_i,\tau_i,\mathrm{R},p',\tau')^*\delta(q_i,\sigma_i,\mathrm{L},q',\sigma') \left\langle 0,\emptyset,\tau_{i-1},0,\emptyset,\tau',2,p',\tau_{i+1} \,\middle|\, 2,q',\sigma_{i-1},0,\emptyset,\sigma',0,\emptyset,\sigma_{i+1}\right\rangle \\
&+ \sum_{\substack{p'\in Q,\\ \tau'\in\Sigma}} \sum_{\substack{q'\in Q,\\ \sigma'\in\Sigma}} \delta(p_i,\tau_i,\mathrm{R},p',\tau')^*\delta(q_i,\sigma_i,\mathrm{N},q',\sigma') \left\langle 0,\emptyset,\tau_{i-1},0,\emptyset,\tau',2,p',\tau_{i+1} \,\middle|\, 0,\emptyset,\sigma_{i-1},2,q',\sigma',0,\emptyset,\sigma_{i+1}\right\rangle \\
&+ \sum_{\substack{p'\in Q,\\ \tau'\in\Sigma}} \sum_{\substack{q'\in Q,\\ \sigma'\in\Sigma}} \delta(p_i,\tau_i,\mathrm{R},p',\tau')^*\delta(q_i,\sigma_i,\mathrm{R},q',\sigma') \left\langle 0,\emptyset,\tau_{i-1},0,\emptyset,\tau',2,p',\tau_{i+1} \,\middle|\, 0,\emptyset,\sigma_{i-1},0,\emptyset,\sigma',2,q',\sigma_{i+1}\right\rangle .
\end{aligned}
$$

Einträge ungleich Null gibt es, wenn $\tau_{i-1} = \sigma_{i-1}$, $\tau_i = \sigma_i$, $\tau_{i+1} = \sigma_{i+1}$ sowie $\tau' = \sigma'$ und $p' = q'$ gilt. Des Weiteren können nur die drei Summanden ungleich Null sein, dessen Quantenzustände unter den genannten Bedingungen gleich sind. Somit lässt sich die Gleichung vereinfachen zu

$$
\begin{aligned}
&\left\langle w_{\tau_{i-1},p_i,\tau_i,\tau_{i+1}} \,\middle|\, w_{\sigma_{i-1},q_i,\sigma_i,\sigma_{i+1}}\right\rangle \\
&\quad= \sum_{p'\in Q,\,\tau'\in\Sigma} \delta(q_i,\tau_i,\mathrm{L},p',\tau')^*\delta(p_i,\tau_i,\mathrm{L},p',\tau') \left\langle 2,p',\tau_{i-1},0,\emptyset,\tau',0,\emptyset,\tau_{i+1} \,\middle|\, 2,p',\tau_{i-1},0,\emptyset,\tau',0,\emptyset,\tau_{i+1}\right\rangle \\
&\qquad+ \sum_{p'\in Q,\,\tau'\in\Sigma} \delta(q_i,\tau_i,\mathrm{N},p',\tau')^*\delta(p_i,\tau_i,\mathrm{N},p',\tau') \left\langle 0,\emptyset,\tau_{i-1},2,p',\tau',0,\emptyset,\tau_{i+1} \,\middle|\, 0,\emptyset,\tau_{i-1},2,p',\tau',0,\emptyset,\tau_{i+1}\right\rangle \\
&\qquad+ \sum_{p'\in Q,\,\tau'\in\Sigma} \delta(q_i,\tau_i,\mathrm{R},p',\tau')^*\delta(p_i,\tau_i,\mathrm{R},p',\tau') \left\langle 0,\emptyset,\tau_{i-1},0,\emptyset,\tau',2,p',\tau_{i+1} \,\middle|\, 0,\emptyset,\tau_{i-1},0,\emptyset,\tau',2,p',\tau_{i+1}\right\rangle .
\end{aligned}
$$

Da die Quantenzustände orthonormiert sind, ergibt sich weiterhin

$$
\left\langle w_{\tau_{i-1},p_i,\tau_i,\tau_{i+1}} \,\middle|\, w_{\sigma_{i-1},q_i,\sigma_i,\sigma_{i+1}}\right\rangle = \sum_{\substack{p'\in Q,\,\tau'\in\Sigma,\\ d\in\{\,\mathrm{L},\mathrm{N},\mathrm{R}\,\}}} \delta(q_i,\tau_i,d,p',\tau')^*\delta(p_i,\tau_i,d,p',\tau')
$$

Für $q_i \neq p_i$ ergibt sich nach Gleichung 4.7 diese Summe zu 0, für $q_i = p_i$ ergibt sich nach Gleichung 4.6 diese Summe zu 1.

Für alle Quantenzustände aus dem Unterraum H konnte gezeigt werden, dass diese orthonormal zu $\left|w_{\tau_{i-1},p_i,\tau_i,\tau_{i+1}}\right\rangle$ sind und $\left|w_{\tau_{i-1},p_i,\tau_i,\tau_{i+1}}\right\rangle$ orthonormal zu sich selbst ist. Somit konnte die Richtigkeit von Lemma 27 gezeigt werden.

Literaturverzeichnis

[1] R. P. Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, vol. 21, no. 6–7, 1982.

[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, pp. 303–332, jan 1999.

[3] I. N. Levine, *Quantum chemistry*. Boston: Pearson, 2014.

[4] C. Cohen-Tannoudji, B. Diu, and F. Laloe, *Quantum mechanics*. New York: Wiley, 2005.

[5] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge New York: Cambridge University Press, 2010.

[6] E. Rieffel and W. Polak, *Quantum Computing: A Gentle Introduction*. The MIT Press, 1st ed., 2011.

[7] F. A. Dziemba, "Adiabatic Quantum Computation," *ArXiv e-prints*, Oct. 2016.

[8] D. Deutsch, "Quantum computational networks," *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 425, no. 1868, pp. 73–90, 1989.

[9] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," *Phys. Rev. A*, vol. 52, pp. 3457–3467, Nov 1995.

[10] D. Deutsch, "Quantum theory, the church–turing principle and the universal quantum computer," *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 400, no. 1818, pp. 97–117, 1985.

[11] E. Bernstein and U. Vazirani, "Quantum complexity theory," in *Proceedings of the Twenty-fifth Annual ACM Symposium on Theory of Computing*, STOC '93, (New York, NY, USA), pp. 11–20, ACM, 1993.

[12] A. C.-C. Yao, "Quantum circuit complexity," in *Foundations of Computer Science, 1993. Proceedings., 34th Annual Symposium on*, pp. 352–361, IEEE, 1993.

[13] H. Nishimura and M. Ozawa, "Computational Complexity of Uniform Quantum Circuit Families and Quantum Turing Machines," *eprint arXiv:quant-ph/9906095*, June 1999.

[14] M. Ozawa and H. Nishimura, "Local Transition Functions of Quantum Turing Machines," *eprint arXiv:quant-ph/9811069*, Nov. 1998.

[15] M. Ozawa, "Quantum Turing Machines: Local Transition, Preparation, Measurement, and Halting," *eprint arXiv:quant-ph/9809038*, Sept. 1998.

[16] H. Nishimura, "Quantum computation with restricted amplitudes," *International Journal of Foundations of Computer Science*, vol. 14, no. 05, pp. 853–870, 2003.

[17] H. Nishimura and M. Ozawa, "Perfect Computational Equivalence between Quantum Turing Machines and Finitely Generated Uniform Quantum Circuit Families," *eprint arXiv:quant-ph/0511117*, Nov. 2005.

[18] H. Nishimura and M. Ozawa, "Uniformity of quantum circuit families for error-free algorithms," *Theoretical Computer Science*, vol. 332, no. 1, pp. 487 – 496, 2005.

[19] U. Vazirani, "A survey of quantum complexity theory," in *Proceedings of Symposia in Applied Mathematics*, vol. 58, pp. 193–220, 2002.

[20] C. Westergaard, "Computational equivalence between quantum Turingmachines and quantum circuit families," Master's thesis, University Copenhagen, 2005.

[21] K.-I. Ko and H. Friedman, "Computational complexity of real functions," *Theoretical Computer Science*, vol. 20, no. 3, pp. 323 – 352, 1982.

[22] G. Buntrock, C. Damm, U. Hertrampf, and C. Meinel, "Structure and importance of logspace-mod class," *Mathematical systems theory*, vol. 25, pp. 223–237, Sep 1992.

[23] R. Raussendorf and H. J. Briegel, "A one-way quantum computer," *Physical Review Letters*, vol. 86, no. 22, pp. 5189–5191, 2001.

Erklärung

Ich versichere hiermit, dass

1. ich die Arbeit selbstständig verfasst habe,
2. keine anderen als die angegebenen Quellen und Hilfsmittel benutzt wurden,
3. alle Stellen der Arbeit, die wörtlich oder sinngemäß aus anderen Quellen übernommen wurden, als solche kenntlich gemacht sind, und
4. die Arbeit in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegt habe.

Hannover, den 03.09.2018