Messungsbasierte Quantenrechner

Seminar: Theoretische Probleme der kondensierten Materie

Daniel Klagges

31. Januar 2010

Inhaltsverzeichnis

Dieses Dokument ist das Konzeptpapier zum Seminarvortrag *Messungsbasierte Quantenrechner* von Daniel Klagges im Rahmen des Seminars *Theoretische Probleme der kondensierten Materie* im Wintersemester 2009/2010. Es soll den Inhalt und die Gliederung des Vortrags darstellen.

1 Überblick

Quantenrechner werden derzeit hauptsächlich durch ein Schaltkreismodell beschrieben [3]. Dabei werden eine Menge von Qubits in einem Basiszustand initialisiert und dann eine Reihe von Quantengattern, in Form von unitären Transformationen, auf sie angewendet. Das Ergebnis der Berechnung wird am Ende durch die Messung der einzelnen Qubits ausgelesen.

Messungsbasierte Quantenrechner bieten eine (im Sinne der polynomiellen Reduzierbarkeit) äquivalentes Modell [16, 9]. Im Gegensatz zu dem Schaltkreismodell werden die Qubits in einem hoch verschränkten Zustand initialisiert. Das Programm ist eine Folge von Messungen zu verschiedenen Basen an den Qubits. Da eine Messung an einem Qubit im allgemeinen mit einer Zustandsveränderung dieses (und durch die Verschränkung auch anderer) Qubits verbunden ist, wird so eine Berechnung durchgeführt.

2 Motivation

Das Schaltkreismodell ist ein weit verbreitetes und gut verstandenes Konzept um Quantenrechner zu beschreiben. Da außerdem die messungsbasierten Quantenrechner im Sinne der polynomiellen Reduzierbarkeit zu dem Schaltkreismodell äquivalent sind [20], stellt sich die Frage, warum man sich überhaupt mit diesen alternativen Modellen für Quantencomputer befassen soll.

Rechnermodelle werden für klassische Computer schon lange untersucht. Bekanntes Beispiel ist die durch Alan Turing im Jahr 1936 entwickelte *Turingmaschine* [35]. Eine Turingmaschine kann lediglich einzelne Zeichen von einem linearem Speicherband lesen bzw. schreiben und den Lese- bzw. Schreibkopf um genau eine Speicherzelle nach links oder rechts bewegen. In diesem Sinn ist sie also ein sehr beschränktes Modell. Trotzdem kann sie alle bekannten klassischen Rechnermodelle und implementierte Rechner effizient simulieren. Die Vermutung, dass alle klassischen Rechnermodelle polynomiell äquivalent sind, ist in der *erweiterten Churchen-These* [36] formuliert.

Hat man eine vielzahl äquivalenter Rechnermodelle zur Verfügung, kann man für eine konkrete Problemstellung das gerade geeigneteste Modell wählen. So ist z.B. ein beschränktes Modell wie die Turing-Maschine nützlich, wenn man eine untere Schranke für die Laufzeit aller Algorithmen für ein bestimmtes Problem sucht, wie es im Rahmen der Komplexitätstheorie der Fall ist [12]. Will man andererseits zu einem Problem einen möglichst effizienten Algorithmus formulieren, bieten es sich an eine in ihrem Befehlsumfang mächtiges und durch Menschen intuitiv erfassbares Modell zu verwenden, wie sie sich z.B. hinter den hohen Programmiersprachen verbergen (C++, Pascal, Pseudocode) [33]. Um einen Rechner zu implementieren nutzt man Modelle, die man einfach auf physikalische Systeme abbilden kann und dabei sowohl in ihrem Preis als auch in ihrer Ausführungsgeschwindigkeit effizient sind (Registermaschine, Von-Neumann-Architektur)[18].

Das Quanten-Schaltkreismodell ist mit seiner Analogie zu klassischen Schaltkreisen und seiner anschaulichen graphischen Darstellung einer für Menschen benutzbaren Programmiersprache für Quantenrechner am nächsten. Entsprechend sind fast alle bekannten Quantenalgorithmen als Quantenschaltkreise formuliert [32]. Eine Quantenturingmaschine teilt die Bedeutung der klassischen Turingmaschine unter anderem in der Quanten-Komplexitätstheorie [13, 6]. Ein Modell in [14] nutzt den adiabatischen Übergang von Grundzuständen (Adiabatic-Quantum-Computation).

Auf welche Weise eine praktisch brauchbarer Quantencomputer in Zukunft realisiert wird lässt sich noch nicht absehen. Das messungsbasierte Modell bietet gegenüber dem Schaltkreismodell womöglich einen einfacher zu realisierenden Ansatz, da es die Notwendigkeit reversible Transformationen an den Qubits durchzuführen einspart (auf Kosten eines allgemeineren Initialisierungs- und Ausleseprozesses) [25, 28].

Durch die gleichzeitige Messung verschiedener Qubits beinhaltet das messungsbasierte

Modell eine Möglichkeit der Parallelisierung. Parallelisierung ist im Rahmen der Quantenfehlerkorrektur meist ohnehin nötig und erleichtert es einen Quantenrechner in einem physikalischen System mit kurzer Dekoherenzzeit zu implementieren [1]. Auf der anderen Seite erzwingt ein messungsbasierter Quantenrechner auch bei einer parallel ausgeführten Messung die anschließende (klassische) Auswertung der Messergebnisse. Dadurch hilft er eine Antwort auf die Frage zu finden, wie viel quantenmechanischen „Anteil“ ein klassischer Computer benötigt, um die Möglichkeiten eines Quantenrechners auszuschöpfen [20].

Unabhängig von den theoretischen und praktischen Anwendungen bieten messungsbasierte Modelle eine alternative Sicht auf Quantenrechner und helfen so ihre Natur und ihre Möglichkeiten besser zu verstehen.

3 Teleportation-Quantum-Computation (TQC)

Teleportation-Quantum-Computation basiert auf einer Idee von Gottesman und Chuang [17]. Sie zeigen wie nahe Messungen und Berechnungen zusammenhängen, sobald man Verschränkung in Betracht zieht. Sie lassen sich als eine Verallgemeinerung der gewöhnlichen Quantenteleportation [5, 24] verstehen.

Bei der Quantenteleportation wird zusätzlich zu dem zu teleportierenden Qubit in dem beliebigen Zustand $|\psi\rangle$ ein EPR-Paar, also ein Paar von Qubits in dem Bell-Zustand

$$|\beta_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

präpariert. An dem zu teleportierendem Qubit und einem der präparierten Qubits wird nun eine Messung bezüglich der Bell-Basis B:

$$\begin{aligned} |\beta_0\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\beta_2\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\beta_1\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\beta_3\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \end{aligned}$$

durchgeführt (Abbildung 3.1 links) . Durch die Verschränkung befindet sich das dritte Qubit dannach in dem Zustand

$$\sigma_j|\psi\rangle,$$

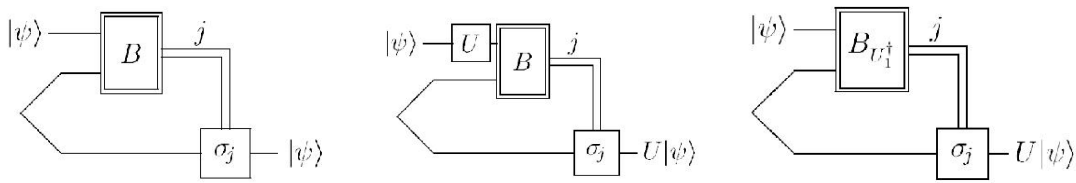

Abbildung 3.1: Quantenteleportation (links), Teleportation eines transformierten Zustands (Mitte) und Gatterteleportation durch Messung (rechts)

wenn man mit σ_j die Pauli-Matrizen

$$\begin{aligned}
\sigma_0 &= I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\
\sigma_1 &= X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\
\sigma_2 &= Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \\
\sigma_3 &= Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}
\end{aligned}$$

und mit j das Ergebnis der obigen Messung meint. Um dies zu zeigen rechnet man nach, dass man den initialen Zustand $|\psi\rangle|\beta_0\rangle$ auch folgendermaßen darstellen kann:

$$|\psi\rangle|\beta_0\rangle = \frac{1}{2}\sum_{i=0}^{3} |\beta_i\rangle \otimes \sigma_i|\psi\rangle.$$

Durch die Anwendung des jeweiligen Pauli Operators, abhängig vom Messergebnis, kann man dann den ursprünglichen Quantenzustand reproduzieren.

Wir wollen nun erreichen, den Quantenzustand nicht nur zu teleportieren, sonder eine beliebige Transformation U auf ihm anzuwenden. Dies lässt sich natürlich trivial umsetzen, in dem man zunächst U auf den Zustand $|\psi\rangle$ anwendet und dann den transformierten Zustand teleportiert (Abbildung 3.1 Mitte). Andererseits ist die Transformation und anschließende Bell-Messung gleichbedeutend mit einer Messung zur rotierten Basis

$$(U^\dagger \otimes I)|\beta_i\rangle \qquad i \in \{0,1,2,3\}.$$

Siehe dazu Abbildung 3.1 rechts.

Nur durch die Präparierung eines verschränkten Zustands und die Messung an zwei Qubits zu einer beliebigen Basis lassen sich also beliebige ein-Qubit-Operatoren realisieren. Leider wird der transformierte Zustand nicht exakt hergestellt, sondern - in Abhängigkeit von dem Messergebnis - nur bis auf einen *Seiteneffektoperator* σ_j. Man kann ihm jedoch immer Rechnung tragen, in dem man die abschließende Messung nicht bezüglich der Standardbasis, sondern bezüglich der um σ_j rotierten Basis durchführt.

Nielsen und Leung haben das Konzept auf mehrere Qubits verallgemeinert und gezeigt, dass 2-Qubit Messungen universell sind [27, 23, 24].

4 One-Way-Quantum-Computer (1-WQC)

Das Modell des One-Way-Quantum-Computer wurde von Raussendorf und Briegel entwickelt [31, 30]. Analog zum TQC benötigt es in der Berechnungsphase nur Messungen und erzeugt Zustände nur bis auf ungewollte Seiteneffektoperatoren. Im Gegensatz zum TQC kommt ein 1-WQC jedoch mit ein-Qubit Messungen aus, benötigt aber einen Initialisierungszustand, in dem alle Qubits verschränkt sind.

4.1 Der Cluster-States

In der Initialisierungsphase wird ein zweidimensionales Gitter von Qubits C (Abbildung 4.1) in einem *Cluster-State* initialisiert [8]. Ein Zustand $|\psi\rangle$ wird Cluster-State genannte, wenn er die folgenden Eigenwertgleichungen erfüllt:

$$K_a := X_a \bigotimes_{b \in \Gamma(a)} Z_b,$$

$$K_a|\psi\rangle = -1^{\kappa_a}|\psi\rangle. \tag{4.1}$$

Dabei ist $\{\kappa_a \in \{0,1\} | a \in C\}$ und mit $\Gamma(a)$ ist die Menge aller direkten Nachbarn von a gemeint. In Worten ausgedrückt: „Wendet man auf ein Qubit eines Cluster-States den X Operator und auf alle benachbarten Qubits den Z Operator an, wird höchstens die Phase des Zustands invertiert.“ Cluster-States werden für festes $\{\kappa_a\}_{a \in C}$ durch die Eigenwertgleichungen eindeutig definiert [8].

Um einen Cluster-State zu präparieren könnte man zu einem beliebigem Zustand Messungen zu allen Operatoren K_a durchführen, oder das System in den Grundzustand eines

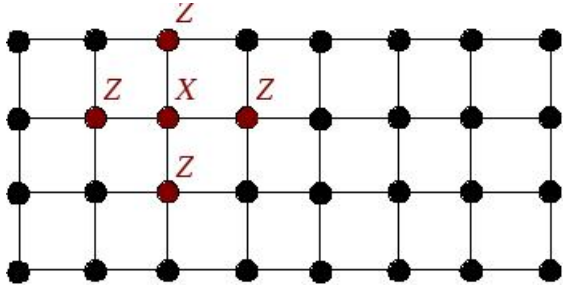

Abbildung 4.1: Cluster-State aus in einem zweidimensionalem Gitter aus Qubits

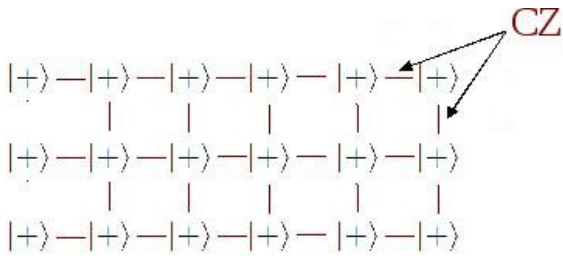

Abbildung 4.2: Initialisierung eines Clusterstates aus einem Produktzustand

geeigneten Hamilton-Operators abkühlen. Eine praktisch eventuell leichter umzusetzende Verfahren initialisiert zunächst den Cluster in dem Produktzustand (Abbildung 4.2):

$$|+\rangle_C := \bigotimes_{a \in C} |+\rangle_a,$$

mit

$$|+\rangle_a := \frac{1}{\sqrt{2}}(|0\rangle_a + |1\rangle_a) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} |0\rangle = H|0\rangle.$$

Dabei ist H die Hadamard-Tranformation. Der Zustand $|+\rangle$ ist Eigenzustand mit Eigenwert 1 des X Operators.

Die Verschränkung wird nun durch Anwendung eines *Controlled-Z*-Operators auf alle benachbarten Qubitpaare erzeugt (Abbildung 4.2):

$$S := \prod_{(a,b) \in C} S_{ab}$$

$$S_{ab} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$|\psi\rangle_C := S|+\rangle_C$$

Um zu sehen, dass dadurch ein Cluster-State hergestellt wird stellt man zunächst fest, dass die Operatoren S_{ab} mit den X_c Operatoren aller nicht beteiligten Qubits c und mit den Z_d Operatoren aller Qubits kommutiert:

$$\begin{aligned} S_{ab} X_c S_{ab}^\dagger &= X_c \ \forall c \in C \backslash \{a, b\}, \\ S_{ab} Z_d S_{ab}^\dagger &= Z_d \ \forall d \in C. \end{aligned}$$

Sie kommutieren aber nicht mit X_a bzw. X_b:

$$\begin{aligned} S_{ab} X_a S_{ab}^\dagger &= X_a \otimes Z_b, \\ S_{ab} X_b S_{ab}^\dagger &= Z_a \otimes X_b. \end{aligned}$$

Die Wirkung von S auf X_a ist also:

$$SX_aS^\dagger = X_a \bigotimes_{b\in\Gamma(a)} Z_b.$$

Da $|+\rangle_a$ der Eigenzustand von X_a zum Eigenwert 1 ist, gilt auch für alle a:

$$X_a|+\rangle_C = |+\rangle_C$$

und so:

$$\begin{aligned} |\psi\rangle_C &= S|+\rangle_C \\ &= SX_a|+\rangle_C \\ &= SX_aS^\dagger|\psi\rangle_C \\ &= X_a \bigotimes_{b\in\Gamma(a)} Z_b|\psi\rangle_C. \end{aligned}$$

Der auf diese Weise erzeugte Zustand ist also tatsächlich ein Cluster-State mit $\kappa_a = 0$ für alle a.

4.2 Berechnung durch Messung

Nach der Initialisierung werden nur noch Ein-Qubit-Messungen an dem Cluster-State durchgeführt. Wie wir sehen werden genügen zwei Arten von Messungen:

- Messungen zur Eigenbasis des Z-Operators:

$$M_z := \{|0\rangle, |1\rangle\}$$

- und Messungen bezüglich der Basis

$$M(\Phi) := \{|0\rangle + e^{i\Phi}|1\rangle, |0\rangle - e^{i\Phi}|1\rangle\}$$

  für einen Winkel Φ.

Bei $M(\Phi)$ handelt sich um Messungen in der xy-Ebene der Bloch-Sphäre. Genauer für den Winkel $\Phi = 0$ die Eigenbasis des X-Operators, und für $\Phi = \frac{\pi}{2}$ die Eigenbasis des Y-Operators.

Messungen bezüglich M_z können benutzt werden, um das Ergebnis einer Berechnung auszulesen. Des weiteren kann gezeigt werden [8], dass Messungen zu dieser Basis an einem Qubit die Cluster Eigenschaft der anderen Qubits nicht aufheben. Man kann solche Messungen also verwenden, um Qubits nachträglich aus einem Cluster zu entfernen.

4.2.1 Ein-Qubit-Operatoren

Um die Wirkung von Messungen bezüglich der Basis $M(\Phi)$ zu demonstrieren, betrachten wir ein System aus zwei Qubits. Das erste Qubit sei in einem Zustand $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ und das zweite Qubit in dem Zustand $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ initialisiert. Der Controlled-Z-Operator bringt sie in den verschränkten Zustand

$$\frac{1}{\sqrt{2}}(\alpha|0\rangle|+\rangle + \beta|1\rangle|-\rangle).$$

Das erste Qubit werde nun bezüglich der Basis $M(\Phi)$ gemessen. Die beiden möglichen Ergebnisse haben gleiche Wahrscheinlichkeit. Je nach dem ob das Ergebnis der Messung der Eigenwert $+1$ oder -1 ist, hinterlässt sie das zweite Qubit in dem Zustand:

$$\alpha|+\rangle \pm e^{i\Phi}\beta|-\rangle.$$

Da die Zustände $|+\rangle$ und $|-\rangle$ aus den Zuständen $|0\rangle$ und $|1\rangle$ durch die Hadamard Transformation hervorgehen:

$$\alpha H|0\rangle \pm e^{i\Phi}\beta H|1\rangle, \tag{4.2}$$

erkennt man den ursprünglichen Zustand $|\psi\rangle$ wieder. Sieht man weiter, dass die Wirkung des Vorfaktors $\pm e^{i\Phi}$ (bis auf eine globale Phase) eine Rotation um die z-Achse der Bloch-Sphäre ist, kann man diesen Zustand auch folgendermaßen schreiben:

$$X^m H U_z(\Phi)|\psi\rangle. \tag{4.3}$$

Dabei ist $m \in \{0, 1\}$ der Index, mit dem das Messergebnis -1^m repräsentiert wird.

Durch die Messung wurde der Zustand $|\psi\rangle$ also auf das zweite Qubit übertragen und gleichzeitig eine Rotation um die z-Achse und einen Hadamard-Operator angewendet. Der Winkel der Rotation lässt sich durch die Wahl der Messbasis einstellen. Analog wie beim Teleportation-Quantum-Computation werden zusätzlich vom Messergebnis abhängige Seiteneffektoperatoren angewendet. Mit dieser Messung lassen sich ein Reihe von Ein-Qubit-Operatoren realisieren. Wir werden sehen, dass als Seiteneffektsoperatoren lediglich die Operatoren X und Z auftreten.

4.2.1.1 Hadamard

Für den Fall $\Phi = 0$, also einer Messung bezüglich der Eigenbasis von X, wird keine Rotation durchgeführt. Es wird eine Hadamard-Transformation ausgeführt:

$$X^m H$$

4.2.1.2 Identität

Führt man zwei Messungen bezüglich der Eigenbasis von X hintereinander aus, erhält man mit $XH = HZ$:

$$X^{m_2} H\, X^{m_1} H = X^{m_2} Z^{m_1}.$$

Bis auf die Seiteneffektsoperatoren wird also keine Transformation durchgeführt. Man kann solche Messungen also nutzen um einen Quantenzustand im Cluster weiter zu leiten. Man beachte, dass man beide Messungen gleichzeitig durchführen kann.

4.2.1.3 Phasengatter

Der Fall $\Phi = \frac{\pi}{2}$, also einer Messung bezüglich der Eigenbasis von Y, bewirkt eine Phasenverschiebung von i:

$$X^m H \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} =: X^m H P_{\frac{\pi}{2}}.$$

Eine weitere Messung mit $\Phi_2 = 0$ macht wieder den Hadamard-Operator rückgängig.

$$X^{m_2} H \, X^{m_1} H P_{\frac{\pi}{2}} = X^{m_2} Z^{m_1} P_{\frac{\pi}{2}}.$$

Man kann ebenfalls beide Messungen gleichzeitig ausführen.

4.2.1.4 Beliebige Rotationen

In der Euler-Darstellung lässt sich jede beliebige Rotation durch drei einzelne Rotationen um Koordinatenachsen darstellen:

$$U = U_z(\gamma) U_x(\beta) U_z(\alpha).$$

Um eine allgemeine Rotation zu erhalten, liegt es also nahe drei Messungen der obigen Art durchzuführen:

$$X^{m_3} H U_z(\Phi_3) \, X^{m_2} H U_z(\Phi_2) \, X^{m_1} H U_z(\Phi_1).$$

Mit den Identitäten $XH = HZ$ und $HU_zH = U_x$ wird dies zu:

$$X^{m_3} H U_z(\Phi_3) \, X^{m_2} U_x(\Phi_2) \, Z^{m_1} U_z(\Phi_1).$$

Da $XU_z(\Phi) = U_z(-\Phi)X$ und $ZU_x(\Phi) = U_x(-\Phi)Z$ wird daraus weiter:

$$X^{m_3} Z^{m_2} X^{m_1} H U_z(-1^{m_2}\Phi_3) U_x(-1^{m_1}\Phi_2) U_z(\Phi_1).$$

Wählt man die Winkel folgendermaßen:

$$\begin{aligned} \Phi_1 &= \alpha, \\ \Phi_2 &= -1^{m_1}\beta, \\ \Phi_3 &= -1^{m_2}\gamma, \end{aligned}$$

hat man also die Rotation U realisiert:

$$X^{m_3} Z^{m_2} X^{m_1} H U.$$

Den Hadamard-Operator kann man wieder durch eine weitere vorgeschaltete Messung zur Eigenbasis von X (Unterabschnitt 4.2.1.1) eliminieren.

Man beachte, dass Messungen von den Ergebnissen vorheriger Messungen abhängen. Man kann also nicht alle Messungen gleichzeitig durchführen.

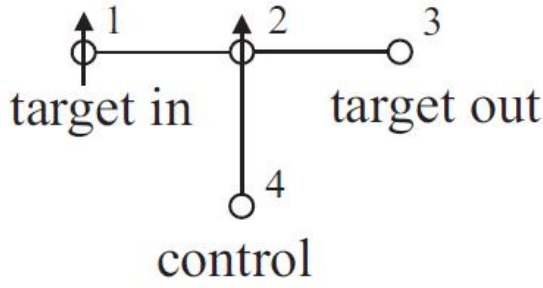

Abbildung 4.3: Implementierung eines CNOT Gatters durch Messungen am Cluster-State

4.2.1.5 Zwei Qubit-Operatoren

Um Zweiqubit-Operatoren in einem One-Way-Quantum-Computer zu implementieren, stellt man zunächst fest, das eine zwei-Qubit-Operator auf natürliche Weise in dem Cluster-State implementiert ist, nämlich der Controlled-Z-Operator, mit der der Cluster-State initialisiert wird. Bringt man also zwei Zustände auf Qubits die in dem Cluster-State verbunden sind, ist auf ihnen durch die Initialisierung der CZ-Operator bereits ausgeführt [9].

Um ein CNOT-Gatter zu implementieren, kann man eine Anordnung wie in Abbildung 4.3 benutzen. Mit den senkrechten Pfeilen sind dabei Messungen zur Eigenbasis von X gemeint. Aus den Eigenwertgleichungen 4.1 des Cluster-States kann man schließen, dass so tatsächlich ein CNOT Gatter realisiert wird [31]. Anschaulich betrachtet, ist die Verschränkung zwischen Qubit zwei und vier einen Controlled-Z-Operator und die Messungen an den Qubits eins und zwei führen zur Anwendung von Hadamard-Operatoren am Zielqubit (Unterabschnitt 4.2.1.1).

$$
\begin{aligned}
& (I \otimes H) \cdot CZ \cdot (I \otimes H) \\
= \; & \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \\
= \; & \frac{1}{2} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \\
= \; & \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 2 & 0 \end{pmatrix} = CNOT
\end{aligned}
$$

Da die Messungen nicht voneinander abhängen, können sie gleichzeitig durchgeführt werden. Sie erzeugen wieder Seiteneffektoperatoren in Form eines X bzw. Z Operators in

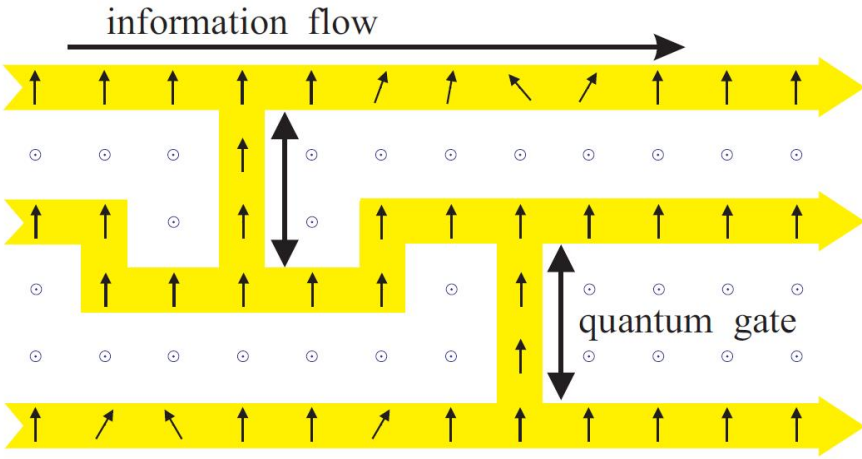

Abbildung 4.4: Simulation eines Quantenschaltkreises auf einem Cluster-State

Abhängigkeit von den Messergebnissen [31].

4.3 Äquivalenz von One-Way-Quantum-Computer und Quantenschaltkreis

Um zu zeigen, dass 1WCQ und Quantenschaltkreis äquivalent sind zeigen wir, dass beide Modelle in der Lage sind, das jeweils andere Modell effizient zu simulieren. Vergleiche dazu [20].

4.3.1 Quantenschaltkreis $\leq_p$ One-Way-Quantum-Computer

Bekanntermaßen sind beliebige ein Bit-Operatoren und das CNOT-Gatter universell [3]. Um einen beliebigen Quantenschaltkreis mit einem One-Way-Quantum-Computer zu simulieren geht man folgendermaßen vor:

- Initialisiere einen Cluster-State (Unterabschnitt 4.1).
- Plane den Quantenschaltkreis so, dass er nur aus beliebigen ein-Qubit-Gattern und CNOT-Gattern besteht.
- Übertrage den Quantenschaltkreis auf dem Cluster-State, in dem man (vergleiche Abbildung 4.4):
  - Die Eingabequbits durch Rotationen des Zustands $|+\rangle$ mittels vier aufeinanderfolgender Messungen wie in Unterabschnitt 4.2.1.4 auf den Cluster schreibt.
  - Leitungen durch Messungen zur Eigenbasis von X (Unterabschnitt 4.2.1.2) darstellt.

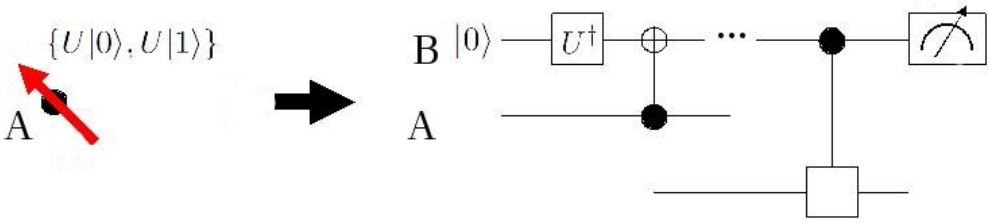

Abbildung 4.5: Simulation eines One-Way-Quantum-Computers mit einem Quantenschaltkreis

  - Ein-Qubit-Operatoren durch vier aufeinanderfolgende Messungen wie in Unterabschnitt 4.2.1.4 darstellt.
  - CNOT-Gatter durch Messungen wie in Abschnitt 4.2.1.5 darstellt.
  - Nicht benötigte Qubits durch Messungen zur Eigenbasis von Z aus dem Cluster entfernt.
  - Das Ergebnis durch Messungen zur Eigenbasis von Z ausliest. Dabei ist zu beachten, dass wenn als Seiteneffektoperator der X-Operator auf dem Ergebnis angewendet ist, das Ergebnis nachträglich invertiert werden muss. (Der Seiteneffekt-Z-Operator kommutiert mit der Messung und kann ignoriert werden.)

- Alle Messungen, die nicht von dem Ergebnis anderer Messungen abhängen können am Anfang gleichzeitig durchgeführt werden (dazu gehören auch die Messungen der Ausgabequbits). Alle Messungen, die von vorherigen Messungen abhängen führt man dann sukzessive durch.

Da für jeden Quantenbausteine nur eine konstante Anzahl von Messungen nötig ist, ist diese Simulation effizient.

4.3.2 One-Way-Quantum-Computer $\leq_p$ Quantenschaltkreis

Auf der anderen Seite ist es möglich, einen One-Way-Quantum-Computer mit einem Quantenschaltkreis zu simulieren. Dazu sieht man zunächst, dass es möglich ist einen Quantenschaltkreis (der nur Messungen am Ende und zur Eigenbasis von Z zulässt) so zu verallgemeinern, dass Messungen zu jeder Zeit und zur jeder Basis möglich sind und nachfolgende Gatter von dem Ergebnis dieser Messung abhängig sind.

Wenn A ein Qubit ist an dem man eine Messung zur Basis $\{U|0\rangle, U|1\rangle\}$ durchführen möchte, führt man dazu ein zusätzliches Qubit B ein und initialisiert es im Zustand $|0\rangle$. Die Messung wird dann durch folgenden Schaltkreis ersetzt: Zunächst wird $U^\dagger$ auf B angewendet und dann CNOT auf AB. Alle weiteren von der Messung abhängigen Gatter werden durch entsprechende von B kontrollierte Bausteine ersetzt (Abbildung 4.5) . Die Wirkung der Messung von A wird so durch die Messung von B (bezüglich Z) am Ende simuliert.

Mit diesem verallgemeinerten Quantenschaltkreis kann man einen One-Way-Quantum-Computer einfach simulieren. Dazu:

- Initialisiert man einen Cluster-State, in dem man wie in Abschnitt 4.1 CZ-Gatter auf die Zustände $|+\rangle = H|0\rangle$ anwendet.
- Fügt für jede 1-Qubit 1-WQC Messung ein weiteres Qubit ein.
- Simuliert die Messungsfolge des 1-WQC durch kontrollierte Bausteine wie oben.
- Alle Qubits zur Eigenbasis von Z misst und das Ergebnis ausgibt.

Da für jede 1-WQC Messung nur ein zusätzliches Qubit und eine höchstens lineare Anzahl von Gattern benötigt wird, ist die Simulation effizient.

Quantenschaltkreise und One-Way-Quantum-Computer sind also tatsächlich im Sinne der polynomiellen Reduzierbarkeit äquivalent.

5 One-Way-Quantum-Computer und Parallelisierbarkeit

Da beim One-Way-Quantum-Computer Messungen immer an unterschiedlichen Qubits durchgeführt werden, kommutieren sie alle als Quantenoperatoren und man könnte sie alle gleichzeit ausführen, wenn die Wahl einiger Messungsbasen nicht von den Messergebnissen vorheriger Messungen abhängen würde. Es stellt sich die Frage, was für Berechnungen parallel ausgeführt werden können, und was für Berechnung eine Abhängigkeit haben müssen. Dazu zwei Definitionen:

Definition 1 (Pauli-Gruppe)**.** Die Pauli-Gruppe $\mathcal{P}_n$ auf n Qubits ist die durch n-fache Tensorprodukte von

$$\pm I, \pm iI, X \text{ und } Z$$

erzeugte Gruppe.

Elemente der Pauli Gruppe finden wir offensichtlich als Seiteneffektoperatoren bei den Berechnungen eines One-Way-Quantum-Computers.

Definition 2 (Clifford-Operator)**.** Ein n-Qubit Operator C heißt Clifford-Operator, wenn es zu jedem $P \in \mathcal{P}_n$ ein $P' \in \mathcal{P}_n$ gibt, so dass

$$CP = P'C$$

gilt.

Die Anwendung für One-Way-Quantum-Computer ist offensichtlich. Führen wir eine Folge C_i von Clifford-Operatoren auf einem Zustand $|\psi\rangle$ auf einem One-Way-Quantum-Computer aus und sind P_i die dazugehörigen (von den Messergebnissen abhängigen) auftretenden Seiteneffektoperatoren, dann gibt es einen (ebenfalls von den Messergebnissen abhängigen) Operatoren $P' \in \mathcal{P}_n$, so dass für den resultierenden Zustand gilt:

$$P_k C_k ... P_2 C_2 P_1 C_1 |\psi\rangle = P' C_k ... C_1 |\psi\rangle.$$

Wir können also eine Folge von Clifford-Operatoren auf einem One-Way-Quantum-Computer immer mit einer einzigen parallelen Messung durchführen. Lediglich die Interpretation der Messergebnisse in den Seiteneffektoperatoren muss man gegebenenfalls anpassen.

Wir haben dieses Verfahren bereits in Unterabschnitt 4.2.1 an dem Hadamard-Operator H angewendet und dabei die Eigenschaften

$$HX = ZH \text{ und } HZ = XH$$

genutzt. Der $P_{\frac{\pi}{2}}$ Operator ist ebenfalls ein Clifford-Operator:

$$P_{\frac{\pi}{2}} Z = Z P_{\frac{\pi}{2}} \text{ und } P_{\frac{\pi}{2}} X = (iXZ) P_{\frac{\pi}{2}}.$$

Für den zwei-Qubit-Operator CZ gelten die folgenden Relationen:

$$CZ(Z \otimes I) = (Z \otimes I)CZ \text{ und } CZ(X \otimes I) = (X \otimes Z)CZ.$$

Analog gilt dies für das zweite Qubit, da CZ symmetrisch ist.

Hierraus und aus der Darstellung von $CNOT$ durch den CZ-Operator und H-Operatoren aus Unterabschnitt 4.2.1.5 folgt, dass auch $CNOT$ ein Clifford-Operator ist. Es gilt sogar:

Theorem 3. *Die Menge der Clifford-Operatoren ist die durch* $\{CNOT, H, P_{\frac{\pi}{2}}\}$ *auf allen Qubits erzeugte Gruppe.*

Zum Beweis siehe [15]. Die Clifford-Gruppe spielt auch z.B. in der Quanten-Fehlerkorrektur eine wichtige Rolle.

Leider ist die Clifford-Gruppe wahrscheinlich nicht universell. Es gilt sogar:

Theorem 4 (Knill-Gottesman)**.** *Quantenschaltkreise aus Clifford-Operatoren können klassisch effizient simuliert werden.*

Siehe dazu [29]. Es ist weiter bekannt, dass es zu jedem Clifford-Operator auf n Qubits einen Quantenschaltkreis der Tiefe $O(\log n)$ gibt. Die Komplexität kann durch die 1-WQC also immerhin von logarithmische auf konstante Tiefe reduziert werden.

Ein weiterer Aspekt des 1-WQC ist die Verknüpfung von Quantenberechnungen mit klassischen Berechnungen. Obwohl es 1-WQC erlauben unter Umständen eine große Zahl von Messungen parallel auszuführen, kommt man nicht umhin, die Messergebnisse vor der nächsten Messung (klassisch) auszuwerten. Genauer geschieht dies durch Berechnung der Summe modulo zwei von gemessenen Bits. Diese Berechnung lässt sich ebenfalls parallelisieren, in dem man zunächst die Summen $i_1 \oplus i_2, i_3 \oplus i_4, ...$ berechnet und im nächsten Schritt dann Paare der Ergebnisse addiert, usw. Man hat also einen klassischen Aufwand logarithmischer Tiefe für jede Schicht aus Clifford-Operatoren. Wir haben die logarithmische Tiefe eines Quantenschaltkreises also in eine klassische Berechnung logarithmischer Tiefe und einen Quantenanteil konstanter Tiefe umgewandelt. Diese Beobachtung lässt vermuten, dass der quantenmechanische „Anteil“ den man benötigt, um die Möglichkeiten eines Quantenrechner voll zu nutzen nicht sehr groß ist.

Conjecture 5. *Jeder polynomielle Quantenalgorithmus kann mit* $O(\log n)$ *Quantenschichten, ergänzt durch polynomielle klassische Berechnungen implementiert werden.*

Obwohl diese Vermutung nicht bewiesen ist, ist zumindest bekannt, dass sie für den Algorithmus von Shore gilt [11].

6 Implementierung

In diesem Kapitel werden Möglichkeiten der Implementierung des One-Way-Quantum-Computer-Modells am Beispiel des optischen Gitters und der Realisierung durch Photonen diskutiert. Weitere Ansätze nutzen sowohl Photonen als auch Materie [4], oder implementieren One-Way-Quantum-Computer in Festkörpern, z.B. in Halb- und Supraleitern [34] oder Quantum-Dots [37].

6.1 Optische Gitter

Durch überlappende Laserfelder wird ein periodisches Potential erzeugt, dessen Minima ein Gitter formen, in dem einzeln kalte, neutrale Atome gefangen werden können. Die Quanteninformation ist in den Zuständen der Atome gespeichert [7]. Siehe Abbildung 6.1. Durch Modulation der Laserfelder lassen sich benachbarte Minima näher zusammen bringen und die Wechselwirkung der Atome mit dem Feld führt zu einer relativen Phase. Steuert man diesen Prozess so, dass diese Phase gleich -1 ist, implementiert er einen CZ-Operator [19]. Da die Modulation auf alle Atome gleichzeitig wirkt, lässt sich ein Cluster-State also simultan im ganzen Gitter herstellen.

Auf der anderen Seite erschwert die Nähe der Atome zueinander (in der Größenordnung der Wellenlänge des Laserfeldes) das Adressieren und Messen der einzelnen Atome. Ansätze die Auflösung zu erhöhen [10], oder weniger dichte optische Gitter zu erzeugen [26] sind jedoch Erfolgversprechend.

6.2 Photonen

Bei dem Versuch Quanteninformationen in den Freiheitsgraden von Photonen zu kodieren stößt man heutzutage auf zwei wesentliche Probleme: Zunächst die zuverlässige Erzeugung und Detektierung einzelner Photonen und die Tatsache, dass sich deterministische zwei-Qubit-Operatoren nicht alleine mit linearen optischen Mitteln realisieren lassen. Um letzteres Problem zu lösen sind nichtlineare Elemente Vorgeschlagen worden [2], aber auch die Erzeugung nichtdeterministischer Gatter durch die Einfügung von messenden Bausteinen [22]. Je nach Ergebnis der Messung führen diese nichtdeterministischen Gatter entweder die Transformation aus, oder versagen. Ein Versagen führt seinerseits zu einer Messung des Quantenzustandes, unterbricht also die Berechnung. Diese Verhalten stellt die Skalierbarkeit des Verfahrens in Frage. Mit Mitteln der Quantenfehlerkorrektur sind zuverlässige und skalierbare lineare optische Quantenrechner jedoch möglich.

One-Way-Quantum-Computer bieten eine andere Möglichkeit dieses Problem zu umgehen. Nutzt man nichtdeterministische CZ-Operatoren um einen Cluster-State herzu-

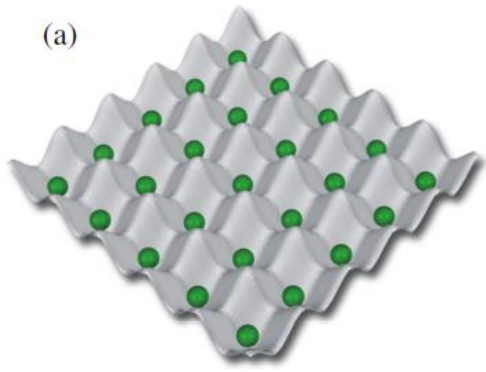

Abbildung 6.1: Optisches Gitter

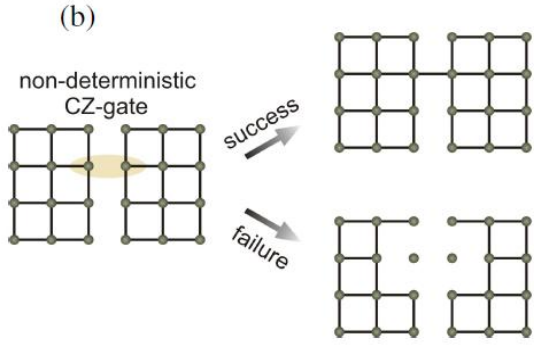

Abbildung 6.2: Erzeugung eines Cluster-States mit nichtdeterministische CZ-Gattern

stellen, führt ein Versagen zwar dazu, dass die Qubits aus dem Cluster entfernt werden, verliert aber den Cluster-State der anderen Qubits nicht. Man kann den Vorgang also widerholen, oder den übrig gebliebenen Cluster-State für Berechnungen verwenden (Abbildung 6.2). Man kann also zunächst einen Cluster-State in einem statistischen Prozess erzeugen und die (deterministischen) Berechnungen dann auf dem resultierenden Cluster-State planen [21].

A Gliederung des Vortrags

Die Gliederung des Vortrags orientiert sich an der Gliederung dieses Dokuments. Die Angaben zur Folienanzahl sind Anhalte.

- Begrüßungsfolie (eine Folie)
- Übersicht (eine Folie)
- Motivation (zwei Folien)
- Teleportation-Quantum-Computation (zwei-drei Folien)
- One-Way-Quantum-Computer
  - Der Cluster State (zwei Folien)
  - Berechnung durch Messung (vier Folien)
  - Äquivalenz 1WCQ/Gatter (zwei-drei Folien)
- 1-WQC und Parallelisierbarkeit (zwei-drei Folien)
- Implementierung (zwei-drei Folien)
- Zusammenfassung (eine Folie)

Der Vortrag hat also ca. 20 inhaltliche Folien. Bei zwei Minuten pro Folie also eine Länge von ca. 40 Minuten.

Literaturverzeichnis

[1] D. Aharonov and M. Ben-Or. Polynomial simulations of decohered quantum computers. *Foundations of Computer Science, Annual IEEE Symposium on*, 0:46, 1996.

[2] Hiroo Azuma. Quantum computation with kerr-nonlinear photonic crystals. *Journal of Physics D: Applied Physics*, 41(2):025102 (10pp), 2008.

[3] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A*, 52(5):3457–3467, Nov 1995.

[4] Sean D. Barrett and Pieter Kok. Efficient high-fidelity quantum computation using matter qubits and linear optics. *Physical Review A*, 71(6):060310+, Jun 2005.

[5] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70(13):1895–1899, Mar 1993.

[6] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. In *STOC '93: Proceedings of the twenty-fifth annual ACM symposium on Theory of computing*, pages 11–20, New York, NY, USA, 1993. ACM.

[7] Immanuel Bloch. Ultracold quantum gases in optical lattices. *Nature*, 2005.

[8] Hans J. Briegel and Robert Raussendorf. Persistent entanglement in arrays of interacting particles, 2000.

[9] Dan E. Browne and Hans J. Briegel. One-way quantum computation - a tutorial introduction, 2006.

[10] Jaeyoon Cho. Addressing individual atoms in optical lattices with standing-wave driving fields. *Physical Review Letters*, 99(2):020502, 2007.

[11] Richard Cleve and John Watrous. Fast parallel circuits for the quantum fourier transform, 2000.

[12] Stephen A. Cook. The complexity of theorem-proving procedures. In *STOC '71: Proceedings of the third annual ACM symposium on Theory of computing*, pages 151–158, New York, NY, USA, 1971. ACM.

[13] D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*, 400(1818):97–117, 1985.

[14] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, Joshua Lapan, Andrew Lundgren, and Daniel Preda. A Quantum Adiabatic Evolution Algorithm Applied to Random Instances of an NP-Complete Problem. *Science*, 292(5516):472–475, 2001.

[15] Daniel Gottesman. Stabilizer codes and quantum error correction, 1997.

[16] Daniel Gottesman and Isaac L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, (402):390–393, 1999.

[17] Daniel Gottesman and Isaac L. Chuang. Quantum teleportation is a universal computational primitive. *Nature*, 402:390, 1999.

[18] J.L. Hennessy and D. Patterson. *Computer Architecture: A Quantitative Approach*. Morgan Kaufmann, 2003.

[19] D. Jaksch, H.-J. Briegel, J. I. Cirac, C. W. Gardiner, and P. Zoller. Entanglement of atoms via cold controlled collisions. *Phys. Rev. Lett.*, 82(9):1975–1978, Mar 1999.

[20] Richard Jozsa. An introduction to measurement based quantum computation, 2005.

[21] K. Kieling, T. Rudolph, and J. Eisert. Percolation, renormalization, and quantum computing with non-deterministic gates. *Physical Review Letters*, 99:130501, 2007.

[22] E. Knill. A scheme for efficient quantum computation with linear optics. *Nature*, 2001.

[23] D. W. Leung. Two-qubit projective measurements are universal for quantum computation, 2001.

[24] Debbie W. Leung. Quantum computation by measurements. *IJQI*, 2:33, 2004.

[25] Olaf Mandel, Markus Greiner, Artur Widera, Tim Rom, Theodor W. Haensch, and Immanuel Bloch. Controlled collisions for multiparticle entanglement of optically trapped atoms, 2003.

[26] Karl D. Nelson, Xiao Li, and David S. Weiss. Imaging single atoms in a three-dimensional array. *Nature Physics*, 2007.

[27] Michael A. Nielsen. Universal quantum computation using only projective measurement, quantum memory, and preparation of the 0 state, 2001.

[28] Michael A. Nielsen. Optical quantum computation using cluster states, 2004.

[29] Michael A. Nielsen, Author, Isaac Chuang, Author, Lov K. Grover, and Reviewer. Quantum computation and quantum information. *American Journal of Physics*, 70(5):558–559, 2002.

[30] R. Raussendorf, D. E. Browne, and H. J. Briegel. Measurement-based quantum computation with cluster states. *Physical Review A*, 68:022312, 2003.

[31] Robert Raussendorf and Hans J. Briegel. Quantum computing via measurements only, 2000.

[32] Martin Sauerhoff. Quantenrechner: Algorithmen und komplexität. Vorlesungsskript, TU Dortmund, 2003.

[33] Johannes Siedersleben. *Softwaretechnik: Praxiswissen für Softwareingenieure*. Hanser Fachbuchverlag, 2002.

[34] Tetsufumi Tanamoto, Yu xi Liu, Shinobu Fujita, Xuedong Hu, and Franco Nori. Producing cluster states in charge qubits and flux qubits. *Physical Review Letters*, 97(23):230501, 2006.

[35] A. M. Turing. On computable numbers, with an application to the entscheidungsproblem. *Proc. London Math. Soc.*, 2(42):230–265, 1936.

[36] Ingo Wegener. *Komplexitätstheorie*. Springer, 2003.

[37] Yaakov S. Weinstein, C. Stephen Hellberg, and Jeremy Levy. Quantum-dot cluster-state computing with encoded qubits. *Phys. Rev. A*, 72(2):020304, Aug 2005.