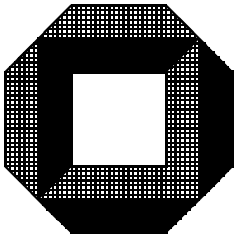
Seminar

Mit Quanten Rechnen



Universität Karlsruhe (TH)
Fakultät für Informatik
Institut für Algorithmen und Kognitive Systeme

Prof. Dr. Th. Beth,
Dipl.–Inform. Th. Decker,
Dipl.–Inform. Med. B. Schnepf,
Dr. F. Schmüser,
Dr. P. Wocjan,
Dipl.–Inform. R. Zeier

Sommersemester 2004

Inhaltsverzeichnis

Vortrag 1

Quantenschaltkreismodell

Marek W. Doniec

1.1 Einleitung

Während man in der Theorie der Quantenmechanik beliebig viele Qubits durch 2^n-dimensionale unitäre Transformationen alle auf einmal manipulieren kann, gestatten es die bisher bekannten praktischen Anwendungen nicht, mehr als 2 oder 3 Qubits gleichzeitig zu kontrollieren, d.h. ihren Zustand in Abhängigkeit voneinander zu verändern. Da für eine sinnvolle Berechnung jedoch Operationen mit wesentlich mehr Qubits nötig sind, wird ein Vorgehen benötigt, nach dem sich jede solche 2^n-dimensionale unitäre Transformationen auf elementare Transformationen zurückführen lässt. Als elementare Transformationen werden hier die 1-Qubit Transformation sowie das kontrollierte nicht-Gatter gewählt, welches den Zustand $|x, y\rangle$ auf den Zustand $|x, x \oplus y\rangle$ transformiert [Bar95, Cyb01].

1.2 Grundlagen

Bevor hier auf die Reduktion beliebiger 2^n-dimensionaler unitärer Transformationen auf elementare Gatter eingegangen wird, hier zuerst einige grundlegende Tatsachen über Qubits und deren Zustände.

1.2.1 Die Schrödingergleichung und ihre Auswirkungen

Der zeitlich veränderliche Zustand eines Quantensystems wird durch die Schrödingergleichung

$$i\hbar\frac{\partial|\Psi(t)\rangle}{\partial t} = H|\Psi(t)\rangle \tag{1.1}$$

beschrieben [Cyb01]. Dabei beschreibt $|\Phi\rangle$ den Quantenzustand des Systems und H ist der Hamilton-Operator, der Hermitesch ist, also

$$H^\dagger = H. \tag{1.2}$$

Die Lösung dieser Differentialgleichung lautet

$$|\Psi(t)\rangle = e^{-iHt/\hbar}|\Psi(0)\rangle \tag{1.3}$$

wobei

$$U = e^{-iHt/\hbar} \tag{1.4}$$

die zeitliche Veränderung des Quantensystems beschreibt. Wie wir leicht sehen, ist U unitär:

$$U^\dagger = e^{iH^\dagger t/\hbar} = U^{-1}. \tag{1.5}$$

Daraus folgt, dass jede mögliche Zustandsänderung in unserem Quantenrechner eine unitäre Transformation im Hilbertraum ist.

1.2.2 Qubits und Quantenregister

Der Zustand eines *Qubits* wird durch einen Vektor im 2-dimensionalen *komplexen Hilbertraum* $\mathcal{H} = \mathbb{C}^2$ dargestellt. Dieser kann als *Ket-Vektor* $|x\rangle$ geschrieben werden. Wegen der einfachen Darstellung werden hier als Basisvektoren die klassischen Zustände $|0\rangle$ und $|1\rangle$ genommen. Der Zustand der Qubits $|\Phi\rangle$ stellt sich in dieser Basis wie folgt dar:

$$|\Phi\rangle = \alpha|0\rangle + \beta|1\rangle. \tag{1.6}$$

Dabei muss die Normierungsbedingung

$$|\alpha|^2 + |\beta|^2 = 1 \tag{1.7}$$

erfüllt sein und im Falle einer Messung erhalten wir mit einer Wahrscheinlichkeit von $|\alpha|^2$ den Wert $|0\rangle$ und mit einer Wahrscheinlichkeit von $|\beta|^2$ den Wert $|1\rangle$. Der Zustand eines Qubits kann ebenfalls als

$$|\Phi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{1.8}$$

geschrieben werden, wobei

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad , \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1.9}$$

gilt.
Ein *Quantenregister* besteht nun aus n Qubits. Es bildet einen 2^n-dimensionalen komplexen Hilbertraum $\mathcal{H}^n = \mathbb{C}^{2^n}$. Wählt man als Basis wieder die 2^n möglichen klassischen Zustände, so ist die Darstellung für $|\Phi\rangle \in \mathcal{H}^n$

$$|\Phi\rangle = \sum_{x=(x_{n-1},\, x_{n-2},\, \ldots, x_1,\; x_0) \in \{0,\,1\}^n} \alpha_x |x_{n-1},\, x_{n-2},\, \ldots, x_0\rangle \tag{1.10}$$

wobei wieder die Normierungsbedingung

$$\sum_{x \in \{0,\,1\}^n} |\alpha_x|^2 = 1 \tag{1.11}$$

erfüllt sein muss [Bar95, Cyb01]. Analog zum Qubit kann der Zustand x des Quantenregisters durch

$$|\Phi\rangle = \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{2^n-1} \end{pmatrix} \tag{1.12}$$

dargestellt werden, wobei der Index der α_i die durch den zugehörigen Basisvektor in Binärdarstellung gegebene Zahl ist. Also z.B. i = 5 für $|101\rangle$.
Während das klassische Register mit n klassischen Bits einen von 2^n möglichen Zuständen annimmt, so besteht der Zustand eines Quantenregisters mit n Qubits aus einer Überlagerung aller klassischer Zustände. Es können also unitäre Transformationen auf einem 2^n-dimensionalen Raum ausgeführt werden, exponentiell zur Anzahl der Qubits also [Cyb01].

1.2.3 Tensorprodukt

Der gemeinsame Zustand $|\Theta\rangle$ zweier Qubits $|\Phi\rangle, |\Psi\rangle \in \mathcal{H}$ wird dargestellt durch deren Tensorprodukt

$$|\Theta\rangle = |\Phi\rangle \otimes |\Psi\rangle. \tag{1.13}$$

Dieses kann wie folgt berechnet werden

$$\begin{pmatrix} \theta_0 \\ \theta_1 \\ \theta_2 \\ \theta_3 \end{pmatrix} = \begin{pmatrix} \phi_0 \\ \phi_1 \end{pmatrix} \otimes \begin{pmatrix} \psi_0 \\ \psi_1 \end{pmatrix} = \begin{pmatrix} \phi_0 \cdot \psi_0 \\ \phi_0 \cdot \psi_1 \\ \phi_1 \cdot \psi_0 \\ \phi_1 \cdot \psi_1 \end{pmatrix}. \tag{1.14}$$

Anzumerken ist jedoch, dass zwei Qubits auch einen gemeinsamen Zustand annehmen können, der sich nicht

mehr durch die Zustände der einzelnen Qubits darstellen lässt. Diese Zustände, die sich nicht als Tensorprodukt von zwei Qubits darstellen lassen, nennt man verschränkte Zustände [Mer04, Gra01]. Ein Beispiel für einen solchen verschränkten Zustand ist

$$|\Theta\rangle = \begin{pmatrix} \frac{\sqrt{2}}{2} \\ 0 \\ 0 \\ \frac{\sqrt{2}}{2} \end{pmatrix} \stackrel{!}{=} \begin{pmatrix} \phi_0 \cdot \psi_0 \\ \phi_0 \cdot \psi_1 \\ \phi_1 \cdot \psi_0 \\ \phi_1 \cdot \psi_1 \end{pmatrix}. \tag{1.15}$$

Da $\theta_1 = 0$ muss gelten $\phi_0 = 0 \vee \psi_1 = 0$. Damit wäre aber $\theta_0 = 0$ oder $\theta_3 = 0$, im Widerspruch zu Definition von $|\Theta\rangle$.
Entsprechendes gilt auch für ein ganzes Quantenregister $|\Phi\rangle \in \mathcal{H}^n$ aus n Qubits $|x_1\rangle, \ldots, |x_n\rangle$. Wenn sich jedes der Qubits in einem eigenem Zustand befindet, so ist der Zustand des gesamten Quantenregisters

$$|\Phi\rangle = |\phi_{n-1}\rangle \otimes |\phi_{n-2}\rangle \otimes \ldots \otimes |\phi_0\rangle. \tag{1.16}$$

Jedoch muss wieder der Zustand eines Quantenregisters nicht das Tensorprodukt von Zuständen einzelner Qubits sein [Mer04, Gra01]!
Seien nun A und B zwei 2-dimensionale unitäre Transformationen.

$$A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \quad , \quad B = \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} \tag{1.17}$$

Betrachtet man nun beide Qubits als Quantenregister, also Ihren gemeinsamen Zustand und wendet jeweils A auf Qubit 1 und B auf Qubit 0 an, so wird insgesamt eine 4-dimensionale unitäre Transformation Z ausgeführt. Diese lässt sich durch das Tensorprodukt von A und B darstellen:

$$Z = A \otimes B = \begin{pmatrix} a_{00} \cdot B & a_{01} \cdot B \\ a_{10} \cdot B & a_{11} \cdot B \end{pmatrix} = \begin{pmatrix} a_{00} \cdot b_{00} & a_{00} \cdot b_{01} & a_{01} \cdot b_{00} & a_{01} \cdot b_{01} \\ a_{00} \cdot b_{10} & a_{00} \cdot b_{11} & a_{01} \cdot b_{10} & a_{01} \cdot b_{11} \\ a_{10} \cdot b_{00} & a_{10} \cdot b_{01} & a_{11} \cdot b_{00} & a_{11} \cdot b_{01} \\ a_{10} \cdot b_{10} & a_{10} \cdot b_{11} & a_{11} \cdot b_{10} & a_{11} \cdot b_{11} \end{pmatrix}. \tag{1.18}$$

Werden, wie überall in diesem Vortrag, als Basis die klassisch möglichen Zustände mit n Bits gewählt, so ist die Darstellung der Transformation als Matrix recht verständlich, da man dort sieht, welche klassischen Zustände auf welche neuen abgebildet werden. Das soll an einem Beispiel klar gemacht werden. Seien

$$A = \begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{array} \quad \text{und} \quad B = \begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{array} \tag{1.19}$$

Die eingetragenen Basisvektoren sollen zeigen, wie die Matrix die entsprechenden Koeffizienten des Zustandsvektors der Qubits beeinflusst. A ist also die Identität und B die Negation. A wirke auf Qubit 1 und B auf Qubit 0. Die resultierende Transformation, die auf 2 Qubits wirkt, lautet dann

$$A \otimes B = \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array} \tag{1.20}$$

Auch hier lässt sich, analog zu (1.16), das Tensorprodukt auf größere unitäre Transformationen anwenden um diese durch eine gemeinsamme Matrix darzustellen. Seien z.B. U eine 2^n-dimensionale unitäre Transformation die auf dem Raum der ersten n Qubits operiert und V eine 2^m-dimensionale unitäre Transformation die auf dem Raum der letzten m Qubits operiert. Dann ist

$$T = V \otimes U \tag{1.21}$$

eine 2^{n+m}-dimensionale unitäre Transformation[1], die auf dem Raum aller $n+m$ Qubits operiert und denselben Effekt hat, wie wenn man vorher U und V einzeln ausgeführt hätte.

[1] Zu beachten ist, dass hier $T = V \otimes U$ und nicht, was falsch wäre, $T = U \otimes V$ steht. Dies liegt daran, dass U auf den ersten n Qubits und V auf die letzten m Qubits operiert!

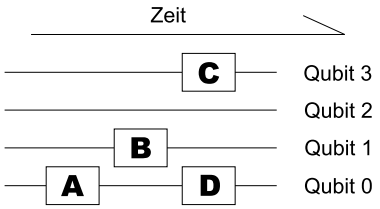


Abbildung 1.1: Darstellung von Quantenschaltkreisen. Auf Qubits 1 und 3 wird jeweils eine unitäre Transformation angewendet. Auf Qubit 0 wirken zwei unitäre Transformationen. Qubit 2 hingegen bleibt unverändert. Die resultierende Transformation über alle 4 Qubits lautet $T = C \otimes 1 \otimes B \otimes (D \cdot A)$ wobei 1 die Identität ist.

1.2.4 Darstellung von Quantenschaltkreisen

Bei der grafischen Darstellung von Transformation in Quantenschaltkreisen werden die betrachteten Qubits als horizontale Linien dargestellt. Qubit 0 ist dabei ganz unten, darüber Qubit 1 usw. . Ganz oben befindet sich schließlich das höchstwertige Qubit. Transformationen werden nun als Kästen auf die Linie des Qubits, auf welches sie wirken, gezeichnet. Dies ist in Abbildung 1.1 zu sehen. Dort wirkt z.B. Transformation B auf Qubit 1. Die Zeit wird auf der x-Achse dargestellt, das bedeutet Transformationen, die sich am weitesten links befinden, werden zuerst ausgeführt. So wird im Beispiel aus Abbildung 1.1 zuerst die Transformation A und dann D ausgeführt. Wenn $|x\rangle$ also der Anfangszustand von Qubit 0 ist, so wird dieser durch die Schaltung zu $D \cdot A \cdot |x\rangle$ geändert[2]. Die Darstellung von weiteren Transformationen wird erst in den folgenden Abschnitten erklärt, wenn diese Transformationen auch tatsächlich gebraucht werden.

1.3 Die Reduktion

Sei U eine 2^n-dimensionale unitäre Transformation, die ein Quantencomputerprogramm darstellt. Diese Transformation kann, solange sie die Unitaritätsbedingung erfüllt, alle n Qubits miteinander wechselwirken lassen. Um sie, wenigstens theoretisch[3], implementieren zu können, bedarf es daher einer geschickten Zerlegung in *Elementaroperationen*. Diese Elementaroperationen sind die *allgemeine 1-Qubit-Transformation*

$$U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad , \quad U^\dagger = U^{-1} \tag{1.22}$$

und das *1-Qubit-kontrollierte Nicht-Quantengatter*

$$X_c = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{1.23}$$

Erstere sind alle unitären Transformationen, die auf ein einziges Qubits wirken. Zweiteres ist ein auf zwei Qubits wirkendes Quantengatter, welches, klassisch betrachtet, Qubit 0 negiert genau dann wenn Qubit 1 gesetzt ist. Die Darstellung für ein 1-Qubit-kontrolliertes V-Gatter ist in Abbildung 1.2 zu sehen. Dieses ist allerdings nur für $V = X$ das 1-Qubit-kontrollierte Nicht-Gatter, wobei

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{1.24}$$

[2]Für die Transformationen A und B aus dem Beispiel hat die Reihenfolge allerdings keine Bedeutung, da diese auf verschiedene Qubits wirken und vollkommen unabhängig voneinander sind. Das heißt, dass die Ergebnisse der einen Transformation nicht für die andere verwendet werden.

[3]Der heutige Stand der Technik erlaubt zwar eine stabile Realisierung von Quantengattern, die zwei Qubits miteinander wechselwirken lassen, jedoch ist man momentan nicht in der Lage, mehrere solcher Quantengatter auf einmal zu realisieren und hintereinander auszuführen. Somit ist die Realisierung von Quantenrechnern durch die hier beschriebene Reduktion momentan eher von theoretischer Bedeutung.

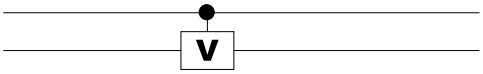


Abbildung 1.2: 1-Qubit-kontrollierte V-Gatter

1.3.1 QR-Zerlegung

Die QR-Zerlegung stammt aus der *linearen Algebra*. Sie erlaubt es, die 2^n-dimensionale unitäre Transformation U in 2^n-dimensionale unitäre Transformationen $G_1, G_2, \ldots$ und eine diagonale unitäre Transformation D zu zerlegen [Gol96]. Diese neuen Transformationen $G_1, G_2, \ldots$ haben den Vorteil, dass jede von Ihnen nur auf einer 2-dimensionalen Ebene operiert. Sie werden von nun an *G-Matrizen* genannt. Bei der Transformation D hingegen handelt es sich um eine diagonalisierte unitäre Transformation, d.h. sie ändert nur die Phase der einzelnen Zustände. D kann daher als Tensorprodukt von auf einzelne Qubits wirkenden Elementaroperationen dargestellt werden.
Die Zerlegung soll hier zuerst an einem Beispiel gezeigt werden. Sei $n = 2$, U also 4-dimensional. Damit sind auch die G-Matrizen 4-dimensional. U sowie die G-Matrizen werden also durch 4×4 Matrizen repräsentiert. Ziel ist es, U in eine obere Dreiecksmatrix D zu überführen. Diese ist unitär, da U und die G-Matrizen unitär sind, und somit sind nur die Einträge auf der Diagonalen ungleich Null. Dies geschieht, indem durch jede Multiplikation mit einer G-Matrix eine weitere Null eingefügt wird. In der folgenden Notation bedeutet $\xrightarrow{i,j}$, dass die neue hinzukommende G-Matrix in der x-ten und y-ten Koordinate operiert.

$$U = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{pmatrix} \xrightarrow{3,4} G_1U = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ 0 & * & * & * \end{pmatrix} \xrightarrow{2,3} G_2G_1U = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \end{pmatrix} \tag{1.25}$$

$$\xrightarrow{3,4} G_3G_2G_1U = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \end{pmatrix} \xrightarrow{1,2} G_4G_3G_2G_1U = \begin{pmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \end{pmatrix}$$

$$\xrightarrow{2,3} G_5G_4G_3G_2G_1U = \begin{pmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & * & * \end{pmatrix} \xrightarrow{1,2} G_6G_5G_4G_3G_2G_1U = \begin{pmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \end{pmatrix} \tag{1.26}$$

Wir erzeugen also entlang der Diagonalen in der Matrix ($\searrow$), von links unten angefangen, Nullen. Dabei bewegen wir uns, wenn eine Diagonale vollständig mit Nullen gefüllt ist, eine weiter nach rechts oben ($\nearrow$). Dort fängt die Prozedur wieder ganz links auf der Diagonalen an. Das Verfahren ist fertig, wenn die resultierende Matrix D eine obere Dreiecksmatrix ist. Wie also hat eine G-Matrix auszusehen? Betrachten wir als Beispiel G_1 aus 1.25. Ziel von G_1 ist es, Eintrag u_{41} von U zu Null werden zu lassen. G_1 muss jedoch unitär sein, so dass das resultierende Produkt ebenfalls unitär ist. Bei der QR-Zerlegung werden die G-Matrizen daher so gewählt, dass sie jeweils den betrachteten Eintrag (hier u_{41}) und den darüber (hier u_{31}) transformieren und dabei die gewünschte Null erzeugen. Im Fall von G_1 und U wird also folgende Änderung gewünscht:

$$\begin{pmatrix} u_{31} \\ u_{41} \end{pmatrix} \longrightarrow \begin{pmatrix} \frac{1}{\sqrt{|u_{31}|^2+|u_{41}|^2}} \\ 0 \end{pmatrix}. \tag{1.27}$$

Das erreicht man mit

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \alpha & \beta \\ 0 & 0 & \gamma & \delta \end{pmatrix} \tag{1.28}$$

mit

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \frac{1}{\sqrt{|u_{31}|^2 + |u_{41}|^2}} \begin{pmatrix} \overline{u_{31}} & \overline{u_{41}} \\ u_{41} & -u_{31} \end{pmatrix}. \tag{1.29}$$

Die Matrix 1.29 wir im folgenden *Drehkästchen* genannt. Generell sieht also das Schema für die G-Matrizen wie folgt aus: Wir betrachten die Matrix V, die als Ergebnis bisheriger Multiplikationen mit G-Matrizen entstanden ist. Die nächste Null soll in Zeile i und Spalte j der Matrix V erzeugt werden. Dann leistet die Matrix

$$G_k = \begin{array}{c} \\ i \end{array} \overset{\overset{\qquad\qquad\qquad\qquad\qquad\quad i}{\qquad\qquad\qquad\qquad\qquad\quad}}{\begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & \alpha & \beta & & & & \\ & & & \gamma & \delta & & & & \\ & & & & & 1 & & & \\ & & & & & & \ddots & & \\ & & & & & & & 1 & \\ & & & & & & & & 1 \end{pmatrix}} \quad \text{mit} \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \frac{1}{\sqrt{|u_{(i-1)j}|^2 + |u_{ij}|^2}} \begin{pmatrix} \overline{u_{(i-1)j}} & \overline{u_{ij}} \\ u_{ij} & -u_{(i-1)j} \end{pmatrix} \tag{1.30}$$

das Gewünschte, wobei alle nicht erwähnten Einträge gleich Null sind [Cyb01]. i und j hängen vom Index k und sind durch die im Verfahren beschriebene Reihenfolge zur Nullenerzeugung festgelegt.
Sei M die Anzahl der benötigten G-Matrizen, die höchstens $\frac{n^2-n}{2}$ beträgt, wobei n die Spalten- / Zeilenanzahl der Matrix ist. M kann jedoch auch kleiner ausfallen, falls es schon vorher günstig plazierte Nullen in der Matrix U gab, oder falls bei Anwendung einer G-Matrix mehrere neue Nullen entstehen. Nach der QR-Zerlegung gilt also

$$\left(\prod_{k=1}^{M} G_k \right) \cdot U = D \tag{1.31}$$

was gleichwertig ist mit

$$U = \left(\prod_{k=1}^{M} G_k \right)^{-1} \cdot D. \tag{1.32}$$

Da die G_k jedoch alle unitär sind, gilt immer, dass auch die Inverse $G_k^{-1} = G_k^\dagger$ in einer 2-dimensionalen Ebene operiert:

$$G_k^\dagger = \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & \alpha & \beta & & & & \\ & & & \gamma & \delta & & & & \\ & & & & & 1 & & & \\ & & & & & & \ddots & & \\ & & & & & & & 1 & \\ & & & & & & & & 1 \end{pmatrix}^\dagger = \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & \overline{\alpha} & \overline{\gamma} & & & & \\ & & & \overline{\beta} & \overline{\delta} & & & & \\ & & & & & 1 & & & \\ & & & & & & \ddots & & \\ & & & & & & & 1 & \\ & & & & & & & & 1 \end{pmatrix}. \tag{1.33}$$

Es bleibt also noch zu zeigen, wie man die $G_k^\dagger$ durch Elementaroperationen darstellen kann. Dann nämlich liefert (1.32) eine Konstruktion von U aus Elementaroperationen.

1.3.2 Realisierung der G-Matrizen

Bei der Konstruktion der $G_{i,j}^\dagger$ stellt sich folgendes Problem. Wir wissen aus 1.2.3, wie sich eine Transformation erstellen lässt, die auf ein Qubit wirkt und die anderen unberührt lässt. Diese ändern also zwei Komponenten des Zustandsvektors. Die zugehörigen Basisvektoren unterscheiden sich also nur in einem Qubit, nämlich dem, das geändert wird. Für die $G_{i,j}^\dagger$ brauchen wir jedoch eine Transformation, die zwar nur zwei Komponenten des Zustandsvektors ändert, diese müssen sich jedoch nicht zwingend zu Basisvektoren gehören, die sich nur in einem Qubit unterscheiden. So kann, beispielsweise für den Fall einer 4-dimensionalen Transformation das

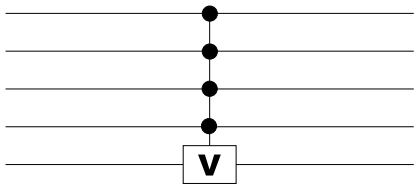


Abbildung 1.3: 4-Qubit-kontrolliertes V-Gatter.

Drehkästchen wie folgt liegen

$$A = \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \alpha & \beta & 0 \\ 0 & \gamma & \delta & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}. \tag{1.34}$$

Wie leicht zu sehen ist, werden die Koeffizienten, die zu den Basisvektoren $|01\rangle$ und $|10\rangle$ gehören, verändert. Eine solche Transformation lässt sich also nicht einfach als Tensorprodukt wie in (1.18) schreiben. Stattdessen wird sie mit Hilfe von *k-Qubit-kontrollierten Gattern* durchgeführt. Ein solches k-Qubit-kontrolliertes Gatter operiert auf $k+1$ Qubits. Während eines der Qubits, sei es o.B.d.A. Qubit 0, das sogenannte *Zielqubit* ist, funktionieren alle anderen k Qubits als Kontrollqubits. Klassisch betrachtet wird auf dem Zielqubit 0 eine Transformation V ausgeführt genau dann, wenn alle Kontrollqubits gleich 1 sind. Die Transformationsmatrix für ein k-Qubit-kontrolliertes Gatter mit Qubits 0 als Zielqubit sieht also wie folgt aus:

$$\begin{array}{c} \\ |0\ldots00\rangle \\ \vdots \\ \vdots \\ |1\ldots10\rangle \\ |1\ldots11\rangle \end{array} \begin{array}{c} \begin{array}{ccccccc} |0\ldots00\rangle & \ldots & \ldots & |1\ldots10\rangle & |1\ldots11\rangle \end{array} \\ \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \alpha & & \beta & \\ & & & \gamma & & \delta & \end{pmatrix} \end{array} \quad \text{mit} \quad V = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{1.35}$$

In Abbildung 1.3 ist das Schaltplansymbol für ein 4-Qubits-kontrolliertes V-Gatter zu sehen.

Mit k-Qubits-kontrollierten Gattern sind wir nun in der Lage, die G-Matrizen zu realisieren.

Sei n die Anzahl der betrachteten Qubits und seien i und j die beiden betroffenen Basisvektoren. Das zu realisierende Drehkästchen der G-Matrix sei V. Da es sich bei i und j immer um zwei verschiedene Basisvektoren handelt (die G-Matrizen operieren ja in 2 Dimensionen) unterscheiden sich i und j in mindestens einem Qubit, welches von nun an das Qubit K genannt wird. Dieses Qubit K verwenden wir im folgenden zur Unterscheidung um welchen der beiden Zustände i und j es sich handelt. Man betrachte nun jeden der möglichen Basisvektoren, die von den n Qubits dargestellt werden können, einzeln. Nur für den Fall i und j soll die Transformation V angewendet werden. Dafür ist es sinnvoll, die Eingabe so zu permutieren, dass sich i und j nur noch in Qubit K unterscheiden. Dies kann erreicht werden, indem auf Qubits in denen sich i und j über K hinaus unterscheiden ein kontrolliertes Nicht-Gatter mit K als Kontrollqubit angewendet wird. Die Ausgabe wird jetzt noch an den Qubits, an denen sie bei Eingabe von i und j Null ist, abgesehen von Qubit K, negiert. Wir erhalten so eine Permutation der Basisvektoren, so dass genau bei Eingabe von i und j alle Qubits bis auf das K Qubit den Zustand $|1\rangle$ haben. Nun können wir also ein $n-1$-Qubits-kontrolliertes V-Gatter auf Qubit K anwenden. Anschließend sind noch alle Permutationen rückgängig zu machen, d.h. Alle Gatter, die vor dem V-Gatter angewendet wurden, müssen jetzt in umgekehrter Reihenfolge angewendet werden [Cyb01].

Zur Veranschaulichung des Verfahrens hier ein Beispiel: Sei $n = 6$ Qubits und seien $i = |100011\rangle$ und $j = |111000\rangle$. i und j unterscheiden sich unter anderem in Qubit 4, dies sei von nun an Qubit K. Weiter Qubits in denen sich i und j unterscheiden sind Qubit 0, Qubit 1 sowie Qubit 3. Die fertige Schaltung ist in Abbildung 1.4 zu sehen. Die ersten drei Gatter sorgen dafür, dass bei Eingabe von i oder j die Qubits den gleichen Zustand haben (abgesehen von Qubit K). Dieser ist in diesem Beispiel $|1k0011\rangle$. Die Qubits, die hier noch den Zustand $|0\rangle$ haben, werden jetzt noch negiert (die zwei Nicht-Gatter). Anschließend wird das 5-Qubit-kontrollierte V-Gatter ausgeführt und alle Permutationen rückgängig gemacht.

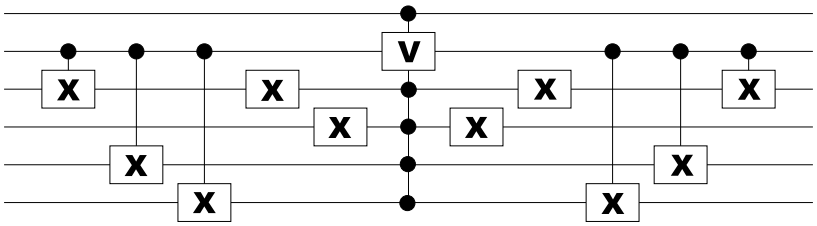


Abbildung 1.4: Realisierung der G-Matrix aus dem Beispiel.

Bis jetzt ist die unitäre Transformation U aus Abschnitt 1.3 bis auf k-Qubit-kontrollierte Gatter heruntergebrochen worden, welche weiter auf Elementaroperationen reduziert werden müssen.

1.3.3 Realisierung k-Qubit-kontrollierter V-Gatter

Bei der Realisierung von k-Qubit-kontrollierten V-Gattern nutzt man aus, dass V eine unitäre Transformation ist. Das bedeutet nämlich, dass es eine unitäre Transformation W gibt, so dass $W^2 = V$. Das Verfahren funktioniert nun im einzelnen so, dass ein k-Qubit-kontrolliertes V-Gatter durch mehrere maximal $k-1$-Qubit-kontrollierte Gatter realisiert wird.

Man betrachte beispielsweise das 4-Qubit-kontrollierte V-Gatter aus Abbildung 1.3 [4]. Mit $W^2 = V$ stellt die Anordnung aus Abbildung 1.5 exakt dieselbe Transformation dar. Dies kann schnell nachgerechnet werden; denn man muss nur 4 Fälle betrachten, da von den k Kontrollqubits die obersten $k-1$ als ein einziges betrachten werden können, welches genau dann gesetzt ist, wenn all diese Qubits gesetzt sind. Dies kann man sich an dem Schaltbild sehr gut verdeutlichen, denn die oberen $k-1$ Qubits dienen immer alle zusammen als Kontrollqubits.

Nun gibt es genau 4 Fälle die eintreten können (es werden hier nur die Kontrollqubits betrachtet):

$|x_k x_{k-1} \dots x_2 0\rangle$ **mit** $|x_k x_{k-1} \dots x_2\rangle \neq |1 \dots 1\rangle$**:** Da bei keinem Gatter alle Kontrollqubits gesetzt sind, wird keine Tranformation angewandt, der Zustand aller Qubits beleibt erhalten.

$|x_k x_{k-1} \dots x_2 1\rangle$ **mit** $|x_k x_{k-1} \dots x_2\rangle \neq |1 \dots 1\rangle$**:** Nur das linke kontrollierte W-Gatter und das kontrollierte $W^\dagger$-Gatter werden auf Qubit 0 angewandt. Diese Transformation enspricht aber genau der Identität $W^\dagger \cdot W = 1$. Damit bleibt auch in diesem Fall der Zustand aller Qubits am Ende unverändert.

$|1 \dots 10\rangle$**:** In diesem Fall werden beide kontrollierten Nicht-Gatter sowie das rechte kontrollierte W-Gatter aktiviert. Die beiden kontrollierten Nicht-Gatter bewirken, dass Qubit 1, welches am Eingang den Zustand $|0\rangle$ hat, kurzzeitig auf den Zustand $|1\rangle$ transformiert wird. Dabei aktiviert es das kontrollierte $W^\dagger$-Gatter. Anschließend wird Qubit 1 zurück auf seinen Originalzustand $|0\rangle$ zurücktransformiert. Auf Qubit 0 wirken also die Transformationen $W^\dagger$ und W, welche wieder die Identität bilden. Am Ende hat also jedes Qubit wieder seinen Originalzustand.

$|1 \dots 11\rangle$**:** Die ersten $k-1$ Kontrollqubits aktivieren beide kontrollierten Nicht-Gatter und das rechte kontrollierte W-Gatter. Qubit 1 aktiviert zuerst das linke kontrollierte W-Gatter, wird dann jedoch von dem linken kontrollierten Nicht-Gatter in den Zustand $|0\rangle$ transformiert, so dass das kontrollierte $W^\dagger$-Gatter von ihm nicht aktiviert wird. Anschließend wird Qubit 1 von dem rechten kontrollierten Nicht-Gatter wieder in seinen Originalzustand transformiert. Daher haben am Ende sämtliche Kontrollquibts ihren Originalzustand. Auf Qubit 0 wirken jedoch zwei Transformationen, nämlich $W \cdot W = V$.

Wir haben also genau das Erwünschte erreicht: Auf Qubit 0 wird die Transformation V nur genau dann angewandt, wenn alle k Kontrollqubits den Zustand $|1\rangle$ aufweisen.

Das Verfahren wird nun rekursiv auf alle k-Qubit-kontrollierten V-Gatter mit $k \geq 2$ angewendet. Damit lässt sich die unitäre Transformation U aus Abschnitt 1.3 bis auf 1-Qubit-kontrollierte Gatter herunterbrechen. Es bleibt noch die Frage, wie man diese schon sehr einfachen Strukturen durch Elementaroperationen darstellen kann.

[4] Dass es nur 4 Kontrollqubits besitzt, ist unerheblich. Man kann sich für V-Gatter mit mehr oder weniger Kontrollqubits als im Beispiel einfach die entsprechenden Linien im Schaltkreis dazudenken, sie sind mit dem Rest der Schaltung genauso verbunden, wie die Qubits 1 bis 3.

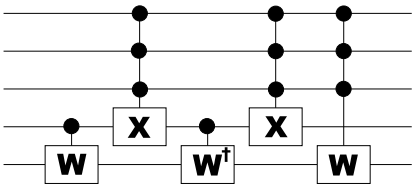


Abbildung 1.5: Konstruktion des k-Qubit-kontrollierten V-Gatters (hier $n = 4$).

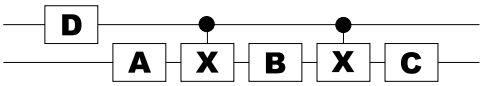


Abbildung 1.6: Konstruktion des 1-Qubit-kontrollierten V-Gatters.

1.3.4 Realisierung 1-Qubit-kontrollierter V-Gatter

Für die Realisierung 1-Qubit-kontrollierter V-Gatter nutzt man die Euler-Zerlegung von unitären 2-dimensionalen Transformationen. Sei V also die gewünschte Transformation, die auf das Zielqubit angewendet werden soll, falls das Kontrollqubit gesetzt ist. Die Euler-Zerlegung von V hat folgende Gestalt:

$$V = \begin{pmatrix} e^{i\delta} & 0 \\ 0 & e^{i\delta} \end{pmatrix} \cdot \begin{pmatrix} e^{-i\alpha/2} & 0 \\ 0 & e^{i\alpha/2} \end{pmatrix} \cdot \begin{pmatrix} \cos(\gamma/2) & \sin(\gamma/2) \\ -\sin(\gamma/2) & \cos(\gamma/2) \end{pmatrix} \cdot \begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix} \tag{1.36}$$

Im folgenden seien die Transformationen A, B und C wie folgt definiert [Cyb01, Bar95]:

$$A = \begin{pmatrix} e^{-i\alpha/2} & 0 \\ 0 & e^{i\alpha/2} \end{pmatrix} \cdot \begin{pmatrix} \cos(\gamma/4) & \sin(\gamma/4) \\ -\sin(\gamma/4) & \cos(\gamma/4) \end{pmatrix} \tag{1.37}$$

$$B = \begin{pmatrix} \cos(-\gamma/4) & \sin(-\gamma/4) \\ -\sin(-\gamma/4) & \cos(-\gamma/4) \end{pmatrix} \cdot \begin{pmatrix} e^{i(\alpha+\beta)/4} & 0 \\ 0 & e^{-i(\alpha+\beta)/2} \end{pmatrix} \tag{1.38}$$

$$C = \begin{pmatrix} e^{i(\alpha-\beta)/4} & 0 \\ 0 & e^{-i(\alpha-\beta)/2} \end{pmatrix} \tag{1.39}$$

Es ist

$$ABC = 1 \tag{1.40}$$

sowie

$$AXBXC = \begin{pmatrix} e^{-i\alpha/2} & 0 \\ 0 & e^{i\alpha/2} \end{pmatrix} \cdot \begin{pmatrix} \cos(\gamma/2) & \sin(\gamma/2) \\ -\sin(\gamma/2) & \cos(\gamma/2) \end{pmatrix} \cdot \begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix} \tag{1.41}$$

$AXBXC$ unterscheiden sich also von V nur durch die Phase. Sei D eine weitere Transformation, nämlich

$$D = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix}. \tag{1.42}$$

Dann ergibt die Konstruktion auf Abbildung 1.6 genau das 1-Qubit-kontrollierte V-Gatter [Cyb01, Bar95]. Das Ergebnis kann man auch nachrechnen, denn

$$V_c = (D \otimes A) \cdot X_c \cdot (1 \otimes B) \cdot X_c \cdot (1 \otimes C) \tag{1.43}$$

wobei V_c das durch Qubit 1 kontrollierte V-Gatter ist und X_c das durch Qubit 1 kontrollierte X-Gatter. Nun ist es also gelungen die unitäre Transformation U aus Abschnitt 1.3 auf Elementaroperationen herunterzubrechen, was Ziel dieses Verfahrens war. Im folgenden Abschnitt soll noch die Effizienz dieses Verfahrens betrachtet werden.

1.4 Zusammenfassung

Ausgehend von einer beliebigen unitären Transformation über n Qubits, wurde diese durch folgende Schritte realisiert:

QR-Zerlegung: Die Transformation wurde in $\Theta(4^n)$ Transformationen zerlegt, von denen jede nur auf einer 2-dimensionalen Ebene operiert, sowie in eine Transformation D. Letztere stellt nur eine Phasenverschiebung der Qubits da und ist somit besonders einfach als Tensorprodukt von elementaren 1 Qubit Gattern realisierbar.

G-Matrizen: Diese wurden durch Permutation der Qubit-Zustände und ein großen k-Qubit-kontrolliertes V-Gatter realisiert. Dabei wurden die Qubit-Zustände so permutiert, dass das V-Gatter nur dann aktiv wurde, wenn es sich um einen Zustand handelt, der in der G-Matrix verändert werden soll.

k-Qubit-kontrollierte V-Gatter: Es wurde gezeigt, wie ein k-Qubit-kontrolliertes V-Gatter auf mehrere $k-1$-Qubit-kontrollierte Gatter zurückgeführt werden kann. Dabei wurde die Tatsache ausgenutzt, dass zu jeder unitären Transformation V eine unitäre Transformation W existiert mit $W^2 = V$. Auf diese Weise können beliebige k-Qubit-kontrollierte V-Gatter bis auf 1-Qubit-kontrollierte V-Gatter heruntergebrochen werden.

1-Qubit-kontrollierte V-Gatter: Zuletzt werden die 1-Qubit-kontrollierten V-Gatter durch 6 Elementaroperationen dargestellt, wobei die Euler-Zerlegung einer 2-dimensionalen unitären Transformation genutzt wird.

Zum Schluss hat man also die beliebig gewählte unitäre Transformation, die das Quantencomputerprogramm darstellt, auf Elementaroperationen zurückgeführt. Diese sind das allgemeine 1-Qubit Gatter sowie das 1-Qubit-kontrollierte X-Gatter.

Literaturverzeichnis

[Fey82] FEYNMAN, RICHARD P., „Simulating Physics with Computers“, *International Journal of Theoretical Physics*, vol. 46, no. 6/7, pp. 467–488, 1982.

[Cyb01] CYBENKO, GEORGE, „Reducing Quantum Computations to Elementary Unitary Operations“, *IEEE 15219615/01*, pp. 27–32, 2001.

[Bar95] BARENCO, ADRIANO, „Elementary gates for quantum computation“, *Physical Review*, vol. 52, no. 5, pp. 3457–3467, 1995.

[Mer04] MERMIN, N. DAVID, „Lecture Notes on Quantum Computation“, *Cornell University, Physics 481-681, CS 483*, 2004.

[Gra01] M.GRASSL, „Fehlerkorrigierende Codes für Quantensysteme: Konstruktionen und Algorithmen“, *Dissertation, Universität Karlsruhe*, 2001.

[Gol96] GOLUB, G.H AND VAN LOAN, C.F., „Matrix Computations“, *John Hopkins Press, Baltimore*, 1996.