Technology
Arts Sciences
TH Köln

Here you can insert the title of your seminar paper

First Student Second Student

Module: Modulename
Course: Coursename

Lecturer: Name of the lecturer

6. Februar 2025

Zusammenfassung

This template can be used for seminar papers. For more tips and tricks regarding the use of figures, tables, quotations, references, footnotes, enumerations, etc. please download the Masterthesis template.

Inhaltsverzeichnis

1 Einführung in die Quanteninformatik

1.1 Quantenbits

Ein Quantenbit, im Folgenden auch Qubit genannt, ist das Medium und die kleinste Einheit, auf dem in der Quanteninformatik gerechnet wird. Auf die genaue physische Realisierung wird in einem späteren Abschnitt der Quantenhardware eingegangen. Bis dahin reicht es das Quantenbit als eine Art Computer-Bit zu verstehen, das sich in einer sogenannten SSuperposition"befindet. Im Zustand der Superposition kann es gleichzeitig den Wert ‚0' und ‚1' annehmen. Ein Quantenbit bleibt in dieser Superposition, bis es gemessen wird, woraufhin die Superposition zerstört wird und das Qubit einen der Zustände 0 oder 1 annimmt. Die Wahrscheinlichkeit, mit der ein Quantenbit in den einen oder anderen Zustand zerfällt, muss nicht gleich verteilt sein und kann beeinflusst werden. Dies macht Berechnungen auf Qubits erst möglich.

Mathematisch betrachtet, werden die Zustände ‚0' und ‚1' in der Quanteninformatik als Vektoren $\binom{1}{0} \equiv 0$ und $\binom{0}{1} \equiv 1$ dargestellt. Für die einfache Lesbarkeit werden diese Vektoren in der Quanteninformatik in der Bra-Ket-Notation dargestellt. Also $\binom{1}{0} \equiv |0\rangle$ und $\binom{0}{1} \equiv |1\rangle$.

Um die Wahrscheinlichkeit zu beschreiben, welchen der beiden Werte ein Quantenbit nach der Messung annehmen wird, wird beiden Werten eine Amplitude α oder β zugeordnet. Demnach wird ein Quantenbit in einer beliebigen Superposition als $\alpha \cdot |0\rangle + \beta \cdot |1\rangle$ dargestellt. α und β sind komplexe Zahlen für die $|\alpha|^2 + |\beta|^2 = 1$ gilt.
Ein Qbit, das nach der Messung mit gleicher Wahrscheinlichkeit in einen der beiden Zustände 0 und 1 zerfällt, würde folglich als $\frac{1}{\sqrt{2}} \cdot |0\rangle + \frac{1}{\sqrt{2}} \cdot |1\rangle$ oder $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ dargestellt werden. Dabei gilt $\alpha = \beta = \frac{1}{\sqrt{2}}$ und erfüllt die Bedingung $\left|\frac{1}{\sqrt{2}}\right|^2 + \left|\frac{1}{\sqrt{2}}\right|^2 = 1$.

Ein Vektor $\binom{\alpha}{\beta}$ wird als „Zustandsvektor" bezeichnet und stellt den Zustand der Superposition eines Qubits dar. Die Bedingung $|\alpha|^2 + |\beta|^2 = 1$ sorgt dafür, dass der Zustandsvektor immer ein Einheitsvektor ist. Dadurch kann jeder Zustand eines Qubits auf dem Einheitskreis eines zweidimensionalen Vektorsystems dargestellt werden. Somit kann ein Quantenbit unendlich viele Zustände haben, die auf einen definierten Bereich abgebildet werden können.

Kommentar

Zu dem Zeitpunkt, als wir uns das Grundwissen erarbeitet haben, war uns nicht klar, weshalb α und β komplexe Zahlen sein müssten und warum sie „Amplituden“ und nicht „Wahrscheinlichkeiten“ oder Ähnliches genannt werden. Wir gingen davon aus, dass wir früher oder später auf einen Use Case stoßen würden, in denen komplexe Zahlen und Amplituden wichtig werden. Dies war allerdings nur für letztes bedingt der Fall. Um kurz vorzugreifen: Amplituden von zwei Qubits können miteinander summiert werden. Dadurch ist es möglich, dass sich manche Amplituden gegenseitig aufheben. Dies wäre mit Wahrscheinlichkeitsverteilungen, die nicht negativ sein dürften, schwer darzustellen. Siehe dazu Erklärung des Mach-Zehnder-Interferometer (S. 255).
Warum α und β komplexe Zahlen sind, war schwer greifbar. Scheinbar hat dies mit der der Quanteninformatik zugrundeliegenden Quantenmechanik zu tun. Nach etwas Recherchearbeit stellte sich heraus, dass eine Antwort auf diese Frage einiges an Vorwissen in der Physik bedurfte. Da wir uns diese Frage am Anfang des Lernprozesses stellten und noch dabei waren in den Konzepten der Quanteninformatik Fuß fassen, entscheiden wir uns auf diese Frage zurück zu kommen, sobald komplexe Zahlen relevant werden würden. Da in der Quanteninformatik mit α und β allerdings gerechnet wird, als seien sie reelle Zahlen (https://www.cs.utep.edu/vladik/2023/tr23-44.pdf Seite 1 und Buch Seite 22), trat dieser Fall nie ein.
Während der Erstellung dieses Dokuments haben uns unsere erlangten Kenntnisse beim Verstehen der Quantenmechanik nicht weiter helfen können, um eine zufriedenstellende Antwort zu formulieren. Da es sehr zeitaufwändig geworden wäre, sämtliche Begrifflichkeiten wie aus dem Kurs Skript von John D Stack (https://courses.physics.illinois.edu/phys580/fa2013/susy_v2.pdf) zu verstehen, nur um diese Frage zu klären, entscheiden wir uns dieser nicht weiter nachzugehen.

Um mit Quantenbits rechnen zu können, muss man den Zustand eines Quantenbits verändern können. Wie dies technisch umgesetzt wird, wird später angerissen. Aus mathematischer Sicht geschieht dies über unitäre 2×2 Matrizen.

Eine Matrix A ist dann unitär, wenn ihre inverse Matrix A^{-1} gleich ihrer adjungierten Matrix $A^\dagger$ ist. Adjungiert ist eine Matrix $A^\dagger$ dann, wenn die Matrix A komplex konjugiert – also jedes Element der Matrix $z_{ij} = a + ib$ zu $z^*_{ij} = a – ib$ komplex konjugiert – und die Matrix dann transponiert wird. Also muss für alle Matritzen A gelten:

$$A^{-1} = (A^*)^T = A^\dagger$$

Für die Quanteninformatik reicht oft die Bedingung $A^{-1} = A^T$, da hier meist mit α und β gerechnet wird, als seien sie reelle Zahlen. Durch diese Bedingung haben unitäre Matrizen die Eigenschaft, dass ein Zustandsvektor unverändert bleibt, wenn eine unitäre Matrix zwei Mal mit ihm verrechnet wird.
Unitäre Transformationen sind also reversibel. Diese Bedingung ist notwendig, um die Länge der Zustandsvektoren beizubehalten.

Beispielhaft kann dies an einer Matrix

$$B = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

demonstriert werden. Wendet man diese Matrix auf ein Qubit im Zustand $|0\rangle$ an, Transformiert sie es in den Zustand $\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$. Diese Transformation wird über eine Multiplikation beschrieben:

$$B|0\rangle = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix}$$

Daraus ergibt sich: $\alpha = \frac{1}{2}$ und $\beta = \frac{\sqrt{3}}{2}$. Die Bedingung $|\alpha|^2 + |\beta|^2 = 1$ trifft für beide Zustandsvektoren $\binom{1}{0}$ und $\binom{\frac{1}{2}}{\frac{\sqrt{3}}{2}}$ zu. Zudem ist B unitär, da $B = B^T = B^{-1}$, und daher eine zulässige Transformation.
Wendet man die Transformation B erneut an, ergibt sich folgendes:

$$B\begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Der Ursprungszustand ist mit der zweiten Anwendung der Transformation wieder hergestellt. Dies ist eine der Grundprinzipien der Quanteninformatik.

1.2 Hadamard-Matrix

Eine unitäre Transformation, die im Laufe unseres Lernprozesses immer wieder vorgekommen ist, ist die sogenannte "Hadamard-Matrix:

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

Multipliziert mit einem Qubit im Zustand $|0\rangle$ transformiert sie es in den Zustand $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ und mit einem im Zustand $|1\rangle$ transformiert sie es in den Zustand $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Beide Folgezustände haben die gleiche Wahrscheinlichkeit bei der Messung einen der Zustände $|0\rangle$ oder $|1\rangle$ anzunehmen.

Kommentar

Beide Zustände haben eine 50%-ige Wahrscheinlichkeit beim Messen den Zustand $|0\rangle$ oder $|1\rangle$ anzunehmen. Sie unterscheiden sich nur im Vorzeichen der β-Amplitude. Würde man die Amplituden als Wahrscheinlichkeiten darstellen (zum Beispiel als $0.5 \cdot |0\rangle + 0.5 \cdot |1\rangle$), ließe sich bei der erneuten Hadamard-Transformation nicht eindeutig sagen, in welchem Zustand sich das Bit vor der ersten Transformation befunden hat. Da die Umkehrbarkeit der Transformationen eine der Grundprinzipien der Quanteninformatik ist, wäre eine Darstellung mit Wahrscheinlichkeitsverteilungen eher unpraktisch.

Mit dieser Gleichverteilung ließe sich beispielsweise ein Münzwurf simulieren. Der Schaltkreis eines Münzwurf Algorithmus sieht folgendermaßen aus:

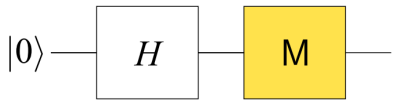

Abbildung 1: Schaltkreis für den Münzwurf Algorithmus

Schaltkreise eigenen sich dafür Quantenalgorithmen anschaulich darzustellen. Auf diese wird später genauer eingegangen.

Zuerst wird ein Quantenbit in den Zustand $|0\rangle$ gebracht. (Man könnte es auch in den Zustand $|1\rangle$ bringen. Das ist für diesen Algorithmus unwichtig.) Danach wendet man die Hadamard-Transformation darauf an, um das Quantenbit in eine Superposition zu bringen, in der die Wahrscheinlichkeit $|0\rangle$ oder $|1\rangle$ zu messen gleich verteilt ist. Anschließend wird gemessen und die Superposition zerfällt zufällig in einen der Zustände $|0\rangle$ oder $|1\rangle$.
Formal beschrieben sieht der Algorithmus so aus:

$$\begin{aligned} |x\rangle &\leftarrow |0\rangle \\ |x\rangle &\leftarrow H\,|x\rangle \\ Miss\,|x\rangle & \end{aligned}$$

„$|x\rangle$“ ist dabei die Bezeichnung des Quantenbits auf dem gerechnet wird.
Mit diesem Algorithmus ist es möglich echte Zufallszahlen zu generieren, da es physikalisch unmöglich ist vorauszusagen, in welchen Zustand die Superposition zerfallen wird. Im Gegensatz zu einem echten Münzwurf, bei dem man das Wurfergebnis theoretisch berechnen könnte, wenn man sämtliche Variablen, wie z.B. Wurfhöhe, Drehmoment der Münze, Luftwiederstand, ect. kennen würde. Oder im Gegensatz zu einem herkömmlichen Computer, der nur Pseudozufallszahlen generieren kann.

1.3 Quantenregister

Ein Quantenregister ist eine Aneinanderreihung mehrerer voneinander unabhängiger Quantenbits. Diese werden benötigt, um Quantenschaltkreise zu realisieren, damit auf ihnen logische Operationen durchgeführt werden können.
Der Zustand eines Quantenregisters der Länge m wird als m-faches Tensorprodukt aller Zustände der einzelnen Quantenbits des Registers dargestellt. Ein Quantenregister R mit 2 Qubits $|x_0\rangle$ und $|x_1\rangle$ in beispielsweise den Basiszuständen $|x_0\rangle = \binom{0}{1}$ und $|x_1\rangle = \binom{1}{0}$ befindet sich im Zustand:

$$R = |x_0\rangle \otimes |x_1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$$

Alternativ würde man $R = |1\rangle \otimes |0\rangle = |10\rangle$ schreiben. Manchmal werden die Basiszustände zur Übersichtlichkeit auch in Dezimalform dargestellt. $|10\rangle$ wäre demnach $|2\rangle$.
Wie auch die einzelnen Qubits, kann sich das gesamte Quantenregister in einer Superposition befinden. Sind die Qubits aus dem obigen Beispiel in den Zuständen $|x_0\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$ und $|x_1\rangle = \gamma_0 |0\rangle + \gamma_1 |1\rangle$ ist der Zustand des Quantenregisters

$$R = |x_0\rangle |x_1\rangle = (\beta_0 |0\rangle + \beta_1 |1\rangle) \cdot (\gamma_0 |0\rangle + \gamma_1 |1\rangle)$$

$$= \beta_0\gamma_0 |0\rangle |0\rangle + \beta_0\gamma_1 |0\rangle |1\rangle + \beta_1\gamma_0 |1\rangle |0\rangle + \beta_1\gamma_1 |1\rangle |1\rangle$$

Substituiert man $\beta_i\gamma_j = \alpha_{ij}$ ergibt sich der Zustand

$$R = \alpha_{00} |0\rangle |0\rangle + \alpha_{01} |0\rangle |1\rangle + \alpha_{10} |1\rangle |0\rangle + \alpha_{11} |1\rangle |1\rangle$$

Und kann als

$$R = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$$

Oder

$$R = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle + \alpha_3 |3\rangle$$

Geschrieben werden.
Da aus $|\beta_0|^2+|\beta_1|^2 = 1$ und $|\gamma_0|^2+|\gamma_1|^2 = 1$ sich $|\alpha_{00}|^2+|\alpha_{01}|^2+|\alpha_{10}|^2+|\alpha_{11}|^2 =1$ ergibt, bildet α die Amplitude für den jeweiligen Zustand $|00\rangle$, $|01\rangle$, $|10\rangle$ und $|11\rangle$.
Allgemeiner gefasst befindet sich ein Quantenregister R der Länge n im Zustand

$$R = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle,$$

für den die Bedingung

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$$

gilt. Dabei entspricht $i = 0, ..., 2^n - 1$ der Dezimaldarstellung der Bits im Quantenregister und $|\alpha_i|^2$ der Wahrscheinlichkeit, dass sich das Register nach einer Messung im jeweiligen Zustand $|i\rangle$ befindet.
Es ist möglich Transformationen nicht nur auf einzelnen Quantenbits durchzuführen, sondern auch auf ganze Register. Um eine Transformation auf einem Register eine Transformation durchzuführen, muss zuerst ein möglicherweise mehrfaches Tensorprodukt der Transformationsmatrix mit sich selbst berechnet werden. Da ein Tensorprodukt nur zwischen Matrizen derselben Größe berechnet werden kann, ist es nur möglich Transformationen auf 2^n langen Registern durchzuführen.
Wir vermuten, dass wenn man eine Transformation auf ein Register der Länge m anwenden möchte, wobei m nicht in der Menge ist, die mit 2^n abgebildet werden kann, man das Register in zwei Unterregister aufteilen kann. Und die Transformation auf die Unterregister ausführt (Länge $2^{max(n)} < m$ und Länge Rest..) Da Rechenschritte physikalisch nur lokal durchgeführt werden können

(s.31) scheint es für uns keinen Unterschied zu machen, auf wie vielen Qubits eine Transformation mathematisch durchgeführt wird.
Die Transformationen $A_1, \ldots, A_{2^n}$ auf die Bits $|x_1\rangle, \ldots, |x_{2^n}\rangle$ mit jeweils A_i auf $|x_i\rangle$ entsprechen also der Transformation $A_1 \otimes, \ldots, \otimes A_{2^n}$ auf das Register $|x_1, ..., x_{2^n}\rangle$.
Möchte man die Hadamard-Transformation H auf ein Register $R = |00\rangle$ anwenden, müsste man zuerst die Hadamard-Transformation auf Registerebene

$$H \otimes H \;=\; H_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} H & H \\ H & -H \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

bilden. Daraus ergibt sich

$$H_2 R \;= \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{matrix} 1 \\ 0 \\ 0 \\ 0 \end{matrix} = \begin{matrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{matrix}$$

Beziehungsweise

$$\frac{1}{2} \left(|00\rangle + |01\rangle + |10\rangle + |11\rangle \right)$$

oder

$$\frac{1}{2} \left(|0\rangle + |1\rangle + |2\rangle + |3\rangle \right).$$

Dabei bleibt die Bedingung

$$\sum_{i=0}^{2^n - 1} |\alpha_i|^2 = 1$$

Mit n = 2 und $\alpha_i = \frac{1}{2} \forall i$ erfüllt. Die Wahrscheinlichkeit, dass jeder Basiszustand nach der Messung auftritt, ist gleichverteilt. Diese Berechnung kann genutzt werden, um echte Zufallszahlen zwischen 0 und 3 zu generieren. Formal beschrieben sieht der Algorithmus aus, wie folgt:

$$R = |x_1 x_0\rangle \leftarrow |00\rangle \; R = H_2 R Miss R$$

Dieser Algorithmus kann auf eine beliebige Registergröße 2^n erweitert werden. Allerdings ist das Rechnen auf Registerebene bisher nur mathematisch sinnvoll. Tatsächlich werden sämtliche Rechenschritte in lokalen unitären Transformationen durchgeführt. „Lokal“ heißt in diesem Fall, dass maximal drei Qubits an der Berechnung beteiligt sind, da es physikalisch einfacher ist Transformationen auf drei Bits auszuführen als auf 2^n mit beliebig hohen n. Zudem sind mindestens drei Bit notwendig, um klassische Rechenverfahren in Quantenalgorithmen zu überführen. Dies wird später deutlich.
In den beiden Münzwurfbeispielen wurde die Hadamard-Transformation nur auf Quantenbits oder -register angewandt, bei denen sich alle Bits im Zustand $|0\rangle$ befunden haben. Ein n langes Quantenregister R, dessen Bits sich alle im Zustand $|0\rangle$ befunden haben und auf das die Hadamard-Transformation angewandt wurde, kann wie folgt dargestellt werden:

$$R = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n - 1} |i\rangle$$

Diese Darstellung reicht allerdings nicht aus, um Quantenregister abzubilden, dessen Quantenbits sich vor der Hadamard-Transformation teilweise im Zustand $|1\rangle$ befunden haben. Wendet man die Hadamard-Transformation auf ein Register $|xy\rangle$ an, das sich im Zustand $|01\rangle$ befindet, sähe das Quantenregister vor dem Ausmultiplizieren wie folgt aus:

$$|01\rangle \xrightarrow{H_2} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \cdot \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Man kann an dieser Stelle die Information, ob sich die jeweiligen Quantenbits vorher im Zustand $|0\rangle$ oder $|1\rangle$ befunden haben, in das Vorzeichen ziehen:

$$|xy\rangle \xrightarrow{H_2} \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x |1\rangle) \cdot \frac{1}{\sqrt{2}}(|0\rangle + (-1)^y |1\rangle).$$

Ausmultipliziert ergibt dies:

$$\frac{1}{2}\left(|00\rangle + (-1)^x |01\rangle + (-1)^y |10\rangle + (-1)^{x\oplus y} |11\rangle\right).$$

Allgemeiner gefasst:

$$\frac{1}{2}\left((-1)^{(0,0)\oplus z} |00\rangle + (-1)^{(0,1)\oplus z} |01\rangle + (-1)^{(1,0)\oplus z} |10\rangle + (-1)^{(1,1)\oplus z} |11\rangle\right),$$

mit $z = (x, y)^T$.
Muss zugeben, den Sinn von diesem Ausmultiplizieren habe ich am Anfang nicht verstanden. Wahrscheinlich wird das bei komplexeren Algorithmen erst relevant. Anhand der letzten Darstellung kann man ein Quantenregister der Länge n im Zustand $x \in \{0,1\}^n$, auf das die Hadamard-Transformation angewandt wurde, wie folgt darstellen:

$$H_n |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in 0,1^n} (-1)^{x \cdot y} |y\rangle .$$

Dabei ist $x \cdot y$ das Skalarprodukt $\oplus_{i=1}^n x_i y_i$ der Vektoren $x, y \in \{0,1\}^n$. Auch die Hadamard-Transformation ist reversibel. Nehmen wir das vorherige Beispiel:

$$|01\rangle \xrightarrow{H_2} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \cdot \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Wendet man die Hadamard-Transformation erneut an, ergibt sich:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \cdot \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{H_2}$$

$$\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) \cdot \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) - \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right)$$

$$= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |0\rangle)\right) \cdot \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|1\rangle + |1\rangle)\right)$$

$$= \frac{1}{2}(|0\rangle + |0\rangle) \cdot \frac{1}{2}(|1\rangle + |1\rangle) = \frac{1}{4}(|01\rangle + |01\rangle + |01\rangle + |01\rangle) = |01\rangle .$$

Die Reversibilität der Hadamard-Transformation ist für komplexere Algorithmen von Bedeutung. Bevor auf diese und deren Darstellung in Form von Quantenschaltkreisen eingegangen werden kann, muss vorher noch auf den Vorgang der Messung eingegangen werden.

1.4 Messen

Die Messung „Miss$|x\rangle$“ ist die einzige Transformation in der Quanteninformatik, die nicht reversibel / unitär ist. Beim Messen verliert ein Quantenbit seine Superposition und fällt zufällig, je nach Wahrscheinlichkeitsverteilung in einen der Basiszustände in denen gemessen wurde. Aus diesen Zuständen ist nicht zu errechnen in welchem Zustand sich das Quantenbit vor der Messung befunden hat. Bisher wurde davon ausgegangen, dass ein Quantenbit nur in die Zustände $|0\rangle$ oder $|1\rangle$ zerfallen kann. Dies geschieht allerdings nur dann, wenn $|0\rangle$ und $|1\rangle$ die Basis der Messung ist, beziehungsweise dies die Basis ist, in dessen Vektorraum der Zustand des Quantenbits abgebildet wird. In der Quanteninformatik müssen diese Basen die Eigenschaften der Orthonormalbasen erfüllen. Die Basis zur Abbildung eines Quantenbits $\{|0\rangle, |1\rangle\}$ erfüllt diese Voraussetzungen. Diese wird Standardbasis genannt (S45). Die Basis zur Abbildung eines Registers mit zwei Quantenbits $\{|00\rangle, |01\rangle\,|10\rangle, |10\rangle\}$ erfüllt diese Bedingung ebenfalls. Diese wird schließlich aus dem einfachen Tensorprodukt der Standardbasis mit sich selbst gebildet. Misst man als Beispiel das Register mit zwei Quantenbits, zerfällt der Zustand des Registers in einen der zugehörigen Basiszustände und man erhält ein Messergebnis. Mathematisch ausgedrückt bestimmen beim Messen des 2 Bit-Quantenregisters "die Projektionen auf die eindimensionalen Unterräume

$$Span\{|00\rangle\}, Span\{|01\rangle\}, Span\{|10\rangle\} \text{ und } Span\{|11\rangle\}$$

das Ergebnis."(S.47) Diese Folge von Unterräumen: $Span\{|00\rangle\}, Span\{|01\rangle\}, Span\{|10\rangle\}$ und $Span\{|11\rangle\}$ die aus der disjunkten Zerlegung der Orthonormalbasis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ entstehen, nennt man Öbservable". Diese Unterräume enthalten jeweils einen Basisvektor, der jeweils einen der Zustände bildet, der nach dem vollständigen Messen des Registers *beobachtet* werden kann.
Es ist zwei zusätzliche Dinge beim Messen möglich. Man kann zum einen nur einzelne Bits messen, statt des gesamten Registers und zum anderen beim Messen eine andere Basis verwenden, als zum Projektieren des Zustandes in einen Vektorraum verwendet wird.
Das Messen einzelner Bits in einem Register ist in manchen Algorithmen wichtig, um anhand eines Zwischenergebnisses zu bestimmen, welche Folgetransformationen durchgeführt werden müssen. Quantenteleportation ist ein Beispiel dafür (siehe quantenteleportation).
Misst man im einem Register mit zwei Bits im Zustand $|\phi\rangle$ beispielsweise nur das erste Bit, bestimmen die Projektionen

$$Span\{|00\rangle\ |01\rangle\} \text{ und } Span\{|10\rangle\ |11\rangle\}$$

das Ergebnis. In dem Fall geht das Register mit der Wahrscheinlichkeit

$$|\alpha_{00}|^2 + |\alpha_{01}|^2$$

in den Zustand

$$|\phi'\rangle = \frac{\alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

über und mit Wahrscheinlichkeit

$$|\alpha_{10}|^2 + |\alpha_{11}|^2$$

in den Zustand

$$|\phi'\rangle = \frac{\alpha_{10}|00\rangle + \alpha_{11}|01\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}.$$

Wir erfahren bei der Messung nur den Wert des gemessenen Bits, nicht die Amplituden des Folgezustandes."(S47)
Das Messen in einer anderen Basis, als der, die zur Projektion ein einem Vektorraum genutzt wird, kann genutzt werden, um die Superposition des Quantenbits nach der Messung nicht vollständig zu zerstören. Misst man ein Quantenbit in der Basis $\{|+\rangle, |-\rangle\}$ mit $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ und $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ erhält man als Ergebnis entweder den Zustand $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ oder $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Dies ist immer noch eine Superposition. Daher kann nach der Messung mit dem Quantenbit immer noch weiter gerechnet werden. Allerdings ist es auch hierbei nicht möglich den Zustand zu ermitteln, in dem sich das Bit vor der Messung befunden hat. Die Messung bleibt irreversibel. Die Basis $\{|+\rangle, |-\rangle\}$ wird Hadamard-Basis genannt.
Zur Veranschaulichung kann man die Abbildung unten dienen.
[Hier Abbildung 2.16 von S 44 einfügen]
Es wird ein Zustandsvektor in der Standardbasis dargestellt. Die Länge der Projektionen des Zustandsvektors auf den beiden Achsen bestimmen die Wahrscheinlichkeit, mit der einer der Zustände nach der Messung eingenommen wird. Mit der Wahrscheinlichkeit $|\alpha|^2$ wird der Zustand nach der Messung $|0\rangle$ sein und mit der Wahrscheinlichkeit $|\beta|^2$ $|1\rangle$.
In der folgenden Abbildung wird derselbe Zustandsvektor gezeigt, mit dem Unterschied, dass die Koordinatenachsen nach der Hadamard-Basis ausgerichtet sind.
[Hier Abbildung 2.17 von S45 einfügen]
Die Projektionen der Achsen haben sich im Vergleich zur Projektion auf die Standardbasis verändert. Mit der Wahrscheinlichkeit $|\alpha'|^2$ wird nach dem Messen der Zustand $|+\rangle$ angenommen und mit der Wahrscheinlichkeit $|\beta'|^2$ $|-\rangle$. (S45)
Mathematisch sieht diese "Basistransformationäus wie folgt:

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

[Wofür das gebraucht wird, ist uns nicht ganz bekannt??]
Allgemeiner lässt sich zusammenfassen: Register R bestehe aus n Quantenbits und befinde sich im Zustand

$$|\phi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$$

Wir messen bezüglich der Basis $|0'\rangle, |1'\rangle, ..., |(2^n-1)'\rangle$ aus zueinander orthogonalen Vektoren der Länge 1."(S.46) Dies ist eine andere Basis, als die in der sich $|\phi\rangle$ befindet. "Dabei wird die Superposition von $|\phi\rangle$ zerstört. Hat $|\phi\rangle$ bezüglich der Messbasis die Darstellung

$$\sum_{i=0}^{2^n-1} \alpha_i' |i\rangle$$

so finden wir das Register nach der Messung mit Wahrscheinlichkeit $|\alpha'_i|^2$ im Zustand $|i'\rangle$ vor. Sämtliche anderen Informationen gehen dabei verloren."(Seite 46)
Das Messen einzelner Bits oder ganzer Register, sowie das Messen von Teilen eines Registers in der Standardbasis oder auch in einer anderen umfasst alles, was beim Messen möglich ist.