QuaC Zusammenfassung

October 24, 2023

Contents

1 Grundlagen

1.1 Definitionen

Definition 1.1. $|\phi\rangle$ ist ein Spaltenvektor und $\langle\phi|$ ein Spaltenvektor.
$\langle\phi|\psi\rangle = \sum_{i=1}^{n} \phi_i^* \cdot \psi_i$ ist das innere Produkt.
$|0\rangle = \binom{1}{0}$ und $|1\rangle = \binom{0}{1}$. Das sind die Basis Vektoren.

Ein Qubit ist ein normierter Vektor der Form $\alpha|0\rangle + \beta|1\rangle$. Auf diesem kann eine Messung durchgeführt werden, sodass das Qubit kollabiert zu 0 mit Wahrscheinlichkeit $|\alpha|^2$ und mit Wahrscheinlichkeit $|\beta|^2$ zu 1.
Ein n-Qubit ist ein Vektor der Dimension 2^n. Das heißt, obiges Beispiel ist ein 1-Qubit und ein 2-Qubit hat vier Einträge. Die Vektoren sind dabei immer normiert. In höher dimensionalen Vektoren kann eine Messung einzelner Bits ausreichen, um das System zum kollabieren zu bringen.
Ein 1-Qubit-Gatter ist eine unitäre 2×2 Matrix U. Das heißt, $U^t U = I$, wobei $U^t = (U^T)^*$. Ein Spezialfall ist dabei

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

Die Transformation eines Qubits ϕ mit H ist dabei einfach $H \cdot \phi$. So ist zum Beispiel

$$H(|0\rangle) = \frac{1}{\sqrt{(2)}}|0\rangle + \frac{1}{\sqrt{(2)}}|1\rangle$$

Im Falle eines 2-Qubit-Gatters würde eine unitäre 4×4 Matrix herangezogen werden. Ein Beispiel ist das *C-NOT* Gatter

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Lemma 1.2. *Das innere Produkt hat folgende Eigenschaften:*

1. $\langle\phi|\phi\rangle \geq 0$
2. $\langle\phi|(a|\phi_1\rangle + b|\phi_2\rangle) = a\langle\phi|\phi_1\rangle + b\langle\phi|\phi_2\rangle$
3. $\langle\psi|\phi\rangle^* = \langle\phi|\psi\rangle$

Für eine $m \times n$ Matrix A ist weiter

$$(|A\psi\rangle, |A\phi\rangle) = \langle AA^t\psi|\phi\rangle$$

Definition 1.3. Wir definieren weiter eine Qubit-Norm $||\cdot|| : \mathbb{C}^n \to \mathbb{C}$ durch

$$|||\phi\rangle|| = \sqrt{\langle\phi|\phi\rangle}$$

Dabei heißt ein Vektor ϕ unitär, wenn $|||\phi\rangle|| = 1$.

Definition 1.4. Wir definieren zu den Vektoren $|0\rangle$ und $|1\rangle$ eine Dualbasis durch

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$$

und

$$|\searrow\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$$

. Dies ist eine Orthonormalbasis.

Definition 1.5. (Tensorprodukt) Seien $x = \binom{x_1}{x_2}$ und $y = \binom{y_1}{y_2}$ zwei Vektoren. Das Tensorprodukt ist definiert als

$$x \otimes y = \begin{pmatrix}x_1y_1\\x_1y_2\\x_2y_1\\x_2y_2\end{pmatrix}$$

Das ist leicht verallgemeinerbar für höher dimensionale Vektoren. Außerdem kann das Tensorprodukt auf Matrizen

$$A = \begin{pmatrix}a_{1,1} & \dots & a_{1,n}\\ \vdots & & \vdots\\ a_{m,1} & \dots & a_{m,n}\end{pmatrix}$$

und eine beliebig dimensionale Matrix B angewandt werden durch

$$A \otimes B = \begin{pmatrix}a_{1,1}B & \dots & a_{1,n}B\\ \vdots & & \vdots\\ a_{m,1}B & \dots & a_{m,n}B\end{pmatrix}$$

Wenn mehrere Qubits $|\phi\rangle = \binom{\alpha}{\beta}$ und $|\psi\rangle = \binom{\gamma}{\delta}$ vorliegen, dann schreiben wir

$$|\phi\rangle|\psi\rangle = |\phi\psi\rangle = |\phi\rangle \otimes |\psi\rangle \in \mathbb{C}^4$$

Wird $|\phi^n\rangle$ geschrieben, so ist damit das n-fache Tensorprodukt von $|\phi\rangle$ gemeint.

Lemma 1.6. *Das Tensorprodukt hat folgende Eigenschaften:*

1. $|v\rangle \otimes |w\rangle + |v\rangle \otimes |u\rangle = |v\rangle(|w\rangle + |u\rangle)$
2. $a(|v\rangle \otimes |w\rangle = a|v\rangle \otimes |w\rangle) = |v\rangle \otimes a|w\rangle$
3. $(|u\rangle \otimes |v\rangle, |w\rangle \otimes |x\rangle) = (|u\rangle \otimes |w\rangle, |v\rangle \otimes |x\rangle)$

1.2 Quantenschaltkreise

Diese unterscheiden sich von klassischen Schaltkreisen insofern, dass Operationen reversibel sind. In klassischen Schaltkreisen ist das nicht der Fall, da zum Beispiel bei einer $\wedge$ Verknüpfung mit Ergebnis 0 nicht auf die Eingabewerte rückgeschlossen werden kann. Quantenschaltkreise können verwendet werden um sowohl klassische als auch probabilistische Schaltkreise zu modellieren.

Theorem 1.7 (no cloning satz)**.** *Es gibt keine unitäre Transformation U, das ein Qubit $|\phi\rangle$ kopiert.*

Proof. Falls so ein U existiert, dann gilt $\forall|\phi\rangle$ und $\forall|\psi\rangle$ immer $U|\phi 0\rangle = |\phi\phi\rangle$ und $U|0\psi\rangle = |\psi\psi\rangle$. Dann gilt

$$\langle\phi|\psi\rangle\langle\phi|\psi\rangle = \langle\phi\psi|\phi\phi\rangle = (U|\phi 0\rangle, U|\psi 0\rangle) = (U^t U|\phi 0\rangle, |\psi 0\rangle) = \langle\phi 0|\psi 0\rangle = \langle\phi|\psi\rangle\langle 0|0\rangle$$

Da 0 die Norm 1 hat folgt $\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2$ was nur für die Werte 0 und 1 der Fall ist. □

1.3 Simulation klassischer Schaltkreise

Wir definieren das Fredkin Gatter $f(a,b,0) = (a,b,0)$ und $f(a,b,1) = (b,a,1)$ für $a,b \in \{0,1\}$. Dafür dient die folgende 8×8 Matrix:

$$F = \begin{pmatrix} I_3 & 0 & 0 \\ 0 & J_3 & 0 \\ 0 & 0 & I_2 \end{pmatrix}$$

wo J_3 die um 90° rotierte 3×3 Einheitsmatrix ist. Mit diesem können klassische Boole'sche Funktionen simuliert werden. Mit der obigen Matrix gilt $f(0,b,c) = (c \wedge b, \overline{c} \wedge b, c)$ und ist somit eine UND-Funktion. Der erste Output ist der für die Operation relevante Teil, die anderen beiden werden für die Umkehrung gebraucht. Ein ODER-Gatter kann mit $f(1,b,c) = (b \wedge \overline{c}, b \wedge c, c)$ simuliert werden. Zum Schluss ist eine Negation durch $f(0,1,c) = (c, \overline{c}, c)$ darstellbar. Da diese drei Funktionen eine vollständige Basis sind,

kann somit jeder klassische Schaltkreis durch Verkettung von Fredkin Gattern simuliert werden. Für einen klassischen Schaltkreis c gibt es einen Quantenschaltkreis der Größe $p(|c|)$, der c berechnet.

1.4 Simulation probabilistischer Schaltkreise

Ein probabilistischer Schaltkreis ist ein klassische Schaltkreis, der als Eingabe mit gewisser Wahrscheinlichkeit eine Konstante bekommt und der das Ergebnis mit einer genügend großen Wahrscheinlichkeit berechnet.
Die Eingabe ist dabei gegeben als Input x und einer Menge z an Zufallsbits. Die Aufgabe des Schaltkreises könnte es sein, mit Wahrscheinlichkeit $p > \frac{3}{4}$ zu berechnen, ob x eine Primzahl ist.
Der Input einer Zufallsvariablen kann durch Transformation mittels eines Hadamard Gatters und anschließender Messung des Qubits simuliert werden.

2 Die Komplexitätsklasse BQP

Im klassischen Sinne ist eine Problem L einer Sprache Σ^* in der Klasse P, wenn es einen polynomiellen Algorithmus gibt, der L entscheidet.

Definition 2.1 (BPP - bounded error probabilistic polynomial time)**.** Sei $L \subseteq \Sigma^*$. Dann gilt $L \in$BPP genau dann, wenn es eine Familie von Quantenschaltkreisen $\{c_1, ...\}$ mit Zufallsbits und ein Polynom p gibt, sodass $\forall x \in \Sigma^*$

- $\forall x$ gilt $x \in L$ impliziert $p[c_n(x) = 1] \geq \frac{3}{4}$
- $\forall x$ gilt $x \notin$ ipliziert $p[c_n(x) = 0] \geq \frac{3}{4}$
- c_n hat höchstes $c(n)$ Gatter

Definition 2.2 (BQP - bounded error quantum polynomial time)**.** Sei $L \subseteq \Sigma^*$. Dann gilt $L \in$BQP genau dann, wenn es eine Familie von Quantenschaltkreisen $\{c_1, ...\}$ und ein Polynom p gibt, sodass $\forall x \in \Sigma^*$

- $\forall x$ gilt $x \in L$ impliziert $p[c_n(x) = 1] \geq \frac{3}{4}$
- $\forall x$ gilt $x \notin$ ipliziert $p[c_n(x) = 0] \geq \frac{3}{4}$
- c_n hat höchstes $c(n)$ Gatter

Remark 2.3. Es gilt BQP$\subset$BPP.

Definition 2.4. Sei S eine Menge an Transformationen. S ist eine universelle Menge für alle U unitär, wenn U mit Gattern aus S approximiert werden kann. D.h.

$$\forall \epsilon > 0 \; \exists G_1, G_2, ...G_k \in S \text{ s.d. } ||U - G_1 G_2 ... G_k|| < \epsilon$$

Ein Beispiel für S ist CNOT mit allen 1-Qubit Gattern. Diese ist aber unendlich groß. $S = \{\text{CNOT, H, } \frac{\pi}{8} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{pi}{4}} \end{pmatrix}\}$ ist ein endliches Beispiel.