Vorlesung 8

15.6.2021

C präpariert zwei Teilchen und kann das beliebig oft wiederholen.

A und B erhalten je ein Teilchen und messen je mit Wahrscheinlichkeit $\frac{1}{2}$

$$
\begin{array}{llll}
A & P_Q & \text{oder} & P_R \\
B & P_S & \text{oder} & P_T
\end{array}
$$

Mögliche Meßwerte: ± 1

$$E(QS) + E(RS) + E(RT) - E(QT) \leq 2 \quad (*)$$

Jetzt quantenmechanisch:

C präpariert stets

$$|\psi\rangle = |\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \in \mathcal{H}^{\otimes 2}$$

$$Q = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad S = \frac{-Z-X}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}$$

$$R = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad T = \frac{Z-X}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix} +1 & -1 \\ -1 & -1 \end{pmatrix}$$

$$\Longrightarrow \quad \langle RS\rangle_\psi + \langle QS\rangle_\psi + \langle RT\rangle_\psi - \langle QT\rangle_\psi = 2\sqrt{2}$$

(z.B.:

$$\langle QS\rangle_\psi = \frac{1}{\sqrt{2}}(0,1,-1,0)\frac{1}{\sqrt{2}}\begin{pmatrix} -1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}$$

$$= \frac{1}{\sqrt{2}}$$

$$\langle QT \rangle_\psi = -\frac{1}{2} \;)$$

Das kann die Physik experimentell bestätigen.

Mögliche <u>Fehler</u> in der Herleitung von (*):

1) P_Q, P_R, P_S, P_T haben festgelegte Werte, die unabhängig sind von der Messung ("Realität")

2) Die Messung von A hat keinen Einfluß auf die Messung von B ("Lokalität")

Quantengatter und Schaltkreise

<u>Klassische Gatter</u> Im klassischen Computer führt der Prozessor eine Abfolge von Transformationen

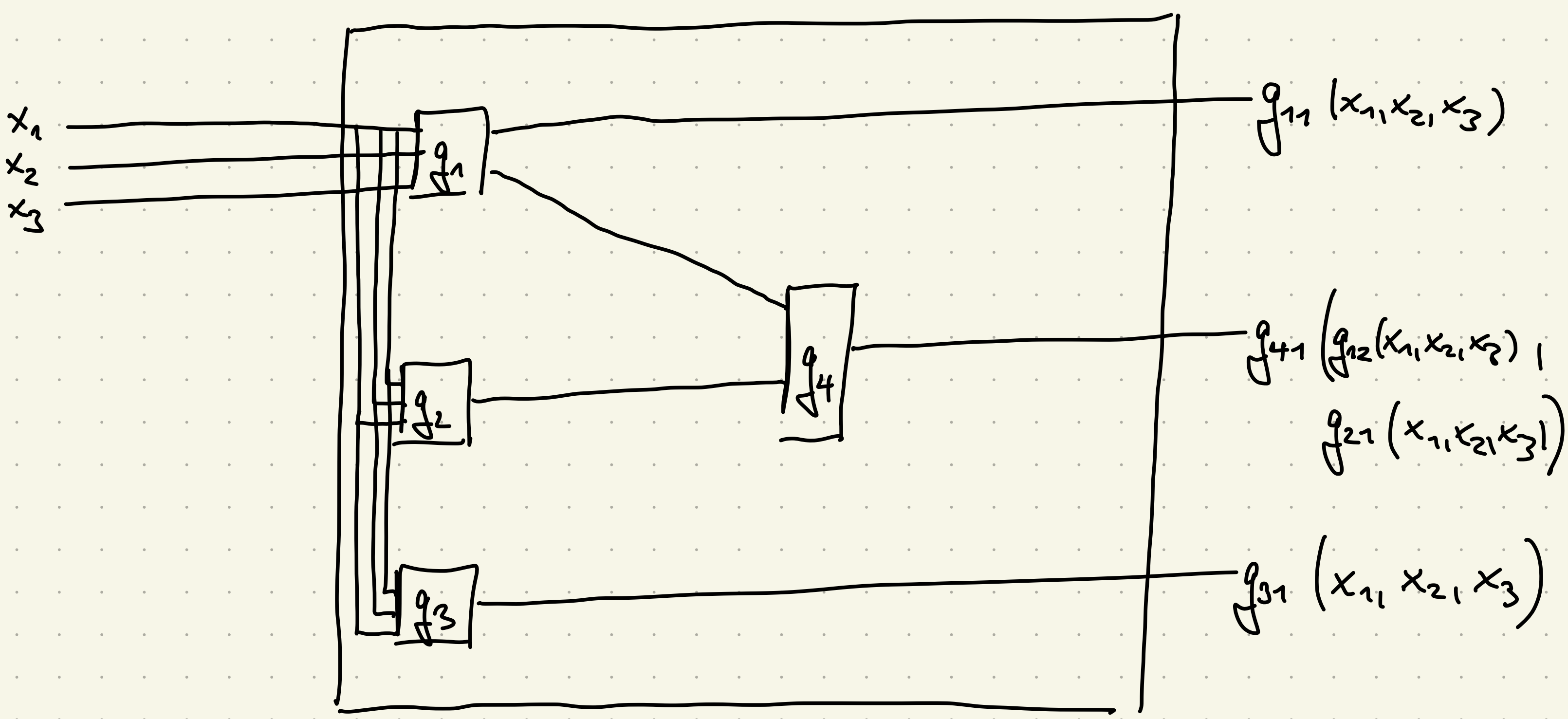
$$f : \{0,1\}^n \longrightarrow \{0,1\}^m$$

<u>Definition:</u> Ein <u>klassisches Gatter</u> g ist eine Abb.

$$g : \{0,1\}^n \to \{0,1\}^m$$
$$(x_1, \dots, x_n) \mapsto (g_1(x_1,\dots,x_n), \dots, g_m(x_1,\dots,x_n))$$

Wir schreiben $g \in \mathcal{F}[\underbrace{g_1, \dots, g_\ell}_{\text{Gatter}}]$, falls g aus $g_1, \dots, g_\ell$ "gebildet werden kann". Eine

Menge $\mathcal{G}$ von Gattern heißt <u>universell</u>, falls jedes beliebige Gatter g aus Gattern $g_1, \dots, g_t \in \mathcal{G}$, $t \in \mathbb{N}$, gebildet werden kann.



<u>Wichtige Beispiele:</u>

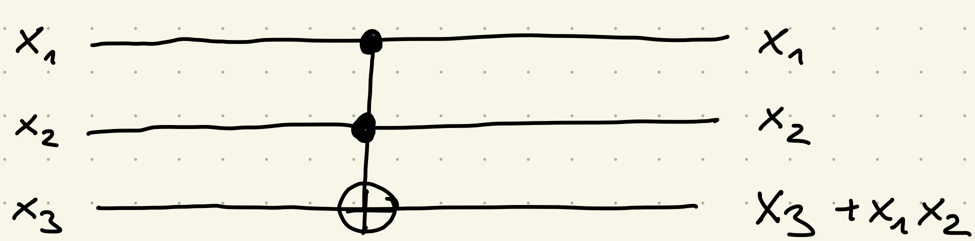
NOT : $\{0,1\} \longrightarrow \{0,1\}$

AND : $\{0,1\}^2 \longrightarrow \{0,1\}$, $(x_1, x_2) \longmapsto x_1 \cdot x_2 \pmod 2$

OR : $\{0,1\}^2 \longrightarrow \{0,1\}$, $(x_1, x_2) \longmapsto x_1 + x_2 + x_1 x_2$

XOR : $\{0,1\}^2 \longrightarrow \{0,1\}$, $(x_1, x_2) \longmapsto x_1 + x_2$

TOF (Tofoli) : $\{0,1\}^3 \longrightarrow \{0,1\}^3$, $(x_1, x_2, x_3) \longmapsto (x_1, x_2, x_3 + x_1 x_2)$



Satz: TOF ist universell und bijektiv.

Beweis: Es genügt

$$f : \{0,1\}^n \longrightarrow \{0,1\}$$

Induktion nach n

$n = 1$

$$\begin{aligned}
ID(x_1) &= x_1 = TOF_1(x_1, 1, 1) \\
FALSE(x_1) &= 0 = TOF_1(0, 0, 0) \\
TRUE(x_1) &= 1 = TOF_1(1, 0, 0) \\
NOT(x_1) &= TOF_3(1, 1, x_1)
\end{aligned}$$

$n-1 \rightarrow n$: Definiere

$$g_0(x_1, \ldots, x_{n-1}) := f(x_1, \ldots, x_{n-1}, 0)$$

$$g_1(x_1, \ldots, x_{n-1}) := f(x_1, \ldots, x_{n-1}, 1)$$

und betrachte

$$h(x_1, \ldots, x_n) := XOR\Big(AND\big(g_0(x_1, \ldots, x_{n-1}), NOT(x_n)\big), AND\big(g_1(x_1, \ldots, x_{n-1}), x_n\big)\Big)$$

$$\left.\begin{aligned}
&\text{Induktion} \Rightarrow g_0, g_1 \text{ darstellbar} \\
&AND(x_1, x_2) = TOF_3(x_1, x_2, 0) \\
&XOR(x_1, x_2) = TOF_3(1, x_1, x_2)
\end{aligned}\right\} \Longrightarrow$$

$\text{NOT}(x_1) = \text{TOF}_3(1, 1, x_1)$

h ist durch Toffoli-Gatter darstellbar.

Rechnung zeigt: $h = f$ (Übung).

Zur Invertierbarkeit: $\text{TOF}^2 = \text{id}$

$\Rightarrow$ TOF ist injektiv $\Longrightarrow$ TOF ist bijektiv. ∎

Quantengatter

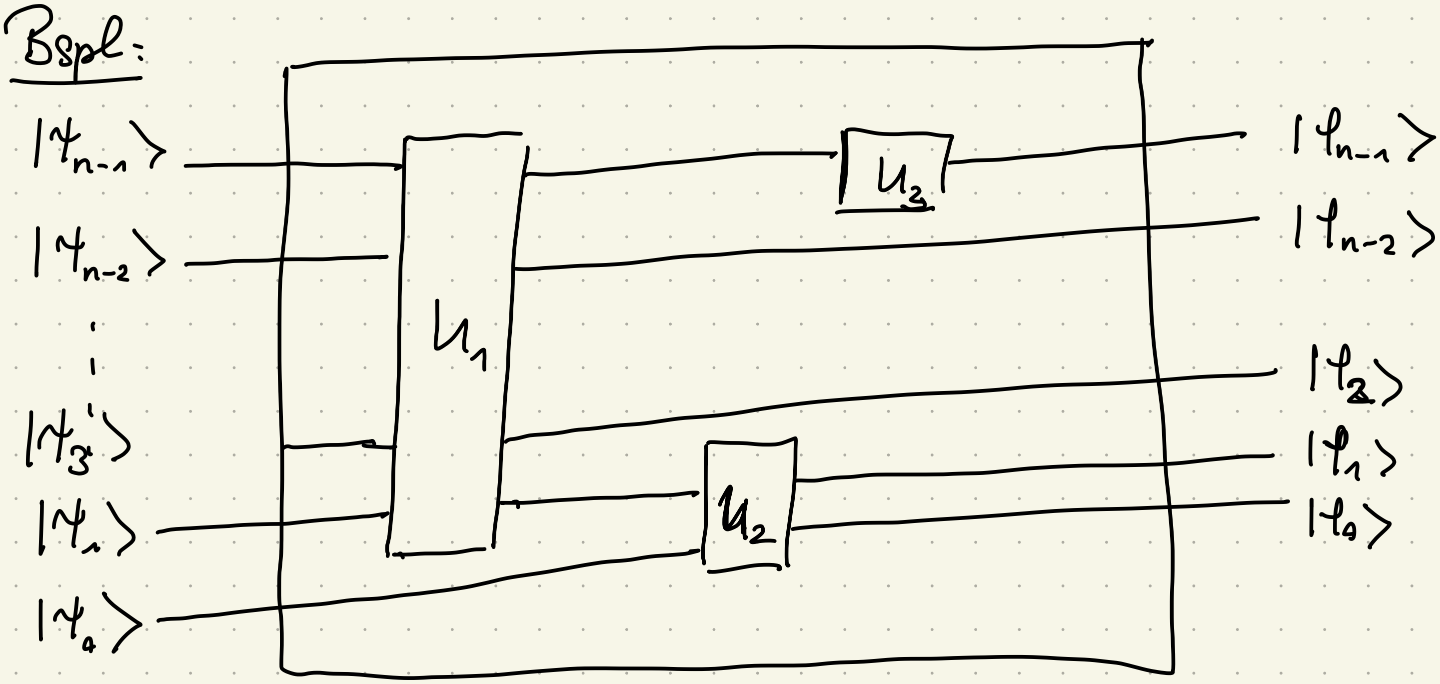
Quantengatter müssen durch unitäre Abb.

$$U : \mathcal{H}^{\otimes n} \longrightarrow \mathcal{H}^{\otimes n}$$

Definition: Ein Quanten-n-Gatter ist ein unitärer Operator

$$U : \mathcal{H}^{\otimes n} \longrightarrow \mathcal{H}^{\otimes n}.$$

Bspl:



$$|\psi_{n-1}\cdots\psi_0\rangle \longmapsto U_1|\psi_{n-1}\cdots\psi_1\rangle \otimes |\psi_0\rangle$$
$$= (U_1 \otimes id)\,|\psi_{n-1}\cdots\psi_0\rangle$$
$$\longmapsto (id \otimes U_2)\,(U_1 \otimes id)\,|\psi_{n-1}\cdots\psi_0\rangle$$
$$\longmapsto (U_3 \otimes id)(id \otimes U_2)(U_1 \otimes id)\,|\psi_{n-1}\cdots\psi_0\rangle$$

Quanten-1-Gatter

$V: \mathcal{H} \to \mathcal{H}$ unitär

Name	Symbol	Operator	Matrix
Identität	$-\!-\!-$	id	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Phasenfaktor	$-\boxed{M(\alpha)}-$	$M(\alpha) = e^{i\alpha} \cdot id$	$\begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$ $0 \leq \alpha < 2\pi$
Phasenschieber	$-\boxed{P(\alpha)}-$	$P(\alpha) = \|0\rangle\langle 0\| + e^{i\alpha}\|1\rangle\langle 1\|$	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$
Pauli-X oder Q-NOT	$-\boxed{X}-$	$X = \sigma_x$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli-Y	$-\boxed{X}-$	$Y = \sigma_y$	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli-Z	$-\boxed{Z}-$	$Z = \sigma_z$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Hadamard	$-\boxed{H}-$	$H = \frac{\sigma_x + \sigma_z}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Spindrehung um n mit Winkel α — $\boxed{D_n(\alpha)}$ — $D_n(\alpha)$ $\quad \exp\left(-i\frac{\alpha}{2}\, n\cdot\sigma\right)$

<u>Erläuterung:</u> $n \in \mathbb{R}^3$, $\|n\| = 1$, $\alpha \in \mathbb{R}$

$$n\cdot\sigma := \begin{pmatrix} n_3 & n_1 - i n_2 \\ n_1 + i n_2 & -n_3 \end{pmatrix} \in U(2)$$

<u>Übung:</u> Für alle $A \in M_n(\mathbb{R})$ mit $A^2 = E_n$ und alle $\alpha \in \mathbb{R}$ gilt:

$$\exp(i\alpha A) = \cos(\alpha \cdot E_n) + i \sin(\alpha A)$$

[Scheurer, Ü. 2.18]

$$\Longrightarrow \exp\left(-i\frac{\alpha}{2}\, n\cdot\sigma\right)$$

$$= \begin{pmatrix} \cos\left(\frac{\alpha}{2}\right) - i\sin\left(n_3\frac{\alpha}{2}\right) & -i\sin\left(\frac{\alpha}{2}(n_1 - i n_2)\right) \\ -i\sin\left(\frac{\alpha}{2}(n_1 + i n_2)\right) & \cos\left(\frac{\alpha}{2}\right) + i\sin\left(n_3\frac{\alpha}{2}\right) \end{pmatrix}$$

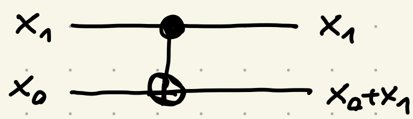
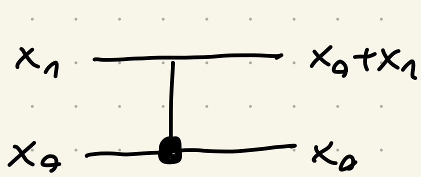
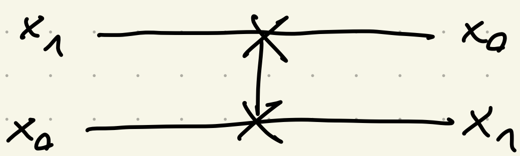
<u>Man kann zeigen:</u>

<u>Lemma:</u> Sei $U : {}^{q}\mathcal{H} \to {}^{q}\mathcal{H}$ unitär. Dann gibt es $\alpha, \xi \in \mathbb{R}$ und $n \in \mathbb{R}^3$, $\|n\| = 1$, so daß $\quad U = e^{i\alpha} D_n(\xi)$.

Quanten-2-Gatter $V: \mathcal{H}^{\otimes 2} \to \mathcal{H}^{\otimes 2}$

unitär

Wichtige Beispiele:

Name	Symbol	Operator	Matrix
C-NOT		$\lvert 0\rangle\langle 0\rvert \otimes 1 + \lvert 1\rangle\langle 1\rvert \otimes X$	$\begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0 \end{pmatrix}$
C-NOT mit Kontrolle in 2. Variablen		$1 \otimes \lvert 0\rangle\langle 0\rvert + X \otimes \lvert 1\rangle\langle 1\rvert$	$\begin{pmatrix} 1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0 \end{pmatrix}$
Swap		$\lvert 00\rangle\langle 00\rvert + \lvert 10\rangle\langle 01\rvert + \lvert 01\rangle\langle 10\rvert + \lvert 11\rangle\langle 11\rvert$	$\begin{pmatrix} 1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1 \end{pmatrix}$

Satz: Die Menge der Quantengatter

$$\mathcal{U} = \{ M, D_y, D_z, \text{C-NOT} \}$$

ist universell.

Beweis: Scherer $\blacksquare$

Bemerkung: TOF : $\mathcal{H}^{\otimes 3} \to \mathcal{H}^{\otimes 3}$ ist unitär

$\Longrightarrow$ jeder klassische Algorithmus kann quantenmechanisch realisiert werden.