Vorlesung 9

22.6.2021

Wiederholung

Quanten-n-Gatter sind unitäre Abb.

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

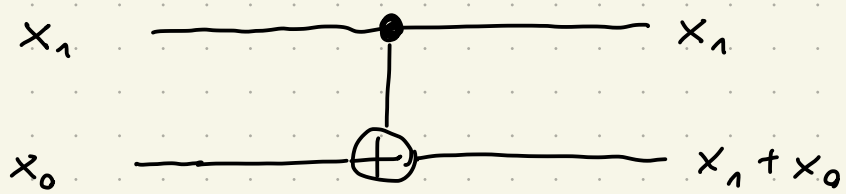
Wichtige Beispiele: Pauli X, Y, Z

↕ auch Q-NOT

$|0\rangle \mapsto |1\rangle$, $|1\rangle \mapsto |0\rangle$

Hadamard $H = \frac{X+Z}{\sqrt{2}}$, $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

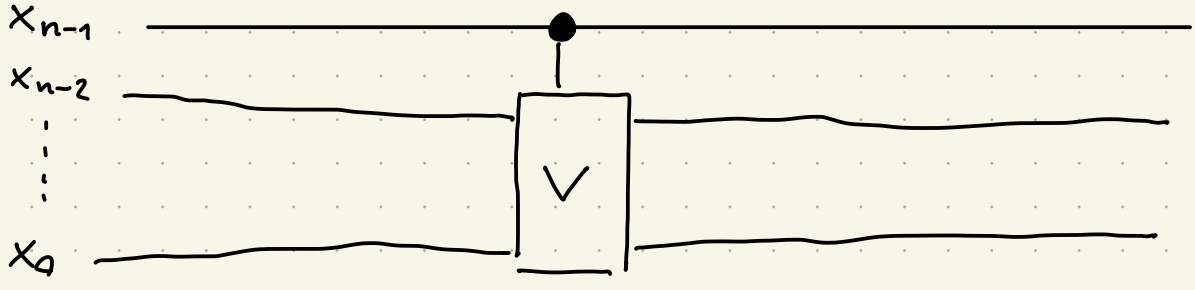
C-NOT



$$|0\rangle\langle 0| \otimes id + |1\rangle\langle 1| \otimes X$$

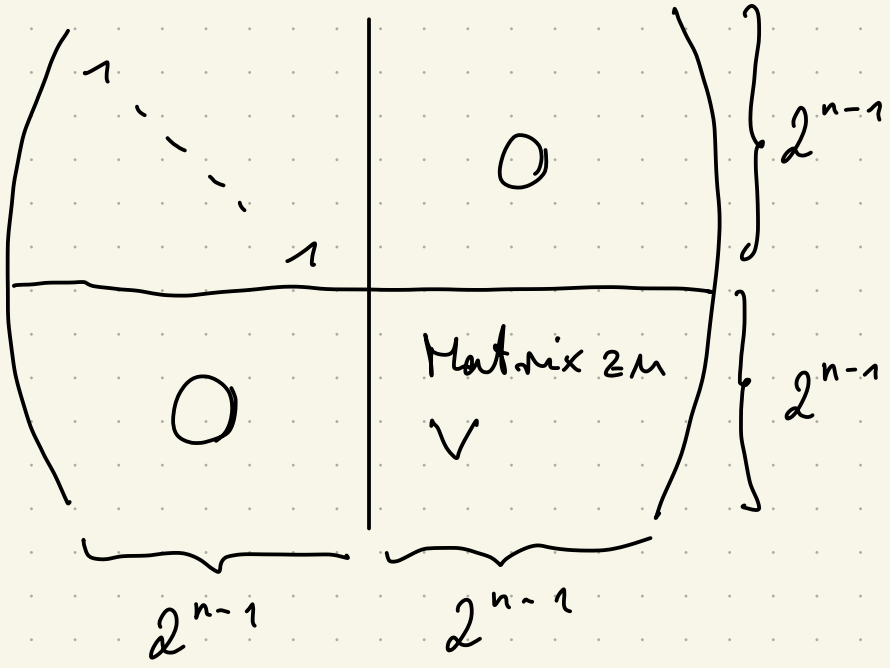
$$\begin{array}{c} \begin{matrix} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

Allgemein: $V : {}^{q}H^{\otimes n-1} \longrightarrow {}^{q}H^{\otimes n-1}$ unitär



$$|0\rangle\langle 0| \otimes id + |1\rangle\langle 1| \otimes V$$

Matrix



Der Ablauf von Quantenalgorithmen

1. Präparation des Inputregisters
2. Darstellung klassischer Funktionen f durch Quantenschaltkreise U_f
3. Transformationen des Quantenregisters durch Gatter und Schaltkreise
4. Auslesen (Beobachtung / Messung) des Resultats

Zu (1): In vielen Algorithmen will man als Input

$$|\psi_0\rangle^n := \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle^n$$

— Rechenbasis, d.h.

$|x\rangle^n = |x_{n-1}\rangle \otimes \dots \otimes |x_0\rangle$, falls

$x = x_0 + x_1 \cdot 2 + \dots + x_{n-1} 2^{n-1}$

präpariert.

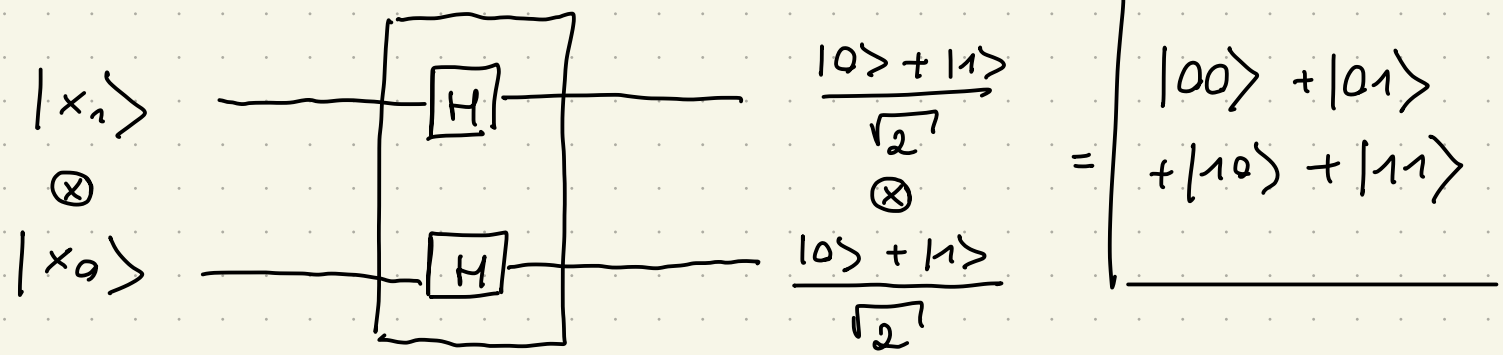
Es gilt:

$$H^{\otimes n} |0\rangle^n = \bigotimes_{i=0}^{n-1} H|0\rangle = \bigotimes_{i=0}^{n-1} \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

(*)

$$= \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle^n .$$

Graphisch im Fall $n = 2$:



Bemerkung: Im Allgemeinen wird man ein Arbeitsregister brauchen. Rechenprozess findet statt in $H^{I/O} \otimes H^{A}$

Problem: Messungen im Arbeitsregister beeinflussen das Input/Output-Register (Verschränkung).

Beispiele:

① Mini-Zufallsgenerator ($n=1$)

Initialisiere mit $|0\rangle \in {}^{?}H$.
Wende H an. Danach Messung!

Das produziert mit Wahrscheinlichkeit $\frac{1}{2}$ eine $|0\rangle$ oder eine $|1\rangle$. (Verallgemeinerung siehe oben (*))

② Algorithmus von Deutsch

Sei $B = \{0, 1\}$.
Betrachte Funktionen $f: B \to B$.
Es gibt zwei Typen:

(K) konstante Funktionen
(B) bijektive Funktionen

Frage: Ist f vom Typ (K) oder $(B)^2$?

Ein klassischer Computer muss f zweimal auswerten. Ein Quantenalgorithmus schafft es mit einer Auswertung.

Man arbeitet in $\mathcal{H}^{\otimes 2} = \mathcal{H} \otimes \mathcal{H} =: H$

Wir definieren $U_f : H \to H$ unitär durch: $B^2 \ni (a, b) \xrightarrow{U_f} (a, f(a) \text{ XOR } b) \in B^2$

	(0,0)	(0,1)	(1,0)	(1,1)
$f = id$	00	01	11	10
$f = 1$	01	00	11	10
$f = 0$	00	01	10	11
$f = NOT$	01	00	10	11

U_f induziert eine unitäre Abb. von $H \to H$ gegeben durch eine Permutationsmatrix bzgl. der Rechenbasis.

Allgemein: $g : \{0,1\}^m \to \{0,1\}^m$ bijektiv induziert stets eine unitäre Abb.

$U_g : \mathcal{H}^{\otimes m} \to \mathcal{H}^{\otimes m}$.

$$|x\rangle^m = |x_{m-1} x_{m-2} \dots x_0\rangle \mapsto |y_{m-1} \dots y_0\rangle$$

falls $f(x_{m-1}, \dots, x_0) = (y_{m-1}, \dots, y_0)$.

Algorithmus:

1. Initialisiere 2 Q-Bits als $|01\rangle$
2. Wende $H \otimes H$
3. Wende U_f
4. Wende $H \otimes H$
5. Messung! Ergebnis $|01\rangle$ bedeutet (K)
   Ergebniss $|11\rangle$ bedeutet (B)

Bem: Das Register befindet sich nach 4. in einem reinen Eigenzustand. Das macht 5. evt sinnvoll.

Analyse des Algorithmus:

Fall: f ist konstant 0

Dann ist $U_f = id$

$$(H \otimes H) \circ (H \otimes H) = H^2 \otimes H^2 = id \otimes id$$

Fall: f ist konstant 1. Dann ist U_f der Flip auf dem zweiten Bit. Auf dem ersten Bit passiert nichts. Was passiert auf dem

zweiten Bit?

$$HNH = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

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

d.h. $|01\rangle \longmapsto -|01\rangle \doteq |01\rangle$

quantenmechanisch wird der gleiche Zustand beschrieben.

Rest Übung. ∎

Die Quanten-Fourier-Transformation

Def.: Sei $H = {}^{q}H^{\otimes n}$ und $\{|j\rangle^n : 0 \le j < 2^n\}$ die Rechenbasis. Dann ist die QFT gegeben durch

$$|j\rangle^n \xmapsto{F} \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \underbrace{e^{2\pi i j k/2^n}}_{\in \mathbb{C}} |k\rangle^n$$

bzw.

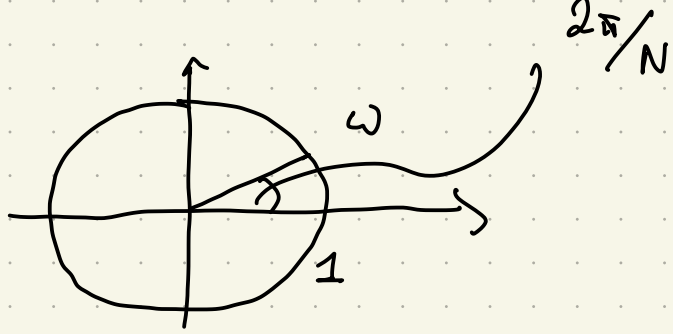
$$\sum_{j=0}^{2^n-1} \underbrace{x_j}_{\in \mathbb{C}} |j\rangle^n \xmapsto{F} \frac{1}{\sqrt{2^n}} \sum_j x_j \sum_k e^{2\pi i jk/2^n} |k\rangle^n$$

$$= \sum_k \underbrace{\left(\frac{1}{\sqrt{2^n}} \sum_j x_j e^{2\pi i jk/2^n} \right)}_{y_k \in \mathbb{C}} |k\rangle^n$$

$y_0, \dots, y_{2^n-1}$ ist die diskrete FT von $x_0, \dots, x_{n-1}$

Lemma: Die QFT ist unitär.

Beweis: Sei $N = 2^n$ und $\omega = e^{2\pi i/N}$



Dann gilt:

$$|j\rangle^n \longmapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{jk} |k\rangle^n$$

$\Rightarrow$ bez. der Rechenbasis (ON-Basis) hat die QFT die Matrix

$$\frac{1}{\sqrt{N}} \left(\omega^{jk} \right)_{0 \le k,j < N} \qquad (*)$$

Wir berechnen das Skalarprodukt zwischen den Spalten zu j_1 und j_2:

$$\frac{1}{N} \sum_{k=0}^{N-1} \omega^{j_1 k} \overline{\omega^{j_2 k}} = \frac{1}{N} \sum_{k=0}^{N-1} \omega^{j_1 k} \omega^{-j_2 k}$$

$$= \frac{1}{N} \sum_{k=0}^{N-1} \left(\omega^{(j_1 - j_2)} \right)^k \overset{!}{=} \begin{cases} 1, & j_1 = j_2 \\ 0, & j_1 \neq j_2 \end{cases}$$

$\Rightarrow (*)$ ist unitär.

Zum !: Folgt aus

$$(X^N - 1) = (X-1)(X^{N-1} + X^{N-2} + \dots + X + 1)$$

Sei $\zeta \neq 1$ eine N-te EHW, d.h. $\zeta^N = 1$.

Einsetzen liefert: $0 = \underbrace{(\zeta - 1)}_{\neq 0} (\zeta^{N-1} + \dots + \zeta + 1)$

$$\Rightarrow \sum_{k=0}^{N-1} \zeta^k = 0.$$

∎

Bemerkung: Es gilt:

$$|k\rangle^n \xrightarrow{F^{-1}} \frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} \overline{\omega}^{sk} |s\rangle^n$$

Beweis: Übung!

Definition: Wir schreiben für $a_1, \dots, a_m \in \{0,1\}$

$$0.a_1 a_2 \dots a_m := \frac{a_1}{2} + \frac{a_2}{2^2} + \dots + \frac{a_m}{2^m}$$

$$= \sum_{\ell=1}^{m} a_\ell \cdot 2^{-\ell}.$$

Lemma: Sei $x = \sum_{j=0}^{n-1} x_j \cdot 2^j$. Dann ist

$$F|x\rangle^n = \frac{1}{\sqrt{N}} \bigotimes_{j=0}^{n-1} \left[|0\rangle + e^{2\pi i 0.x_j \dots x_0} |1\rangle \right].$$

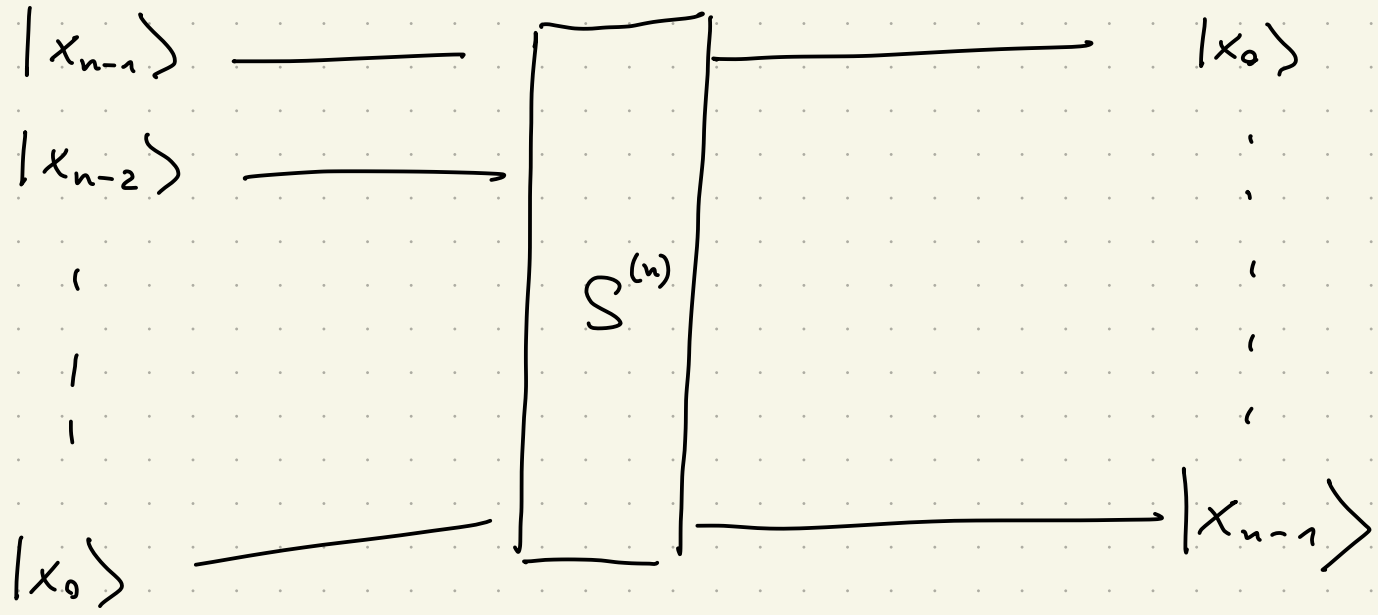
$N = 2^n$

Beweis: Rechnung, [Scherer, ~S. 183] ∎

Viele Rechnungen führen zu Phasenschieber

$$F = S^{(n)} \prod_{j=0}^{n-1} \left(\left[\prod_{k=0}^{j-1} P_{jk} \right] H_j \right)$$

$$= S^{(n)} H_0 P_{10} H_1 \cdots P_{n-1,0} \cdots P_{n-1,n-2} H_{n-1}$$


$|x_{n-1}\rangle$
$|x_{n-2}\rangle$
$|x_0\rangle$
$S^{(n)}$
$|x_0\rangle$
$|x_{n-1}\rangle$