Nachtrag Letzte Vorlesung

- Messung von A mit Ergebnis α, β, γ oder δ projeziert System auf entsprechenden EV $|\Psi^-\rangle_{12}$, $|\Psi^+\rangle_{12}$, ... und entsprechenden Zustand bei Bob. z.B Ergebnis $\alpha \rightarrow |\Psi\rangle_{123} = |\Psi^-\rangle_{12}(a|+\rangle_3 + b|-\rangle_3)$
- Alice teilt Bob mit klassischer Datenübertragung das Ergebnis der Messung mit.
- bei Ergebnis α → bei B $|\Psi\rangle_3 = -(a|+\rangle_3 + b|-\rangle_3) = -\begin{pmatrix} a \\ b \end{pmatrix}$

⇒ Teleportation ist erfolgt.

bei Ergebnis β → $|\Psi\rangle_3 = -\begin{pmatrix} a \\ -b \end{pmatrix}$ Bob drehrt mit σ_z → $\sigma_z \begin{pmatrix} a \\ -b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$

bei Ergebnis γ → $|\Psi\rangle_3 = \begin{pmatrix} b \\ a \end{pmatrix}$ σ_x → $\sigma_x \begin{pmatrix} b \\ a \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$

δ → $|\Psi\rangle_3 = \begin{pmatrix} -b \\ a \end{pmatrix}$ σ_y → $\sigma_y \begin{pmatrix} -b \\ a \end{pmatrix} = -i\begin{pmatrix} a \\ b \end{pmatrix}$

Anwendung in Quantenkryptographie

3.5 Konzepte eines Quantencomputers

Klassische Computer

Bit : 0 oder 1

Register : jedes Bit → binäre Darstellung 00100 = 4

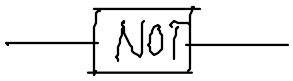
Programm: aufgebaut aus Serie von Gattern

Gatter

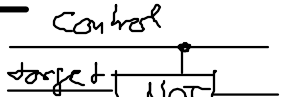
1-Bit Gatter

NOT

1	→ 0
0	→ 1



2-Bit Gatter



CNOT

c	t	
0	0	0 0
0	1	→ 0 1
1	0	1 1
1	1	1 0

NAND (nur 1 weiteres Element noch für alle Schaltungen)

SWAP

00	00
01	→ 10
10	01
11	11

Quantencomputer

Quantenbits: $0 \hat{=} |+\rangle$, $1 \hat{=} |-\rangle$

neu: Superposition $\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ sowohl 0 als auch 1

Superposition aller Zahlen ist möglich

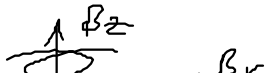
(bei N-Qubit von 0 bis $2^N - 1$ Zahlen)

$$\frac{1}{2^{\frac{N}{2}}} \sum_{u=0}^{2^N-1} |u\rangle = \frac{1}{2^{\frac{N}{2}}} (|+\rangle_1 + |-\rangle_1) \otimes (|+\rangle_2 + |-\rangle_2) \dots \otimes (|+\rangle_N + |-\rangle_N)$$

- kann parallel berechnet werden $\Rightarrow$ massiver Zeitgewinn
- Aus Lösemöglichkeiten sind begrenzt (nur N-Qubit auslesen)

$\Rightarrow$ Gewinn i. A. wieder verloren

Quantengates und Programm



ideales Hamilton Operator $\mu = g \frac{\mu_B}{2}$

$$H = \sum_{i=1}^{N} \left(-\mu B_x^{(i)}(t) \sigma_x^{(i)} - \mu B_z^{(i)}(t) \sigma_z^{(i)} \right) - \sum_{i \neq j}^{N} J^{(ij)}(t) \left(\sigma_+^{(i)} \sigma_-^{(j)} + \sigma_-^{(i)} \sigma_+^{(j)} \right)$$

① Präparier Anfangszustand: z.B. alle Spins in $|+\rangle$

② schalte alle $B_x^{(i)}(t)$ und $J^{(ij)}(t)$ aus, außer $B_x^{(j)} \neq 0$

$\Rightarrow U(t,0) = \exp\left[i \frac{\mu B_x^{(j)}}{\hbar} t \, \sigma_x \right] = \exp[i \gamma \sigma_x]$ mit $\gamma = \frac{\mu B_x^{(j)}}{\hbar} t$

$U(t) = \cos\gamma + i \sin\gamma \, \sigma_x$ **wähle** $\gamma = \frac{\pi}{2}$ Produkt B_x und t

$\Rightarrow U(t) = i\sigma_x \hat{=} i\text{NOT}$

wähle $\gamma = \frac{\pi}{4}$ $\Rightarrow U(t) = \frac{1}{\sqrt{2}} (\mathbb{1} + i\sigma_x) = \sqrt{i\text{NOT}}$

$\sqrt{i\text{NOT}} |+\rangle = \frac{1}{\sqrt{2}} (|+\rangle + i|-\rangle)$

Quantengates

③ Mit $B_z^{(j)}$ können Phasen verschoben werden

④ Schalte nun ein $J^{(ij)}$ an $\quad \delta = \frac{J^{(ij)} t}{\hbar}$

$$U(t) = \exp\left[\frac{i}{\hbar} J^{(ij)} t \left(\sigma_+^{(i)} \sigma_-^{(j)} + \sigma_-^{(i)} \sigma_+^{(j)} \right) \right]$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\delta & i\sin\delta & 0 \\ 0 & i\sin\delta & \cos\delta & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

für $\delta = \frac{\pi}{2} \rightarrow U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = i\,\text{SWAP}$

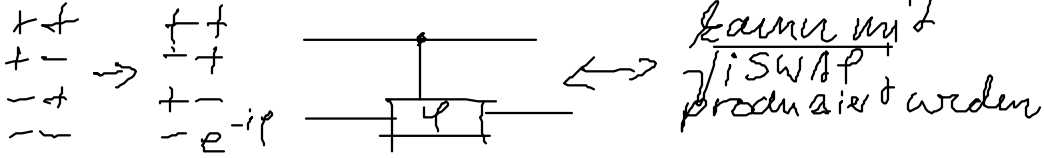
$\delta = \frac{\pi}{4}$ $\quad U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} & 0 \\ 0 & \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \sqrt{i\,\text{SWAP}}$

Mit den Gattern, die hier vorgestellt waren, können alle Rechenschritte eines klassischen oder Quanten computers durchgeführt werden.

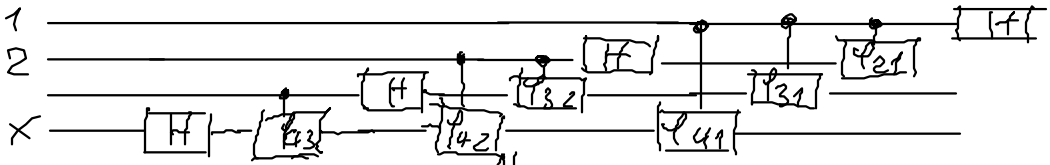
Beispiel: Quantentransformation

Hadamard Gate $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \exp\left[-i\frac{\pi}{2}\left(\frac{\sigma_x + \sigma_z - 1}{\sqrt{2}}\right)\right]$ — H —

Controlled phasenshift



Qubit H φ



Eingangszustand $\sum_{x=0}^{2^N-1} a_x |x\rangle$

$c_n = \frac{1}{2^N}\sum_{x=0}^{2^N-1} \exp\left[i\frac{2\pi}{2^N}nx\right]\cdot a_x$ diskrete Fourier Trafo

- Zahl der Gatter wächst wie Potenz $\sim N^2$
- klassische FTrafo exponentiell $\sim 2^N$

⇒ Es gibt Probleme bei denen Rechenzeit eines klassischen Computers exponentiell mit Größe der Zahlen wächst

z.B. Faktorisierung großer ganzer Zahlen $n = p\cdot q$, $p = ?, q = ?$
(120 dezimalstellen → 3 Monate)
dieses Lösung auf Q. Comp. nur wie Potenz wächst

z.B. Faktorisierung mit Shor'scher Algo
(FT ist Teil des Shor'schen Algorithmus)

Realisierung

① mit einzelnen Elektronenspins in Quantenpunkten

↑ ↗ ↘ ↑

② mit effektiven Q.M. 2-Niveau System z.B supraleitende Bauelementen (z.B Ustinov Physik Hochhaus)

③  NMR mit geeigneten Molekülen

- alle Atome verschieden ⇒ verschiedene lokale Felder
- einzeln adressieren des Kernspins, durch Einstellen der Resonanzfrequenz
- an Molekülen mit 7 Kernspins ist der Shor'sche Algorithmus demonstriert worden (≈2000) $15 = 3 \cdot 5$
  Q.C. in einer Kaffeetasse

(4) Atome oder Ionen in Fallen

- Einzelne 2-Zustandsatome können separat durch Laser manipuliert werden ≈ 10 Qubits