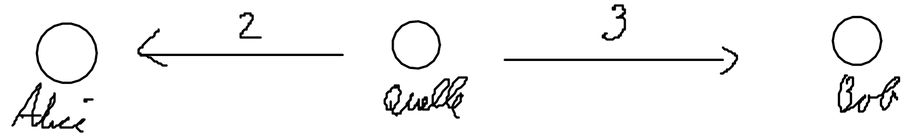
Quantenteleportation

Zustand $|\phi\rangle_1 = \alpha|+\rangle_1 + \beta|-\rangle_1$

soll instantan teleportiert werden



$$|\psi\rangle_{23} = \frac{1}{\sqrt{2}}\left(|+\rangle_2|-\rangle_3 - |-\rangle_2|+\rangle_3\right)$$

$$A = \alpha|\Psi^-\rangle_{12}\,{}_{21}\langle\Psi^-| + \beta|\Psi^+\rangle_{12}\,{}_{12}\langle\Psi^+| + \gamma|\phi^-\rangle_{12}\,{}_{21}\langle\phi^-| + \delta|\phi^+\rangle_{12}\,{}_{12}\langle\phi^+|$$

$$|\psi\rangle_{123} = |\phi\rangle_1 \otimes |\phi\rangle_{23}$$

$$= \ldots$$

$$\begin{aligned}
= \frac{1}{2}\Big\{ & -|\Psi^-\rangle_{12} \otimes (a|+\rangle_3 + b|-\rangle_3) \\
& -|\Psi^+\rangle_{12} \otimes (a|+\rangle_3 - b|-\rangle_3) \\
& +|\phi^-\rangle_{12} \otimes (a|-\rangle_3 + b|+\rangle_3) \\
& +|\phi^+\rangle_{12} \otimes (a|-\rangle_3 - b|+\rangle_3)
\end{aligned}$$

Messung mit A (mit EW α, β, γ oder δ) projeziert System auf entsprechenden EV $|\Psi^-\rangle_{12}$, $|\Psi^+\rangle_{12}$ oder $|\phi^-\rangle_{12}$ oder $|\phi^+\rangle_{12}$

und entsprechenden Zustand bei Bob.

Alice teilt Bob mit klassischer Datenübertragung das Ergebnis der Messung mit

z.B. Ergebnis α $\Rightarrow$ bei B

$$|\psi\rangle_3 = -(a|+\rangle_3 + b|-\rangle_3) = -\begin{pmatrix} a \\ b \end{pmatrix}$$

β: $\Rightarrow |\psi\rangle_3 = -\begin{pmatrix} a \\ -b \end{pmatrix} \xrightarrow[\text{B dreht mit } \sigma_z]{} \sigma_z\begin{pmatrix} a \\ -b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$

γ: $|\psi\rangle_3 = \begin{pmatrix} b \\ a \end{pmatrix} \xrightarrow[\sigma_x]{} \sigma_x\begin{pmatrix} b \\ a \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$

δ: $|\psi\rangle_3 = \begin{pmatrix} -b \\ a \end{pmatrix} \underset{\sigma_y}{\Rightarrow} \quad \sigma_y \begin{pmatrix} -b \\ a \end{pmatrix} = -i \begin{pmatrix} a \\ b \end{pmatrix}$

Wozu ist das gut?

9.5 Konzepte eines Quantencomputers

Klassisch: Bit 0 oder 1

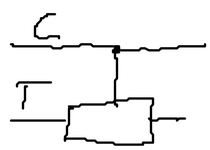
Register: viele Bits   Binäre Darstellung

Gatter: 1 bit Gatter

NOT $1 \to 0$
      $0 \to 1$

2-Bit Gatter   CNOT

C	T		C	T
0	0	→	0	0
0	1	→	0	1
1	0	→	1	1
1	1	→	1	0



$\Longleftrightarrow$ NAND im klass. Comput.

SWAP

0	0	→	0	0
0	1	→	1	0
1	0	→	0	1
1	1	→	1	1

0	0	→	1
0	1	→	1
1	0	→	1
1	1	→	0

?

Quantencomputer

Q-Bits $0 \mathrel{\hat{=}} |+\rangle$
         $1 \mathrel{\hat{=}} |-\rangle$

neu: Superposition $\frac{1}{\sqrt{2}}\left(|+\rangle + |1\rangle\right)$

sowohl 0 als auch 1

⇒ Superposition aller Zahlen von 0 bis $2^N - 1$
mit N Qbits

$$\frac{1}{2^{N/2}} \sum_{n=0}^{2^N-1} |\text{"}n\text{"}\rangle = \frac{1}{2^{N/2}} \left(|+\rangle_1 + |-\rangle_1\right) \otimes \left(|+\rangle_2 + |-\rangle_2\right) \otimes \ldots$$

Kann parallel bearbeitet werden ⇒ massiver Gewinn

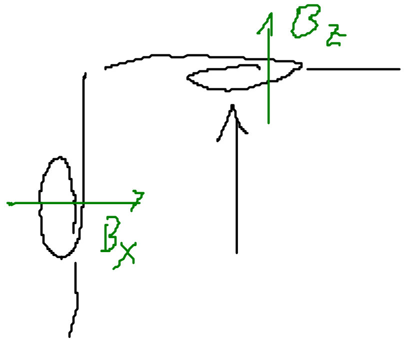
aber: Auslesemöglichkeiten begrenzt,
nur N Qbits können gemessen werden
i.A. geht der Gewinn wieder verloren.

Quantengatter und Programme

idealer Hamilton-Operator

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

$\mu = -g\frac{\mu_B}{2}$



$\uparrow \quad \uparrow \quad \Longrightarrow \quad \upuparrows$

γ klein $\qquad\qquad$ γ groß

1) präpariere Anfangszustand: z.B. alle Spins im Zustand $|+\rangle$

2) Schalte alle $B_{x\,z}^{(i)}(t)$ und $\gamma^{(ij)}(t)$ aus außer $B_x^{(i)} \neq 0$ (ein B)

$$\Longrightarrow U(t,0) = \exp\left(i\mu\frac{B_x}{\hbar}\,\sigma_x\right) = \exp(i\gamma\sigma_x)$$

$$\gamma = \frac{\mu B_x^{(i)}\, t}{\hbar}$$

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

$$\Longrightarrow U(t) = i\sigma_x \overset{?}{\hat{=}} i\,NOT$$

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

neues Gatter

$$\sqrt{i\,NOT}\;|+\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle + i\,|-\rangle\right)$$

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

($z.B.$ $i\,NOT \Rightarrow NOT$)

4) 2 Bit Gatter

Schalte nur ein $J^{(ij)}$ an

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

$$\delta = \frac{J^{(ij)} t}{\hbar} \qquad \begin{pmatrix} 1 & & & 0 \\ & \cos\delta & i\sin\delta & \\ & i\sin\delta & \cos\delta & \\ 0 & & & 1 \end{pmatrix}$$

in Basis $|++\rangle$, $|+-\rangle$, $|-+\rangle$, $|--\rangle$

für $\delta = \frac{\pi}{2}$ $\Rightarrow$ $i\,SWAP$

($+\,B_z \Rightarrow SWAP$)

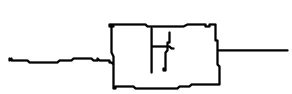
oder für $\delta = \frac{\pi}{4}$ $\rightarrow$ $U = \begin{pmatrix} 1 & & & 0 \\ & 1/\sqrt{2} & i/\sqrt{2} & \\ & i/\sqrt{2} & 1/\sqrt{2} & \\ 0 & & & 1 \end{pmatrix} = \sqrt{i\,SWAP}$

$\Rightarrow$ SWAP ist äquivalent zu NAND (?)

Mit diesen Gattern lassen sich alle klassischen Schaltungen aufgebaut werden. Dazu auch die Operationen eines Quantencomputers

Beispiel: Quantenfouriertrafo

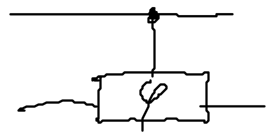
brauche Hadamard-Gate $\quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$



$$= \exp\left(-i\frac{\pi}{2}\left(\frac{\sigma_x + \sigma_z}{\sqrt{2}} - 1\right)\right)$$

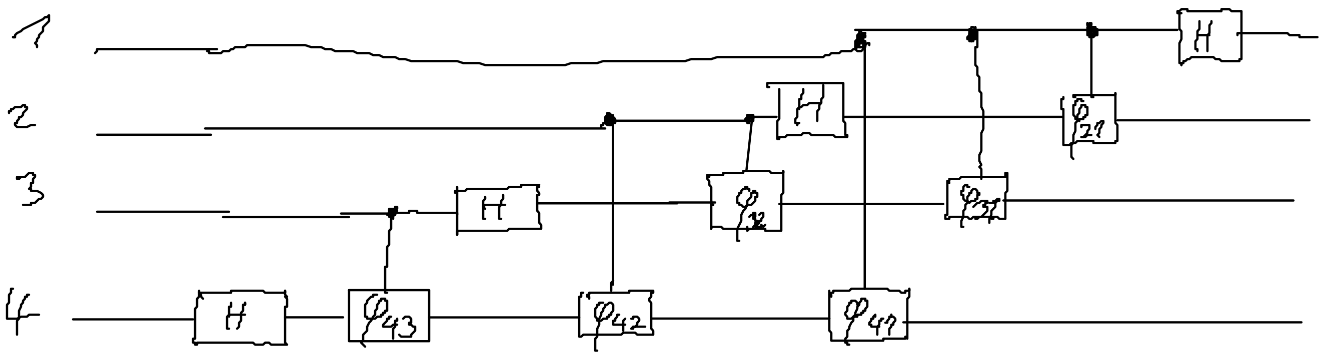
controlled phase shift

$$
\begin{array}{lcl}
++ & \longrightarrow & ++ \\
+- & \longrightarrow & +- \\
-+ & \longrightarrow & -+ \\
-- & \longrightarrow & --e^{i\varphi}
\end{array}
$$



$\Longleftrightarrow \sqrt{iSWAP}$

Qbit



Anfangszustand

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

$$\Longrightarrow \quad c_k = \frac{1}{2^N} \sum_{x=0}^{2^N-1} \exp\left(i\, \frac{2\pi k x}{2^N}\right) a_x \qquad \text{diskrete FT}$$

Zahl der Gatter $\sim N^2$ // klassisch 2^N

Es gibt Probleme, bei der die Rechenzeit eines klass. Comp. exponentiell mit der Größe der Zahlen wächst

z.B. $n = p \cdot q$, $p = ?$, $q = ?$

p prim, q prim

deren Lösung auf Quantencomp. nur wie eine Potenz.

Bsp Faktorisierung Shor

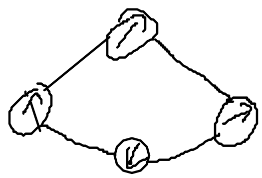
(QFT ist teil des Shor-Algorithmus)

Realisierung

1) mit einzelnen Elektronenspins in
Quantenpunkten

2) mit effektiven QM. 2-Niveau System
z.B. supraleitenden Bauelementen
(z.B. Ustinov PI)

3) NMR mit geeigneten Molekülen,
alle Atome verschieden
⇒ verschiedene Resonanz



Einstellen der Spins durch
verwenden der jeweiligen Resonanz

an Molekülen mit 7 (4 ?) Kernspins ist der
Shor-Algorithmus demonstriert worden
⇒ $15 = 3 \cdot 5$ "Quantencomp. in Kaffetasse"

4) Atome in Fallen
Einzelne 2 Zustands Atome können durch
Laser manipuliert werden (10 Qubits)