Hauptseminar „Quantum Computing“

Quantengatter und Schaltkreise

Florian Echtler
<echtler@fs.tum.de>

9. Januar 2003

Übersicht

0. Einführung
1. Quantengatter
    1.1. Grundmerkmale
    1.2. wichtige Ein–Qubit–Gatter
    1.3. wichtige Mehr–Qubit–Gatter
2. Quantenschaltkreise
    2.1. Grundmerkmale
    2.2. Beispielschaltkreise
    2.3. physikalische Realisierung
3. Fragen

Qubit: Quantensystem mit 2 Basisvektoren ($|0\rangle$ und $|1\rangle$)

Zustand des Qubits: Linearkombination der Basisvektoren

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (\alpha,\beta \in \mathbb{C})$$

Quantensystem mit n Qubits

$\Rightarrow$ Hilbertraum mit 2^n Basisvektoren

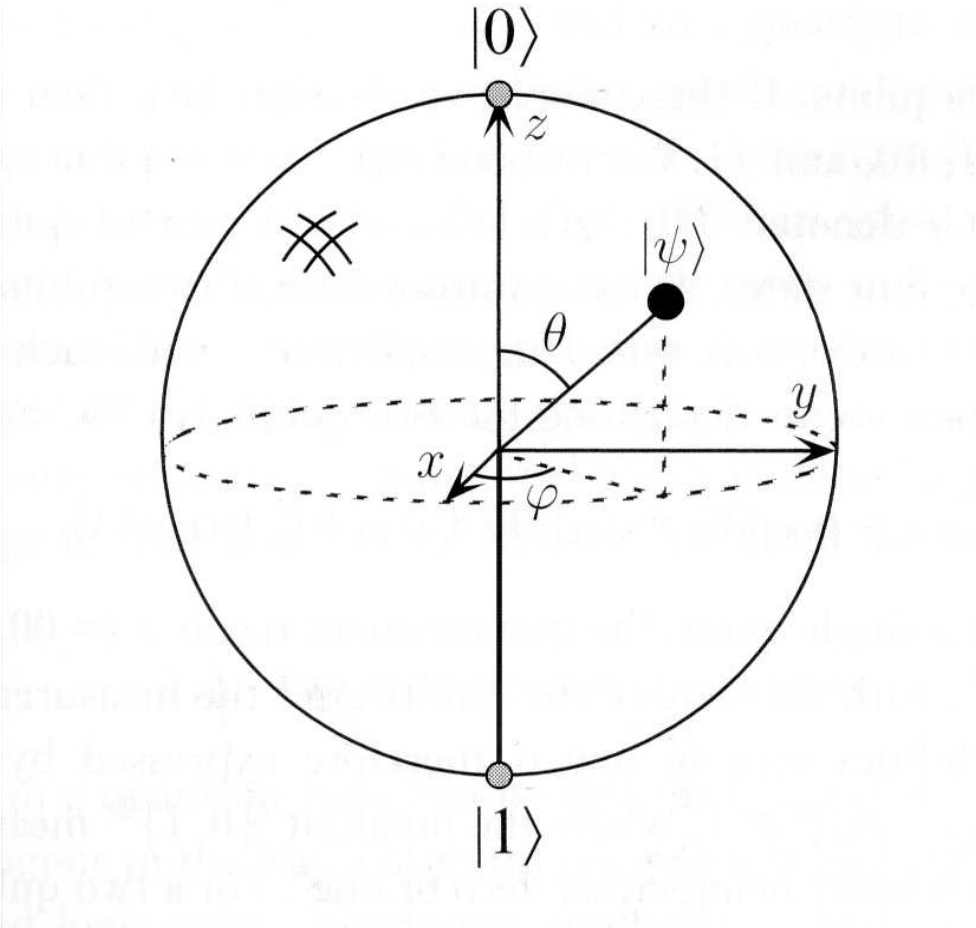
z.B. zwei Qubits:

$$\begin{aligned}|\Psi_1\rangle|\Psi_2\rangle &= (\alpha_1|0\rangle + \beta_1|1\rangle)(\alpha_2|0\rangle + \beta_2|1\rangle) = \\ &= \alpha_1\alpha_2|0\rangle|0\rangle + \alpha_1\beta_2|0\rangle|1\rangle + \beta_1\alpha_2|1\rangle|0\rangle + \beta_1\beta_2|1\rangle|1\rangle = \\ &= \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \\ &= |\Psi'\rangle\end{aligned}$$

Blochkugel

$$|\Psi> = e^{i\gamma}\left(\cos\frac{\theta}{2}|0> + e^{i\phi}\sin\frac{\theta}{2}|1>\right)$$

$$|\Psi> = \cos\frac{\theta}{2}|0> + e^{i\phi}\sin\frac{\theta}{2}|1>$$



Grundmerkmale

Quantengatter sind quadratische 2^n x 2^n –Matrizen,
die auf n Qubits operieren.

Anforderung: unitär, d.h. $U^\dagger U = I$
($U^\dagger$ bedeutet die adjungierte, d.h. komplex konjugierte
und transponierte Matrix)

Grund: Operation muss längeninvariant sein, $|x| = 1 = |x'|$
für jedes Qubit x

Ein–Qubit–Gatter: Pauli–Matrizen

Pauli–X (NOT): $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = X \,,\; X*(\alpha|0>+\beta|1>) = (\beta|0>+\alpha|1>)$

Pauli–Y: $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = Y \,,\; Y*(\alpha|0>+\beta|1>) = (-i\beta|0>+i\alpha|1>)$

Pauli–Z: $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z \,,\; Z*(\alpha|0>+\beta|1>) = (\alpha|0>-\beta|1>)$

Hadamard, Phase, $\pi/8$

Hadamard: $$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = H,\ H*(\alpha|0>+\beta|1>) = \frac{1}{\sqrt{2}}((\alpha+\beta)|0>+(\alpha-\beta)|1>)$$

Phase: $$\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix} = S,\ S*(\alpha|0>+\beta|1>) = (\alpha|0>+i\beta|1>)$$

$\pi/8$: $$\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix} = T,\ T*(\alpha|0>+\beta|1>) = (\alpha|0>+e^{i\pi/4}\beta|1>)$$

$$T = e^{i\frac{\pi}{8}}\begin{bmatrix}e^{-i\frac{\pi}{8}} & 0\\ 0 & e^{i\frac{\pi}{8}}\end{bmatrix}$$

Eigenschaften des Hadamard–Gatters

Hadamard–Gatter: auch bekannt als $\sqrt{NOT} = \begin{bmatrix} \frac{1}{2} - \frac{1}{2}i & \frac{1}{2} + \frac{1}{2}i \\ \frac{1}{2} + \frac{1}{2}i & \frac{1}{2} - \frac{1}{2}i \end{bmatrix}$

obwohl $H^2 = I \neq X$

transformiert $|0\rangle$ *bzw.* $|1\rangle$ *nach* $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ *bzw.* $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Bei diesen Zuständen ist bei der Messung $p(|0\rangle) = p(|1\rangle) = 0.5$

Zerlegung von Ein–Qubit–Gattern

$$U = e^{i\alpha} \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix} \begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix} \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix}$$

wobei $\alpha, \beta, \gamma, \delta \in \mathbb{R}$

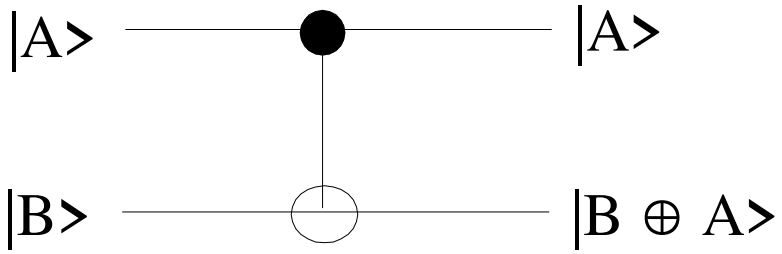
Term 1: Phasenverschiebung

Term 2–4: Rotationen/Spiegelung

Mehr–Qubit–Gatter: Controlled NOT

$$U_{cn} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

z.B. $|00\rangle \rightarrow |00\rangle$
$|01\rangle \rightarrow |01\rangle$
$|10\rangle \rightarrow |11\rangle$
$|11\rangle \rightarrow |10\rangle$



Das einfachste Gatter mit mehreren Qubits ist das Controlled NOT Gate.
Mit dem CNOT und den Ein–Qubit–Gattern Hadamard, Phase, $\pi/8$ lässt sich jedes andere Mehr–Qubit–Gatter simulieren, diese Gattermenge ist universell.

Universelle Gattermenge

Beweisskizze:

– Gatter auf 2–elementigem Unterraum sind universell

$$U = M_1 * M_2 * M_3 ... * M_n \; wobei \; M = \begin{bmatrix} a & 0 & .. & 0 & b \\ 0 & 1 & 0 & .. & 0 \\ .. & .. & .. & .. & .. \\ 0 & .. & 0 & 1 & 0 \\ c & 0 & 0 & 0 & d \end{bmatrix}$$

– CNOT und Ein–Qubit–Gatter sind universell

$$M = A_1 * A_2 * A_3 * .. * A_n \; wobei \; A \in \left\{ CNOT, N_{2,2} \right\}$$

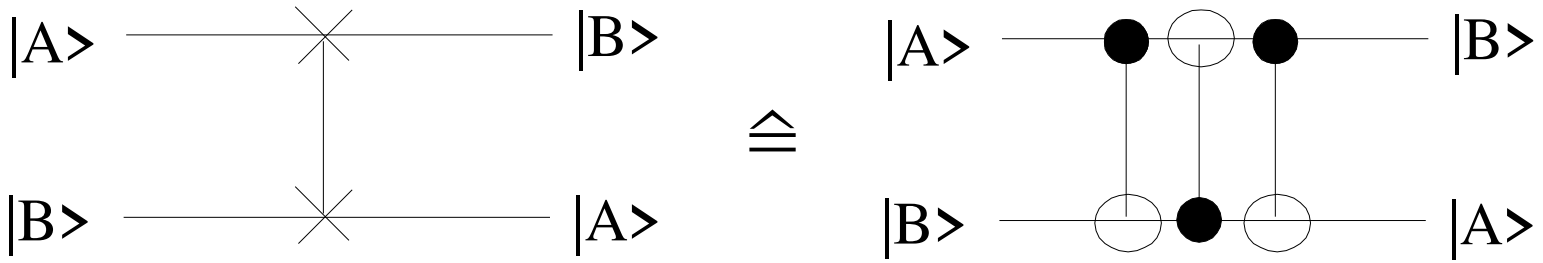
– Hadamard, Phase und $\pi/8$ nähern alle anderen Ein–Qubit–Gatter beliebig genau

$$N_{2,2} = B_1 * B_2 * B_3 * ... * B_n \; wobei \; B \in \left\{ H, S, T \right\}$$

Mehr–Qubit–Gatter: Swap–Gatter

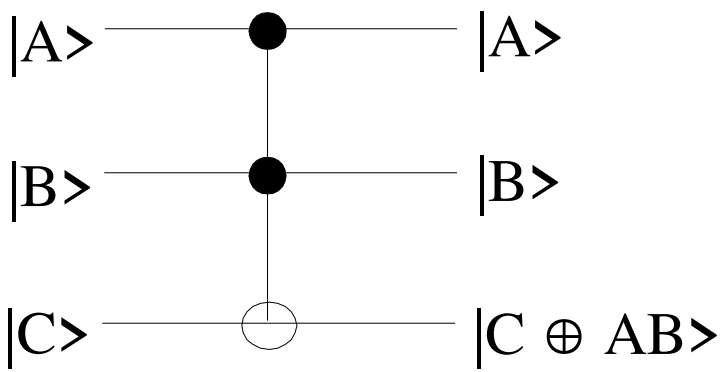
$$U_{cn} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

z.B. $|00\rangle \rightarrow |00\rangle$
$|01\rangle \rightarrow |10\rangle$
$|10\rangle \rightarrow |01\rangle$
$|11\rangle \rightarrow |11\rangle$



$$|a,b\rangle \rightarrow |a,a\oplus b\rangle \rightarrow |a\oplus(a\oplus b),a\oplus b\rangle = |b,a\oplus b\rangle \rightarrow |b,(a\oplus b)\oplus b\rangle = |b,a\rangle$$

Mehr–Qubit–Gatter: Toffoli



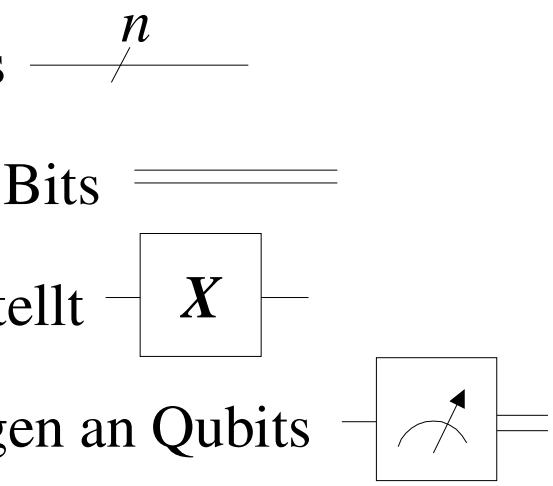
$$U_T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Das Toffoli–Gatter kann ein klassisches NAND–Gatter simulieren.
Dazu ist C = 1 und der Ausgang damit (1⊕ AB) = !(AB).
Ebenso ist die FANOUT–Funktion möglich (A=1,C=0).

Mit diesen beiden Funktionen ist die Implementation klassischer Schaltkreise möglich, da das NAND–Gatter universell ist.

Symbolik von Quantenschaltkreisen

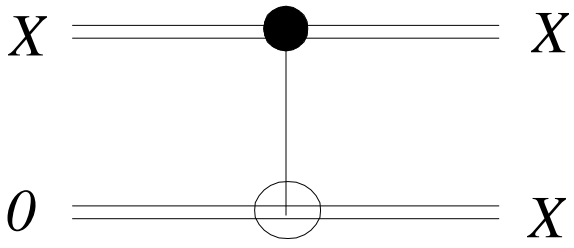
- einfache Linien bezeichnen Qubits,
- Einzellinien mit Querstrich n Qubits
- Doppellinien bezeichnen klassische Bits
- Gatter werden als Rechtecke dargestellt
- Zeigersymbole bezeichnen Messungen an Qubits



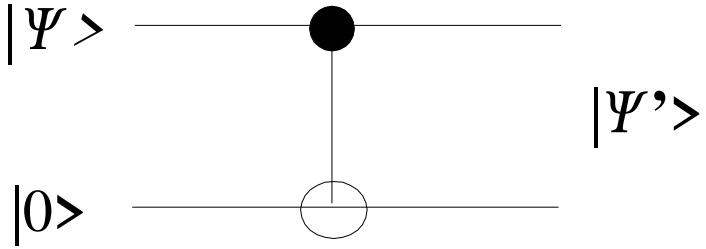
Eigenschaften von Quantenschaltkreisen

- azyklisch, kein Feedback von anderen Teilen des Schaltkreises
- alle Operationen müssen reversibel sein
- FANOUT verboten bzw. unmöglich

Qubit–Kopie?



klassisches Modell



Quantenmodell

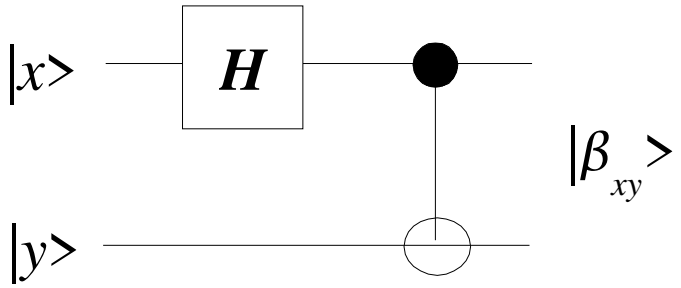
$|\Psi\rangle = a|0\rangle + b|1\rangle$

$|\Psi\rangle|0\rangle = [a|0\rangle + b|1\rangle]\,|0\rangle = a|00\rangle + b|10\rangle$

$\Rightarrow \quad |\Psi'\rangle = a|00\rangle + b|11\rangle$, aber:

$|\Psi\rangle|\Psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle \neq |\Psi'\rangle$

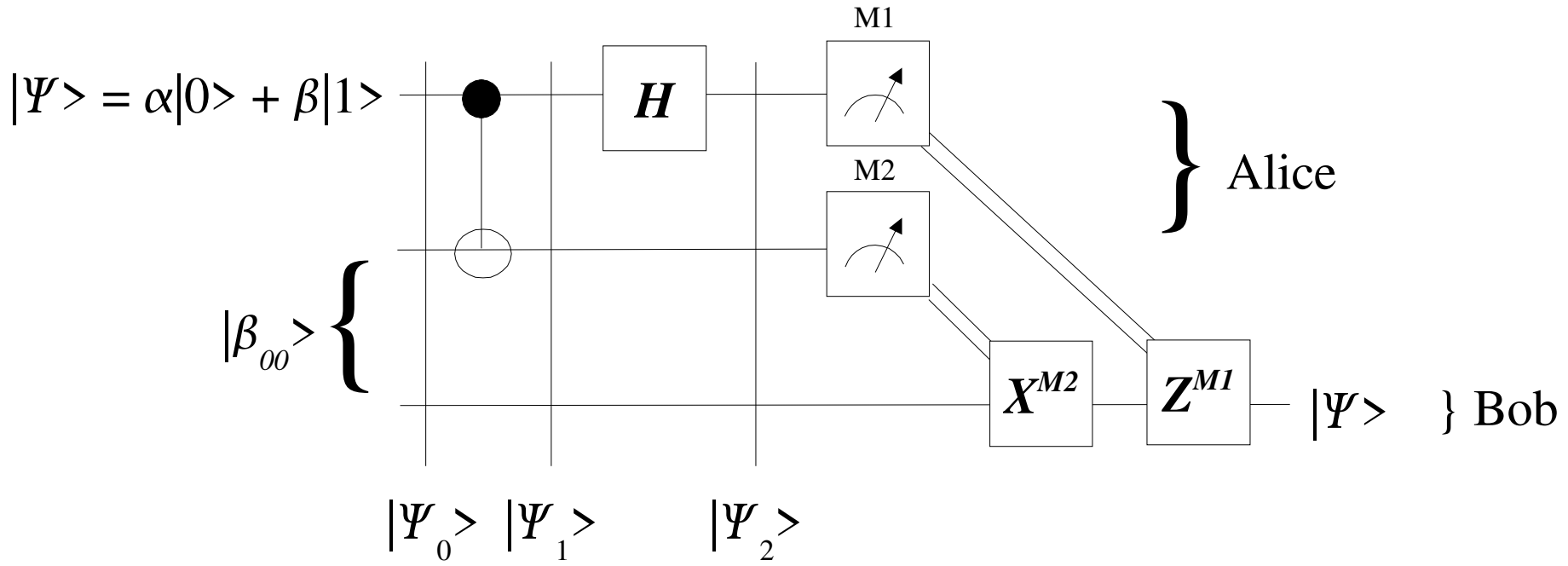
Erzeugung von EPR–Paaren



$$|\beta_{xy}\rangle = \frac{|0,y\rangle + (-1)^x |1,\overline{y}\rangle}{\sqrt{2}}$$

z.B. $$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

Teleportation eines Qubit



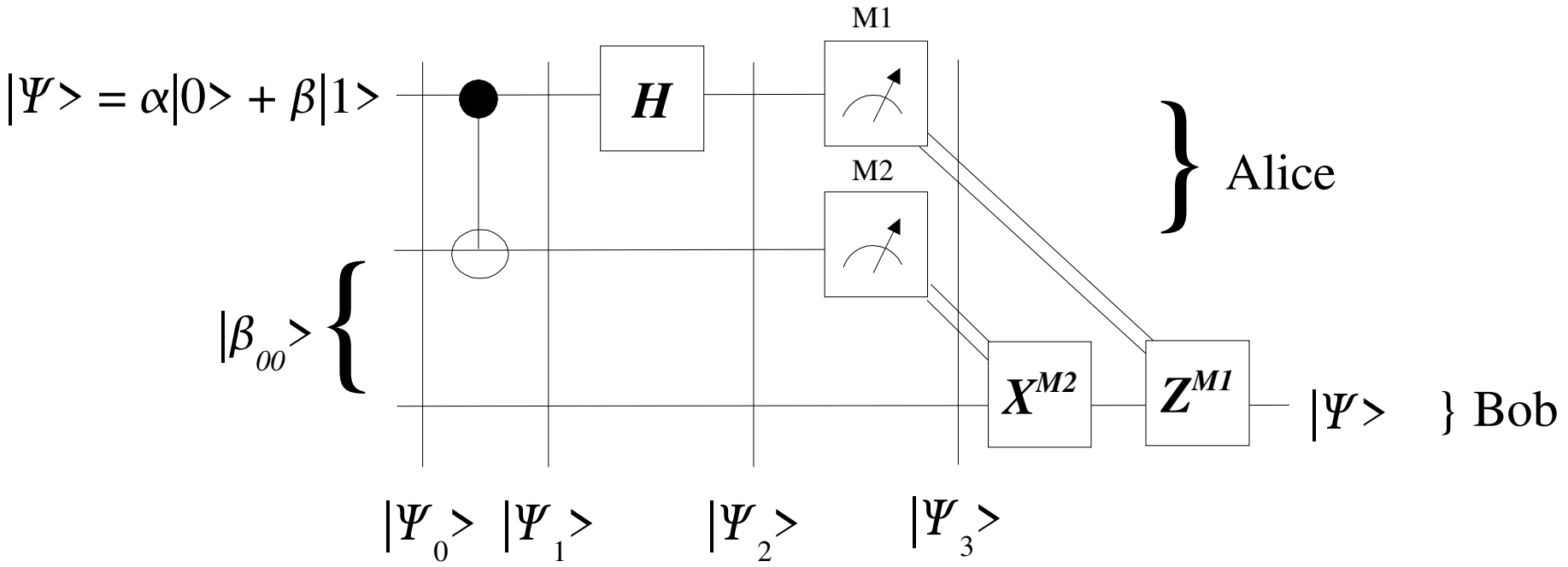
$$|\Psi_0> = |\Psi> |\beta_{00}> = \frac{1}{\sqrt{2}}\left[\alpha|0>(|00>+|11>)+\beta|1>(|00>+|11>)\right]$$

$$|\Psi_1> = \frac{1}{\sqrt{2}}\left[\alpha|0>(|00>+|11>)+\beta|1>(|10>+|01>)\right]$$

$$|\Psi_2> = \frac{1}{2}\left[\alpha(|0>+|1>)(|00>+|11>)+\beta(|0>-|1>)(|10>+|01>)\right]$$

$$|\Psi_2> = \frac{1}{2}\left[|00>(\alpha|0>+\beta|1>)+|01>(\alpha|1>+\beta|0>)+|10>(\alpha|0>-\beta|1>)+|11>(\alpha|1>-\beta|0>)\right]$$

Teleportation eines Qubit



$$00 \rightarrow |\Psi_3(00)> = \left[\alpha|0> + \beta|1>\right]$$
$$01 \rightarrow |\Psi_3(01)> = \left[\alpha|1> + \beta|0>\right]$$
$$10 \rightarrow |\Psi_3(10)> = \left[\alpha|0> - \beta|1>\right]$$
$$11 \rightarrow |\Psi_3(11)> = \left[\alpha|1> - \beta|0>\right]$$

Mögliche Realisierungen für Qubits und Gatter

Ionenfallen:
– Kernspin als Informationsträger
– Photonen zur Kopplung der Einzelatome

optisch durchlässige Trägermedien: ähnlich Ionenfalle

Dotierungsatome in Halbleitern

Kernspin von Flüssigkeitsmolekülen (grosse Mengen gleichartiger Qubits)

Quantum mechanics: real black magic calculus.
–Albert Einstein

Vielen Dank für Ihre Aufmerksamkeit!