Stichworte zur Quantentheorie

Franz Embacher[1] und Beatrix Hiesmayr[2]

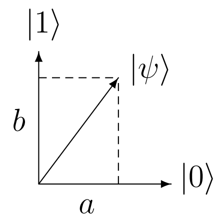
Unterlagen zum Workshop “Quantenkryptographie und Quantencomputer”
im Rahmen der 58. Fortbildungswoche Physik/Chemie
Institut für Theoretische Physik der Universität Wien, 25. 2. 2004

1 Qubits

Ein Qubit ist ein Quantensystem, dessen Zustandsvektoren sich als Linearkombinationen (Überlagerungen) zweier fix gewählter Zustandsvektoren $|0\rangle$ und $|1\rangle$ darstellen lassen:

$$|\psi\rangle = a|0\rangle + b|1\rangle \longleftrightarrow \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbf{C}^2 \qquad \text{wobei } |a|^2 + |b|^2 = 1. \tag{1.1}$$

Jeder solche Zustandsvektor beschreibt einen physikalisch realisierbaren Zustand. Die Zustandsvektoren $|0\rangle$ und $|1\rangle$ (sie bilden die “Standardbasis”) werden manchmal auch in der Form $|\uparrow\rangle$ und $|\downarrow\rangle$ oder $|H\rangle$ und $|V\rangle$ geschrieben. Für viele Zwecke der Quanteninformation können die Koeffizienten a und b als reell angenommen werden. Die Zustandsvektoren des Systems können dann als (Einheits-)Vektoren in der Zeichenebene dargestellt werden:



Die Zahlen a und b sind die (orientierten) Projektionen von $|\psi\rangle$ auf die Vektoren der Standardbasis. Gemeinsam bilden sie die “Wellen*funktion*” des Systems: Was aus dem quantenmechanischen Formalismus für den Ort eines Teilchens als Funktion $\vec{x} \mapsto \psi(\vec{x})$ (mit $\vec{x} \in \mathbf{R}^3$) bekannt ist, reduziert sich hier auf eine Funktion $j \mapsto \psi_j$ (mit $j \in \{0, 1\}$), spielt aber in der Theorie dieselbe Rolle.

[1] fe@ap.univie.ac.at
[2] hiesmayr@ap.univie.ac.at

2 Messung

Jede (orthonormale) Basis von Zustandsvektoren entspricht einer physikalischen Mess-Anordnung. Eine Messung des Zustands (1.1) “in der Standardbasis” ergibt eines der zwei möglichen Resultate (0 oder 1) mit Wahrscheinlichkeiten

$$w(0) = |a|^2 \qquad w(1) = |b|^2. \tag{2.1}$$

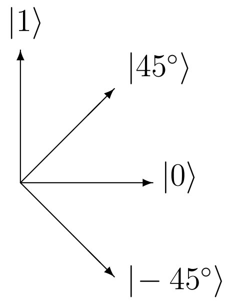
Konkrete für die Quanteninformation relevante Systeme sind:

Physikalisches System	Basisvektoren	beschreiben...
abstrakt	$\|0\rangle$, $\|1\rangle$	Messung in der Standardbasis
Elektronenspin	$\|\uparrow\rangle, \|\downarrow\rangle$	Messung der z-Komponente des Spins (“up” oder “down”)
Ploarisationsfreiheitsgrad eines Photons	$\|H\rangle$, $\|V\rangle$	Wirkung eines Polarisationsfilters in horizontaler (vertikaler) Stellung
Gebundenes System (z.B. Atom)	$\|E_0\rangle$, $\|E_1\rangle$	Messung der Energie (Grund- oder erster angeregter Zustand)
Katze	$\|\text{lebend}\rangle, \|\text{tot}\rangle$	Beobachten der Katze

Ist ein Qubit-System im Zustand (1.1) und wird eine Messung in einer *anderen* Basis durchgeführt, so können die Wahrscheinlichkeiten für die möglichen Messresultate leicht berechnet werden. Wir betrachten als (wichtiges) Beispiel die aus den beiden Zustandsvektoren

$$|45^\circ\rangle = \frac{1}{\sqrt{2}}\,(|0\rangle + |1\rangle) \qquad |-45^\circ\rangle = \frac{1}{\sqrt{2}}\,(|0\rangle - |1\rangle) \tag{2.2}$$

bestehende Basis. (Physikalisch beschreibt sie im Fall des Photons um 45° verdrehte Polarisationsfilter, im Fall des Elektrons die Messung der x-Komponente des Spins). Geometrisch kann sie in der Zeichenebene so visualisiert werden:



Für die Berechnung der Wahrscheinlichkeiten muss der Zustandsvektor (1.1) zunächst in die neue Basis entwickelt werden:

$$|\psi\rangle = a'|45°\rangle + b'|-45°\rangle = \frac{a'+b'}{\sqrt{2}}|0\rangle + \frac{a'-b'}{\sqrt{2}}|1\rangle, \tag{2.3}$$

woraus durch Koeffizientenvergleich mit (1.1)

$$a' = \frac{a+b}{\sqrt{2}} \qquad b' = \frac{a-b}{\sqrt{2}} \tag{2.4}$$

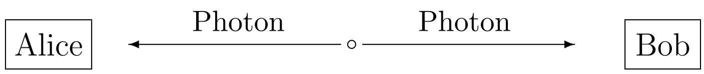
folgt. Analog zu (2.1) ergeben sich die Wahrscheinlichkeiten für die Messresultate (hier $\pm 45°$) als Quadrate (der Absolutbeträge) der Koeffizienten (hier a' und b'):

$$w(45°) = |a'|^2 = \frac{1}{2}|a+b|^2 \qquad w(-45°) = |b'|^2 = \frac{1}{2}|a-b|^2. \tag{2.5}$$

Auf dieselbe Weise können Vorhersagen für Messungen in beliebigen anderen (orthonormalen) Basen berechnet werden.

3 2-Qubit-System

Ein 2-Qubits-System ist ein Quantensystem, das aus zwei Qubits (z.B. den Polarisationsfreiheitsgraden eines Photonenpaars) besteht. Es ist nützlich, sich zwei Beobachter (Alice und Bob) vorzustellen, denen jeweils nur ein Qubit experimentell zugänglich ist.



Ist Alices Teilsystem im Zustand $|0\rangle$ und Bobs Teilsystem im Zustand $|1\rangle$, so schreiben wir den Zustandsvektor des Gesamtsystems als $|0\rangle|1\rangle$. Das Gesamtsystem besitzt die vier Zustandsvektoren $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$ und $|1\rangle|1\rangle$ als Basis. Daher stellen auch Linearkombinationen wie

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right) \tag{3.1}$$

physikalisch realisierbare Zustände dar. Wenn das System in diesem (dem berühmten EPR-)Zustand ist und Alice und Bob jeweils eine Messung in ihrer Standardbasis durchführen, so können die Wahrscheinlichkeiten für die möglichen Messresultate als Quadrate der (Absolutbeträge) der Koeffizienten in (3.1) abgelesen werden:

$$w(\text{Alice: } 0,\ \text{Bob: } 0) = 0 \tag{3.2}$$
$$w(\text{Alice: } 0,\ \text{Bob: } 1) = \frac{1}{2} \tag{3.3}$$
$$w(\text{Alice: } 1,\ \text{Bob: } 0) = \frac{1}{2} \tag{3.4}$$
$$w(\text{Alice: } 1,\ \text{Bob: } 1) = 0. \tag{3.5}$$

(Das EPR-Paradoxon ergibt sich, wenn Alice und Bob die Basen, die ihre Messungen definieren, frei wählen können).

4 Zeitentwicklung

In der Quanteninformation wird oft nur für kurze Zeit eine Wechselwirkung "eingeschaltet", um eine ganz bestimmte Änderung des Zustandsvektors zu erreichen. Es liegt dann keine kontinuierliche Zeitentwicklung vor, sondern eine diskrete: $|\psi_{\text{vorher}}\rangle$ wird in $|\psi_{\text{nachher}}\rangle$ übergeführt. Zwei wichtige Beispiele solcher Transformationen für Qubits sind:

- Die **NOT-Transformation** führt $|0\rangle$ in $|1\rangle$ und $|1\rangle$ in $|0\rangle$ über:

  $$\text{NOT}|0\rangle = |1\rangle \qquad \text{NOT}|1\rangle = |0\rangle. \tag{4.1}$$

  Im Fall des Photons kann sie als Wirkung einer Vorrichtung zur Drehung der Polarisationsebene um 90° (die *nicht* mit einer Messung verbunden ist) interpretiert werden. Transformationen, die Wechselwirkungen beschreiben, sind *linear* und *unitär*. Linearität bedeutet, dass die Transformation einer Überlagerung von Zustandsvektoren gleich der Überlagerung der Transformierten dieser Zustandsvektoren ist. Im Fall der NOT-Transformation bedeutet das

  $$\text{NOT}(a|0\rangle + b|1\rangle) = b|0\rangle + a|1\rangle \tag{4.2}$$

  für alle a, b. Unitarität verlangt, dass Einheitsvektoren immer in Einheitsvektoren übergeführt werden. Physikalisch kann sie als "Erhaltung der Wahrscheinlichkeit" interpretiert werden.

- Die **Hadamard-Transformation** ist durch

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{4.3}$$

  definiert. Im Fall des Photons kann sie als Wirkung einer Vorrichtung zur Drehung der Polarisationsebene um 45° (die *nicht* mit einer Messung verbunden ist) interpretiert werden.

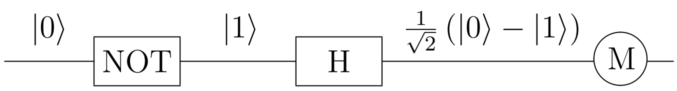
Für die Zeitentwicklung eines Qubits kann eine bequeme graphische Visualisierungsmethode verwendet werden. Ein Qubit wird durch eine horizontale Linie dargestellt, wobei die Zeit von links nach rechts verläuft:

Soll angedeutet werden, dass sich das System in einem bestimmten Zustand befindet, wird die Linie entsprechend beschriftet, beispielsweise so:

$|0\rangle$

Eine Transformation wird als beschriftetes Kästchen dargestellt, hier zum Beispiel das NOT:

Damit lassen sich Folgen von hintereinander ausgeführten Transformationen übersichtlich darstellen. Beispiel:



Mit M ist hier eine abschließende Messung (in der Standardbasis) bezeichnet. (Was wird sie mit welcher Wahrscheinlichkeit ergeben?) Werden Systeme betrachtet, die aus mehreren Qubits bestehen (wie beim Quantencomputer), so lassen sich auf diese Weise "Schaltpläne" darstellen.

Links und Literatur
zu diesem Workshop finden Sie am Web unter

http://www.ap.univie.ac.at/users/fe/Quantentheorie/Fortbildungswoche2004/