Quantenfehlerkorrektur

Julian Lorenz

Technische Universität München
lorenz@informatik.tu-muenchen.de

Zusammenfassung Shor's Algorithmen zur Faktorisierung und für das Diskrete Logarithmus Problem sowie der Algorithmus von Grover zur Suche in unstrukturierten Datensätzen liefern Algorithmen für einen hypothetischen Quantenrechner, die den bisher bekannten Algorithmen für klassische Turingmaschinen deutlich überlegen sind. Die technische Realisierung der hierfür nötigen hinreichend großen Anzahl verschränkter Quantenzustände scheint noch in weiter Ferne, jedoch prinzipiell möglich. Doch selbst die beste physikalische Realisierung wird die durch *Dekohärenz* und viele andere Effekte verursachte Fragilität der Quantenzustände nicht verhindern können. Quantenrechnungen werden hierdurch stark gestört. Man wird auf einen fortwährenden Fehlerkorrekturmechanismus angewiesen sein, oder wird sich auf extrem kurze Rechnungen beschränken müssen. Hierbei ist man allerdings vor eine Reihe von Problemen gestellt, die Quantenfehlerkorrektur im Gegensatz zur klassischen Fehlerkorrektur scheinbar unmöglich machen, vor allem die Tatsache, dass Quantenzustände nicht duplizierbar sind (*no cloning theorem*).
Dennoch gelang es Peter Shor 1995, einen fehlerkorrigierenden Code vorzustellen, mit dessen Hilfe der tatsächlichen Nutzung eines physikalischen Quantenrechners nichts im Wege stehen würde. Seitdem wurden viele weitere Verfahren entwickelt.
Dieser Text möchte einen einführenden Überblick über das Thema Quantenfehlerkorrektur geben.

1 Notwendigkeit von Quantenfehlerkorrektur und inärente Schwierigkeiten

> *A computer is a physical system, subject to the laws of nature. No errors occur in the application of these laws. What we call an error is a mismatch between what the computer does and what we wanted it to do.*
> - A. Peres (1996)

Die Basis der Überlegenheit eines Quantenrechners liegt in der Überlagerung und und vor allem Verschränkung von Quantenzuständen, d.h. der nicht-lokale Korrelationen von verschiedenen Teilen eines Quantensystems. Allerdings erweisen sich derartige Quantenzustände als sehr unbeständig. Der Grund ist, dass das präparierte Quantensystem (Quantenrechner) unausweichlich Kontakt zu einem weiteren riesigen Quantensystem bekommt, nämlich seiner Umgebung (environment). Ein vollkommen isolierter Quantenrechner (geschlossenen Quantensystem, im

Gegensatz zu einem offenen Quantensystem) ist nicht realisierbar, und selbst wenn höchst sinnlos, da dies jeglichen Zugriff durch den Quantenrechner-User auf die produzierten Ergebnisse ausschließen würde.

Jede Interaktion der Umgebung mit dem Quantenrechner (Steuerung von Operationen, Messungen) führt zu Verschränkungen des Quantenrechners mit der Umgebung. In einem solchen Zustand lässt sich durch Messung innerhalb des Quantenrechners allein keine vollständige Information mehr gewinnen, man müsste die Umgebung mitmessen! Praktisch gesehen wird die Information unwiderruflich verloren sein. Diesen Vorgang nennt man *Dekohärenz* eines Quantensystems. Ein bekanntes Beispiel ist Schrödingers Katze, die man mit einer geschickten Apparatur versucht in einen Zustand der Art

$$|Katze\rangle = \frac{1}{\sqrt{2}}\left(|tot\rangle + |lebendig\rangle\right)$$

zu bringen, in dem sie mit gleicher Wahrscheinlichkeit tot und lebendig ist. Ein solcher Zustand ist zwar theoretisch herstellbar, praktisch aber extrem instabil. Der Zustand $|Katze\rangle$ würde sofort in Interaktion mit seiner Umgebung treten, und hätte zur Folge, dass die Katze entweder tot oder lebendig wäre. Die Umgebung führt sozusagen unmittelbar eine Messung an der Katze durch, die den Zustand kollabieren lässt.

Doch nicht nur Schrödingers Katze (diese aufgrund der Grösse des sie bildenden Quantensystems und der daraus resultierenden gigantischen Verschränkungen mit der Umgebung aber ganz besonders!), sondern jedes auch noch so kleine Quantensystem ist diesen Effekten unterworfen, also auch die Qubits eines Quantenrechners. Die Folge ist, dass man sich bei Quantenrechnungen mit extrem kurze Versuchszeiten (d.h. Rechenzeiten) begnügen müßte, da die Wahrscheinlichkeit von Fehlern sonst zu groß wäre. Eine andere naheliegende Alternative ist die Entwicklung von Fehlerkorrekturverfahren, wie sie auch in der klassischen Informationsverarbeitung verwendet werden. Die klassische Codierungstheorie hat sich in den letzten Jahrzehnten zu einer komplexen Wissenschaft entwickelt, die in Anwendungen große Erfolge erzielen konnte (CD-Player, Mobiltelefone usw.).

Die grundlegende Idee jedes Codierungs- und Korrekturverfahrens ist die Redundanz der zu übermittelnden Information. Die einfachste Idee ist etwa die folgende: Wir haben ein Bit b, dass während einer Übertragung (oder innerhalb einer bestimmten Zeit, in dem es gespeichert ist - die Codierungstheorie spricht allgemein von einem *channel*) mit einer Wahrscheinlichkeit p negiert wird (*bit flip*). Um die Information zu schützen, kodieren wir

$$0 \mapsto 0_L = 000 \quad 1 \mapsto 1_L = 111$$

In jedem der drei Bits des Codeworts trete nun weiterhin unabhängig ein *bit flip* mit Wahrscheinlichkeit p auf. Nach der Übertragung führen wir nun einen *Mehrheitsentscheid* der drei Qubits durch. Trat höchstens ein *bit flip* unter den drei Qubits auf, ist der Mehrheitsentscheid korrekt. Die Wahrscheinlichkeit für einen falschen Mehrheitsentscheid ist damit $3p^2(1-p)+p^3$. Wegen $3p^2(1-p)+p^3 < p \Leftrightarrow p < 1/2$ verbessert dieses Verfahren für kleine Fehlerwahrscheinlichkeiten p die Zuverlässigkeit der Übertragung des Bits. Unmittelbar einsichtig ist, dass bei Verwendung hinreichend vieler Kopien die Wahrscheinlichkeit eines falschen Mehrheitsentscheids beliebig klein gemacht werden kann.

Man nennt dieses Verfahren einen *repetition code*. Es ist allerdings nicht sehr effizient. Die klassische Codierungstheorie hat Codes entwickelt, bei denen das Verhältnis zwischen Redundanz und Verlässlichkeit wesentlich besser ausfällt.

Leider sind die Verfahren der klassischen Codierungstheorie nicht unmittelbar zur Quantenfehlerkorrektur verwendbar! Gründe sind vor allem:

- *„No-Cloning-Theorem*: Quantenzustände können nicht dupliziert werden. Nur der Präparator eines Quantenzustands kann Kopien anfertigen, indem er die Präparation wiederholt.
  Dies folgt unmittelbar aus der Tatsache, dass die Quantenmechanik nur unitäre Evolutionen von (geschlossenen) Quantensystemenen zulässt:

  Theorem (Wootters/Zurek, 1982):
  Kein Quantenalgorithmus kann Quantenzustände duplizieren.
  Beweis:
  Sei A das Quellquantensystem im reinen Zustand $|\psi\rangle$ und B das Ziel-Quantensystem im reinen Zustand $|s\rangle$. Der Zustand von $A \otimes B$ soll also mit unitären Evolution wie folgt transformiert werden:

  $$|\psi\rangle|s\rangle \mapsto U(|\psi\rangle|s\rangle) = |\psi\rangle|\psi\rangle$$

  Speziell für zwei beliebige Zustände $|\psi\rangle, |\phi\rangle$

  $$U(|\psi\rangle|s\rangle) = |\psi\rangle|\psi\rangle$$

  $$U(|\phi\rangle|s\rangle) = |\phi\rangle|\phi\rangle$$

  Das Skalarprodukt dieser beiden Gleichungen ergibt

  $$(\langle\psi|\phi\rangle) = (\langle\psi|\phi\rangle)^2$$

  Die Gleichung $x^2 = x$ hat in $\mathbb{C}$ die beiden Lösungen $x = 0 \vee x = 1$. Also gilt entweder $\langle\psi|\phi\rangle = 0$ (d.h. $|\psi\rangle \perp |\phi\rangle$) oder $\langle\psi|\phi\rangle = 1$ (d.h. $|\psi\rangle = |\phi\rangle$). □

- *Verschiedene Fehlerarten möglich*: Ein Qubit $|\psi\rangle$ sei im Zustand $|\psi\rangle = a|0\rangle + b|1\rangle$ präpariert. Das quantenmechanische Analogon zum klassischen *bit flip* ist die Transformation

  $$|\psi\rangle \mapsto b|0\rangle + a|1\rangle$$

  d.h. die (bekannte) unitäre Evolution *Pauli X*

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

  Anders als im Fall klassischer (binären) Informationsverarbeitung hat Quanteninformationsverarbeitung aber noch mit anderen Fehlern zu kämpfen!

Eine weitere solche Fehlerquelle ist der sogenannte *phase flip*:

$$|\psi\rangle \mapsto a|0\rangle - b|1\rangle$$

Das ist gerade die unitäre Operation *Pauli Z*

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

Möglich ist auch das gleichzeitige Auftreten von *bit flip* und *phase flip*

$$|\psi\rangle \mapsto \underbrace{iXZ}_{Y}|\psi\rangle = i\,(a|1\rangle - b|0\rangle)$$

In der Tat ist sogar ein Kontinuum von Störungen möglich!

- *Messungen zerstören Quantenzustände*: Die zum klassischen *repetition code* analoge Idee, einen Quantenzustand $|\psi\rangle = a|0\rangle + b|1\rangle$ gemäss einer Kodierungsvorschrift der Art

  $$|0\rangle \mapsto |0_L\rangle = |000\rangle, \quad |1\rangle \mapsto |1_L\rangle = |111\rangle$$

  zu kodieren, d.h. in das Codewort

  $$|\psi\rangle = a|0\rangle + b|1\rangle \mapsto a|000\rangle + b|111\rangle$$

  lässt sich zwar mit einer unitären Evolution realisieren. Nicht möglich ist allerdings eine Fehlerdiagnose durch Messen der drei Qubits und Mehrheitsentscheid, da eine Messung der drei Qubits des Codesworts die Informationen (d.h. a und b) zerstört.

2 Projective Measurements

Im Folgenden wird das Konzept der *projective measurements* verwendet: Eine *projective measurement* wird durch einen hermiteschen Operator M beschrieben, genannt *observable*. M besitzt eine Spektraldarstellung

$$M = \sum_m m P_m$$

wobei P_m den Projektionsoperator auf den Eigenraum zum Eigenwert m bezeichne. Mögliche Ergebnisse der Messung sind die Eigenwerte m.
Bei Messung des Zustands $|\psi\rangle$ ist die Wahrscheinlichkeit für m gegeben durch

$$p(m) = \langle\psi|P_m|\psi\rangle$$

Nach einer Messung mit Ergebnis m ist das System im Zustand

$$\frac{P_m|\psi\rangle}{p(m)}$$

Beispiel: Messung der Observablen *Pauli-Z*

Z besitzt die *Spektralzerlegung:* $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$. Als Beispiel betrachten wir die Messung des Zustands $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Sie ergibt $+1$ mit Wahrscheinlichkeit $\langle\psi|0\rangle\langle 0|\psi\rangle = 1/2$ und -1 mit Wahrscheinlichkeit $\langle\psi|1\rangle\langle 1|\psi\rangle = 1/2$. Nach der Messung befindet sich das System im Zustand $|0\rangle$ bzw. $|1\rangle$.

Wie lässt sich dieses Konzept im Schaltkreismodell realisieren? Wir betrachten dazu die Messung einer Observablen M mit den Eigenwerten ± 1?
Es stellt sich heraus, dass die Messung des ersten Qubits im Schaltkreis in Abbildung (1) die Phase ϕ von $m = e^{\pi i \phi}$ ergibt.

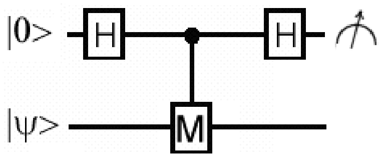

Abbildung 1. Schaltkreis zur Messung einer Observablen M mit den Eigenwerten ± 1

Dies sieht man so: Sei $|\psi_{\pm 1}\rangle$ die Eigenbasis von M. Dann operiert der dargestellte Quantenalgorithmus wie folgt:

$$|0\rangle|\psi_{\pm 1}\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|\psi_{\pm 1}\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\,|\psi_{\pm 1}\rangle \mapsto \begin{cases} |0\rangle|\psi_{+1}\rangle \\ |1\rangle|\psi_{-1}\rangle \end{cases}$$

d.h. die Messung des ersten Qubits ergibt $m = e^{\pi i \cdot 0} = +1$, falls $|\psi_{+1}\rangle$ im zweiten Qubit präpariert gewesen ist, und $m = e^{\pi i \cdot 1} = -1$ bei $|\psi_{-1}\rangle$.
Aufgrund der Linearität von Quantenprozessen folgt für $|\psi\rangle = \alpha|\psi_{+1}\rangle + \beta|\psi_{-1}\rangle$, dass eine Messung das Ergebnis $+1$ mit Wahrscheinlichkeit $p(+1) = |\alpha|^2$ und das Ergebnis -1 mit Wahrscheinlichkeit $p(-1) = |\beta|^2$ erzeugt, was mit dem Konzept der Messung von Observablen (s.o.) übereinstimmt.

3 Der 9 Qubit Shor Code

3.1 3 Qubit Bit Flip Code

Wir wollen zunächst ein Verfahren konstruieren, mit dem sich ein Qubit $|\psi\rangle$ gegen *bit flips* schützen lässt, d.h. gegen einen Fehler in Form einer (ungewollten) Evolution durch den unitären Operator *Pauli X*. Dazu verwenden wir die Kodierung

$$|0\rangle \mapsto |0_L\rangle = |000\rangle, \quad |1\rangle \mapsto |1_L\rangle = |111\rangle$$

d.h.

$$|\psi\rangle = a|0\rangle + b|1\rangle \mapsto a|000\rangle + b|111\rangle \tag{1}$$

Hierbei beachte man, dass

$$a|000\rangle + b|111\rangle \neq (a|0\rangle + b|1\rangle)^{\otimes 3} \tag{2}$$

Die rechte Seite in (2) ist eine dreifache Kopie des zu schützenden Qubits, lässt sich also wegen des No-Cloning-Theorems nicht herstellen. Die Kodierung (1) lässt sich hingegen mit dem Schaltkreis in Abbildung (2) realisieren. Um nun

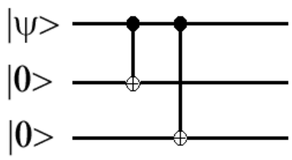

Abbildung 2. Schaltkreis zur Kodierung beim *bit flip code*

festzustellen, ob in unserem Codewort in einem der drei Qubits ein *bit flip* aufgetreten ist, messen wir nun die beiden Observablen $Z_1Z_2 = Z \otimes Z \otimes I$ und $Z_2Z_3 = I \otimes Z \otimes Z$. Z_1Z_2 besitzt die Spektralzerlegung

$$\begin{aligned} Z \otimes Z \otimes I &= (|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes (|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) \\ &= \quad (|000\rangle\langle 000| + |111\rangle\langle 111| + |001\rangle\langle 001| + |110\rangle\langle 110|) \\ &\quad - (|010\rangle\langle 010| + |101\rangle\langle 101| + |011\rangle\langle 011| + |100\rangle\langle 100|) \end{aligned}$$

Die Messung der Observablen Z_1Z_2 *vergleicht* also die ersten beiden Qubits und liefert $+1$ mit Wahrscheinlichkeit 1, *falls* diese übereinstimmen, und -1 mit Wahrscheinlichkeit 1, *falls* sich diese unterscheiden. Wir nennen das Ergebnis $(\pm 1, \pm 1)$ der beiden Messungen das *Fehlersyndrom*. Unter der Annahme, dass höchstens ein Qubit fehlerhaft ist, lässt sich dieses eindeutig aus dem Fehlersyndrom lokalisieren:

$(+1, +1)$ $\rightarrow$ Kein Fehler (oder 3 Fehler)
$(+1, -1)$ $\rightarrow$ Fehler im dritten Qubit (oder in den ersten beiden Qubits)
$(-1, +1)$ $\rightarrow$ Fehler im ersten Qubit (oder in den letzten beiden Qubits)
$(-1, -1)$ $\rightarrow$ Fehler im zweiten Qubit (oder im ersten und dritten Qubit)

Die Korrektur des als fehlerhaft lokalisierten Qubits erfolgt nun durch Anwenden des Operators X_k (mit k entsprechend gewählt).

Sei p die Wahrscheinlichkeit eines *bit flips*. Dann tritt mit einer Wahrscheinlichkeit von $(1-p)^3+3p(1-p)^2 = 1-3p^2+2p^3$ höchstens *ein bit flip* im Codewort auf. Wiederum gilt

$$3p^2 - 2p^3 < p \Longleftrightarrow p < 1/2$$

In der (fernen ...) Praxis wird man nun die Fehlerdiagnose (und falls nötig natürlich auch die Korrektur) jedes Qubits im „Speicher" des Quantenrechners in so kurzen Intervallen durchführen, dass die Wahrscheinlichkeit des Auftretens von mehr als zwei *bit flips* unterhalb einer sehr kleinen Toleranz liegt. Wesentlich dabei ist, dass die Messung der Observablen Z_1Z_2 und Z_2Z_3 Zustände der Form $X_1^{b_1}X_2^{b_2}X_3^{b_3}\,(a|0_L\rangle + b|1_L\rangle)$ $(b_k \in \mathbb{Z}_2)$ nicht verändert. Der Grund hierfür ist, dass alle Zustände dieser Form Eigenvektoren zu einem der beiden Eigenwerten ± 1 sind, wie man an der Spektralzergelgung von Z_1Z_2 erkennt. Das Verfahren stört also den Ablauf einer Quantenrechnung, in das es eingebaut ist, in keiner Weise.

Wie realisiert man nun die Messung der Observablen Z_1Z_2 in Form eines Quantenschaltkreises? Z_1Z_2 ist eine Observable mit Eigenwerten ± 1. Nach Abschnitt 2 können wir die Messung also mit dem Schaltkreises in Abbildung (3) erledigen.

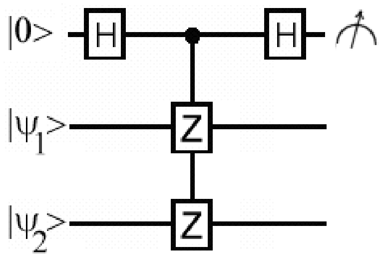

Abbildung 3. Schaltkreis zur Messung der Observablen Z_1Z_2

Dieser Schaltkreis lässt sich noch vereinfachen zu dem in Abbildung (4).

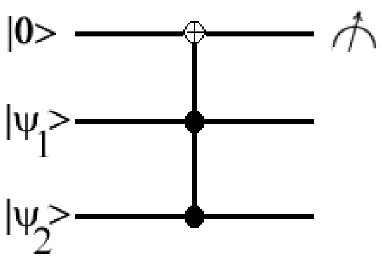

Abbildung 4. Vereinfachter Schaltkreis zur Messung der Observablen Z_1Z_2

Von der Äquivalenz überzeugt man sich am geschicktesten dadurch, indem man die Ergebnisse der Schaltkreise bei Anwendung auf der Eigenbasis von $Z_1 Z_2$ testet, die praktischerweise in diesem Fall mit der Rechenbasis übereinstimmt. (Bem.: $|00\rangle$ und $|11\rangle$ spannen den zweidimensionalen Eigenraum zum Eigenwert $+1$ auf, $|01\rangle$ und $|10\rangle$ den zum Eigenwert -1)

3.2 3 Qubit Phase Flip Code

Wir wollen nun einen Code entwickeln, der gegen *phase flips* schützt, d.h. gegen das Auftreten eines Fehlers in Form des unitären Operators *Pauli Z*. Die grundlegende Beobachtung ist hier, dass nach einem Basiswechsel *phase flips* nichts anderes sind als *bit flips*. Mit

$$|+\rangle := H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{und} \quad |-\rangle := H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

gilt nämlich

$$Z|+\rangle = |-\rangle \quad \text{und} \quad Z|-\rangle = |+\rangle$$

d.h. in der *Basis* $\{|+\rangle, |-\rangle\}$ operiert Z wie ein *bit flip*. Die Idee ist deshalb, die Kodierung

$$|0_L\rangle = |+++\rangle, \quad |1_L\rangle = |---\rangle$$

zu verwenden. Der Schaltkreis zur Kodierung ist in Abbildung (5) zu sehen. Die Fehlerdiagnose für den *bit flip code* lässt sich für den *phase flip code* im

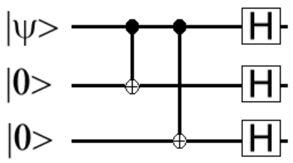

Abbildung 5. Schaltkreis zur Kodierung beim *phase flip code*

Wesentlichen übernehmen, es müssen lediglich alle verwendeten Operationen mit dem Hadamard-Gate konjugiert werden, d.h. vor und nach Operationen ein Basiswechsel durchgeführt werden: Es müssen also nun die Observablen

$$H^{\otimes 3} Z_1 Z_2 H^{\otimes 3} = X_1 X_2 \quad \text{und} \quad H^{\otimes 3} Z_2 Z_3 H^{\otimes 3} = X_2 X_3$$

gemessen werden. (Beachte $H^\dagger = H$ und $HZH = X$) Für die Fehlerkorrektur gilt dies analog: Ein *phase flip* im k-ten Qubit eines Codeswortes korrigiert man mit $H_k X_k H_k = Z_k$. Da nach einem Basiswechsel alle Operationen für den *phase flip code* denen für den *bit flip code* entsprechen, nennt man die beiden Codes *unitär äquivalent*.

3.3 9 Qubit Shor Code

In einem nächsten Schritt wollen wir nun einen Code angeben, der sowohl gegen *bit flips* als auch gegen *phase flips* (und auch gegen deren gleichzeitigem Auftreten in einem Qubit) schützt. Hierzu müssen wir lediglich die beiden bisher entwickelten Codes kombinieren!
Wir kodieren zunachst $|0\rangle, |1\rangle$ mit dem *3 qubit phase flip code*

$$|0\rangle \mapsto |+++\rangle, \quad |1\rangle \mapsto |---\rangle$$

Anschliessend kodieren wir jedes der 3 Qubits mit dem *3 qubit bit flip code*

$$|+\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \mapsto \frac{(|000\rangle + |111\rangle)}{\sqrt{2}}$$

$$|-\rangle = \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} \mapsto \frac{(|000\rangle - |111\rangle)}{\sqrt{2}}$$

Diese Kodierung lässt sich durch Konkatenation der Schaltkreise für den *phase flip code* und den *bit flip code* realisieren. Diese Code-Kombination, der sogenannte *9 Qubit Code* (Shror, 1995), liefert letztlich die logischen Codewörter

$$|0_L\rangle = \frac{(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)}{2\sqrt{2}}$$

$$|1_L\rangle = \frac{(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)}{2\sqrt{2}}$$

Abbildung (6) zeigt den zusammangesetzten Schaltkreis zur Kodierung.

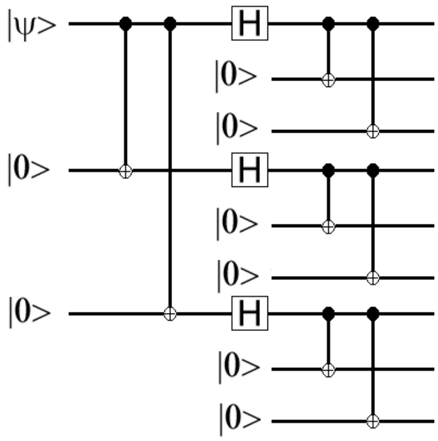

Abbildung 6. Schaltkreis zur Kodierung beim *Shor-Code*

Wie hat man nun für die Fehlerdiagnose vorzugehen?

Die Diagnose von *bit flips* X_k in einem der 9 Qubits läuft wie beim bit flip Code ab: Im ersten 3er-Block misst man hierzu die Observablen Z_1Z_2 und Z_2Z_3, und schließt hieraus darauf, ob und welches der drei ersten Qubits fehlerhaft ist. Für die andere Blöcke geht man analog vor. Die Korrektur eines diagnostizierten *bit flips* erfolgt wie gehabt mit X_k (k entsprechend gewählt).

Phase flips Z_k in einem der 9 Qubits erkennt man durch Messung der Observablen

$$X_1X_2X_3X_4X_5X_6 = H_1..H_6Z_1Z_2Z_3Z_4Z_5Z_6H_1..H_6$$

und

$$X_4X_5X_6X_7X_8X_9 = H_4..H_9Z_4Z_5Z_6Z_7Z_8Z_9H_4..H_9$$

Denn die Messung von z.B. $X_1X_2X_3$ ergibt mit Wahrscheinlichkeit $p = 1$

$+1$ für den Zustand $(|000\rangle + |111\rangle)$
-1 für den Zustand $(|000\rangle - |111\rangle)$

Die Messung von $X_1X_2X_3X_4X_5X_6$ vergleicht also die Phasen der beiden ersten 3er-Blöcke des Codeworts, analog die Messung von $X_4X_5X_6X_7X_8X_9$ die der beiden letzten 3r-Blöcke. Ein so diagnostizierter *phase flip* z.B. im ersten Block (bzw. genauer eigentlich in einem der drei Qubits des ersten Blocks, aber in welchem Qubit eines Blocks ein *phase flip* auftritt, ist unerheblich und resultiert im gleichen Zustand) lässt sich mit $Z_1Z_2Z_3$ korrigieren.

Was nun, wenn *phase flip* **und** *bit flip* gleichzeitig in einem Qubit auftreten, z.B. Z_1X_1? Hierzu zunächst eine *grundlegende Beobachtung:*
Sei M eine Observable (d.h. hermitesch), die gleichzeitig *unitär* ist, d.h. eine (reversible) Quantenoperation darstellt. Dann gilt: Eine Messung von M auf dem Zustand $|\psi\rangle$ ist einer Messung von M auf $M|\psi\rangle$ äquivalent.

Um dies einzusehen, betrachte man $p(m) = \langle\psi|M^\dagger P_m M|\psi\rangle = \langle\psi|P_m|\psi\rangle$ und beachte dabei, dass M und P_m wegen $M = \sum_m mP_m$ kommutieren.

Tritt nun also der Fehler $E = Z_1X_1$ auf, wird im ersten Schritt der *bit flip* X_1 mit den Observablen Z_1Z_2 und Z_2Z_3 korrekt diagnostiziert. Die *Korrektur* mit X_1 ergibt $X_1E = X_1Z_1X_1 = -Z_1X_1^2 = -Z_1$, da X und Z antikommutieren, d.h. $\{X, Z\} = 0$, wie man leicht nachrechnet. Im zweiten Schritt wird nun der *phase flip* Z_1 diagnostiziert und korrigiert. Übrig bleibt eine für die Messstatistik unerhebliche (globale) *Phase* $-I$. Der Shor Code erlaubt also die Korrektur der Fehler $\{X, Z, iXZ = Y\}$ auf *einem* Qubit. Treten allerdings derartige Fehler auf mehr als einem Qubit in einem Codewort auf, wird die Korrektur im Allgemeinen versagen. Abbildung (7) zeigt den kompletten Schaltkreis zur Fehlerdiagnose des Shor-Codes. Mit den Überlegungen von oben in Zusammenhang mit den Schaltkreisen zur Messung der Observablen Z_1Z_2 lässt sich auch dieser Schaltkreis vereinfachen, siehe Abbildung (8).

Tatsächlich bekommt man mit dem Shor Code jedoch noch mehr in Griff als die Fehler $\{X, Z, iXZ = Y\}$. Er erlaubt die Diagnose und Korrektur *beliebiger* Fehler auf einem Qubit!

Wir gehen dabei von einem etwas vereinfachten Fehlermodell aus, bei dem ein Fehler eine beliebige ungewollte unitäre Operation ist. Um zu sehen, dass der

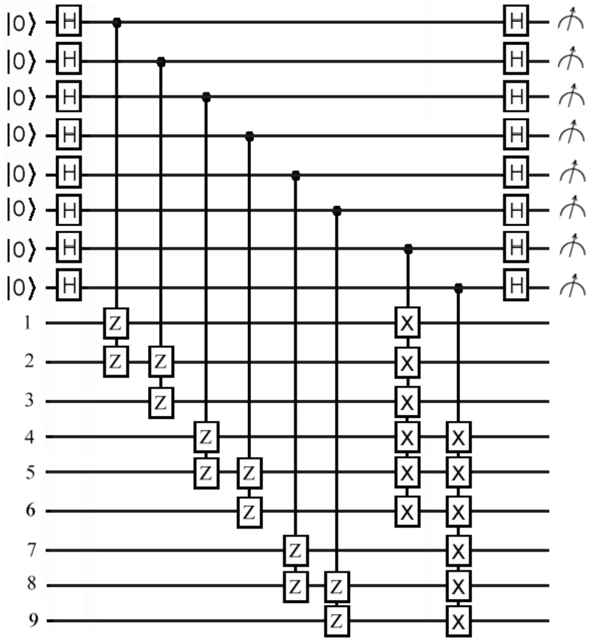

Abbildung 7. Vollständiger Schaltkreis zur Fehlerdiagnose beim Shor-Code

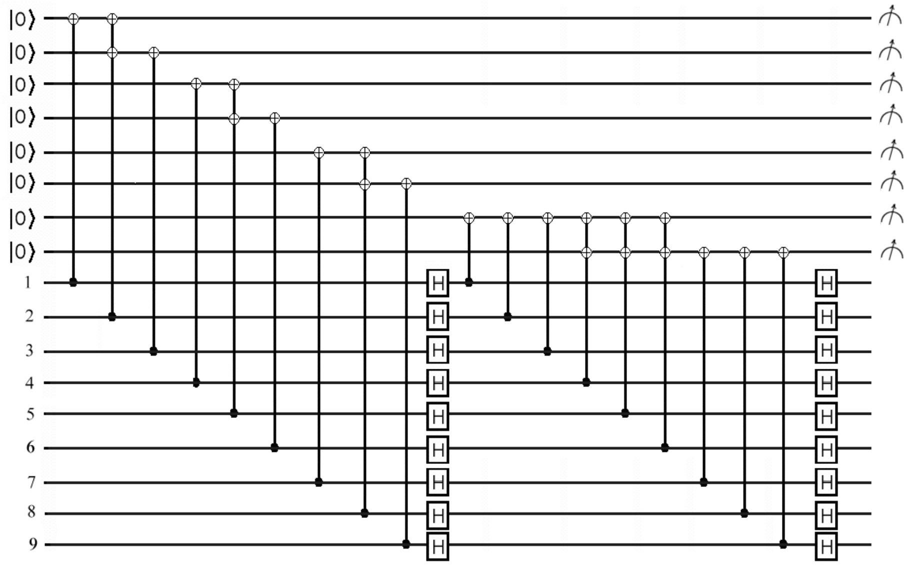

Abbildung 8. Schaltkreis zur Fehlerdiagnose beim Shor-Code nach Vereinfachung

Shor-Code hier ebenfalls funktioniert, benötigen wir zunächst zwei Lemmata.

Lemma:
$U \in \mathbb{C}^{2\times 2}$ unitär $\Leftrightarrow U = e^{i\phi} \underbrace{\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}}_{=:A}$ mit $\det A = 1$, d.h. $A \in SU(2)$

Beweis:
Lässt sich mit elementaren Mitteln zeigen. □

Lemma:
$A \in SU(2) = \{A \in \mathbb{C}^{2\times 2} | A^\dagger A = I \text{ und } \det A = 1\}$ lässt sich schreiben als

$$A = a_0 I + i\,(a_1 X + a_2 Y + a_3 Z)$$

mit $a_i \in \mathbb{R}$ und $\sum_i a_i^2 = 1$.

Beweis:
A hat wegen des vorhergehenden Lemmas die Form

$$A = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}$$

Für den Ansatz

$$A = a_0 I + i\,(a_1 X + a_2 Y + a_3 Z)$$

ermittelt man

$$a_0 = \mathrm{Re}\,\alpha,\ a_1 = \mathrm{Im}\,\beta,\ a_2 = \mathrm{Re}\,\beta,\ a_3 = \mathrm{Im}\,\alpha \qquad \square$$

Gegeben sei nun mit $|\psi\rangle$ ein 9-Qubit-Codewort zusammen mit den acht Ancilla Qubits zur Ermittlung des Fehlersyndroms im Zustand $|0_8\rangle = |00000000\rangle$. Tritt nun ein Fehler E im Codewort auf (o.E. im ersten Qubit), so lässt sich dieser dank der beiden obigen Lemmata schreiben als

$$E|\psi\rangle|0_8\rangle = e^{i\phi}\,(e_0|\psi\rangle|0_8\rangle + e_1 X_1|\psi\rangle|0_8\rangle + e_2 Z_1|\psi\rangle|0_8\rangle + e_3 Y_1|\psi\rangle|0_8\rangle)$$

Die Anwendung des Schaltkreises zur Fehlerdiagnose liefert wegen Linearität

$$e^{i\phi}\,(e_0|\psi\rangle|S_I\rangle + e_1 X_1|\psi\rangle|S_{X_1}\rangle + e_2 Z_1|\psi\rangle|S_{Z_1}\rangle + e_3 Y_1|\psi\rangle|S_{Y_1}\rangle)$$

wobei S_{X_1}, S_{Y_1}, S_{Z_1} die Fehlersyndrome für die Fehler X_1, Y_1, Z_1 bezeichnen. Wegen $\sum_i |e_i|^2 = 1$ und der Tatsache, dass die Fehlersyndrome $|S_{I,X_1,Y_1,Z_1}\rangle$ orthogonal sind, stellt dies tatsächlich einen zulässigen Quantenzustand dar. Bei Messung der Ancilllas, d.h. des Fehlersyndroms, kollabiert der Zustand deshalb in einen der vier Zustände

$$|\psi\rangle|S_I\rangle,\ X_1|\psi\rangle|S_{X_1}\rangle,\ Z_1|\psi\rangle|S_{Z_1}\rangle,\ X_1 Z_1|\psi\rangle|S_{Y_1}\rangle$$

Nun korrigiert man wie gehabt den Fehler, den das Fehlersyndrom anzeigt, und das Codewort ist - sofern höchsten *ein* Qubit gestört wurde - gerettet. Bemerkenswert ist, dass sich eine *kontinuierliche Menge* von Fehlern korrigieren lässt, indem man in der Lage ist, eine endliche diskrete (noch dazu sehr kleine) Menge von Fehlern zu korrigieren! In der klassichen digitalen Informationsverarbeitung ist man vor dieses Problem nicht gestellt, da es nur einen einzigen möglichen Fehler gibt (*bit flip*). In der klassischen analogen Informationsverarbeitung hingegen ist die Situation ähnlich. Analoge Daten können ebenfalls unendlich vielen verschiedenen Störungen ausgesetzt sein. Ein vergleichbares, elegantes Verfahren wie den Shor-Code kennt man dort allerdings nicht.

Wie wird man den Shor-Code in einem Quantenrechner der Zukunft anwenden? Es bietet sich grob zum Beispiel folgendes Vorgehen an:

- Kodiere den Input des Quantenalgorithmus mit dem Shor-Code
- Führe die Operationen des Algorithmus *direkt* auf den kodierten Zuständen aus. Zu diesem Zweck muss jedes Gatter U im Quantenschaltkreises des Algorithmus entsprechend transfomiert werden. Dies kann man sich so erreichen: Man konjugiert U mit dem Schaltkreis zur Kodierung des Shor-Codes, und vereinfacht den hieraus entstehenden Schaltkreis so weit wie möglich.
- Während der Durchführung des Algorithmus führt man regelmäßig eine Fehlerdiagnose und falls nötig die Korrektur der Codewörter durch. In welchen Abständen dieser Prozess nötig sein wird, hängt vom Dekohärenzverhalten der gewählten Quantenrechnerrealisierung ab.
- Am Ende des Algorithmus führt man die Dekodierung der Codewörter durch und messe das Ergebnis der Berechnung.

Obiges Vorgehen wird allerdings in der Praxis noch nicht ausreichen. Eine weiterführende Idee ist es, den Kodierungsprozess zu iterieren. Ein weiteres Problem ist, dass die naive Realisierung bestimmter Gatter zur Fehlerpropagation führt (Ein Fehler auf nur einem Qubit vor dem Gatter führt zu mehreren fehlerhaften Qubits nach dem Gatter). Hier sind weitere Ideen nötig (*Fault-tolerant quantum computation, Threshold Theorem*), siehe z.B. [NC00]

Literatur

[Bor01] F. Bornemann: *Begleitmaterial zur Vorlesung 'Quantencomputer': Folien der Vorlesung und Matlab-Simulator*; http://www-m3.mathematik.tu-muenchen.de/m3/teaching/QCOMP0102 (TU München, WS 2001/02)

[NC00] M. Nielsen, I. Chuang: *Quantum computation and quantum information*; Cambridge University Press (2000)

[Pre98] J. Preskill: *Quantum Information and Computation*; http://www.theory.caltech.edu/people/preskill/ph229; California Institute of Technology (1998)