Zur Einstimmung

The great modern achievements of applied mathematics have been in relativity and quantum mechanics, and these subjects are, at present at any rate, almost as 'useless' as the theory of numbers.

- G.H. Hardy (engl. Zahlentheoretiker, 1877-1947):
„A Mathematician's Apology“ (1940)

Quantenfehlerkorrektur

I. Grundlegende Überlegungen

- Warum ist Fehlerkorrektur nötig?
- Was erschwert sie?

II. 3-Qubit Bit Flip Code

III. 3-Qubit Phase Flip Code

IV. Kombination: 9 Qubit Shor Code

Zugabe: Simulation (Matlab-Bibliothek v. Prof. Bornemann, TUM)

Einführung

- Quantenrechner $\hat{=}$ Quantensystem, auf das ein Quantenuser zugreift (Präparation, Operationen, Messungen)

  → notwendigerweise *offenes System*

  → unerwünschte Störungen unvermeidbar (*Dekohärenz*), Verschränkungen mit der Umgebung (vgl. *Schrödingers Katze*)

  → Zustand der Qubits sehr fragil

- Entweder Beschränkung auf extrem kurze Rechenzeiten oder Einsatz von Mechanismen zur Fehlerkorrektur

- Grundlegende Idee zur Fehlerkorrektur: *Redundanz, Codierung*

Einfachstes (klassisches) Beispiel: Repetition code

Zunächst: Einfachstes Beispiel aus der klassischen Fehlerkorrektur

Situation: Klassisches Bit, *bit flip* mit Wahrscheinlichkeit p

Fehlerkorrektur: *repetition code* und *Mehrheitsentscheid*

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

Wahrscheinlichkeit für falschen Mehrheitsentscheid: $3p^2(1-p) + p^3$

Es gilt:

$$3p^2(1-p) + p^3 < p \Leftrightarrow p < 1/2$$

- Hinreichend viele Kopien $\rightarrow$ beliebige Zuverlässigkeit erreichbar
- Klassische Codierungstheorie versucht Verhältnis zwischen Redundanz und Zuverlässigkeit zu optimieren

Schwierigkeiten der Quantenfehlerkorrektur

Gleiche Idee unmittelbar zur Quantenfehlerkorrektur anwendbar?
NEIN! Caveats sind

- *No cloning theorem:*
  Quantenzustände können nicht kopiert werden!
- *Verschiedene Fehlerarten möglich:* $|\psi\rangle = a|0\rangle + b|1\rangle$
  - *bit flip:* $|\psi\rangle \mapsto X|\psi\rangle = a|1\rangle + b|0\rangle$
  - *phase flip:* $|\psi\rangle \mapsto Z|\psi\rangle = a|0\rangle - b|1\rangle$
  - *bit und phase flip:* $|\psi\rangle \mapsto \underbrace{iXZ}_{Y}|\psi\rangle = i\,(a|1\rangle - b|0\rangle)$
  - *Kontinuierliche Störungen*: $\rightarrow$ Unendlich viele Fehlerarten!
- *Messungen zerstören Quantenzustände*:
  Mehrheitsentscheid *so* nicht möglich

Das No-Cloning-Theorem

Theorem (Wootters/Zurek, 1982):
Kein Quantenalgorithmus kann Quantenzustände duplizieren.
Beweis:
$A \hat{=}$ Quell-Quantensystem im reinen Zustand $|\psi\rangle$
$B \hat{=}$ Ziel-Quantensystem im reinen Zustand $|s\rangle$
Wir wollen folgende unitäre Transformation von $A \otimes B$:

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

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

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

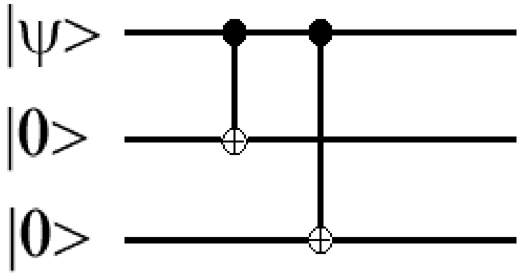
$$U(|\phi\rangle|s\rangle) = |\phi\rangle|\phi\rangle$$

Skalarprodukt der beiden Gleichungen ergibt: $(\langle\psi|\phi\rangle) = (\langle\psi|\phi\rangle)^2$
Also: $\langle\psi|\phi\rangle = 0$ (d.h. $|\psi\rangle \perp |\phi\rangle$) oder $\langle\psi|\phi\rangle = 1$ (d.h. $|\psi\rangle = |\phi\rangle$).

3 qubit bit flip code

Ziel: Korrekturverfahren für *bit flip*, d.h. für $|\psi\rangle \mapsto X|\psi\rangle$

- *Idee:* Kodiere $|0\rangle \mapsto |0_L\rangle = |000\rangle, \quad |1\rangle \mapsto |1_L\rangle = |111\rangle$
- *Achtung!* $a|0\rangle + b|1\rangle \mapsto a|000\rangle + b|111\rangle \neq (a|0\rangle + b|1\rangle)^{\otimes 3}$
- *Schaltkreis* für die Kodierung:

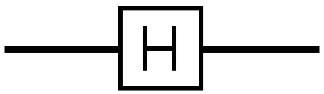


Ein *bit flip* z.B. im zweiten Qubit führt zu

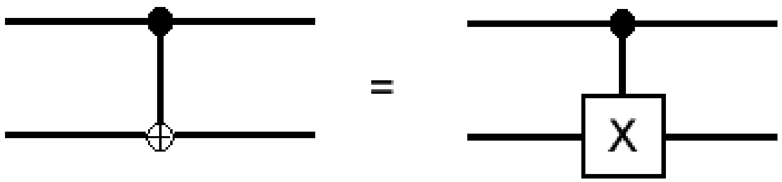
$$a|000\rangle + b|111\rangle \mapsto X_2 a|000\rangle + b|111\rangle = a|010\rangle + b|101\rangle$$

$\rightarrow$ Wie diagnostiziert man den Fehler ohne Zustand zu zerstören?

Schaltkreismodell

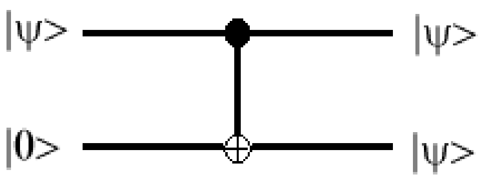


$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



CNOT: $|x\rangle|y\rangle \longmapsto |x\rangle|y \oplus x\rangle$

d.h.
$$\begin{aligned} |0\rangle|0\rangle &\longmapsto |0\rangle|0\rangle \\ |0\rangle|1\rangle &\longmapsto |0\rangle|1\rangle \\ |1\rangle|0\rangle &\longmapsto |1\rangle|1\rangle \\ |1\rangle|1\rangle &\longmapsto |1\rangle|0\rangle \end{aligned}$$



Projective measurements

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

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

Projective measurements: Die Observable Z

Beispiel: Messung der Observablen *Pauli-Z*

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

Spektralzerlegung: $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$

Messung des Zustands $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ ergibt

$+1$ mit Wahrscheinlichkeit $\langle\psi|0\rangle\langle 0|\psi\rangle = 1/2$

-1 mit Wahrscheinlichkeit $\langle\psi|1\rangle\langle 1|\psi\rangle = 1/2$

Nach der Messung befindet sich das System im Zustand

$$|0\rangle \quad \text{bzw.} \quad |1\rangle$$

3 qubit bit flip code (Fort.)

Fehlerdiagnose z.B. für *bit flip* im zweiten Qubit

$$a|000\rangle + b|111\rangle \mapsto X_2 a|000\rangle + b|111\rangle = a|010\rangle + b|101\rangle$$

$\rightarrow$ Messung in *Rechenbasis* zerstört Zustand

Trick: Messung der Observablen $Z_1 Z_2 = Z \otimes Z \otimes I$

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

$\Rightarrow$ Messung *vergleicht* die ersten beiden Qubits und liefert

$+1$ mit Wahrscheinlichkeit 1, *falls* diese übereinstimmen

-1 mit Wahrscheinlichkeit 1, *falls* sich diese unterscheiden

$\Rightarrow$ Messung verändert $X_1^{b_1} X_2^{b_2} X_3^{b_3} \left(a|0_L\rangle + b|1_L\rangle\right)$ $(b_k \in \mathbb{Z}_2)$ nicht

3 qubit bit flip code (Fort.)

Fehlerdiagnose (Fort.):

Wir messen die beiden Observablen Z_1Z_2 und Z_2Z_3. Das Messtupel $(\pm 1, \pm 1)$ nennen wir *Fehlersyndrom.*

Unter der Annahme, dass höchstens ein Qubit fehlerhaft ist, wird dieses damit eindeutig lokalisiert.

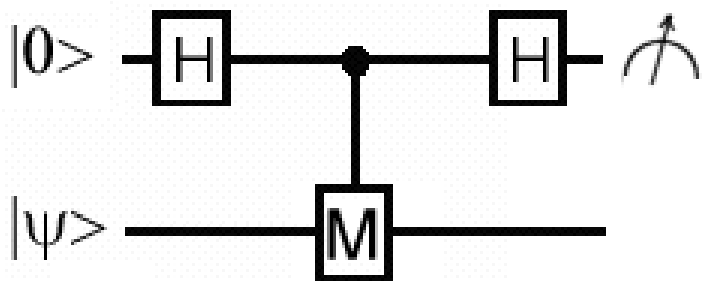
Beachte: *Fehlersyndrom* enthält *keine* Information über den präparierten Zustand $a|0_L\rangle + b|1_L\rangle$!

Fehlerkorrektur: Anwenden von X_k auf dem kodierten Zustand

Messung von Observablen

Schaltkreis für Messung einer Observablen M mit Eigenwerten ± 1?

$\rightarrow$ Messung 1.Qubit im folg. Schaltkreis: Phase ϕ von $m = e^{\pi i \phi}$



Sei $|\psi_{\pm 1}\rangle$ die Eigenbasis von M. Dann gilt:

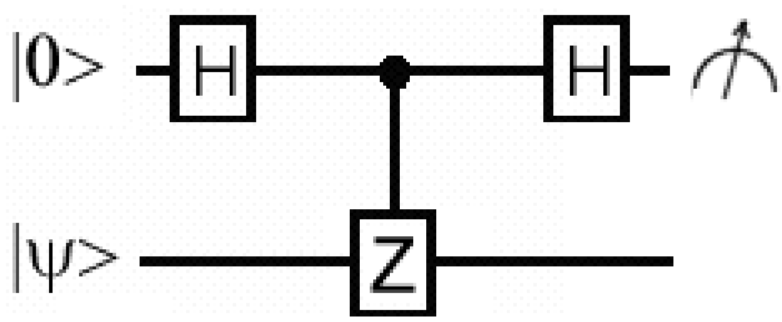
$$|0\rangle|\psi_{\pm 1}\rangle \mapsto \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)|\psi_{\pm 1}\rangle \mapsto \frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right)|\psi_{\pm 1}\rangle \mapsto \begin{cases} |0\rangle|\psi_{+1}\rangle \\ |1\rangle|\psi_{-1}\rangle \end{cases}$$

d.h. $m = e^{\pi i \cdot 0} = +1$ bei $|\psi_{+1}\rangle$ und $m = e^{\pi i \cdot 1} = -1$ bei $|\psi_{-1}\rangle$.
Für $|\psi\rangle = \alpha|\psi_{+1}\rangle + \beta|\psi_{-1}\rangle$ folgt $p(+1) = |\alpha|^2$ und $p(-1) = |\beta|^2$.

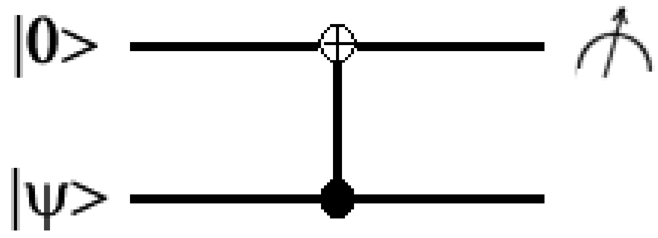
3 qubit bit flip code (Fort.)

Quantenschaltkreis für die Messung der Observablen $Z_1 Z_2$?

Zunächst: Messung der Observablen Z (Eigenwerte: ± 1)



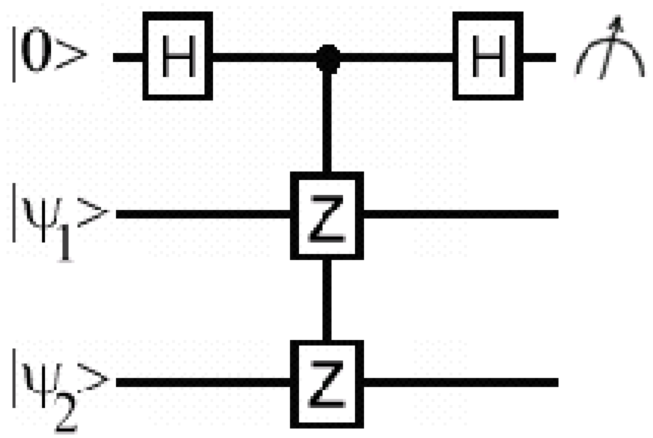
Dieser Schaltkreis lässt sich vereinfachen:

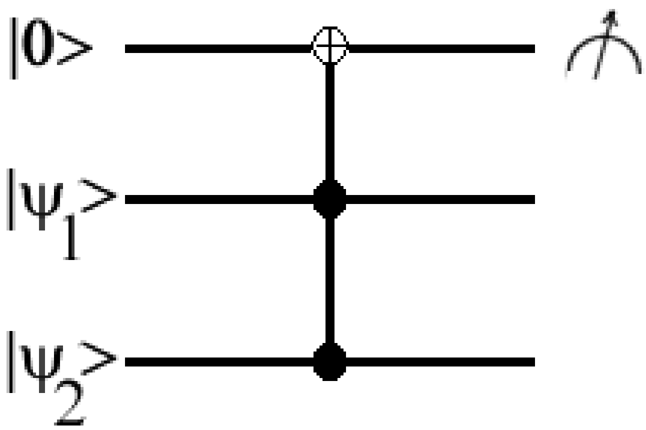


3 qubit bit flip code (Fort.)

Quantenschaltkreis für die Messung der Observablen Z_1Z_2? (Fort.)

Die Erweiterung auf Observablen wie Z_1Z_2 ist nun leicht:

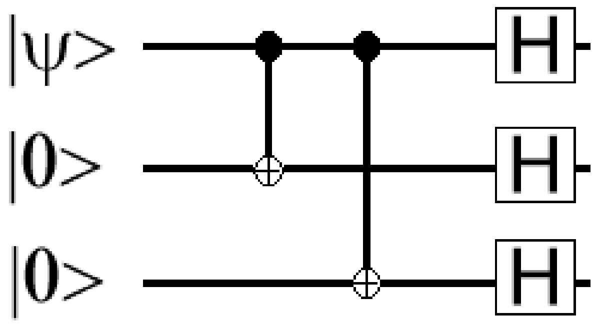




3 qubit phase flip code

Jetzt: Korrekturverfahren für *phase flip*, d.h. für $|\psi\rangle \mapsto Z|\psi\rangle$

- *Beobachtung:*
  $|+\rangle := H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,, \quad |-\rangle := H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
  $\Rightarrow Z|+\rangle = |-\rangle$ und $Z|-\rangle = |+\rangle$
  d.h. in der *Basis* $\{|+\rangle, |-\rangle\}$ operiert Z wie ein *bit flip*
- *Idee:* Verwende Kodierung $|0_L\rangle = |+++\rangle$, $|1_L\rangle = |---\rangle$
- *Schaltkreis* für die Kodierung:



3 qubit phase flip code (Fort.)

- *Fehlerdiagnose:*

  Nach Wechsel in Basis $\{|0\rangle, |1\rangle\}$ Fehler mit $Z_1 Z_2$ und $Z_2 Z_3$ diagnostizieren, dann wieder zurück in Basis $\{|+\rangle, |-\rangle\}$

  Entspricht den Observablen

$$H_1 H_2 H_3\, Z_1 Z_2\, H_1 H_2 H_3 = X_1 X_2$$

$$H_1 H_2 H_3\, Z_2 Z_3\, H_1 H_2 H_3 = X_2 X_3$$

  (wegen $H^\dagger = H$ und $HZH = X$)

- *Fehlerkorrektur:* Anwenden von $H_k X_k H_k = Z_k$

9 Qubit Shor Code

Was wenn *bit flip* **und** *phase flip* möglich? $\rightarrow$ Codes kombinieren

- Kodiere $|0\rangle, |1\rangle$ mit *3 qubit phase flip code*

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

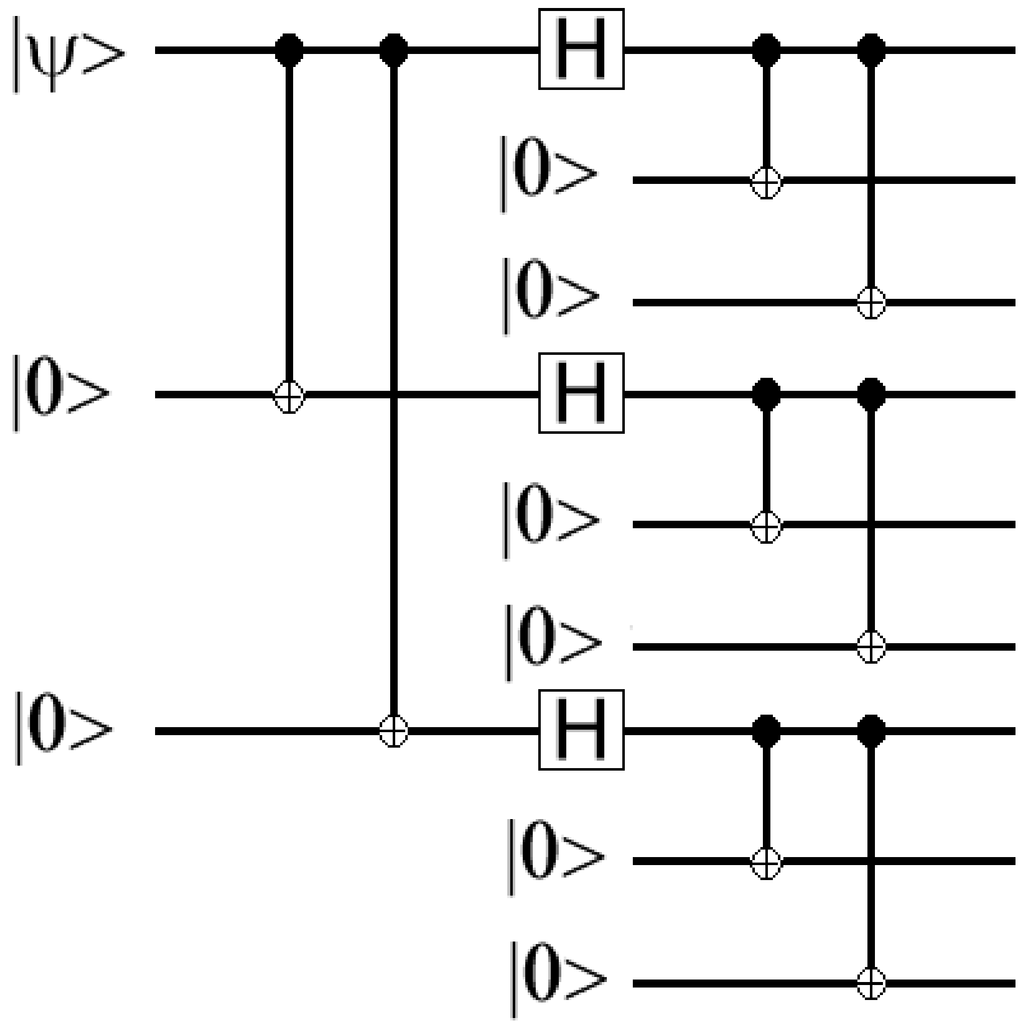
- Dann kodiere jedes der 3 Qubits mit *3 qubit bit flip code*

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

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

- Schaltkreis zur Kodierung: Konkatenation der Schaltkreise für *phase flip code* und *bit flip code*

9 Qubit Shor Code: Schaltkreis zur Kodierung



9 Qubit Shor Code (Fort.)

Logische Codewörter:

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

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

Fehlerdiagnose:

- *bit flip* X_k in einem der 9 Qubits: Diagnose wie gehabt
  Im ersten 3er-Block mit $Z_1 Z_2$ und $Z_2 Z_3$, andere Blöcke analog.
  Korrektur mit X_k.
- *phase flip* Z_k in einem der 9 Qubits: Messung der Observablen

$$X_1 X_2 X_3 X_4 X_5 X_6 = H_1..H_6 Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 H_1..H_6$$

$$X_4 X_5 X_6 X_7 X_8 X_9 = H_4..H_9 Z_4 Z_5 Z_6 Z_7 Z_8 Z_9 H_4..H_9$$

9 Qubit Shor Code (Fort.)

- Fehlerdiagnose *phase flip* (Fort).

  Denn Messung von $X_1X_2X_3$ ergibt mit Wahrscheinlichkeit 1

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

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

  (andere 3er-Blöcke analog)

  Korrektur des *phase flips* mit $Z_1Z_2Z_3$ (bzw. analog)

- *phase flip* **und** *bit flip* gleichzeitig: z.B. Z_1X_1

  Grundlegende Beobachtung: M Observable, die gleichzeitig *unitär* ist. Dann gilt: Messung von M auf Zustand $|\psi\rangle$ identisch mit Messung von M auf $M|\psi\rangle$.

  Denn: $p(m) = \langle\psi|M^\dagger P_m M|\psi\rangle = \langle\psi|P_m|\psi\rangle$, da M und P_m wegen $M = \sum_m mP_m$ kommutieren.

9 Qubit Shor Code (Fort.)

Messung von $Z_1 Z_2$ auf $Z_1 X_1|\psi\rangle \hat{=}$ Messung von $Z_1 Z_2$ auf $X_1|\psi\rangle$

$\Rightarrow$ Bei Auftreten des Fehlers $Z_1 X_1$ wird im ersten Schritt der *bit flip* X_1 mit den Observablen $Z_1 Z_2$ und $Z_2 Z_3$ korrekt diagnostiziert.

Korrektur ergibt $X_1 Z_1 X_1 = -Z_1 X_1^2 = -Z_1$, da $\{X, Z\} = 0$

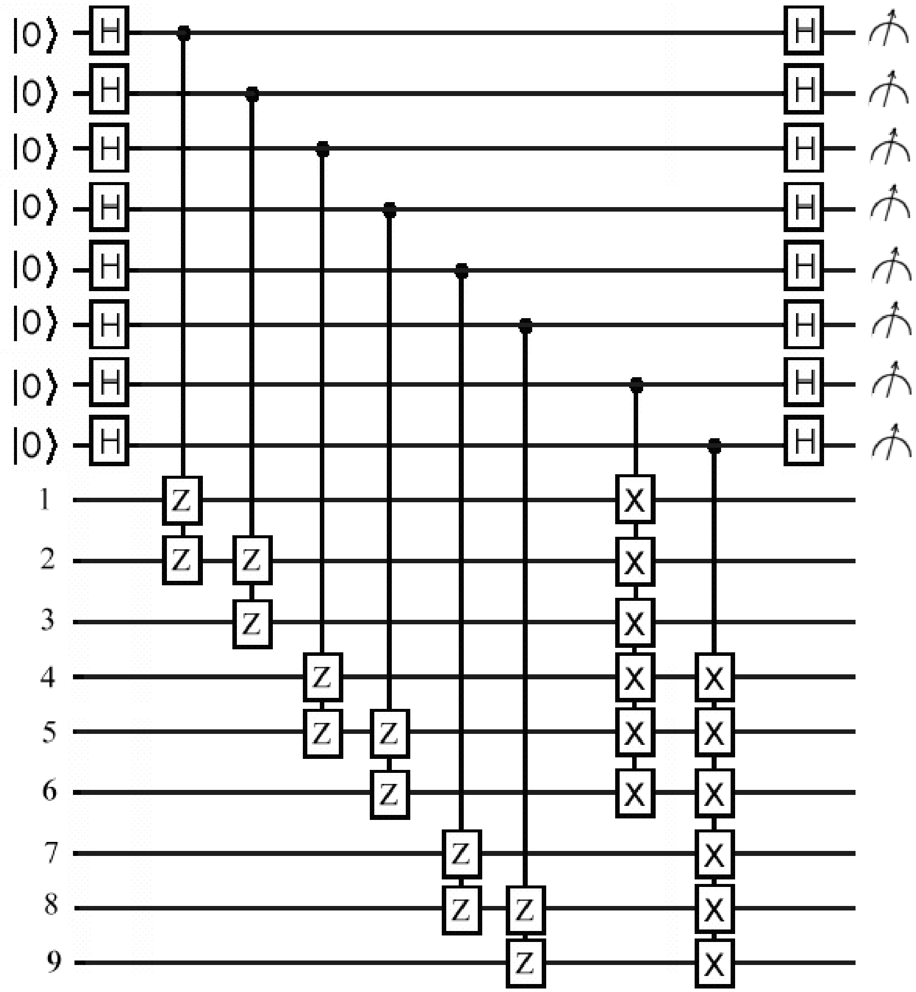
$\Rightarrow$ Zweiter Schritt diagnostiziert und korrigiert *phase flip* Z_1

Übrig bleibt eine für die Quantenmechanik unerhebliche *Phase* $-I$

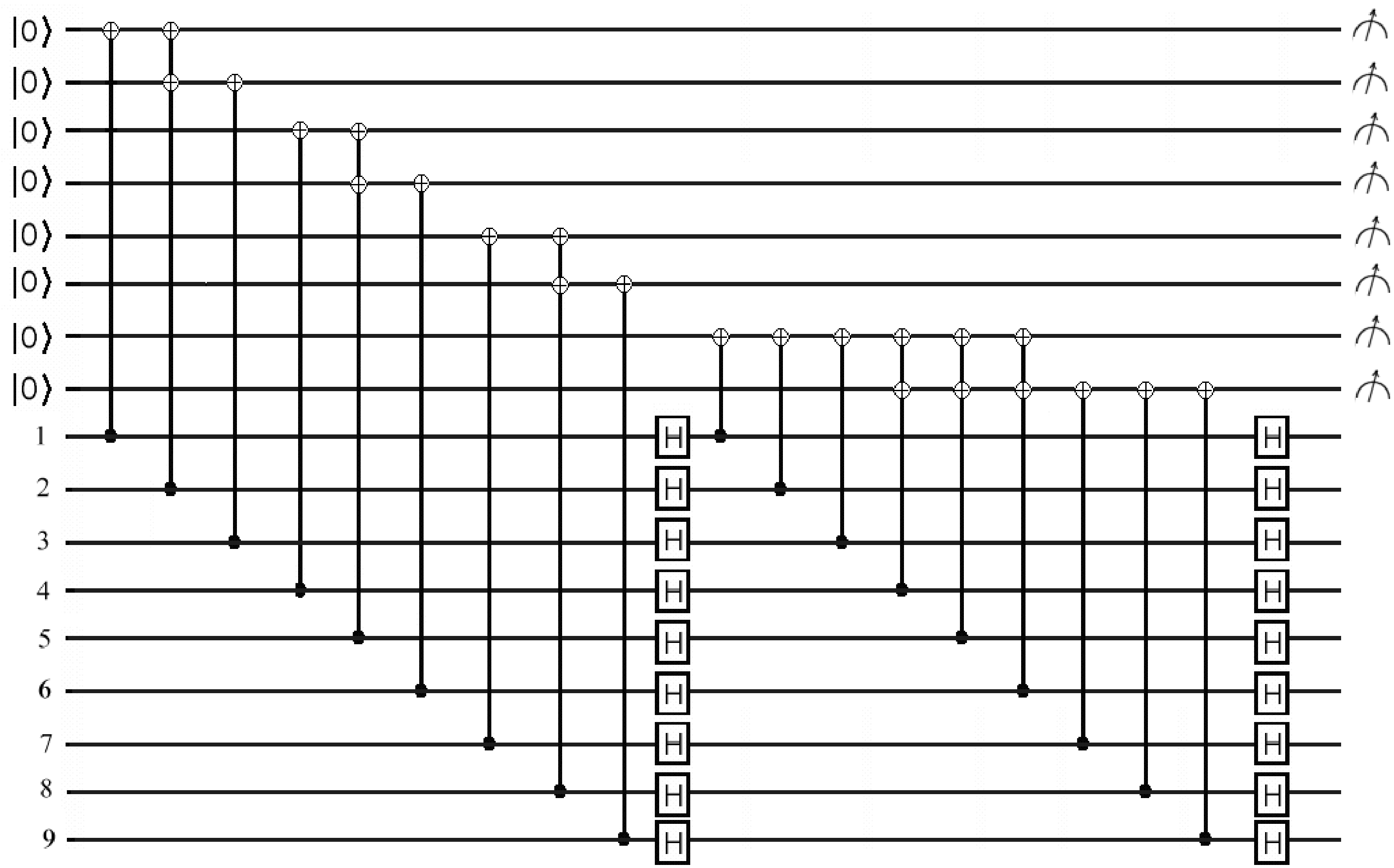
Fazit: Shor Code korrigiert Fehler X, Z, $iXZ = Y$, sofern nur *ein* Qubit fehlerhaft ist.

Tatsächlich kann der Shor Code jedoch noch mehr: Er korrigiert *beliebige* Fehler auf einem Qubit!

9 Qubit Shor Code: Schaltkreis zur Fehlerdiagnose



9 Qubit Shor Code: Schaltkreis (vereinfacht)



9 Qubit Shor Code (Fort.)

Beliebiger unitärer Operator auf einem Qubit als Fehler

Lemma:

$$U \in \mathbb{C}^{2\times 2} \text{ unitär} \Leftrightarrow U = e^{i\phi} \underbrace{\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}}_{=:A}$$

mit $\det A = |\alpha|^2 + |\beta|^2 = 1$, d.h. $A \in SU(2)$

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 $\sum_i a_i^2 = 1$.

9 Qubit Shor Code (Fort.)

Gegeben sei $|\psi\rangle$ ein 9-Qubit-Codewort zusammen mit den acht Ancilla Qubits ($\rightarrow$ Fehlersyndrom) im Zustand $|0_8\rangle = |00000000\rangle$.

Tritt nun ein Fehler E im Codewort auf (o.E. im ersten Qubit)

$$E|\psi\rangle|0_8\rangle = e^{i\phi}\left(e_0|\psi\rangle|0_8\rangle + e_1X_1|\psi\rangle|0_8\rangle + e_2Z_1|\psi\rangle|0_8\rangle + e_3Y_1|\psi\rangle|0_8\rangle\right)$$

Die Fehlerdiagnose liefert wegen Linearität

$$e^{i\phi}\left(e_0|\psi\rangle|S_I\rangle + e_1X_1|\psi\rangle|S_{X_1}\rangle + e_2Z_1|\psi\rangle|S_{Z_1}\rangle + e_3Y_1|\psi\rangle|S_{Y_1}\rangle\right)$$

wobei S_{X_1} das Fehlersyndrom für den Fehler X_1 bezeichnet usw.

Wegen $\sum_i |e_i|^2 = 1$ und der Tatsache, dass die Fehlersyndrom $|S_{I,X_1,Y_1,Z_1}\rangle$ orthogonal sind, stellt dies tatsächlich einen zulässigen Quantenzustand dar.

9 Qubit Shor Code (Fort.)

Bei Messung der Ancillas kollabiert der Zustand deshalb in einen der vier Zustände

$$|\psi\rangle|S_I\rangle,\ X_1|\psi\rangle|S_{X_1}\rangle,\ Z_1|\psi\rangle|S_{Z_1}\rangle,\ X_1Z_1|\psi\rangle|S_{Y_1}\rangle$$

Die Fehlerkorrektur im Codewort läuft nun wie gehabt weiter.

Bemerkenswert: Kontinuierliche Menge von Fehlern lässt sich korrigieren, indem eine endliche diskrete (noch dazu kleine) Menge von Fehlern korrigiert werden kann!

Beispiel: Beliebiger *phase error*

$$R_{\theta/2} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} = e^{i\theta/2} \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Z$$

Fault Tolerant Quantum Computation

Anwendung des Shor Codes in einem Quantenrechner

- Kodiere Input des Algorithmus
- Führe Operationen des Algorithmus *direkt* auf den kodierten Zuständen aus
  $\rightarrow$ Gatter entsprechend transformieren!
- Führe regelmäßig Fehlerdiagnose und ggf. Korrektur der Codewörter durch
- Dekodiere am Ende des Algorithmus und messe das Ergebnis der Berechnung

Ausblick: Gibt es weitere Codes? – JA! ($\rightarrow$ Literatur)