Dekohärenz und Grundprinzip der Quantenfehlerkorrektur

Bachelorarbeit

Gregor Wurm,
Betreuer: Prof. E. Arrigoni

Institut für Theoretische Physik
der Technischen Universiät Graz

24. Sept. 2010

Übersicht

1. Quantenfehler
   - Qubit, Bit
   - Quantenverschränkung
   - Dekohärenz
   - unitäre Operatoren
2. Klassische Fehlerkorrektur
   - Codierungstheorie
   - Hammingcode
3. Quantenfehlerkorrektur
   - 3- Qubit- Code
4. 7- Qubit- Code

Der Unterschied zwischen Qubit und Bit

Bit:

- Nur diskrete Zustände 0 oder 1
- Messung des Bits möglich
- Technische Umsetzung durch makroskopische Anzahl von Atomen

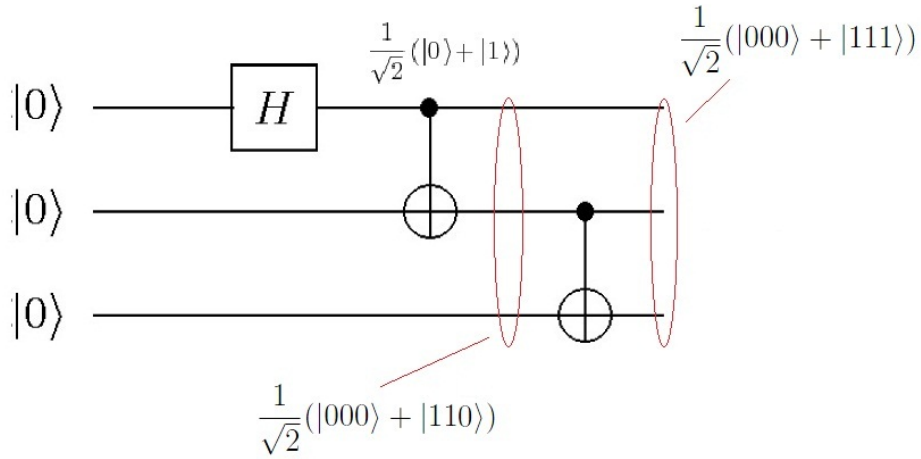
Qubit:

- Unendlich viele Zustände möglich
- Kann nur durch QM beschrieben werden
- Superpositionsprinzip: $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$
- Messung zerstört die Superposition
- Technische Umsetzung mit einem einzelnen Atom

Quantenverschränkung: GHZ- Zustand

- Hadamard- Gatter überführt $|0\rangle$ und $|1\rangle$ in überlagerte Zustände $\rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- CNOT- Gatter transformiert die Zustände $|a\rangle$ und $|b\rangle$ zweier Qubits zu $|a\rangle\,|b\rangle \rightarrow |a\rangle\,|a \oplus b\rangle$

Bsp. eines Quantennetzwerk:



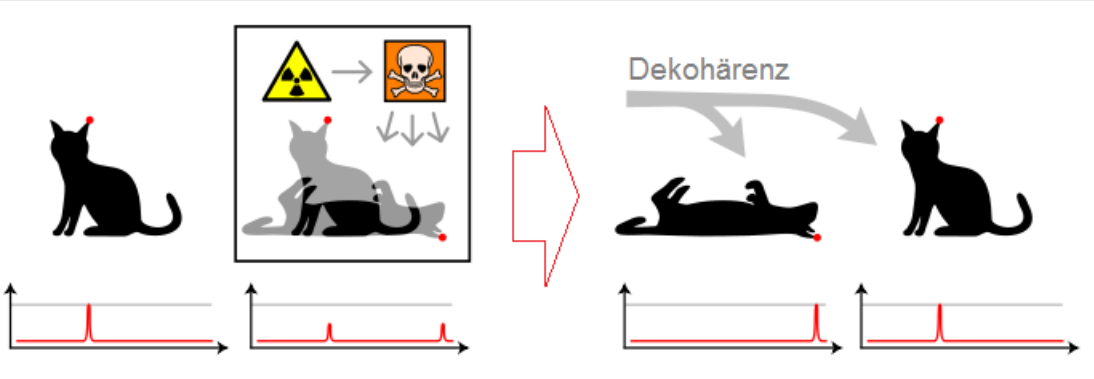
$\rightarrow$ Verschränkter Zustand:

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

Dekohärenz

Ein Dekohärenzprozess zerstört bzw. verändert die Phaseninformation quantenmechanischer Zustände.

Beispiel: Schrödingers Katze



- QM beschreibt ein physikalisches System mittels Wellenfunktion;
  - Wellenfunktion beschreibt die Überlagerung von Zuständen;
- Das Beobachten entspricht einer qm. Messung $\rightarrow$ Kollaps der Wellenfunktion in einen der Zustände;

Fehlerkorrektur

Wichtige Annahmen

- Das Auftreten eines Fehlers ist unabhängig von anderen Fehlern.
- Ein Fehlerprozess beeinflusst nur ein Qubit auf einmal;

  Bsp.: Mögliche Auswirkungen eines Fehlers auf einem GHZ-Zustand sind:
  $|111\rangle + |000\rangle\,, |011\rangle + |100\rangle\,, |101\rangle + |010\rangle\,, |110\rangle + |001\rangle.$

- Zur Vereinfachung werden kontinuierliche Fehler nicht betrachtet.

Wechselwirkung mit der Umgebung

Dekohärenz bewirkt eine Verschränkung der Qubits mit der Umgebung:

$$\begin{aligned}\alpha|1\rangle + \beta|0\rangle \rightarrow & +(\alpha|0\rangle + \beta|1\rangle) \otimes |A_{\text{kein Fehler}}\rangle_{\text{Umgeb.}} \\ & +(\alpha|1\rangle + \beta|0\rangle) \otimes |A_{\text{Bit-Flip}}\rangle_{\text{Umgeb.}} \\ & +(\alpha|0\rangle - \beta|1\rangle) \otimes |A_{\text{Phasen}}\rangle_{\text{Umgeb.}} \\ & +(\alpha|1\rangle - \beta|0\rangle) \otimes \underbrace{|A_{\text{Phasen-Flip}}\rangle_{\text{Umgeb.}}}_{\text{Zustand der Umgebung}}\end{aligned}$$

$\rightarrow$ es können drei verschiedene Fehler auftreten:

1. Bit-Flip- Fehler
2. Phasenfehler
3. Phasen-Flip- Fehler

Pauli-Matrizen

Quantenfehler können mithilfe von Pauli-Matrizen beschrieben werden:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

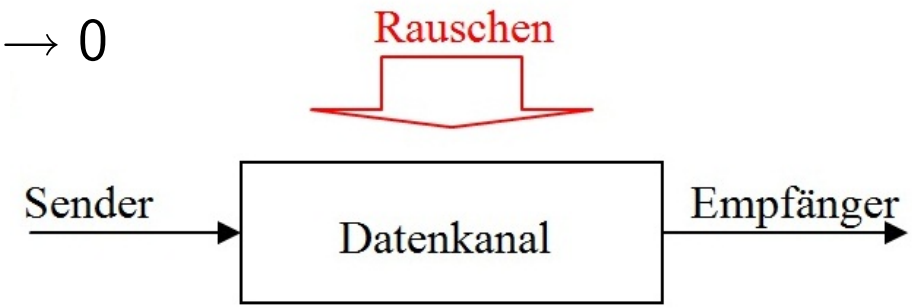
Wirkung auf ein Qubit $|a\rangle$:

$$\begin{aligned} X|a\rangle &= |a \oplus 1\rangle && \rightarrow \text{Bit-Flip- Fehler} \\ Y|a\rangle &= i(-1)^a |a \oplus 1\rangle && \rightarrow \text{Phasen-Flip- Fehler} \\ Z|a\rangle &= (-1)^a |a\rangle && \rightarrow \text{Phasenfehler} \end{aligned}$$

Klassische Fehler

Durch Rauschen im Datenkanal können Fehler auftreten:

- Bit-Flip- Fehler $0 \longrightarrow 1$ oder $1 \longrightarrow 0$
- Bit- Relaxation $1 \longrightarrow 0$



$\longrightarrow$ Fehlerkorrektur ist notwendig!

Einfacher Code: Wiederholungscode

Nutzdaten mit zusätzlicher Redundanz:

$$0 \longrightarrow 000, \qquad 1 \longrightarrow 111$$

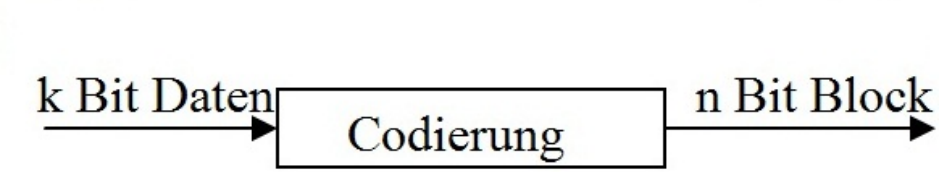
Mittels Mehrheitsentscheid kann der Fehler korrigiert werden.

Beispiel: $000 \longrightarrow 010 \longrightarrow 000$

Codierungstheorie

Grundlegendes Konzept:

- Daten werden codiert $\longrightarrow$ Codewörter
- Codewort = Daten + Kontrollbits



  - Redundanz: $r = n - k$
- Empfänger überprüft die Daten $\longrightarrow$ Syndrombestimmung
- Syndrom liefert die genaue Position des Fehlers

Codierungstheorie

- Blockcode: [n,M,d]-Code
  - besteht aus 2^M Codewörtern c gleicher Länge n;
  - Codewörter bestehen aus Elementen der Menge $\{0, 1\}$;
  - d entspricht der minimalen Hammingdistanz;
- Hammingdistanz d(A,B)
  - Anzahl der unterschiedlichen Stellen von zwei Codewörter $A, B \in C$; Bsp.: $d(A, B) = d(1111, 0010) = 3$
  - minimale Hammingdistanz $\rightarrow$ minimalste Distanz aller Codewörter in einem Blockcode C;

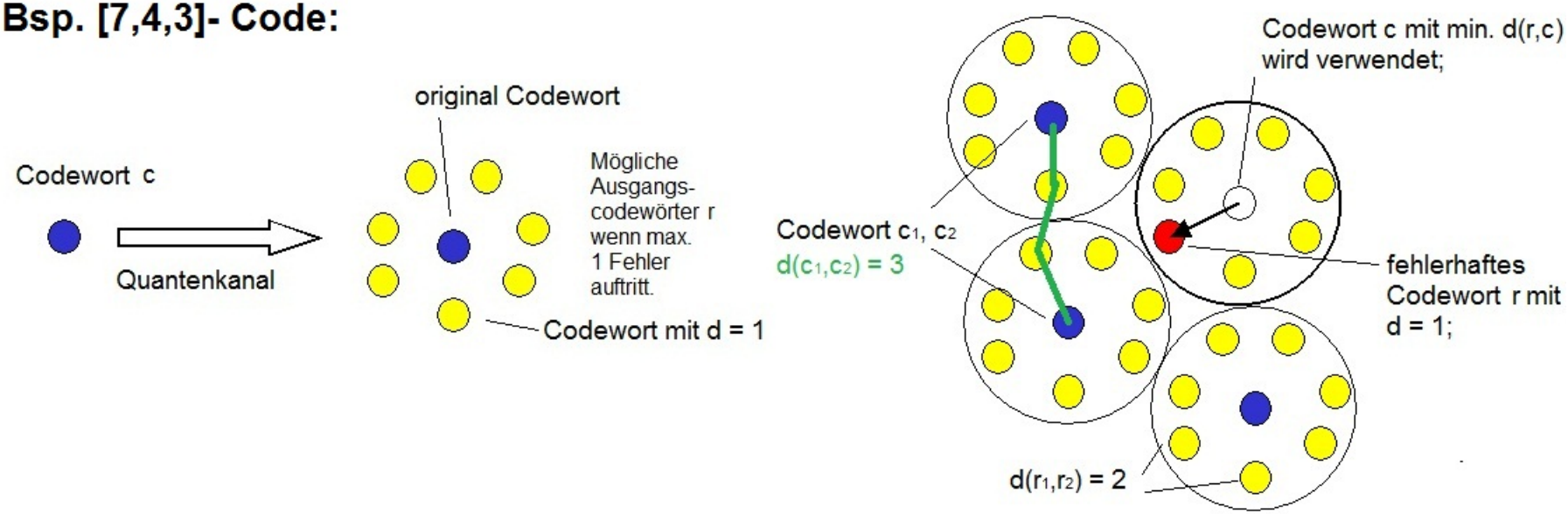
Bsp.: C beinhaltet die 4 Codewörter A, B, C, D:

	Daten		redundantes Codewort
A =	00	$\rightarrow$	000000
B =	01	$\rightarrow$	010101
C =	10	$\rightarrow$	101010
D =	11	$\rightarrow$	111111

Fehlerkorrektur

Über die minimale Hammingdistanz ist die Anzahl der korrigierbaren Fehler definiert.

Bsp. [7,4,3]- Code:



Der Decodierer wählt das „näheste“ Codewort.

Definition

Mit einem Blockcode C können $\left[\frac{d-1}{2}\right]$ Fehler korrigiert und $[d-1]$ Fehler erkannt werden.

Hammingcode

Der Hammingcode ist ein linearer fehlerkorrigierender Blockcode:

- Codiert 4 Bits Information in 7 Bits $\rightarrow$ [7,4,3]-Code;
- Minimale Hammingdistanz $d = 3$
- $\left[\frac{d-1}{2}\right] = 1 \rightarrow$ Korrektur von Einfachfehlern;
- Syndrom über Kontrollmatrix H;
- Dient als Grundlage für Quantencodes;

Kontrollmatrix

Spaltenvektoren j entsprechen der Binärdarstellung der Spaltenummer j.

Kontrollmatrix

$$H = \underbrace{\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}}_{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}}$$

Erzeugung der Generatormatrix

Durch Spalten vertauschen folgt:

$$\bar{H} = H \cdot S = \left[P^T I_3\right] = \underbrace{\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}}_{\begin{pmatrix} 7 & 6 & 5 & 3 & 4 & 2 & 1 \end{pmatrix}}$$

S...Permutationsmatrix

$$\bar{G} = [I_4 P] = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \Rightarrow G = \bar{G} \cdot S^T$$

Durch Spalten zurücktauschen mit $S^T \rightarrow$ Generatormatrix

Generatormatrix

$$G = \underbrace{\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}}_{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}}$$

- Codierung der Nutzdaten D: $C = D \cdot G$
- Kontrollmatrix ist orthogonal zu den Codewörtern $\rightarrow C \cdot H^T = 0$.
- Syndrom: $C \cdot H^T \neq 0 \rightarrow$ Binärdarstellung der j-ten Spalte inwelchen sich der Fehler befindet.

Beispiel: [7,4,3]- Code

4- Bit Datenwort D = 1011 wird codiert.

$$C = D \cdot G = \begin{pmatrix} 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} = 1010\underline{1}01.$$

Bei Bit-Flip-Fehler an der 5.Stelle $\rightarrow x = \text{Fehler(C)} = 1010\underline{0}01$

$$x \cdot H^T = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix} = 5$$

Quantenfehlerkorrektur

Folgende Probleme treten dabei auf:

- No-Cloning-Theorem
  - Quantenmechanische Zustände können nicht kopiert werden;
  - $a|0\rangle + b|1\rangle \rightarrow (a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle)$
- Phasenfehler: $|0\rangle \rightarrow |0\rangle$, $|1\rangle \rightarrow -|1\rangle$;
- Kollaps der Quantenzustände durch Messung;

Folgerung

Eine klassische Fehlerkorrektur in Quantencomputern ist unmöglich.

Abhilfe

Lösung der Probleme:

- Informationsbits mit „Hilfsqubits“ verschränken
  - $|\psi\rangle \rightarrow (|111\rangle + |000\rangle)$
  - Erzeugung von redundanten Zuständen mithilfe von CNOT-Gattern;
- Messung der „Hilfsqubits“ liefert Information über Fehler $\rightarrow$ Fehlersyndrom

Grundgedanke

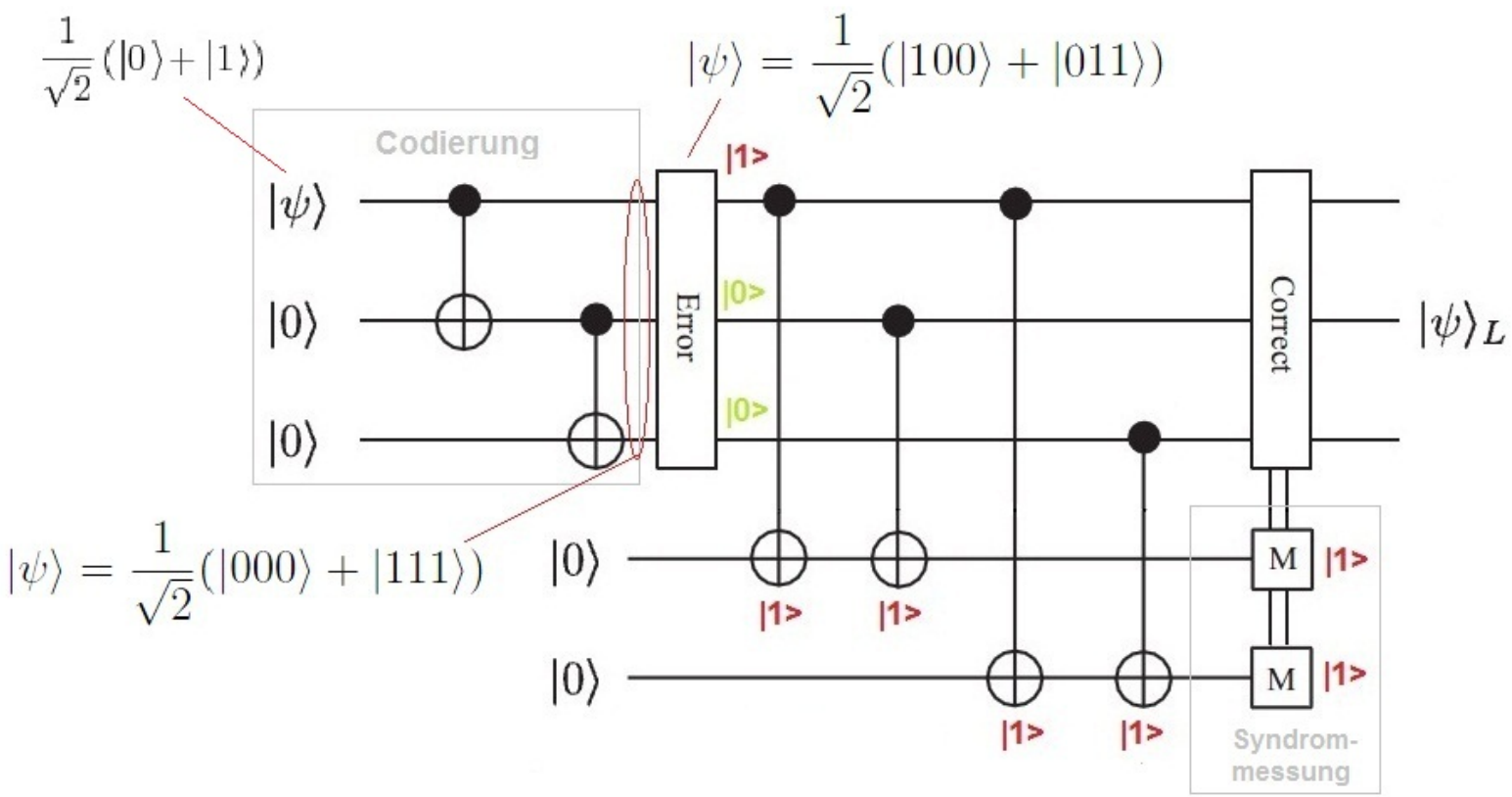
Im Prinzip wird versucht die Fehler zu messen, ohne dabei das Informationsbit zu beeinflussen.

3- Qubit- Code

Eigenschaften des 3-Qubit-Codes:

- Kein vollständiger Quantencode;
  - kann Bit-Flip-Fehler und Phasenfehler nicht gleichzeitig korrigieren;
- Codiert ein logisches Qubit in drei physikalische Qubits;
  - $|\psi\rangle \rightarrow (|111\rangle + |000\rangle)$
- Fehlererkennung mittels Syndrommessung;
- Einfachfehler korrigierender Code;

Schaltbild für den 3-Qubit-Code

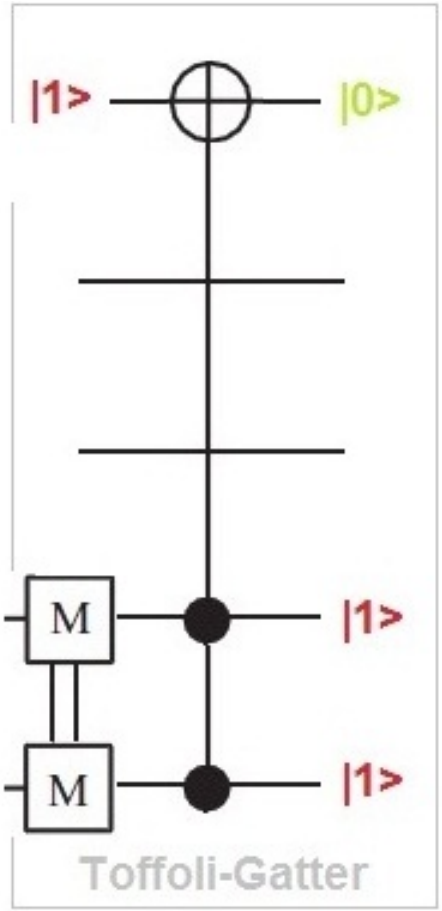


Bit-Flip	Zustand	Syndrom
kein Fehler	$\|000\rangle + \|111\rangle$	$\|00\rangle$
Qubit 1	$\|100\rangle + \|011\rangle$	$\|11\rangle$
Qubit 2	$\|010\rangle + \|101\rangle$	$\|10\rangle$
Qubit 3	$\|001\rangle + \|110\rangle$	$\|01\rangle$

Syndrom liefert die Position des Fehlers; Qubit 1 wird nicht gemessen!

3- Qubit- Code: Wiederherstellung

- Qubit 1 entspricht dem Datenbit;
- Bsp.: Bei Syndromzustand $|11\rangle \rightarrow$ Qubit 1 flippen;
- Toffoli- Gatter:
  - Qubit 2 und 3 werden abgegriffen;
  - Nur wenn Qubit 2 und 3 im Zustand $|1\rangle \rightarrow$ Qubit 1 wird geflippt;



7-Qubit Steane Code

Eigenschaften:

- Vollständiger Quantencode
  - kann Bit-Flip-Fehler und Phasenfehler gleichzeitig korrigieren;
- Codiert ein logisches Qubit in 7 physikalische Qubits;
- Als Basis dient der [7,4,3]- Hammingcode;
- Es werden zwei lineare [n,M,d]- Codes verwendet
  - $\rightarrow$ CSS- Code;
- Einfachfehler korrigierender Code;

Dual- Code

- Gegeben ist ein lineare Code C mit
  - Generatormatrix G und
  - Kontrollmatrix H.
  - z.B.: Hammingcode
- Für den dazugehörigen Dual- Code gilt:
  - Linearer Code $C_2^\perp$ mit
  - Generatormatrix $G_2^\perp = H$ und
  - Kontrollmatrix $H_2^\perp = G$.
- Codewörter von $C_2^\perp$
  - stehen orthogonal zu allen Codewörter $v \in C$
  - $C_2^\perp = \{v \in F_2^n : v \cdot c = 0 \forall c \in C\}$
- $C_2^\perp \subseteq C_1 \subseteq F_2^n$

CSS- Code

Kontrollmatrix H, Generatormatrix G

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \widehat{=} \quad G_2^{\perp} \rightarrow [7,3,4]\text{- Code}$$

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \widehat{=} \quad H_2^{\perp} \rightarrow [7,4,3]\text{- Code}$$

$\rightarrow [n, M_1 - M_2, min(d)] - \text{Code} = [7,1,3] - \text{ CSS- Code}$

Konstruktion des Steane Codes

Anforderungen an die Codewörter:

- Codewörter von $C_2^{\perp}$ müssen orthogonal zu C_1 stehen;
- Kontrollmatrix von C_1 entspricht der Generatormatrix von $C_2^{\perp}$;

Zustände des Steane Codes (Basis 1)

$$|0\rangle_{code} = \frac{1}{\sqrt{8}} \sum_{\substack{\text{even v} \\ \in Hamming}} |v\rangle = \frac{1}{\sqrt{8}}(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle),$$

$$|1\rangle_{code} = \frac{1}{\sqrt{8}} \sum_{\substack{\text{odd v} \\ \in Hamming}} |v\rangle = \frac{1}{\sqrt{8}}(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle).$$

Basiszustände

Um Bit-Flip- und Phasenfehler zu korrigieren unterscheidet man zwischen Basis 1 und Basis 2.

- Basis 2 mit $\left|\bar{0}\right\rangle$ und $\left|\bar{1}\right\rangle$ kann als Superposition von Zuständen der Basis 1 mit $|0\rangle_{code}$ und $|1\rangle_{code}$ geschrieben werden
- Bsp.: Basis 2 für 1 Qubit:

$$\left|\bar{0}\right\rangle = |0\rangle_{code} + |1\rangle_{code}$$
$$\left|\bar{1}\right\rangle = |0\rangle_{code} - |1\rangle_{code}$$

- $\rightarrow$ Hadarmardgatter transformieren Basis 1 in Basis 2
- $\rightarrow$ Phasenfehler werden in Bit-Flip- Fehler transformiert

Rotation der Basis 1

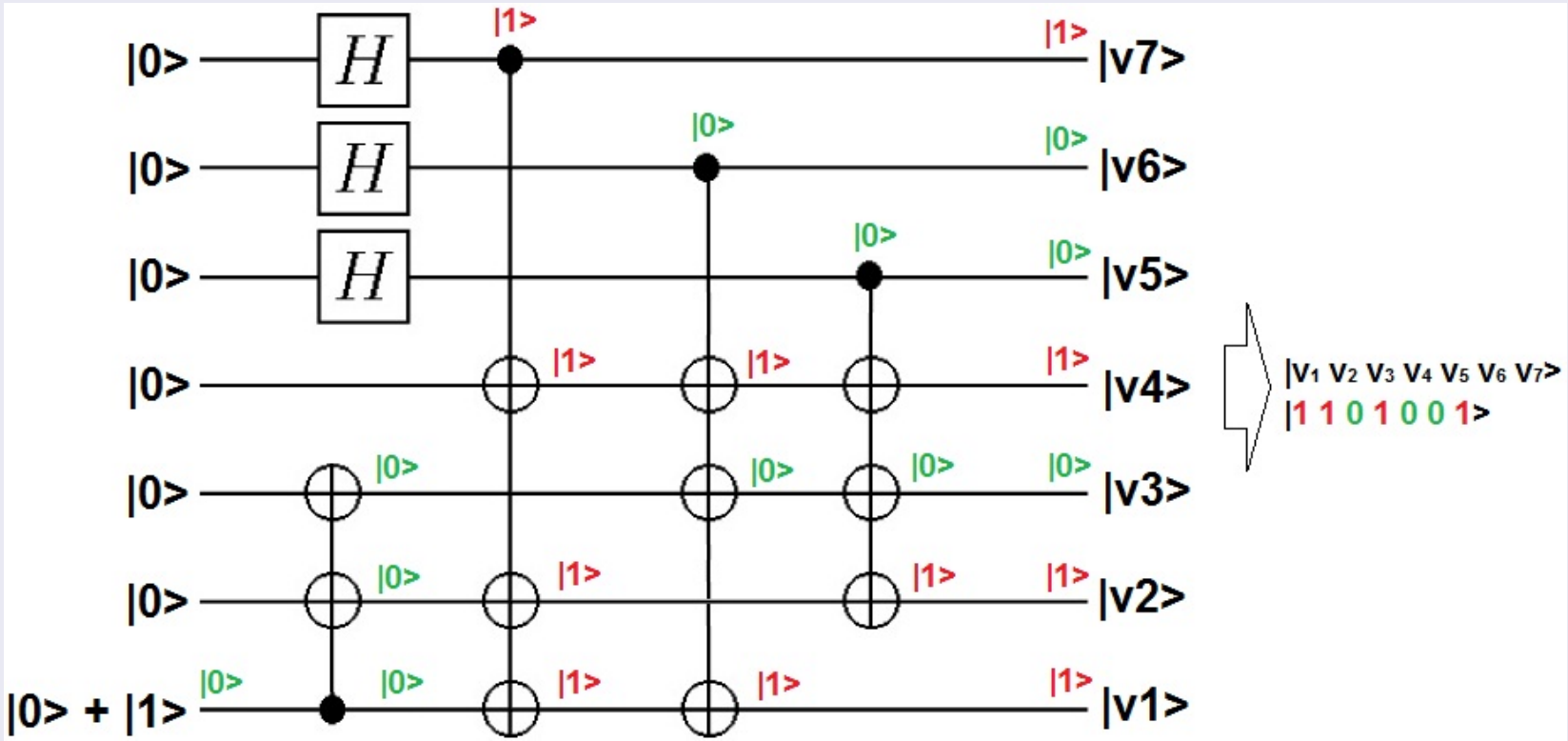
Durch das Anwenden einer Hadamardrotation erhält man Basis 2 Zustände:

Basis 2

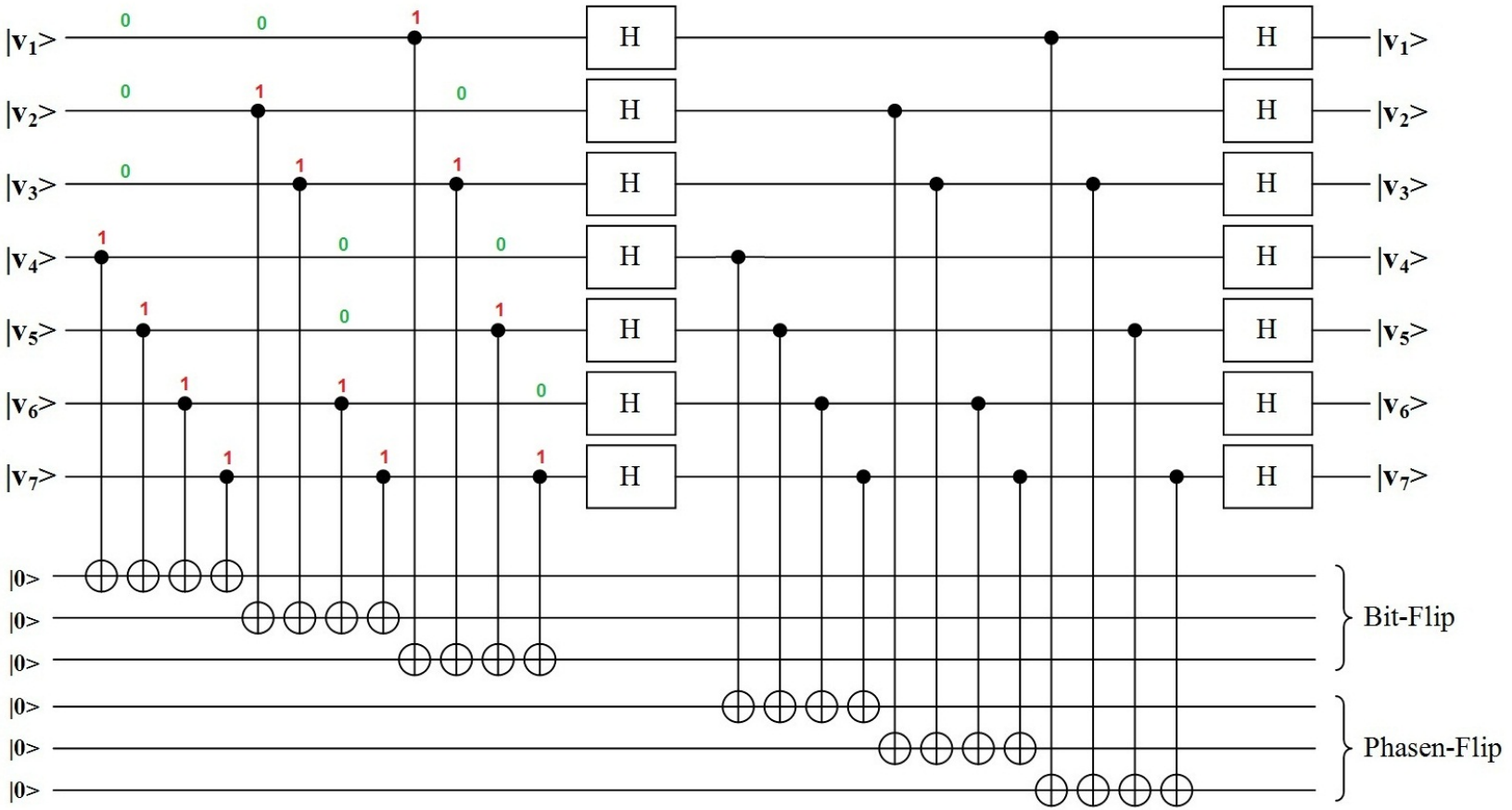
$$|\bar{0}\rangle_{code} = \frac{1}{4} \sum_{v \in Hamming} |v\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{code} + |1\rangle_{code})$$

$$|\bar{1}\rangle_{code} = \frac{1}{4} \sum_{v \in Hamming} (-1)^{wt(v)} |v\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{code} - |1\rangle_{code})$$

Codierschaltung



Syndrommessung



Zusammenfassung

- Quantenrauschen oder Dekohärenz bewirken Fehler im Datenblock:
  - Bit-Flip- Fehler
  - Phasenfehler
  - Phasen-Flip- Fehler
- Korrektur der Fehler mittels Redundanz;
- Keine direkte Messung des Informationsqubits;
- Quantenfehlerkorrektur baut auf klassische Fehlerkorrektur auf;

Vielen Dank...

für Ihre Aufmerksamkeit!