

Quantenfehlerkorrekturcodes

Christian Hartler

2. Dezember 2009

- Unterschiede zwischen klassischem Computer und Quantencomputer

- Unterschiede zwischen klassischem Computer und Quantencomputer
- Quantengatter

- Unterschiede zwischen klassischem Computer und Quantencomputer
- Quantengatter
- Auftretende Fehler im Quantencomputer und mögliche Korrekturen:
 - Bitfehler
 - Phasenfehler

- Unterschiede zwischen klassischem Computer und Quantencomputer
- Quantengatter
- Auftretende Fehler im Quantencomputer und mögliche Korrekturen:
 - Bitfehler
 - Phasenfehler
- Fehlerkorrekturcodes
 - 9QECC
 - 7QECC

Unterschiede zwischen klassischem Computer und Quantencomputer

Klassisch

Quantenmechanisch

Unterschiede zwischen klassischem Computer und Quantencomputer

Klassisch

- Bit 0: 0 bis 1 V
Bit 1: 3 bis 5 V

Quantenmechanisch

- QBit $|0\rangle$: $|\uparrow\rangle$
QBit $|1\rangle$: $|\downarrow\rangle$
Relative Phase zwischen $|1\rangle$ und $|0\rangle$

Unterschiede zwischen klassischem Computer und Quantencomputer

Klassisch

- Bit 0: 0 bis 1 V
Bit 1: 3 bis 5 V

- Es tritt nur 1 Zustand auf:
Entweder Bit 0 oder Bit 1

Quantenmechanisch

- QBit $|0\rangle$: $|\uparrow\rangle$
QBit $|1\rangle$: $|\downarrow\rangle$
Relative Phase zwischen $|1\rangle$ und $|0\rangle$

- Superpositionsprinzip:
 $|\Psi\rangle = |\rightarrow\rangle = a|0\rangle + b|1\rangle$
Mit $|a|^2 + |b|^2 = 1$

Unterschiede zwischen klassischem Computer und Quantencomputer

Klassisch

- Bit 0: 0 bis 1 V
Bit 1: 3 bis 5 V
- Es tritt nur 1 Zustand auf:
Entweder Bit 0 oder Bit 1
- Irreversibilität von Gatter
 $0 \vee 1 \rightarrow 1$

Quantenmechanisch

- QBit $|0\rangle$: $|\uparrow\rangle$
QBit $|1\rangle$: $|\downarrow\rangle$
Relative Phase zwischen $|1\rangle$ und $|0\rangle$
- Superpositionsprinzip:
 $|\Psi\rangle = |\rightarrow\rangle = a|0\rangle + b|1\rangle$
Mit $|a|^2 + |b|^2 = 1$
- Reversibilität von Gatter *NOT* $|0\rangle = |1\rangle$

Unterschiede zwischen klassischem Computer und Quantencomputer

Klassisch

- Bit 0: 0 bis 1 V
Bit 1: 3 bis 5 V
- Es tritt nur 1 Zustand auf:
Entweder Bit 0 oder Bit 1
- Irreversibilität von Gatter
 $0 \vee 1 \rightarrow 1$
- Je 1 Operationschritt für
jeden Zustand

Quantenmechanisch

- QBit $|0\rangle$: $|\uparrow\rangle$
QBit $|1\rangle$: $|\downarrow\rangle$
Relative Phase zwischen $|1\rangle$ und $|0\rangle$
- Superpositionsprinzip:
 $|\Psi\rangle = |\rightarrow\rangle = a|0\rangle + b|1\rangle$
Mit $|a|^2 + |b|^2 = 1$
- Reversibilität von Gatter *NOT* $|0\rangle = |1\rangle$
- 1 Operationschritt für alle Zustände

Unterschiede zwischen klassischem Computer und Quantencomputer

Klassisch

- Bit 0: 0 bis 1 V
Bit 1: 3 bis 5 V
- Es tritt nur 1 Zustand auf:
Entweder Bit 0 oder Bit 1
- Irreversibilität von Gatter
 $0 \vee 1 \rightarrow 1$
- Je 1 Operationschritt für
jeden Zustand

Quantenmechanisch

- QBit $|0\rangle$: $|\uparrow\rangle$
QBit $|1\rangle$: $|\downarrow\rangle$
Relative Phase zwischen $|1\rangle$ und $|0\rangle$
- Superpositionsprinzip:
 $|\Psi\rangle = |\rightarrow\rangle = a|0\rangle + b|1\rangle$
Mit $|a|^2 + |b|^2 = 1$
- Reversibilität von Gatter *NOT* $|0\rangle = |1\rangle$
- 1 Operationschritt für alle Zustände
- Messung zerstört Superposition

Unterschiede zwischen klassischem Computer und Quantencomputer

Quantenmechanisch Elemente die der klassische PC nicht besitzt

Unterschiede zwischen klassischem Computer und Quantencomputer

Quantenmechanisch Elemente die der klassische PC nicht besitzt

- QBits besitzen relative Phasen

Unterschiede zwischen klassischem Computer und Quantencomputer

Quantenmechanisch Elemente die der klassische PC nicht besitzt

- QBits besitzen relative Phasen
 - Sie kontrollierung Orientierung des Spins

Unterschiede zwischen klassischem Computer und Quantencomputer

Quantenmechanisch Elemente die der klassische PC nicht besitzt

- QBits besitzen relative Phasen
 - Sie kontrollierung Orientierung des Spins
 - Sie werden durch den Phasenfaktor beschrieben:
 $e^{i\phi x} |x\rangle$

Unterschiede zwischen klassischem Computer und Quantencomputer

Quantenmechanisch Elemente die der klassische PC nicht besitzt

- QBits besitzen relative Phasen
 - Sie kontrollierung Orientierung des Spins
 - Sie werden durch den Phasenfaktor beschrieben:
 $e^{i\phi x} |x\rangle$
- Verschränkte Zustände: $|\Psi\rangle = a|00\rangle + b|11\rangle$:

Unterschiede zwischen klassischem Computer und Quantencomputer

Quantenmechanisch Elemente die der klassische PC nicht besitzt

- QBits besitzen relative Phasen
 - Sie kontrollierung Orientierung des Spins
 - Sie werden durch den Phasenfaktor beschrieben:
 $e^{i\phi x} |x\rangle$
- Verschränkte Zustände: $|\Psi\rangle = a|00\rangle + b|11\rangle$:
 - Entsteht durch Wechselwirkung zwischen 2 Teilchen

Unterschiede zwischen klassischem Computer und Quantencomputer

Quantenmechanisch Elemente die der klassische PC nicht besitzt

- QBits besitzen relative Phasen
 - Sie kontrollierung Orientierung des Spins
 - Sie werden durch den Phasenfaktor beschrieben:
 $e^{i\phi x} |x\rangle$
- Verschränkte Zustände: $|\Psi\rangle = a|00\rangle + b|11\rangle$:
 - Entsteht durch Wechselwirkung zwischen 2 Teilchen
 - kein Produktzustand von 2 Teilchen

Unterschiede zwischen klassischem Computer und Quantencomputer

Quantenmechanisch Elemente die der klassische PC nicht besitzt

- QBits besitzen relative Phasen
 - Sie kontrollierung Orientierung des Spins
 - Sie werden durch den Phasenfaktor beschrieben:
 $e^{i\phi x} |x\rangle$
- Verschränkte Zustände: $|\Psi\rangle = a|00\rangle + b|11\rangle$:
 - Entsteht durch Wechselwirkung zwischen 2 Teilchen
 - kein Produktzustand von 2 Teilchen
 - können gemeinsame Informationen haben

Unterschiede zwischen klassischem Computer und Quantencomputer

Quantenmechanisch Elemente die der klassische PC nicht besitzt

- QBits besitzen relative Phasen
 - Sie kontrollierung Orientierung des Spins
 - Sie werden durch den Phasenfaktor beschrieben:
 $e^{i\phi x} |x\rangle$
- Verschränkte Zustände: $|\Psi\rangle = a|00\rangle + b|11\rangle$:
 - Entsteht durch Wechselwirkung zwischen 2 Teilchen
 - kein Produktzustand von 2 Teilchen
 - können gemeinsame Informationen haben
 - Getrennte Messungen können Zustand nicht aufschlüsseln

Unterschiede zwischen klassischem Computer und Quantencomputer

Quantenmechanisch Elemente die der klassische PC nicht besitzt

- QBits besitzen relative Phasen
 - Sie kontrollierung Orientierung des Spins
 - Sie werden durch den Phasenfaktor beschrieben:
 $e^{i\phi_x} |x\rangle$
- Verschränkte Zustände: $|\Psi\rangle = a|00\rangle + b|11\rangle$:
 - Entsteht durch Wechselwirkung zwischen 2 Teilchen
 - kein Produktzustand von 2 Teilchen
 - können gemeinsame Informationen haben
 - Getrennte Messungen können Zustand nicht aufschlüsseln
- Interferenzen

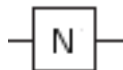
Quantengatter mit einem Eingang

Gatter die nur auf 1 QBit angewendet werden:

Quantengatter mit einem Eingang

Gatter die nur auf 1 QBit angewendet werden:

- Not Gatter
entspricht einem Bitwechsel:
Not $|0\rangle \rightarrow |1\rangle$
Not $|1\rangle \rightarrow |0\rangle$



Quantengatter mit einem Eingang

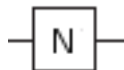
Gatter die nur auf 1 QBit angewendet werden:

- Not Gatter

entspricht einem Bitwechsel:

$$\text{Not}|0\rangle \rightarrow |1\rangle$$

$$\text{Not}|1\rangle \rightarrow |0\rangle$$

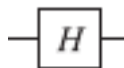


- Hadamard Gatter

bewirkt eine Drehung des Spins um 90° :

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |\rightarrow\rangle$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |\leftarrow\rangle$$



Quantengatter mit einem Eingang

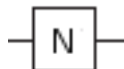
Gatter die nur auf 1 QBit angewendet werden:

- Not Gatter

entspricht einem Bitwechsel:

$$\text{Not}|0\rangle \rightarrow |1\rangle$$

$$\text{Not}|1\rangle \rightarrow |0\rangle$$

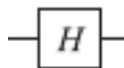


- Hadamard Gatter

bewirkt eine Drehung des Spins um 90° :

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |\rightarrow\rangle$$

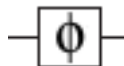
$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |\leftarrow\rangle$$



- Phase-Shift Gatter

verschiebt die Relative Phase:

$$U_\Phi|x\rangle = e^{i\Phi x}|x\rangle$$



Quantengatter mit mehreren Eingängen

Gatter die auf mehrere QBits angewendet werden

Quantengatter mit mehreren Eingängen

Gatter die auf mehrere QBits angewendet werden

- C-Not Gatter

Das Ziel-Qbit wechselt nur dann, wenn das kontrollierende QBit $|1\rangle$ ist

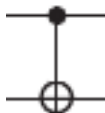


Quantengatter mit mehreren Eingängen

Gatter die auf mehrere QBits angewendet werden

- C-Not Gatter

Das Ziel-Qbit wechselt nur dann, wenn das kontrollierende QBit $|1\rangle$ ist



- Toffoli Gatter

funktioniert wie das C-Not Gatter mit 2 kontrollierende QBits und beide müssen $|1\rangle$ sein, damit das Ziel-QBit wechselt.



Fehler im Quantencomputer

2 Arten von Fehlerquellen:

Fehler im Quantencomputer

2 Arten von Fehlerquellen:

- Gatter
Unitären Fehler

Fehler im Quantencomputer

2 Arten von Fehlerquellen:

- Gatter
Unitären Fehler
- Umgebung/Dekohärenz
Nicht unitärer Fehler

Fehler im Quantencomputer

2 Arten von Fehlerquellen:

- Gatter
Unitären Fehler
- Umgebung/Dekohärenz
Nicht unitärer Fehler

Daraus können 3 Arten von Fehlern entstehen:

2 Arten von Fehlerquellen:

- Gatter
Unitären Fehler
- Umgebung/Dekohärenz
Nicht unitärer Fehler

Daraus können 3 Arten von Fehlern entstehen:

- Bitfehler

entspricht $\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \triangleq |1\rangle\langle 0| + |0\rangle\langle 1| = X$

Fehler im Quantencomputer

2 Arten von Fehlerquellen:

- Gatter
Unitären Fehler
- Umgebung/Dekohärenz
Nicht unitärer Fehler

Daraus können 3 Arten von Fehlern entstehen:

- Bitfehler

entspricht $\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \triangleq |1\rangle\langle 0| + |0\rangle\langle 1| = X$

- Phasenfehler

entspricht $\sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \triangleq |0\rangle\langle 0| - |1\rangle\langle 1| = Z$

Fehler im Quantencomputer

2 Arten von Fehlerquellen:

- Gatter
Unitären Fehler
- Umgebung/Dekohärenz
Nicht unitärer Fehler

Daraus können 3 Arten von Fehlern entstehen:

- Bitfehler

entspricht $\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \triangleq |1\rangle\langle 0| + |0\rangle\langle 1| = X$

- Phasenfehler

entspricht $\sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \triangleq |0\rangle\langle 0| - |1\rangle\langle 1| = Z$

- Phasen- und Bitfehler

entspricht $i * \sigma_Y = \sigma_Z * \sigma_X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \triangleq |0\rangle\langle 1| - |1\rangle\langle 0| = Y$

Fehler im Quantencomputer

2 Arten von Fehlerquellen:

- Gatter
Unitären Fehler
- Umgebung/Dekohärenz
Nicht unitärer Fehler

Daraus können 3 Arten von Fehlern entstehen:

- Bitfehler

entspricht $\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \triangleq |1\rangle\langle 0| + |0\rangle\langle 1| = X$

- Phasenfehler

entspricht $\sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \triangleq |0\rangle\langle 0| - |1\rangle\langle 1| = Z$

- Phasen- und Bitfehler

entspricht $i * \sigma_Y = \sigma_Z * \sigma_X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \triangleq |0\rangle\langle 1| - |1\rangle\langle 0| = Y$

Diese Fehlerarten sind auch kontinuierlich

→ Messung wandelt kontinuierliche Fehler in diskrete um.

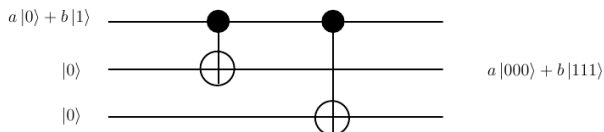
- Klassisch: Redundanz der Bits:
Kopien von Bits

- Klassisch: Redundanz der Bits:
Kopien von Bits
- Problem in der Quantenmechanik: No-Cloning-Theorem
Perfekte Kopie eines QBit verletzt die Heisenberg'sche Unschärferelation

- Lösung: Verschränkung von Zuständen

- Lösung: Verschränkung von Zuständen
- $|\Psi\rangle = a|0\rangle + b|1\rangle$
- $C_{NOT(12)}C_{NOT(13)}|\Psi\rangle|0\rangle|0\rangle$
- $= C_{NOT(12)}C_{NOT(13)}(a|0\rangle|0\rangle|0\rangle + b|1\rangle|0\rangle|0\rangle)$
- $= a|000\rangle + b|111\rangle$

- Lösung: Verschränkung von Zuständen
- $|\Psi\rangle = a|0\rangle + b|1\rangle$
- $C_{NOT(12)}C_{NOT(13)}|\Psi\rangle|0\rangle|0\rangle$
- $= C_{NOT(12)}C_{NOT(13)}(a|0\rangle|0\rangle|0\rangle + b|1\rangle|0\rangle|0\rangle)$
- $= a|000\rangle + b|111\rangle$



Bitfehler-Schaltplan

- Keine Messung der kodierten QBits

$$|t_1, t_2, t_3 \rangle$$

- Keine Messung der kodierten QBits

$$\begin{array}{l} |t_1, t_2, t_3\rangle \\ (t_1 \stackrel{?}{=} t_2, t_1 \stackrel{?}{=} t_3) \end{array}$$

Bitfehler-Schaltplan

- Keine Messung der kodierten QBits

$$\begin{array}{c} |t_1, t_2, t_3 \rangle \\ (t_1 \stackrel{?}{=} t_2, t_1 \stackrel{?}{=} t_3) \end{array}$$

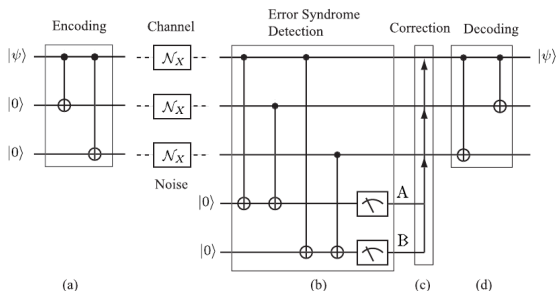
- Verwendung zweier Hilfs-QBits im Grundzustand
- Messung der Hilfs-QBits

Bitfehler-Schaltplan

- Keine Messung der kodierten QBits

$$|t_1, t_2, t_3\rangle$$
$$(t_1 \stackrel{?}{=} t_2, t_1 \stackrel{?}{=} t_3)$$

- Verwendung zweier Hilfs-QBits im Grundzustand
- Messung der Hilfs-QBits



- $|0\rangle \rightarrow \cos(\alpha)|0\rangle - i \sin(\alpha)|1\rangle$
- $|1\rangle \rightarrow \cos(\alpha)|1\rangle - i \sin(\alpha)|0\rangle$

- $|0\rangle \rightarrow \cos(\alpha)|0\rangle - i \sin(\alpha)|1\rangle$
 - $|1\rangle \rightarrow \cos(\alpha)|1\rangle - i \sin(\alpha)|0\rangle$
- $\Rightarrow |\Psi\rangle = a|000\rangle + b|111\rangle$
- $\rightarrow \cos(\alpha)(a|000\rangle + b|111\rangle) -$
 $i \sin(\alpha)(a|100\rangle + b|011\rangle)$

- $|0\rangle \rightarrow \cos(\alpha)|0\rangle - i \sin(\alpha)|1\rangle$
 - $|1\rangle \rightarrow \cos(\alpha)|1\rangle - i \sin(\alpha)|0\rangle$
- $\Rightarrow |\Psi\rangle = a|000\rangle + b|111\rangle$
- $\rightarrow \cos(\alpha)(a|000\rangle + b|111\rangle) -$
 $i \sin(\alpha)(a|100\rangle + b|011\rangle)$
- Messung von $|\Psi\rangle$ liefert:

- $|0\rangle \rightarrow \cos(\alpha)|0\rangle - i \sin(\alpha)|1\rangle$
 - $|1\rangle \rightarrow \cos(\alpha)|1\rangle - i \sin(\alpha)|0\rangle$
- $\Rightarrow |\Psi\rangle = a|000\rangle + b|111\rangle$
- $\rightarrow \cos(\alpha)(a|000\rangle + b|111\rangle) -$
 $i \sin(\alpha)(a|100\rangle + b|011\rangle)$
- Messung von $|\Psi\rangle$ liefert:
 - $(0,0)$ mit $P = \cos^2(\alpha)$
 Ψ zerfällt in $a|000\rangle + b|111\rangle$

- $|0\rangle \rightarrow \cos(\alpha)|0\rangle - i \sin(\alpha)|1\rangle$
 - $|1\rangle \rightarrow \cos(\alpha)|1\rangle - i \sin(\alpha)|0\rangle$
- $\Rightarrow |\Psi\rangle = a|000\rangle + b|111\rangle$
- $\rightarrow \cos(\alpha)(a|000\rangle + b|111\rangle) - i \sin(\alpha)(a|100\rangle + b|011\rangle)$
- Messung von $|\Psi\rangle$ liefert:
 - (0,0) mit $P = \cos^2(\alpha)$
 Ψ zerfällt in $a|000\rangle + b|111\rangle$
 - (1,1) mit $P = \sin^2(\alpha)$
 Ψ zerfällt in $a|100\rangle + b|011\rangle$

Phasenfehler-Schaltplan

Phasenfehler-Schaltplan

- Änderung einer Phase ($U_\phi|x\rangle = e^{i\phi x}|x\rangle$) wirkt sich auch auf die anderen QBits aus:

$$a|000\rangle + b|111\rangle \rightarrow a|000\rangle - b|111\rangle$$

Phasenfehler-Schaltplan

- Änderung einer Phase ($U_\Phi|x\rangle = e^{i\Phi x}|x\rangle$) wirkt sich auch auf die anderen QBits aus:

$$a|000\rangle + b|111\rangle \rightarrow a|000\rangle - b|111\rangle$$

- Hadamard Gatter:

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

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

Phasenfehler-Schaltplan

- Änderung einer Phase ($U_\phi|x\rangle = e^{i\phi x}|x\rangle$) wirkt sich auch auf die anderen QBits aus:

$$a|000\rangle + b|111\rangle \rightarrow a|000\rangle - b|111\rangle$$

- Hadamard Gatter:

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

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

- Redundanz der Phase:

$$\Rightarrow a(|0\rangle + |1\rangle \otimes |\bar{0}\rangle \otimes |\bar{0}\rangle) + b(|0\rangle - |1\rangle \otimes |\bar{1}\rangle \otimes |\bar{1}\rangle)$$

Phasenfehler-Schaltplan

- Änderung einer Phase ($U_\phi|x\rangle = e^{i\phi x}|x\rangle$) wirkt sich auch auf die anderen QBits aus:

$$a|000\rangle + b|111\rangle \rightarrow a|000\rangle - b|111\rangle$$

- Hadamard Gatter:

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

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

- Redundanz der Phase:

$$\Rightarrow a(|0\rangle + |1\rangle \otimes |\bar{0}\rangle \otimes |\bar{0}\rangle) + b(|0\rangle - |1\rangle \otimes |\bar{1}\rangle \otimes |\bar{1}\rangle)$$

- Umwandlung des Phasenfehlers zu einem Bitfehler

Phasenfehler-Schaltplan

- Änderung einer Phase ($U_\Phi|x\rangle = e^{i\Phi}x|x\rangle$) wirkt sich auch auf die anderen QBits aus:

$$a|000\rangle + b|111\rangle \rightarrow a|000\rangle - b|111\rangle$$

- Hadamard Gatter:

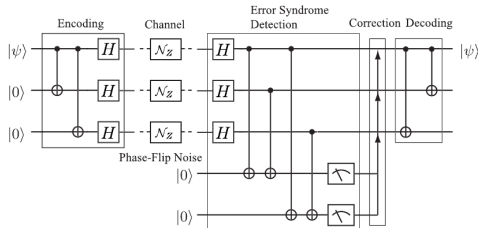
$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

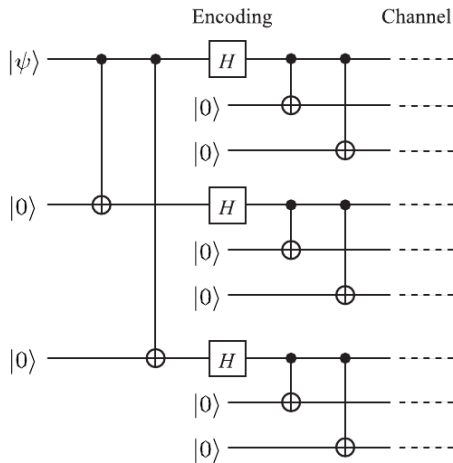
$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- Redundanz der Phase:

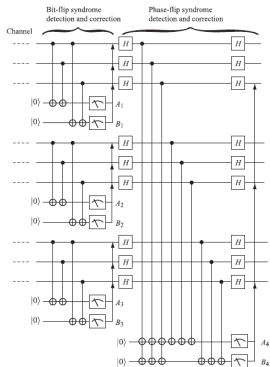
$$\Rightarrow a(|0\rangle + |1\rangle \otimes |\bar{0}\rangle \otimes |\bar{0}\rangle) + b(|0\rangle - |1\rangle \otimes |\bar{1}\rangle \otimes |\bar{1}\rangle)$$

- Umwandlung des Phasenfehlers zu einem Bitfehler

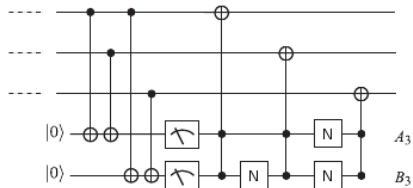
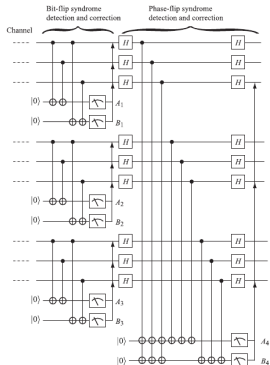




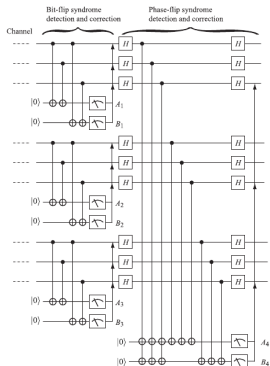
9QECC-Bitmessung



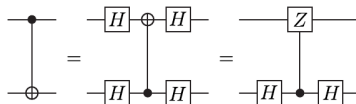
9QECC-Bitmessung



9QECC-Performancesteigerung

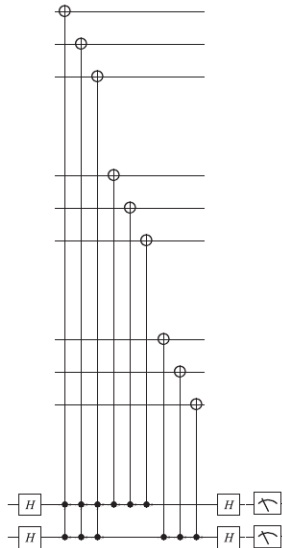
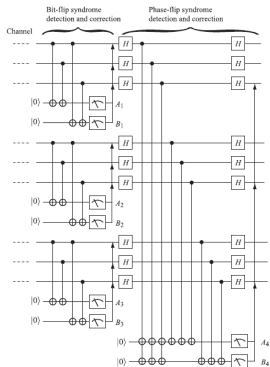


- Vertauschung des kontrollierenden- und des Ziel-QBits

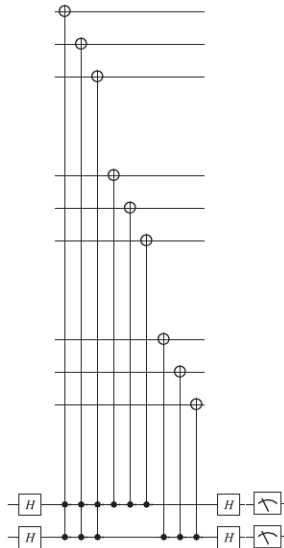
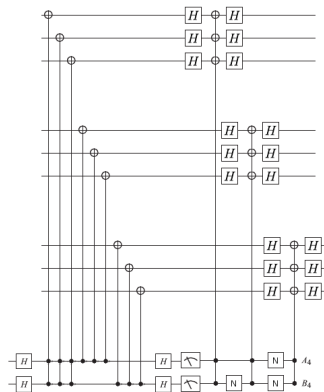


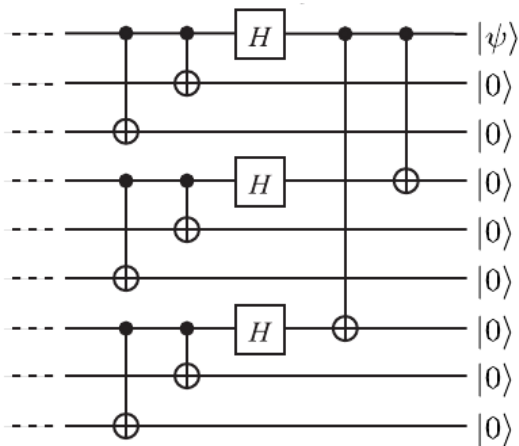
- $U_H X U_H = Z$

9QECC-Phasenmessung



9QECC-Phasenmessung





7QECC-Klassischer Hintergrund

- k bits an Information, Code c der Länge n und Paritätskontrollmatrix H
- $k=4, n=7$

7QECC-Klassischer Hintergrund

- k bits an Information, Code c der Länge n und Paritätskontrollmatrix H
- $k=4, n=7$
- $Hc^t = 0$

- k bits an Information, Code c der Länge n und Paritätskontrollmatrix H
- $k=4, n=7$
- $Hc^t = 0$
- Syndrom Hc^t

- k bits an Information, Code c der Länge n und Paritätskontrollmatrix H
- $k=4, n=7$
- $Hc^t = 0$
- Syndrom Hc^t
- Fehleridentifizierung durch 3 Bits:
001,010,...,111

- k bits an Information, Code c der Länge n und Paritätskontrollmatrix H
- $k=4, n=7$
- $Hc^t = 0$
- Syndrom Hc^t
- Fehleridentifizierung durch 3 Bits:
001,010,...,111

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

- $C = \text{Kern}(H)$

- $C = \text{Kern}(H)$
- $\dim C = n - 3 = k$

- $C = \text{Kern}(H)$
- $\dim C = n - 3 = k$
- Ordnung der Menge C : $2^k = 16$

- $C = \text{Kern}(H)$
- $\dim C = n - 3 = k$
- Ordnung der Menge C : $2^k = 16$

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

- M ...erzeugende Matrix
- Hamming Code wird durch M erzeugt

7QECC-Klassischer Hintergrund

- Erzeugen von Codevektoren c aus C mit Hilfe eines Vektors v mit der Länge k
- Vektoren in C werden als $v \cdot M$ angeschrieben

7QECC-Klassischer Hintergrund

- Erzeugen von Codevektoren c aus C mit Hilfe eines Vektors v mit der Länge k
- Vektoren in C werden als $v \cdot M$ angeschrieben

| v | $v \cdot M$ | v | $v \cdot M$ |
|--------|-------------|--------|-------------|
| (0000) | (0000000) | (1000) | (0001111) |
| (0001) | (1111111) | (1001) | (1110000) |
| (0010) | (1010101) | (1010) | (1011010) |
| (0011) | (0101010) | (1011) | (0100101) |
| (0100) | (0110011) | (1100) | (0111100) |
| (0101) | (1001100) | (1101) | (1000011) |
| (0110) | (1100110) | (1110) | (1101001) |
| (0111) | (0011001) | (1111) | (0010110) |

7QECC-Klassischer Hintergrund

- Erzeugen von Codevektoren c aus C mit Hilfe eines Vektors v mit der Länge k
- Vektoren in C werden als $v \cdot M$ angeschrieben

| v | $v \cdot M$ | v | $v \cdot M$ |
|--------|-------------|--------|-------------|
| (0000) | (0000000) | (1000) | (0001111) |
| (0001) | (1111111) | (1001) | (1110000) |
| (0010) | (1010101) | (1010) | (1011010) |
| (0011) | (0101010) | (1011) | (0100101) |
| (0100) | (0110011) | (1100) | (0111100) |
| (0101) | (1001100) | (1101) | (1000011) |
| (0110) | (1100110) | (1110) | (1101001) |
| (0111) | (0011001) | (1111) | (0010110) |

- Zuordnung gerader Anzahlen von 1en zu logisch 0
- Zuordnung ungerader Anzahlen von 1en zu logisch 1

- logisch 0:

- logisch 0:
 - erzeugt durch gerade Binärzahlen von v

- logisch 0:
 - erzeugt durch gerade Binärzahlen von v
 - werden als C^\perp bezeichnet, da sie (mod 2)-orthogonal zu allen Codes in C sind

- logisch 0:
 - erzeugt durch gerade Binärzahlen von v
 - werden als C^\perp bezeichnet, da sie (mod 2)-orthogonal zu allen Codes in C sind
 - H besteht aus Zeilenvektoren mit geraden Anzahlen von 1en, diese sind gleich mit einigen $c \in C^\perp$

- logisch 0:
 - erzeugt durch gerade Binärzahlen von v
 - werden als C^\perp bezeichnet, da sie (mod 2)-orthogonal zu allen Codes in C sind
 - H besteht aus Zeilenvektoren mit geraden Anzahlen von 1en, diese sind gleich mit einigen $c \in C^\perp$
 - M besteht aus Zeilenvektoren von Codes aus C

$$H = \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix}, M = \begin{pmatrix} h_1 \\ h_2 \\ h_3 \\ \text{II} \end{pmatrix}$$

- logisch 0:
 - erzeugt durch gerade Binärzahlen von v
 - werden als C^\perp bezeichnet, da sie (mod 2)-orthogonal zu allen Codes in C sind
 - H besteht aus Zeilenvektoren mit geraden Anzahlen von 1en, diese sind gleich mit einigen $c \in C^\perp$
 - M besteht aus Zeilenvektoren von Codes aus C

$$H = \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix}, M = \begin{pmatrix} h_1 \\ h_2 \\ h_3 \\ \text{II} \end{pmatrix}$$

$$\rightarrow HM^t = 0$$

- logisch 0:
 - erzeugt durch gerade Binärzahlen von v
 - werden als C^\perp bezeichnet, da sie (mod 2)-orthogonal zu allen Codes in C sind
 - H besteht aus Zeilenvektoren mit geraden Anzahlen von 1en, diese sind gleich mit einigen $c \in C^\perp$
 - M besteht aus Zeilenvektoren von Codes aus C

$$H = \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix}, M = \begin{pmatrix} h_1 \\ h_2 \\ h_3 \\ \text{II} \end{pmatrix}$$

$$\rightarrow HM^t = 0$$

$$\rightarrow HM^t v^t = Hc^t = 0$$

- logisch 0:
 - erzeugt durch gerade Binärzahlen von v
 - werden als C^\perp bezeichnet, da sie (mod 2)-orthogonal zu allen Codes in C sind
 - H besteht aus Zeilenvektoren mit geraden Anzahlen von 1en, diese sind gleich mit einigen $c \in C^\perp$
 - M besteht aus Zeilenvektoren von Codes aus C

$$H = \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix}, M = \begin{pmatrix} h_1 \\ h_2 \\ h_3 \\ \text{II} \end{pmatrix}$$

$$\rightarrow HM^t = 0$$

$$\rightarrow HM^t v^t = Hc^t = 0$$

- logisch 1:

- logisch 0:
 - erzeugt durch gerade Binärzahlen von v
 - werden als C^\perp bezeichnet, da sie (mod 2)-orthogonal zu allen Codes in C sind
 - H besteht aus Zeilenvektoren mit geraden Anzahlen von 1en, diese sind gleich mit einigen $c \in C^\perp$
 - M besteht aus Zeilenvektoren von Codes aus C

$$H = \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix}, M = \begin{pmatrix} h_1 \\ h_2 \\ h_3 \\ \text{II} \end{pmatrix}$$

$$\rightarrow HM^t = 0$$

$$\rightarrow HM^t v^t = Hc^t = 0$$

- logisch 1:
 - $C-C^\perp$

7QECC-Klassischer Hintergrund

- c_1 und c_2 sind Codes in C

7QECC-Klassischer Hintergrund

- c_1 und c_2 sind Codes in C
- $d_H(c_1, c_2)$...Hammingabstand zwischen c_1 und c_2

- c_1 und c_2 sind Codes in C
- $d_H(c_1, c_2)$...Hammingabstand zwischen c_1 und c_2
- $d_H(c_1, c_2)$ misst wieviele Bits sich unterscheiden

- c_1 und c_2 sind Codes in C
 - $d_H(c_1, c_2)$...Hammingabstand zwischen c_1 und c_2
 - $d_H(c_1, c_2)$ misst wieviele Bits sich unterscheiden
- 1 $d_H(c, c) \geq 0$ für beliebige $c \in C$.
 - 2 $d_H(c_1, c_2) = d_H(c_2, c_1)$ für beliebige $c_1, c_2 \in C$.
 - 3 $d_H(c_1, c_3) \leq d_H(c_1, c_2) + d_H(c_2, c_3)$ für beliebige $c_1, c_2, c_3 \in C$.
 - 4 $d_H(C) = \min_{c, c' \in C} d_H(c, c')$

- c_1 und c_2 sind Codes in C
- $d_H(c_1, c_2)$...Hammingabstand zwischen c_1 und c_2
- $d_H(c_1, c_2)$ misst wieviele Bits sich unterscheiden
- ① $d_H(c, c) \geq 0$ für beliebige $c \in C$.
- ② $d_H(c_1, c_2) = d_H(c_2, c_1)$ für beliebige $c_1, c_2 \in C$.
- ③ $d_H(c_1, c_3) \leq d_H(c_1, c_2) + d_H(c_2, c_3)$ für beliebige $c_1, c_2, c_3 \in C$.
- ④ $d_H(C) = \min_{c, c' \in C} d_H(c, c')$
- Der Minimalabstand zwischen 2 Codes vom 7QECC beträgt 3

- c_1 und c_2 sind Codes in C
- $d_H(c_1, c_2)$...Hammingabstand zwischen c_1 und c_2
- $d_H(c_1, c_2)$ misst wieviele Bits sich unterscheiden

- ① $d_H(c, c) \geq 0$ für beliebige $c \in C$.
- ② $d_H(c_1, c_2) = d_H(c_2, c_1)$ für beliebige $c_1, c_2 \in C$.
- ③ $d_H(c_1, c_3) \leq d_H(c_1, c_2) + d_H(c_2, c_3)$ für beliebige $c_1, c_2, c_3 \in C$.
- ④ $d_H(C) = \min_{c, c' \in C} d_H(c, c')$

- Der Minimalabstand zwischen 2 Codes vom 7QECC beträgt 3
- Maximale Fehleranzahl: $\lfloor \frac{d_H(C)-1}{2} \rfloor$
wobei $\lfloor x \rfloor$ die Abrundungsfunktion bezeichnet.

- c_1 und c_2 sind Codes in C
- $d_H(c_1, c_2)$...Hammingabstand zwischen c_1 und c_2
- $d_H(c_1, c_2)$ misst wieviele Bits sich unterscheiden
- ① $d_H(c, c) \geq 0$ für beliebige $c \in C$.
- ② $d_H(c_1, c_2) = d_H(c_2, c_1)$ für beliebige $c_1, c_2 \in C$.
- ③ $d_H(c_1, c_3) \leq d_H(c_1, c_2) + d_H(c_2, c_3)$ für beliebige $c_1, c_2, c_3 \in C$.
- ④ $d_H(C) = \min_{c, c' \in C} d_H(c, c')$
- Der Minimalabstand zwischen 2 Codes vom 7QECC beträgt 3
- Maximale Fehleranzahl: $\lfloor \frac{d_H(C)-1}{2} \rfloor$
wobei $\lfloor x \rfloor$ die Abrundungsfunktion bezeichnet.
- 1 Bit Fehlererkennung muss der Minimalabstand zumindest 3 Bits betragen

Operatoren die nötig sind, um den 7 QECC zu erzeugen:

Operatoren die nötig sind, um den 7 QECC zu erzeugen:
Operatoren für die Bits:

$$M_0 = X_4 X_3 X_2 X_1, M_1 = X_5 X_3 X_2 X_0, M_2 = X_6 X_3 X_1 X_0$$

Operatoren die nötig sind, um den 7 QECC zu erzeugen:

Operatoren für die Bits:

$$M_0 = X_4 X_3 X_2 X_1, M_1 = X_5 X_3 X_2 X_0, M_2 = X_6 X_3 X_1 X_0$$

Operatoren für die Phasen:

$$N_0 = Z_4 Z_3 Z_2 Z_1, N_1 = Z_5 Z_3 Z_2 Z_0, N_2 = Z_6 Z_3 Z_1 Z_0$$

Operatoren die nötig sind, um den 7 QECC zu erzeugen:
Operatoren für die Bits:

$$M_0 = X_4 X_3 X_2 X_1, M_1 = X_5 X_3 X_2 X_0, M_2 = X_6 X_3 X_1 X_0$$

Operatoren für die Phasen:

$$N_0 = Z_4 Z_3 Z_2 Z_1, N_1 = Z_5 Z_3 Z_2 Z_0, N_2 = Z_6 Z_3 Z_1 Z_0$$

Es gelten folgende Regeln:

$$M_i^2 = N_i^2 = I$$

$$M_i(I + M_i) = I + M_i, [M_i, M_j] = [N_i, N_j] = 0$$

und

$$[M_i, N_j] = [M_i, \bar{X}] = [\bar{X}, N_j] = 0$$

Kodierung der Superposition von 7-QBits:

$$|0\rangle_L = \frac{1}{\sqrt{8}}(I + M_0)(I + M_1)(I + M_2)|0\rangle^{\otimes 7}$$

und

$$|1\rangle_L = \frac{1}{\sqrt{8}}(I + M_0)(I + M_1)(I + M_2)|1\rangle^{\otimes 7}$$

Kodierung der Superposition von 7-QBits:

$$|0\rangle_L = \frac{1}{\sqrt{8}}(I + M_0)(I + M_1)(I + M_2)|0\rangle^{\otimes 7}$$

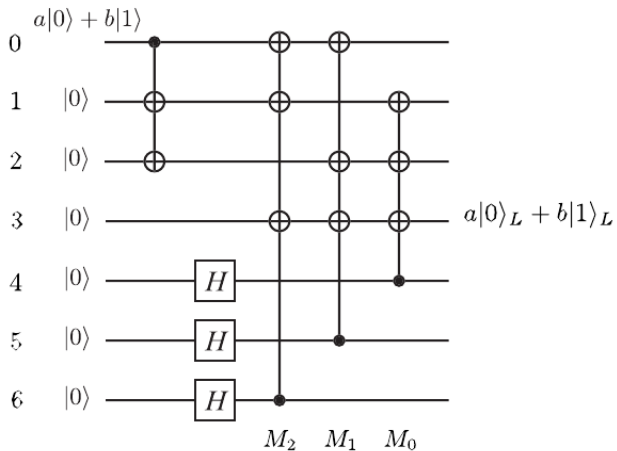
und

$$|1\rangle_L = \frac{1}{\sqrt{8}}(I + M_0)(I + M_1)(I + M_2)|1\rangle^{\otimes 7}$$

- $|0\rangle_L$ und $|1\rangle_L$ sind Eigenvektoren von M_i und N_i mit dem Eigenwert $+1$

$$M_i|x\rangle_L = N_i|x\rangle_L = |x\rangle_L$$

7QECC-Kodierung



7QECC-Fehlersyndrom

- Fehler Z_0 auf $|0\rangle_L$

7QECC-Fehlersyndrom

- Fehler Z_0 auf $|0\rangle_L$
- $M_1 Z_0 |0\rangle_L = -Z_0 M_1 |0\rangle_L = -Z_0 |0\rangle_L$
- $M_2 Z_0 |0\rangle_L = -Z_0 |0\rangle_L, M_0 Z_0 |0\rangle_L = Z_0 |0\rangle_L$

7QECC-Fehlersyndrom

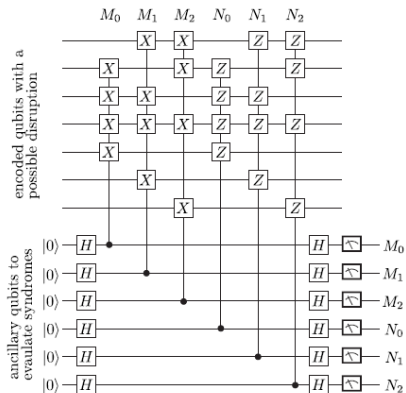
- Fehler Z_0 auf $|0\rangle_L$
- $M_1 Z_0 |0\rangle_L = -Z_0 M_1 |0\rangle_L = -Z_0 |0\rangle_L$
- $M_2 Z_0 |0\rangle_L = -Z_0 |0\rangle_L, M_0 Z_0 |0\rangle_L = Z_0 |0\rangle_L$
- Eigenwerte charakterisiert durch $(M_0, M_1, M_2; N_0, N_1, N_2)$

7QECC-Fehlersyndrom

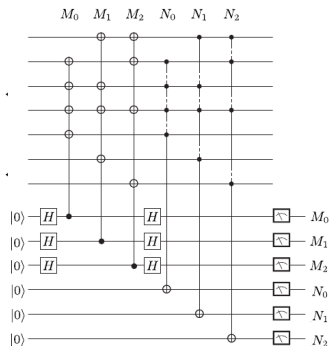
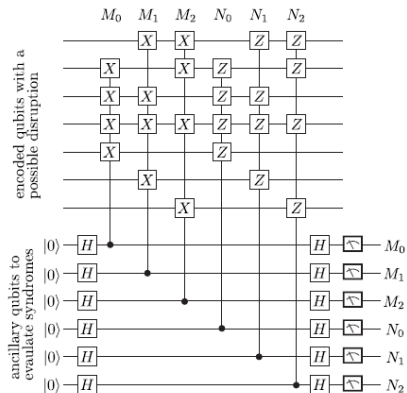
- Fehler Z_0 auf $|0\rangle_L$
- $M_1 Z_0 |0\rangle_L = -Z_0 M_1 |0\rangle_L = -Z_0 |0\rangle_L$
- $M_2 Z_0 |0\rangle_L = -Z_0 |0\rangle_L, M_0 Z_0 |0\rangle_L = Z_0 |0\rangle_L$
- Eigenwerte charakterisiert durch $(M_0, M_1, M_2; N_0, N_1, N_2)$

| | Y_0 | Y_1 | Y_2 | Y_3 | Y_4 | Y_5 | Y_6 |
|-------|-------|-------|-------|-------|-------|-------|-------|
| M_0 | | * | * | * | * | | |
| M_1 | * | | * | * | | * | |
| M_2 | * | * | | * | | | * |
| N_0 | | * | * | * | * | | |
| N_1 | * | | * | * | | * | |
| N_2 | * | * | | * | | | * |

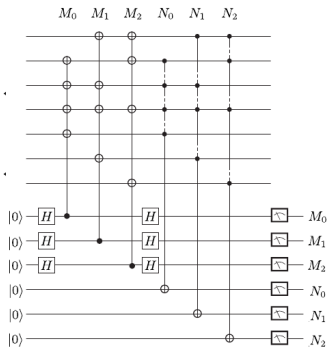
7QECC-Schaltplan



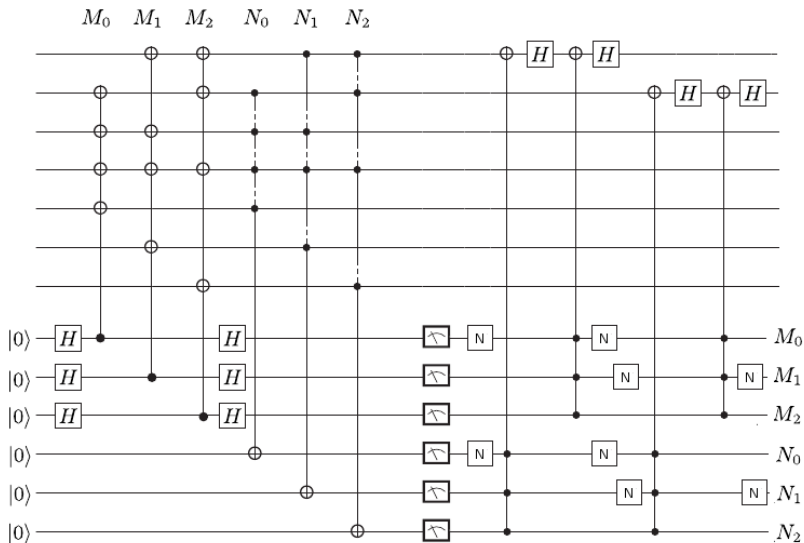
7QECC-Schaltplan

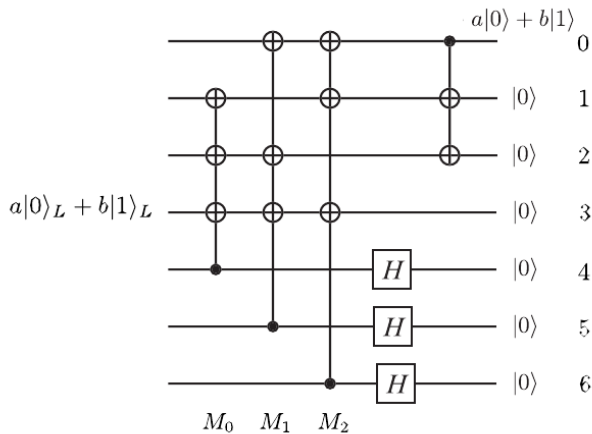


| | Y_0 | Y_1 | Y_2 | Y_3 | Y_4 | Y_5 | Y_6 |
|-------|-------|-------|-------|-------|-------|-------|-------|
| M_0 | | * | * | * | * | | |
| M_1 | * | | * | * | | * | |
| M_2 | * | * | | * | | | * |
| N_0 | | * | * | * | * | | |
| N_1 | * | | * | * | | * | |
| N_2 | * | * | | * | | | * |



7QECC-Korrektur





VIELEN DANK

FÜR IHRE AUFMERKSAMKEIT