Quantenfehlerkorrekturcodes

Christian Hartler

2. Dezember 2009

Übersicht

- 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

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

Unterschiede zwischen klassischem Computer und Quantencomputer

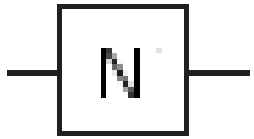
Quantenmechanisch Elemente die der klassische PC nicht besitzt

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

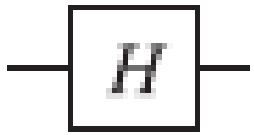
Quantengatter mit einem Eingang

Gatter die nur auf 1 QBit angewendet werden:

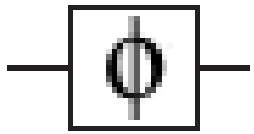
- Not Gatter
  entspricht einem Bitwechsel:
  $\text{Not}|0> \rightarrow |1>$
  $\text{Not}|1> \rightarrow |0>$



- Hadamard Gatter
  bewirkt eine Drehung des Spins um 90°:
  $H|0> = \frac{1}{\sqrt{2}}(|0> + |1>) = |\rightarrow>$
  $H|1> = \frac{1}{\sqrt{2}}(|0> - |1>) = |\leftarrow>$



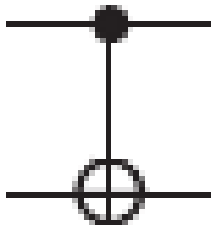
- Phase-Shift Gatter
  verschiebt die Relative Phase:
  $U_\Phi|x> = e^{i\Phi x}|x>$



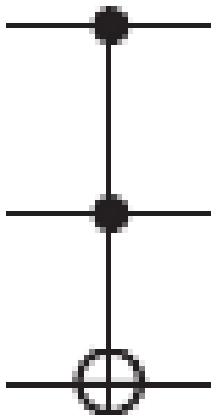
Quantengatter mit mehreren Eingängen

Gatter die auf mehrere QBits angewendet werden

- C-Not Gatter
  Das Ziel-Qbit wechselt nur dann, wenn das kontrollierende QBit $|1>$ ist



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



Fehler im Quantencomputer

2 Arten von Fehlerquellen:

- Gatter
  Unitären Fehler
- Umgebung/Dekohärenz
  Nicht unitärer Fehler

Daraus können 3 Arten von Fehlern entstehen:

- Bitfehler
  entspricht $\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \triangleq |1><0| + |0><1| = X$
- Phasenfehler
  entspricht $\sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \triangleq |0><0| - |1><1| = Z$
- Phasen- und Bitfehler
  entspricht $i * \sigma_Y = \sigma_Z * \sigma_X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \triangleq |0><1| - |1><0| = Y$

Diese Fehlerarten sind auch kontinuierlich
$\rightarrow$Messung wandelt kontinuierliche Fehler in diskrete um.

Bitfehler-Redundanz

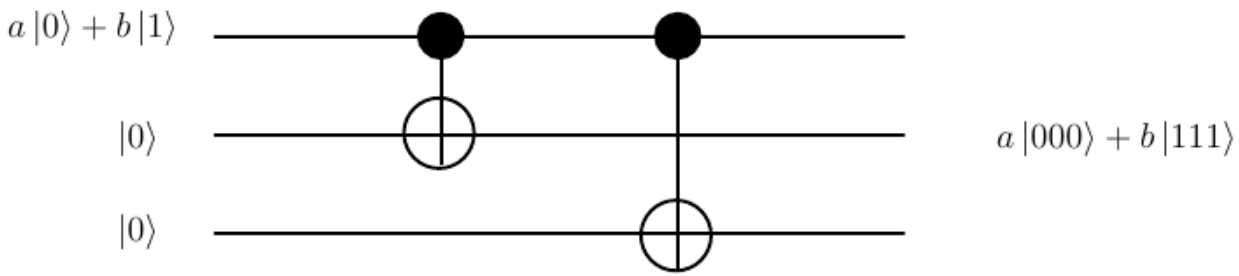
- Klassisch: Redundanz der Bits:
  Kopien von Bits
- Problem in der Quantenmechanik: No-Cloning-Theorem
  Perfekte Kopie eines QBit verletzt die Heisenberg'sche Unschärferelation

Bitfehler-Redundanz

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

$= C_{NOT(12)} C_{NOT(13)} (a|0> |0> |0> + b|1> |0> |0>)$

$= a|000> + b|111>$

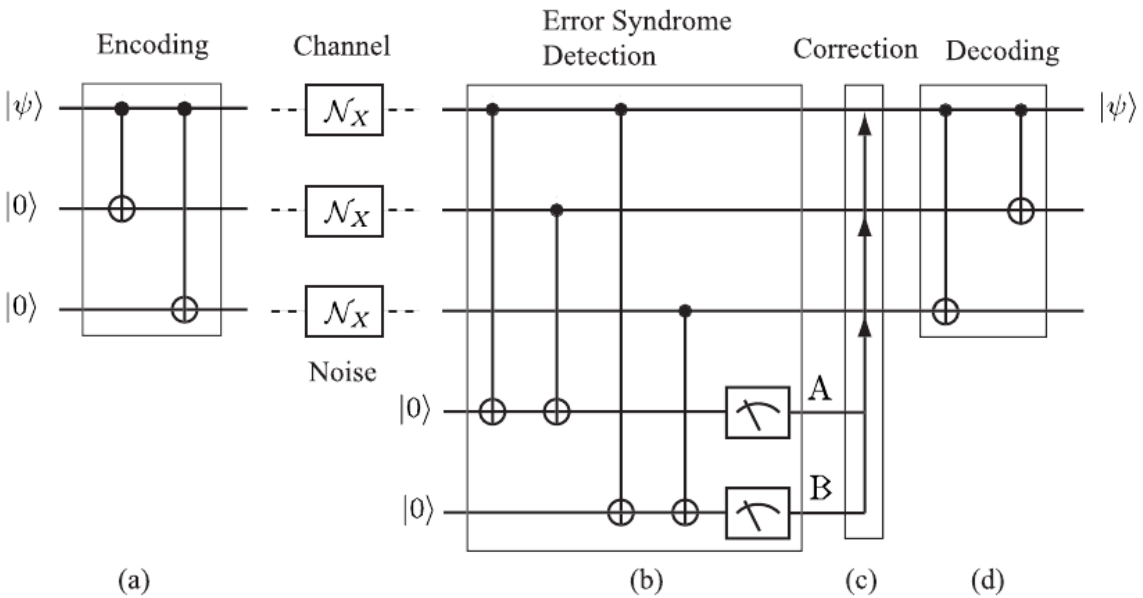


Bitfehler-Schaltplan

- Keine Messung der kodierten QBits

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

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



Bitfehler-Messung

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

$\Rightarrow$ $|\Psi> = a|000> + b|111>$

$\rightarrow$ $cos(\alpha)(a|000> + b|111>) -$
$i * sin(\alpha)(a|100> + b|011>)$

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

Phasenfehler-Schaltplan

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

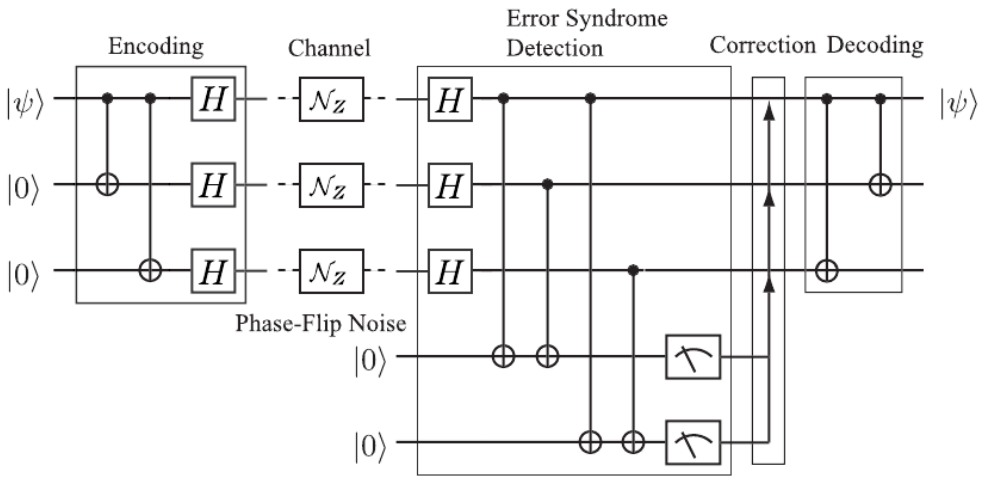
$$a|000>+b|111>\rightarrow a|000>-b|111>$$

- Hadamard Gatter:
  $H|0>=\frac{1}{\sqrt{2}}(|0>+|1>)$
  $H|1>=\frac{1}{\sqrt{2}}(|0>-|1>)$

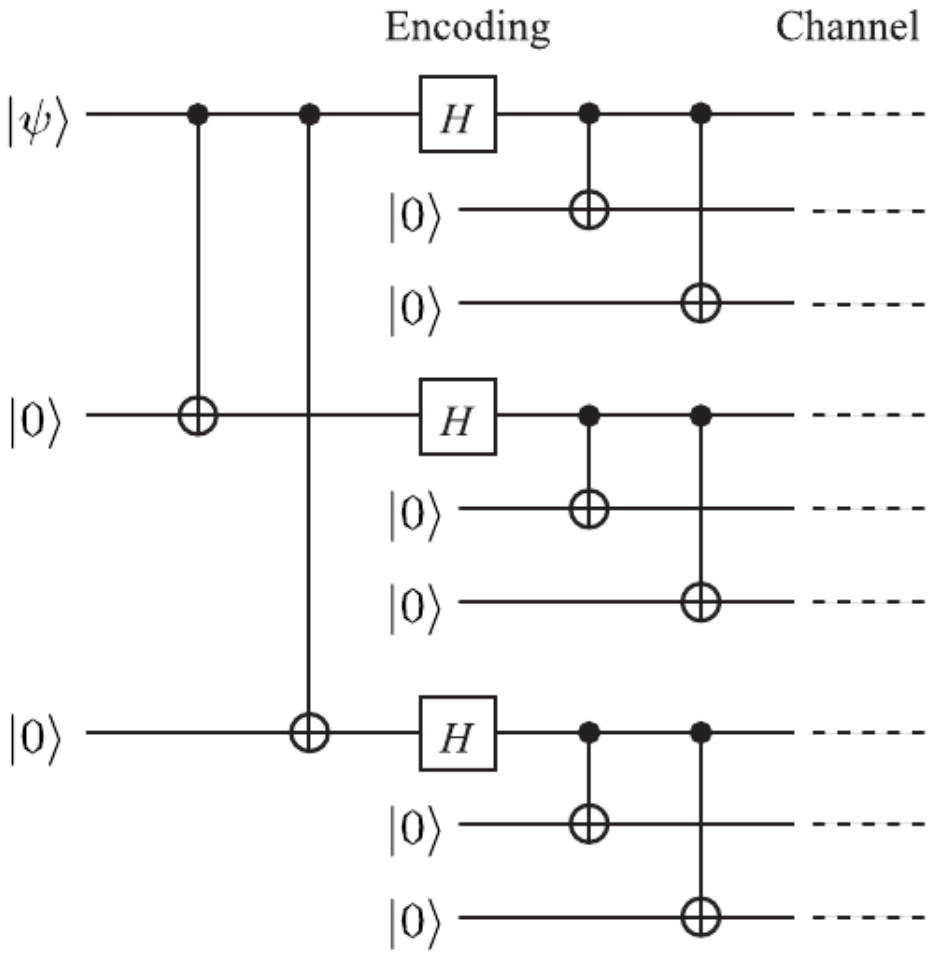
- Redundanz der Phase:

$\Rightarrow$ $a(|0>+|1>\otimes|\overline{0}>\otimes|\overline{0}>)+b(|0>-|1>\otimes|\overline{1}>\otimes|\overline{1}>)$

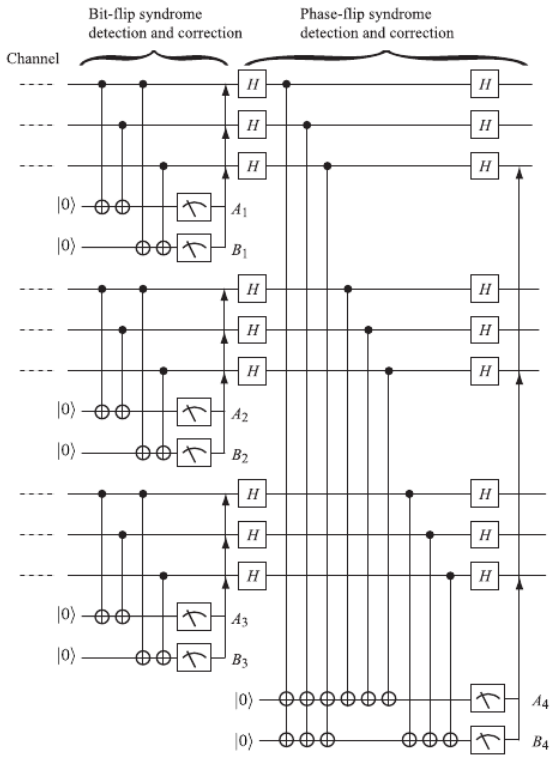
- Umwandlung des Phasenfehlers zu einem Bitfehler

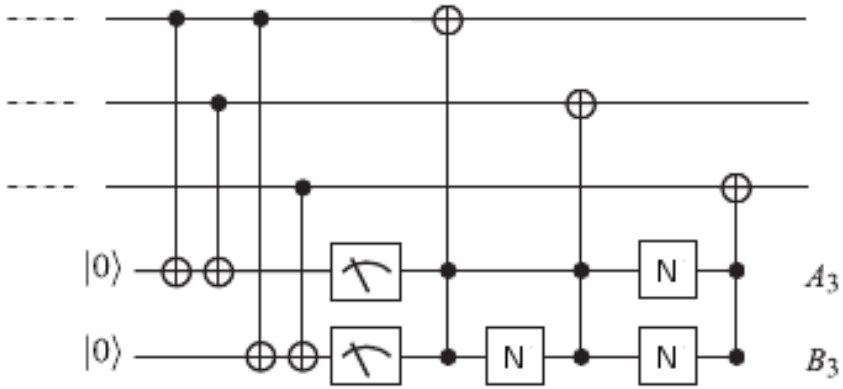


9QECC-Kodierung

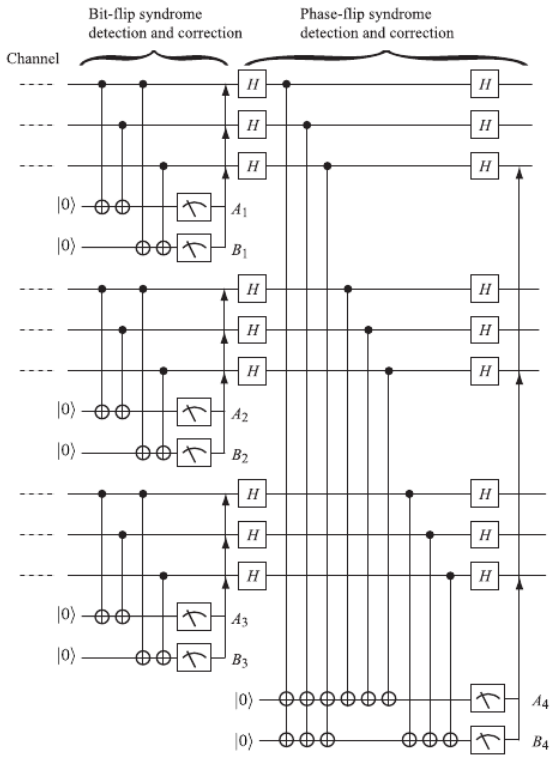


9QECC-Bitmessung

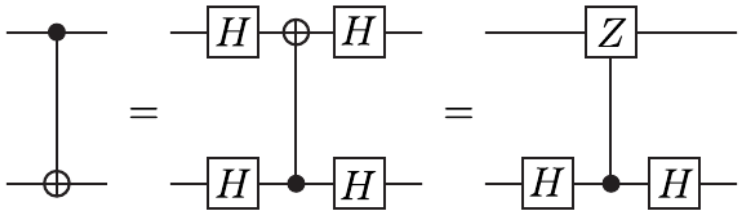




9QECC-Performancesteigerung

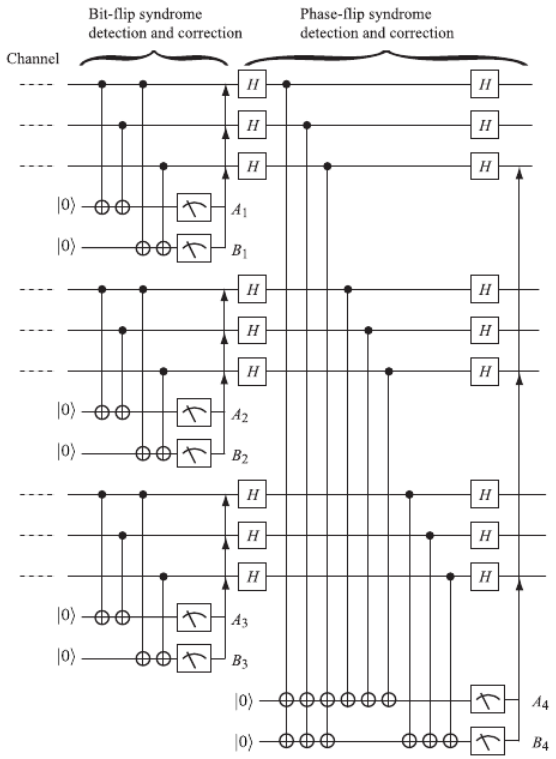


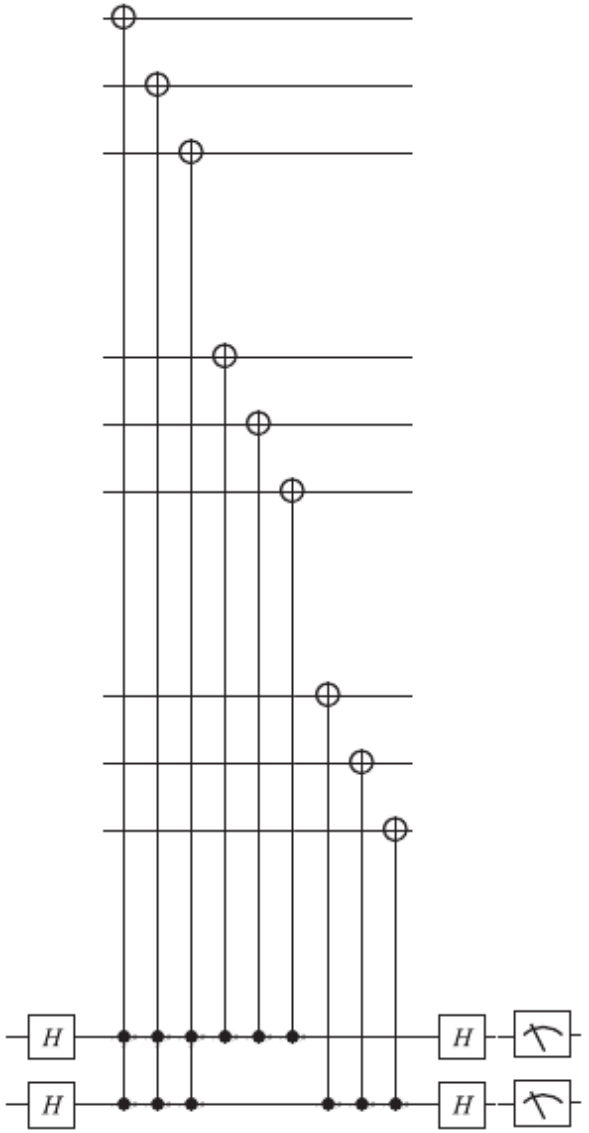
- Vertauschung des kontrollierenden- und des Ziel-QBits



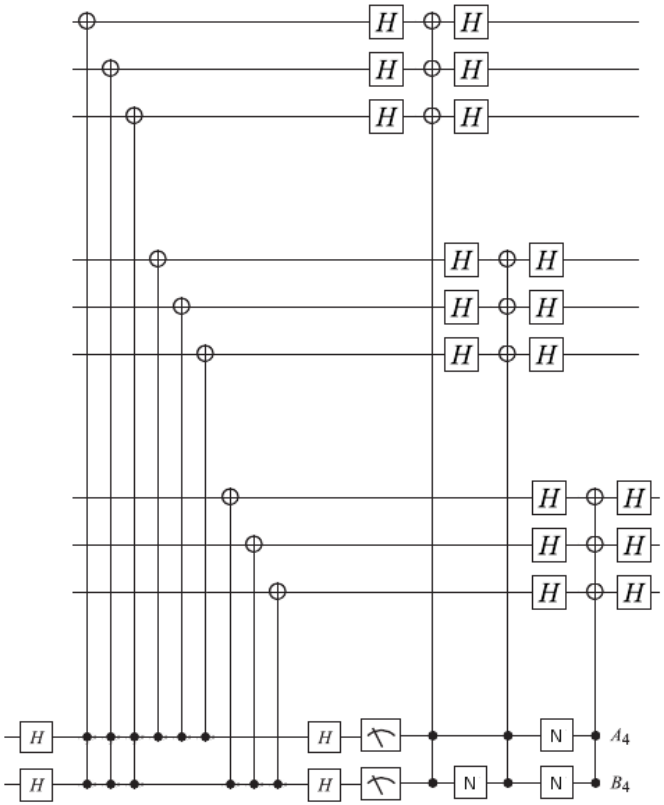
- $U_H X U_H = Z$

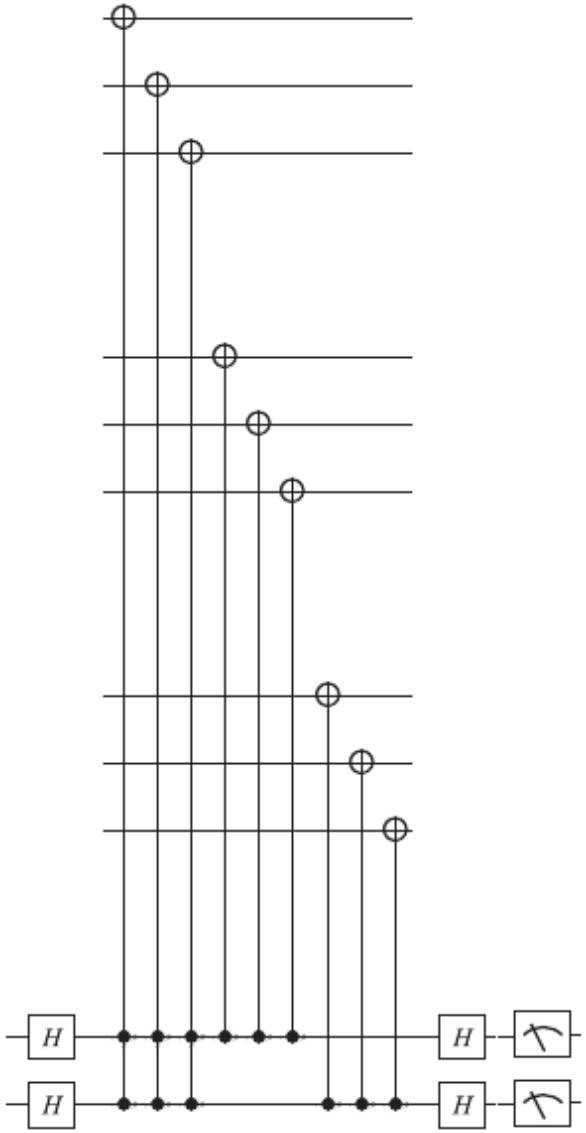
9QECC-Phasenmessung



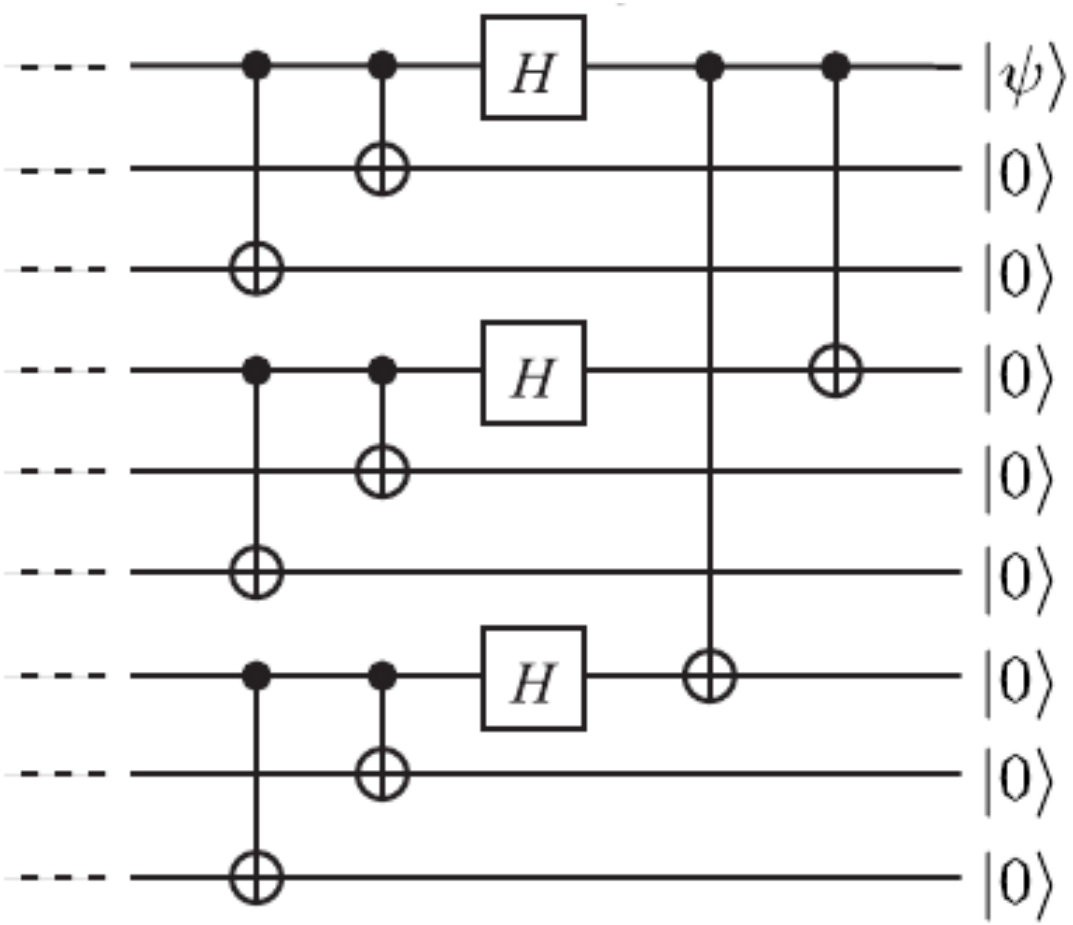


9QECC-Phasenmessung





9QECC-Dekodierung



7QECC-Klassischer Hintergrund

- 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

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

7QECC-Klassischer Hintergrund

- C=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*M angeschrieben

v	v*M	v	v*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

7QECC-Klassischer Hintergrund

- 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
- $d_H(c_1, c_2)$...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

7QECC-Kodierung

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

$$M_0 = X_4X_3X_2X_1, M_1 = X_5X_3X_2X_0, M_2 = X_6X_3X_1X_0$$

Operatoren für die Phasen:

$$N_0 = Z_4Z_3Z_2Z_1, N_1 = Z_5Z_3Z_2Z_0, N_2 = Z_6Z_3Z_1Z_0$$

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

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

7QECC-Kodierung

Kodierung der Superposition von 7-QBits:

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

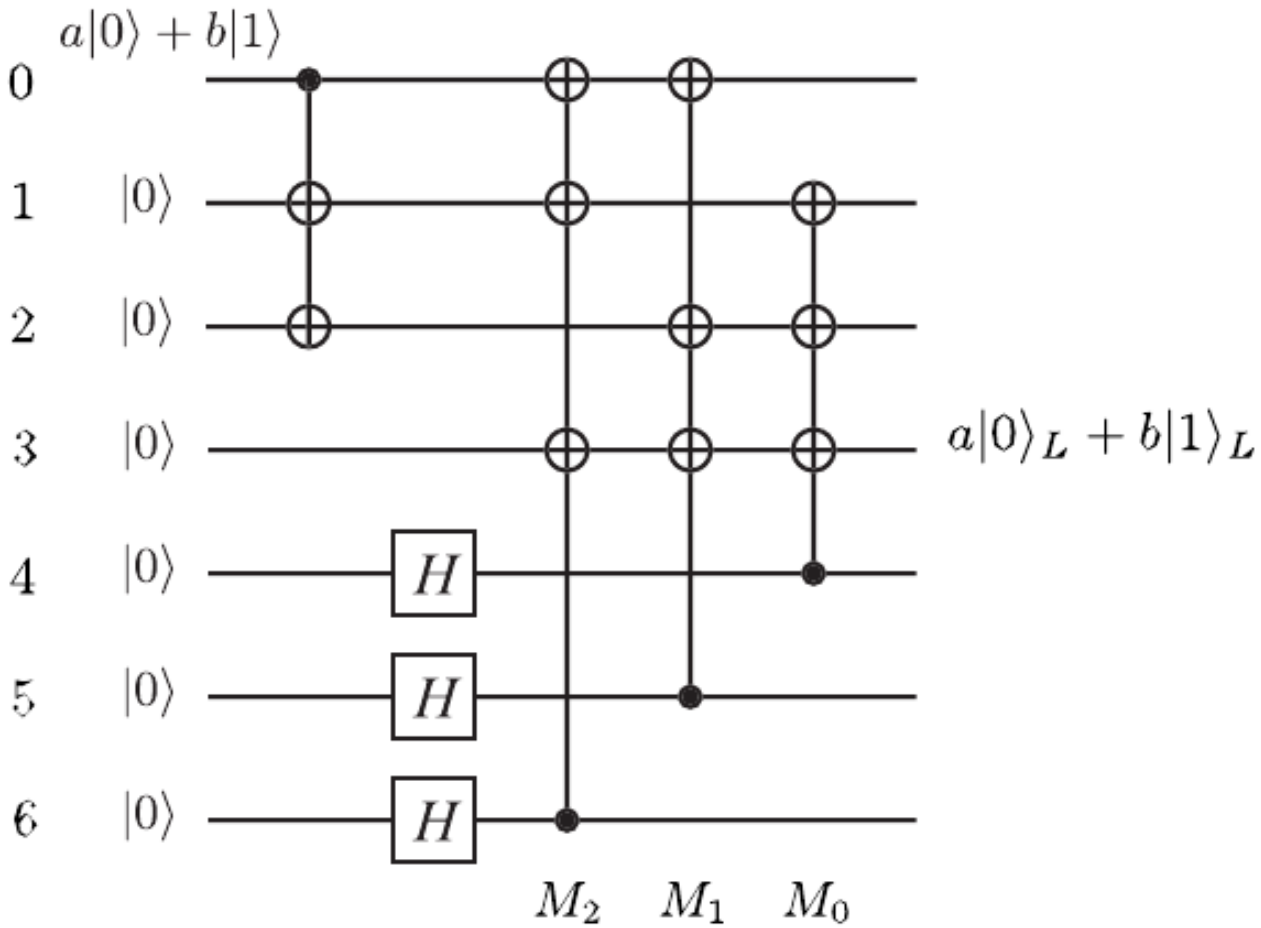
und

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

- $|0>_L$ und $|1>_L$ sind Eigenvektoren von M_i und N_i mit dem Eigenwert $+1$

$$M_i|x>_L = N_i|x>_L = |x>_L$$

7QECC-Kodierung

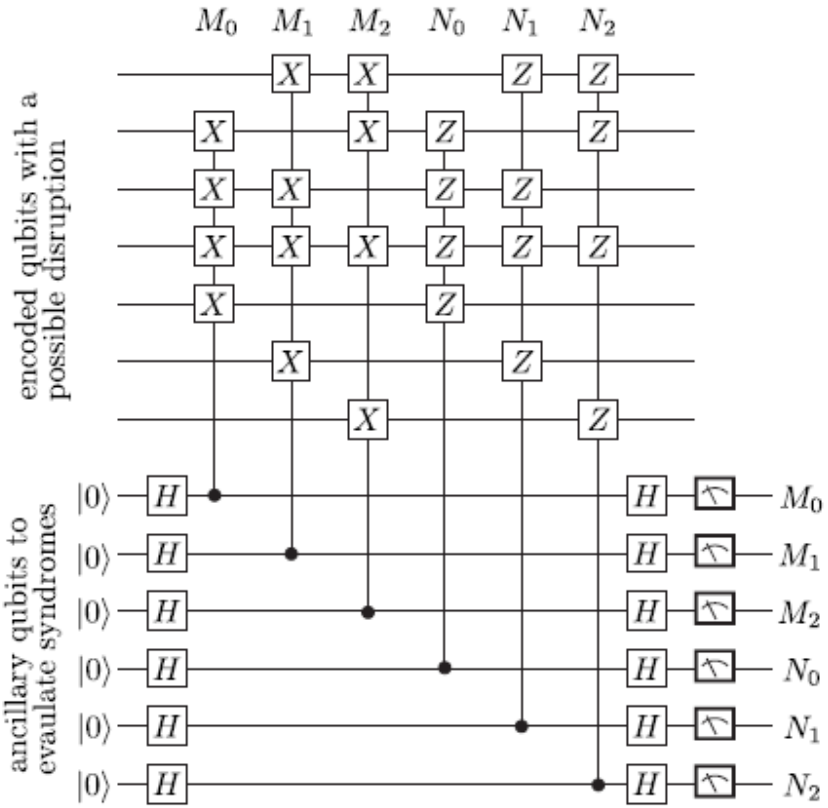


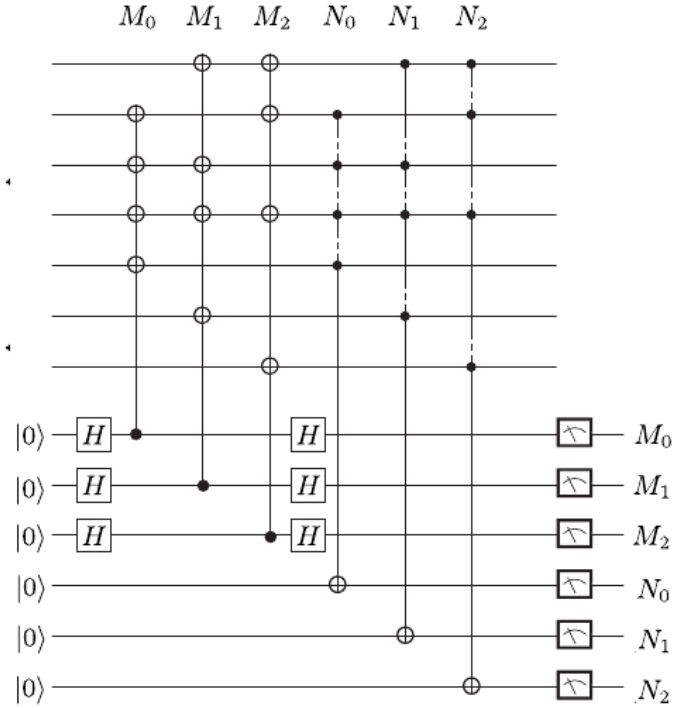
7QECC-Fehlersyndrom

- Fehler Z_0 auf $|0>_L$
- $M_1 Z_0 |0>_L = -Z_0 M_1 |0>_L = -Z_0 |0>_L$
- $M_2 Z_0 |0>_L = -Z_0 |0>_L$, $M_0 Z_0 |0>_L = Z_0 |0>_L$
- 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	*	*		*			*

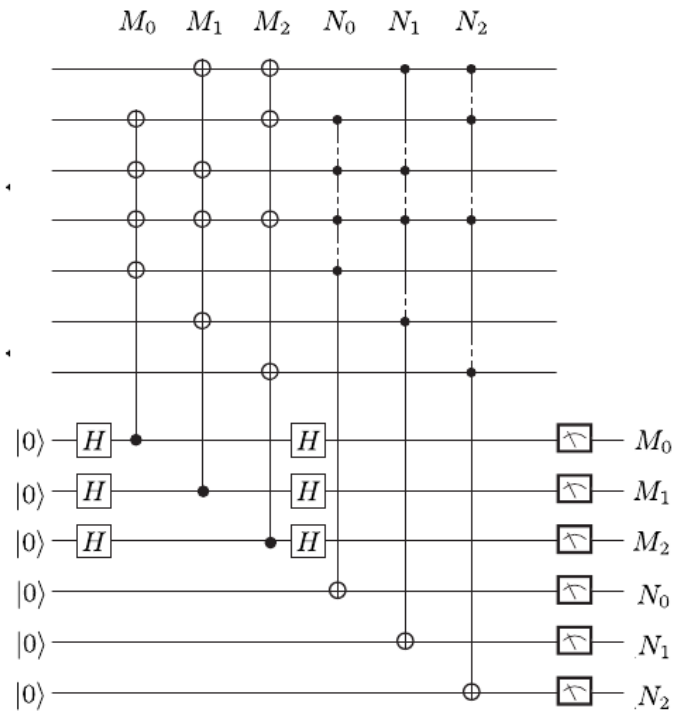
7QECC-Schaltplan



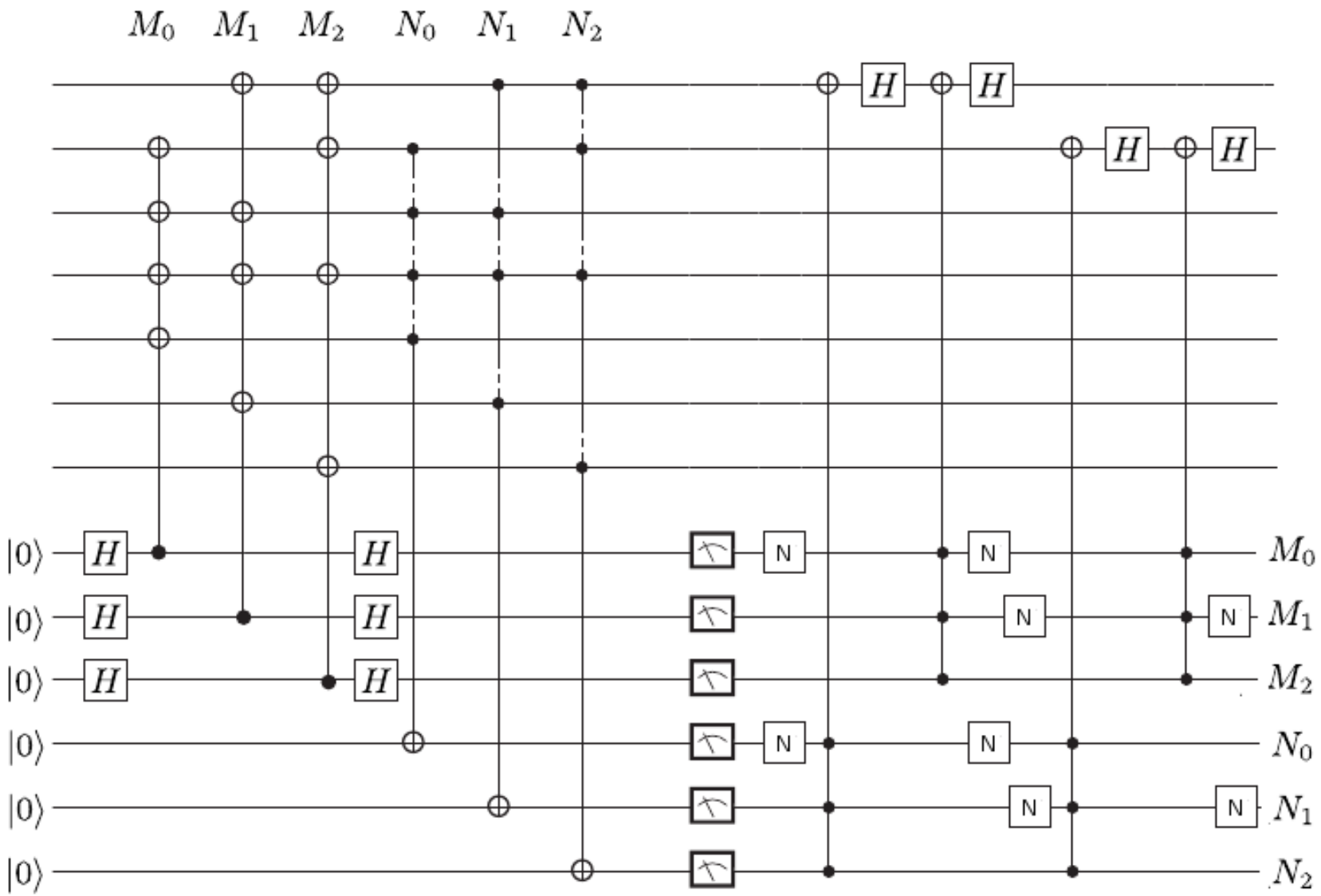


7QECC-Messung

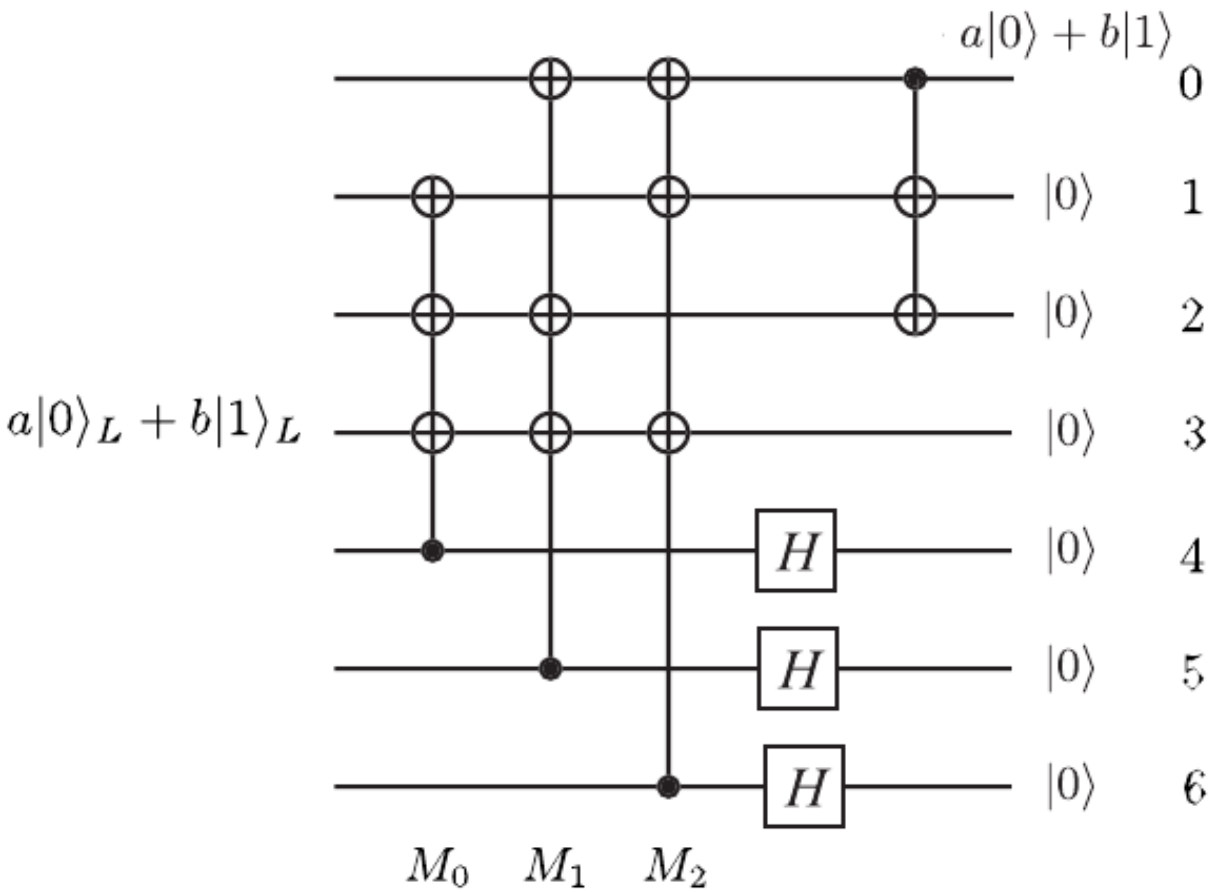
	Y_0	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6
M_0		$*$	$*$	$*$	$*$		
M_1	$*$		$*$	$*$		$*$	
M_2	$*$	$*$		$*$			$*$
N_0		$*$	$*$	$*$	$*$		
N_1	$*$		$*$	$*$		$*$	
N_2	$*$	$*$		$*$			$*$



7QECC-Korrektur



7QECC


$a|0\rangle + b|1\rangle$
$a|0\rangle_L + b|1\rangle_L$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
H
H
H
0
1
2
3
4
5
6
M_0
M_1
M_2

VIELEN DANK

FÜR IHRE AUFMERKSAMKEIT