Fachtagung

Informations– und Mikrosystemtechnik

Magdeburg, 25.–27. März 1998

Codierung und Decodierung zyklischer Quantencodes

Grundlagen der Quanten–Codierungstheorie

Markus Grassl

Thomas Beth

Institut für Algorithmen und Kognitive Systeme

Universität Karlsruhe

Übersicht

- Grundbegriffe
- Kanalmodell
- Vergleich zu klassischen Codes:
  Warum es nicht mit „klassischen“ Codes geht.
- Fehlermodell
- Quantencodes:
  Wie es doch mit „klassischen“ Codes geht.
- Bemerkungen

Grundbegriffe

klassisch	quantenmechanisch
Bit: Wert 0 *oder* 1	Qubit: $\lvert\psi\rangle = \alpha\,\lvert 0\rangle + \beta\,\lvert 1\rangle$ mit $\alpha, \beta \in \mathbb{C}$, d. h. *gleichzeitig* $\lvert 0\rangle$ und $\lvert 1\rangle$
Register mit n Bit: *ein* Wert von 2^n Werten	Quantenregister mit n Qubit: *gleichzeitig* alle 2^n Werte möglich
Auslesen: deterministisch, beliebig oft	Messung: probabilistisch, ein *klassischer* Wert 0 oder 1, Messung von 0 mit Wahrscheinlichkeit $\lvert\alpha^2\rvert$

Quantengatter

NOT–Gatter

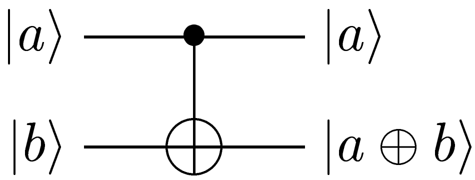
$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \begin{array}{ccc} |0\rangle & \mapsto & |1\rangle \\ |1\rangle & \mapsto & |0\rangle \end{array}$$

Hadamard–Transformation

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \begin{array}{ccc} |0\rangle & \mapsto & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle & \mapsto & \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{array}$$

$CNOT$–Gatter

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \begin{array}{ccc} |00\rangle & \mapsto & |00\rangle \\ |01\rangle & \mapsto & |01\rangle \\ |10\rangle & \mapsto & |11\rangle \\ |11\rangle & \mapsto & |10\rangle \end{array}$$



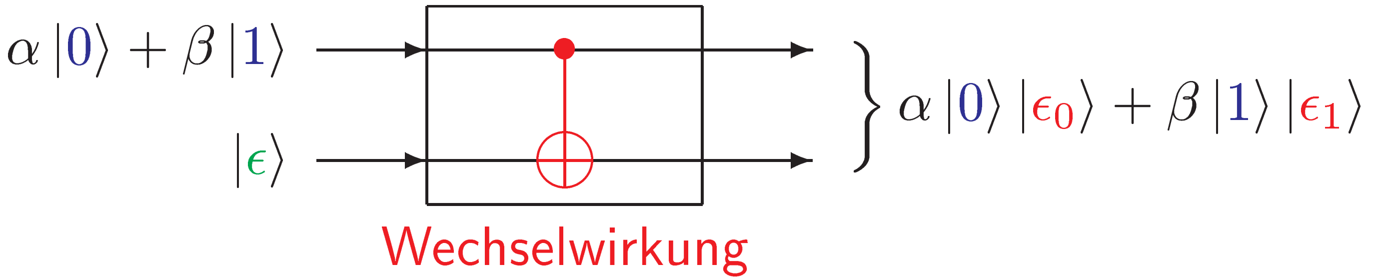
Quantenkanal (I)

fehlerfreie Übertragung:

$\alpha\,|0\rangle + \beta\,|1\rangle \longrightarrow$ System $\longrightarrow \alpha\,|0\rangle + \beta\,|1\rangle$

$|\epsilon\rangle \longrightarrow$ Umgebung $\longrightarrow |\epsilon\rangle$

gestörte Übertragung:



Quantenkanal (II): Beispiel

Interferenz bei ungestörter Übertragung:

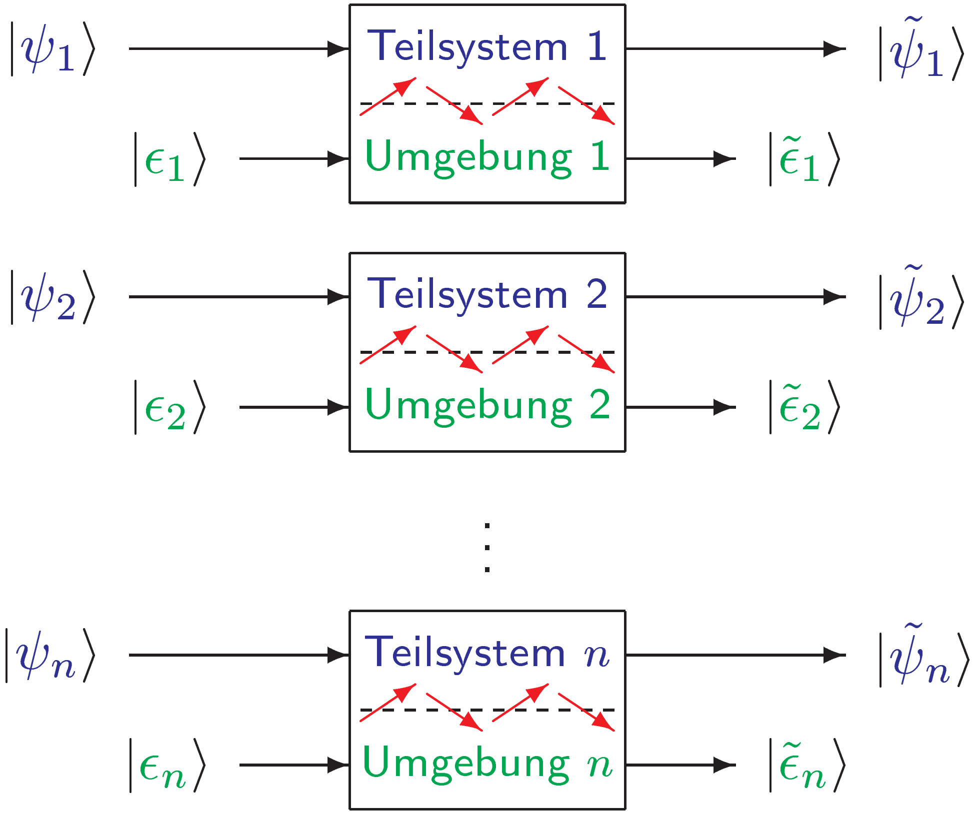
$$(H \otimes \mathbb{1}) \left(\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) |\epsilon\rangle \right) = |0\rangle |\epsilon\rangle$$

Aufhebung der Interferenz durch Störungen:

$$\begin{aligned} (H \otimes \mathbb{1}) \left(\frac{1}{\sqrt{2}} (|0\rangle |\epsilon_0\rangle + |1\rangle |\epsilon_1\rangle) \right) &= \tfrac{1}{2}(|0\rangle + |1\rangle) |\epsilon_0\rangle + \tfrac{1}{2}(|0\rangle - |1\rangle) |\epsilon_1\rangle \\ &= \tfrac{1}{2} |0\rangle (|\epsilon_0\rangle + |\epsilon_1\rangle) + \underbrace{\tfrac{1}{2} |1\rangle (|\epsilon_0\rangle - |\epsilon_1\rangle)}_{\text{Störterm}} \end{aligned}$$

Quantenkanal (III): Produktkanal

nur *lokale* Wechselwirkung, d. h., jedes Teilsystem hat *seine eigene* Umgebung:



Wiederholungscode

klassisch:

Sender: mehrfaches Senden der Information,

z. B. $0 \mapsto 000$, $1 \mapsto 111$

Empfänger: Vergleich der Ergebnisse und Mehrheitsentscheid

quantenmechanischer *Ansatz*:

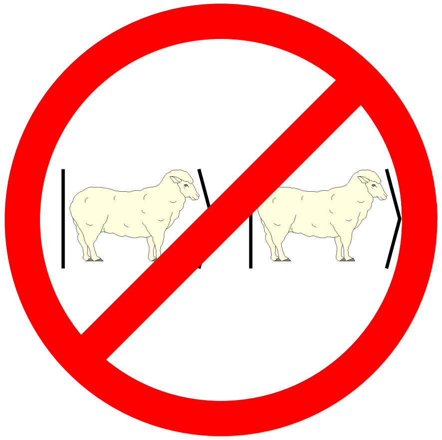
Sender: Kopieren der Information,

z. B. $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \mapsto |\psi\rangle\,|\psi\rangle\,|\psi\rangle$

Empfänger: Vergleich der Ergebnisse und Mehrheitsentscheid

aber ...

. . . so geht's nicht!



No-Cloning

- *universelles* Kopieren von Quantenzuständen ist unmöglich:

$$
\begin{array}{rcl}
|0\rangle\,|\text{Träger}\rangle & \mapsto & |0\rangle\,|0\rangle \\
|1\rangle\,|\text{Träger}\rangle & \mapsto & |1\rangle\,|1\rangle \\
\hline
(\alpha\,|0\rangle + \beta\,|1\rangle)\,|\text{Träger}\rangle & \mapsto & \alpha\,|0\rangle\,|0\rangle + \beta\,|1\rangle\,|1\rangle \\
 & & \neq \alpha^2\,|0\rangle\,|0\rangle + \beta^2\,|1\rangle\,|1\rangle \\
 & & \quad + \alpha\beta(|0\rangle\,|1\rangle + |1\rangle\,|0\rangle)
\end{array}
$$

- Vergleich von *unbekannten Quantenzuständen* ist nur *statistisch* möglich

Elementare Fehler (I)

Bit–Flip:

- Vertauschung der Basiszustände $|0\rangle$ und $|1\rangle$
- entspricht dem klassischen Bitfehler
- NOT–Gatter bzw. $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Phasenfehler:

- Invertierung der *relativen* Phase der Basiszustände $|0\rangle$ und $|1\rangle$
- ohne klassische Entsprechung
- $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Elementare Fehler (II)

Kombination:

- $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = i\sigma_x\sigma_z$

Konjugation:

$$\left.\begin{array}{l} \bullet \quad H\sigma_x H = \sigma_z \\ \bullet \quad H\sigma_z H = \sigma_x \end{array}\right\}$$ Vertauschung von Bit– und Phasenfehlern

Elementare Fehler (III)

Basis:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \frac{a_{11}+a_{22}}{2}\mathbb{1} + \frac{a_{11}-a_{22}}{2}\sigma_z + \frac{a_{12}+a_{21}}{2}\sigma_x + \frac{i(a_{12}-a_{21})}{2}\sigma_y$$

Lokale Fehler:

Fehler auf n Qubit:

$$\boldsymbol{e} = e_{i_1} \otimes \ldots \otimes e_{i_n} \qquad \text{mit } e_{i_k} \in \{\mathbb{1}, \sigma_x, \sigma_y, \sigma_z\}$$

Fehlergewicht:

Anzahl der Tensorfaktoren ungleich $\mathbb{1}$

Einfacher Quantencode (I)

$$\left.\begin{array}{lll} |0\rangle & \mapsto & |000\rangle \\ |1\rangle & \mapsto & |111\rangle \end{array}\right\} \Longrightarrow \alpha\,|0\rangle + \beta\,|1\rangle \mapsto \alpha\,|000\rangle + \beta\,|111\rangle$$

zweidimensionaler Unterraum $\mathcal{H}_\mathcal{C} \leq \mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2$

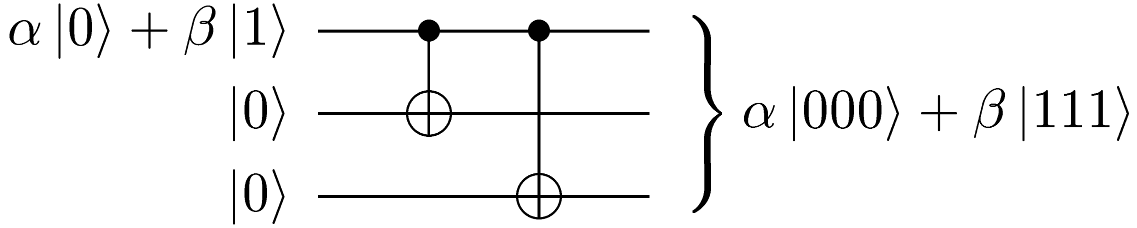
Bit–Flip	Zustand	Unterraum
ungestört	$\alpha\,\|000\rangle + \beta\,\|111\rangle$	$(\mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1})\mathcal{H}_\mathcal{C}$
1. Stelle	$\alpha\,\|100\rangle + \beta\,\|011\rangle$	$(\sigma_x \otimes \mathbb{1} \otimes \mathbb{1})\mathcal{H}_\mathcal{C}$
2. Stelle	$\alpha\,\|010\rangle + \beta\,\|101\rangle$	$(\mathbb{1} \otimes \sigma_x \otimes \mathbb{1})\mathcal{H}_\mathcal{C}$
3. Stelle	$\alpha\,\|001\rangle + \beta\,\|110\rangle$	$(\mathbb{1} \otimes \mathbb{1} \otimes \sigma_x)\mathcal{H}_\mathcal{C}$

orthogonale Zerlegung:

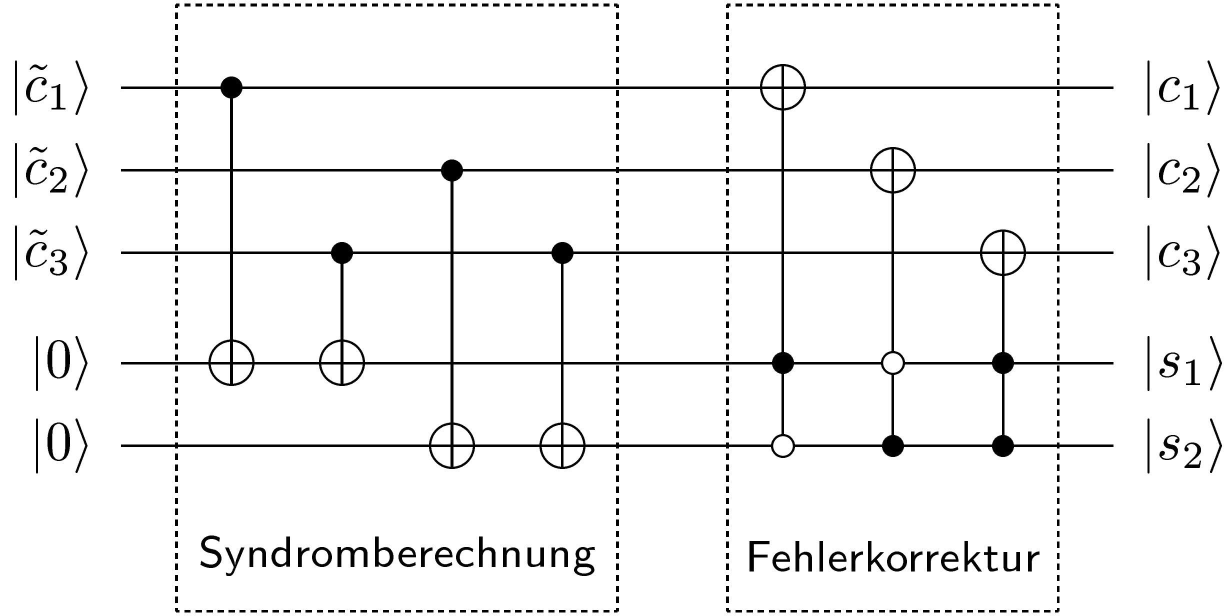
$$\mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2 =$$
$$(\mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1})\mathcal{H}_\mathcal{C} \oplus (\sigma_x \otimes \mathbb{1} \otimes \mathbb{1})\mathcal{H}_\mathcal{C} \oplus (\mathbb{1} \otimes \sigma_x \otimes \mathbb{1})\mathcal{H}_\mathcal{C} \oplus (\mathbb{1} \otimes \mathbb{1} \otimes \sigma_x)\mathcal{H}_\mathcal{C}$$

Einfacher Quantencode (II)

Codierung:



Decodierung:



Kurz & Knapp

- Korrektur von Phasenfehlern:
  nach Hadamard–Transformation über den dualen Code
- Konstruktion von Quantencodes:
  über schwach selbstduale Binärcodes (mit $\mathcal{C} \leq \mathcal{C}^{\perp}$) bzw. spezielle Codes über $GF(4)$
- Reduzierung der Komplexität des Decodierers:
  Adaption des Meggitt–Decoders für zyklische Codes

weitere Fragestellungen:

- reale Kanalmodelle
- Fehler durch ungenaue Operationen