

# Topologische Quantenfehlerkorrektur: Eine Einführung

Nicolai Lang\*

Institut für theoretische Physik III, Universität Stuttgart, 70550 Stuttgart, Deutschland

(Dated: 29. Januar 2013)

## I. MOTIVATION

- **Speichern von Qubits:** 2-Level System ("Spin")  $\leftrightarrow$  1 Qubit  
(Bsp. NV-Zentren, Elektronen-/Kernspins, Photonen, Atome)
- **Problem:** Schwer kontrollierbare Umgebung koppelt an 2-Level System.  
 $\hookrightarrow$  "Unbeobachtete Messung/Operation an/auf dem Qubit"  $\hookrightarrow$  Dekohärenz!
- **Fehlerkorrekturcodes:** "Verteile" (codiere) Information auf mehrere 2-Level Systeme.  
(klassisches Beispiel: Wiederholungs-Codes:  $0 \rightarrow 000, 1 \rightarrow 111$ )
- **Probleme:**
  - **No-Cloning-Theorem:** Kopieren von Qubit-Registern i.A. unmöglich.
  - **Kontinuierliche Fehler:** Fehler kann beliebige Rotation auf der Blochkugel erzeugen.
  - **Messungen:** Zerstören i.A. die Kohärenz.
- **Lösung:** Quantenfehlerkorrektur (Proof of Concept: Shor Code)

## II. DER STABILIZER FORMALISMUS

- **Ziel:** Beschreibung und Transformation hochverschränkter Zustände.
- **Problem:** Hohe Komplexität des Hilbertraums.  
 $N$  Qubits  $\hookrightarrow \mathcal{H} = \bigotimes_{i=1}^N \mathbb{C}_i^2 \hookrightarrow \dim \mathcal{H}^N = 2^N \hookrightarrow \sim 2^N$  komplexe Koordinaten.
- **Lösung:** Beschreibe spezielle Klasse von Multi-Qubit Zuständen mit Hilfe gruppentheoretischer Methoden  
 $\hookrightarrow$  Stabilizer Gruppen.

In diesem Zusammenhang benötigen wir die **Pauli-Gruppe**  $G_N$ :

**Definition 1** (Pauli-Gruppe). Die **Pauli-Gruppe** ist definiert als

$$G_1 := \text{span} \{ \sigma^x, \sigma^y, \sigma^z \} = \{ \pm \mathbb{1}, \pm i \mathbb{1}, \pm \sigma^x, \pm i \sigma^x, \pm \sigma^y, \pm i \sigma^y, \pm \sigma^z, \pm i \sigma^z \}$$

und wird von den Pauli-Matrizen erzeugt. Die Verallgemeinerung ist

$$G_N := \text{span} \left\{ \mathbb{1}_1 \otimes \cdots \otimes \sigma_k^i \cdots \otimes \mathbb{1}_N \mid i \in \{x, y, z\}; 1 \leq k \leq N, k \in \mathbb{N} \right\}$$

und operiert auf dem  $N$ -Qubit Hilbertraum  $\mathcal{H}^N$ .

Wir betrachten nun spezielle Untergruppen der Pauli-Gruppe  $G_N$ :

---

\* [nicolai@itp3.uni-stuttgart.de](mailto:nicolai@itp3.uni-stuttgart.de)

**Definition 2** (Stabilizer). Gegeben sei eine Menge  $\mathcal{G} = \{g_i\}_{i=1}^d \subseteq G_N$  **unabhängiger und paarweise kommutierender** Pauli-Operatoren. Dann nennen wir

$$\mathcal{S} := \text{span } \mathcal{G} \quad \text{and} \quad \mathcal{PS} := \left\{ |\Phi\rangle \in \mathcal{H}^N \mid \mathcal{S} |\Phi\rangle = |\Phi\rangle \right\}$$

den **Stabilizer**  $\mathcal{S}$  des **geschützten Unterraums**  $\mathcal{PS} \leq \mathcal{H}^N$ .

$\mathcal{G}$  umfasst die **Erzeuger** von  $\mathcal{S}$  und  $d = \text{rank } \mathcal{S}$  heißt **Rang** des Stabilizers.

- **Bemerkung:**  $\mathcal{S}$  ist eine **abelsche Untergruppe** von  $G_N$ .
- **Idee:** Beschreibe den Unterraum  $\mathcal{PS}$  durch Angabe/Transformation der Erzeuger  $\mathcal{G}$ .
- **Bemerkung:** Ist  $-\mathbb{1} \in \mathcal{S}$ , so ist  $\mathcal{PS} = \{0\}$  trivial.

**Satz 1** (Dimension von  $\mathcal{PS}$ ). Ist  $-\mathbb{1} \notin \mathcal{S}$ , dann gilt  $\dim \mathcal{PS} = 2^{N-d}$ .

*Beweis.* Siehe Nielsen and Chuang, Quantum Computation and Quantum Information. ■

Es folgt ein einfaches

**Beispiel 1** (EPR Zustand). Sei  $N = 2$  und  $\mathcal{G} = \{\sigma_1^x \sigma_2^x, \sigma_1^z \sigma_2^z\} \subseteq G_2$ . Offensichtlich sind die Erzeuger unabhängig und  $[\sigma_1^x \sigma_2^x, \sigma_1^z \sigma_2^z] = 0$ . Mit  $d = 2$  folgt also  $\dim \mathcal{PS} = 2^{2-2} = 1$ . Bis auf eine globale Phase ist der stabilisierte Zustand eindeutig bestimmt:

$$|EPR\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

- **Bemerkung:** Nicht alle Zustände in  $\mathcal{H}^N$  lassen sich mit Stabilizern beschreiben.

**Beispiel 2** (W Zustand). Der hochgradig verschränkte 3-Qubit Zustand

$$|W\rangle = \frac{1}{\sqrt{3}} (|001\rangle + |010\rangle + |100\rangle)$$

lässt sich **nicht** durch einen Stabilizer  $\mathcal{S}$  beschreiben (o.B.).

- Stabilizer Zustände sind also **sehr spezielle** (aber dennoch **hochverschränkte**) Multi-Qubit Zustände.
- **Spezielle unitäre Transformationen** von Stabilizer Zuständen lassen sich innerhalb des Stabilizer Formalismus durch Transformation der Erzeuger beschreiben.

**Beispiel 3** (Hadamard Gatter). Wende das (unitäre) Hadamard Gatter

$$H_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

auf den EPR-Zustand von oben an:

$$H_1 |EPR\rangle = \frac{1}{\sqrt{2}} (|+0\rangle + |-1\rangle)$$

Im Stabilizer Formalismus erfolgt diese Transformation durch das Vertauschen von  $\sigma_1^x$  und  $\sigma_1^z$  bei den Erzeugern:

$$H_1[\mathcal{G}] \equiv H_1 \mathcal{G} H_1^\dagger = \{\sigma_1^z \sigma_2^x, \sigma_1^x \sigma_2^z\} \subseteq G_2$$

Man überprüft leicht, dass  $H_1 |EPR\rangle$  durch  $\text{span } H_1[\mathcal{G}]$  beschrieben wird.

- **Gottesman-Knill Theorem:** Die Beschreibung und Transformation von Stabilizer Zuständen kann effizient (d.h. in Polynomialzeit) auf **klassischen Computern** simuliert werden.  $\leftrightarrow$  QC sind nicht immer "schneller".

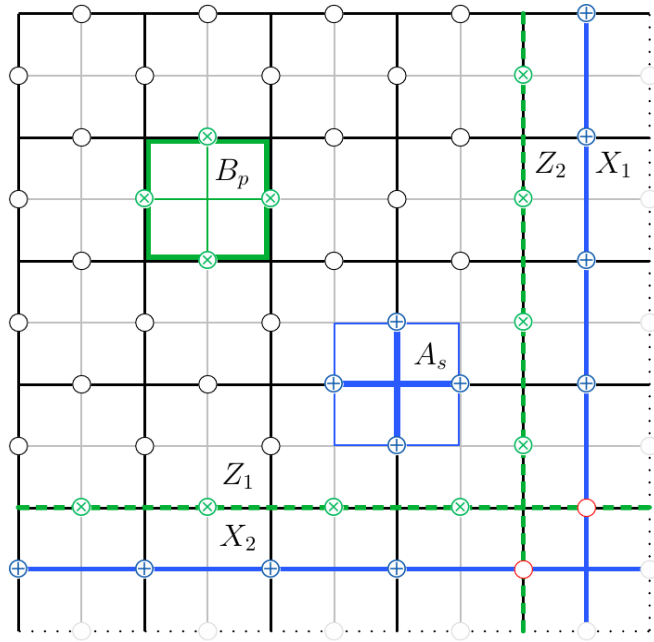


Abbildung 1. Zur Struktur des TCM.

### III. TOPOLOGISCHE QFK: DER TORIC CODE

Das Toric Code Model (TCM) – kurz “Toric Code” – wurde von A. Kitaev 1997 auf arXiv veröffentlicht. (*Annals of Physics* 303, 2 (2003) oder *quant-ph/9707021*)

#### A. Das Setting

- Betrachte ein Quadratgitter  $\mathcal{L}$  mit  $L \times L$  Zellen.
- Bette  $\mathcal{L}$  in den Torus  $\mathbb{T}^2$  ein  $\leftrightarrow$  Identifiziere Oben/Unten und Links/Rechts.
- – **Anzahl der Kanten:**  $|\mathbb{E}(\mathcal{L})| = 2L^2$ .  
– **Anzahl der Vertices:**  $|\mathbb{V}(\mathcal{L})| = L^2$ .  
– **Anzahl der Flächen:**  $|\mathbb{P}(\mathcal{L})| = L^2$ .
- Ordne jeder **Kante** ein 2-Level System zu, beschrieben durch einen Zustand in  $\mathbb{C}_e^2$ ,  $e \in \mathbb{E}(\mathcal{L})$ .
- Der Hilbertraum ist also  $\mathcal{H}(\mathcal{L}) = \bigotimes_{e \in \mathbb{E}(\mathcal{L})} \mathbb{C}_e^2$ .

#### B. Der Stabilizer

Wir definieren auf diesem Hilbertraum einen Stabilizer wie folgt:

**Definition 3** (TCM Stabilizer). *Definiere einen **Stern-Operator** für jeden Vertex*

$$A_s := \prod_{i \in s} \sigma_i^x \quad s \in \mathbb{V}(\mathcal{L})$$

*und einen **Plaketten-Operator** für jede Fläche des Gitters  $\mathcal{L}$*

$$B_p := \prod_{i \in p} \sigma_i^z \quad p \in \mathbb{P}(\mathcal{L}).$$

Der TCM Stabilizer ist gegeben durch

$$\mathcal{S} := \text{span} \{A_s, B_p\}_{s \in \mathbb{V}(\mathcal{L}), p \in \mathbb{P}(\mathcal{L})}.$$

- **Bemerkung:** Auf dem **dualen Gitter**  $\mathcal{L}^*$  werden Stern- zu Plaketten-Operatoren und umgekehrt.
- Die Operatoren kommutieren paarweise (da  $\{\sigma^x, \sigma^z\} = 0$ ),

$$[A_s, A_{s'}] = [B_p, B_{p'}] = [A_s, B_p] = 0 \quad \text{und} \quad A_s, B_p \in G_{2L^2}.$$

- Sind sie unabhängig? **Nein!** (**Wichtig:** Topologie des Torus)

$$\prod_{s \in \mathbb{V}(\mathcal{L})} A_s = \mathbb{1} = \prod_{p \in \mathbb{P}(\mathcal{L})} B_p$$

$\hookrightarrow$  2 Relationen zwischen den Erzeugern  $\hookrightarrow \text{rank } \mathcal{S} = (L^2 - 1) + (L^2 - 1) = 2L^2 - 2$

- Der geschützte Unterraum ist also  $\dim \mathcal{PS} = 2^{2L^2 - (2L^2 - 2)} = 2^2 = 4$  dimensional!
- **Idee:** Codiere 2 (logische) Qubits in  $\mathcal{PS}$ .

### C. Der Toric Code (TCM)

- **Ziel:** Finde Operatoren zum Auslesen und Manipulieren der 2 Qubits.  $\hookrightarrow \mathcal{PS}$  wird zu einem Quantencode.

**Definition 4** (String Operatoren). Sei  $\mathcal{C}$  ( $\mathcal{C}^*$ ) ein – nicht notwendigerweise geschlossener – Pfad auf dem Gitter  $\mathcal{L}$  (dualen Gitter  $\mathcal{L}^*$ ). Dann nennen wir

$$X[\mathcal{C}^*] := \prod_{i^* \in \mathcal{C}^*} \sigma_{i^*}^x, \quad Z[\mathcal{C}] := \prod_{i \in \mathcal{C}} \sigma_i^z$$

die zugeordneten **String Operatoren**.

- X- bzw. Z-String Operatoren antikommutieren mit den Plaketten- bzw. Stern-Operatoren an den Endpunkten von  $\mathcal{C}^*$  bzw.  $\mathcal{C}$  (mit allen anderen Stabilizer Operatoren kommutieren sie).
- Es gilt also für alle  $s \in \mathbb{V}(\mathcal{L})$  und  $p \in \mathbb{P}(\mathcal{L})$

$$\begin{aligned} [A_s, X[\mathcal{C}^*]] &= [B_p, X[\mathcal{C}^*]] = 0 \\ [A_s, Z[\mathcal{C}]] &= [B_p, Z[\mathcal{C}]] = 0 \end{aligned}$$

**genau dann wenn**  $\mathcal{C}$  bzw.  $\mathcal{C}^*$  **geschlossen** sind.

- $\hookrightarrow$  **Loop Operatoren** sind über  $\mathcal{PS}$  diagonalisierbar.
- Wähle **nicht-homologe** Loops  $\hookrightarrow X_1, X_2, Z_1, Z_2$ . ( $\mathcal{C}_1$  und  $\mathcal{C}_2$  heißen **homolog** gdw.  $\mathcal{C}_1 + \mathcal{C}_2$  der Rand einer Fläche auf dem Torus ist.)
- Die zugeordneten Loop Operatoren gehorchen der **Pauli Spin Algebra**: (Verhalten sich wie  $\sigma_1^{x,z}$  und  $\sigma_2^{x,z}$  auf 2-Qubit Hilbertraum.)

$$[Z_i, X_j] = [X_i, X_j] = [Z_i, Z_j] = 0, \quad \{Z_i, X_i\} = 0, \quad i \neq j.$$

- $Z_1$  und  $Z_2$  kommutieren untereinander und mit allen Operatoren in  $\mathcal{S}$ .  
 $\hookrightarrow$  Wähle eine **Eigenbasis** von  $Z_1, Z_2$  in  $\mathcal{PS}$ :

$$Z_j |v_1, v_2\rangle = v_j |v_1, v_2\rangle, \quad v_j \in \{-1, 1\}$$

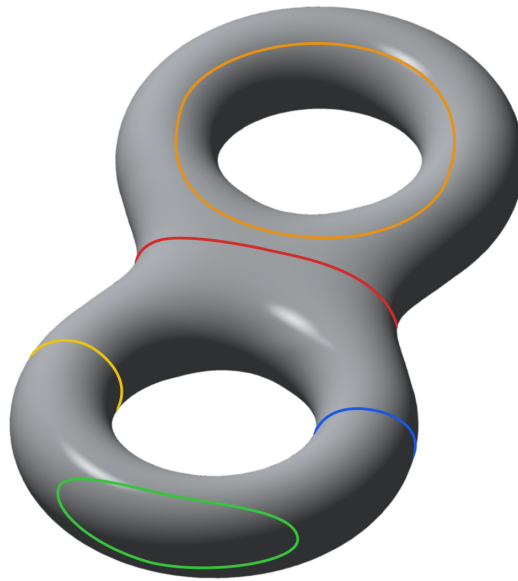


Abbildung 2. Zur ersten Homologiegruppe auf kompakten, orientierbaren 2-Mannigfaltigkeiten. Der gelbe (rote) Loop ist homolog zum blauen (grünen). Der orangene Loop ist zu keinem der anderen homolog.

- $\{|v_1, v_2\rangle\}_{v_i \in \{1, -1\}}$  ist eine ONB von  $\mathcal{PS}$ ;  $v_j$  heißen **Topologische Quantenzahlen**.
- $|v_1, v_2\rangle$  sind unsere gesuchten **logischer 2-Qubit Zustände**.
- **Flippe** Qubits mit  $X_j$ :

$$X_j |v_1, v_2\rangle = \begin{cases} |-v_1, v_2\rangle, & j = 1 \\ |v_1, -v_2\rangle, & j = 2 \end{cases}$$

- **Messe** Qubits mit  $Z_j$ .  
 $\hookrightarrow$  Wir codieren also **2 logische Qubits** in ein System aus  $2L^2$  **2-Level Systemen**.
- **Bemerkung:** Wird  $\mathcal{L}$  allgemein in eine orientierbare, kompakte 2-Mannigfaltigkeit mit Geschlecht  $g$  ("Anzahl der Löcher") eingebettet, so gilt  $\dim \mathcal{PS} = 4^g \leftrightarrow 2g$  Qubits (Torus  $\leftrightarrow g = 1 \leftrightarrow 2$  Qubits).

#### D. Zur topologischen Bedeutung des TCM

- **Erste Homologie Gruppe**  $H_1$ : Abelsche Gruppe bestehend aus Äquivalenzklassen von Loops auf dem eingebetteten Gitter  $\mathcal{L}$ :  $[\mathcal{C}_1] = [\mathcal{C}_2] \in H_1$  gdw. sich  $\mathcal{C}_1$  und  $\mathcal{C}_2$  um eine Menge von Plaketten  $p \in \mathbb{P}(\mathcal{L})$  unterscheiden.
- Ist  $\mathcal{C}$  der Rand einer Menge von Plaketten so folgt  $[\mathcal{C}] = 1 \in H_1$ .
- Außerdem gilt:  $Z[\mathcal{C}]$  ist das Produkt von **Plaketten Operatoren**  $\leftrightarrow Z[\mathcal{C}] = \mathbb{1} \in \text{Aut } \mathcal{PS}$ .
- Man erkennt dann leicht:  $Z : H_1 \rightarrow \text{Aut } \mathcal{PS}$  ist eine **Darstellung** von  $H_1$  auf  $\mathcal{PS}$ :

$$Z[\mathcal{C}_1 + \mathcal{C}_2] = Z[\mathcal{C}_1] \circ Z[\mathcal{C}_2]$$

- **Speziell gilt:**  $Z[\mathcal{C}_1] = Z[\mathcal{C}_2] \in \text{Aut } \mathcal{PS}$  gdw.  $[\mathcal{C}_1] = [\mathcal{C}_2] \in H_1$ , d.h. gdw.  $\mathcal{C}_1$  und  $\mathcal{C}_2$  homolog sind (sich also um eine Menge von Plaketten unterscheiden).  
 $\hookrightarrow$  Man kann Loops "stetig" deformieren ohne die Wirkungsweise des Loopoperators auf  $\mathcal{PS}$  zu verändern.
- Das Selbe gilt für  $X$  und  $H_1^*$  auf dem dualen Gitter  $\mathcal{L}^*$ .

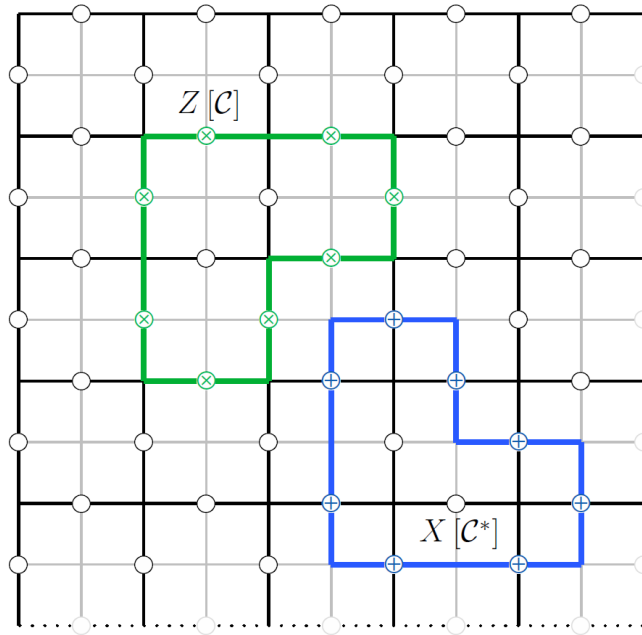


Abbildung 3. Zur Wirkung der Stringoperatoren.  
Beide Loops sind topologisch trivial. Die zugehörigen Loopoperatoren wirken also als  $\mathbb{1}$  auf  $\mathcal{PS}$ .

## E. Fehlerkorrektur

### 1. Vorbemerkungen

- Wir betrachten die folgenden (lokalen) Fehler:

$$\begin{aligned} \text{Spin-Flip Error (X-Typ): } \mathcal{PS} \ni |\Psi\rangle &\longrightarrow \sigma_i^x |\Psi\rangle \notin \mathcal{PS} \\ \text{Phase-Flip Error (Z-Typ): } \mathcal{PS} \ni |\Psi\rangle &\longrightarrow \sigma_i^z |\Psi\rangle \notin \mathcal{PS} \end{aligned}$$

- **Detektion:** Messung der Stabilizer Operatoren

$$\begin{aligned} \text{Spin-Flip Error: } B_p \sigma_i^x |\Psi\rangle &= -\sigma_i^x |\Psi\rangle \quad \text{falls } i \in p \\ \text{Phase-Flip Error: } A_s \sigma_i^z |\Psi\rangle &= -\sigma_i^z |\Psi\rangle \quad \text{falls } i \in s \end{aligned}$$

$\hookrightarrow$  Fehler können detektiert werden, ohne die codierte Information zu zerstören!

- **Wichtig:** Wegen  $\prod_{s \in \mathcal{V}(\mathcal{L})} A_s = \mathbb{1} = \prod_{p \in \mathcal{P}(\mathcal{L})} B_p$  treten positive Fehlermessungen (Eigenwert  $-1$ ) für jeden Fehlertyp (X oder Y) immer **paarweise** auf.
- Wirken Fehler gleichen Typs auf benachbarte Spins, bilden sich "Fehlerstrings", die durch entsprechende Stringoperatoren  $Z[\mathcal{C}_{rs}]$  (Z-Typ) bzw.  $X[\mathcal{C}_{pq}^*]$  (X-Typ) beschrieben werden.
  - $\hookrightarrow$  Nur Detektion der **Enden der Strings** möglich!
  - $\hookrightarrow$  Verlauf (speziell: Topologie) der Fehlerstrings ist **nicht** messbar.

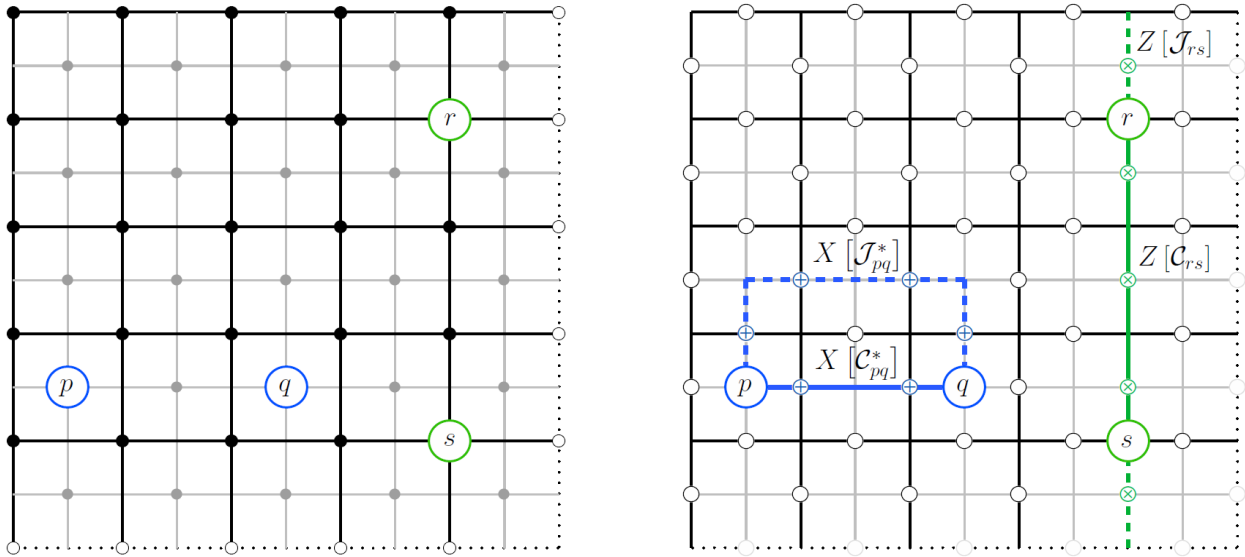


Abbildung 4. Zur algorithmischen Fehlerkorrektur. Links: Syndrome-Messung. Rechts: Korrektur-Operatoren.

## 2. Der Fehlerkorrekturalgorithmus

1. **Messe** alle Stern- und Plakettenoperatoren und markiere die Vertices/Plaketten an denen ein  $-1$  Eigenwert gemessen wurde.  $\hookrightarrow$  **Error-Syndrom**
2. **Korrigiere** die Fehler mittels Stringoperatoren minimaler Länge, indem die Vertices (Plaketten) mit  $-1$  Eigenwert über Z- (X-) Typ Stringoperatoren verbunden werden.

- **Idee:** Die Stringoperatoren komplettieren die Fehler zu Loopoperatoren.

$\hookrightarrow$  Diese führen nicht aus  $\mathcal{PS}$  heraus und operieren trivial auf  $\mathcal{PS}$  falls  $\mathcal{C}_{rs}^* + \mathcal{J}_{rs}^*$  trivial bzgl. Homologie ist:

$$X[\mathcal{C}_{rs}^*]X[\mathcal{J}_{rs}^*] = X[\mathcal{C}_{rs}^* + \mathcal{J}_{rs}^*] = 1 \quad \text{auf } \mathcal{PS} \quad \text{falls} \quad [\mathcal{C}_{rs}^* + \mathcal{J}_{rs}^*] = 1 \in H_1$$

- **Problem:** Bei zu vielen Fehlern führt der Algorithmus zu nicht-trivialen Loops.

$\hookrightarrow$  Unbeabsichtigter Bit/Phase-Flip auf dem Codespace  $\mathcal{PS}$ :

$$Z[\mathcal{C}_{rs}]Z[\mathcal{J}_{rs}] = Z[\mathcal{C}_{rs} + \mathcal{J}_{rs}] = Z_2 \quad \text{auf } \mathcal{PS} \quad \text{falls} \quad [\mathcal{C}_{rs} + \mathcal{J}_{rs}] \neq 1 \in H_1$$

$\hookrightarrow$  Qubit zerstört!

- Der Toric Code kann demnach  $\lfloor \frac{L-1}{2} \rfloor$  Fehler (X oder Y) korrigieren.

$\hookrightarrow$  Größeres Gitter (i.e. mehr Spins)  $\Rightarrow$  Mehr Fehler korrigierbar.