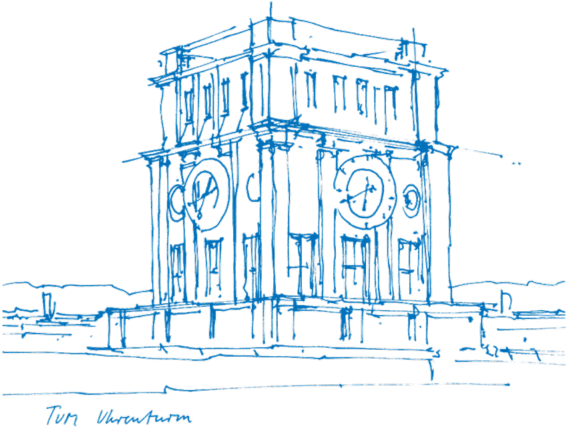
# Clifford Tableaus and the Stabilizer Algorithm

**Leonard Uscinowicz**

Technical University of Munich

December 20th, 2024



# Outline

# Pauli Matrices

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

[1] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Pauli Matrices

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

**Products of Pauli matrices:**

$$I^2 = X^2 = Y^2 = Z^2 = I$$

$$IX = XI = X \qquad IY = YI = Y \qquad IZ = ZI = Z$$

$$XY = iZ \qquad YX = -iZ$$

$$YZ = iX \qquad ZY = -iX$$

$$ZX = iY \qquad XZ = -iY$$

[1] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Group Theory

**Group** $(G, \cdot)$ is a non-empty set $G$ with a binary group multiplication operation $" \cdot "$.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Group Theory

**Group** $(G, \cdot)$ is a non-empty set $G$ with a binary group multiplication operation "$\cdot$".

Properties:

- **Closure:** $\forall g_1, g_2 \in G \implies g_1 \cdot g_2 \in G$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Group Theory

**Group** $(G, \cdot)$ is a non-empty set $G$ with a binary group multiplication operation $" \cdot "$.

Properties:

- **Closure:** $\forall g_1, g_2 \in G \implies g_1 \cdot g_2 \in G$
- **Associativity:** $\forall g_1, g_2, g_3 \in G \implies g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Group Theory

**Group** $(G, \cdot)$ is a non-empty set $G$ with a binary group multiplication operation $" \cdot "$.

Properties:

- **Closure:** $\forall g_1, g_2 \in G \implies g_1 \cdot g_2 \in G$
- **Associativity:** $\forall g_1, g_2, g_3 \in G \implies g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$
- **Identity:** $\exists e \in G$ such that $\forall g \in G \implies e \cdot g = g \cdot e = g$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

## Group Theory

**Group** $(G, \cdot)$ is a non-empty set $G$ with a binary group multiplication operation "$\cdot$".

Properties:

- **Closure:** $\forall g_1, g_2 \in G \implies g_1 \cdot g_2 \in G$
- **Associativity:** $\forall g_1, g_2, g_3 \in G \implies g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$
- **Identity:** $\exists e \in G$ such that $\forall g \in G \implies e \cdot g = g \cdot e = g$
- **Inverse:** $\forall g \in G \implies \exists g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Pauli Group
## Definitions

$\mathcal{P}_n$ is defined as the group of $n$-qubit Pauli operators.
It consists of all tensor products of $n$ Pauli matrices, with a phase factor $\pm 1$ or $\pm i$.

[1] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Pauli Group
## Definitions

$\mathcal{P}_n$ is defined as the group of $n$-qubit Pauli operators.
It consists of all tensor products of $n$ Pauli matrices, with a phase factor $\pm 1$ or $\pm i$.

$$\mathcal{P}_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$$

[1] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Pauli Group
## Definitions

$\mathcal{P}_n$ is defined as the group of $n$-qubit Pauli operators.
It consists of all tensor products of $n$ Pauli matrices, with a phase factor $\pm 1$ or $\pm i$.

$$\mathcal{P}_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$$

$$\mathcal{P}_n = \left\{ i^m \bigotimes_{j=1}^{n} \sigma_{k_j} \middle| m, k_j \in \{0,1,2,3\}, \sigma_0 = I, \sigma_1 = X, \sigma_2 = Y, \sigma_3 = Z \right\}$$


[1] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Pauli Group
## Definitions

$\mathcal{P}_n$ is defined as the group of $n$-qubit Pauli operators.
It consists of all tensor products of $n$ Pauli matrices, with a phase factor $\pm 1$ or $\pm i$.

$$\mathcal{P}_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$$

$$\mathcal{P}_n = \left\{ i^m \bigotimes_{j=1}^{n} \sigma_{k_j} \middle| m, k_j \in \{0,1,2,3\}, \sigma_0 = I, \sigma_1 = X, \sigma_2 = Y, \sigma_3 = Z \right\}$$

Size of a Pauli Group: $|\mathcal{P}_n| = 4^{n+1}$


[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Pauli Group
## Operations

Given two Pauli operators $P = i^{m_P} \bigotimes_{j=1}^{n} P_j$ and $Q = i^{m_Q} \bigotimes_{j=1}^{n} Q_j$, their product, as necessitated by Group Definition, is:

$$P \cdot Q = i^{m_P + m_Q} \bigotimes_{j=1}^{n} P_j Q_j$$

[1] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Pauli Group
## Operations

Given two Pauli operators $P = i^{m_P} \bigotimes_{j=1}^{n} P_j$ and $Q = i^{m_Q} \bigotimes_{j=1}^{n} Q_j$, their product, as necessitated by Group Definition, is:

$$P \cdot Q = i^{m_P + m_Q} \bigotimes_{j=1}^{n} P_j Q_j$$

$P$ commutes with $Q$ if the number of indices $j$ such that $P_j$ anti-commutes with $Q_j$ is even.

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Group Generators

A set of $l$ elements $\{g_i\}_{1\leq i\leq l}$ generates a group $G$ if every element $g \in G$ can be written as a product of the generators.
In this case, the group $G$ can be written in terms of its generators:

$$G = \langle g_i \mid i \in \mathbb{N}, 1 \leq i \leq l \rangle$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Group Generators

A set of $l$ elements $\{g_i\}_{1\leq i\leq l}$ generates a group $G$ if every element $g \in G$ can be written as a product of the generators.

In this case, the group $G$ can be written in terms of its generators:

$$G = \langle g_i \mid i \in \mathbb{N}, 1 \leq i \leq l \rangle$$

**Examples:**

$$\mathcal{P}_1 = \langle X, Z, iI \rangle$$
$$\langle X \rangle = \{I, X\}$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Outline

# Stabilizer Groups
## Definitions

- Element $g \in \mathcal{P}_n$ **stabilizes** $|\psi\rangle$ iff $g|\psi\rangle = |\psi\rangle$.
  $|\psi\rangle$ is eigenstate of $g$ with eigenvalue $+1$.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Stabilizer Groups
## Definitions

- Element $g \in \mathcal{P}_n$ **stabilizes** $|\psi\rangle$ iff $g|\psi\rangle = |\psi\rangle$.
  $|\psi\rangle$ is eigenstate of $g$ with eigenvalue $+1$.

- $S \widehat{=}$Subgroup of the Pauli Group $\mathcal{P}_n$: $S \subseteq \mathcal{P}_n$.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Stabilizer Groups
## Definitions

- Element $g \in \mathcal{P}_n$ **stabilizes** $|\psi\rangle$ iff $g|\psi\rangle = |\psi\rangle$.
  $|\psi\rangle$ is eigenstate of $g$ with eigenvalue $+1$.

- $S \widehat{=}$Subgroup of the Pauli Group $\mathcal{P}_n$: $S \subseteq \mathcal{P}_n$.

- $V_S \widehat{=}$Set of $n$-qubit states stabilized by $S$:

$$V_S = \{|\psi\rangle \mid S \subseteq \mathcal{P}_n, \forall g \in S \text{ holds: } g|\psi\rangle = |\psi\rangle\}$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Stabilizer Groups

## Properties

Not just any subgroup $S$ of the Pauli group can be used as the stabilizer for a non-trivial vector space $V_S$.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Stabilizer Groups
## Properties

Not just any subgroup $S$ of the Pauli group can be used as the stabilizer for a non-trivial vector space $V_S$.

**Example:** $S = \{\pm I, \pm X\}$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Stabilizer Groups
## Properties

Not just any subgroup $S$ of the Pauli group can be used as the stabilizer for a non-trivial vector space $V_S$.

**Example:** $S = \{\pm I, \pm X\}$

$$(-I) \in S \text{ and } (-I)\left|\psi\right\rangle = -\left|\psi\right\rangle \implies \left|\psi\right\rangle = \vec{0} \implies V_S = \left\{\vec{0}\right\} \text{ (trivial)}$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Stabilizer Groups
## Properties

Not just any subgroup $S$ of the Pauli group can be used as the stabilizer for a non-trivial vector space $V_S$.

**Example:** $S = \{\pm I, \pm X\}$

$$(-I) \in S \text{ and } (-I)\left|\psi\right\rangle = -\left|\psi\right\rangle \implies \left|\psi\right\rangle = \vec{0} \implies V_S = \left\{\vec{0}\right\} \text{ (trivial)}$$

Conditions for $S$ such that $V_S$ not trivial:

- **Commutativity:** $\forall g_1, g_2 \in S$ holds: $g_1 g_2 = g_2 g_1$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Stabilizer Groups
## Properties

Not just any subgroup $S$ of the Pauli group can be used as the stabilizer for a non-trivial vector space $V_S$.

**Example:** $S = \{\pm I, \pm X\}$

$$(-I) \in S \text{ and } (-I)\left|\psi\right\rangle = -\left|\psi\right\rangle \implies \left|\psi\right\rangle = \vec{0} \implies V_S = \left\{\vec{0}\right\} \text{ (trivial)}$$

Conditions for $S$ such that $V_S$ not trivial:

- **Commutativity:** $\forall g_1, g_2 \in S$ holds: $g_1 g_2 = g_2 g_1$
- **Strict Identity:** $-I \notin S$, $iI \notin S$, $-iI \notin S$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Stabilizer Conditions

## Commutativity Proof

Let $V_S$ be non-trivial and let $g_1, g_2 \in S$.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Stabilizer Conditions

## Commutativity Proof

Let $V_S$ be non-trivial and let $g_1, g_2 \in S$.

$\implies g_1$ and $g_2$ are tensor products of Pauli matrices.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Stabilizer Conditions

## Commutativity Proof

Let $V_S$ be non-trivial and let $g_1, g_2 \in S$.

$\implies g_1$ and $g_2$ are tensor products of Pauli matrices.

$\implies g_1$ and $g_2$ must either commute or anti-commute.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Stabilizer Conditions
## Commutativity Proof

Let $V_S$ be non-trivial and let $g_1, g_2 \in S$.

$\implies g_1$ and $g_2$ are tensor products of Pauli matrices.

$\implies g_1$ and $g_2$ must either commute or anti-commute.

Suppose $g_1$ and $g_2$ anti-commute:

$$|\psi\rangle = g_1 g_2 |\psi\rangle = -g_2 g_1 |\psi\rangle = -|\psi\rangle \quad \iff \quad |\psi\rangle = \vec{0} \quad \implies \quad V_S \text{ is trivial.}$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Stabilizer Conditions

## Commutativity Proof

Let $V_S$ be non-trivial and let $g_1, g_2 \in S$.

$\implies g_1$ and $g_2$ are tensor products of Pauli matrices.

$\implies g_1$ and $g_2$ must either commute or anti-commute.

Suppose $g_1$ and $g_2$ anti-commute:

$$|\psi\rangle = g_1 g_2 |\psi\rangle = -g_2 g_1 |\psi\rangle = -|\psi\rangle \quad \iff \quad |\psi\rangle = \vec{0} \quad \implies \quad V_S \text{ is trivial.}$$

$\implies g_1$ and $g_2$ anti-commuting leads to a contradiction.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Stabilizer Conditions

## Commutativity Proof

Let $V_S$ be non-trivial and let $g_1, g_2 \in S$.

$\implies g_1$ and $g_2$ are tensor products of Pauli matrices.

$\implies g_1$ and $g_2$ must either commute or anti-commute.

Suppose $g_1$ and $g_2$ anti-commute:

$$|\psi\rangle = g_1 g_2 |\psi\rangle = -g_2 g_1 |\psi\rangle = -|\psi\rangle \quad \iff \quad |\psi\rangle = \vec{0} \quad \implies \quad V_S \text{ is trivial.}$$

$\implies g_1$ and $g_2$ anti-commuting leads to a contradiction.

$\implies g_1$ and $g_2$ commute.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Stabilizer Conditions
## Strict Identity Proof

Let $V_S$ be non-trivial.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Stabilizer Conditions
## Strict Identity Proof

Let $V_S$ be non-trivial.

$$
\begin{aligned}
(-I) \in S &\implies |\psi\rangle = (-I)\,|\psi\rangle = -\,|\psi\rangle &&\iff |\psi\rangle = \vec{0} &&\implies V_S \text{ is trivial.}\\
(iI) \in S &\implies |\psi\rangle = (iI)\,|\psi\rangle = i\,|\psi\rangle &&\iff |\psi\rangle = \vec{0} &&\implies V_S \text{ is trivial.}\\
(-iI) \in S &\implies |\psi\rangle = (-iI)\,|\psi\rangle = -i\,|\psi\rangle &&\iff |\psi\rangle = \vec{0} &&\implies V_S \text{ is trivial.}
\end{aligned}
$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Stabilizer Conditions
## Strict Identity Proof

Let $V_S$ be non-trivial.

$$(-I) \in S \implies |\psi\rangle = (-I)\,|\psi\rangle = -\,|\psi\rangle \iff |\psi\rangle = \vec{0} \implies V_S \text{ is trivial.}$$

$$(iI) \in S \implies |\psi\rangle = (iI)\,|\psi\rangle = i\,|\psi\rangle \iff |\psi\rangle = \vec{0} \implies V_S \text{ is trivial.}$$

$$(-iI) \in S \implies |\psi\rangle = (-iI)\,|\psi\rangle = -i\,|\psi\rangle \iff |\psi\rangle = \vec{0} \implies V_S \text{ is trivial.}$$

$-I \in S$, $iI \in S$, $-iI \in S$ lead to contradictions.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Check Matrix
## Structure

Suppose $S = \langle g_i \mid i \in \mathbb{N}, 1 \leq i \leq l \rangle$.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Check Matrix
## Structure

Suppose $S = \langle g_i \mid i \in \mathbb{N}, 1 \leq i \leq l \rangle$.

Extremely useful way of presenting the generators: **Check Matrix** $H_S$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Check Matrix

## Structure

Suppose $S = \langle g_i \mid i \in \mathbb{N}, 1 \leq i \leq l \rangle$.

Extremely useful way of presenting the generators: **Check Matrix** $H_S$

$H_S$ is an $l \times 2n$ binary matrix whose rows correspond to the generators $g_1$ through $g_l$.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Check Matrix
## Structure

Suppose $S = \langle g_i \mid i \in \mathbb{N}, 1 \leq i \leq l \rangle$.

Extremely useful way of presenting the generators: **Check Matrix** $H_S$

$H_S$ is an $l \times 2n$ binary matrix whose rows correspond to the generators $g_1$ through $g_l$.

Example:
$$l \left\{ \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ \underbrace{0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0}_{n} & & & & & & & \underbrace{1 \;\; 0 \;\; 1 \;\; 0 \;\; 1 \;\; 0 \;\; 1}_{n} \end{bmatrix} \right.$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Check Matrix
## Interpretation

- Row $i$ corresponds to generator $g_i \in S$.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Check Matrix
## Interpretation

- Row $i$ corresponds to generator $g_i \in S$.
- Left $l \times n$ submatrix contains 1s to indicate which generators contain $X$s.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Check Matrix
## Interpretation

- Row $i$ corresponds to generator $g_i \in S$.
- Left $l \times n$ submatrix contains 1s to indicate which generators contain $X$s.
- Right $l \times n$ submatrix contains 1s to indicate which generators contain $Z$s.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Check Matrix
## Interpretation

- Row $i$ corresponds to generator $g_i \in S$.
- Left $l \times n$ submatrix contains 1s to indicate which generators contain $X$s.
- Right $l \times n$ submatrix contains 1s to indicate which generators contain $Z$s.
- Presence of 1 in both submatrices indicates $Y$ in that generator.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Check Matrix
## Interpretation

- Row $i$ corresponds to generator $g_i \in S$.
- Left $l \times n$ submatrix contains 1s to indicate which generators contain $X$s.
- Right $l \times n$ submatrix contains 1s to indicate which generators contain $Z$s.
- Presence of 1 in both submatrices indicates $Y$ in that generator.

More explicitly, with $h_{i,j}$ denoting the element of $H_S$ at row $i$ and column $j$:

- If $g_i$ contains $I$ on the $j^{\text{th}}$ qubit $\implies h_{i,j} = 0$ and $h_{i,n+j} = 0$.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Check Matrix
## Interpretation

- Row $i$ corresponds to generator $g_i \in S$.
- Left $l \times n$ submatrix contains 1s to indicate which generators contain $X$s.
- Right $l \times n$ submatrix contains 1s to indicate which generators contain $Z$s.
- Presence of 1 in both submatrices indicates $Y$ in that generator.

More explicitly, with $h_{i,j}$ denoting the element of $H_S$ at row $i$ and column $j$:

- If $g_i$ contains $I$ on the $j^{\text{th}}$ qubit $\Longrightarrow h_{i,j} = 0$ and $h_{i,n+j} = 0$.
- If $g_i$ contains $X$ on the $j^{\text{th}}$ qubit $\Longrightarrow h_{i,j} = 1$ and $h_{i,n+j} = 0$.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Check Matrix
## Interpretation

- Row $i$ corresponds to generator $g_i \in S$.
- Left $l \times n$ submatrix contains 1s to indicate which generators contain $X$s.
- Right $l \times n$ submatrix contains 1s to indicate which generators contain $Z$s.
- Presence of 1 in both submatrices indicates $Y$ in that generator.

More explicitly, with $h_{i,j}$ denoting the element of $H_S$ at row $i$ and column $j$:

- If $g_i$ contains $I$ on the $j^{\text{th}}$ qubit $\implies h_{i,j} = 0$ and $h_{i,n+j} = 0$.
- If $g_i$ contains $X$ on the $j^{\text{th}}$ qubit $\implies h_{i,j} = 1$ and $h_{i,n+j} = 0$.
- If $g_i$ contains $Z$ on the $j^{\text{th}}$ qubit $\implies h_{i,j} = 0$ and $h_{i,n+j} = 1$.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Check Matrix
## Interpretation

- Row $i$ corresponds to generator $g_i \in S$.
- Left $l \times n$ submatrix contains 1s to indicate which generators contain $X$s.
- Right $l \times n$ submatrix contains 1s to indicate which generators contain $Z$s.
- Presence of 1 in both submatrices indicates $Y$ in that generator.

More explicitly, with $h_{i,j}$ denoting the element of $H_S$ at row $i$ and column $j$:

- If $g_i$ contains $I$ on the $j^{\text{th}}$ qubit $\implies h_{i,j} = 0$ and $h_{i,n+j} = 0$.
- If $g_i$ contains $X$ on the $j^{\text{th}}$ qubit $\implies h_{i,j} = 1$ and $h_{i,n+j} = 0$.
- If $g_i$ contains $Z$ on the $j^{\text{th}}$ qubit $\implies h_{i,j} = 0$ and $h_{i,n+j} = 1$.
- If $g_i$ contains $Y$ on the $j^{\text{th}}$ qubit $\implies h_{i,j} = 1$ and $h_{i,n+j} = 1$.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Check Matrix
## Example Steane Code

For Readability tensor product operator signs are left out. $\sigma_i \sigma_j$ corresponds to $\sigma_i \otimes \sigma_j$.

$$\left[\begin{array}{ccccccc|ccccccc}
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1
\end{array}\right] \widehat{=}$$

| Generator | Operator |
|---|---|
| $g_1$ | $I\,I\,I\,X\,X\,X\,X$ |
| $g_2$ | $I\,X\,X\,I\,I\,X\,X$ |
| $g_3$ | $X\,I\,X\,I\,X\,I\,X$ |
| $g_4$ | $I\,I\,I\,Z\,Z\,Z\,Z$ |
| $g_5$ | $I\,Z\,Z\,I\,I\,Z\,Z$ |
| $g_6$ | $Z\,I\,Z\,I\,Z\,I\,Z$ |

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Unitary Operations
## Main Revelation

Suppose $U$ is a unitary operator, $|\psi\rangle \in V_S$ and $g \in S$.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Unitary Operations
## Main Revelation

Suppose $U$ is a unitary operator, $|\psi\rangle \in V_S$ and $g \in S$.

$$U|\psi\rangle = Ug|\psi\rangle = UgI|\psi\rangle = UgU^\dagger U|\psi\rangle = \left(UgU^\dagger\right)U|\psi\rangle$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Unitary Operations
## Main Revelation

Suppose $U$ is a unitary operator, $|\psi\rangle \in V_S$ and $g \in S$.

$$U|\psi\rangle = Ug|\psi\rangle = UgI|\psi\rangle = UgU^\dagger U|\psi\rangle = \left(UgU^\dagger\right)U|\psi\rangle$$

$\implies$ State $U|\psi\rangle$ is stabilized by $UgU^\dagger$.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Unitary Operations
## Main Revelation

Suppose $U$ is a unitary operator, $|\psi\rangle \in V_S$ and $g \in S$.

$$U|\psi\rangle = Ug|\psi\rangle = UgI|\psi\rangle = UgU^\dagger U|\psi\rangle = \left(UgU^\dagger\right)U|\psi\rangle$$

$\implies$ State $U|\psi\rangle$ is stabilized by $UgU^\dagger$.

$\implies$ If we can describe a state by its stabilizers, we can easily compute the stabilizers of the state that emerges from the previous state under a unitary operation.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Unitary Operations
## Advantages for Computation

For certain special unitary operations $U$ this transformation of the generators takes on a particularly appealing form.

# Unitary Operations

## Advantages for Computation

For certain special unitary operations $U$ this transformation of the generators takes on a particularly appealing form.

$$HXH^\dagger = Z \qquad HYH^\dagger = -Y \qquad HZH^\dagger = X$$

# Unitary Operations
## Advantages for Computation

For certain special unitary operations $U$ this transformation of the generators takes on a particularly appealing form.

$$HXH^\dagger = Z \qquad HYH^\dagger = -Y \qquad HZH^\dagger = X$$

**Example:**
(Unkown) State $|\psi\rangle$ stabilized by $X$.

# Unitary Operations
## Advantages for Computation

For certain special unitary operations $U$ this transformation of the generators takes on a particularly appealing form.

$$HXH^\dagger = Z \qquad HYH^\dagger = -Y \qquad HZH^\dagger = X$$

**Example:**

(Unkown) State $|\psi\rangle$ stabilized by $X$.

$\longrightarrow$ Apply Hadamard gate $H$ to $|\psi\rangle$.

# Unitary Operations

## Advantages for Computation

For certain special unitary operations $U$ this transformation of the generators takes on a particularly appealing form.

$$HXH^\dagger = Z \qquad HYH^\dagger = -Y \qquad HZH^\dagger = X$$

**Example:**

(Unkown) State $|\psi\rangle$ stabilized by $X$.

$\longrightarrow$ Apply Hadamard gate $H$ to $|\psi\rangle$.

$\Longrightarrow$ Resulting (Unkown) state $|\psi'\rangle$ stabilized by $Z$.

# Unitary Operations
## Transformation under Conjugation

| Operation | Input | Output |
|---|---|---|
| $CX$ | $X_1$ | $X_1X_2$ |
| | $X_2$ | $X_2$ |
| | $Z_1$ | $Z_1$ |
| | $Z_2$ | $Z_1Z_2$ |
| $H$ | $X$ | $Z$ |
| | $Z$ | $X$ |
| $S$ | $X$ | $Y$ |
| | $Z$ | $Z$ |

| Operation | Input | Output |
|---|---|---|
| $X$ | $X$ | $X$ |
| | $Z$ | $-Z$ |
| $Y$ | $X$ | $-X$ |
| | $Z$ | $-Z$ |
| $Z$ | $X$ | $-X$ |
| | $Z$ | $Z$ |

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement
## Main Principles

We want to measure observable $g \in \mathcal{P}_n$ of state $|\psi\rangle$, stabilized by $\langle g_i \mid i \in \mathbb{N}, 1 \leq i \leq l \rangle$.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement
## Main Principles

We want to measure observable $g \in \mathcal{P}_n$ of state $|\psi\rangle$, stabilized by $\langle g_i \mid i \in \mathbb{N}, 1 \leq i \leq l\rangle$.

**Two possibilities:**

1. $g$ commutes with all generators of the stabilizer.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement
## Main Principles

We want to measure observable $g \in \mathcal{P}_n$ of state $|\psi\rangle$, stabilized by $\langle g_i \mid i \in \mathbb{N}, 1 \leq i \leq l \rangle$.

**Two possibilities:**

1. $g$ commutes with all generators of the stabilizer.
   $\Longrightarrow$ Measurement outcome is deterministic.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement
## Main Principles

We want to measure observable $g \in \mathcal{P}_n$ of state $|\psi\rangle$, stabilized by $\langle g_i \mid i \in \mathbb{N}, 1 \leq i \leq l\rangle$.

**Two possibilities:**

1. $g$ commutes with all generators of the stabilizer.
   $\implies$ Measurement outcome is deterministic.
2. $g$ anti-commutes with at least 1 generator of the stabilizer.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement
## Main Principles

We want to measure observable $g \in \mathcal{P}_n$ of state $|\psi\rangle$, stabilized by $\langle g_i \mid i \in \mathbb{N}, 1 \leq i \leq l \rangle$.

**Two possibilities:**

1. $g$ commutes with all generators of the stabilizer.
   $\implies$ Measurement outcome is deterministic.
2. $g$ anti-commutes with at least 1 generator of the stabilizer.
   $\implies$ Measurement outcome is not deterministic.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement
## Deterministic case

$g$ commutes with all $g_i$ and assume $g$ does not have a global phase.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement
## Deterministic case

$g$ commutes with all $g_i$ and assume $g$ does not have a global phase.

$$\forall i \text{ holds: } g_i g \left|\psi\right\rangle = g g_i \left|\psi\right\rangle = g \left|\psi\right\rangle \quad \Longrightarrow \quad g \left|\psi\right\rangle \in V_S$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement
## Deterministic case

$g$ commutes with all $g_i$ and assume $g$ does not have a global phase.

$$\forall i \text{ holds: } g_i g \left|\psi\right\rangle = g g_i \left|\psi\right\rangle = g \left|\psi\right\rangle \implies g \left|\psi\right\rangle \in V_S$$

$$g^2 \left|\psi\right\rangle = I \left|\psi\right\rangle = \left|\psi\right\rangle \implies g \left|\psi\right\rangle = \pm \left|\psi\right\rangle \implies g \in S \veebar (-g) \in S$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement
## Deterministic case

$g$ commutes with all $g_i$ and assume $g$ does not have a global phase.

$$\forall i \ \text{holds:}\ g_i g \left|\psi\right\rangle = g g_i \left|\psi\right\rangle = g \left|\psi\right\rangle \quad \implies \quad g \left|\psi\right\rangle \in V_S$$

$$g^2 \left|\psi\right\rangle = I \left|\psi\right\rangle = \left|\psi\right\rangle \quad \implies \quad g \left|\psi\right\rangle = \pm \left|\psi\right\rangle \quad \implies \quad g \in S \veebar (-g) \in S$$

$$g \in S \quad \implies \quad g \left|\psi\right\rangle = \left|\psi\right\rangle \quad \implies \quad \text{Measurement yields } +1$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement
## Deterministic case

$g$ commutes with all $g_i$ and assume $g$ does not have a global phase.

$$\forall i \text{ holds: } g_i g \left|\psi\right\rangle = g g_i \left|\psi\right\rangle = g \left|\psi\right\rangle \quad \Longrightarrow \quad g \left|\psi\right\rangle \in V_S$$

$$g^2 \left|\psi\right\rangle = I \left|\psi\right\rangle = \left|\psi\right\rangle \quad \Longrightarrow \quad g \left|\psi\right\rangle = \pm \left|\psi\right\rangle \quad \Longrightarrow \quad g \in S \veebar (-g) \in S$$

$$\begin{aligned} g \in S \quad &\Longrightarrow \quad g \left|\psi\right\rangle = \left|\psi\right\rangle &&\Longrightarrow \quad \text{Measurement yields } +1 \\ (-g) \in S \quad &\Longrightarrow \quad g \left|\psi\right\rangle = - \left|\psi\right\rangle &&\Longrightarrow \quad \text{Measurement yields } -1 \end{aligned}$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement
## Deterministic case

$g$ commutes with all $g_i$ and assume $g$ does not have a global phase.

$$\forall i \text{ holds: } g_i g |\psi\rangle = g g_i |\psi\rangle = g |\psi\rangle \implies g|\psi\rangle \in V_S$$

$$g^2 |\psi\rangle = I |\psi\rangle = |\psi\rangle \implies g|\psi\rangle = \pm |\psi\rangle \implies g \in S \veebar (-g) \in S$$

$$\begin{aligned} g \in S &\implies g|\psi\rangle = |\psi\rangle &&\implies \text{Measurement yields } +1 \\ (-g) \in S &\implies g|\psi\rangle = -|\psi\rangle &&\implies \text{Measurement yields } -1 \end{aligned}$$

In both cases the measurement does not disturb the state of the system, and leaves the stabilizer invariant.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement

## Non-deterministic case preliminaries

Without loss of generality, let $g$ anti-commute with $g_1$ and $g$ does not have a global phase.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement

## Non-deterministic case preliminaries

Without loss of generality, let $g$ anti-commute with $g_1$ and $g$ does not have a global phase.

$$\forall g_j \text{ with } j \neq 1 \text{ and } g_j g = -g g_j : \text{ Replace } g_j \text{ with } g'_j = g_1 g_j$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement

## Non-deterministic case preliminaries

Without loss of generality, let $g$ anti-commute with $g_1$ and $g$ does not have a global phase.

$$\forall g_j \text{ with } j \neq 1 \text{ and } g_j g = -g g_j : \text{ Replace } g_j \text{ with } g'_j = g_1 g_j$$
$$\implies g'_j g = g_1 g_j g = -g_1 g g_j = g g_1 g_j = g g'_j$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement
## Non-deterministic case preliminaries

Without loss of generality, let $g$ anti-commute with $g_1$ and $g$ does not have a global phase.

$$\forall g_j \text{ with } j \neq 1 \text{ and } g_j g = -g g_j : \text{ Replace } g_j \text{ with } g'_j = g_1 g_j$$
$$\implies g'_j g = g_1 g_j g = -g_1 g g_j = g g_1 g_j = g g'_j$$
$$\implies g \text{ commutes with } g'_j$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement

## Non-deterministic case preliminaries

Without loss of generality, let $g$ anti-commute with $g_1$ and $g$ does not have a global phase.

$$\forall g_j \text{ with } j \neq 1 \text{ and } g_j g = -g g_j : \text{ Replace } g_j \text{ with } g_j' = g_1 g_j$$
$$\implies g_j' g = g_1 g_j g = -g_1 g g_j = g g_1 g_j = g g_j'$$
$$\implies g \text{ commutes with } g_j'$$

$\implies g$ only commutes with $g_1$.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement
## Non-deterministic case preliminaries

Without loss of generality, let $g$ anti-commute with $g_1$ and $g$ does not have a global phase.

$$\forall g_j \text{ with } j \neq 1 \text{ and } g_j g = -g g_j : \text{ Replace } g_j \text{ with } g_j' = g_1 g_j$$
$$\implies g_j' g = g_1 g_j g = -g_1 g g_j = g g_1 g_j = g g_j'$$
$$\implies g \text{ commutes with } g_j'$$

$\implies g$ only commutes with $g_1$.

Because $g$ has eigenvalues $\pm 1$, the measurement operators are: $M_{\pm g} = \frac{I \pm g}{2}$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement

## Non-deterministic case continuation

Measurement probabilities:

$$p(+1) = \text{tr}\left(\frac{I+g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) \qquad \wedge \qquad p(-1) = \text{tr}\left(\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right)$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement

## Non-deterministic case continuation

Measurement probabilities:

$$p(+1) = \text{tr}\left(\frac{I+g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) \qquad \wedge \qquad p(-1) = \text{tr}\left(\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right)$$

$$p(+1) = \text{tr}\left(\frac{I+g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right)$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement

## Non-deterministic case continuation

Measurement probabilities:

$$p(+1) = \text{tr}\left(\frac{I+g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) \qquad \wedge \qquad p(-1) = \text{tr}\left(\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right)$$

$$p(+1) = \text{tr}\left(\frac{I+g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) = \text{tr}\left(\frac{I+g}{2}g_1\left|\psi\right\rangle\left\langle\psi\right|\right)$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement
## Non-deterministic case continuation

Measurement probabilities:

$$p(+1) = \text{tr}\left(\frac{I+g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) \qquad \wedge \qquad p(-1) = \text{tr}\left(\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right)$$

$$p(+1) = \text{tr}\left(\frac{I+g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) = \text{tr}\left(\frac{I+g}{2}g_1\left|\psi\right\rangle\left\langle\psi\right|\right) = \text{tr}\left(g_1\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right)$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement

## Non-deterministic case continuation

Measurement probabilities:

$$p(+1) = \text{tr}\left(\frac{I+g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) \qquad \wedge \qquad p(-1) = \text{tr}\left(\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right)$$

$$\begin{aligned}
p(+1) &= \text{tr}\left(\frac{I+g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) = \text{tr}\left(\frac{I+g}{2}g_1\left|\psi\right\rangle\left\langle\psi\right|\right) = \text{tr}\left(g_1\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) \\
&= \text{tr}\left(\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right| g_1\right)
\end{aligned}$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement

## Non-deterministic case continuation

Measurement probabilities:

$$p(+1) = \text{tr}\left(\frac{I+g}{2} \left|\psi\right\rangle \left\langle\psi\right|\right) \qquad \wedge \qquad p(-1) = \text{tr}\left(\frac{I-g}{2} \left|\psi\right\rangle \left\langle\psi\right|\right)$$

$$\begin{aligned} p(+1) &= \text{tr}\left(\frac{I+g}{2} \left|\psi\right\rangle \left\langle\psi\right|\right) = \text{tr}\left(\frac{I+g}{2} g_1 \left|\psi\right\rangle \left\langle\psi\right|\right) = \text{tr}\left(g_1 \frac{I-g}{2} \left|\psi\right\rangle \left\langle\psi\right|\right) \\ &= \text{tr}\left(\frac{I-g}{2} \left|\psi\right\rangle \left\langle\psi\right| g_1\right) = \text{tr}\left(\frac{I-g}{2} \left|\psi\right\rangle \left\langle\psi\right| g_1^\dagger\right) \end{aligned}$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement

## Non-deterministic case continuation

Measurement probabilities:

$$p(+1) = \text{tr}\left(\frac{I+g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) \qquad \wedge \qquad p(-1) = \text{tr}\left(\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right)$$

$$\begin{aligned} p(+1) &= \text{tr}\left(\frac{I+g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) = \text{tr}\left(\frac{I+g}{2}g_1\left|\psi\right\rangle\left\langle\psi\right|\right) = \text{tr}\left(g_1\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) \\ &= \text{tr}\left(\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|g_1\right) = \text{tr}\left(\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|g_1^\dagger\right) = \text{tr}\left(\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) \end{aligned}$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement

## Non-deterministic case continuation

Measurement probabilities:

$$p(+1) = \text{tr}\left(\frac{I+g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) \qquad \wedge \qquad p(-1) = \text{tr}\left(\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right)$$

$$\begin{aligned} p(+1) &= \text{tr}\left(\frac{I+g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) = \text{tr}\left(\frac{I+g}{2}g_1\left|\psi\right\rangle\left\langle\psi\right|\right) = \text{tr}\left(g_1\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) \\ &= \text{tr}\left(\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|g_1\right) = \text{tr}\left(\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|g_1^\dagger\right) = \text{tr}\left(\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) = p(-1) \end{aligned}$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Measurement
## Non-deterministic case continuation

Measurement probabilities:

$$p(+1) = \text{tr}\left(\frac{I+g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) \qquad \wedge \qquad p(-1) = \text{tr}\left(\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right)$$

$$\begin{aligned} p(+1) &= \text{tr}\left(\frac{I+g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) = \text{tr}\left(\frac{I+g}{2}g_1\left|\psi\right\rangle\left\langle\psi\right|\right) = \text{tr}\left(g_1\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) \\ &= \text{tr}\left(\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|g_1\right) = \text{tr}\left(\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|g_1^\dagger\right) = \text{tr}\left(\frac{I-g}{2}\left|\psi\right\rangle\left\langle\psi\right|\right) = p(-1) \end{aligned}$$

$$p(+1) = p(-1) \text{ and } p(+1) + p(-1) = 1 \quad \implies \quad p(+1) = p(-1) = \frac{1}{2}$$

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Outline

# Gottesman–Knill Theorem

Suppose a quantum computation is performed which involves only the following elements:

- State preparations in the computational basis
- Hadamard gates
- Phase gates
- Controlled-NOT gates
- Pauli gates
- Measurements of observables in the Pauli group

Together with the possibility of classical control conditioned on the outcome of such measurements. Such a computation may be efficiently simulated on a classical computer.

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010

# Stabilizer Circuit

**Mainly:**

Circuit consisting solely of $CX$, $H$, $S$ and $M$ gates.

# Stabilizer Circuit

**Mainly:**

Circuit consisting solely of $CX$, $H$, $S$ and $M$ gates.

Can actually also implement $X$, $Y$, $Z$ and $SWAP$.

# Stabilizer Circuit

**Mainly:**

Circuit consisting solely of $CX$, $H$, $S$ and $M$ gates.

Can actually also implement $X$, $Y$, $Z$ and $SWAP$.

$$Z = SS$$

# Stabilizer Circuit

**Mainly:**
Circuit consisting solely of $CX$, $H$, $S$ and $M$ gates.

Can actually also implement $X$, $Y$, $Z$ and $SWAP$.

$$Z = SS$$
$$X = HZH$$

# Stabilizer Circuit

**Mainly:**

Circuit consisting solely of $CX$, $H$, $S$ and $M$ gates.

Can actually also implement $X$, $Y$, $Z$ and $SWAP$.

$$Z = SS$$
$$X = HZH$$
$$Y = SXSSS$$

# Stabilizer Circuit

**Mainly:**

Circuit consisting solely of $CX$, $H$, $S$ and $M$ gates.

Can actually also implement $X$, $Y$, $Z$ and $SWAP$.

$$Z = SS$$
$$X = HZH$$
$$Y = SXSSS$$
$$SWAP(a,b) = CX(a,b)CX(b,a)CX(a,b)$$

# Clifford Tableau

## Structure

Basically an expanded Check Matrix.

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Clifford Tableau

## Structure

Basically an expanded Check Matrix.

$$
\left(\begin{array}{ccc|ccc|c}
x_{1,1} & \cdots & x_{1,n} & z_{1,1} & \cdots & z_{1,n} & r_1 \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
x_{n,1} & \cdots & x_{n,n} & z_{n,1} & \cdots & z_{n,n} & r_n \\
\hline
x_{(n+1),1} & \cdots & x_{(n+1),n} & z_{(n+1),1} & \cdots & z_{(n+1),n} & r_{n+1} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
x_{(2n),1} & \cdots & x_{(2n),n} & z_{(2n),1} & \cdots & z_{(2n),n} & r_{2n} \\
\hline
x_{(2n+1),1} & \cdots & x_{(2n+1),n} & z_{(2n+1),1} & \cdots & z_{(2n+1),n} & r_{2n+1}
\end{array}\right)
$$

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Clifford Tableau

## Interpretation

Developers of the following algorithm introduce additional $n$ "Destabilizer" generators, which are Pauli operators that together with the stabilizer generators generate the full Pauli group.

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Clifford Tableau

## Interpretation

Developers of the following algorithm introduce additional $n$ "Destabilizer" generators, which are Pauli operators that together with the stabilizer generators generate the full Pauli group.

- Rows $1$ to $n$ represent Destabilizers.

$$\left(\begin{array}{ccc|ccc|c}
x_{1,1} & \cdots & x_{1,n} & z_{1,1} & \cdots & z_{1,n} & r_1 \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
x_{n,1} & \cdots & x_{n,n} & z_{n,1} & \cdots & z_{n,n} & r_n \\
\hline
x_{(n+1),1} & \cdots & x_{(n+1),n} & z_{(n+1),1} & \cdots & z_{(n+1),n} & r_{n+1} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
x_{(2n),1} & \cdots & x_{(2n),n} & z_{(2n),1} & \cdots & z_{(2n),n} & r_{2n} \\
\hline
x_{(2n+1),1} & \cdots & x_{(2n+1),n} & z_{(2n+1),1} & \cdots & z_{(2n+1),n} & r_{2n+1}
\end{array}\right)$$

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Clifford Tableau
## Interpretation

Developers of the following algorithm introduce additional $n$ "Destabilizer" generators, which are Pauli operators that together with the stabilizer generators generate the full Pauli group.

- Rows $1$ to $n$ represent Destabilizers.
- Rows $n+1$ to $2n$ represent Stabilizers.

$$\left(\begin{array}{ccc|ccc|c}
x_{1,1} & \cdots & x_{1,n} & z_{1,1} & \cdots & z_{1,n} & r_1 \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
x_{n,1} & \cdots & x_{n,n} & z_{n,1} & \cdots & z_{n,n} & r_n \\
\hline
x_{(n+1),1} & \cdots & x_{(n+1),n} & z_{(n+1),1} & \cdots & z_{(n+1),n} & r_{n+1} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
x_{(2n),1} & \cdots & x_{(2n),n} & z_{(2n),1} & \cdots & z_{(2n),n} & r_{2n} \\
\hline
x_{(2n+1),1} & \cdots & x_{(2n+1),n} & z_{(2n+1),1} & \cdots & z_{(2n+1),n} & r_{2n+1}
\end{array}\right)$$

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Clifford Tableau
## Interpretation

Developers of the following algorithm introduce additional $n$ "Destabilizer" generators, which are Pauli operators that together with the stabilizer generators generate the full Pauli group.

- Rows $1$ to $n$ represent Destabilizers.
- Rows $n+1$ to $2n$ represent Stabilizers.
- Row $2n+1$ is scratch-space.

$$\left(\begin{array}{ccc|ccc|c}
x_{1,1} & \cdots & x_{1,n} & z_{1,1} & \cdots & z_{1,n} & r_1 \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
x_{n,1} & \cdots & x_{n,n} & z_{n,1} & \cdots & z_{n,n} & r_n \\
\hline
x_{(n+1),1} & \cdots & x_{(n+1),n} & z_{(n+1),1} & \cdots & z_{(n+1),n} & r_{n+1} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
x_{(2n),1} & \cdots & x_{(2n),n} & z_{(2n),1} & \cdots & z_{(2n),n} & r_{2n} \\
\hline
x_{(2n+1),1} & \cdots & x_{(2n+1),n} & z_{(2n+1),1} & \cdots & z_{(2n+1),n} & r_{2n+1}
\end{array}\right)$$

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Clifford Tableau

## Interpretation

Developers of the following algorithm introduce additional $n$ "Destabilizer" generators, which are Pauli operators that together with the stabilizer generators generate the full Pauli group.

- Rows $1$ to $n$ represent Destabilizers.
- Rows $n+1$ to $2n$ represent Stabilizers.
- Row $2n+1$ is scratch-space.
- $r_i$ of row $i$ represents the global phase, $r_i = 0$ for $+1$ and $r_i = 1$ for $-1$.

$$
\left(\begin{array}{ccc|ccc|c}
x_{1,1} & \cdots & x_{1,n} & z_{1,1} & \cdots & z_{1,n} & r_1 \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
x_{n,1} & \cdots & x_{n,n} & z_{n,1} & \cdots & z_{n,n} & r_n \\
\hline
x_{(n+1),1} & \cdots & x_{(n+1),n} & z_{(n+1),1} & \cdots & z_{(n+1),n} & r_{n+1} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
x_{(2n),1} & \cdots & x_{(2n),n} & z_{(2n),1} & \cdots & z_{(2n),n} & r_{2n} \\
\hline
x_{(2n+1),1} & \cdots & x_{(2n+1),n} & z_{(2n+1),1} & \cdots & z_{(2n+1),n} & r_{2n+1}
\end{array}\right)
$$

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Clifford Tableau
## Initial Tableau

Pauli-$Z$ gates stabilize $|0\rangle$ states and Pauli-$X$ gates destabilize $|0\rangle$ states.

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Clifford Tableau
## Initial Tableau

Pauli-$Z$ gates stabilize $|0\rangle$ states and Pauli-$X$ gates destabilize $|0\rangle$ states.

$\implies$ Tableau for $|0\rangle^{\otimes n}$ has an Identity submatrix for its first $(2n) \times (2n)$ submatrix.

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Clifford Tableau
## Initial Tableau

Pauli-$Z$ gates stabilize $|0\rangle$ states and Pauli-$X$ gates destabilize $|0\rangle$ states.

$\implies$ Tableau for $|0\rangle^{\otimes n}$ has an Identity submatrix for its first $(2n) \times (2n)$ submatrix.

$$\text{Tableau for } |00\rangle \text{ is } \left(\begin{array}{cc|cc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Clifford Tableau
## Initial Tableau

Pauli-$Z$ gates stabilize $|0\rangle$ states and Pauli-$X$ gates destabilize $|0\rangle$ states.

$\implies$ Tableau for $|0\rangle^{\otimes n}$ has an Identity submatrix for its first $(2n) \times (2n)$ submatrix.

Tableau for $|00\rangle$ is
$$\left(\begin{array}{cc|cc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

In the following slides, let $R_i$ denote the $i$-th row of the stabilizer tableau.

[1] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Hadamard Gate Algorithm

Suppose we apply a Hadamard gate to qubit $a$ of current state $|\psi\rangle$.

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Hadamard Gate Algorithm

Suppose we apply a Hadamard gate to qubit $a$ of current state $|\psi\rangle$.

$\implies$ For all stabilizers and destabilizers $R_i$ the entries $x_{i,a}$ and $z_{i,a}$ determine the entries $x'_{i,a}$ and $z'_{i,a}$ of the new stabilizers and destabilizers $R'_i$ after the Hadamard gate application in the following way:

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Hadamard Gate Algorithm

Suppose we apply a Hadamard gate to qubit $a$ of current state $|\psi\rangle$.

$\implies$ For all stabilizers and destabilizers $R_i$ the entries $x_{i,a}$ and $z_{i,a}$ determine the entries $x'_{i,a}$ and $z'_{i,a}$ of the new stabilizers and destabilizers $R'_i$ after the Hadamard gate application in the following way:

- $x_{i,a}z_{i,a} = 00 \implies P_{i,a} = I \implies P'_{i,a} = HIH^\dagger = I \implies x'_{i,a}z'_{i,a} = 00 \land r'_i = r_i$

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Hadamard Gate Algorithm

Suppose we apply a Hadamard gate to qubit $a$ of current state $|\psi\rangle$.

$\implies$ For all stabilizers and destabilizers $R_i$ the entries $x_{i,a}$ and $z_{i,a}$ determine the entries $x'_{i,a}$ and $z'_{i,a}$ of the new stabilizers and destabilizers $R'_i$ after the Hadamard gate application in the following way:

- $x_{i,a}z_{i,a} = 00 \implies P_{i,a} = I \implies P'_{i,a} = HIH^\dagger = I \implies x'_{i,a}z'_{i,a} = 00 \wedge r'_i = r_i$
- $x_{i,a}z_{i,a} = 01 \implies P_{i,a} = Z \implies P'_{i,a} = HZH^\dagger = X \implies x'_{i,a}z'_{i,a} = 10 \wedge r'_i = r_i$

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Hadamard Gate Algorithm

Suppose we apply a Hadamard gate to qubit $a$ of current state $|\psi\rangle$.

$\implies$ For all stabilizers and destabilizers $R_i$ the entries $x_{i,a}$ and $z_{i,a}$ determine the entries $x'_{i,a}$ and $z'_{i,a}$ of the new stabilizers and destabilizers $R'_i$ after the Hadamard gate application in the following way:

- $x_{i,a}z_{i,a} = 00 \implies P_{i,a} = I \implies P'_{i,a} = HIH^\dagger = I \implies x'_{i,a}z'_{i,a} = 00 \wedge r'_i = r_i$
- $x_{i,a}z_{i,a} = 01 \implies P_{i,a} = Z \implies P'_{i,a} = HZH^\dagger = X \implies x'_{i,a}z'_{i,a} = 10 \wedge r'_i = r_i$
- $x_{i,a}z_{i,a} = 10 \implies P_{i,a} = X \implies P'_{i,a} = HXH^\dagger = Z \implies x'_{i,a}z'_{i,a} = 01 \wedge r'_i = r_i$

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Hadamard Gate Algorithm

Suppose we apply a Hadamard gate to qubit $a$ of current state $|\psi\rangle$.

$\implies$ For all stabilizers and destabilizers $R_i$ the entries $x_{i,a}$ and $z_{i,a}$ determine the entries $x'_{i,a}$ and $z'_{i,a}$ of the new stabilizers and destabilizers $R'_i$ after the Hadamard gate application in the following way:

- $x_{i,a}z_{i,a} = 00 \implies P_{i,a} = I \implies P'_{i,a} = HIH^\dagger = I \implies x'_{i,a}z'_{i,a} = 00 \wedge r'_i = r_i$
- $x_{i,a}z_{i,a} = 01 \implies P_{i,a} = Z \implies P'_{i,a} = HZH^\dagger = X \implies x'_{i,a}z'_{i,a} = 10 \wedge r'_i = r_i$
- $x_{i,a}z_{i,a} = 10 \implies P_{i,a} = X \implies P'_{i,a} = HXH^\dagger = Z \implies x'_{i,a}z'_{i,a} = 01 \wedge r'_i = r_i$
- $x_{i,a}z_{i,a} = 11 \implies P_{i,a} = Y \implies P'_{i,a} = HYH^\dagger = -Y \implies x'_{i,a}z'_{i,a} = 11 \wedge r'_i = \neg r_i$

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Hadamard Gate Algorithm

Suppose we apply a Hadamard gate to qubit $a$ of current state $|\psi\rangle$.

$\implies$ For all stabilizers and destabilizers $R_i$ the entries $x_{i,a}$ and $z_{i,a}$ determine the entries $x'_{i,a}$ and $z'_{i,a}$ of the new stabilizers and destabilizers $R'_i$ after the Hadamard gate application in the following way:

- $x_{i,a}z_{i,a} = 00 \implies P_{i,a} = I \implies P'_{i,a} = HIH^\dagger = I \implies x'_{i,a}z'_{i,a} = 00 \wedge r'_i = r_i$
- $x_{i,a}z_{i,a} = 01 \implies P_{i,a} = Z \implies P'_{i,a} = HZH^\dagger = X \implies x'_{i,a}z'_{i,a} = 10 \wedge r'_i = r_i$
- $x_{i,a}z_{i,a} = 10 \implies P_{i,a} = X \implies P'_{i,a} = HXH^\dagger = Z \implies x'_{i,a}z'_{i,a} = 01 \wedge r'_i = r_i$
- $x_{i,a}z_{i,a} = 11 \implies P_{i,a} = Y \implies P'_{i,a} = HYH^\dagger = -Y \implies x'_{i,a}z'_{i,a} = 11 \wedge r'_i = \neg r_i$

**Operation summary:** $x'_{i,a} = z_{i,a} \quad \wedge \quad z'_{i,a} = x_{i,a} \quad \wedge \quad r'_i = r_i \oplus (x_{i,a} \cdot z_{i,a})$

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Phase Gate Algorithm

Suppose we apply a Phase gate to qubit $a$ of current state $|\psi\rangle$.

[1] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Phase Gate Algorithm

Suppose we apply a Phase gate to qubit $a$ of current state $|\psi\rangle$.

$\Longrightarrow$ For all stabilizers and destabilizers $R_i$ the entries $x_{i,a}$ and $z_{i,a}$ determine the entries $x'_{i,a}$ and $z'_{i,a}$ of the new stabilizers and destabilizers $R'_i$ after the Phase gate application in the following way:

[1] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Phase Gate Algorithm

Suppose we apply a Phase gate to qubit $a$ of current state $|\psi\rangle$.

$\Longrightarrow$ For all stabilizers and destabilizers $R_i$ the entries $x_{i,a}$ and $z_{i,a}$ determine the entries $x'_{i,a}$ and $z'_{i,a}$ of the new stabilizers and destabilizers $R'_i$ after the Phase gate application in the following way:

- $x_{i,a} z_{i,a} = 00 \implies P_{i,a} = I \implies P'_{i,a} = SIS^\dagger = I \implies x'_{i,a} z'_{i,a} = 00 \wedge r'_i = r_i$

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Phase Gate Algorithm

Suppose we apply a Phase gate to qubit $a$ of current state $|\psi\rangle$.

$\implies$ For all stabilizers and destabilizers $R_i$ the entries $x_{i,a}$ and $z_{i,a}$ determine the entries $x'_{i,a}$ and $z'_{i,a}$ of the new stabilizers and destabilizers $R'_i$ after the Phase gate application in the following way:

- $x_{i,a}z_{i,a} = 00 \implies P_{i,a} = I \implies P'_{i,a} = SIS^\dagger = I \implies x'_{i,a}z'_{i,a} = 00 \wedge r'_i = r_i$
- $x_{i,a}z_{i,a} = 01 \implies P_{i,a} = Z \implies P'_{i,a} = SZS^\dagger = Z \implies x'_{i,a}z'_{i,a} = 01 \wedge r'_i = r_i$

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Phase Gate Algorithm

Suppose we apply a Phase gate to qubit $a$ of current state $|\psi\rangle$.

$\implies$ For all stabilizers and destabilizers $R_i$ the entries $x_{i,a}$ and $z_{i,a}$ determine the entries $x'_{i,a}$ and $z'_{i,a}$ of the new stabilizers and destabilizers $R'_i$ after the Phase gate application in the following way:

- $x_{i,a}z_{i,a} = 00 \implies P_{i,a} = I \implies P'_{i,a} = SIS^\dagger = I \implies x'_{i,a}z'_{i,a} = 00 \wedge r'_i = r_i$
- $x_{i,a}z_{i,a} = 01 \implies P_{i,a} = Z \implies P'_{i,a} = SZS^\dagger = Z \implies x'_{i,a}z'_{i,a} = 01 \wedge r'_i = r_i$
- $x_{i,a}z_{i,a} = 10 \implies P_{i,a} = X \implies P'_{i,a} = SXS^\dagger = Y \implies x'_{i,a}z'_{i,a} = 11 \wedge r'_i = r_i$

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Phase Gate Algorithm

Suppose we apply a Phase gate to qubit $a$ of current state $|\psi\rangle$.

$\implies$ For all stabilizers and destabilizers $R_i$ the entries $x_{i,a}$ and $z_{i,a}$ determine the entries $x'_{i,a}$ and $z'_{i,a}$ of the new stabilizers and destabilizers $R'_i$ after the Phase gate application in the following way:

- $x_{i,a}z_{i,a} = 00 \implies P_{i,a} = I \implies P'_{i,a} = SIS^\dagger = I \implies x'_{i,a}z'_{i,a} = 00 \wedge r'_i = r_i$
- $x_{i,a}z_{i,a} = 01 \implies P_{i,a} = Z \implies P'_{i,a} = SZS^\dagger = Z \implies x'_{i,a}z'_{i,a} = 01 \wedge r'_i = r_i$
- $x_{i,a}z_{i,a} = 10 \implies P_{i,a} = X \implies P'_{i,a} = SXS^\dagger = Y \implies x'_{i,a}z'_{i,a} = 11 \wedge r'_i = r_i$
- $x_{i,a}z_{i,a} = 11 \implies P_{i,a} = Y \implies P'_{i,a} = SYS^\dagger = -X \implies x'_{i,a}z'_{i,a} = 10 \wedge r'_i = \neg r_i$

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Phase Gate Algorithm

Suppose we apply a Phase gate to qubit $a$ of current state $|\psi\rangle$.

$\implies$ For all stabilizers and destabilizers $R_i$ the entries $x_{i,a}$ and $z_{i,a}$ determine the entries $x'_{i,a}$ and $z'_{i,a}$ of the new stabilizers and destabilizers $R'_i$ after the Phase gate application in the following way:

- $x_{i,a}z_{i,a} = 00 \implies P_{i,a} = I \implies P'_{i,a} = SIS^\dagger = I \implies x'_{i,a}z'_{i,a} = 00 \wedge r'_i = r_i$
- $x_{i,a}z_{i,a} = 01 \implies P_{i,a} = Z \implies P'_{i,a} = SZS^\dagger = Z \implies x'_{i,a}z'_{i,a} = 01 \wedge r'_i = r_i$
- $x_{i,a}z_{i,a} = 10 \implies P_{i,a} = X \implies P'_{i,a} = SXS^\dagger = Y \implies x'_{i,a}z'_{i,a} = 11 \wedge r'_i = r_i$
- $x_{i,a}z_{i,a} = 11 \implies P_{i,a} = Y \implies P'_{i,a} = SYS^\dagger = -X \implies x'_{i,a}z'_{i,a} = 10 \wedge r'_i = \neg r_i$

**Operation summary:** $x'_{i,a} = x_{i,a} \quad \wedge \quad z'_{i,a} = x_{i,a} \oplus z_{i,a} \quad \wedge \quad r'_i = r_i \oplus (x_{i,a} \cdot z_{i,a})$

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Measurement Algorithm

## Deterministic Case

Measuring qubit $a$

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Measurement Algorithm

## Deterministic Case

Measuring qubit $a \implies$ Stabilizers have $I$ or $Z$ on $a$ and $g$ is either $-Z_a$ or $Z_a$.

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Measurement Algorithm
## Deterministic Case

Measuring qubit $a \implies$ Stabilizers have $I$ or $Z$ on $a$ and $g$ is either $-Z_a$ or $Z_a$.

Invariants: $\forall\, i \in [1, n]$ holds: $R_i$ anti-commutes with $R_{n+i}$ and commutes with all $R_{j \neq n+i}$

[1] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Measurement Algorithm

## Deterministic Case

Measuring qubit $a \implies$ Stabilizers have $I$ or $Z$ on $a$ and $g$ is either $-Z_a$ or $Z_a$.

Invariants: $\forall\, i \in [1, n]$ holds: $R_i$ anti-commutes with $R_{n+i}$ and commutes with all $R_{j \neq n+i}$

$Z_a$ anti-commutes with all $R_i$ for which $x_{i,a} = 1$.

$g$ the product of $R_{n+i}$ for such $i \longleftrightarrow$ it anti-commutes exactly with these $R_i$.

[1] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Measurement Algorithm

## Deterministic Case

Measuring qubit $a \implies$ Stabilizers have $I$ or $Z$ on $a$ and $g$ is either $-Z_a$ or $Z_a$.

Invariants: $\forall\, i \in [1, n]$ holds: $R_i$ anti-commutes with $R_{n+i}$ and commutes with all $R_{j \neq n+i}$

$Z_a$ anti-commutes with all $R_i$ for which $x_{i,a} = 1$.

$g$ the product of $R_{n+i}$ for such $i \longleftrightarrow$ it anti-commutes exactly with these $R_i$.

$$g = \prod_{i=1}^{n} (R_{n+i})^{x_{i,a}} = \pm Z_a$$

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Measurement Algorithm

## Deterministic Case

Measuring qubit $a \implies$ Stabilizers have $I$ or $Z$ on $a$ and $g$ is either $-Z_a$ or $Z_a$.
Invariants: $\forall\, i \in [1, n]$ holds: $R_i$ anti-commutes with $R_{n+i}$ and commutes with all $R_{j \neq n+i}$
$Z_a$ anti-commutes with all $R_i$ for which $x_{i,a} = 1$.
$g$ the product of $R_{n+i}$ for such $i \longleftrightarrow$ it anti-commutes exactly with these $R_i$.

$$g = \prod_{i=1}^{n} (R_{n+i})^{x_{i,a}} = \pm Z_a$$

Compute $g$ in scratch-space row $2n+1$ and extract $r_{2n+1}$:

$$r_{2n+1} = 0 \implies g = Z_a \implies \text{Measurement: } 0$$

$$r_{2n+1} = 1 \implies g = -Z_a \implies \text{Measurement: } 1$$

Measurement result is just $r_{2n+1}$.

[1] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Measurement Algorithm

## Non-deterministic Case

Measuring qubit $a$: $\implies g$ is either $-Z_a$ or $Z_a$.

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Measurement Algorithm
## Non-deterministic Case

Measuring qubit $a$: $\implies g$ is either $-Z_a$ or $Z_a$.

1. Find $p \in [n+1, 2n]$ such that $x_{p,a} = 1$.
   This $R_p$ corresponds to our previous $g_1$, which anti-commutes with $g$.

[1] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Measurement Algorithm
## Non-deterministic Case

Measuring qubit $a$: $\Longrightarrow g$ is either $-Z_a$ or $Z_a$.

1. Find $p \in [n+1, 2n]$ such that $x_{p,a} = 1$.
   This $R_p$ corresponds to our previous $g_1$, which anti-commutes with $g$.
2. Multiply $g_1$ on to all $g_j$ for which $x_{j,a} = 1$.
   This transforms all $g_j$ anti-commuting with $g$ to $g'_j$ commuting with $g$.

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Measurement Algorithm

## Non-deterministic Case

Measuring qubit $a$: $\implies g$ is either $-Z_a$ or $Z_a$.

1. Find $p \in [n+1, 2n]$ such that $x_{p,a} = 1$.
   This $R_p$ corresponds to our previous $g_1$, which anti-commutes with $g$.
2. Multiply $g_1$ on to all $g_j$ for which $x_{j,a} = 1$.
   This transforms all $g_j$ anti-commuting with $g$ to $g_j'$ commuting with $g$.
3. Push $R_p$ onto $R_{p-n}$.
   After measurement, the stabilizer anti-commuting with $g$ becomes a destabilizer.

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Measurement Algorithm

## Non-deterministic Case

Measuring qubit $a$: $\Longrightarrow g$ is either $-Z_a$ or $Z_a$.

1. Find $p \in [n+1, 2n]$ such that $x_{p,a} = 1$.
   This $R_p$ corresponds to our previous $g_1$, which anti-commutes with $g$.
2. Multiply $g_1$ on to all $g_j$ for which $x_{j,a} = 1$.
   This transforms all $g_j$ anti-commuting with $g$ to $g_j'$ commuting with $g$.
3. Push $R_p$ onto $R_{p-n}$.
   After measurement, the stabilizer anti-commuting with $g$ becomes a destabilizer.
4. Assign $R_p = g$, either $Z_a$ or $-Z_a$ with equal probability.
   Retrieve the measurement result from $r_p$ like before.

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004)

# Advantages

Simulation of stabilizer circuit runs
in polynomial $O\left(n^2\right)$ time complexity.

Measurement and state update during simulation run
in polynomial $O\left(n^2\right)$ time complexity.

# References

[1] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* (2004).

[2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.