

Clifford Tableaus and the Stabilizer Algorithm

Leonard Uscinowicz

Technical University of Munich

December 20th, 2024



Outline



- Preliminary Definitions
- Stabilizer Formalism
- Stabilizer Algorithm

Pauli Matrices



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

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* 70.5 (2004), p. 052328



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



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

Properties:

■ Closure: $\forall g_1, g_2 \in G \Longrightarrow g_1 \cdot g_2 \in G$



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

Properties:

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



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

Properties:

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



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

Properties:

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



 \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 ± 1 or $\pm i$.

[1] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". In: *Physical Review A—Atomic, Molecular, and Optical Physics* 70.5 (2004), p. 052328



 \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 ± 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* 70.5 (2004), p. 052328



 \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 ± 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* 70.5 (2004), p. 052328



 \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 ± 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* 70.5 (2004), p. 052328

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:

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

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* 70.5 (2004), p. 052328

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:

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

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 ${\cal G}$ can be written in terms of its generators:

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

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

Outline



- Preliminary Definitions
- Stabilizer Formalism
- Stabilizer Algorithm

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.

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

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.
- $S \cong$ Subgroup of the Pauli Group \mathcal{P}_n : $S \subseteq \mathcal{P}_n$.
- $V_S =$ Set of n-qubit states stabilized by S:

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



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



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

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



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

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

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



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

Conditions for S such that V_S not trivial:

Commutativity: $\forall g_1, g_2 \in S$ holds: $g_1g_2 = g_2g_1$



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

Conditions for S such that V_S not trivial:

- **Commutativity:** $\forall g_1, g_2 \in S$ holds: $g_1g_2 = g_2g_1$
- 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
Leonard Uscinowicz | Clifford Tableaus and the Stabilizer Algorithm | 20/12/2024



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



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.



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.



Let V_S be non-trivial and let $q_1, q_2 \in S$.

- \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:

$$|\psi\rangle=g_1g_2\,|\psi\rangle=-g_2g_1\,|\psi\rangle=-\,|\psi\rangle\quad\Longleftrightarrow\quad |\psi\rangle=\vec{0}\quad\Longrightarrow\quad V_S \ \text{is trivial}.$$

Stabilizer Conditions



Commutativity Proof

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

- $\Longrightarrow g_1$ 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:

$$|\psi\rangle=g_1g_2\,|\psi\rangle=-g_2g_1\,|\psi\rangle=-\,|\psi\rangle\quad\Longleftrightarrow\quad |\psi\rangle=\vec{0}\quad\Longrightarrow\quad V_S \ \text{is trivial}.$$

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

Stabilizer Conditions



Commutativity Proof

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

- $\Longrightarrow g_1$ 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:

$$|\psi\rangle=g_1g_2\,|\psi\rangle=-g_2g_1\,|\psi\rangle=-\,|\psi\rangle\quad\Longleftrightarrow\quad |\psi\rangle=\vec{0}\quad\Longrightarrow\quad V_S \ \text{is trivial}.$$

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

Stabilizer ConditionsStrict Identity Proof



Let V_S be non-trivial.

Stabilizer Conditions Strict Identity Proof



Let V_S be non-trivial.

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

Stabilizer Conditions Strict Identity Proof



Let V_S be non-trivial.

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

Check MatrixStructure



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

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

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 .

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 .



Row *i* corresponds to generator $q_i \in S$.



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



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



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



- Row *i* corresponds to generator $g_i \in S$.
- Left $l \times n$ submatrix contains 1s to indicate which generators contain Xs.
- Right $l \times n$ submatrix contains 1s to indicate which generators contain Zs.
- \blacksquare 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^{th} qubit $\Longrightarrow h_{i,j} = 0$ and $h_{i,n+j} = 0$.



- Row *i* corresponds to generator $g_i \in S$.
- Left $l \times n$ submatrix contains 1s to indicate which generators contain Xs.
- Right $l \times n$ submatrix contains 1s to indicate which generators contain Zs.
- \blacksquare 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^{th} qubit $\Longrightarrow h_{i,j} = 0$ and $h_{i,n+j} = 0$.
- If g_i contains X on the j^{th} qubit $\Longrightarrow h_{i,j} = 1$ and $h_{i,n+j} = 0$.



- Row *i* corresponds to generator $g_i \in S$.
- Left $l \times n$ submatrix contains 1s to indicate which generators contain Xs.
- Right $l \times n$ submatrix contains 1s to indicate which generators contain Zs.
- \blacksquare 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^{th} qubit $\Longrightarrow h_{i,j} = 0$ and $h_{i,n+j} = 0$.
- If g_i contains X on the j^{th} qubit $\Longrightarrow h_{i,j} = 1$ and $h_{i,n+j} = 0$.
- If g_i contains Z on the j^{th} qubit $\Longrightarrow h_{i,j} = 0$ and $h_{i,n+j} = 1$.



- Row *i* corresponds to generator $g_i \in S$.
- Left $l \times n$ submatrix contains 1s to indicate which generators contain Xs.
- Right $l \times n$ submatrix contains 1s to indicate which generators contain Zs.
- \blacksquare 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 jth qubit $\Longrightarrow h_{i,j} = 0$ and $h_{i,n+j} = 0$.
- If g_i contains X on the j^{th} qubit $\Longrightarrow h_{i,j} = 1$ and $h_{i,n+j} = 0$.
- If g_i contains Z on the j^{th} qubit $\Longrightarrow h_{i,j} = 0$ and $h_{i,n+j} = 1$.
- If g_i contains Y on the j^{th} qubit $\Longrightarrow h_{i,j} = 1$ and $h_{i,n+j} = 1$.

Check Matrix Example Steane Code



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

Γ0	0	0	1	1	1	1	0	0	0	0	0	0	07
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	$1 \rfloor$

	Generator	Operator			
	g_1	IIIXXXX			
<u></u>	g_2	IXXIIXX			
	g_3	XIXIXIX			
	g_4	IIIZZZZ			
	g_5	IZZIIZZ			
	g_6	ZIZIZIZ			



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



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

$$U |\psi\rangle = Ug |\psi\rangle = UgI |\psi\rangle = UgU^{\dagger}U |\psi\rangle = (UgU^{\dagger}) U |\psi\rangle$$



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

$$U |\psi\rangle = Ug |\psi\rangle = UgI |\psi\rangle = UgU^{\dagger}U |\psi\rangle = (UgU^{\dagger}) U |\psi\rangle$$

 \Longrightarrow State $U | \psi \rangle$ is stabilized by UgU^{\dagger} .



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

$$U |\psi\rangle = Ug |\psi\rangle = UgI |\psi\rangle = UgU^{\dagger}U |\psi\rangle = (UgU^{\dagger}) U |\psi\rangle$$

 \Longrightarrow State $U | \psi \rangle$ is stabilized by UgU^{\dagger} .

⇒ 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.



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



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

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



For certain special unitary operations ${\cal U}$ 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.



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

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

Example:

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

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



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

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

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
	X_1	X_1X_2
CX	X_2	X_2
	Z_1	Z_1
	Z_2	Z_1Z_2
Н	X	Z
	Z	X
S	X	Y
) 3	Z	Z

Operation	Input	Output
X	X	X
Λ	Z	-Z
V	X	-X
1	Z	-Z
Z	X	-X
Z	Z	Z



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



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. q commutes with all generators of the stabilizer.



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.
 - ⇒ Measurement outcome is deterministic.



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.
 - ⇒ Measurement outcome is deterministic.
- 2. *g* anti-commutes with at least 1 generator of the stabilizer.



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.
 - ⇒ Measurement outcome is deterministic.
- 2. *g* anti-commutes with at least 1 generator of the stabilizer.
 - ⇒ Measurement outcome is not deterministic.



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



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

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

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



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

$$\forall i \text{ holds: } g_ig \, |\psi\rangle = gg_i \, |\psi\rangle = g \, |\psi\rangle \quad \Longrightarrow \quad g \, |\psi\rangle \in V_S$$

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

$$g \in S \quad \Longrightarrow \quad g \, |\psi\rangle = |\psi\rangle \qquad \Longrightarrow \quad \text{Measurement yields } +1$$



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

$$\forall i \text{ holds: } g_ig \ |\psi\rangle = gg_i \ |\psi\rangle = g \ |\psi\rangle \qquad \Longrightarrow \qquad g \ |\psi\rangle \in V_S$$

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

$$g \in S \qquad \Longrightarrow \qquad g \ |\psi\rangle = |\psi\rangle \qquad \Longrightarrow \qquad \text{Measurement yields} \qquad +1$$

$$(-g) \in S \qquad \Longrightarrow \qquad g \ |\psi\rangle = -\ |\psi\rangle \qquad \Longrightarrow \qquad \text{Measurement yields} \qquad -1$$



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

$$\forall i \text{ holds: } g_ig \ |\psi\rangle = gg_i \ |\psi\rangle = g \ |\psi\rangle \quad \Longrightarrow \quad g \ |\psi\rangle \in V_S$$

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

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

$$(-g) \in S \quad \Longrightarrow \quad g \ |\psi\rangle = - \ |\psi\rangle \quad \Longrightarrow \quad \text{Measurement yields} \quad -1$$

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

MeasurementNon-deterministic case preliminaries



Without loss of generality, let q anti-commute with q_1 and q does not have a global phase.

MeasurementNon-deterministic case preliminaries



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

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

MeasurementNon-deterministic case preliminaries



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

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

$$\implies g_j' g = g_1 g_j g = -g_1 g g_j = g g_1 g_j = g g_j'$$

MeasurementNon-deterministic case preliminaries



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

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

$$\implies g_j' g = g_1 g_j g = -g_1 g g_j = g g_1 g_j = g g_j'$$

$$\implies g \text{ commutes with } g_j'$$

Measurement Non-deterministic case preliminaries



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

$$orall g_j$$
 with $j
eq 1$ and $g_j g = -g g_j$: Replace g_j with $g_j' = g_1 g_j$
$$\Longrightarrow g_j' g = g_1 g_j g = -g_1 g g_j = g g_1 g_j = g g_j'$$

$$\Longrightarrow g \text{ commutes with } g_j'$$

 $\Longrightarrow g$ only commutes with g_1 .

MeasurementNon-deterministic case preliminaries



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

$$orall g_j$$
 with $j
eq 1$ and $g_j g = -g g_j$: Replace g_j with $g_j' = g_1 g_j$
$$\Longrightarrow g_j' g = g_1 g_j g = -g_1 g g_j = g g_1 g_j = g g_j'$$

$$\Longrightarrow g \text{ commutes with } g_j'$$

 $\Longrightarrow g$ only commutes with g_1 .

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

Measurement Non-deterministic case continuation



Measurement probabilities:

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



Non-deterministic case continuation

Measurement probabilities:

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

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



Non-deterministic case continuation

Measurement probabilities:

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

Measurement Non-deterministic case continuation



Measurement probabilities:

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



Non-deterministic case continuation

Measurement probabilities:

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

Non-deterministic case continuation



Measurement probabilities:

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



Non-deterministic case continuation

Measurement probabilities:

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



Non-deterministic case continuation

Measurement probabilities:

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



Non-deterministic case continuation

Measurement probabilities:

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

Outline



- Preliminary Definitions
- Stabilizer Formalism
- Stabilizer Algorithm

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.



Mainly:

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



Mainly:

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



Mainly:

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

$$Z = SS$$



Mainly:

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

$$Z = SS$$

$$X=HZH$$



Mainly:

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

$$Z = SS$$

$$X = HZH$$

$$Y = SXSSS$$



Mainly:

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

$$Z = SS$$

$$X = HZH$$

$$Y = SXSSS$$

$$SWAP(a, b) = CX(a, b)CX(b, a)CX(a, b)$$

Clifford Tableau Structure



Basically an expanded Check Matrix.

Clifford Tableau



Structure

Basically an expanded Check Matrix.



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.



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.

 \blacksquare Rows 1 to n represent Destabilizers.

			-				
1	$x_{1,1}$		$x_{1,n}$	$z_{1,1}$		$z_{1,n}$	$ r_1 \rangle$
	i	٠	:	:	٠.,	÷	:
	$x_{n,1}$		$x_{n,n}$	$z_{n,1}$		$z_{n,n}$	r_n
	$x_{(n+1),1}$		$x_{(n+1),n}$	$z_{(n+1),1}$		$z_{(n+1),n}$	r_{n+1}
	:	٠	:	:	٠	:	;
	$x_{(2n),1}$		$x_{(2n),n}$	$z_{(2n),1}$		$z_{(2n),n}$	r_{2n}
	$x_{(2n+1),1}$		$x_{(2n+1),n}$	$z_{(2n+1),1}$		$z_{(2n+1),n}$	r_{2n+1}



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.

- \blacksquare Rows 1 to n represent Destabilizers.
- Rows n+1 to 2n represent Stabilizers.

	•		•				•
($x_{1,1}$		$x_{1,n}$	$z_{1,1}$		$z_{1,n}$	$ r_1 \rangle$
	÷	٠.,	:	:	٠.,	÷	:
	$x_{n,1}$		$x_{n,n}$	$z_{n,1}$		$z_{n,n}$	r_n
	$x_{(n+1),1}$		$x_{(n+1),n}$	$z_{(n+1),1}$		$z_{(n+1),n}$	r_{n+1}
	:	٠.,	:	:	٠.,	÷	;
	$x_{(2n),1}$		$x_{(2n),n}$	$z_{(2n),1}$		$z_{(2n),n}$	r_{2n}
	$x_{(2n+1),1}$		$x_{(2n+1),n}$	$z_{(2n+1),1}$		$z_{(2n+1),n}$	r_{2n+1}



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.

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

	3		- 3				5 - 1
($x_{1,1}$		$x_{1,n}$	$z_{1,1}$		$z_{1,n}$	$ r_1 \rangle$
	:	٠.	÷	:	٠.,	÷	:
	$x_{n,1}$		$x_{n,n}$	$z_{n,1}$		$z_{n,n}$	r_n
	$x_{(n+1),1}$		$x_{(n+1),n}$	$z_{(n+1),1}$		$z_{(n+1),n}$	r_{n+1}
	:	٠.	:	:	٠.	:	:
	$x_{(2n),1}$		$x_{(2n),n}$	$z_{(2n),1}$		$z_{(2n),n}$	r_{2n}
	$x_{(2n+1),1}$		$x_{(2n+1),n}$	$z_{(2n+1),1}$		$z_{(2n+1),n}$	r_{2n+1}



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.

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

,	3		3				0 1-
($x_{1,1}$		$x_{1,n}$	$z_{1,1}$		$z_{1,n}$	$ r_1 \rangle$
	i	٠	:	:	٠.,	÷	:
	$x_{n,1}$		$x_{n,n}$	$z_{n,1}$		$z_{n,n}$	r_n
	$x_{(n+1),1}$		$x_{(n+1),n}$	$z_{(n+1),1}$		$z_{(n+1),n}$	r_{n+1}
	÷	٠	:	:	٠	÷	:
	$x_{(2n),1}$		$x_{(2n),n}$	$z_{(2n),1}$		$z_{(2n),n}$	r_{2n}
	$x_{(2n+1),1}$		$x_{(2n+1),n}$	$z_{(2n+1),1}$	• • •	$z_{(2n+1),n} \\$	r_{2n+1}

Clifford Tableau Initial Tableau



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

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.

Clifford Tableau Initial Tableau



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

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

Tableau for
$$|00\rangle$$
 is
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

References



- [1] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". In: *Physical Review A—Atomic, Molecular, and Optical Physics* 70.5 (2004), p. 052328.
- [2] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.