Winter School on Quantum Information Science (Jan 10-21, 2022)

Quantum Error-Correction Codes II

1. Stabilizer Formalism
2. Stabilizer Codes
3. Surface Codes

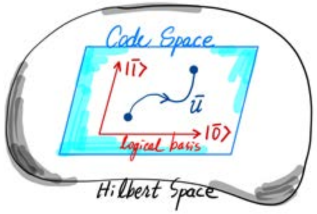
Mahn-Soo Choi (Korea University)

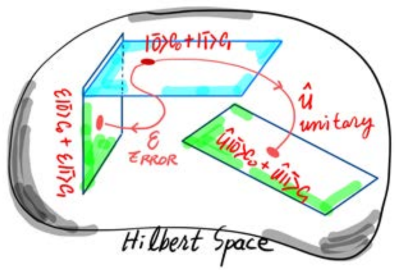
January 20, 2022 (v1.4)

Quantum Error-Correction Codes

A Geometrical View

Code Geometry





Example: Bit-Flip Code I

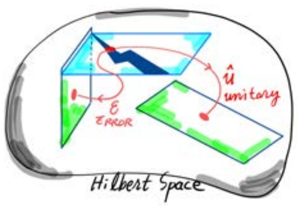
- The code space
$$\mathcal{V} = \mathrm{Span}\{|\bar{0}\rangle := |000\rangle, |\bar{1}\rangle := |111\rangle\}$$
- Consider a logical quantum state
$$|\psi\rangle = |000\rangle c_0 + |111\rangle c_1$$
- When the first qubit is flipped ($\hat{E} = \hat{X} \otimes \hat{I} \otimes \hat{I}$),
$$|\psi'\rangle = |100\rangle c_0 + |011\rangle c_1.$$
Note that $\langle\psi'|\psi\rangle = 0$ for any $c_0, c_1 \in \mathbb{C}$.

Example: Bit-Flip Code II

- What if
$$\hat{E} = \alpha \hat{X} \otimes \hat{I} \otimes \hat{I} + \beta \hat{I} \otimes \hat{X} \otimes \hat{I} \quad (\alpha, \beta \in \mathbb{C})?$$
Then,
$$|\psi''\rangle = \alpha\left(|100\rangle c_0 + |011\rangle c_1\right) + \beta\left(|010\rangle c_0 + |101\rangle c_1\right)$$
Note that still $\langle\psi''|\psi\rangle = 0$.
- How do we detect and correct the error?
- Diagnose the syndrome of $\hat{Z} \otimes \hat{I} \otimes \hat{Z}$.
$$\begin{cases} -1, & |100\rangle c_0 + |011\rangle c_1\,, \quad \text{with } P = |\alpha|^2 \\ +1, & |010\rangle c_0 + |101\rangle c_1\,, \quad \text{with } P = |\beta|^2 \end{cases}$$
Whatever the syndrome is, the error is corrected!

Collective vs Sequential Measurements

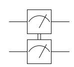
Not too much or less information!



Collective vs Sequential Measurements

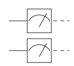
- Collective measurement

$\hat{Z} \otimes \hat{Z}$:



- Sequential measurement

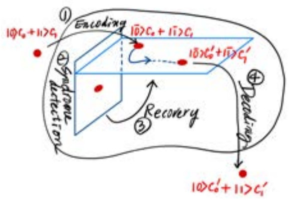
$\hat{Z} \otimes \hat{I}$ followed by $\hat{I} \otimes \hat{Z}$:



$$|000\rangle c_0 + |111\rangle c_1 \xrightarrow{\text{error}} |100\rangle c_0 + |011\rangle c_1 \xrightarrow{\text{measurement } \hat{Z}_1} |100\rangle \xrightarrow{\text{measurement } \hat{Z}_2} |100\rangle$$

Quantum Error-Correction Procedure

1. Encoding
2. Syndrome detection
3. Recovery
4. Decoding



Winter School on Quantum Information Science (Jan 10-21, 2022)

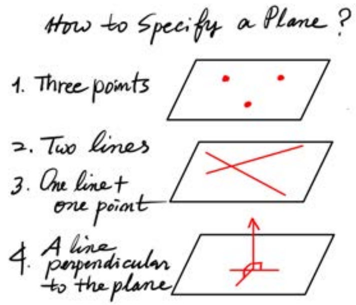
Stabilizer Formalism

Mahn-Soo Choi (Korea University)

January 20, 2022 (v1.4)

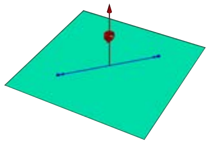
A Strange Way to Describe Code Space and Codewords

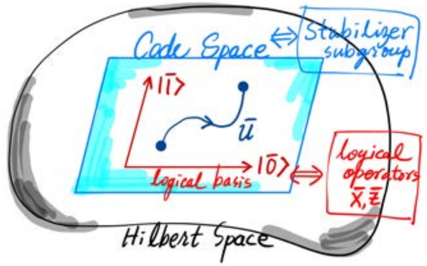
Using groups and operators



How about This Method ...
... To specify the *xy*-plane?

"The plane invariant under all ortations around the z-axis and the spatial inversion about the origin."





Why Stabilizers?
(partially personal)

- Extensibility
- Surface codes (a more general and wider class of codes)
- Topological quantum computation
- Other methods are boring (to me).

Key Moments
in the history of stabilizer codes

- Gottesman, Phys. Rev. A (1996) & Gottesman, Phys. Rev. A (1998): Stabilizer codes
- Kitaev, Ann. Phys. (2003) = quant-ph/9707021: Topological quantum computation
- Freedman, Foundations of Computational Mathematics (2001) & Dennis et al., Journal of Mathematical Physics (2002): Surface codes

Overview

1. What is stabilizer?
2. The Pauli and Clifford groups
3. Properties of stabilizers in the Pauli group
4. Unitary gates in stabilizer formalism
5. Measurements in stabilizer formalism
6. Examples

What is stabilizer?

What is group?

A group is a set $\mathcal{G}$ with an algebraic structure determined by the "multiplication".

- For any $G_1, G_2 \in \mathcal{G}$, $G_1 G_2 \in \mathcal{G}$. (In general, $G_1 G_2 \neq G_2 G_1$.)
- There exists $I \in \mathcal{G}$ such that $IG = GI = G$ for all $G \in \mathcal{G}$.
- For each $G \in \mathcal{G}$, there exists $G^{-1} \in \mathcal{G}$ such that $GG^{-1} = G^{-1}G = I$.
- For any $G_1, G_2, G_3 \in \mathcal{G}$, $(G_1 G_2) G_3 = G_1 (G_2 G_3)$.

vector space	$\leftrightarrow$	linear superposition
group	$\leftrightarrow$	multiplication (and division)

$$\mathcal{G} = \{\pm\hat{I}, \pm i\hat{I}, \pm\hat{X}, \pm i\hat{X}, \pm\hat{Y}, \pm i\hat{Y}, \pm\hat{Z}, \pm i\hat{Z}\}$$

	$\hat{I}$	$\hat{X}$	$\hat{Y}$	$\hat{Z}$	$-\hat{I}$	$-\hat{X}$	$-\hat{Y}$	$-\hat{Z}$	$i\hat{I}$	$i\hat{X}$	$i\hat{Y}$	$i\hat{Z}$	$-i\hat{I}$	$-i\hat{X}$	$-i\hat{Y}$	$-i\hat{Z}$
$\hat{I}$	$\hat{I}$	$\hat{X}$	$\hat{Y}$	$\hat{Z}$	$-\hat{I}$	$-\hat{X}$	$-\hat{Y}$	$-\hat{Z}$	$i\hat{I}$	$i\hat{X}$	$i\hat{Y}$	$i\hat{Z}$	$-i\hat{I}$	$-i\hat{X}$	$-i\hat{Y}$	$-i\hat{Z}$
$\hat{X}$	$\hat{X}$	$\hat{I}$	$i\hat{Z}$	$-i\hat{Y}$	$-\hat{X}$	$-\hat{I}$	$-i\hat{Z}$	$i\hat{Y}$	$i\hat{X}$	$i\hat{I}$	$-\hat{Z}$	$\hat{Y}$	$-i\hat{X}$	$-i\hat{I}$	$\hat{Z}$	$-\hat{Y}$
$\hat{Y}$	$\hat{Y}$	$-i\hat{Z}$	$\hat{I}$	$i\hat{X}$	$-\hat{Y}$	$i\hat{Z}$	$-\hat{I}$	$-i\hat{X}$	$i\hat{Y}$	$\hat{Z}$	$i\hat{I}$	$-\hat{X}$	$-i\hat{Y}$	$-\hat{Z}$	$-i\hat{I}$	$\hat{X}$
$\hat{Z}$	$\hat{Z}$	$i\hat{Y}$	$-i\hat{X}$	$\hat{I}$	$-\hat{Z}$	$-i\hat{Y}$	$i\hat{X}$	$-\hat{I}$	$i\hat{Z}$	$-\hat{Y}$	$\hat{X}$	$i\hat{I}$	$-i\hat{Z}$	$\hat{Y}$	$-\hat{X}$	$-i\hat{I}$
$-\hat{I}$	$-\hat{I}$	$-\hat{X}$	$-\hat{Y}$	$-\hat{Z}$	$\hat{I}$	$\hat{X}$	$\hat{Y}$	$\hat{Z}$	$-i\hat{I}$	$-i\hat{X}$	$-i\hat{Y}$	$-i\hat{Z}$	$i\hat{I}$	$i\hat{X}$	$i\hat{Y}$	$i\hat{Z}$
$-\hat{X}$	$-\hat{X}$	$-\hat{I}$	$-i\hat{Z}$	$i\hat{Y}$	$\hat{X}$	$\hat{I}$	$i\hat{Z}$	$-i\hat{Y}$	$-i\hat{X}$	$-i\hat{I}$	$\hat{Z}$	$-\hat{Y}$	$i\hat{X}$	$i\hat{I}$	$-\hat{Z}$	$\hat{Y}$
$-\hat{Y}$	$-\hat{Y}$	$i\hat{Z}$	$-\hat{I}$	$-i\hat{X}$	$\hat{Y}$	$-i\hat{Z}$	$\hat{I}$	$i\hat{X}$	$-i\hat{Y}$	$-\hat{Z}$	$-i\hat{I}$	$\hat{X}$	$i\hat{Y}$	$\hat{Z}$	$i\hat{I}$	$-\hat{X}$
$-\hat{Z}$	$-\hat{Z}$	$-i\hat{Y}$	$i\hat{X}$	$-\hat{I}$	$\hat{Z}$	$i\hat{Y}$	$-i\hat{X}$	$\hat{I}$	$-i\hat{Z}$	$\hat{Y}$	$-\hat{X}$	$-i\hat{I}$	$i\hat{Z}$	$-\hat{Y}$	$\hat{X}$	$i\hat{I}$
$i\hat{I}$	$i\hat{I}$	$i\hat{X}$	$i\hat{Y}$	$i\hat{Z}$	$-i\hat{I}$	$-i\hat{X}$	$-i\hat{Y}$	$-i\hat{Z}$	$-\hat{I}$	$-\hat{X}$	$-\hat{Y}$	$-\hat{Z}$	$\hat{I}$	$\hat{X}$	$\hat{Y}$	$\hat{Z}$
$i\hat{X}$	$i\hat{X}$	$i\hat{I}$	$-\hat{Z}$	$\hat{Y}$	$-i\hat{X}$	$-i\hat{I}$	$\hat{Z}$	$-\hat{Y}$	$-\hat{X}$	$-\hat{I}$	$-i\hat{Z}$	$i\hat{Y}$	$\hat{X}$	$\hat{I}$	$i\hat{Z}$	$-i\hat{Y}$
$i\hat{Y}$	$i\hat{Y}$	$\hat{Z}$	$i\hat{I}$	$-\hat{X}$	$-i\hat{Y}$	$-\hat{Z}$	$-i\hat{I}$	$\hat{X}$	$-\hat{Y}$	$i\hat{Z}$	$-\hat{I}$	$-i\hat{X}$	$\hat{Y}$	$-i\hat{Z}$	$\hat{I}$	$i\hat{X}$
$i\hat{Z}$	$i\hat{Z}$	$-\hat{Y}$	$\hat{X}$	$i\hat{I}$	$-i\hat{Z}$	$\hat{Y}$	$-\hat{X}$	$-i\hat{I}$	$-\hat{Z}$	$-i\hat{Y}$	$i\hat{X}$	$-\hat{I}$	$\hat{Z}$	$i\hat{Y}$	$-i\hat{X}$	$\hat{I}$
$-i\hat{I}$	$-i\hat{I}$	$-i\hat{X}$	$-i\hat{Y}$	$-i\hat{Z}$	$i\hat{I}$	$i\hat{X}$	$i\hat{Y}$	$i\hat{Z}$	$\hat{I}$	$\hat{X}$	$\hat{Y}$	$\hat{Z}$	$-\hat{I}$	$-\hat{X}$	$-\hat{Y}$	$-\hat{Z}$
$-i\hat{X}$	$-i\hat{X}$	$-i\hat{I}$	$\hat{Z}$	$-\hat{Y}$	$i\hat{X}$	$i\hat{I}$	$-\hat{Z}$	$\hat{Y}$	$\hat{X}$	$\hat{I}$	$i\hat{Z}$	$-i\hat{Y}$	$-\hat{X}$	$-\hat{I}$	$-i\hat{Z}$	$i\hat{Y}$
$-i\hat{Y}$	$-i\hat{Y}$	$-\hat{Z}$	$-i\hat{I}$	$\hat{X}$	$i\hat{Y}$	$\hat{Z}$	$i\hat{I}$	$-\hat{X}$	$\hat{Y}$	$-i\hat{Z}$	$\hat{I}$	$i\hat{X}$	$-\hat{Y}$	$i\hat{Z}$	$-\hat{I}$	$-i\hat{X}$
$-i\hat{Z}$	$-i\hat{Z}$	$\hat{Y}$	$-\hat{X}$	$-i\hat{I}$	$i\hat{Z}$	$-\hat{Y}$	$\hat{X}$	$i\hat{I}$	$\hat{Z}$	$i\hat{Y}$	$-i\hat{X}$	$\hat{I}$	$-\hat{Z}$	$-i\hat{Y}$	$i\hat{X}$	$-\hat{I}$

Group Generators
cf. "basis" for vector space

$$\mathcal{G} = \mathrm{Gen}\{G_1, G_2, \cdots, G_k\}$$

Example: The single-qubit Pauli group

$$\mathcal{G} = \{\pm\hat{I}, \pm i\hat{I}, \pm\hat{X}, \pm i\hat{X}, \pm\hat{Y}, \pm i\hat{Y}, \pm\hat{Z}, \pm i\hat{Z}\}$$

is generated by $\hat{X}, \hat{Y}, \hat{Z}$; and hence

$$\mathcal{G} = \mathrm{Gen}\{\hat{X}, \hat{Y}, \hat{Z}\}.$$

Stabilizer Subgroup (Stabilizer)
Stabilizer of a Single State

- Let $|\psi\rangle \in \mathcal{V}$ be a quantum state.
- An operator $\hat{G}$ is said to stabilize $|\psi\rangle$ if
$$\hat{G}|\psi\rangle = |\psi\rangle.$$
$|\psi\rangle$ is said to be stabilized by $\hat{G}$.
- The set of operators $\hat{G}$ stabilizing a quantum state $|\psi\rangle$ forms a subgroup $\mathcal{S}$.
- $\mathcal{S}$ is called the *stabilizer subgroup* (or *stabilizer* for short) of $|\psi\rangle$.

Example

$$|\Phi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

- $\hat{X} \otimes \hat{X}$ stabilizes $|\Phi\rangle$.
- $\hat{Z} \otimes \hat{Z}$ stabilizes $|\Phi\rangle$.
- The stabilizer subgroup of $|\Phi\rangle$ is
$$\mathcal{S} = \{\hat{I} \otimes \hat{I},\ \hat{X} \otimes \hat{X},\ \hat{Z} \otimes \hat{Z},\ -\hat{Y} \otimes \hat{Y}\}$$
Or, equivalently,
$$\mathcal{S} = \mathrm{Gen}\{\hat{X} \otimes \hat{X}, \hat{Z} \otimes \hat{Z}\}$$

Stabilizer Subgroup (Stabilizer)
Stabilizer of a Subspace

- Let $\mathcal{V}$ be a subspace of the Hilbert space of concern.
- A subgroup $\mathcal{S} \subset \mathcal{G}$ is called a *stabilizer subgroup* of $\mathcal{V}$ if
$$\hat{S}|\psi\rangle = |\psi\rangle, \quad \forall\hat{S} \in \mathcal{S}, \forall|\psi\rangle \in \mathcal{V}.$$
$\mathcal{V}$ is said to be stabilized by $\mathcal{S}$.

* Not to be confused with an *invariant subspace*:
$$\hat{S}|\psi\rangle \in \mathcal{V}, \quad \forall\hat{S} \in \mathcal{S}, \forall|\psi\rangle \in \mathcal{V}.$$
That is, $\hat{S}|\psi\rangle \neq |\psi\rangle$ and yet $\hat{S}|\psi\rangle \in \mathcal{V}$.

Example

Bit-Flip Code

$$\mathcal{V} = \mathrm{Span}\left\{|000\rangle, |111\rangle\right\}$$

- $\hat{Z} \otimes \hat{Z} \otimes \hat{I}$ stabilizes $\mathcal{V}$.
- $\hat{I} \otimes \hat{Z} \otimes \hat{Z}$ stabilizes $\mathcal{V}$.
- The stabilizer subgroup $\mathcal{S}$ of $\mathcal{V}$ is given by

$$\mathcal{S} = \{\hat{I} \otimes \hat{I} \otimes \hat{I},\ \hat{Z} \otimes \hat{Z} \otimes \hat{I},\ \hat{I} \otimes \hat{Z} \otimes \hat{Z},\ \hat{Z} \otimes \hat{I} \otimes \hat{Z}\}.$$

Or, equivalently,

$$\mathcal{S} = \mathrm{Gen}\{\hat{Z} \otimes \hat{Z} \otimes \hat{I}, \hat{I} \otimes \hat{Z} \otimes \hat{Z}\}$$

How to find the stabilizer of a given quantum state?

- In unitary group $U(d)$, relatively easy!
- In $U(d) \otimes U(d) \otimes \cdots \otimes U(d)$, not easy in general.
- In the Pauli group, quite easy!

Stabilizer Formalism: Overview

What can you do with stabilizers?

Unitary Gates in Stabilizer Formalism

- In the usual Schrödinger picture,

$$|\psi\rangle \mapsto |\psi'\rangle = \hat{U}|\psi\rangle.$$

- In the stabilizer formalism?
  - In general, $\mathcal{S}$ of $|\psi\rangle$ cannot stabilize $|\psi'\rangle$ any longer.
  - How can you find $\mathcal{S}'$ of $|\psi'\rangle$?

$$\hat{G}|\psi\rangle = |\psi\rangle, \quad \hat{U}\hat{G}|\psi\rangle = \hat{U}|\psi\rangle, \quad \hat{U}\hat{G}\hat{U}^\dagger\hat{U}|\psi\rangle = \hat{U}|\psi\rangle$$
$$\mathcal{S}' = \hat{U}\mathcal{S}\hat{U}^\dagger.$$

Verdict:

- Relatively easy once the inital $\mathcal{S}$ is known.
- In general, however, **highly ineffective** since one has to keep track of **operators** in the stabilizers.

Measurements in Stabilizer Formalism

- Consider a projection measurement of an observable $\hat{M}$.
- In the usual Schrödinger picture, the post-measurement state is given by

$$|\psi\rangle \mapsto |\psi'\rangle = \hat{P}_m |\psi\rangle ,$$

where $\hat{P}_m$ is the projection onto the eigenspace belonging to the measurement outcome m.

Verdict:

- In general, it is not easy to get $\mathcal{S}'$ of $|\psi'\rangle$.
- Let alone keeping track of the operators in the stabilizers.

Still, stabilizers? What is the point?

The devil is in the details.

Or

God is in the details.

Stabilizers in the Pauli group is extremely simple!

The Pauli and Clifford Groups

Switch to the Quantum Workbook

Exercise Problems

... about the Pauli group?

1. Given a set of independent Pauli operators $\hat{G}_1, \hat{G}_2, \cdots, \hat{G}_k$, find $\hat{G}$ that anti-commutes with one and only one of them and commute with the rest.
   - For example, consider

$$\hat{Z}\otimes\hat{Z}\otimes\hat{I}, \quad \hat{Z}\otimes\hat{I}\otimes\hat{Z}.$$

   - What about these?

$$\begin{gathered}\hat{X}\otimes\hat{Z}\otimes\hat{Z}\otimes\hat{X}\otimes\hat{I},\\ \hat{I}\otimes\hat{X}\otimes\hat{Z}\otimes\hat{Z}\otimes\hat{X},\\ \hat{X}\otimes\hat{I}\otimes\hat{X}\otimes\hat{Z}\otimes\hat{Z},\\ \hat{Z}\otimes\hat{X}\otimes\hat{I}\otimes\hat{X}\otimes\hat{Z},\\ \hat{Z}\otimes\hat{Z}\otimes\hat{Z}\otimes\hat{Z}\otimes\hat{Z}.\end{gathered}$$

Exercise Problems (continued)

... about the Clifford group?

1. Given a unitary $\hat{U}$, how can you tell if it is Clifford or not?
   - Is controlled-Pauli a Clifford?
   - Is controlled-Clifford a Clifford?
   - ...
2. Given a Clifford $\hat{U}$, decompose it into elementary Clifford gates.

Clifford Decomposition I

vs. Gray Decomposition

1. Consider a Clifford

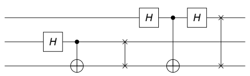
$$\hat{U} \doteq \frac{1}{2\sqrt{2}} \begin{pmatrix} 1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 \\ -1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 \\ -1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \end{pmatrix}$$

Can you see this is a Clifford?

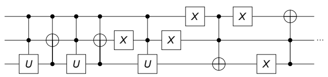
Clifford Decomposition II

vs. Gray Decomposition

2. In terms of elementary Clifford gates,

$\hat{U} \doteq$ 

3. The Gray-code-based decomposition gives (total 149 gates!)

$\hat{U} \doteq$ 

Exercise Problems (continued)

... about the Clifford group?

- How can you list the elements of, say, the three-qubit Clifford group?
  Note that there are 92,897,280 elements in $\mathcal{C}(3)$. Why would you want to do that?

Properties of Stabilizers

In the Pauli Group

Elementary Properties of Stabilizers

1. All elements of $\mathcal{S}$ commute with each other ($\mathcal{S}$ is Abelian).
2. $\mathcal{S}$ cannot include $-\hat{I}$. ($\mathcal{S}$ includes no Pauli operators with phase factors $\pm i$.)

Fundamental Properties of Stabilizers

Code Space and Stabilizer

Suppose that $\mathcal{S}$ is a stabilizer on n qubits generated by k independent operators $\hat{G}_1, \cdots, \hat{G}_k$. Let $\mathcal{V}$ is the subspace stabilized by $\mathcal{S}$.

1. $\mathcal{S}$ is Abelian and $\mathcal{S} \simeq \mathbb{Z}_2^k$ (with the group multiplication given by the addition modulo 2).
2. The dimension of $\mathcal{V}$ is equal to 2^{n-k}. In other words, the subspace $\mathcal{V}$ can encode $(n-k)$ logical qubits.

Example

- $\hat{Z} \otimes \hat{Z}$ stabilizes both $|00\rangle$ and $|11\rangle$, and hence any combination of
$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad \frac{|00\rangle - |11\rangle}{\sqrt{2}}.$$
- $\hat{X} \otimes \hat{X}$ stabilizes any combination of
$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad \frac{|01\rangle + |10\rangle}{\sqrt{2}}.$$
- $\mathcal{S} := \mathrm{Gen}\{\hat{Z} \otimes \hat{Z}, \hat{X} \otimes \hat{X}\}$ stabilizes only
$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$
Therefore, $\dim \mathcal{V} = 1$ consistent with $2^{n-k} = 1$ for $n = k = 2$.

Is any state stabilized by the Pauli group?

No. Only "stabilizer states" are.

- A quantum state is a stabilizer state if it can be obtained from $|0, 0, \cdots, 0\rangle$ by operating a *Clifford operator*.

Exercise Problems

1. Given a quantum state, how can you tell if it is a stabilizer state or not?
2. Given a stabilizer state, find its stabilizer.

* Although not of much meaning in the stabilizer formalism.

Clifford Gates in Stabilizer Formalism

Stabilizer under a Clifford Gate

- Generators of the stabilizer

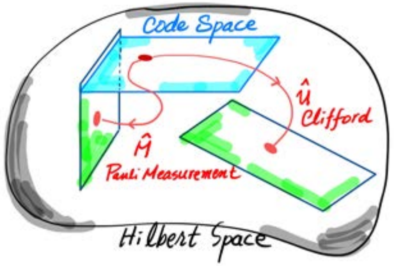
$$\hat{G}_j \mapsto \hat{U}\hat{G}_j\hat{U}^\dagger$$

- Logical operators

$$\bar{X}_j \mapsto \hat{U}\bar{X}_j\hat{U}^\dagger$$
$$\bar{Z}_j \mapsto \hat{U}\bar{Z}_j\hat{U}^\dagger$$

Recall:

$$\hat{U}\hat{X}_j\hat{U}^\dagger = (-1)^{p_j} \prod_i X_i^{a_{ij}} Z_i^{b_{ij}}$$
$$\hat{U}\hat{Z}_j\hat{U}^\dagger = (-1)^{q_j} \prod_i X_i^{c_{ij}} Z_i^{d_{ij}}$$



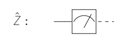
Pauli Measurements in Stabilizer Formalism

Pauli Measurements

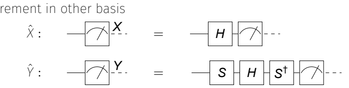
- Any Pauli operator has eigenvalues ± 1 only.
- Measurement outcome is either 0 $(+1)$ or 1 (-1).

Pauli Measurements
Physical Implementations

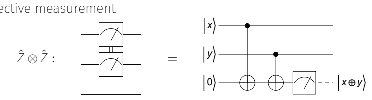
- Measurement in the computational basis



- Measurement in other basis



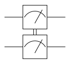
- Collective measurement



Collective vs Sequential Measurements

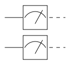
- Collective measurement

$\hat{Z}\otimes\hat{Z}$:



- Sequential measurement

$\hat{Z}\otimes\hat{I}$ followed by $\hat{I}\otimes\hat{Z}$:

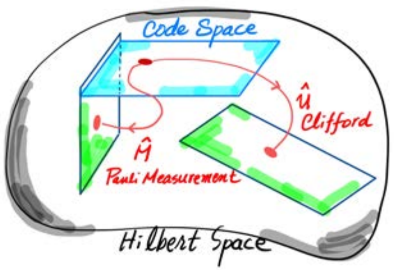


$$|000\rangle\, c_0 + |111\rangle\, c_1 \xrightarrow{\text{error}} |100\rangle\, c_0 + |011\rangle\, c_1 \xrightarrow{\text{measurement } \hat{Z}_1} |100\rangle \xrightarrow{\text{measurement } \hat{Z}_2} |100\rangle$$

Pauli Measurements on Stabilizers

Let $\hat{M}$ be a Pauli operator to measure. Let $\hat{G}_1, \hat{G}_2, \cdots, \hat{G}_k$ be independent generators of the stabilizer $\mathcal{S}$.

1. $\hat{M}$ anti-commutes with at least one of the generator of the stabilizer.
2. $\hat{M}$ commutes with all generators of the stabilizer.
   - $\hat{M}$ belongs to the stabilizer: No change.
   - $\hat{M}$ does not belong to the stabilizer: The stabilizer breaks!



Stabilizer under Pauli Measurement

- Let $\hat{M}$ anti-commute with $\hat{G} := \hat{G}_j$ $(j = 1, 2, \cdots, k)$.
- The post-measurement state is given by

$$|\psi'_\pm\rangle := \frac{1}{2}(1 \pm \hat{M})\,|\psi\rangle\ .$$

1. If the outcome is 0 $(+1)$, then $|\psi'_+\rangle$ is stabilized by $\hat{M}$.
   $\Rightarrow$ Just replace $\hat{G}$ by $\hat{M}$.
2. If the outcome is 1 (-1), then $\hat{G}\,|\psi'_-\rangle$ is stabilized by $\hat{M}$.
   $\Rightarrow$ Operate $\hat{G}$ and then replace $\hat{G}$ by $\hat{M}$.

$$\hat{G}\,|\psi'_-\rangle = \frac{1}{2}\hat{G}(1-\hat{M})\,|\psi\rangle = \frac{1}{2}(1+\hat{M})\hat{G}\,|\psi\rangle = \frac{1}{2}(1+\hat{M})\,|\psi\rangle$$

- In any case, operate $\hat{G}$ *conditioned* on the measurement outcome, and then replace $\hat{G}$ by $\hat{M}$ in the generating set.

Stabilizer under Pauli Measurement
The Full Set of Rules

1. Identify a generator $\hat{G} := \hat{G}_j$ that anti-commutes with $\hat{M}$.
2. Operate $\hat{G}$ *conditioned* on the measurement outcome.

3. Replace $\hat{G}$ by $\hat{M}$ in the generating set.
4. For each $\hat{G}_i$ $(i \neq j)$ of other generators,
   - Keep it if it commutes with $\hat{M}$.
   - Replace it with $\hat{G}\hat{G}_i$ if it anti-commutes with $\hat{M}$.

5. For each logical operator $\hat{L}_i$ ($\bar{X}_i$ or $\bar{Z}_i$),
   - Keep it if it commutes with $\hat{M}$.
   - Replace it with $\hat{G}\hat{L}_i$ if it anti-commutes with $\hat{M}$.

Examples
Switch to the Quantum Workbook

Gottesman-Knill Theorem

Clifford Circuits

A quantum circuit consisting of Clifford gates only.

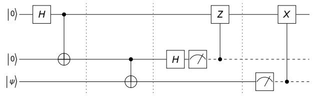
The Clifford group $= \mathbf{Gen}\,\{\text{Hadamard}, \text{quadrant}, \text{CNOT}\}$

Note that together with the octant phase gate (the so-called T-gate) as well, the stabilizer circuit become universal.

Stabilizer Circuits

cf. Clifford Circuits

1. Clifford gates.
2. Pauli measurements followed by semi-classical control.



Gottesman-Knill Theorem

"Any stabilizer circuit can be efficiently simulated on a classical computer."

Surprise?

- The Clifford operators are sufficient to generate a rich range of quantum effects including the Greenberger-Horne-Zeilinger (GHZ) experiment, quantum teleportation, and super dense coding.
- They are also sufficient to encode and decode quantum error-correction codes (to be seen soon).

So, yes, indeed surprising!

On the other hand, the Clifford gates are not sufficient for universal quantum computation. In addition to Clifford gates, we need octant phase gates (or Toffoli gates) to implement an arbitrary unitary gate to an arbitrary accuracy

What's the secrete?

- **Key Point**: Stabilizer formalism tracks the generators of the stabilizer rather than the quantum states as in the usual methods.
- To follow the evolution of the quantum states, one needs to keep track of 2^n complex amplitudes.

  vs.

  There are an order of n generators of the stabilizer because any finite group $\mathcal{G}$ has a generating set of at most $\log_2|\mathcal{G}|$ elements.

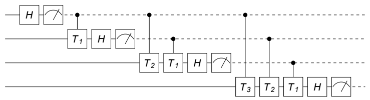
- The Clifford group is generated by the Hadamard, octant phase, and CNOT gates.
- The generators under the conjugate by these elementary gates can be updated in polynomial time, $\mathcal{O}(n)$ time, for the gate.
- See the algorithm by Aaronson & Gottesman, Physical Review A (2004).

Superpower vs. Enaglement

The GK theorem implies that entanglement alone is not enough?

- Entanglement may not even be necessary:

QFT =



- What governs “superpower” ≫ “superweakness”? Nobody knows.

References

Aaronson, S. & D. Gottesman, Physical Review A **70 (5)** (2004). “Improved simulation of stabilizer circuits”.
Dennis, E., A. Kitaev, A. Landahl, & J. Preskill, Journal of Mathematical Physics **43 (9)**, 4452 (2002). “Topological quantum memory”.
Freedman, M. H., Foundations of Computational Mathematics **1 (2)**, 183 (2001). “Quantum Computation and the Localization of Modular Functors”.
Gottesman, D., Phys. Rev. A **54 (3)**, 1862 (1996). “Class of quantum error-correcting codes saturating the quantum Hamming bound”.
Gottesman, D., Phys. Rev. A **57 (1)**, 127 (1998). “Theory of fault-tolerant quantum computation”.
Kitaev, A. Y., Ann. Phys. **303 (1)**, 2 (2003). “Fault-tolerant quantum computation by anyons”.