Efficient simulation of quantum computers: the Gottesman-Knill theorem or an application of group theory to quantum information (part 2)

Vlad Gheorghiu

Department of Physics
Carnegie Mellon University
Pittsburgh, PA 15213, U.S.A.

January 30, 2008

- Both lectures (Wed. Jan 28 and Today, Jan 30) are available online at http://quantum.phys.cmu.edu/groupth

- Classical computers

- Classical computers
- Quantum computers - evolution is unitary, the group $\mathcal{U}(2^n)$

$$|\psi\rangle_{final} = U|\psi\rangle_{initial} = U|0,0,\ldots,0\rangle$$

Evolving a quantum state requires in general $\mathcal{O}(2^n)$ operations!

- Classical computers
- Quantum computers - evolution is unitary, the group $\mathcal{U}(2^n)$

$$|\psi\rangle_{final} = U|\psi\rangle_{initial} = U|0,0,\ldots,0\rangle$$

Evolving a quantum state requires in general $\mathcal{O}(2^n)$ operations!

- The Pauli group on one qudit

$$\mathcal{P}_1 = \{\pm 1, \pm i\}\{I, X, Y, Z\}$$

where the Pauli matrices are

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

with $XY = iZ$ and $X^2 = Y^2 = Z^2 = I$.

- Classical computers
- Quantum computers - evolution is unitary, the group $\mathcal{U}(2^n)$

$$|\psi\rangle_{final} = U|\psi\rangle_{initial} = U|0,0,\ldots,0\rangle$$

Evolving a quantum state requires in general $\mathcal{O}(2^n)$ operations!

- The Pauli group on one qudit

$$\mathcal{P}_1 = \{\pm 1, \pm i\}\{I, X, Y, Z\}$$

where the Pauli matrices are

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

with $XY = iZ$ and $X^2 = Y^2 = Z^2 = I$.

- The Pauli group on n qudits

$$\mathcal{P}_n = \{\pm 1, \pm i\}\{X^{a_1}Z^{b_1} \otimes X^{a_2}Z^{b_2} \otimes \ldots \otimes X^{a_n}Z^{b_n}\}$$

- The Clifford group $\mathcal{C}_1$ on one qubit

$$\mathcal{C}_1 \mathcal{P}_1 \mathcal{C}_1^\dagger = \mathcal{P}_1$$

- The Clifford group $\mathcal{C}_1$ on one qubit

$$\mathcal{C}_1 \mathcal{P}_1 \mathcal{C}_1^\dagger = \mathcal{P}_1$$

- The Clifford group $\mathcal{C}_n$ on n qubits

$$\mathcal{C}_n \mathcal{P}_n \mathcal{C}_n^\dagger = \mathcal{P}_n$$

- The Clifford group $\mathcal{C}_1$ on one qubit

$$\mathcal{C}_1 \mathcal{P}_1 \mathcal{C}_1^\dagger = \mathcal{P}_1$$

- The Clifford group $\mathcal{C}_n$ on n qubits

$$\mathcal{C}_n \mathcal{P}_n \mathcal{C}_n^\dagger = \mathcal{P}_n$$

Up to complex phases, the Clifford group $\mathcal{C}_n$ is generated by H,S and $CNOT$, where

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \text{ and } CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

- The Clifford group $\mathcal{C}_1$ on one qubit

$$\mathcal{C}_1 \mathcal{P}_1 \mathcal{C}_1^\dagger = \mathcal{P}_1$$

- The Clifford group $\mathcal{C}_n$ on n qubits

$$\mathcal{C}_n \mathcal{P}_n \mathcal{C}_n^\dagger = \mathcal{P}_n$$

Up to complex phases, the Clifford group $\mathcal{C}_n$ is generated by H,S and $CNOT$, where

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \text{ and } CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

- For example, $HXH^\dagger = Z$, $CNOT(X \otimes I)CNOT^\dagger = X \otimes X$.

- The action of a group G on a set A is defined as a binary function

$$G \times A \longrightarrow A$$

denoted by $(g, a) \longrightarrow g \cdot a$ that satisfies the following two axioms

- The action of a group G on a set A is defined as a binary function

$$G \times A \longrightarrow A$$

denoted by $(g, a) \longrightarrow g \cdot a$ that satisfies the following two axioms

1. $(gh) \cdot a = g \cdot (h \cdot a)$ for all $g, h \in G$ and $a \in A$;

- The action of a group G on a set A is defined as a binary function

$$G \times A \longrightarrow A$$

denoted by $(g, a) \longrightarrow g \cdot a$ that satisfies the following two axioms

1. $(gh) \cdot a = g \cdot (h \cdot a)$ for all $g, h \in G$ and $a \in A$;
2. $e \cdot a = a$ for every $a \in A$ (here e is the identity of G).

- The action of a group G on a set A is defined as a binary function

$$G \times A \longrightarrow A$$

denoted by $(g, a) \longrightarrow g \cdot a$ that satisfies the following two axioms

1. $(gh) \cdot a = g \cdot (h \cdot a)$ for all $g, h \in G$ and $a \in A$;
2. $e \cdot a = a$ for every $a \in A$ (here e is the identity of G).

- Now let G be the Pauli group $\mathcal{P}_1$ and A the Hilbert space of 1 qudit, $\mathbb{C}_2$.

- The action of a group G on a set A is defined as a binary function

$$G \times A \longrightarrow A$$

denoted by $(g, a) \longrightarrow g \cdot a$ that satisfies the following two axioms

1. $(gh) \cdot a = g \cdot (h \cdot a)$ for all $g, h \in G$ and $a \in A$;
2. $e \cdot a = a$ for every $a \in A$ (here e is the identity of G).

- Now let G be the Pauli group $\mathcal{P}_1$ and A the Hilbert space of 1 qudit, $\mathbb{C}_2$.
- A basis of $\mathbb{C}_2$ is formally denoted by $\{|0\rangle, |1\rangle\}$.

- The action of a group G on a set A is defined as a binary function

$$G \times A \longrightarrow A$$

denoted by $(g, a) \longrightarrow g \cdot a$ that satisfies the following two axioms

1. $(gh) \cdot a = g \cdot (h \cdot a)$ for all $g, h \in G$ and $a \in A$;
2. $e \cdot a = a$ for every $a \in A$ (here e is the identity of G).

- Now let G be the Pauli group $\mathcal{P}_1$ and A the Hilbert space of 1 qudit, $\mathbb{C}_2$.
- A basis of $\mathbb{C}_2$ is formally denoted by $\{|0\rangle, |1\rangle\}$.
- We define an action of the Pauli group on the Hilbert space of one qubit by specifying how the elements of G act on the basis
  1. $I|0\rangle = |0\rangle$, $I|1\rangle = |1\rangle$ (identity)

- The action of a group G on a set A is defined as a binary function

$$G \times A \longrightarrow A$$

denoted by $(g, a) \longrightarrow g \cdot a$ that satisfies the following two axioms

1. $(gh) \cdot a = g \cdot (h \cdot a)$ for all $g, h \in G$ and $a \in A$;
2. $e \cdot a = a$ for every $a \in A$ (here e is the identity of G).

- Now let G be the Pauli group $\mathcal{P}_1$ and A the Hilbert space of 1 qudit, $\mathbb{C}_2$.
- A basis of $\mathbb{C}_2$ is formally denoted by $\{|0\rangle, |1\rangle\}$.
- We define an action of the Pauli group on the Hilbert space of one qubit by specifying how the elements of G act on the basis
  1. $I|0\rangle = |0\rangle$, $I|1\rangle = |1\rangle$ (identity)
  2. $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$ (bit flip)

- The action of a group G on a set A is defined as a binary function

$$G \times A \longrightarrow A$$

denoted by $(g, a) \longrightarrow g \cdot a$ that satisfies the following two axioms

1. $(gh) \cdot a = g \cdot (h \cdot a)$ for all $g, h \in G$ and $a \in A$;
2. $e \cdot a = a$ for every $a \in A$ (here e is the identity of G).

- Now let G be the Pauli group $\mathcal{P}_1$ and A the Hilbert space of 1 qudit, $\mathbb{C}_2$.
- A basis of $\mathbb{C}_2$ is formally denoted by $\{|0\rangle, |1\rangle\}$.
- We define an action of the Pauli group on the Hilbert space of one qubit by specifying how the elements of G act on the basis
  1. $I|0\rangle = |0\rangle$, $I|1\rangle = |1\rangle$ (identity)
  2. $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$ (bit flip)
  3. $Z|0\rangle = |0\rangle$, $Z|1\rangle = -1|1\rangle$ (phase flip)

- The action of a group G on a set A is defined as a binary function

$$G \times A \longrightarrow A$$

denoted by $(g, a) \longrightarrow g \cdot a$ that satisfies the following two axioms

1. $(gh) \cdot a = g \cdot (h \cdot a)$ for all $g, h \in G$ and $a \in A$;
2. $e \cdot a = a$ for every $a \in A$ (here e is the identity of G).

- Now let G be the Pauli group $\mathcal{P}_1$ and A the Hilbert space of 1 qudit, $\mathbb{C}_2$.
- A basis of $\mathbb{C}_2$ is formally denoted by $\{|0\rangle, |1\rangle\}$.
- We define an action of the Pauli group on the Hilbert space of one qubit by specifying how the elements of G act on the basis

1. $I|0\rangle = |0\rangle$, $I|1\rangle = |1\rangle$ (identity)
2. $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$ (bit flip)
3. $Z|0\rangle = |0\rangle$, $Z|1\rangle = -1|1\rangle$ (phase flip)
4. $Y|0\rangle =?$, $Y|1\rangle =?$.

- The action of a group G on a set A is defined as a binary function

$$G \times A \longrightarrow A$$

denoted by $(g, a) \longrightarrow g \cdot a$ that satisfies the following two axioms

1. $(gh) \cdot a = g \cdot (h \cdot a)$ for all $g, h \in G$ and $a \in A$;
2. $e \cdot a = a$ for every $a \in A$ (here e is the identity of G).

- Now let G be the Pauli group $\mathcal{P}_1$ and A the Hilbert space of 1 qudit, $\mathbb{C}_2$.
- A basis of $\mathbb{C}_2$ is formally denoted by $\{|0\rangle, |1\rangle\}$.
- We define an action of the Pauli group on the Hilbert space of one qubit by specifying how the elements of G act on the basis
  1. $I|0\rangle = |0\rangle$, $I|1\rangle = |1\rangle$ (identity)
  2. $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$ (bit flip)
  3. $Z|0\rangle = |0\rangle$, $Z|1\rangle = -1|1\rangle$ (phase flip)
  4. $Y|0\rangle =?$, $Y|1\rangle =?$.
- Now we know how G is acting on any element of $\mathbb{C}_2$, by linearity, e.g. $X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$.

- The action of a group G on a set A is defined as a binary function

$$G \times A \longrightarrow A$$

denoted by $(g, a) \longrightarrow g \cdot a$ that satisfies the following two axioms

1. $(gh) \cdot a = g \cdot (h \cdot a)$ for all $g, h \in G$ and $a \in A$;
2. $e \cdot a = a$ for every $a \in A$ (here e is the identity of G).

- Now let G be the Pauli group $\mathcal{P}_1$ and A the Hilbert space of 1 qudit, $\mathbb{C}_2$.
- A basis of $\mathbb{C}_2$ is formally denoted by $\{|0\rangle, |1\rangle\}$.
- We define an action of the Pauli group on the Hilbert space of one qubit by specifying how the elements of G act on the basis
  1. $I|0\rangle = |0\rangle$, $I|1\rangle = |1\rangle$ (identity)
  2. $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$ (bit flip)
  3. $Z|0\rangle = |0\rangle$, $Z|1\rangle = -1|1\rangle$ (phase flip)
  4. $Y|0\rangle =?$, $Y|1\rangle =?$.
- Now we know how G is acting on any element of $\mathbb{C}_2$, by linearity, e.g. $X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$.
- Check that we have a valid action function.

- Similarly, we define the action of the Pauli group on n qudits $\mathcal{P}_n$ on the Hilbert space of n qudits $\mathbb{C}_2^n$

- Similarly, we define the action of the Pauli group on n qudits $\mathcal{P}_n$ on the Hilbert space of n qudits $\mathbb{C}_2^n$
- First note that a basis of $\mathbb{C}_2^n$ is formally specified as $\{|0,0,\ldots,0\rangle, |0,0,\ldots,1\rangle, \ldots, |1,1,\ldots,1\rangle\}$

- Similarly, we define the action of the Pauli group on n qudits $\mathcal{P}_n$ on the Hilbert space of n qudits $\mathbb{C}_2^n$
- First note that a basis of $\mathbb{C}_2^n$ is formally specified as $\{|0,0,\ldots,0\rangle, |0,0,\ldots,1\rangle, \ldots, |1,1,\ldots,1\rangle\}$
- Recall that an element g of $\mathcal{P}_n$ consists of a phase times a tensor product of n Pauli matrices

- Similarly, we define the action of the Pauli group on n qudits $\mathcal{P}_n$ on the Hilbert space of n qudits $\mathbb{C}_2^n$
- First note that a basis of $\mathbb{C}_2^n$ is formally specified as $\{|0,0,\ldots,0\rangle, |0,0,\ldots,1\rangle, \ldots, |1,1,\ldots,1\rangle\}$
- Recall that an element g of $\mathcal{P}_n$ consists of a phase times a tensor product of n Pauli matrices
- Each component of g acts individually on the corresponding component of the basis element

- Similarly, we define the action of the Pauli group on n qudits $\mathcal{P}_n$ on the Hilbert space of n qudits $\mathbb{C}_2^n$
- First note that a basis of $\mathbb{C}_2^n$ is formally specified as $\{|0,0,\ldots,0\rangle, |0,0,\ldots,1\rangle, \ldots, |1,1,\ldots,1\rangle\}$
- Recall that an element g of $\mathcal{P}_n$ consists of a phase times a tensor product of n Pauli matrices
- Each component of g acts individually on the corresponding component of the basis element
- Example: consider 3 qubits, let $g = X \otimes I \otimes Z$ be an element of $\mathcal{P}_3$ and let us see how it acts on $|1,0,1\rangle$; then $X \otimes I \otimes Z|1,0,1\rangle = -|0,0,1\rangle$. Extend the action by linearity.

- Similarly, we define the action of the Pauli group on n qudits $\mathcal{P}_n$ on the Hilbert space of n qudits $\mathbb{C}_2^n$
- First note that a basis of $\mathbb{C}_2^n$ is formally specified as $\{|0,0,\ldots,0\rangle, |0,0,\ldots,1\rangle, \ldots, |1,1,\ldots,1\rangle\}$
- Recall that an element g of $\mathcal{P}_n$ consists of a phase times a tensor product of n Pauli matrices
- Each component of g acts individually on the corresponding component of the basis element
- Example: consider 3 qubits, let $g = X \otimes I \otimes Z$ be an element of $\mathcal{P}_3$ and let us see how it acts on $|1,0,1\rangle$; then $X \otimes I \otimes Z|1,0,1\rangle = -|0,0,1\rangle$. Extend the action by linearity.
- So now we know how $\mathcal{P}_n$ acts on the Hilbert space $\mathbb{C}_2^n$ of n qubits

- Similarly, we define the action of the Pauli group on n qudits $\mathcal{P}_n$ on the Hilbert space of n qudits $\mathbb{C}_2^n$
- First note that a basis of $\mathbb{C}_2^n$ is formally specified as $\{|0,0,\ldots,0\rangle, |0,0,\ldots,1\rangle, \ldots, |1,1,\ldots,1\rangle\}$
- Recall that an element g of $\mathcal{P}_n$ consists of a phase times a tensor product of n Pauli matrices
- Each component of g acts individually on the corresponding component of the basis element
- Example: consider 3 qubits, let $g = X \otimes I \otimes Z$ be an element of $\mathcal{P}_3$ and let us see how it acts on $|1,0,1\rangle$; then $X \otimes I \otimes Z|1,0,1\rangle = -|0,0,1\rangle$. Extend the action by linearity.
- So now we know how $\mathcal{P}_n$ acts on the Hilbert space $\mathbb{C}_2^n$ of n qubits
- What is $(Z \otimes X \otimes X)(\alpha|0,0,1\rangle + \beta|1,1,0\rangle)$?

- Similarly, we define the action of the Pauli group on n qudits $\mathcal{P}_n$ on the Hilbert space of n qudits $\mathbb{C}_2^n$
- First note that a basis of $\mathbb{C}_2^n$ is formally specified as $\{|0,0,\ldots,0\rangle, |0,0,\ldots,1\rangle, \ldots, |1,1,\ldots,1\rangle\}$
- Recall that an element g of $\mathcal{P}_n$ consists of a phase times a tensor product of n Pauli matrices
- Each component of g acts individually on the corresponding component of the basis element
- Example: consider 3 qubits, let $g = X \otimes I \otimes Z$ be an element of $\mathcal{P}_3$ and let us see how it acts on $|1,0,1\rangle$; then $X \otimes I \otimes Z|1,0,1\rangle = -|0,0,1\rangle$. Extend the action by linearity.
- So now we know how $\mathcal{P}_n$ acts on the Hilbert space $\mathbb{C}_2^n$ of n qubits
- What is $(Z \otimes X \otimes X)(\alpha|0,0,1\rangle + \beta|1,1,0\rangle)$? The result is $\alpha|0,1,0\rangle - \beta|1,0,1\rangle$.

- We now have an action of $\mathcal{P}_n$ on the Hilbert space $\mathbb{C}_2^n$

- We now have an action of $\mathcal{P}_n$ on the Hilbert space $\mathbb{C}_2^n$
- Suppose S is a subgroup of $\mathcal{P}_n$

- We now have an action of $\mathcal{P}_n$ on the Hilbert space $\mathbb{C}_2^n$
- Suppose S is a subgroup of $\mathcal{P}_n$
- Define V_S to be the set of n qubit states which are fixed by every element of S, i.e.

$$V_S = \{|\psi\rangle \in \mathbb{C}_2^n : s|\psi\rangle = (+1)|\psi\rangle, \forall s \in S\}$$

- We now have an action of $\mathcal{P}_n$ on the Hilbert space $\mathbb{C}_2^n$
- Suppose S is a subgroup of $\mathcal{P}_n$
- Define V_S to be the set of n qubit states which are fixed by every element of S, i.e.

$$V_S = \{|\psi\rangle \in \mathbb{C}_2^n : s|\psi\rangle = (+1)|\psi\rangle, \forall s \in S\}$$

- V_S is the vector space stabilized by S, and S is called the stabilizer of V_S

- We now have an action of $\mathcal{P}_n$ on the Hilbert space $\mathbb{C}_2^n$
- Suppose S is a subgroup of $\mathcal{P}_n$
- Define V_S to be the set of n qubit states which are fixed by every element of S, i.e.

$$V_S = \{|\psi\rangle \in \mathbb{C}_2^n : s|\psi\rangle = (+1)|\psi\rangle, \forall s \in S\}$$

- V_S is the vector space stabilized by S, and S is called the stabilizer of V_S
- Convince yourself that V_S is a vector space (show that an arbitrary linear combination of elements from V_S also belongs to V_S)

- We now have an action of $\mathcal{P}_n$ on the Hilbert space $\mathbb{C}_2^n$
- Suppose S is a subgroup of $\mathcal{P}_n$
- Define V_S to be the set of n qubit states which are fixed by every element of S, i.e.

$$V_S = \{|\psi\rangle \in \mathbb{C}_2^n : s|\psi\rangle = (+1)|\psi\rangle, \forall s \in S\}$$

- V_S is the vector space stabilized by S, and S is called the stabilizer of V_S
- Convince yourself that V_S is a vector space (show that an arbitrary linear combination of elements from V_S also belongs to V_S)
- Show that V_S is the intersection of the subspaces fixed by each operator in S (that is, the eigenvalues one eigenspaces of elements of S)

- Example: what is the vector space stabilized by $\{I, X\} \subset \mathcal{P}_1$?

- Example: what is the vector space stabilized by $\{I, X\} \subset \mathcal{P}_1$? Answer: $\{|0\rangle\}$.

- Example: what is the vector space stabilized by $\{I, X\} \subset \mathcal{P}_1$? Answer: $\{|0\rangle\}$.
- Another example: what about $\{I \otimes I, Z \otimes Z\} \subset \mathcal{P}_n$?

- Example: what is the vector space stabilized by $\{I, X\} \subset \mathcal{P}_1$? Answer: $\{|0\rangle\}$.
- Another example: what about $\{I \otimes I, Z \otimes Z\} \subset \mathcal{P}_n$? Answer: Span$\{|0,0\rangle, |1,1\rangle\}$.

- Example: what is the vector space stabilized by $\{I, X\} \subset \mathcal{P}_1$? Answer: $\{|0\rangle\}$.
- Another example: what about $\{I \otimes I, Z \otimes Z\} \subset \mathcal{P}_n$? Answer: $\text{Span}\{|0,0\rangle, |1,1\rangle\}$.
- The last one... $\{I, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$ stabilizes $\text{Span}\{|0,0,0\rangle, |1,1,1\rangle\}$

- Example: what is the vector space stabilized by $\{I, X\} \subset \mathcal{P}_1$? Answer: $\{|0\rangle\}$.
- Another example: what about $\{I \otimes I, Z \otimes Z\} \subset \mathcal{P}_n$? Answer: $\text{Span}\{|0,0\rangle, |1,1\rangle\}$.
- The last one... $\{I, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$ stabilizes $\text{Span}\{|0,0,0\rangle, |1,1,1\rangle\}$
- S and V_S are dual to each other, in the sense that one uniquely determines the other and vice versa.

- Example: what is the vector space stabilized by $\{I, X\} \subset \mathcal{P}_1$? Answer: $\{|0\rangle\}$.
- Another example: what about $\{I \otimes I, Z \otimes Z\} \subset \mathcal{P}_n$? Answer: $\text{Span}\{|0,0\rangle, |1,1\rangle\}$.
- The last one... $\{I, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$ stabilizes $\text{Span}\{|0,0,0\rangle, |1,1,1\rangle\}$
- S and V_S are dual to each other, in the sense that one uniquely determines the other and vice versa.
- Clever idea: one can describe (some) subspaces (V_S) by subgroups (S). What's the advantage?

- The necessary and sufficient conditions that S must satisfy in order to stabilize a nontrivial vector space V_S are
  1. S must be Abelian

- The necessary and sufficient conditions that S must satisfy in order to stabilize a nontrivial vector space V_S are
  1. S must be Abelian
  2. $-I$ does not belong to S

- The necessary and sufficient conditions that S must satisfy in order to stabilize a nontrivial vector space V_S are
  1. S must be Abelian
  2. $-I$ does not belong to S
- The necessity is easy...

- The necessary and sufficient conditions that S must satisfy in order to stabilize a nontrivial vector space V_S are
  1. S must be Abelian
  2. $-I$ does not belong to S
- The necessity is easy...
- Describe the stabilizer group S of some subspace V_S by specifying its generators

- The necessary and sufficient conditions that S must satisfy in order to stabilize a nontrivial vector space V_S are
  1. S must be Abelian
  2. $-I$ does not belong to S
- The necessity is easy...
- Describe the stabilizer group S of some subspace V_S by specifying its generators
- A group of size K has at most $\log(K)$ generators!

- The necessary and sufficient conditions that S must satisfy in order to stabilize a nontrivial vector space V_S are
  1. S must be Abelian
  2. $-I$ does not belong to S
- The necessity is easy...
- Describe the stabilizer group S of some subspace V_S by specifying its generators
- A group of size K has at most $\log(K)$ generators!
- So a stabilizer subspace of n qubits can be specified by a set of k independent generators, and it turns out that k is always smaller than n

- The necessary and sufficient conditions that S must satisfy in order to stabilize a nontrivial vector space V_S are
  1. S must be Abelian
  2. $-I$ does not belong to S
- The necessity is easy...
- Describe the stabilizer group S of some subspace V_S by specifying its generators
- A group of size K has at most $\log(K)$ generators!
- So a stabilizer subspace of n qubits can be specified by a set of k independent generators, and it turns out that k is always smaller than n
- In the last example from the previous slide, S was generated by $\langle Z_1 Z_2, Z_2 Z_3 \rangle = \langle Z \otimes Z \otimes I, I \otimes Z \otimes Z \rangle$

Theorem

Let $S = \langle g_1, g_2, \ldots, g_k \rangle$ be a stabilizer group generated by k independent and commuting generators from $\mathcal{P}_n$, such that $-I \notin S$. Then the vector space stabilized by S has dimension 2^{n-k}.

Theorem

Let $S = \langle g_1, g_2, \ldots, g_k \rangle$ be a stabilizer group generated by k independent and commuting generators from $\mathcal{P}_n$, such that $-I \notin S$. Then the vector space stabilized by S has dimension 2^{n-k}.

- Enlarging S reduces the dimension of V_S

Theorem

Let $S = \langle g_1, g_2, \ldots, g_k \rangle$ be a stabilizer group generated by k independent and commuting generators from $\mathcal{P}_n$, such that $-I \notin S$. Then the vector space stabilized by S has dimension 2^{n-k}.

- Enlarging S reduces the dimension of V_S
- What if $k = n$?

Theorem

Let $S = \langle g_1, g_2, \ldots, g_k \rangle$ be a stabilizer group generated by k independent and commuting generators from $\mathcal{P}_n$, such that $-I \notin S$. Then the vector space stabilized by S has dimension 2^{n-k}.

- Enlarging S reduces the dimension of V_S
- What if $k = n$?

Stabilizer states

A stabilizer group generated by n independent generators stabilizes a one-dimensional vector space. The latter is called a stabilizer state.

Theorem

Let $S = \langle g_1, g_2, \ldots, g_k \rangle$ be a stabilizer group generated by k independent and commuting generators from $\mathcal{P}_n$, such that $-I \notin S$. Then the vector space stabilized by S has dimension 2^{n-k}.

- Enlarging S reduces the dimension of V_S
- What if $k = n$?

Stabilizer states

A stabilizer group generated by n independent generators stabilizes a one-dimensional vector space. The latter is called a stabilizer state.

- Example: Let $S = \langle Z \otimes I, I \otimes Z \rangle$. So $n = 2$, $k = 2$. What is the state stabilized by S?

Theorem

Let $S = \langle g_1, g_2, \ldots, g_k \rangle$ be a stabilizer group generated by k independent and commuting generators from $\mathcal{P}_n$, such that $-I \notin S$. Then the vector space stabilized by S has dimension 2^{n-k}.

- Enlarging S reduces the dimension of V_S
- What if $k = n$?

Stabilizer states

A stabilizer group generated by n independent generators stabilizes a one-dimensional vector space. The latter is called a stabilizer state.

- Example: Let $S = \langle Z \otimes I, I \otimes Z \rangle$. So $n = 2$, $k = 2$. What is the state stabilized by S? Answer: $|00\rangle$.

Theorem

Let $S = \langle g_1, g_2, \ldots, g_k \rangle$ be a stabilizer group generated by k independent and commuting generators from $\mathcal{P}_n$, such that $-I \notin S$. Then the vector space stabilized by S has dimension 2^{n-k}.

- Enlarging S reduces the dimension of V_S
- What if $k = n$?

Stabilizer states

A stabilizer group generated by n independent generators stabilizes a one-dimensional vector space. The latter is called a stabilizer state.

- Example: Let $S = \langle Z \otimes I, I \otimes Z \rangle$. So $n = 2$, $k = 2$. What is the state stabilized by S? Answer: $|00\rangle$.
- So the state $|0, 0, \ldots, 0\rangle$ is a stabilizer state with stabilizer group generated by ...

Theorem

Let $S = \langle g_1, g_2, \ldots, g_k \rangle$ be a stabilizer group generated by k independent and commuting generators from $\mathcal{P}_n$, such that $-I \notin S$. Then the vector space stabilized by S has dimension 2^{n-k}.

- Enlarging S reduces the dimension of V_S
- What if $k = n$?

Stabilizer states

A stabilizer group generated by n independent generators stabilizes a one-dimensional vector space. The latter is called a stabilizer state.

- Example: Let $S = \langle Z \otimes I, I \otimes Z \rangle$. So $n = 2$, $k = 2$. What is the state stabilized by S? Answer: $|00\rangle$.
- So the state $|0, 0, \ldots, 0\rangle$ is a stabilizer state with stabilizer group generated by ... ...

Theorem

Let $S = \langle g_1, g_2, \ldots, g_k \rangle$ be a stabilizer group generated by k independent and commuting generators from $\mathcal{P}_n$, such that $-I \notin S$. Then the vector space stabilized by S has dimension 2^{n-k}.

- Enlarging S reduces the dimension of V_S
- What if $k = n$?

Stabilizer states

A stabilizer group generated by n independent generators stabilizes a one-dimensional vector space. The latter is called a stabilizer state.

- Example: Let $S = \langle Z \otimes I, I \otimes Z \rangle$. So $n = 2$, $k = 2$. What is the state stabilized by S? Answer: $|00\rangle$.
- So the state $|0, 0, \ldots, 0\rangle$ is a stabilizer state with stabilizer group generated by ... ...

Theorem

Let $S = \langle g_1, g_2, \ldots, g_k \rangle$ be a stabilizer group generated by k independent and commuting generators from $\mathcal{P}_n$, such that $-I \notin S$. Then the vector space stabilized by S has dimension 2^{n-k}.

- Enlarging S reduces the dimension of V_S
- What if $k = n$?

Stabilizer states

A stabilizer group generated by n independent generators stabilizes a one-dimensional vector space. The latter is called a stabilizer state.

- Example: Let $S = \langle Z \otimes I, I \otimes Z \rangle$. So $n = 2$, $k = 2$. What is the state stabilized by S? Answer: $|00\rangle$.
- So the state $|0, 0, \ldots, 0\rangle$ is a stabilizer state with stabilizer group generated by ... ...

Theorem

Let $S = \langle g_1, g_2, \ldots, g_k \rangle$ be a stabilizer group generated by k independent and commuting generators from $\mathcal{P}_n$, such that $-I \notin S$. Then the vector space stabilized by S has dimension 2^{n-k}.

- Enlarging S reduces the dimension of V_S
- What if $k = n$?

Stabilizer states

A stabilizer group generated by n independent generators stabilizes a one-dimensional vector space. The latter is called a stabilizer state.

- Example: Let $S = \langle Z \otimes I, I \otimes Z \rangle$. So $n = 2$, $k = 2$. What is the state stabilized by S? Answer: $|00\rangle$.
- So the state $|0, 0, \ldots, 0\rangle$ is a stabilizer state with stabilizer group generated by ... ... $\langle Z_1, Z_2, \ldots, Z_n \rangle$

- Remember that the Clifford group maps Pauli operators to Pauli operators

- Remember that the Clifford group maps Pauli operators to Pauli operators
- Let $c \in \mathcal{C}_n$. Note that $S' = cSc^\dagger$ is also a stabilizer group, and the dimension of $V_{S'}$ equals the dimension of V_S. Why?

- Remember that the Clifford group maps Pauli operators to Pauli operators
- Let $c \in \mathcal{C}_n$. Note that $S' = cSc^\dagger$ is also a stabilizer group, and the dimension of $V_{S'}$ equals the dimension of V_S. Why?
- Convince yourself that if S stabilizes a stabilizer state $|\psi\rangle$, then $S' = cSc^\dagger$ stabilizes $|\psi'\rangle =$

- Remember that the Clifford group maps Pauli operators to Pauli operators
- Let $c \in \mathcal{C}_n$. Note that $S' = cSc^\dagger$ is also a stabilizer group, and the dimension of $V_{S'}$ equals the dimension of V_S. Why?
- Convince yourself that if S stabilizes a stabilizer state $|\psi\rangle$, then $S' = cSc^\dagger$ stabilizes $|\psi'\rangle = c|\psi\rangle$.

- Remember that the Clifford group maps Pauli operators to Pauli operators
- Let $c \in \mathcal{C}_n$. Note that $S' = cSc^\dagger$ is also a stabilizer group, and the dimension of $V_{S'}$ equals the dimension of V_S. Why?
- Convince yourself that if S stabilizes a stabilizer state $|\psi\rangle$, then $S' = cSc^\dagger$ stabilizes $|\psi'\rangle = c|\psi\rangle$.
- If we know how c conjugates the generators of S, we then know how c conjugates the whole S. Why?

- Remember that the Clifford group maps Pauli operators to Pauli operators
- Let $c \in \mathcal{C}_n$. Note that $S' = cSc^\dagger$ is also a stabilizer group, and the dimension of $V_{S'}$ equals the dimension of V_S. Why?
- Convince yourself that if S stabilizes a stabilizer state $|\psi\rangle$, then $S' = cSc^\dagger$ stabilizes $|\psi'\rangle = c|\psi\rangle$.
- If we know how c conjugates the generators of S, we then know how c conjugates the whole S. Why?

- We can now state and prove the following theorem

- We can now state and prove the following theorem

The Gottesman-Knill theorem

A quantum unitary evolution that uses only the following elements can be simulated efficiently on a classical computer:

1. preparation of qubits in computational basis states (w.l.o.g. can be taken to be $|0, 0, \ldots, 0\rangle$)
2. evolution U from the Clifford group
3. measurements in the computational basis.

- We can now state and prove the following theorem

The Gottesman-Knill theorem

A quantum unitary evolution that uses only the following elements can be simulated efficiently on a classical computer:

1. preparation of qubits in computational basis states (w.l.o.g. can be taken to be $|0, 0, \ldots, 0\rangle$)
2. evolution U from the Clifford group
3. measurements in the computational basis.

- The proof is now quite simple...

- We can now state and prove the following theorem

The Gottesman-Knill theorem

A quantum unitary evolution that uses only the following elements can be simulated efficiently on a classical computer:

1. preparation of qubits in computational basis states (w.l.o.g. can be taken to be $|0, 0, \ldots, 0\rangle$)
2. evolution U from the Clifford group
3. measurements in the computational basis.

- The proof is now quite simple...
- The first assumption guarantees that we start with a stabilizer state $|\psi\rangle$, with stabilizer group S_ψ generated by n independent generators $\langle Z_1, Z_2, \ldots, Z_n\rangle$

- We can now state and prove the following theorem

The Gottesman-Knill theorem

A quantum unitary evolution that uses only the following elements can be simulated efficiently on a classical computer:

1. preparation of qubits in computational basis states (w.l.o.g. can be taken to be $|0, 0, \ldots, 0\rangle$)
2. evolution U from the Clifford group
3. measurements in the computational basis.

- The proof is now quite simple...
- The first assumption guarantees that we start with a stabilizer state $|\psi\rangle$, with stabilizer group S_ψ generated by n independent generators $\langle Z_1, Z_2, \ldots, Z_n\rangle$
- Now let's pick a generator of the Clifford group, call it u

- Under the action of u, the initial stabilizer state $|\psi\rangle$ stabilized by some S_ψ will evolve to $u|\psi\rangle$

- Under the action of u, the initial stabilizer state $|\psi\rangle$ stabilized by some S_ψ will evolve to $u|\psi\rangle$
- Remember the duality between a stabilizer state and a stabilizer group

- Under the action of u, the initial stabilizer state $|\psi\rangle$ stabilized by some S_ψ will evolve to $u|\psi\rangle$
- Remember the duality between a stabilizer state and a stabilizer group
- Now $|\psi'\rangle = u|\psi\rangle$ can be as well described by its stabilizer group $S_{\psi'} = uS_\psi u^\dagger$

- Under the action of u, the initial stabilizer state $|\psi\rangle$ stabilized by some S_ψ will evolve to $u|\psi\rangle$
- Remember the duality between a stabilizer state and a stabilizer group
- Now $|\psi'\rangle = u|\psi\rangle$ can be as well described by its stabilizer group $S_{\psi'} = uS_\psi u^\dagger$
- To specify $S_{\psi'}$, it is enough to see how the n generators of S transform under conjugation by u, so we need to find $uZ_1u^\dagger, \ldots, uZ_nu^\dagger$

- Under the action of u, the initial stabilizer state $|\psi\rangle$ stabilized by some S_ψ will evolve to $u|\psi\rangle$
- Remember the duality between a stabilizer state and a stabilizer group
- Now $|\psi'\rangle = u|\psi\rangle$ can be as well described by its stabilizer group $S_{\psi'} = uS_\psi u^\dagger$
- To specify $S_{\psi'}$, it is enough to see how the n generators of S transform under conjugation by u, so we need to find $uZ_1u^\dagger, \ldots, uZ_nu^\dagger$
- To summarize, implementing a generator u of the Clifford group implies updating the n generators that describe the initial quantum state

- Under the action of u, the initial stabilizer state $|\psi\rangle$ stabilized by some S_ψ will evolve to $u|\psi\rangle$
- Remember the duality between a stabilizer state and a stabilizer group
- Now $|\psi'\rangle = u|\psi\rangle$ can be as well described by its stabilizer group $S_{\psi'} = uS_\psi u^\dagger$
- To specify $S_{\psi'}$, it is enough to see how the n generators of S transform under conjugation by u, so we need to find $uZ_1u^\dagger, \ldots, uZ_nu^\dagger$
- To summarize, implementing a generator u of the Clifford group implies updating the n generators that describe the initial quantum state
- This step requires $\mathcal{O}(n^2)$ operations on a classical computer

- Under the action of u, the initial stabilizer state $|\psi\rangle$ stabilized by some S_ψ will evolve to $u|\psi\rangle$
- Remember the duality between a stabilizer state and a stabilizer group
- Now $|\psi'\rangle = u|\psi\rangle$ can be as well described by its stabilizer group $S_{\psi'} = uS_\psi u^\dagger$
- To specify $S_{\psi'}$, it is enough to see how the n generators of S transform under conjugation by u, so we need to find $uZ_1u^\dagger, \ldots, uZ_nu^\dagger$
- To summarize, implementing a generator u of the Clifford group implies updating the n generators that describe the initial quantum state
- This step requires $\mathcal{O}(n^2)$ operations on a classical computer
- In conclusion, if our unitary evolution U is a product of m terms, each a generator of the Clifford group, then the computation can be simulated by a classical computer in time $\mathcal{O}(mn^2)$

- Intuitively, the way the classical computer performs the simulation is simply to keep track of the generators of the stabilizer as the various Clifford elementary operations are being performed in the computation

- Intuitively, the way the classical computer performs the simulation is simply to keep track of the generators of the stabilizer as the various Clifford elementary operations are being performed in the computation
- At the end, we are left with some stabilizer group that stabilizes some state

- Intuitively, the way the classical computer performs the simulation is simply to keep track of the generators of the stabilizer as the various Clifford elementary operations are being performed in the computation
- At the end, we are left with some stabilizer group that stabilizes some state
- Knowing the stabilizer is equivalent to knowing the state (remember the duality)

- Intuitively, the way the classical computer performs the simulation is simply to keep track of the generators of the stabilizer as the various Clifford elementary operations are being performed in the computation
- At the end, we are left with some stabilizer group that stabilizes some state
- Knowing the stabilizer is equivalent to knowing the state (remember the duality)
- End of story...

- Intuitively, the way the classical computer performs the simulation is simply to keep track of the generators of the stabilizer as the various Clifford elementary operations are being performed in the computation
- At the end, we are left with some stabilizer group that stabilizes some state
- Knowing the stabilizer is equivalent to knowing the state (remember the duality)
- End of story...
- It is clear that one cannot perform universal quantum computation with only Clifford operations and measurements in the computational basis

- Intuitively, the way the classical computer performs the simulation is simply to keep track of the generators of the stabilizer as the various Clifford elementary operations are being performed in the computation
- At the end, we are left with some stabilizer group that stabilizes some state
- Knowing the stabilizer is equivalent to knowing the state (remember the duality)
- End of story...
- It is clear that one cannot perform universal quantum computation with only Clifford operations and measurements in the computational basis
- It is not at all obvious that Clifford operations together with only one qubit unitary that does not belong to the Clifford group form a dense set in $\mathcal{U}(2^n)$, that is, one can implement universal quantum computing using this gates!

- Simulate the evolution of the state $|\psi_{initial}\rangle = |00\rangle$ through $U = CNOT_{12}H_1$

- Simulate the evolution of the state $|\psi_{initial}\rangle = |00\rangle$ through $U = CNOT_{12}H_1$
- The following table is all we need for simulating any Clifford evolution

- Simulate the evolution of the state $|\psi_{initial}\rangle = |00\rangle$ through $U = CNOT_{12}H_1$
- The following table is all we need for simulating any Clifford evolution
  1. Conjugation by $CNOT$: $X_1 \rightarrow X_1X_2, X_2 \rightarrow X_2, Z_1 \rightarrow Z_1, Z_2 \rightarrow Z_1Z_2$
  2. Conjugation by H: $X \rightarrow Z, Z \rightarrow X$
  3. Conjugation by S: $X \rightarrow Y, Z \rightarrow Z$
  4. Conjugation by X: $X \rightarrow X, Z \rightarrow -Z$
  5. Conjugation by Y: $X \rightarrow -X, Z \rightarrow -Z$
  6. Conjugation by Z: $X \rightarrow -X, Z \rightarrow Z$

- Simulate the evolution of the state $|\psi_{initial}\rangle = |00\rangle$ through $U = CNOT_{12}H_1$
- The following table is all we need for simulating any Clifford evolution
  1. Conjugation by $CNOT$: $X_1 \rightarrow X_1X_2, X_2 \rightarrow X_2, Z_1 \rightarrow Z_1, Z_2 \rightarrow Z_1Z_2$
  2. Conjugation by H: $X \rightarrow Z, Z \rightarrow X$
  3. Conjugation by S: $X \rightarrow Y, Z \rightarrow Z$
  4. Conjugation by X: $X \rightarrow X, Z \rightarrow -Z$
  5. Conjugation by Y: $X \rightarrow -X, Z \rightarrow -Z$
  6. Conjugation by Z: $X \rightarrow -X, Z \rightarrow Z$
- $|00\rangle \Leftrightarrow \langle Z \otimes I, I \otimes Z\rangle$

- Simulate the evolution of the state $|\psi_{initial}\rangle = |00\rangle$ through $U = CNOT_{12}H_1$
- The following table is all we need for simulating any Clifford evolution
  1. Conjugation by $CNOT$: $X_1 \rightarrow X_1X_2, X_2 \rightarrow X_2, Z_1 \rightarrow Z_1, Z_2 \rightarrow Z_1Z_2$
  2. Conjugation by H: $X \rightarrow Z, Z \rightarrow X$
  3. Conjugation by S: $X \rightarrow Y, Z \rightarrow Z$
  4. Conjugation by X: $X \rightarrow X, Z \rightarrow -Z$
  5. Conjugation by Y: $X \rightarrow -X, Z \rightarrow -Z$
  6. Conjugation by Z: $X \rightarrow -X, Z \rightarrow Z$
- $|00\rangle \Leftrightarrow \langle Z \otimes I, I \otimes Z\rangle$
- After H, $\langle X \otimes I, I \otimes Z\rangle$

- Simulate the evolution of the state $|\psi_{initial}\rangle = |00\rangle$ through $U = CNOT_{12}H_1$
- The following table is all we need for simulating any Clifford evolution
  1. Conjugation by $CNOT$: $X_1 \rightarrow X_1X_2, X_2 \rightarrow X_2, Z_1 \rightarrow Z_1, Z_2 \rightarrow Z_1Z_2$
  2. Conjugation by H: $X \rightarrow Z, Z \rightarrow X$
  3. Conjugation by S: $X \rightarrow Y, Z \rightarrow Z$
  4. Conjugation by X: $X \rightarrow X, Z \rightarrow -Z$
  5. Conjugation by Y: $X \rightarrow -X, Z \rightarrow -Z$
  6. Conjugation by Z: $X \rightarrow -X, Z \rightarrow Z$
- $|00\rangle \Leftrightarrow \langle Z \otimes I, I \otimes Z\rangle$
- After H, $\langle X \otimes I, I \otimes Z\rangle$
- After $CNOT$, $\langle X \otimes X, Z \otimes Z\rangle$

- Simulate the evolution of the state $|\psi_{initial}\rangle = |00\rangle$ through $U = CNOT_{12}H_1$
- The following table is all we need for simulating any Clifford evolution
  1. Conjugation by $CNOT$: $X_1 \rightarrow X_1X_2, X_2 \rightarrow X_2, Z_1 \rightarrow Z_1, Z_2 \rightarrow Z_1Z_2$
  2. Conjugation by H: $X \rightarrow Z, Z \rightarrow X$
  3. Conjugation by S: $X \rightarrow Y, Z \rightarrow Z$
  4. Conjugation by X: $X \rightarrow X, Z \rightarrow -Z$
  5. Conjugation by Y: $X \rightarrow -X, Z \rightarrow -Z$
  6. Conjugation by Z: $X \rightarrow -X, Z \rightarrow Z$
- $|00\rangle \Leftrightarrow \langle Z \otimes I, I \otimes Z\rangle$
- After H, $\langle X \otimes I, I \otimes Z\rangle$
- After $CNOT$, $\langle X \otimes X, Z \otimes Z\rangle$
- The final stabilizer defines $|\psi_{final}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, so we simulated the evolution without computing $U|\psi_{initial}\rangle$

1. Michael A. Nielsen and Isaac L. Chuang, **Quantum Computation and Quantum Information**, Cambridge University Press (2000)
2. Daniel Gottesman, **PhD Thesis, arXiv:quant-ph/9705052**, preprint