Simulation of Stabilizer Circuits

A Mathematical Approach

Aeriana M. V. Narbonne

Dalhousie University

Winter 2021

Outline

Preliminaries

Definition

The **Dirac notation** can be used to represent states. Each state corresponds to a complex vector.

Example

We will represent quantum bits (qubits) zero and one are represented as follows:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Preliminaries

Definition

Quantum **gates** are unitary matrices.

Example

Hadamard gate

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

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Preliminaries

Definition

The **tensor product**, denoted by $\otimes$, is an operation of two matrices or vectors which results in a block matrix or vector.

$$A \otimes B = \begin{pmatrix} a_{1,1}B \dots a_{1,n}B \\ \vdots \ddots \vdots \\ a_{m,1}B \dots a_{m,n}B \end{pmatrix}$$

Example

We can use the tensor product to extend states and gates to multiple qubits. Given states $|0\rangle$ and $|1\rangle$ as defined above we can calculate the tensor product of the two states as follows:

$$|0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot 0 \\ 1 \cdot 1 \\ 0 \cdot 0 \\ 0 \cdot 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01\rangle$$

Preliminaries

Definition

Classical States, unlike quantum states, are those which are not in a superposition.

Example

For 2 bits, we have 2^2 classical states:

$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \quad |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \quad |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \quad |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Remark

For n qubits we 2^n classical states.

Preliminaries

Definition

A quantum state $|\phi\rangle$ is a complex linear combinations of basis states of the form

$$|\phi\rangle = \alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle$$

where:

$$|\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 + |\alpha_4|^2 = 1$$

In other words, they are unit vectors. A non-basis state is said to be in a **superposition**.

Example

Two common quantum states which we will use are "plus" and "minus".

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Preliminaries

Definition

Pauli matrices:

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

We have the following identities:

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

$$XY = iZ \quad YZ = iX \quad ZX = iY \quad YX = -iZ \quad ZY = -iX \quad XZ = -iY$$

Definition

The **Pauli group** $\mathscr{P}_n$ consists of matrices of the form $i^k P_1 \otimes ... \otimes P_n$ where $P_j \in \{I, X, Y, Z\}$

Preliminaries

Definition

The Clifford group (up to scalars) is the normalizer of the Pauli group, ie $\mathscr{C}_n = \{C \mid C\mathscr{P}_n C^{-1} \subset \mathscr{P}_n\}$

Example

$$H,\ CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \text{ and } S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \text{ are Clifford operators.}$$

Remark

If P is Pauli and C is Clifford, then $CPC^{-1} = Q$ is Pauli, ie the Clifford group acts on the Pauli group by conjugation.

Preliminaries

Definition

A quantum **circuit** is a sequence of gates acting on a set of qubits. Each gate acts on a subset of the qubits, and leaves the rest unchanged.

Definition

Clifford Circuits are quantum circuits in which every gate belongs to the Clifford group. They are generated by the following gates: $CNOT, H, S$.

Preliminaries

Definition

If P is a Pauli matrix and $|\phi\rangle$ is a state, we say that P **stabilizes** $|\phi\rangle$ if $P|\phi\rangle = |\phi\rangle$

Definition

We define the **stabilizer** of $|\phi\rangle$ as $stab(|\phi\rangle) = \{P \mid P|\phi\rangle = |\phi\rangle\}$

Definition

We say that $|\phi\rangle$ is a **stabilizer state** if $|\phi\rangle$ is uniquely defined (up to scalars) by its stabilizer.

Remark

$|\phi\rangle$ is a stabilizer state iff $|\phi\rangle = C|0\rangle$ for some Clifford operator C.

Preliminaries

Definition

Measurement in quantum computing describes collapsing a state in a superposition to a numeric outcome.

Example

Suppose we have a state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. We say $|\phi\rangle$ has a probability of $|\alpha|^2$ of outcome 0 and a probability of $|\beta|^2$ of outcome 1.

Example

Suppose we have a state $|\phi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \mu|11\rangle$. We say $|\phi\rangle$ has a probability of $|\alpha|^2 + |\beta|^2$ of outcome 0 and a probability of $|\gamma|^2 + |\mu|^2$ of outcome 1.

What is the significance of this talk?

Quantum computers cannot be simulated efficiently. Classical computers can simulate Clifford circuits.

This talk explains how.

Tableaux

Given a stabilizer state $|\phi\rangle$ a tableau for $|\phi\rangle$ is a list of $2n$ Pauli operators:

$$\left\{\begin{array}{c} \mathrm{D}_1 \\ \vdots \\ \mathrm{D}_n \\ \hline \mathrm{S}_1 \\ \vdots \\ \mathrm{S}_n \end{array}\right\}$$

1. $D_1, ..., D_n, S_1, ..., S_n$ generate the Pauli group
2. $S_1, ..., S_n$ generate the stabilizer of $|\phi\rangle$
3. $D_1, ..., D_n$ commute with each other
4. For $i, j \in \{1, ..., n\}$, D_i and S_j commute if $i \neq j$

Eigenvectors of Pauli Matrices

Matrix	Eigenvalue	Eigenvector
$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$+1$	$\lvert + \rangle = \frac{\lvert 0 \rangle + \lvert 1 \rangle}{\sqrt{2}}$
	-1	$\lvert - \rangle = \frac{\lvert 0 \rangle - \lvert 1 \rangle}{\sqrt{2}}$
$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$+1$	$\lvert + i \rangle = \frac{\lvert 0 \rangle + i \lvert 1 \rangle}{\sqrt{2}}$
	-1	$\lvert - i \rangle = \frac{\lvert 0 \rangle - i \lvert 1 \rangle}{\sqrt{2}}$
$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$+1$	$\lvert 0 \rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
	-1	$\lvert 1 \rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Stabilizer Algorithms

The idea of the simulated algorithm is: instead of keeping track of a quantum state $|\phi\rangle$ of 2^n complex vectors we keep track of its tableau of $2n$ Pauli operators.

Algorithm for Unitary (Clifford) Operations

To apply a unitary operator U to a state $|\phi\rangle$, replace:

$$T = \left\{\frac{D_1}{S_1}\right\} \quad by \quad T' = \left\{\frac{UD_1U^t}{US_1U^t}\right\}.$$

Theorem

If T is a tableau for $|\phi\rangle$, then T' is a tableau for $U|\phi\rangle$

Example of Unitary Operations

1. Consider the unitary operator $H = H^\dagger = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
2. Let $|\phi\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ and find the $stab(|\phi\rangle) = \{X, I\}$
3. The following is a tableau for $|\phi\rangle$:

$$\left\{ \frac{Z}{X} \right\}$$

   note the properties are satisfied.

4. A tableau for $H|\phi\rangle$ is:

$$\left\{ \frac{HZH^\dagger}{HXH^\dagger} \right\} = \left\{ \frac{X}{Z} \right\}$$

   .

5. We can verify that this is indeed a tableau for $H|+\rangle = |0\rangle$ by the fact that $+Z$ stabilizes $|0\rangle$ and X and Z do not commute.

Algorithm for Measurement

1. Consider the state $|\phi\rangle$ with a tableau

$$T = \left\{\begin{array}{c} D_1 \\ D_2 \\ \hline S_1 \\ S_2 \end{array}\right\} = \left\{\begin{array}{c} \tau_1 D_{1,1} \otimes D_{1,2} \\ \tau_2 D_{2,1} \otimes D_{2,2} \\ \hline \sigma_1 S_{1,1} \otimes S_{1,2} \\ \sigma_2 S_{2,1} \otimes S_{2,2} \end{array}\right\}$$

   where $\sigma_j, \tau_j \in \{+1, -1\}$ and $D_{j,k}, S_{j,k} \in \{I, X, Y, Z\}$
2. Set k equal to the qubit we wish to measure. For example, if we had a 2 dimensional qubit we would then set $k = 0$ for leftmost or $k = 1$ for rightmost.
3. Now, we determine whether probabilistic or deterministic. To measure the k^{th} qubit, check whether there exists $q \in \{1, ..., n\}$ such that $S_{q,k} \in \{X, Y\}$. If no it is determinate; if yes then it is probabilistic.

Algorithm for Measurement - Case 1

if yes: CASE I - Probabilistic

- Let q be the smallest index such that $q \in \{1, ..., n\}$ such that $\mathrm{S}_{q,k} \in \{\mathrm{X, Y}\}$
- Randomly select bit $r \in \{0, 1\}$ uniformly distributed. This will serve as the outcome of the simulated measurement
- Define the updated tableau as follows.
  For each $i \neq q$:

$$D_i' = \begin{cases} D_i & \text{if } D_{i,k} \in \{\mathrm{I, Z}\} \\ D_i \mathrm{S}_q & \text{otherwise} \end{cases}$$

$$\mathrm{S}_i' = \begin{cases} S_i & \text{if } S_{i,q} \in \{\mathrm{I, Z}\} \\ \mathrm{S}_i S_q & \text{otherwise} \end{cases}$$

- $D_q = S_q$
- $S_q = (-1)^r I \otimes ... \otimes I \otimes Z \otimes I ... \otimes I$ where Z is placed at the k^{th} qubit.

Algorithm for Measurement - Case 2

if no: CASE II - Determinate:

- Let $J = \{i \mid D_{i,k} \in \{X, Y\}\}$
- Let $P = \prod_{i \in J} S_i$
- Then $P = (-1)^r P_1 \otimes ... \otimes P_n$
- Measurement result is 0 if $+P$, or 1 if $-P$

Remark

In this case, we do not update the tableau.

Example of Measurement

1. Consider $|\phi\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}$
2. First, it is important to recognize that this state can be written as: $|\phi\rangle = |+\rangle \otimes |0\rangle$
3. $stab(|\phi\rangle) = \{I \otimes I, I \otimes Z, X \otimes I, X \otimes Z\}$, hence

$$T = \left\{\begin{array}{c} X \otimes X \\ Z \otimes I \\ \hline I \otimes Z \\ X \otimes I \end{array}\right\}$$

We will first do an example of case 1, then an example of case 2.

Measurement - Case 1

$$T = \left\{\begin{array}{c} \text{X} \otimes X \\ \text{Z} \otimes I \\ \hline \text{I} \otimes Z \\ \text{X} \otimes I \end{array}\right\} \longrightarrow \left\{\begin{array}{c} (\text{X} \otimes X)(X \otimes I) \\ \text{Z} \otimes I \\ \hline \text{I} \otimes Z \\ \text{X} \otimes I \end{array}\right\} = \left\{\begin{array}{c} (\text{I} \otimes X) \\ \text{Z} \otimes I \\ \hline \text{I} \otimes Z \\ \text{X} \otimes I \end{array}\right\}$$

1. To measure the 1st qubit, we set $k = 1$
2. We now check for $q \in \{1, 2\}$ such that $\text{S}_{q,1} \in \{\text{X, Y}\}$ We find $q = 2$ such that $S_{2,1} = X$.
   If **yes**, then case 1.
3. For all $i \neq 2$ and if $S_{1,1},\ D_{1,1} \in \{X, Y\}$ we multiply by $S_2 = X \otimes I$.

Measurement - Case 1 (continued)

$$\left\{\begin{array}{c}(\mathrm{I} \otimes X) \\ \mathrm{Z} \otimes I \\ \hline \mathrm{I} \otimes Z \\ \mathrm{X} \otimes I\end{array}\right\} \longrightarrow \left\{\begin{array}{c}\mathrm{I} \otimes X \\ (\mathrm{X} \otimes I) \\ \hline \mathrm{I} \otimes Z \\ \mathrm{X} \otimes I\end{array}\right\} \longrightarrow \left\{\begin{array}{c}\mathrm{I} \otimes X \\ \mathrm{X} \otimes I \\ \hline \mathrm{I} \otimes Z \\ (\mathrm{Z} \otimes I)\end{array}\right\}$$

1. we replace D_2 by S_2
2. We randomly select $r = 0$ or 1. Suppose we select $r = 0$
3. we replace S_2 by $Z \otimes I$

The updated tableau is a tableau for the state $|00\rangle$

Example of Measurement - Case 2

$$|\phi\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}, \quad T = \left\{\begin{array}{c} \mathrm{X} \otimes X \\ \mathrm{Z} \otimes I \\ \hline \mathrm{I} \otimes Z \\ \mathrm{X} \otimes I \end{array}\right\}$$

1. To measure the 2nd qubit, we set $k = 2$
2. We now check for $q \in \{1, 2\}$ such that $\mathrm{S}_{q,2} \in \{\mathrm{X}, \mathrm{Y}\}$.
   If **no**, then case 2.
3. Let $J = \{i \mid D_{i,k} \in \{X, Y\}\} = \{1\}$.
4. Let $P = \prod_{i \in J} S_i = I \otimes Z$.
5. Then $P = (-1)^r P_1 \otimes ... \otimes P_n \implies r = 0$.
6. Therefore the measurement result is 0.

Correctness of Algorithm - Case 1

There are a couple reasons why this algorithmn is correct.

1. For all k, n there cannot exists $S_{i,k}$ such that $S_{i,k} \in \{X, Y, Z\}$ and $S_{i,k-n} \in \{X, Y, Z\} \setminus S_{i,k}$
   $\implies$ once updated, the tableau still satisfies the properties.
2. X, Y have eigenvectors superposition
   $\implies$ the algorithm targets specifically these rows to be updated.
3. $r = 0 \implies (-1)^0 Z$ where $|0\rangle$ is the eigenvector of $+Z$
   $r = 1 \implies (-1)^1 Z$ where $|1\rangle$ is the eigenvector of $-Z$
   $\implies$ Selecting r determines the outcome