Quantum Algorithms tutorial 2

Postulates of quantum mechanics and circuit evaluation

Casper Gyurik

Leiden Institute of Advanced Computer Science

September 12th, 2019

Universiteit Leiden
The Netherlands

Postulates of quantum mechanics

Refresher: how to work with different bases

Evaluating a quantum circuit

Solovay Kitaev theorem

The postulates of quantum mechanics

What are the rules of quantum computing?

Postulate 1: State space

Associated to any physical system is a complex vector space $\mathbb{C}^N$ called the *state space*. The system is completely described by the *state vector*, which is a unit vector in the state space $|\psi\rangle \in \mathbb{C}^N$.

The postulates of quantum mechanics

What are the rules of quantum computing?

Postulate 1: State space

Associated to any physical system is a complex vector space $\mathbb{C}^N$ called the *state space*. The system is completely described by the *state vector*, which is a unit vector in the state space $|\psi\rangle \in \mathbb{C}^N$.

The state spaces and state vectors we will work with are

- A qubit system, who is completely described by the state vector

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \in \mathbb{C}^2.$$

The postulates of quantum mechanics

What are the rules of quantum computing?

Postulate 1: State space

Associated to any physical system is a complex vector space $\mathbb{C}^N$ called the *state space*. The system is completely described by the *state vector*, which is a unit vector in the state space $|\psi\rangle \in \mathbb{C}^N$.

The state spaces and state vectors we will work with are

- A qubit system, who is completely described by the state vector

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \in \mathbb{C}^2.$$

- An n-qubit system, which is completely described by the state vector

$$|\psi\rangle = \sum_{j\in\{0,1\}^n} \alpha_j\,|j\rangle \in \left(\mathbb{C}^2\right)^{\otimes n} \cong \mathbb{C}^{2^n}.$$

The postulates of quantum mechanics

What are the rules of quantum computing?

Postulate 2: Evolution

The evaluation of a quantum system is described by *unitary* transformation.

The postulates of quantum mechanics

What are the rules of quantum computing?

Postulate 2: Evolution

The evaluation of a quantum system is described by *unitary* transformation.

That is, the state of a qubit system $|\psi\rangle$ at some time t_1 is related to the state $|\psi'\rangle$ of the same system at some time $t_2 > t_1$ by a unitary matrix U via

$$|\psi'\rangle = U\,|\psi\rangle\,.$$

The postulates of quantum mechanics

What are the rules of quantum computing?

Postulate 2: Evolution

The evaluation of a quantum system is described by *unitary* transformation.

That is, the state of a qubit system $|\psi\rangle$ at some time t_1 is related to the state $|\psi'\rangle$ of the same system at some time $t_2 > t_1$ by a unitary matrix U via

$$|\psi'\rangle = U\,|\psi\rangle\,.$$

So, we are only allowed to apply unitary matrices to qubits during computation.

The postulates of quantum mechanics

What are the rules of quantum computing?

Postulate 2: Evolution

The evaluation of a quantum system is described by *unitary* transformation.

That is, the state of a qubit system $|\psi\rangle$ at some time t_1 is related to the state $|\psi'\rangle$ of the same system at some time $t_2 > t_1$ by a unitary matrix U via

$$|\psi'\rangle = U\,|\psi\rangle\,.$$

So, we are only allowed to apply unitary matrices to qubits during computation.

Characterizations of unitary matrices

- U is unitary $\iff$ U is norm-preserving.
- U is unitary $\iff$ the columns of U form orthonormal basis for $\mathbb{C}^n$.
- U is unitary $\iff$ $U^\dagger U = UU^\dagger = I$, where I is the identity and $U^\dagger = \overline{U}^T$.

The postulates of quantum mechanics

What are the rules of quantum computing?

Postulate 2: Evolution

The evaluation of a quantum system is described by *unitary* transformation.

That is, the state of a qubit system $|\psi\rangle$ at some time t_1 is related to the state $|\psi'\rangle$ of the same system at some time $t_2 > t_1$ by a unitary matrix U via

$$|\psi'\rangle = U\,|\psi\rangle\,.$$

So, we are only allowed to apply unitary matrices to qubits during computation.

Characterizations of unitary matrices

- U is unitary $\iff$ U is norm-preserving.
- U is unitary $\iff$ the columns of U form orthonormal basis for $\mathbb{C}^n$.
- U is unitary $\iff$ $U^\dagger U = UU^\dagger = I$, where I is the identity and $U^\dagger = \overline{U}^T$.

Exercise: U norm-preserving $\implies$ U is invertible.

The postulates of quantum mechanics

What are the rules of quantum computing?

Postulate 3: Measurement in the computational basis

If the system is in state $|\psi\rangle$ immediately before a measurement, then the probability that result φ occurs is given by the *Born rule*:

$$\Pr(\varphi) = |\langle\varphi \mid \psi\rangle|^2,$$

The postulates of quantum mechanics

What are the rules of quantum computing?

Postulate 3: Measurement in the computational basis

If the system is in state $|\psi\rangle$ immediately before a measurement, then the probability that result φ occurs is given by the *Born rule*:

$$\mathsf{Pr}(\varphi) = |\langle \varphi \mid \psi \rangle|^2,$$

E.g., for a single qubit state $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ we recover that

$$\mathsf{Pr}(0) = |\langle 0 \mid \psi \rangle|^2 = |\alpha|^2.$$

The postulates of quantum mechanics

What are the rules of quantum computing?

Postulate 3: Measurement in the computational basis

If the system is in state $|\psi\rangle$ immediately before a measurement, then the probability that result φ occurs is given by the *Born rule*:

$$\mathsf{Pr}(\varphi) = |\langle \varphi \mid \psi \rangle|^2,$$

E.g., for a single qubit state $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ we recover that

$$\mathsf{Pr}(0) = |\langle 0 \mid \psi \rangle|^2 = |\alpha|^2.$$

Moreover, for an n-qubit state $|\psi\rangle = \sum_{j \in \{0,1\}^n} \alpha_j |j\rangle$ we recover that

$$\mathsf{Pr}(j) = |\langle j \mid \psi \rangle|^2 = |\alpha_j|^2.$$

The postulates of quantum mechanics

What are the rules of quantum computing?

Postulate 3: Measurement in the computational basis

If the system is in state $|\psi\rangle$ immediately before a measurement, then the probability that result φ occurs is given by the *Born rule*:

$$\Pr(\varphi) = |\langle\varphi \mid \psi\rangle|^2,$$

E.g., for a single qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ we recover that

$$\Pr(0) = |\langle 0 \mid \psi\rangle|^2 = |\alpha|^2.$$

Moreover, for an n-qubit state $|\psi\rangle = \sum_{j\in\{0,1\}^n} \alpha_j |j\rangle$ we recover that

$$\Pr(j) = |\langle j \mid \psi\rangle|^2 = |\alpha_j|^2.$$

Note: this motivates these α's being called *probability amplitudes*.

The postulates of quantum mechanics

What are the rules of quantum computing?

Postulate 3: Measurement in the computational basis

If the system is in state $|\psi\rangle$ immediately before a measurement, then the probability that result φ occurs is given by the *Born rule*:

$$\mathsf{Pr}(\varphi) = |\langle \varphi \mid \psi \rangle|^2,$$

E.g., for a single qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ we recover that

$$\mathsf{Pr}(0) = |\langle 0 \mid \psi \rangle|^2 = |\alpha|^2.$$

Moreover, for an n-qubit state $|\psi\rangle = \sum_{j \in \{0,1\}^n} \alpha_j |j\rangle$ we recover that

$$\mathsf{Pr}(j) = |\langle j \mid \psi \rangle|^2 = |\alpha_j|^2.$$

Note: this motivates these α's being called *probability amplitudes*.

More on the postulates in N&C chapters 2.2.1-2.2.3

Working with different bases

Expressing vectors in different bases

For single qubit states, we know the following two bases:

Computational basis:

$$\{|0\rangle, |1\rangle\}.$$

Hadamard basis:

$$\{|+\rangle, |-\rangle\}.$$

Working with different bases

Expressing vectors in different bases

For single qubit states, we know the following two bases:

Computational basis:	**Hadamard basis**:
$\{\|0\rangle, \|1\rangle\}.$	$\{\|+\rangle, \|-\rangle\}.$

- Consider an arbitrary single qubit state

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle .$$

Working with different bases

Expressing vectors in different bases

For single qubit states, we know the following two bases:

Computational basis:	**Hadamard basis**:
$\{\|0\rangle, \|1\rangle\}$.	$\{\|+\rangle, \|-\rangle\}$.

- Consider an arbitrary single qubit state

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle .$$

- We can rewrite this vector *in the Hadamard basis* as

$$|\psi\rangle = \alpha_+ |+\rangle + \alpha_- |-\rangle .$$

where we can compute the values α_+ and α_- using

$$\alpha_+ = \langle + \mid \psi\rangle \text{ and } \alpha_- = \langle - \mid \psi\rangle .$$

Working with different bases

Expressing vectors in different bases

For single qubit states, we know the following two bases:

Computational basis:	**Hadamard basis**:
$\{\|0\rangle, \|1\rangle\}.$	$\{\|+\rangle, \|-\rangle\}.$

- Consider an arbitrary single qubit state
$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle .$$
- We can rewrite this vector *in the Hadamard basis* as
$$|\psi\rangle = \alpha_+ |+\rangle + \alpha_- |-\rangle .$$
where we can compute the values α_+ and α_- using
$$\alpha_+ = \langle + \mid \psi\rangle \text{ and } \alpha_- = \langle - \mid \psi\rangle .$$

Example

Consider $|\psi\rangle = |1\rangle$, then $\langle + \mid \psi\rangle = \frac{1}{\sqrt{2}}$ and $\langle - \mid \psi\rangle = -\frac{1}{\sqrt{2}}$ and thus
$$|1\rangle = \frac{1}{\sqrt{2}} |+\rangle - \frac{1}{\sqrt{2}} |-\rangle .$$

Working with different bases

Expressing vectors in different bases

For n-qubit states, we know the following two bases:

Computational basis:

$$\{|j\rangle \mid j \in \{0,1\}^n\}.$$

Hadamard basis:

$$\{|c\rangle \mid c \in \{+,-\}^n\}.$$

Working with different bases

Expressing vectors in different bases

For n-qubit states, we know the following two bases:

Computational basis:	**Hadamard basis**:
$\{\|j\rangle \mid j \in \{0,1\}^n\}\,.$	$\{\|c\rangle \mid c \in \{+,-\}^n\}\,.$

- Consider an arbitrary n-qubit state

$$|\psi\rangle = \sum_{j\in\{0,1\}^n} \alpha_j \, |j\rangle\,.$$

Working with different bases

Expressing vectors in different bases

For n-qubit states, we know the following two bases:

Computational basis: $\{\lvert j\rangle \mid j \in \{0,1\}^n\}$.	**Hadamard basis**: $\{\lvert c\rangle \mid c \in \{+,-\}^n\}$.

- Consider an arbitrary n-qubit state

$$\lvert\psi\rangle = \sum_{j\in\{0,1\}^n} \alpha_j \lvert j\rangle .$$

- We can rewrite this vector *in the Hadamard basis* as

$$\lvert\psi\rangle = \sum_{c\in\{+,-\}^n} \alpha_c \lvert c\rangle ,$$

where we can compute the values α_c using

$$\alpha_c = \langle c \mid \psi\rangle .$$

Working with different bases

Expressing vectors in different bases

For n-qubit states, we know the following two bases:

Computational basis:	**Hadamard basis**:
$\{\|j\rangle \mid j \in \{0,1\}^n\}\,.$	$\{\|c\rangle \mid c \in \{+,-\}^n\}\,.$

- Consider an arbitrary n-qubit state

$$|\psi\rangle = \sum_{j \in \{0,1\}^n} \alpha_j |j\rangle\,.$$

- We can rewrite this vector *in the Hadamard basis* as

$$|\psi\rangle = \sum_{c \in \{+,-\}^n} \alpha_c |c\rangle\,,$$

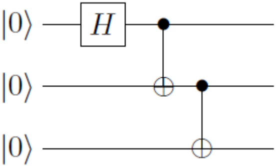
where we can compute the values α_c using

$$\alpha_c = \langle c \mid \psi\rangle\,.$$

Exercise: rewrite $|\psi\rangle = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle$ in the Hadamard basis.

Evaluating a quantum circuit

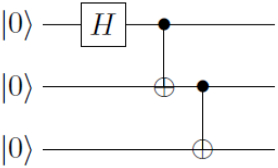
How do we compute its output?



Initial state: $|\psi\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle = |000\rangle$.

Evaluating a quantum circuit

How do we compute its output?

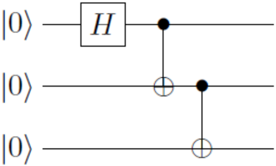


Initial state: $|\psi\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle = |000\rangle$.
After first layer of gates:

$$\begin{aligned} |\psi\rangle &= (H \otimes I \otimes I)(|0\rangle \otimes |0\rangle \otimes |0\rangle) = H\,|0\rangle \otimes |0\rangle \otimes |0\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |100\rangle) \end{aligned}$$

Evaluating a quantum circuit

How do we compute its output?



Initial state: $|\psi\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle = |000\rangle$.
After first layer of gates:

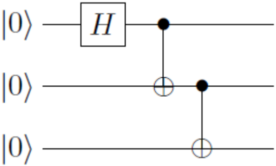
$$\begin{aligned} |\psi\rangle &= (H \otimes I \otimes I)(|0\rangle \otimes |0\rangle \otimes |0\rangle) = H|0\rangle \otimes |0\rangle \otimes |0\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |100\rangle) \end{aligned}$$

After second layer of gates:

$$|\psi\rangle = (CNOT \otimes I)\frac{1}{\sqrt{2}}(|000\rangle + |100\rangle) = \frac{1}{\sqrt{2}}(|000\rangle + |110\rangle).$$

Evaluating a quantum circuit

How do we compute its output?



Initial state: $|\psi\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle = |000\rangle$.
After first layer of gates:

$$|\psi\rangle = (H \otimes I \otimes I)(|0\rangle \otimes |0\rangle \otimes |0\rangle) = H|0\rangle \otimes |0\rangle \otimes |0\rangle$$
$$= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |100\rangle)$$

After second layer of gates:

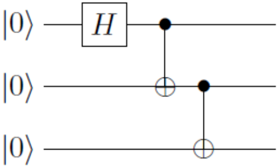
$$|\psi\rangle = (CNOT \otimes I)\frac{1}{\sqrt{2}}(|000\rangle + |100\rangle) = \frac{1}{\sqrt{2}}(|000\rangle + |110\rangle).$$

After final layer of gates:

$$|\psi\rangle = (I \otimes CNOT)\frac{1}{\sqrt{2}}(|000\rangle + |110\rangle) = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

Evaluating a quantum circuit

How do we compute its output?



After final layer of gates:

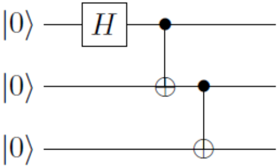
$$|\psi\rangle = (I \otimes CNOT)\frac{1}{\sqrt{2}}(|000\rangle + |110\rangle) = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

Measurement outcome probabilities:

$$\mathsf{Pr}(000) = \mathsf{Pr}(111) = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}.$$

Evaluating a quantum circuit

How do we compute its output?



After final layer of gates:

$$|\psi\rangle = (I \otimes CNOT)\frac{1}{\sqrt{2}}(|000\rangle + |110\rangle) = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

Measurement outcome probabilities:

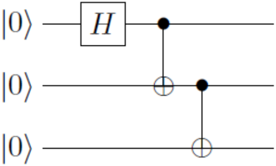
$$\mathsf{Pr}(000) = \mathsf{Pr}(111) = |\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}.$$

Matrix corresponding to the above circuit:

$$U = (I \otimes CNOT) \cdot (CNOT \otimes I) \cdot (H \otimes I \otimes I).$$

Evaluating a quantum circuit

How do we compute its output?



After final layer of gates:

$$|\psi\rangle = (I \otimes CNOT)\frac{1}{\sqrt{2}}(|000\rangle + |110\rangle) = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

Measurement outcome probabilities:

$$\mathsf{Pr}(000) = \mathsf{Pr}(111) = |\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}.$$

Matrix corresponding to the above circuit:

$$U = (I \otimes CNOT) \cdot (CNOT \otimes I) \cdot (H \otimes I \otimes I).$$

More on quantum circuits in N&C chapters 1.2-1.3, 4.1-4.4 and 4.6

For classical computation, we have the following universality statement.

Universality of a set of logical gates

Any Boolean function can be computed by a Boolean circuit that only involves fanouts and the logical gates AND, OR and NOT.

For classical computation, we have the following universality statement.

Universality of a set of logical gates

Any Boolean function can be computed by a Boolean circuit that only involves fanouts and the logical gates `AND`, `OR` and `NOT`.

In quantum computation we have the following counterpart.

Universality of a set of quantum gates

Any unitary operation can we approximated to arbitrary accuracy by a quantum circuit only involving single qubit gates and $CNOT$.

For classical computation, we have the following universality statement.

Universality of a set of logical gates

Any Boolean function can be computed by a Boolean circuit that only involves fanouts and the logical gates `AND`, `OR` and `NOT`.

In quantum computation we have the following counterpart.

Universality of a set of quantum gates

Any unitary operation can we approximated to arbitrary accuracy by a quantum circuit only involving single qubit gates and $CNOT$.

This implies that for quantum computation it is sufficient to only consider quantum circuits involving single qubit gates and $CNOT$.

Solovay Kitaev theorem

Universality of set of quantum gates

For classical computation, we have the following universality statement.

Universality of a set of logical gates

Any Boolean function can be computed by a Boolean circuit that only involves fanouts and the logical gates `AND`, `OR` and `NOT`.

In quantum computation we have the following counterpart.

Universality of a set of quantum gates

Any unitary operation can we approximated to arbitrary accuracy by a quantum circuit only involving single qubit gates and $CNOT$.

This implies that for quantum computation it is sufficient to only consider quantum circuits involving single qubit gates and $CNOT$.
Moreover, it turns out that the set $\{H, R_{\pi/8}\}$ is universal for single qubit gates.