Unitary Operators

By using a quantum circuit, any problem in \textbf{NP} can be solved with a nonvanishing correctness probability in time

\[ O\left(\sqrt{2^n} p(n)\right) \]

Where \( p \) is polynomial depending on the particular problem.
Question

- Why can a quantum algorithm improve on NP problems in $O\left(\sqrt{2^n p(n)}\right)$ and not $O(np(n))$?
  - We have Quantum Parallelism and the results...
  - But we can not obtain the results

- Why is it so difficult to obtain the results?
- Lets look into the evolution of our system..

Unitary Evolution

- If the Hamiltonian is time independent, and the computer is started off with memory register in the state $|\Psi(0)\rangle$, then we can write the general solution of the Schrödinger equation as
  \[
  |\Psi(t)\rangle = e^{-i\hat{H}t/\hbar} |\Psi(0)\rangle = \hat{U}(t) |\Psi(0)\rangle
  \]

- Where $\hat{U}(t) = e^{i\hat{H}t/\hbar}$ is called the evolution operator
The operator $U(t)$ is always a **unitary matrix**

- The conjugate transpose is equal to its inverse

**Important implication**
- It means that the evolution operator of an ideal quantum computer, isolated from environment, is **reversible**
- Any ideal quantum computer must be also reversible

Hamilton operator is known (represents the total energy of the system)
- Schrodinger equation is used to determine the energy eigenstates, which form the basis states of a quantum system
  - Time evolution which is described by $U_i$ is continuous
  - We interested in the state of the system a discrete time points $t_1$, $t_2$, $t_3$, ....
- Therefore we will regard the evolution as a sequence of init-length vectors $x$, $U_1 x$, $U_2 U_1 x$, $U_3 U_2 U_1 x$, $U_i$ is unitary
Description of quantum circuit everything to simulate a quantum computer
- Description tells us what transformation will be effected on any given input state
- It does not embody any dynamics
- Quantum computer is a physical system whose evolution over time can be interpreted
- Circuit level tells us what the evolution has look like
- Embody the computation in dynamical process, Schrodinger equation

Composed of quantum circuits, they describe the computation
- The overall unitary transformation achieved by the circuits can be written as
  \( A_k A_{k-1} \cdots A_1 \) where \( A_i \) is the operator describing the \( i \)th gate
- Notice: \( A_2 A_1 \neq A_1 A_2 \)
Compound systems

- Suppose we have \( n \) and \( m \)-states
  \[
  \{|x_i\}, |x_2\}, \ldots, |x_n\}\rangle \quad \text{of} \quad H_n
  \]
  \[
  \{|y_i\}, |y_2\}, \ldots, |y_m\rangle \quad \text{of} \quad H_m
  \]
  - The compound system is described as a tensor product
    \[
    H_n \otimes H_m \cong H_{nm}
    \]
  - With the basis states
    \[
    |x_i\rangle \otimes |y_j\rangle = |x_i, y_j\rangle \quad i \in \{1, \ldots, n\} \quad j \in \{1, \ldots, m\}
    \]
**New Basis**

A general state of a 2-bit memory register is

\[
\begin{align*}
|00\rangle &= \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},
|01\rangle &= \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},
|10\rangle &= \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix},
|11\rangle &= \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}
\end{align*}
\]

Generalization is straightforward

**Measurement**

The initial state of the system is projected to the subspace that corresponds to the observed state (highest amplitude) and renormalized to the unit length.

Projection is **not consistent with the unitary time evolution**

- Since unitary evolution is always reversible, but there is now way to recover from a projection
- No explanation exists
  - (Measurement paradox)
After the projection, information about all other states is lost

In the Deutsch-Jozsa problem, we are given a black box quantum computer known as an oracle that implements the function. We are promised that the function \( f : \{0,1\} \rightarrow \{0,1\} \) is either constant (0 on all inputs or 1 on all inputs) or balanced (returns 1 for half of the input domain and 0 for the other half); the task then is to determine if \( f \) is constant or balanced by utilizing the oracle.
Evaluation of oracle $f$. Is it balanced?

$$H_n|0\rangle|0\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{F}_2^n} |x\rangle|0\rangle$$

- How can we obtain the values of $f(x)$?

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{F}_2^n} |x\rangle|0 \oplus f(x)\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{F}_2^n} |x\rangle|f(x)\rangle$$

⊕ means addition modulo 2, exclusive or operation

- We do not need the target bit anymore!

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle y \mid x \rangle} |x\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$
Finally we examine the probability of measuring

\[ \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \sum_{y=0}^{2^n-1} (-1)^{x\cdot y} |y\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left[ \sum_{x=0}^{2^n-1} (-1)^{f(x)}(-1)^{x\cdot y} \right] |y\rangle \]

which evaluates to 1 if \( f(x) \) is constant and 0 if \( f(x) \) is balanced

- We used the Hadamard matrix
- We mapped the \( f \) values into the amplitude
- Value of each \( f \) contributed to the amplitude
  - “Same” idea for Shor’s factorization algorithm
Why:

- Quantum Fourier Transform corresponds to a Hadamard matrix!
- QFT is also called a Hadamard-Walsh transform, where each element (of the group $\mathbb{Z}_n$) after QFT is represented as

$$N_j(x) = e^{\frac{2\pi i j x}{n}}$$

and

$$|x\rangle \rightarrow \sum_{y=0}^{n-1} e^{\frac{2\pi i n y}{n}} |y\rangle$$

$\H_2$

$W_2 = H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$H_2 |0\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$

$H_2 |1\rangle = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle$

$W_2$, $H_2$ is called Walsh matrix, Hadamard matrix or Hamarad-Walsh matrix

$$W_2 \left( \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right) = \frac{1}{\sqrt{2}} W_2 |0\rangle + \frac{1}{\sqrt{2}} W_2 |1\rangle = \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = |0\rangle$$
Hadamard matrix

- $H_n = H_2 \otimes H_2 \otimes \ldots \otimes H_2$ $n$ times

$$H_n |z\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in F_2^n} (-1)^{z \cdot x} |x\rangle$$

$z \cdot x = z_1 x_1 + \cdots + z_n x_n$

- $H_n$ is called Hadamard matrix

$$H_2 = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$

$$H_4 = \begin{bmatrix} H_2 & H_2 \\ -H_2 & H_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$
http://www.iasri.res.in/webhadamard/

\[
\begin{array}{cccc}
1 & 1 & 1 & 1 \\
1-1 & 1-1 \\
1 & 1-1-1 \\
1-1-1 & 1 \\
\end{array}
\]

- Is \( f_y(x) = 1 \) for any of the elements?
Another idea

Suppose we “just” want to test if a $f_y(x) = 1$ exists or not

If it does not exist than $f_y(x) = 0$ for all $x$

$$
\sum_{x \in \mathbb{F}_2^n} (-1)^{f_y(x)}|x\rangle
= \frac{1}{\sqrt{2^n}} H_n \left( \sum_{x \in \mathbb{F}_2^n} |x\rangle \right)
= |0\rangle
$$

And we are sure!

But....
We separate $|0\rangle$ from all other state by designing a function $f_0 : F_2^n \rightarrow F_2$.

- It gets a 1 for $0$ and 0 for all other values.
- Such a function is possible to construct

$$\left(1 - \frac{2}{2^n}\right)|0\rangle - \frac{2}{2^n} \sum_{x \neq 0} (-1)^x |x\rangle |0\rangle$$

The observation of the last qubit results in $|0\rangle|1\rangle$.

With a probability

$$\left(1 - \frac{2}{2^n}\right)^2 = 1 - \frac{4}{2^n} + \frac{4}{2^{2n}}$$
\[
\left(1 - \frac{2}{2^n}\right)\lvert \theta \rangle \lvert 0 \rangle - \frac{2}{2^n} \sum_{x=0}^{2^n-1} (-1)^x \lvert x \rangle \lvert 0 \rangle
\]

- And the observation of the last qubit results in

\[
\frac{1}{\sqrt{2^n - 1}} \sum_{x=0}^{2^n-1} (-1)^x \langle x | \langle 0 | = \frac{1}{\sqrt{2^n - 1}} \left( \sum_{x \in \mathbb{F}_2} (-1)^x \langle x | - \langle \theta | \right) \langle 0 |
\]

- With a probability
  - (both probabilities are 1)

\[
1 - \left(1 - \frac{2}{2^n}\right)^2 = \frac{4}{2^n} - \frac{4}{2^{2n}}
\]

- What is the problem?

  - There is still a higher probability to measuring the state \(\lvert 0 \rangle\)
  - Why, because one dimension has not a big impact on changing the amplitude
  - \(H_n\) is “just” a linear mapping!
  - Can we amplify this linear mapping?
    - Yes, but only a little....
Orthogonal Subspace

- Let be $W$ a subspace of $H$, then we have as well an orthogonal subspace, which is called the orthogonal complement of $W$

$$W^\perp = \{ y \in H | \langle y | x \rangle = 0 \}$$

$$H = W \oplus W^\perp$$

- If $v$ is given as a column unit vector
- $I$ is the identity matrix

$$Q = I - 2vv^*.$$  

- The linear transformation described above is given by the Householder matrix
- $Q$ is unitary
The mapping $Qx$

$$Qx = x - 2vv^*x = x - 2\langle v, x \rangle v,$$

- Reflects $x$ on the hyperplane which is defined by a unit vector $v$ that is orthogonal to the hyperplane.
- $\langle v, x \rangle$ is equal to the distance from $x$ to the hyperplane.
Grover’s Amplification

- Operators which we will use:
  - We need a query operator which calls for value \( f_y \) uses \( n \) qubits for the source register and one target bit \( y \in F_2^n \)
    \[
    V_f |x\rangle = (-1)^{f(x)} |x\rangle
    \]
    \[
    f_y(x) = \begin{cases} 
      1, & \text{if } x = y \\
      0, & \text{otherwise} 
    \end{cases}
    \]
  - We need a quantum operator \( R_n \) defined on \( n \) qubits and operating as
    \[
    R_n |0\rangle = -|0\rangle \quad \text{and} \quad R_n |x\rangle = |x\rangle, x \neq 0
    \]

Amplitude Amplification

- Finding \( y \) by the quantum operator
  - \( G_n = H_n R_n H_n V_f \)
  - Working on \( n \) qubits representing elements \( x \)
  - \( H_n R_n H_n \) can be written as a \( 2^n \times 2^n \) matrix
  \[
  H_n R_n H_n = \begin{pmatrix} 
  1 & -2^n & 2^n & -2^n & \cdots & -2^n \\
  -2^n & 2^n & -2^n & 2^n & \cdots & -2^n \\
  2^n & -2^n & 2^n & -2^n & \cdots & -2^n \\
  \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\
  -2^n & 2^n & -2^n & 2^n & \cdots & 1-2^n \\
  -2^n & 2^n & -2^n & 2^n & \cdots & 1-2^n \\
  \end{pmatrix}
  \]
\( H_n R_n H_n \) can be also expressed as

\[ H_n R_n H_n = I - 2P \]

Where \( I \) is a \( 2^n \times 2^n \) identity matrix and \( P \) is a \( 2^n \times 2^n \) projection matrix whose every entry is \( 1/2^n \).

\( P \) represents a projection into a one dimensional subspace generated by

\[
\psi = \frac{1}{\sqrt{2^n}} \sum_{x \in F_2^n} |x\rangle
\]

\[
P = |\psi\rangle\langle\psi|\]
Therefore

\[ P \sum_{x \in F_2^n} c_x |x\rangle = A \sum_{x \in F_2^n} |x\rangle \]

and

\[ -H \cdot R \cdot H \sum_{x \in F_2^n} c_x |x\rangle = (2P - I) \sum_{x \in F_2^n} c_x |x\rangle \]

\[ (2P - I) \sum_{x \in F_2^n} c_x |x\rangle = 2A \sum_{x \in F_2^n} |x\rangle - \sum_{x \in F_2^n} c_x |x\rangle \]

\[ 2A \sum_{x \in F_2^n} |x\rangle - \sum_{x \in F_2^n} c_x |x\rangle = \sum_{x \in F_2^n} (2A - c_x) |x\rangle \]

\[
\begin{align*}
\frac{1}{\sqrt{2^n}} \mapsto 2A - \frac{1}{\sqrt{2^n}} = \frac{1}{\sqrt{2^n}} \\
\frac{-1}{\sqrt{2^n}} \mapsto 2A + \frac{1}{\sqrt{2^n}} = 3 \cdot \frac{1}{\sqrt{2^n}}
\end{align*}
\]
- We get an amplification, but only in a linear way
- We indicate, which part to amplify by a minus sign
- But the amplification is related to the number of state in which we search
- With to many states it is minimal

\[ \text{amplification} + \frac{1}{{\sqrt{2}^n}} \text{, versus } - \frac{1}{{\sqrt{2}^n}} \]

- Can we do it better?
- Until now, we can’t :-(

- To find following mapping corresponds to the statement, that we can solve \textbf{NP} problems in \textbf{P} on a quantum computer
Remember?

- Another quantum gate

\[
\sqrt{M} = \begin{pmatrix}
\frac{1+i}{2} & \frac{1-i}{2} \\
\frac{1-i}{2} & \frac{1+i}{2}
\end{pmatrix}
\]

\[
\sqrt{M} |0\rangle = \frac{1+i}{2} |0\rangle + \frac{1-i}{2} |1\rangle
\]

- $0$ and $1$ with a probability $1/2$, because

\[
\left| \frac{1+i}{2} \right|^2 = \left| \frac{1-i}{2} \right|^2 = \frac{1}{2}
\]

- Is called square root of the not-gate

\[
\sqrt{M} \cdot \sqrt{M} = M
\]

Can this matrixes help?

Can we decompose it?

\[
S_1 = \begin{pmatrix}
\frac{1+i}{2} & \frac{1-i}{2} \\
\frac{1-i}{2} & \frac{1+i}{2}
\end{pmatrix}
\]

\[
S_n = \begin{pmatrix}
\frac{1+i}{2^n} & \frac{1-i}{2^n} & \cdots & \frac{1-i}{2^n} \\
\frac{1-i}{2^n} & \frac{1+i}{2^n} & \cdots & \frac{1-i}{2^n} \\
\vdots & \vdots & \ddots & \vdots \\
\frac{1-i}{2^n} & \frac{1+i}{2^n} & \cdots & \frac{1+i}{2^n}
\end{pmatrix}
\]
We interested

- Unitary (symmetric) operators:

  \[ \text{Sharp} \xrightarrow{U} \text{Superposition} \]

  \[ |x\rangle \xrightarrow{U} \sum_{z \in F^*_2} N(x) |z\rangle \]

  - \( N(x) \) codes \( x \) in the superposition

- Is there a \( N(x) \) that represents \( x \) only in one dimension

  \[ |x\rangle \xrightarrow{U} \sum_{z \in F^*_2} N(x) |z\rangle \]

  \[ N(x) = \begin{cases} 1 & \text{if } x = z \\ -1 & \text{else} \end{cases} \]
Exists any spy system?

- A spy system is composed of a unitary operator which does not map the information about the dimension in which the answer is present into the amplitude.
- It maps it in all registers.

Spy system, does it exist?
- It seems there is no unitary operator which can do it.....

\[
\begin{align*}
\{000\}, \{001\}, \{010\}, \{011\}, \{100\}, \{101\}, \{110\}, \{111\} \\
\downarrow \\
\{000\} \{010\}, \{001\} \{010\}, \{010\} \{010\}, \{010\} \{101\}, \{100\} \{010\}, \{100\} \{111\}, \{101\} \{010\}, \{110\} \{010\}
\end{align*}
\]
Example of a non unitary projection $P$

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$P \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 2 \\ 2 \end{pmatrix}$$

Is there some-thing which is “related” to this trivial $P$, which is unitary?