Quantum Computation

Why, What, Where (When)

Andrew Duncan

March 14, 2007

Outline

Quantum Mechanics

1. Associated to an isolated quantum mechanical system is a complex inner product space V. The state of the system at any time is described by a unit vector in V.
2. The evolution of the state vector $|v\rangle$ of an isolated quantum mechanical system is given by the Schrödinger equation

$$ih\frac{d|v\rangle}{dt} = H|v\rangle,$$

where h is a constant (*Plank's constant*) and H is a fixed self-adjoint linear operator called the *Hamiltonian* of the system.
The states $|v_1\rangle$ and $|v_2\rangle$ of the system at times t_1 and t_2, respectively, are related by a unitary transformation ϕ, which depends only on t_1 and t_2, such that $\phi(|v_1\rangle) = |v_2\rangle$.

Quantum Mechanics

1. Associated to an isolated quantum mechanical system is a complex inner product space V. The state of the system at any time is described by a unit vector in V.
2. The evolution of the state vector $|v\rangle$ of an isolated quantum mechanical system is given by the Schrödinger equation

$$ih\frac{d|v\rangle}{dt} = H|v\rangle,$$

where h is a constant (*Plank's constant*) and H is a fixed self-adjoint linear operator called the *Hamiltonian* of the system.

The states $|v_1\rangle$ and $|v_2\rangle$ of the system at times t_1 and t_2, respectively, are related by a unitary transformation ϕ, which depends only on t_1 and t_2, such that $\phi(|v_1\rangle) = |v_2\rangle$.

Quantum Mechanics

1. Associated to an isolated quantum mechanical system is a complex inner product space V. The state of the system at any time is described by a unit vector in V.
2. The evolution of the state vector $|v\rangle$ of an isolated quantum mechanical system is given by the Schrödinger equation

$$ih\frac{d\,|v\rangle}{dt} = H\,|v\rangle\,,$$

where h is a constant (*Plank's constant*) and H is a fixed self-adjoint linear operator called the *Hamiltonian* of the system.
The states $|v_1\rangle$ and $|v_2\rangle$ of the system at times t_1 and t_2, respectively, are related by a unitary transformation ϕ, which depends only on t_1 and t_2, such that $\phi(|v_1\rangle) = |v_2\rangle$.

Measurement

3. A measurement of a quantum system consists of a set $\{M_m : m = 1, \ldots, k\}$ of linear operators on V, such that

$$\sum_{m=1}^{k} M_m^\dagger M_m = I. \tag{1}$$

The measurement result is one of the indices m.
If V is in state $|v\rangle$ then the probability that m observed is

$$p(m) = \left\langle v | M_m^\dagger M_m | v \right\rangle = \langle M_m(|v\rangle) | M_m |v\rangle\rangle .$$

If m is observed then the state of V is transformed from v to

$$\frac{M_m |v\rangle}{\sqrt{p(m)}}.$$

Measurement

3. A measurement of a quantum system consists of a set $\{M_m : m = 1, \ldots, k\}$ of linear operators on V, such that

$$\sum_{m=1}^{k} M_m^\dagger M_m = I. \tag{1}$$

The measurement result is one of the indices m.

If V is in state $|v\rangle$ then the probability that m observed is

$$p(m) = \left\langle v | M_m^\dagger M_m | v \right\rangle = \langle M_m(|v\rangle) | M_m |v\rangle \rangle .$$

If m is observed then the state of V is transformed from v to

$$\frac{M_m |v\rangle}{\sqrt{p(m)}}.$$

Measurement

3. A measurement of a quantum system consists of a set $\{M_m : m = 1, \ldots, k\}$ of linear operators on V, such that

$$\sum_{m=1}^{k} M_m^\dagger M_m = I. \tag{1}$$

The measurement result is one of the indices m.
If V is in state $|v\rangle$ then the probability that m observed is

$$p(m) = \left\langle v | M_m^\dagger M_m | v \right\rangle = \langle M_m(|v\rangle) | M_m |v\rangle \rangle .$$

If m is observed then the state of V is transformed from v to

$$\frac{M_m |v\rangle}{\sqrt{p(m)}}.$$

Measurement

3. A measurement of a quantum system consists of a set $\{M_m : m = 1, \ldots, k\}$ of linear operators on V, such that

$$\sum_{m=1}^{k} M_m^\dagger M_m = I. \tag{1}$$

The measurement result is one of the indices m.
If V is in state $|v\rangle$ then the probability that m observed is

$$p(m) = \left\langle v | M_m^\dagger M_m | v \right\rangle = \langle M_m(|v\rangle) | M_m |v\rangle \rangle .$$

If m is observed then the state of V is transformed from v to

$$\frac{M_m |v\rangle}{\sqrt{p(m)}}.$$

Composites

4. Given quantum mechanical systems associated to vector spaces V and W there is a composite quantum mechanical system associated to $V \otimes W$.

Quantum Computatation

The state space is finite dimensional.

The basic system is the 2-dimensional space $\mathbb{C}\mathbb{Z}_2$ with basis $\{|0\rangle, |1\rangle\}$, known as a single *qubit* system.

A state of a single qubit system is a vector $\alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$.

If neither α nor β is zero the state is called a *superposition*.

For example, $(|0\rangle + |1\rangle)/\sqrt{2}$ is a superposition, which is also *uniform*.

Quantum Computatation

The state space is finite dimensional.
The basic system is the 2-dimensional space $\mathbb{C}\mathbb{Z}_2$ with basis $\{|0\rangle, |1\rangle\}$, known as a single *qubit* system.
A state of a single qubit system is a vector $\alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$.
If neither α nor β is zero the state is called a *superposition*.
For example, $(|0\rangle + |1\rangle)/\sqrt{2}$ is a superposition, which is also *uniform*.

Quantum Computatation

The state space is finite dimensional.
The basic system is the 2-dimensional space $\mathbb{C}\mathbb{Z}_2$ with basis $\{|0\rangle, |1\rangle\}$, known as a single *qubit* system.
A state of a single qubit system is a vector $\alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$.
If neither α nor β is zero the state is called a *superposition*.
For example, $(|0\rangle + |1\rangle)/\sqrt{2}$ is a superposition, which is also *uniform*.

Quantum Computatation

The state space is finite dimensional.
The basic system is the 2-dimensional space $\mathbb{C}\mathbb{Z}_2$ with basis $\{|0\rangle, |1\rangle\}$, known as a single *qubit* system.
A state of a single qubit system is a vector $\alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$.
If neither α nor β is zero the state is called a *superposition*.
For example, $(|0\rangle + |1\rangle)/\sqrt{2}$ is a superposition, which is also *uniform*.

Quantum Computatation

The state space is finite dimensional.
The basic system is the 2-dimensional space $\mathbb{C}\mathbb{Z}_2$ with basis $\{|0\rangle, |1\rangle\}$, known as a single *qubit* system.
A state of a single qubit system is a vector $\alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$.
If neither α nor β is zero the state is called a *superposition*.
For example, $(|0\rangle + |1\rangle)/\sqrt{2}$ is a superposition, which is also *uniform*.

Quantum Computatation

The composite of 2 single qubit systems is $\mathbb{C}\mathbb{Z}_2 \otimes \mathbb{C}\mathbb{Z}_2$,
a 4–dimensional space with basis vectors $|00\rangle$,$|01\rangle$, $|10\rangle$,$|11\rangle$.
We call this a 2–*qubit system* or 2–*qubit quantum register*.
Similarly an *n–qubit system* or *quantum register* is a copy of the 2^n–dimensional space $\mathbb{C}\mathbb{Z}_2^{\otimes n}$,
which, has basis $\{|i\rangle : i = 0, \ldots, 2^n - 1\}$.
Given an m–qubit system V_m and an n–qubit system V_n, we may form the mn–qubit system $V_m \otimes V_n$, which is naturally equipped with the basis $\{|ij\rangle : i = 0, \ldots, 2^m - 1, j = 0, \ldots, 2^n - 1\}$.

Quantum Computatation

The composite of 2 single qubit systems is $\mathbb{C}\mathbb{Z}_2 \otimes \mathbb{C}\mathbb{Z}_2$,
a 4–dimensional space with basis vectors $|00\rangle$,$|01\rangle$, $|10\rangle$,$|11\rangle$.
We call this a 2–*qubit system* or 2–*qubit quantum register*.
Similarly an *n–qubit system* or *quantum register* is a copy of the 2^n–dimensional space $\mathbb{C}\mathbb{Z}_2^{\otimes n}$,
which, has basis $\{|i\rangle : i = 0, \ldots, 2^n - 1\}$.
Given an m–qubit system V_m and an n–qubit system V_n, we may form the mn–qubit system $V_m \otimes V_n$, which is naturally equipped with the basis $\{|ij\rangle : i = 0, \ldots, 2^m - 1, j = 0, \ldots, 2^n - 1\}$.

Quantum Computatation

The composite of 2 single qubit systems is $\mathbb{C}\mathbb{Z}_2 \otimes \mathbb{C}\mathbb{Z}_2$,
a 4–dimensional space with basis vectors $|00\rangle$,$|01\rangle$, $|10\rangle$,$|11\rangle$.
We call this a 2–*qubit system* or 2–*qubit quantum register*.
Similarly an *n–qubit system* or *quantum register* is a copy of the 2^n–dimensional space $\mathbb{C}\mathbb{Z}_2^{\otimes n}$,
which, has basis $\{|i\rangle : i = 0, \ldots, 2^n - 1\}$.
Given an *m*–qubit system V_m and an *n*–qubit system V_n, we may form the *mn*–qubit system $V_m \otimes V_n$, which is naturally equipped with the basis $\{|ij\rangle : i = 0, \ldots, 2^m - 1, j = 0, \ldots, 2^n - 1\}$.

Quantum Computatation

The composite of 2 single qubit systems is $\mathbb{C}\mathbb{Z}_2 \otimes \mathbb{C}\mathbb{Z}_2$,
a 4–dimensional space with basis vectors $|00\rangle$,$|01\rangle$, $|10\rangle$,$|11\rangle$.
We call this a 2–*qubit system* or 2–*qubit quantum register*.
Similarly an *n–qubit system* or *quantum register* is a copy of the 2^n–dimensional space $\mathbb{C}\mathbb{Z}_2^{\otimes n}$,
which, has basis $\{|i\rangle : i = 0, \ldots, 2^n - 1\}$.
Given an m–qubit system V_m and an n–qubit system V_n, we may form the mn–qubit system $V_m \otimes V_n$, which is naturally equipped with the basis $\{|ij\rangle : i = 0, \ldots, 2^m - 1, j = 0, \ldots, 2^n - 1\}$.

Quantum Computatation

The composite of 2 single qubit systems is $\mathbb{C}\mathbb{Z}_2 \otimes \mathbb{C}\mathbb{Z}_2$,
a 4–dimensional space with basis vectors $|00\rangle$,$|01\rangle$, $|10\rangle$,$|11\rangle$.
We call this a 2–*qubit system* or 2–*qubit quantum register*.
Similarly an *n–qubit system* or *quantum register* is a copy of the 2^n–dimensional space $\mathbb{C}\mathbb{Z}_2^{\otimes n}$,
which, has basis $\{|i\rangle : i = 0, \ldots, 2^n - 1\}$.
Given an m–qubit system V_m and an n–qubit system V_n, we may form the mn–qubit system $V_m \otimes V_n$, which is naturally equipped with the basis $\{|ij\rangle : i = 0, \ldots, 2^m - 1, j = 0, \ldots, 2^n - 1\}$.

Quantum Computatation

The composite of 2 single qubit systems is $\mathbb{C}\mathbb{Z}_2 \otimes \mathbb{C}\mathbb{Z}_2$,
a 4–dimensional space with basis vectors $|00\rangle$,$|01\rangle$, $|10\rangle$,$|11\rangle$.
We call this a 2–*qubit system* or 2–*qubit quantum register*.
Similarly an *n–qubit system* or *quantum register* is a copy of the
2^n–dimensional space $\mathbb{C}\mathbb{Z}_2^{\otimes n}$,
which, has basis $\{|i\rangle : i = 0, \ldots, 2^n - 1\}$.
Given an m–qubit system V_m and an n–qubit system V_n, we may form the mn–qubit system $V_m \otimes V_n$, which is naturally equipped with the basis $\{|ij\rangle : i = 0, \ldots, 2^m - 1, j = 0, \ldots, 2^n - 1\}$.

An n–qubit system is the quantum analogue of the classical n–bit computer.

Whereas n–bits can contain, at any one time, one of 2^n possible values, a quantum computer can be in a superposition of all of these values,

in principle in infinitely many different ways.

An n–qubit system is the quantum analogue of the classical n–bit computer.

Whereas n–bits can contain, at any one time, one of 2^n possible values, a quantum computer can be in a superposition of all of these values,

in principle in infinitely many different ways.

An n–qubit system is the quantum analogue of the classical n–bit computer.

Whereas n–bits can contain, at any one time, one of 2^n possible values, a quantum computer can be in a superposition of all of these values,

in principle in infinitely many different ways.

Evolution in quantum computation

Evolution is assumed to take place at discrete time intervals and is goverened by unitary operators.

e.g. $\mathbb{C}\mathbb{Z}_2$ has basis $\{|0\rangle, |1\rangle\}$
and the quantum NOT gate can be written as

$$|0\rangle\langle 1| + |1\rangle\langle 0|.$$

$\mathrm{NOT}|0\rangle = |1\rangle$

$\mathrm{NOT}|1\rangle = |0\rangle.$

Evolution in quantum computation

Evolution is assumed to take place at discrete time intervals and is goverened by unitary operators.

e.g. $\mathbb{C}\mathbb{Z}_2$ has basis $\{|0\rangle, |1\rangle\}$
and the quantum NOT gate can be written as

$$|0\rangle\langle 1| + |1\rangle\langle 0|.$$

$$\mathrm{NOT}|0\rangle = |1\rangle$$

$$\mathrm{NOT}|1\rangle = |0\rangle.$$

Evolution in quantum computation

Evolution is assumed to take place at discrete time intervals and is goverened by unitary operators.

e.g. $\mathbb{C}\mathbb{Z}_2$ has basis $\{|0\rangle, |1\rangle\}$
and the quantum NOT gate can be written as

$$|0\rangle\langle 1| + |1\rangle\langle 0|.$$

$\mathrm{NOT}|0\rangle = |1\rangle$

$\mathrm{NOT}|1\rangle = |0\rangle.$

Evolution in quantum computation

Evolution is assumed to take place at discrete time intervals and is goverened by unitary operators.

e.g. $\mathbb{C}\mathbb{Z}_2$ has basis $\{|0\rangle, |1\rangle\}$
and the quantum NOT gate can be written as

$$|0\rangle\langle 1| + |1\rangle\langle 0|.$$

$\mathrm{NOT}|0\rangle = |1\rangle$

$\mathrm{NOT}|1\rangle = |0\rangle.$

Measurements in quantum computation

Usually restrict attention to the special case of measurement where M_m is self-adjoint and $M_m^2 = M_m$, for all m, and $M_m M_n = 0$, when $m \neq n$.

Such measurements are called *projective* measurements.
In the case of projective measurement there are mutually orthogonal subspaces $P_1, \ldots, P_k$ of V such that $V = \sum_m P_m$ and $M_m = \sum_i |i\rangle\langle i|$, for some orthonormal basis $\{|i\rangle : i = 0, \ldots, d_m - 1\}$ of P_m.

That is M_m is projection onto P_m.
Most measurements will be of the form $\{M_m = |m\rangle\langle m| : m = 0, \ldots, n-1\}$, where V is n–dimensional and the basis used to describe the state vector and evolution of V is $\{|m\rangle : m = 0, \ldots, n-1\}$.

These are called *measurements with respect to the computational basis*.

Measurements in quantum computation

Usually restrict attention to the special case of measurement where M_m is self-adjoint and $M_m^2 = M_m$, for all m, and $M_m M_n = 0$, when $m \neq n$.

Such measurements are called *projective* measurements.

In the case of projective measurement there are mutually orthogonal subspaces $P_1, \ldots, P_k$ of V such that $V = \sum_m P_m$ and $M_m = \sum_i |i\rangle\langle i|$, for some orthonormal basis $\{|i\rangle : i = 0, \ldots, d_m - 1\}$ of P_m.

That is M_m is projection onto P_m.
Most measurements will be of the form $\{M_m = |m\rangle\langle m| : m = 0, \ldots, n-1\}$, where V is n–dimensional and the basis used to describe the state vector and evolution of V is $\{|m\rangle : m = 0, \ldots, n-1\}$.

These are called *measurements with respect to the computational basis*.

Measurements in quantum computation

Usually restrict attention to the special case of measurement where M_m is self-adjoint and $M_m^2 = M_m$, for all m, and $M_m M_n = 0$, when $m \neq n$.

Such measurements are called *projective* measurements.
In the case of projective measurement there are mutually orthogonal subspaces $P_1, \ldots, P_k$ of V such that $V = \sum_m P_m$ and $M_m = \sum_i |i\rangle\langle i|$, for some orthonormal basis $\{|i\rangle : i = 0, \ldots, d_m - 1\}$ of P_m.

That is M_m is projection onto P_m.
Most measurements will be of the form $\{M_m = |m\rangle\langle m| : m = 0, \ldots, n-1\}$, where V is n–dimensional and the basis used to describe the state vector and evolution of V is $\{|m\rangle : m = 0, \ldots, n-1\}$.

These are called *measurements with respect to the computational basis*.

Measurements in quantum computation

Usually restrict attention to the special case of measurement where M_m is self-adjoint and $M_m^2 = M_m$, for all m, and $M_m M_n = 0$, when $m \neq n$.

Such measurements are called *projective* measurements.
In the case of projective measurement there are mutually orthogonal subspaces $P_1, \ldots, P_k$ of V such that $V = \sum_m P_m$ and $M_m = \sum_i |i\rangle\langle i|$, for some orthonormal basis $\{|i\rangle : i = 0, \ldots, d_m - 1\}$ of P_m.

That is M_m is projection onto P_m.
Most measurements will be of the form $\{M_m = |m\rangle\langle m| : m = 0, \ldots, n-1\}$, where V is n–dimensional and the basis used to describe the state vector and evolution of V is $\{|m\rangle : m = 0, \ldots, n-1\}$.

These are called *measurements with respect to the computational basis*.

Measurements in quantum computation

Usually restrict attention to the special case of measurement where M_m is self-adjoint and $M_m^2 = M_m$, for all m, and $M_m M_n = 0$, when $m \neq n$.

Such measurements are called *projective* measurements.
In the case of projective measurement there are mutually orthogonal subspaces $P_1, \ldots, P_k$ of V such that $V = \sum_m P_m$ and $M_m = \sum_i |i\rangle\langle i|$, for some orthonormal basis $\{|i\rangle : i = 0, \ldots, d_m - 1\}$ of P_m.

That is M_m is projection onto P_m.
Most measurements will be of the form $\{M_m = |m\rangle\langle m| : m = 0, \ldots, n-1\}$, where V is n–dimensional and the basis used to describe the state vector and evolution of V is $\{|m\rangle : m = 0, \ldots, n-1\}$.

These are called *measurements with respect to the computational basis*.

For example suppose we have a single qubit system in state $Q = a|0\rangle + b|1\rangle$, where $|a|^2 + |b|^2 = 1$.

If we observe Q with respect to the computational basis we obtain 0 with probability $\langle Q|0\rangle \langle 0| Q\rangle = |a|^2$ and 1 with probability $\langle Q|1\rangle \langle 1| Q\rangle = |b|^2$.

The quantum system enters the state

$$\frac{|0\rangle \langle 0|Q\rangle}{|a|} = \frac{a}{|a|}|0\rangle,$$

if 0 is measured and

$$\frac{|1\rangle \langle 1|Q\rangle}{|b|} = \frac{b}{|b|}|1\rangle,$$

if 1 is measured.

For example suppose we have a single qubit system in state $Q = a|0\rangle + b|1\rangle$, where $|a|^2 + |b|^2 = 1$.

If we observe Q with respect to the computational basis we obtain 0 with probability $\langle Q|0\rangle \langle 0| Q\rangle = |a|^2$ and 1 with probability $\langle Q|1\rangle \langle 1| Q\rangle = |b|^2$.

The quantum system enters the state

$$\frac{|0\rangle \langle 0|Q\rangle}{|a|} = \frac{a}{|a|}|0\rangle,$$

if 0 is measured and

$$\frac{|1\rangle \langle 1|Q\rangle}{|b|} = \frac{b}{|b|}|1\rangle,$$

if 1 is measured.

For example suppose we have a single qubit system in state $Q = a\,|0\rangle + b\,|1\rangle$, where $|a|^2 + |b|^2 = 1$.

If we observe Q with respect to the computational basis we obtain 0 with probability $\langle Q|0\rangle \langle 0|\, Q\rangle = |a|^2$ and 1 with probability $\langle Q|1\rangle \langle 1|\, Q\rangle = |b|^2$.

The quantum system enters the state

$$\frac{|0\rangle \langle 0|Q\rangle}{|a|} = \frac{a}{|a|}\,|0\rangle\,,$$

if 0 is measured and

$$\frac{|1\rangle \langle 1|Q\rangle}{|b|} = \frac{b}{|b|}\,|1\rangle\,,$$

if 1 is measured.

Single Qubit Walsh-Hadamard

$$W(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ and}$$
$$W(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{2}$$

$$W(|x\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x |1\rangle)$$
$$= \frac{1}{\sqrt{2}} \sum_{k=0}^{1} (-1)^{kx} |k\rangle .$$

W is an involution: $W^2 = I_2$.

W is reflection in the line which makes an angle of $\pi/8$ with the $|0\rangle$–axis.

Single Qubit Walsh-Hadamard

$$W(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ and}$$
$$W(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{2}$$

$$W(|x\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x |1\rangle)$$
$$= \frac{1}{\sqrt{2}} \sum_{k=0}^{1} (-1)^{kx} |k\rangle .$$

W is an involution: $W^2 = I_2$.

W is reflection in the line which makes an angle of $\pi/8$ with the $|0\rangle$–axis.

Single Qubit Walsh-Hadamard

$$W(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ and}$$
$$W(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{2}$$

$$W(|x\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x |1\rangle)$$
$$= \frac{1}{\sqrt{2}} \sum_{k=0}^{1} (-1)^{kx} |k\rangle .$$

W is an involution: $W^2 = I_2$.

W is reflection in the line which makes an angle of $\pi/8$ with the $|0\rangle$–axis.

Single Qubit Walsh-Hadamard

$$W(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ and}$$
$$W(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{2}$$

$$W(|x\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x |1\rangle)$$
$$= \frac{1}{\sqrt{2}} \sum_{k=0}^{1} (-1)^{kx} |k\rangle .$$

W is an involution: $W^2 = I_2$.

W is reflection in the line which makes an angle of $\pi/8$ with the $|0\rangle$–axis.

n-qubit Walsh-Hadamard

W_n is defined to be $W^{\otimes n}$.

W is an involution so $W_n^2 = I_2^{\otimes n} = I_{2^n}$,

so W_n is also an involution.

Applied to $|0\rangle^{\otimes n}$, W_n generates a uniform linear combination of the integers from 0 to $2^n - 1$, i.e.

$$W_n(|0 \cdots 0\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle.$$

n-qubit Walsh-Hadamard

W_n is defined to be $W^{\otimes n}$.

W is an involution so $W_n^2 = I_2^{\otimes n} = I_{2^n}$,

so W_n is also an involution.

Applied to $|0\rangle^{\otimes n}$, W_n generates a uniform linear combination of the integers from 0 to $2^n - 1$, i.e.

$$W_n(|0 \cdots 0\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle.$$

n-qubit Walsh-Hadamard

W_n is defined to be $W^{\otimes n}$.

W is an involution so $W_n^2 = I_2^{\otimes n} = I_{2^n}$,

so W_n is also an involution.

Applied to $|0\rangle^{\otimes n}$, W_n generates a uniform linear combination of the integers from 0 to $2^n - 1$, i.e.

$$W_n(|0 \cdots 0\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle.$$

n-qubit Walsh-Hadamard

W_n is defined to be $W^{\otimes n}$.

W is an involution so $W_n^2 = I_2^{\otimes n} = I_{2^n}$,

so W_n is also an involution.

Applied to $|0\rangle^{\otimes n}$, W_n generates a uniform linear combination of the integers from 0 to $2^n - 1$, i.e.

$$W_n(|0 \cdots 0\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle.$$

n-qubit Walsh-Hadamard

W_n is defined to be $W^{\otimes n}$.

W is an involution so $W_n^2 = I_2^{\otimes n} = I_{2^n}$,

so W_n is also an involution.

Applied to $|0\rangle^{\otimes n}$, W_n generates a uniform linear combination of the integers from 0 to $2^n - 1$, i.e.

$$W_n(|0 \cdots 0\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle.$$

Define

$$x \cdot y = \sum_{i=0}^{n-1} x_i y_i.$$

setting $m = 2^n$, we have

$$\begin{aligned}
W_n |x\rangle &= \bigotimes_{i=0}^{n-1} W |x_i\rangle \\
&= \bigotimes_{i=0}^{n-1} \frac{1}{\sqrt{2}} \sum_{k_i=0}^{1} (-1)^{k_i x_i} |k_i\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_0=0}^{1} \cdots \sum_{k_{n-1}=0}^{1} (-1)^{x_0 k_0} \cdots (-1)^{x_{n-1} k_{n-1}} |k_0 \cdots k_{n-1}\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_0 \cdots k_{n-1}=0}^{m-1} (-1)^{x_0 k_0} \cdots (-1)^{x_{n-1} k_{n-1}} |k_0 \cdots k_{n-1}\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{m-1} (-1)^{x \cdot k} |k\rangle . \qquad (3)
\end{aligned}$$

Define

$$x \cdot y = \sum_{i=0}^{n-1} x_i y_i.$$

setting $m = 2^n$, we have

$$\begin{aligned}
W_n |x\rangle &= \bigotimes_{i=0}^{n-1} W |x_i\rangle \\
&= \bigotimes_{i=0}^{n-1} \frac{1}{\sqrt{2}} \sum_{k_i=0}^{1} (-1)^{k_i x_i} |k_i\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_0=0}^{1} \cdots \sum_{k_{n-1}=0}^{1} (-1)^{x_0 k_0} \cdots (-1)^{x_{n-1} k_{n-1}} |k_0 \cdots k_{n-1}\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_0 \cdots k_{n-1}=0}^{m-1} (-1)^{x_0 k_0} \cdots (-1)^{x_{n-1} k_{n-1}} |k_0 \cdots k_{n-1}\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{m-1} (-1)^{x \cdot k} |k\rangle . \qquad (3)
\end{aligned}$$

Reversibilisatitation of a Function

Let $f : \mathbb{Z}_2^m \to \mathbb{Z}_2^k$ be a function, not necessarily invertible.

To simulate f we use a quantum system V which is the tensor product of an m–qubit quantum system with a k–qubit quantum system.

V has basis consisting of the vectors $|x\rangle \otimes |y\rangle$, where x and y are binary representations of integers in $\{0, \ldots, 2^m - 1\} = \mathbb{Z}_2^m$ and $\{0, \ldots, 2^k - 1\} = \mathbb{Z}_2^k$ respectively.

Define the linear transformation

$$U_f : |x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y \oplus f(x)\rangle ,$$

where $\oplus$ denotes addition in the group $\mathbb{Z}_2^k$.

Reversibilisatitation of a Function

Let $f : \mathbb{Z}_2^m \to \mathbb{Z}_2^k$ be a function, not necessarily invertible.

To simulate f we use a quantum system V which is the tensor product of an m–qubit quantum system with a k–qubit quantum system.

V has basis consisting of the vectors $|x\rangle \otimes |y\rangle$, where x and y are binary representations of integers in $\{0, \ldots, 2^m - 1\} = \mathbb{Z}_2^m$ and $\{0, \ldots, 2^k - 1\} = \mathbb{Z}_2^k$ respectively.

Define the linear transformation

$$U_f : |x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y \oplus f(x)\rangle ,$$

where $\oplus$ denotes addition in the group $\mathbb{Z}_2^k$.

Reversibilisatitation of a Function

Let $f : \mathbb{Z}_2^m \to \mathbb{Z}_2^k$ be a function, not necessarily invertible.

To simulate f we use a quantum system V which is the tensor product of an m–qubit quantum system with a k–qubit quantum system.

V has basis consisting of the vectors $|x\rangle \otimes |y\rangle$, where x and y are binary representations of integers in $\{0, \ldots, 2^m - 1\} = \mathbb{Z}_2^m$ and $\{0, \ldots, 2^k - 1\} = \mathbb{Z}_2^k$ respectively.

Define the linear transformation

$$U_f : |x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y \oplus f(x)\rangle ,$$

where $\oplus$ denotes addition in the group $\mathbb{Z}_2^k$.

Reversibilisatitation of a Function

Let $f : \mathbb{Z}_2^m \to \mathbb{Z}_2^k$ be a function, not necessarily invertible.

To simulate f we use a quantum system V which is the tensor product of an m–qubit quantum system with a k–qubit quantum system.

V has basis consisting of the vectors $|x\rangle \otimes |y\rangle$, where x and y are binary representations of integers in $\{0, \ldots, 2^m - 1\} = \mathbb{Z}_2^m$ and $\{0, \ldots, 2^k - 1\} = \mathbb{Z}_2^k$ respectively.

Define the linear transformation

$$U_f : |x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y \oplus f(x)\rangle \,,$$

where $\oplus$ denotes addition in the group $\mathbb{Z}_2^k$.

For fixed x, $y \oplus f(x)$ takes every value in $\mathbb{Z}_2^k$ exactly once, as y varies over $\{0, \ldots, 2^k - 1\}$.

Therefore U_f simply permutes all 2^{m+k} basis elements of V and it follows that it is unitary.

Moreover $U_f(|x\rangle \otimes |0\rangle) = |x\rangle \otimes |f(x)\rangle$ and in this sense U_f simulates f.

The map U_f is referred to as the *standard oracle* for the function f.

For fixed x, $y \oplus f(x)$ takes every value in $\mathbb{Z}_2^k$ exactly once, as y varies over $\{0, \ldots, 2^k - 1\}$.

Therefore U_f simply permutes all 2^{m+k} basis elements of V and it follows that it is unitary.

Moreover $U_f(|x\rangle \otimes |0\rangle) = |x\rangle \otimes |f(x)\rangle$ and in this sense U_f simulates f.

The map U_f is referred to as the *standard oracle* for the function f.

For fixed x, $y \oplus f(x)$ takes every value in $\mathbb{Z}_2^k$ exactly once, as y varies over $\{0, \ldots, 2^k - 1\}$.

Therefore U_f simply permutes all 2^{m+k} basis elements of V and it follows that it is unitary.

Moreover $U_f(|x\rangle \otimes |0\rangle) = |x\rangle \otimes |f(x)\rangle$ and in this sense U_f simulates f.

The map U_f is referred to as the *standard oracle* for the function f.

For fixed x, $y \oplus f(x)$ takes every value in $\mathbb{Z}_2^k$ exactly once, as y varies over $\{0, \ldots, 2^k - 1\}$.

Therefore U_f simply permutes all 2^{m+k} basis elements of V and it follows that it is unitary.

Moreover $U_f(|x\rangle \otimes |0\rangle) = |x\rangle \otimes |f(x)\rangle$ and in this sense U_f simulates f.

The map U_f is referred to as the *standard oracle* for the function f.

Parallel Computation

If we apply U_f to

$$W_m(|0\rangle^{\otimes m}) \otimes |0\rangle^{\otimes k}$$

we obtain

$$\begin{aligned} U_f\left(\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle\otimes|0\rangle\right) &= \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}U_f(|x\rangle\otimes|0\rangle) \\ &= \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle\otimes|f(x)\rangle\,. \end{aligned}$$

Parallel Computation

If we apply U_f to

$$W_m(|0\rangle^{\otimes m}) \otimes |0\rangle^{\otimes k}$$

we obtain

$$\begin{aligned} U_f\left(\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle \otimes |0\rangle\right) &= \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1} U_f(|x\rangle \otimes |0\rangle) \\ &= \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle \otimes |f(x)\rangle\,. \end{aligned}$$

Doing Nothing in Parallel

$$
\begin{aligned}
|0\rangle \otimes |0\rangle \quad &\overset{W \otimes W}{\mapsto} \quad \frac{1}{\sqrt{2^{m+k}}} \sum_{x=0}^{2^m-1} \sum_{y=0}^{2^k-1} |x\rangle \otimes |y\rangle \\
&\overset{U_f}{\mapsto} \quad \frac{1}{\sqrt{2^{m+k}}} \sum_{x=0}^{2^m-1} \sum_{y=0}^{2^k-1} |x\rangle \otimes |y \oplus f(x)\rangle \\
&= \quad \frac{1}{\sqrt{2^{m+k}}} \sum_{x=0}^{2^m-1} \sum_{y=0}^{2^k-1} |x\rangle \otimes |y\rangle \,,
\end{aligned}
$$

because $y \oplus f(x)$ takes each possible value exactly once, as y ranges over $\{0, \ldots, 2^k - 1\}$.

Doing Nothing in Parallel

$$
\begin{aligned}
|0\rangle \otimes |0\rangle \quad &\overset{W\otimes W}{\mapsto} \quad \frac{1}{\sqrt{2^{m+k}}} \sum_{x=0}^{2^m-1} \sum_{y=0}^{2^k-1} |x\rangle \otimes |y\rangle \\
&\overset{U_f}{\mapsto} \quad \frac{1}{\sqrt{2^{m+k}}} \sum_{x=0}^{2^m-1} \sum_{y=0}^{2^k-1} |x\rangle \otimes |y \oplus f(x)\rangle \\
&= \quad \frac{1}{\sqrt{2^{m+k}}} \sum_{x=0}^{2^m-1} \sum_{y=0}^{2^k-1} |x\rangle \otimes |y\rangle \,,
\end{aligned}
$$

because $y \oplus f(x)$ takes each possible value exactly once, as y ranges over $\{0, \ldots, 2^k - 1\}$.

Single qubit Simon-Deutsch Algorithm

$$(W \otimes W)(|0\rangle \otimes |1\rangle) = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

Now, if $x \in \{0, 1\}$, we have

$$\begin{aligned} U_f\left(|x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) &= |x\rangle \otimes \left(\frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}\right) \\ &= |x\rangle \otimes \frac{1}{\sqrt{2}}\left(\begin{cases} |0\rangle - |1\rangle & \text{if } f(x) = 0 \\ |1\rangle - |0\rangle & \text{if } f(x) = 1 \end{cases}\right) \\ &= (-1)^{f(x)}|x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \end{aligned}$$

Single qubit Simon-Deutsch Algorithm

$$(W \otimes W)(|0\rangle \otimes |1\rangle) = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

Now, if $x \in \{0, 1\}$, we have

$$\begin{aligned} U_f\left(|x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) &= |x\rangle \otimes \left(\frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}\right) \\ &= |x\rangle \otimes \frac{1}{\sqrt{2}}\left(\begin{cases} |0\rangle - |1\rangle & \text{if } f(x) = 0 \\ |1\rangle - |0\rangle & \text{if } f(x) = 1 \end{cases}\right) \\ &= (-1)^{f(x)}|x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \end{aligned}$$

Therefore, by linearity, after passing through the U_f gate the system is in state

$$\left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

which is equal to

$$\pm\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right), \text{ if } f \text{ is constant,}$$

and

$$\pm\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right), \text{ if } f \text{ is balanced.}$$

Therefore, by linearity, after passing through the U_f gate the system is in state

$$\left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

which is equal to

$$\pm\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right), \quad \text{if } f \text{ is constant,}$$

and

$$\pm\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right), \quad \text{if } f \text{ is balanced.}$$

After passing through the final Walsh–Hadamard gate, the first qubit is in state

$$\begin{array}{ll} \pm|0\rangle & \text{if } f \text{ is constant} \\ \pm|1\rangle & \text{if } f \text{ is balanced} \end{array}.$$

So measuring this qubit, with respect to the computational basis, we observe 0 with probability 1, if f is constant, and 1 with probability 1, if f is balanced.

After passing through the final Walsh–Hadamard gate, the first qubit is in state

$$\begin{array}{ll} \pm|0\rangle & \text{if } f \text{ is constant} \\ \pm|1\rangle & \text{if } f \text{ is balanced} \end{array}.$$

So measuring this qubit, with respect to the computational basis, we observe 0 with probability 1, if f is constant, and 1 with probability 1, if f is balanced.

Characters of Abelian Groups

A *character* of a finite Abelian group G over a field k is a homomorphism from G to the multiplicative group k^* of non–zero elements of k.

The set of characters of G over $\mathbb{C}$ is denoted $\hat{G}$.

The characters of the finite cyclic group $\mathbb{Z}_m$ are the homomorphisms $\chi_m^c = \chi^c$ defined by

$$\chi^c(a) = e^{2\pi iac/m}, \quad \text{where } a \in \mathbb{Z}_m,$$

for $c = 0, \ldots, m-1$.

The map $\chi : \mathbb{Z}_m \to \hat{\mathbb{Z}}_m$ defined by $\chi(a) = \chi^a$ is an isomorphism from $\mathbb{Z}_m$ to $\hat{\mathbb{Z}}_m$.

Characters of Abelian Groups

A *character* of a finite Abelian group G over a field k is a homomorphism from G to the multiplicative group k^* of non–zero elements of k.

The set of characters of G over $\mathbb{C}$ is denoted $\hat{G}$.

The characters of the finite cyclic group $\mathbb{Z}_m$ are the homomorphisms $\chi_m^c = \chi^c$ defined by

$$\chi^c(a) = e^{2\pi iac/m}, \quad \text{where } a \in \mathbb{Z}_m,$$

for $c = 0, \ldots, m-1$.

The map $\chi : \mathbb{Z}_m \to \hat{\mathbb{Z}}_m$ defined by $\chi(a) = \chi^a$ is an isomorphism from $\mathbb{Z}_m$ to $\hat{\mathbb{Z}}_m$.

Characters of Abelian Groups

A *character* of a finite Abelian group G over a field k is a homomorphism from G to the multiplicative group k^* of non–zero elements of k.

The set of characters of G over $\mathbb{C}$ is denoted $\hat{G}$.

The characters of the finite cyclic group $\mathbb{Z}_m$ are the homomorphisms $\chi_m^c = \chi^c$ defined by

$$\chi^c(a) = e^{2\pi iac/m}, \text{ where } a \in \mathbb{Z}_m,$$

for $c = 0, \ldots, m-1$.

The map $\chi : \mathbb{Z}_m \to \hat{\mathbb{Z}}_m$ defined by $\chi(a) = \chi^a$ is an isomorphism from $\mathbb{Z}_m$ to $\hat{\mathbb{Z}}_m$.

Characters of Abelian Groups

A *character* of a finite Abelian group G over a field k is a homomorphism from G to the multiplicative group k^* of non–zero elements of k.

The set of characters of G over $\mathbb{C}$ is denoted $\hat{G}$.

The characters of the finite cyclic group $\mathbb{Z}_m$ are the homomorphisms $\chi_m^c = \chi^c$ defined by

$$\chi^c(a) = e^{2\pi iac/m}, \text{ where } a \in \mathbb{Z}_m,$$

for $c = 0, \ldots, m-1$.

The map $\chi : \mathbb{Z}_m \to \hat{\mathbb{Z}}_m$ defined by $\chi(a) = \chi^a$ is an isomorphism from $\mathbb{Z}_m$ to $\hat{\mathbb{Z}}_m$.

A property of characters of $\mathbb{Z}_m$

Lemma

The characters of $\mathbb{Z}_m$ satisfy

(i)

$$\sum_{a=0}^{m-1} \chi^c(a) = \begin{cases} m & if\ c = 0 \mod m \\ 0 & if\ c \neq 0 \mod m \end{cases} . \tag{4}$$

(ii) *(Orthogonality of characters)*

$$\sum_{a=0}^{m-1} \chi^c(a)\overline{\chi^d(a)} = \begin{cases} m & if\ c = d \mod m \\ 0 & if\ c \neq d \mod m \end{cases} . \tag{5}$$

A property of characters of $\mathbb{Z}_m$

Lemma

The characters of $\mathbb{Z}_m$ satisfy

(i)

$$\sum_{a=0}^{m-1} \chi^c(a) = \begin{cases} m & if\ c = 0 \mod m \\ 0 & if\ c \neq 0 \mod m \end{cases} . \tag{4}$$

(ii) *(Orthogonality of characters)*

$$\sum_{a=0}^{m-1} \chi^c(a)\overline{\chi^d(a)} = \begin{cases} m & if\ c = d \mod m \\ 0 & if\ c \neq d \mod m \end{cases} . \tag{5}$$

The Complex Group Algebra

For a finite group G the $|G|$–dimensional complex vector space

$$\mathbb{C}G = \bigoplus_{g \in G} \mathbb{C}\,|g\rangle$$

is a ring called the *complex group algebra*,

with multiplication defined by

$$\left(\sum_{g \in G} a(g)\,|g\rangle\right)\left(\sum_{h \in G} b(h)\,|h\rangle\right) = \sum_{g \in G} c(g)\,|g\rangle\,,$$

$a(g), b(g) \in \mathbb{C}$ and $c(g) = \sum_{x \in G} a(x)b(x^{-1}g)$.

The group algebra is the ring of maps from G to $\mathbb{C}$, the map a sending g to $a(g)$ corresponding to $\sum_{g \in G} a(g)\,|g\rangle$.

An element of $\mathbb{C}\mathbb{Z}_n$ will be said to be *periodic* if it is periodic as a map from $\mathbb{Z}_n$ to $\mathbb{C}$.

The Complex Group Algebra

For a finite group G the $|G|$–dimensional complex vector space

$$\mathbb{C}G = \bigoplus_{g \in G} \mathbb{C}\,|g\rangle$$

is a ring called the *complex group algebra*,

with multiplication defined by

$$\left(\sum_{g \in G} a(g)\,|g\rangle\right)\left(\sum_{h \in G} b(h)\,|h\rangle\right) = \sum_{g \in G} c(g)\,|g\rangle\,,$$

$a(g), b(g) \in \mathbb{C}$ and $c(g) = \sum_{x \in G} a(x)b(x^{-1}g)$.

The group algebra is the ring of maps from G to $\mathbb{C}$, the map a sending g to $a(g)$ corresponding to $\sum_{g \in G} a(g)\,|g\rangle$.

An element of $\mathbb{C}\mathbb{Z}_n$ will be said to be *periodic* if it is periodic as a map from $\mathbb{Z}_n$ to $\mathbb{C}$.

The Complex Group Algebra

For a finite group G the $|G|$–dimensional complex vector space

$$\mathbb{C}G = \bigoplus_{g \in G} \mathbb{C}\,|g\rangle$$

is a ring called the *complex group algebra*,

with multiplication defined by

$$\left(\sum_{g \in G} a(g)\,|g\rangle\right)\left(\sum_{h \in G} b(h)\,|h\rangle\right) = \sum_{g \in G} c(g)\,|g\rangle\,,$$

$a(g), b(g) \in \mathbb{C}$ and $c(g) = \sum_{x \in G} a(x)b(x^{-1}g)$.

The group algebra is the ring of maps from G to $\mathbb{C}$, the map a sending g to $a(g)$ corresponding to $\sum_{g \in G} a(g)\,|g\rangle$.

An element of $\mathbb{C}\mathbb{Z}_n$ will be said to be *periodic* if it is periodic as a map from $\mathbb{Z}_n$ to $\mathbb{C}$.

The Complex Group Algebra

For a finite group G the $|G|$–dimensional complex vector space

$$\mathbb{C}G = \bigoplus_{g \in G} \mathbb{C}\,|g\rangle$$

is a ring called the *complex group algebra*,

with multiplication defined by

$$\left(\sum_{g \in G} a(g)\,|g\rangle\right)\left(\sum_{h \in G} b(h)\,|h\rangle\right) = \sum_{g \in G} c(g)\,|g\rangle\,,$$

$a(g), b(g) \in \mathbb{C}$ and $c(g) = \sum_{x \in G} a(x)b(x^{-1}g)$.

The group algebra is the ring of maps from G to $\mathbb{C}$, the map a sending g to $a(g)$ corresponding to $\sum_{g \in G} a(g)\,|g\rangle$.

An element of $\mathbb{C}\mathbb{Z}_n$ will be said to be *periodic* if it is periodic as a map from $\mathbb{Z}_n$ to $\mathbb{C}$.

The Quantum Fourier Transform

The *quantum Fourier transform* on $\mathbb{Z}_n$ is a $\mathbb{C}$-linear map $\mathcal{Q} = \mathcal{Q}_n$ from $\mathbb{C}\mathbb{Z}_n$ to itself

defined on the basis vector $|x\rangle$ by

$$\mathcal{Q}\,|x\rangle = \frac{1}{\sqrt{n}} \sum_{c=0}^{n-1} \overline{\chi^c(x)}\,|c\rangle\,.$$

Extending by linearity:

$$\mathcal{Q}\left(\sum_{x=0}^{n-1} \alpha(x)\,|x\rangle\right) = \sum_{c=0}^{n-1} \hat{\alpha}(c)\,|c\rangle\,,$$

where

$$\hat{\alpha}(c) = \frac{1}{\sqrt{n}} \sum_{x=0}^{n-1} \alpha(x) e^{-\frac{2\pi cxi}{n}}. \tag{6}$$

The Quantum Fourier Transform

The *quantum Fourier transform* on $\mathbb{Z}_n$ is a $\mathbb{C}$-linear map $\mathcal{Q} = \mathcal{Q}_n$ from $\mathbb{C}\mathbb{Z}_n$ to itself

defined on the basis vector $|x\rangle$ by

$$\mathcal{Q}\,|x\rangle = \frac{1}{\sqrt{n}} \sum_{c=0}^{n-1} \overline{\chi^c(x)}\,|c\rangle\,.$$

Extending by linearity:

$$\mathcal{Q}\left(\sum_{x=0}^{n-1} \alpha(x)\,|x\rangle\right) = \sum_{c=0}^{n-1} \hat{\alpha}(c)\,|c\rangle\,,$$

where

$$\hat{\alpha}(c) = \frac{1}{\sqrt{n}} \sum_{x=0}^{n-1} \alpha(x) e^{-\frac{2\pi cxi}{n}}. \tag{6}$$

The Quantum Fourier Transform

The *quantum Fourier transform* on $\mathbb{Z}_n$ is a $\mathbb{C}$-linear map $\mathcal{Q} = \mathcal{Q}_n$ from $\mathbb{C}\mathbb{Z}_n$ to itself

defined on the basis vector $|x\rangle$ by

$$\mathcal{Q}\,|x\rangle = \frac{1}{\sqrt{n}} \sum_{c=0}^{n-1} \overline{\chi^c(x)}\,|c\rangle\,.$$

Extending by linearity:

$$\mathcal{Q}\left(\sum_{x=0}^{n-1} \alpha(x)\,|x\rangle\right) = \sum_{c=0}^{n-1} \hat{\alpha}(c)\,|c\rangle\,,$$

where

$$\hat{\alpha}(c) = \frac{1}{\sqrt{n}} \sum_{x=0}^{n-1} \alpha(x) e^{-\frac{2\pi cxi}{n}}. \tag{6}$$

The Quantum Fourier Transform

The *quantum Fourier transform* on $\mathbb{Z}_n$ is a $\mathbb{C}$-linear map $\mathcal{Q} = \mathcal{Q}_n$ from $\mathbb{C}\mathbb{Z}_n$ to itself

defined on the basis vector $|x\rangle$ by

$$\mathcal{Q}\,|x\rangle = \frac{1}{\sqrt{n}} \sum_{c=0}^{n-1} \overline{\chi^c(x)}\,|c\rangle\,.$$

Extending by linearity:

$$\mathcal{Q}\left(\sum_{x=0}^{n-1} \alpha(x)\,|x\rangle\right) = \sum_{c=0}^{n-1} \hat{\alpha}(c)\,|c\rangle\,,$$

where

$$\hat{\alpha}(c) = \frac{1}{\sqrt{n}} \sum_{x=0}^{n-1} \alpha(x) e^{-\frac{2\pi cxi}{n}}\,. \tag{6}$$

QFT and Periodicity

Lemma

Let $f \in \mathbb{C}\mathbb{Z}_n$ and suppose that f is periodic of period r, where $r|n$.

Then

$$\hat{f}(c) = \begin{cases} \frac{\sqrt{n}}{r} \sum_{s=0}^{r-1} f(s)\overline{\chi_n^c(s)}, & if \ c = 0 \mod n/r \\ 0, & otherwise \end{cases} . \quad (7)$$

QFT and Periodicity

Lemma

Let $f \in \mathbb{C}\mathbb{Z}_n$ and suppose that f is periodic of period r, where $r|n$.

Then

$$\hat{f}(c) = \begin{cases} \dfrac{\sqrt{n}}{r} \displaystyle\sum_{s=0}^{r-1} f(s)\overline{\chi_n^c(s)}, & \text{if } c = 0 \mod n/r \\ 0, & \text{otherwise} \end{cases} . \quad (7)$$

Proof

$$\hat{f}(c) = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} f(k)\overline{\chi^c(k)}$$

$$= \frac{1}{\sqrt{n}} \sum_{a=0}^{r-1} \sum_{s=0}^{\frac{n}{r}-1} f(a+sr)\overline{\chi^c(a+sr)}$$

$$= \frac{1}{\sqrt{n}} \sum_{a=0}^{r-1} f(a)\overline{\chi^c(a)} \sum_{s=0}^{\frac{n}{r}-1} \overline{\chi^c(sr)}.$$

The result follows on applying the lemma above modulo n/r.

Proof

$$\hat{f}(c) = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} f(k)\overline{\chi^c(k)}$$

$$= \frac{1}{\sqrt{n}} \sum_{a=0}^{r-1} \sum_{s=0}^{\frac{n}{r}-1} f(a+sr)\overline{\chi^c(a+sr)}$$

$$= \frac{1}{\sqrt{n}} \sum_{a=0}^{r-1} f(a)\overline{\chi^c(a)} \sum_{s=0}^{\frac{n}{r}-1} \overline{\chi^c(sr)}.$$

The result follows on applying the lemma above modulo n/r.

Cutting Teeth

Assume $f : \mathbb{Z} \to \mathbb{Z}_N$ is periodic of period r and U_f is the standard oracle for f.

Assume $r|N$ and that we use N-ary registers (instead of qubits).

Begin with two registers, of one N-ary quantum bit each, in initial state $|0\rangle\,|0\rangle$.

To the first register apply the Walsh–Hadamard transform to obtain the state

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\,|0\rangle\,.$$

Now apply U_f:

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\,|f(x)\rangle\,.$$

Cutting Teeth

Assume $f : \mathbb{Z} \to \mathbb{Z}_N$ is periodic of period r and U_f is the standard oracle for f.

Assume $r|N$ and that we use N-ary registers (instead of qubits).

Begin with two registers, of one N-ary quantum bit each, in initial state $|0\rangle\,|0\rangle$.

To the first register apply the Walsh–Hadamard transform to obtain the state

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\,|0\rangle\,.$$

Now apply U_f:

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\,|f(x)\rangle\,.$$

Cutting Teeth

Assume $f : \mathbb{Z} \to \mathbb{Z}_N$ is periodic of period r and U_f is the standard oracle for f.

Assume $r|N$ and that we use N-ary registers (instead of qubits).

Begin with two registers, of one N-ary quantum bit each, in initial state $|0\rangle\,|0\rangle$.

To the first register apply the Walsh–Hadamard transform to obtain the state

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\,|0\rangle\,.$$

Now apply U_f:

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\,|f(x)\rangle\,.$$

Cutting Teeth

Assume $f : \mathbb{Z} \to \mathbb{Z}_N$ is periodic of period r and U_f is the standard oracle for f.

Assume $r|N$ and that we use N-ary registers (instead of qubits).

Begin with two registers, of one N-ary quantum bit each, in initial state $|0\rangle\,|0\rangle$.

To the first register apply the Walsh–Hadamard transform to obtain the state

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\,|0\rangle\,.$$

Now apply U_f:

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\,|f(x)\rangle\,.$$

Cutting Teeth

Assume $f : \mathbb{Z} \to \mathbb{Z}_N$ is periodic of period r and U_f is the standard oracle for f.

Assume $r|N$ and that we use N-ary registers (instead of qubits).

Begin with two registers, of one N-ary quantum bit each, in initial state $|0\rangle\,|0\rangle$.

To the first register apply the Walsh–Hadamard transform to obtain the state

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\,|0\rangle\,.$$

Now apply U_f:

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\,|f(x)\rangle\,.$$

Now observe the second register and obtain, uniformly at random, some value y_0 in the image of f.

The system then projects to the state

$$\frac{1}{\sqrt{|f^{-1}(y_0)|}} \sum_{x \in f^{-1}(y_0)} |x\rangle |y_0\rangle .$$

Since f is periodic with period r there is precisely one value x_0 with $0 \leq x_0 < r$ such that $f(x_0) = y_0$.

Now observe the second register and obtain, uniformly at random, some value y_0 in the image of f.

The system then projects to the state

$$\frac{1}{\sqrt{|f^{-1}(y_0)|}} \sum_{x \in f^{-1}(y_0)} |x\rangle \, |y_0\rangle \, .$$

Since f is periodic with period r there is precisely one value x_0 with $0 \leq x_0 < r$ such that $f(x_0) = y_0$.

Now observe the second register and obtain, uniformly at random, some value y_0 in the image of f.

The system then projects to the state

$$\frac{1}{\sqrt{|f^{-1}(y_0)|}} \sum_{x \in f^{-1}(y_0)} |x\rangle \, |y_0\rangle \, .$$

Since f is periodic with period r there is precisely one value x_0 with $0 \leq x_0 < r$ such that $f(x_0) = y_0$.

If we set $K = N/r$ then, in the first register, we have the state

$$|\psi\rangle = \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} |x_0 + kr\rangle$$
$$= \sum_{x=0}^{N-1} \psi(x) |x\rangle ,$$

where

$$\psi(x) = \begin{cases} \frac{1}{\sqrt{K}} = \sqrt{\frac{r}{N}}, & \text{if } r|x - x_0 \\ 0, & \text{otherwise} \end{cases} .$$

Thus $\psi \in \mathbb{C}\mathbb{Z}_N$ is periodic with period r.

If we set $K = N/r$ then, in the first register, we have the state

$$|\psi\rangle = \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} |x_0 + kr\rangle$$
$$= \sum_{x=0}^{N-1} \psi(x) |x\rangle ,$$

where

$$\psi(x) = \begin{cases} \frac{1}{\sqrt{K}} = \sqrt{\frac{r}{N}}, & \text{if } r|x - x_0 \\ 0, & \text{otherwise} \end{cases} .$$

Thus $\psi \in \mathbb{C}\mathbb{Z}_N$ is periodic with period r.

If we set $K = N/r$ then, in the first register, we have the state

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} |x_0 + kr\rangle \\ &= \sum_{x=0}^{N-1} \psi(x) |x\rangle , \end{aligned}$$

where

$$\psi(x) = \begin{cases} \dfrac{1}{\sqrt{K}} = \sqrt{\dfrac{r}{N}}, & \text{if } r|x - x_0 \\ 0, & \text{otherwise} \end{cases} .$$

Thus $\psi \in \mathbb{C}\mathbb{Z}_N$ is periodic with period r.

If we set $K = N/r$ then, in the first register, we have the state

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} |x_0 + kr\rangle \\ &= \sum_{x=0}^{N-1} \psi(x) \, |x\rangle \, , \end{aligned}$$

where

$$\psi(x) = \begin{cases} \dfrac{1}{\sqrt{K}} = \sqrt{\dfrac{r}{N}}, & \text{if } \; r | x - x_0 \\ 0, & \text{otherwise} \end{cases} \; .$$

Thus $\psi \in \mathbb{C}\mathbb{Z}_N$ is periodic with period r.

Apply $\mathcal{Q}$ to the first register:

$$\mathcal{Q}\,|\psi\rangle = \sum_{c=0}^{N-1} \hat{\psi}(c)\,|c\rangle\,,$$

where

$$\hat{\psi}(c) = \begin{cases} \dfrac{\sqrt{N}}{r} \displaystyle\sum_{s=0}^{r-1} \psi(s)\overline{\chi^c(s)}, & \text{if } c = 0 \mod \frac{N}{r} \\ 0, & \text{otherwise} \end{cases}$$

$$= \begin{cases} \dfrac{1}{\sqrt{r}}\overline{\chi^c(x_0)}, & \text{if } c = 0 \mod \frac{N}{r} \\ 0, & \text{otherwise} \end{cases},$$

since $\psi(x_0) = 1/\sqrt{K}$ and $\psi(s) = 0$ for all $s \neq x_0$.

Apply $\mathcal{Q}$ to the first register:

$$\mathcal{Q}\,|\psi\rangle = \sum_{c=0}^{N-1} \hat{\psi}(c)\,|c\rangle\,,$$

where

$$\hat{\psi}(c) = \begin{cases} \dfrac{\sqrt{N}}{r} \displaystyle\sum_{s=0}^{r-1} \psi(s)\overline{\chi^c(s)}, & \text{if } c = 0 \mod \frac{N}{r} \\ 0, & \text{otherwise} \end{cases}$$

$$= \begin{cases} \dfrac{1}{\sqrt{r}}\overline{\chi^c(x_0)}, & \text{if } c = 0 \mod \frac{N}{r} \\ 0, & \text{otherwise} \end{cases},$$

since $\psi(x_0) = 1/\sqrt{K}$ and $\psi(s) = 0$ for all $s \neq x_0$.

Observe this state to obtain a value $c = c(s)$ which is a multiple of N/r.

In fact, for a uniformly random $s \in \{0, \ldots, r-1\}$ we have

$$c = s\frac{N}{r} \implies \frac{c}{N} = \frac{s}{r}$$

where the fraction c/N is known.

If we reduce c/N down to lowest terms then we may determine r, as the denominator of this irreducible fraction, provided that $\gcd(s, r) = 1$.

If s and r are not coprime then we will obtain a proper factor of r and not r itself ....

Observe this state to obtain a value $c = c(s)$ which is a multiple of N/r.

In fact, for a uniformly random $s \in \{0, \ldots, r-1\}$ we have

$$c = s\frac{N}{r} \implies \frac{c}{N} = \frac{s}{r}$$

where the fraction c/N is known.

If we reduce c/N down to lowest terms then we may determine r, as the denominator of this irreducible fraction, provided that $\gcd(s, r) = 1$.

If s and r are not coprime then we will obtain a proper factor of r and not r itself ....

Observe this state to obtain a value $c = c(s)$ which is a multiple of N/r.

In fact, for a uniformly random $s \in \{0, \ldots, r-1\}$ we have

$$c = s\frac{N}{r} \implies \frac{c}{N} = \frac{s}{r}$$

where the fraction c/N is known.

If we reduce c/N down to lowest terms then we may determine r, as the denominator of this irreducible fraction, provided that $\gcd(s, r) = 1$.

If s and r are not coprime then we will obtain a proper factor of r and not r itself ....

Observe this state to obtain a value $c = c(s)$ which is a multiple of N/r.

In fact, for a uniformly random $s \in \{0, \ldots, r-1\}$ we have

$$c = s\frac{N}{r} \implies \frac{c}{N} = \frac{s}{r}$$

where the fraction c/N is known.

If we reduce c/N down to lowest terms then we may determine r, as the denominator of this irreducible fraction, provided that $\gcd(s, r) = 1$.

If s and r are not coprime then we will obtain a proper factor of r and not r itself ....

....however

$$\liminf \left(\frac{\phi(n)}{n/\log_e \log_e n} \right) = e^{-\gamma}$$

where γ is *Euler's constant*.

This means that if we choose a random number from $\{0, \ldots, n-1\}$ then the probability $p(n)$ that it is coprime to n satisfies

$$p(n) = \frac{\phi(n)}{n} \geq \frac{e^{-\gamma}}{\log_e \log_e n}. \tag{8}$$

So we obtain a number coprime to N with probability $1 - \varepsilon$, where $\varepsilon > 0$ can be made arbitrarily small, by repeating the above observation $O(\log_e \log_e N)$ times.

....however

$$\liminf \left(\frac{\phi(n)}{n/\log_e \log_e n} \right) = e^{-\gamma}$$

where γ is *Euler's constant*.

This means that if we choose a random number from $\{0, \ldots, n-1\}$ then the probability $p(n)$ that it is coprime to n satisfies

$$p(n) = \frac{\phi(n)}{n} \geq \frac{e^{-\gamma}}{\log_e \log_e n}. \tag{8}$$

So we obtain a number coprime to N with probability $1 - \varepsilon$, where $\varepsilon > 0$ can be made arbitrarily small, by repeating the above observation $O(\log_e \log_e N)$ times.

....however

$$\liminf \left(\frac{\phi(n)}{n/\log_e \log_e n} \right) = e^{-\gamma}$$

where γ is *Euler's constant*.

This means that if we choose a random number from $\{0, \ldots, n-1\}$ then the probability $p(n)$ that it is coprime to n satisfies

$$p(n) = \frac{\phi(n)}{n} \geq \frac{e^{-\gamma}}{\log_e \log_e n}. \tag{8}$$

So we obtain a number coprime to N with probability $1 - \varepsilon$, where $\varepsilon > 0$ can be made arbitrarily small, by repeating the above observation $O(\log_e \log_e N)$ times.

....however

$$\liminf \left(\frac{\phi(n)}{n/\log_e \log_e n} \right) = e^{-\gamma}$$

where γ is *Euler's constant*.

This means that if we choose a random number from $\{0, \ldots, n-1\}$ then the probability $p(n)$ that it is coprime to n satisfies

$$p(n) = \frac{\phi(n)}{n} \geq \frac{e^{-\gamma}}{\log_e \log_e n}. \tag{8}$$

So we obtain a number coprime to N with probability $1 - \varepsilon$, where $\varepsilon > 0$ can be made arbitrarily small, by repeating the above observation $O(\log_e \log_e N)$ times.

Example

Suppose the function $f : \mathbb{Z}_{21} \to \mathbb{Z}_{21}$ is given by $f(k) = 4^k$ and has period r, which we wish to find.

After applying W_{21} and U_f we have the state

$$\frac{1}{\sqrt{21}}[(|0\rangle + |3\rangle + |6\rangle + |9\rangle + |12\rangle + |15\rangle + |18\rangle)\,|1\rangle$$
$$+(|1\rangle + |4\rangle + |7\rangle + |10\rangle + |13\rangle + |16\rangle + |19\rangle)\,|4\rangle$$
$$+(|2\rangle + |5\rangle + |8\rangle + |11\rangle + |14\rangle + |17\rangle + |20\rangle)\,|16\rangle].$$

Example

Suppose the function $f : \mathbb{Z}_{21} \to \mathbb{Z}_{21}$ is given by $f(k) = 4^k$ and has period r, which we wish to find.

After applying W_{21} and U_f we have the state

$$\frac{1}{\sqrt{21}}[(|0\rangle + |3\rangle + |6\rangle + |9\rangle + |12\rangle + |15\rangle + |18\rangle)\,|1\rangle$$
$$+(|1\rangle + |4\rangle + |7\rangle + |10\rangle + |13\rangle + |16\rangle + |19\rangle)\,|4\rangle$$
$$+(|2\rangle + |5\rangle + |8\rangle + |11\rangle + |14\rangle + |17\rangle + |20\rangle)\,|16\rangle].$$

Observing the second register we obtain, with probability 1/3, one of 1, 4 or 16.

The first register then contains $|\psi_0\rangle$, $|\psi_1\rangle$ or $|\psi_2\rangle$, where $|\psi_s\rangle = \sum_{k=0}^{6} |s+3k\rangle$.

Applying $\mathcal{Q}_{21}$ to these states we have

$$\mathcal{Q}\,|\psi_0\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |7\rangle + |14\rangle) \text{ or}$$

$$\mathcal{Q}\,|\psi_1\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \omega\,|7\rangle + \omega^2\,|14\rangle) \text{ or}$$

$$\mathcal{Q}\,|\psi_2\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \omega^2\,|7\rangle + \omega\,|14\rangle),$$

where $\omega = e^{-2\pi i/3}$.

Observing the second register we obtain, with probability $1/3$, one of 1, 4 or 16.

The first register then contains $|\psi_0\rangle$, $|\psi_1\rangle$ or $|\psi_2\rangle$, where $|\psi_s\rangle = \sum_{k=0}^{6} |s + 3k\rangle$.

Applying $\mathcal{Q}_{21}$ to these states we have

$$\mathcal{Q}\,|\psi_0\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |7\rangle + |14\rangle) \text{ or}$$

$$\mathcal{Q}\,|\psi_1\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \omega\,|7\rangle + \omega^2\,|14\rangle) \text{ or}$$

$$\mathcal{Q}\,|\psi_2\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \omega^2\,|7\rangle + \omega\,|14\rangle),$$

where $\omega = e^{-2\pi i/3}$.

Observing the second register we obtain, with probability $1/3$, one of 1, 4 or 16.

The first register then contains $|\psi_0\rangle$, $|\psi_1\rangle$ or $|\psi_2\rangle$, where $|\psi_s\rangle = \sum_{k=0}^{6} |s+3k\rangle$.

Applying $\mathcal{Q}_{21}$ to these states we have

$$\mathcal{Q}\,|\psi_0\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |7\rangle + |14\rangle) \text{ or}$$
$$\mathcal{Q}\,|\psi_1\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \omega\,|7\rangle + \omega^2\,|14\rangle) \text{ or}$$
$$\mathcal{Q}\,|\psi_2\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \omega^2\,|7\rangle + \omega\,|14\rangle),$$

where $\omega = e^{-2\pi i/3}$.

Whichever of these we have, observation now yields, with equal probabilities, $c = 0$, $c = 7$ or $c = 14$.

If we observe $c = 0$ then the process must be run again.

If we observe $c = 7$ then $c/N = 7/21 = 1/3$ and the denominator of this fraction is r.

Similarly, if $c = 14$ we read r off from $c/N = 14/21 = 2/3$.

Whichever of these we have, observation now yields, with equal probabilities, $c = 0$, $c = 7$ or $c = 14$.

If we observe $c = 0$ then the process must be run again.

If we observe $c = 7$ then $c/N = 7/21 = 1/3$ and the denominator of this fraction is r.

Similarly, if $c = 14$ we read r off from $c/N = 14/21 = 2/3$.

Whichever of these we have, observation now yields, with equal probabilities, $c = 0$, $c = 7$ or $c = 14$.

If we observe $c = 0$ then the process must be run again.

If we observe $c = 7$ then $c/N = 7/21 = 1/3$ and the denominator of this fraction is r.

Similarly, if $c = 14$ we read r off from $c/N = 14/21 = 2/3$.

Whichever of these we have, observation now yields, with equal probabilities, $c = 0$, $c = 7$ or $c = 14$.

If we observe $c = 0$ then the process must be run again.

If we observe $c = 7$ then $c/N = 7/21 = 1/3$ and the denominator of this fraction is r.

Similarly, if $c = 14$ we read r off from $c/N = 14/21 = 2/3$.

The Search Problem

Given an N element set X and a map $P : X \to \{0, 1\}$ find $x \in X$ such that $P(x) = 1$.

Assume there's an oracle to evaluate $P(x)$ for a given $x \in X$.

Classically: requires $N - M + 1$ evaluations to find a solution x with certainty,

and $O(N/M)$ evaluations to find one with high probability.

Grover's quantum algorithm: $O(\sqrt{N/M})$.

The Search Problem

Given an N element set X and a map $P : X \to \{0, 1\}$ find $x \in X$ such that $P(x) = 1$.

Assume there's an oracle to evaluate $P(x)$ for a given $x \in X$.

Classically: requires $N - M + 1$ evaluations to find a solution x with certainty,

and $O(N/M)$ evaluations to find one with high probability.

Grover's quantum algorithm: $O(\sqrt{N/M})$.

The Search Problem

Given an N element set X and a map $P : X \to \{0, 1\}$ find $x \in X$ such that $P(x) = 1$.

Assume there's an oracle to evaluate $P(x)$ for a given $x \in X$.

Classically: requires $N - M + 1$ evaluations to find a solution x with certainty,

and $O(N/M)$ evaluations to find one with high probability.

Grover's quantum algorithm: $O(\sqrt{N/M})$.

The Search Problem

Given an N element set X and a map $P : X \to \{0, 1\}$ find $x \in X$ such that $P(x) = 1$.

Assume there's an oracle to evaluate $P(x)$ for a given $x \in X$.

Classically: requires $N - M + 1$ evaluations to find a solution x with certainty,

and $O(N/M)$ evaluations to find one with high probability.

Grover's quantum algorithm: $O(\sqrt{N/M})$.

The Search Problem

Given an N element set X and a map $P : X \to \{0, 1\}$ find $x \in X$ such that $P(x) = 1$.

Assume there's an oracle to evaluate $P(x)$ for a given $x \in X$.

Classically: requires $N - M + 1$ evaluations to find a solution x with certainty,

and $O(N/M)$ evaluations to find one with high probability.

Grover's quantum algorithm: $O(\sqrt{N/M})$.

Overview

- Suppose that N has size 2^n.
- Prepare the standard superposition of all possible outputs
- Find a state $|x\rangle \otimes |1\rangle$ for some x. By direct measurement at this stage, there is only a probability of $M/2^n$ of finding such a state.
- Increase the amplitude of vectors of the form $|x\rangle \otimes |1\rangle$ and decrease the amplitude of those of the form $|x\rangle \otimes |0\rangle$ (somehow) until the state approximates

$$\frac{1}{\sqrt{M}} \sum_{i=1}^{M} |x_i\rangle \otimes |1\rangle \,, \tag{9}$$

  where the solution set is $\{x_1, \ldots, x_M\}$.
- Measuring this altered state then gives a solution with high probability.

Overview

- Suppose that N has size 2^n.
- Prepare the standard superposition of all possible outputs
- Find a state $|x\rangle \otimes |1\rangle$ for some x. By direct measurement at this stage, there is only a probability of $M/2^n$ of finding such a state.
- Increase the amplitude of vectors of the form $|x\rangle \otimes |1\rangle$ and decrease the amplitude of those of the form $|x\rangle \otimes |0\rangle$ (somehow) until the state approximates

$$\frac{1}{\sqrt{M}} \sum_{i=1}^{M} |x_i\rangle \otimes |1\rangle \,, \tag{9}$$

  where the solution set is $\{x_1, \ldots, x_M\}$.
- Measuring this altered state then gives a solution with high probability.

Overview

- Suppose that N has size 2^n.
- Prepare the standard superposition of all possible outputs
- Find a state $|x\rangle \otimes |1\rangle$ for some x. By direct measurement at this stage, there is only a probability of $M/2^n$ of finding such a state.
- Increase the amplitude of vectors of the form $|x\rangle \otimes |1\rangle$ and decrease the amplitude of those of the form $|x\rangle \otimes |0\rangle$ (somehow) until the state approximates

$$\frac{1}{\sqrt{M}} \sum_{i=1}^{M} |x_i\rangle \otimes |1\rangle \,, \tag{9}$$

  where the solution set is $\{x_1, \ldots, x_M\}$.
- Measuring this altered state then gives a solution with high probability.

Overview

- Suppose that N has size 2^n.
- Prepare the standard superposition of all possible outputs
- Find a state $|x\rangle \otimes |1\rangle$ for some x. By direct measurement at this stage, there is only a probability of $M/2^n$ of finding such a state.
- Increase the amplitude of vectors of the form $|x\rangle \otimes |1\rangle$ and decrease the amplitude of those of the form $|x\rangle \otimes |0\rangle$ (somehow) until the state approximates

$$\frac{1}{\sqrt{M}} \sum_{i=1}^{M} |x_i\rangle \otimes |1\rangle , \tag{9}$$

  where the solution set is $\{x_1, \ldots, x_M\}$.
- Measuring this altered state then gives a solution with high probability.

Overview

- Suppose that N has size 2^n.
- Prepare the standard superposition of all possible outputs
- Find a state $|x\rangle \otimes |1\rangle$ for some x. By direct measurement at this stage, there is only a probability of $M/2^n$ of finding such a state.
- Increase the amplitude of vectors of the form $|x\rangle \otimes |1\rangle$ and decrease the amplitude of those of the form $|x\rangle \otimes |0\rangle$ (somehow) until the state approximates

$$\frac{1}{\sqrt{M}} \sum_{i=1}^{M} |x_i\rangle \otimes |1\rangle , \tag{9}$$

where the solution set is $\{x_1, \ldots, x_M\}$.

- Measuring this altered state then gives a solution with high probability.

Overview

- Suppose that N has size 2^n.
- Prepare the standard superposition of all possible outputs
- Find a state $|x\rangle \otimes |1\rangle$ for some x. By direct measurement at this stage, there is only a probability of $M/2^n$ of finding such a state.
- Increase the amplitude of vectors of the form $|x\rangle \otimes |1\rangle$ and decrease the amplitude of those of the form $|x\rangle \otimes |0\rangle$ (somehow) until the state approximates

$$\frac{1}{\sqrt{M}} \sum_{i=1}^{M} |x_i\rangle \otimes |1\rangle , \tag{9}$$

  where the solution set is $\{x_1, \ldots, x_M\}$.
- Measuring this altered state then gives a solution with high probability.

Overview

- Suppose that N has size 2^n.
- Prepare the standard superposition of all possible outputs
- Find a state $|x\rangle \otimes |1\rangle$ for some x. By direct measurement at this stage, there is only a probability of $M/2^n$ of finding such a state.
- Increase the amplitude of vectors of the form $|x\rangle \otimes |1\rangle$ and decrease the amplitude of those of the form $|x\rangle \otimes |0\rangle$ (somehow) until the state approximates

$$\frac{1}{\sqrt{M}} \sum_{i=1}^{M} |x_i\rangle \otimes |1\rangle , \tag{9}$$

  where the solution set is $\{x_1, \ldots, x_M\}$.
- Measuring this altered state then gives a solution with high probability.

For simplicity we assume that we know in advance that there are exactly M solutions, where $M \geq 1$.

The standard oracle for P is U_P: $|x\rangle \otimes |y\rangle$ to $|x\rangle \otimes |P(x) \oplus y\rangle$.

The underlying quantum system consists of a first register of n qubits and second register, called the *oracle workspace*, of a single qubit.

Apply $W^n \otimes W$ followed by U_P to the input state $|0\rangle^{\otimes n} \otimes |1\rangle$.

The first register then contains

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{P(x)} |x\rangle. \tag{10}$$

For simplicity we assume that we know in advance that there are exactly M solutions, where $M \geq 1$.

The standard oracle for P is U_P: $|x\rangle \otimes |y\rangle$ to $|x\rangle \otimes |P(x) \oplus y\rangle$.

The underlying quantum system consists of a first register of n qubits and second register, called the *oracle workspace*, of a single qubit.

Apply $W^n \otimes W$ followed by U_P to the input state $|0\rangle^{\otimes n} \otimes |1\rangle$.

The first register then contains

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{P(x)} |x\rangle. \tag{10}$$

For simplicity we assume that we know in advance that there are exactly M solutions, where $M \geq 1$.

The standard oracle for P is U_P: $|x\rangle \otimes |y\rangle$ to $|x\rangle \otimes |P(x) \oplus y\rangle$.

The underlying quantum system consists of a first register of n qubits and second register, called the *oracle workspace*, of a single qubit.

Apply $W^n \otimes W$ followed by U_P to the input state $|0\rangle^{\otimes n} \otimes |1\rangle$.

The first register then contains

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{P(x)} |x\rangle. \tag{10}$$

For simplicity we assume that we know in advance that there are exactly M solutions, where $M \geq 1$.

The standard oracle for P is U_P: $|x\rangle \otimes |y\rangle$ to $|x\rangle \otimes |P(x) \oplus y\rangle$.

The underlying quantum system consists of a first register of n qubits and second register, called the *oracle workspace*, of a single qubit.

Apply $W^n \otimes W$ followed by U_P to the input state $|0\rangle^{\otimes n} \otimes |1\rangle$.

The first register then contains

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{P(x)} |x\rangle. \tag{10}$$

For simplicity we assume that we know in advance that there are exactly M solutions, where $M \geq 1$.

The standard oracle for P is U_P: $|x\rangle \otimes |y\rangle$ to $|x\rangle \otimes |P(x) \oplus y\rangle$.

The underlying quantum system consists of a first register of n qubits and second register, called the *oracle workspace*, of a single qubit.

Apply $W^n \otimes W$ followed by U_P to the input state $|0\rangle^{\otimes n} \otimes |1\rangle$.

The first register then contains

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{P(x)} |x\rangle. \tag{10}$$

Inversion about the Mean

Define the unitary transformation $F = W_n T W_n$, where T is the *conditional phase shift* operator given by

$$T|0\rangle = |0\rangle \quad \text{and} \quad T|x\rangle = -|x\rangle, \quad \text{for all} \quad x \neq 0.$$

Apply F to the state (10) (that is apply $F \otimes I$ to the quantum system).

Repeat the process, applying U_P followed by F untill the amplitudes of the solutions approach $1/\sqrt{M}$ and the amplitudes of all other basis vectors approach zero.

Inversion about the Mean

Define the unitary transformation $F = W_n T W_n$, where T is the *conditional phase shift* operator given by

$$T|0\rangle = |0\rangle \quad \text{and} \quad T|x\rangle = -|x\rangle, \quad \text{for all} \quad x \neq 0.$$

Apply F to the state (10) (that is apply $F \otimes I$ to the quantum system).

Repeat the process, applying U_P followed by F untill the amplitudes of the solutions approach $1/\sqrt{M}$ and the amplitudes of all other basis vectors approach zero.

Inversion about the Mean

Define the unitary transformation $F = W_n T W_n$, where T is the *conditional phase shift* operator given by

$$T|0\rangle = |0\rangle \quad \text{and} \quad T|x\rangle = -|x\rangle, \quad \text{for all} \quad x \neq 0.$$

Apply F to the state (10) (that is apply $F \otimes I$ to the quantum system).

Repeat the process, applying U_P followed by F untill the amplitudes of the solutions approach $1/\sqrt{M}$ and the amplitudes of all other basis vectors approach zero.

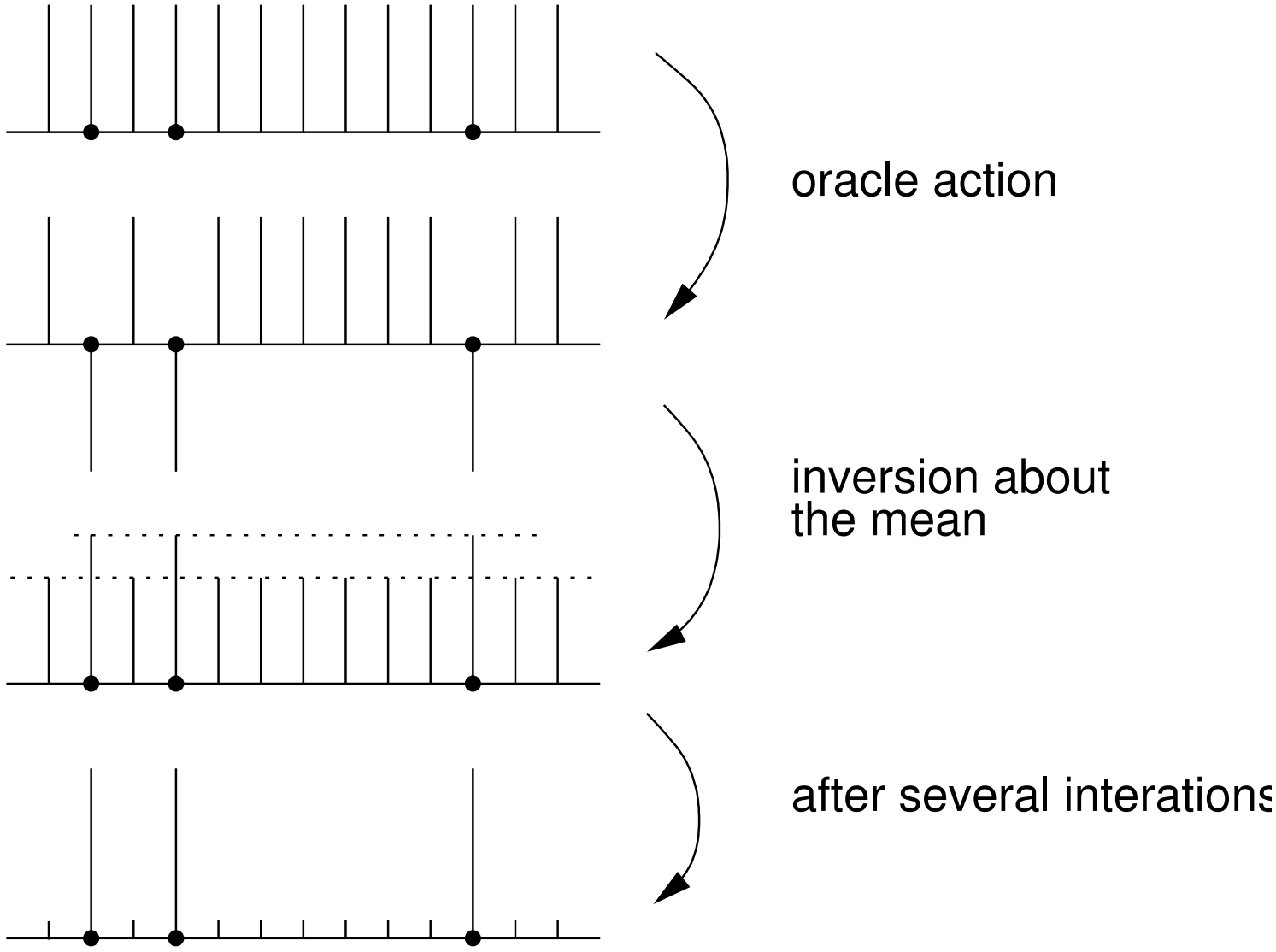

Figure: Operation of Grover's algorithm

Call the composite function $\mathcal{G} = (F \otimes I) \circ U_P$ the *Grover operator*.

The question is how many iterations of $\mathcal{G}$ to repeat before halting.

The number of iterations must be chosen carefully, as the amplitudes of the solutions do not approach a steady state but rather oscillate.

As we shall see, the required number of iterations is $O(\sqrt{N/M})$.

Call the composite function $\mathcal{G} = (F \otimes I) \circ U_P$ the *Grover operator*.

The question is how many iterations of $\mathcal{G}$ to repeat before halting.

The number of iterations must be chosen carefully, as the amplitudes of the solutions do not approach a steady state but rather oscillate.

As we shall see, the required number of iterations is $O(\sqrt{N/M})$.

Call the composite function $\mathcal{G} = (F \otimes I) \circ U_P$ the *Grover operator*.

The question is how many iterations of $\mathcal{G}$ to repeat before halting.

The number of iterations must be chosen carefully, as the amplitudes of the solutions do not approach a steady state but rather oscillate.

As we shall see, the required number of iterations is $O(\sqrt{N/M})$.

Call the composite function $\mathcal{G} = (F \otimes I) \circ U_P$ the *Grover operator*.

The question is how many iterations of $\mathcal{G}$ to repeat before halting.

The number of iterations must be chosen carefully, as the amplitudes of the solutions do not approach a steady state but rather oscillate.

As we shall see, the required number of iterations is $O(\sqrt{N/M})$.

Call the composite function $\mathcal{G} = (F \otimes I) \circ U_P$ the *Grover operator*.

The question is how many iterations of $\mathcal{G}$ to repeat before halting.

The number of iterations must be chosen carefully, as the amplitudes of the solutions do not approach a steady state but rather oscillate.

As we shall see, the required number of iterations is $O(\sqrt{N/M})$.

Inversion about the Mean

$$T = 2|0\rangle\langle 0| - I.$$

Inversion about the mean is then given by

$$F = W^{\otimes n}(2|0\rangle\langle 0| - I)W^{\otimes n}. \tag{11}$$

If we let

$$|\psi\rangle = W^{\otimes n}|0\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$

then we have

$$\langle\psi| = \langle 0|W^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\langle x|.$$

It follows that

$$F = 2|\psi\rangle\langle\psi| - I. \tag{12}$$

Inversion about the Mean

$$T = 2|0\rangle\langle 0| - I.$$

Inversion about the mean is then given by

$$F = W^{\otimes n}(2|0\rangle\langle 0| - I)W^{\otimes n}. \tag{11}$$

If we let

$$|\psi\rangle = W^{\otimes n}|0\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$

then we have

$$\langle\psi| = \langle 0|W^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\langle x|.$$

It follows that

$$F = 2|\psi\rangle\langle\psi| - I. \tag{12}$$

Inversion about the Mean

$$T = 2|0\rangle\langle 0| - I.$$

Inversion about the mean is then given by

$$F = W^{\otimes n}(2|0\rangle\langle 0| - I)W^{\otimes n}. \tag{11}$$

If we let

$$|\psi\rangle = W^{\otimes n}|0\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$

then we have

$$\langle\psi| = \langle 0|W^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\langle x|.$$

It follows that

$$F = 2|\psi\rangle\langle\psi| - I. \tag{12}$$

Inversion about the Mean

$$T = 2|0\rangle\langle 0| - I.$$

Inversion about the mean is then given by

$$F = W^{\otimes n}(2|0\rangle\langle 0| - I)W^{\otimes n}. \tag{11}$$

If we let

$$|\psi\rangle = W^{\otimes n}|0\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$

then we have

$$\langle\psi| = \langle 0|W^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\langle x|.$$

It follows that

$$F = 2|\psi\rangle\langle\psi| - I. \tag{12}$$

Inversion about the Mean

$$T = 2|0\rangle\langle 0| - I.$$

Inversion about the mean is then given by

$$F = W^{\otimes n}(2|0\rangle\langle 0| - I)W^{\otimes n}. \tag{11}$$

If we let

$$|\psi\rangle = W^{\otimes n}|0\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$

then we have

$$\langle\psi| = \langle 0|W^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\langle x|.$$

It follows that

$$F = 2|\psi\rangle\langle\psi| - I. \tag{12}$$

Consider the action of this operator on a general quantum state.

$$(2|\psi\rangle\langle\psi| - I)\sum_k \alpha_k|k\rangle = 2\sum_k \alpha_k|\psi\rangle\langle\psi|k\rangle - \sum_k \alpha_k|k\rangle.$$

Now (after some calculation)

$$\sum_k \alpha_k|\psi\rangle\langle\psi|k\rangle = A\sum_{x=0}^{N-1}|x\rangle,$$

where

$$A = \frac{1}{N}\sum_k \alpha_k$$

is the mean of the α_k's.

So

$$F\left(\sum_{k=0}^{N-1}\alpha_k|k\rangle\right) = \sum_{k=0}^{N-1}(2A - \alpha_k)|k\rangle.$$

i.e. F reflects the amplitudes α_k about their mean value A.

Consider the action of this operator on a general quantum state.

$$(2|\psi\rangle\langle\psi| - I)\sum_k \alpha_k|k\rangle = 2\sum_k \alpha_k|\psi\rangle\langle\psi|k\rangle - \sum_k \alpha_k|k\rangle.$$

Now (after some calculation)

$$\sum_k \alpha_k|\psi\rangle\langle\psi|k\rangle = A\sum_{x=0}^{N-1}|x\rangle,$$

where

$$A = \frac{1}{N}\sum_k \alpha_k$$

is the mean of the α_k's.

So

$$F\left(\sum_{k=0}^{N-1}\alpha_k|k\rangle\right) = \sum_{k=0}^{N-1}(2A - \alpha_k)|k\rangle.$$

i.e. F reflects the amplitudes α_k about their mean value A.

Consider the action of this operator on a general quantum state.

$$(2|\psi\rangle\langle\psi| - I)\sum_k \alpha_k|k\rangle = 2\sum_k \alpha_k|\psi\rangle\langle\psi|k\rangle - \sum_k \alpha_k|k\rangle.$$

Now (after some calculation)

$$\sum_k \alpha_k|\psi\rangle\langle\psi|k\rangle = A\sum_{x=0}^{N-1}|x\rangle,$$

where

$$A = \frac{1}{N}\sum_k \alpha_k$$

is the mean of the α_k's.

So

$$F\left(\sum_{k=0}^{N-1}\alpha_k\,|k\rangle\right) = \sum_{k=0}^{N-1}(2A - \alpha_k)|k\rangle.$$

i.e. F reflects the amplitudes α_k about their mean value A.

Consider the action of this operator on a general quantum state.

$$(2|\psi\rangle\langle\psi| - I)\sum_k \alpha_k|k\rangle = 2\sum_k \alpha_k|\psi\rangle\langle\psi|k\rangle - \sum_k \alpha_k|k\rangle.$$

Now (after some calculation)

$$\sum_k \alpha_k|\psi\rangle\langle\psi|k\rangle = A\sum_{x=0}^{N-1}|x\rangle,$$

where

$$A = \frac{1}{N}\sum_k \alpha_k$$

is the mean of the α_k's.

So

$$F\left(\sum_{k=0}^{N-1}\alpha_k\,|k\rangle\right) = \sum_{k=0}^{N-1}(2A - \alpha_k)|k\rangle.$$

i.e. F reflects the amplitudes α_k about their mean value A.

The Grover operator as rotation

Let

$$|a\rangle = \frac{1}{\sqrt{N-M}} \sum_{P(x)=0} |x\rangle, \quad |b\rangle = \frac{1}{\sqrt{M}} \sum_{P(x)=1} |x\rangle.$$

The initial state of the system is

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle,$$

which can be written as

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}|a\rangle + \sqrt{\frac{M}{N}}|b\rangle. \tag{13}$$

Claim: the Grover operator keeps the quantum state in the plane S spanned by $|a\rangle$ and $|b\rangle$.

The Grover operator as rotation

Let

$$|a\rangle = \frac{1}{\sqrt{N-M}} \sum_{P(x)=0} |x\rangle, \quad |b\rangle = \frac{1}{\sqrt{M}} \sum_{P(x)=1} |x\rangle.$$

The initial state of the system is

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle,$$

which can be written as

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}|a\rangle + \sqrt{\frac{M}{N}}|b\rangle. \tag{13}$$

Claim: the Grover operator keeps the quantum state in the plane S spanned by $|a\rangle$ and $|b\rangle$.

The Grover operator as rotation

Let

$$|a\rangle = \frac{1}{\sqrt{N-M}} \sum_{P(x)=0} |x\rangle, \quad |b\rangle = \frac{1}{\sqrt{M}} \sum_{P(x)=1} |x\rangle.$$

The initial state of the system is

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle,$$

which can be written as

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}|a\rangle + \sqrt{\frac{M}{N}}|b\rangle. \tag{13}$$

Claim: the Grover operator keeps the quantum state in the plane S spanned by $|a\rangle$ and $|b\rangle$.

The Grover operator as rotation

Let

$$|a\rangle = \frac{1}{\sqrt{N-M}} \sum_{P(x)=0} |x\rangle, \quad |b\rangle = \frac{1}{\sqrt{M}} \sum_{P(x)=1} |x\rangle.$$

The initial state of the system is

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle,$$

which can be written as

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}|a\rangle + \sqrt{\frac{M}{N}}|b\rangle. \tag{13}$$

Claim: the Grover operator keeps the quantum state in the plane S spanned by $|a\rangle$ and $|b\rangle$.

Define an operator O of the first register by

$$U_P(|x\rangle \otimes |w\rangle) = (O\,|x\rangle) \otimes |w\rangle\,.$$

This is possible since U_P leaves $|w\rangle$ unchanged.

O determins the action of the oracle on the first register, given that the second register is in state $|w\rangle$.

Now let $G = F \circ O$. Then the operation of $\mathcal{G}$ on the first register is determined by G.

The aim is to show that S is invariant under G.

Define an operator O of the first register by

$$U_P(|x\rangle \otimes |w\rangle) = (O\,|x\rangle) \otimes |w\rangle\,.$$

This is possible since U_P leaves $|w\rangle$ unchanged.

O determins the action of the oracle on the first register, given that the second register is in state $|w\rangle$.

Now let $G = F \circ O$. Then the operation of $\mathcal{G}$ on the first register is determined by G.

The aim is to show that S is invariant under G.

Define an operator O of the first register by

$$U_P(|x\rangle \otimes |w\rangle) = (O\,|x\rangle) \otimes |w\rangle\,.$$

This is possible since U_P leaves $|w\rangle$ unchanged.

O determins the action of the oracle on the first register, given that the second register is in state $|w\rangle$.

Now let $G = F \circ O$. Then the operation of $\mathcal{G}$ on the first register is determined by G.

The aim is to show that S is invariant under G.

Define an operator O of the first register by

$$U_P(|x\rangle \otimes |w\rangle) = (O\,|x\rangle) \otimes |w\rangle\,.$$

This is possible since U_P leaves $|w\rangle$ unchanged.

O determins the action of the oracle on the first register, given that the second register is in state $|w\rangle$.

Now let $G = F \circ O$. Then the operation of $\mathcal{G}$ on the first register is determined by G.

The aim is to show that S is invariant under G.

Define an operator O of the first register by

$$U_P(|x\rangle \otimes |w\rangle) = (O\,|x\rangle) \otimes |w\rangle\,.$$

This is possible since U_P leaves $|w\rangle$ unchanged.

O determins the action of the oracle on the first register, given that the second register is in state $|w\rangle$.

Now let $G = F \circ O$. Then the operation of $\mathcal{G}$ on the first register is determined by G.

The aim is to show that S is invariant under G.

First consider the action of the oracle O on S.

We have $O|a\rangle = |a\rangle$ and $O|b\rangle = -|b\rangle$.

Thus

$$O(\alpha|a\rangle + \beta|b\rangle) = \alpha|a\rangle - \beta\,|b\rangle \in \mathrm{span}\{|a\rangle\,, |b\rangle\},$$

so S is invariant under the action of the oracle.

Geometrically, $O|_S$ is a reflection in the line through the origin defined by $|a\rangle$.

First consider the action of the oracle O on S.

We have $O|a\rangle = |a\rangle$ and $O|b\rangle = -|b\rangle$.

Thus

$$O(\alpha|a\rangle + \beta|b\rangle) = \alpha|a\rangle - \beta\,|b\rangle \in \mathrm{span}\{|a\rangle\,, |b\rangle\},$$

so S is invariant under the action of the oracle.

Geometrically, $O|_S$ is a reflection in the line through the origin defined by $|a\rangle$.

First consider the action of the oracle O on S.

We have $O|a\rangle = |a\rangle$ and $O|b\rangle = -|b\rangle$.

Thus

$$O(\alpha|a\rangle + \beta|b\rangle) = \alpha|a\rangle - \beta\,|b\rangle \in \mathrm{span}\{|a\rangle\,, |b\rangle\},$$

so S is invariant under the action of the oracle.

Geometrically, $O|_S$ is a reflection in the line through the origin defined by $|a\rangle$.

First consider the action of the oracle O on S.

We have $O|a\rangle = |a\rangle$ and $O|b\rangle = -|b\rangle$.

Thus

$$O(\alpha|a\rangle + \beta|b\rangle) = \alpha|a\rangle - \beta\,|b\rangle \in \mathrm{span}\{|a\rangle\,, |b\rangle\},$$

so S is invariant under the action of the oracle.

Geometrically, $O|_S$ is a reflection in the line through the origin defined by $|a\rangle$.

Next consider the action of inversion about the mean, that is the operator F, on S.

$$F\left(\alpha|a\rangle + \beta|b\rangle\right) \quad = \quad 2\alpha\langle\psi|a\rangle|\psi\rangle + 2\beta\langle\psi|b\rangle|\psi\rangle - \alpha|a\rangle - \beta|b\rangle.$$

Since $|\psi\rangle \in S$ it follows that S is invariant under F and, with the above, this implies that S is invariant under G, as required.

$F|\psi\rangle = |\psi\rangle$ and if $|\phi\rangle$ is orthogonal to $|\psi\rangle$ then $F|\phi\rangle = -|\phi\rangle$.

Thus $F|_S$ is a reflection in the line through the origin defined by $|\psi\rangle$.

Next consider the action of inversion about the mean, that is the operator F, on S.

$$F\left(\alpha|a\rangle + \beta|b\rangle\right) \quad = \quad 2\alpha\langle\psi|a\rangle|\psi\rangle + 2\beta\langle\psi|b\rangle|\psi\rangle - \alpha|a\rangle - \beta|b\rangle.$$

Since $|\psi\rangle \in S$ it follows that S is invariant under F and, with the above, this implies that S is invariant under G, as required.

$F|\psi\rangle = |\psi\rangle$ and if $|\phi\rangle$ is orthogonal to $|\psi\rangle$ then $F|\phi\rangle = -|\phi\rangle$.

Thus $F|_S$ is a reflection in the line through the origin defined by $|\psi\rangle$.

Next consider the action of inversion about the mean, that is the operator F, on S.

$$F\left(\alpha|a\rangle + \beta|b\rangle\right) \quad = \quad 2\alpha\langle\psi|a\rangle|\psi\rangle + 2\beta\langle\psi|b\rangle|\psi\rangle - \alpha|a\rangle - \beta|b\rangle.$$

Since $|\psi\rangle \in S$ it follows that S is invariant under F and, with the above, this implies that S is invariant under G, as required.

$F|\psi\rangle = |\psi\rangle$ and if $|\phi\rangle$ is orthogonal to $|\psi\rangle$ then $F|\phi\rangle = -|\phi\rangle$.

Thus $F|_S$ is a reflection in the line through the origin defined by $|\psi\rangle$.

Next consider the action of inversion about the mean, that is the operator F, on S.

$$F\left(\alpha|a\rangle + \beta|b\rangle\right) \quad = \quad 2\alpha\langle\psi|a\rangle|\psi\rangle + 2\beta\langle\psi|b\rangle|\psi\rangle - \alpha|a\rangle - \beta|b\rangle.$$

Since $|\psi\rangle \in S$ it follows that S is invariant under F and, with the above, this implies that S is invariant under G, as required.

$F|\psi\rangle = |\psi\rangle$ and if $|\phi\rangle$ is orthogonal to $|\psi\rangle$ then $F|\phi\rangle = -|\phi\rangle$.

Thus $F|_S$ is a reflection in the line through the origin defined by $|\psi\rangle$.

Next consider the action of inversion about the mean, that is the operator F, on S.

$$F\left(\alpha|a\rangle + \beta|b\rangle\right) \quad = \quad 2\alpha\langle\psi|a\rangle|\psi\rangle + 2\beta\langle\psi|b\rangle|\psi\rangle - \alpha|a\rangle - \beta|b\rangle.$$

Since $|\psi\rangle \in S$ it follows that S is invariant under F and, with the above, this implies that S is invariant under G, as required.

$F|\psi\rangle = |\psi\rangle$ and if $|\phi\rangle$ is orthogonal to $|\psi\rangle$ then $F|\phi\rangle = -|\phi\rangle$.

Thus $F|_S$ is a reflection in the line through the origin defined by $|\psi\rangle$.

$G|_S$, being the composition of two reflections in lines through the origin, is a rotation about the origin of the plane S.

Since $1 \leq M \leq N$ we have $0 \leq \sqrt{N - M/N} < 1$, so that there exists $\theta \in \mathbb{R}$ such that $0 < \theta \leq \pi$ and $\cos(\theta/2) = \sqrt{N - M/N}$.

From (13)

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|a\rangle + \sin\left(\frac{\theta}{2}\right)|b\rangle.$$

Thus $G|_S$ is an anticlockwise rotation about the origin, through an angle θ,

$G|_S$, being the composition of two reflections in lines through the origin, is a rotation about the origin of the plane S.

Since $1 \leq M \leq N$ we have $0 \leq \sqrt{N - M/N} < 1$, so that there exists $\theta \in \mathbb{R}$ such that $0 < \theta \leq \pi$ and $\cos(\theta/2) = \sqrt{N - M/N}$.

From (13)

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|a\rangle + \sin\left(\frac{\theta}{2}\right)|b\rangle.$$

Thus $G|_S$ is an anticlockwise rotation about the origin, through an angle θ,

$G|_S$, being the composition of two reflections in lines through the origin, is a rotation about the origin of the plane S.

Since $1 \leq M \leq N$ we have $0 \leq \sqrt{N - M/N} < 1$, so that there exists $\theta \in \mathbb{R}$ such that $0 < \theta \leq \pi$ and $\cos(\theta/2) = \sqrt{N - M/N}$.

From (13)

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|a\rangle + \sin\left(\frac{\theta}{2}\right)|b\rangle.$$

Thus $G|_S$ is an anticlockwise rotation about the origin, through an angle θ,

$G|_S$, being the composition of two reflections in lines through the origin, is a rotation about the origin of the plane S.

Since $1 \leq M \leq N$ we have $0 \leq \sqrt{N - M/N} < 1$, so that there exists $\theta \in \mathbb{R}$ such that $0 < \theta \leq \pi$ and $\cos(\theta/2) = \sqrt{N - M/N}$.

From (13)

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|a\rangle + \sin\left(\frac{\theta}{2}\right)|b\rangle.$$

Thus $G|_S$ is an anticlockwise rotation about the origin, through an angle θ,

$G|_S$, being the composition of two reflections in lines through the origin, is a rotation about the origin of the plane S.

Since $1 \leq M \leq N$ we have $0 \leq \sqrt{N - M/N} < 1$, so that there exists $\theta \in \mathbb{R}$ such that $0 < \theta \leq \pi$ and $\cos(\theta/2) = \sqrt{N - M/N}$.

From (13)

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|a\rangle + \sin\left(\frac{\theta}{2}\right)|b\rangle.$$

Thus $G|_S$ is an anticlockwise rotation about the origin, through an angle θ,

Hence

$$G|\psi\rangle = \cos\left(\frac{3\theta}{2}\right)|a\rangle + \sin\left(\frac{3\theta}{2}\right)|b\rangle$$

and in general,

$$G^k|\psi\rangle = \cos\left(\frac{(2k+1)\theta}{2}\right)|a\rangle + \sin\left(\frac{(2k+1)\theta}{2}\right)|b\rangle.$$

If we rotate $|\psi\rangle$ through $\cos^{-1}\left(\sqrt{M/N}\right)$ radians then we obtain a state close to the desired vector $|b\rangle$.

Measuring this state we will, with high probability, observe x such that $P(x) = 1$, that is a solution to the search problem.

Thus the number of times we should iterate the Grover operator is given by

$$R = \left\lfloor \frac{\cos^{-1}\left(\sqrt{M/N}\right)}{\theta} \right\rfloor.$$

Hence

$$G|\psi\rangle = \cos\left(\frac{3\theta}{2}\right)|a\rangle + \sin\left(\frac{3\theta}{2}\right)|b\rangle$$

and in general,

$$G^k|\psi\rangle = \cos\left(\frac{(2k+1)\theta}{2}\right)|a\rangle + \sin\left(\frac{(2k+1)\theta}{2}\right)|b\rangle.$$

If we rotate $|\psi\rangle$ through $\cos^{-1}\left(\sqrt{M/N}\right)$ radians then we obtain a state close to the desired vector $|b\rangle$.

Measuring this state we will, with high probability, observe x such that $P(x) = 1$, that is a solution to the search problem.

Thus the number of times we should iterate the Grover operator is given by

$$R = \left\lfloor \frac{\cos^{-1}\left(\sqrt{M/N}\right)}{\theta} \right\rfloor.$$

Hence

$$G|\psi\rangle = \cos\left(\frac{3\theta}{2}\right)|a\rangle + \sin\left(\frac{3\theta}{2}\right)|b\rangle$$

and in general,

$$G^k|\psi\rangle = \cos\left(\frac{(2k+1)\theta}{2}\right)|a\rangle + \sin\left(\frac{(2k+1)\theta}{2}\right)|b\rangle.$$

If we rotate $|\psi\rangle$ through $\cos^{-1}\left(\sqrt{M/N}\right)$ radians then we obtain a state close to the desired vector $|b\rangle$.

Measuring this state we will, with high probability, observe x such that $P(x) = 1$, that is a solution to the search problem.

Thus the number of times we should iterate the Grover operator is given by

$$R = \left\lfloor \frac{\cos^{-1}\left(\sqrt{M/N}\right)}{\theta} \right\rfloor.$$

Hence

$$G|\psi\rangle = \cos\left(\frac{3\theta}{2}\right)|a\rangle + \sin\left(\frac{3\theta}{2}\right)|b\rangle$$

and in general,

$$G^k|\psi\rangle = \cos\left(\frac{(2k+1)\theta}{2}\right)|a\rangle + \sin\left(\frac{(2k+1)\theta}{2}\right)|b\rangle.$$

If we rotate $|\psi\rangle$ through $\cos^{-1}\left(\sqrt{M/N}\right)$ radians then we obtain a state close to the desired vector $|b\rangle$.

Measuring this state we will, with high probability, observe x such that $P(x) = 1$, that is a solution to the search problem.

Thus the number of times we should iterate the Grover operator is given by

$$R = \left\lfloor \frac{\cos^{-1}\left(\sqrt{M/N}\right)}{\theta} \right\rfloor.$$

Hence

$$G|\psi\rangle = \cos\left(\frac{3\theta}{2}\right)|a\rangle + \sin\left(\frac{3\theta}{2}\right)|b\rangle$$

and in general,

$$G^k|\psi\rangle = \cos\left(\frac{(2k+1)\theta}{2}\right)|a\rangle + \sin\left(\frac{(2k+1)\theta}{2}\right)|b\rangle.$$

If we rotate $|\psi\rangle$ through $\cos^{-1}\left(\sqrt{M/N}\right)$ radians then we obtain a state close to the desired vector $|b\rangle$.

Measuring this state we will, with high probability, observe x such that $P(x) = 1$, that is a solution to the search problem.

Thus the number of times we should iterate the Grover operator is given by

$$R = \left\lfloor \frac{\cos^{-1}\left(\sqrt{M/N}\right)}{\theta} \right\rfloor.$$

If $M \leq N/2$ then $\theta/2 \geq \sin(\theta/2) = \sqrt{M/N}$.

Thus we obtain, in this case,

$$\frac{\pi}{4}\sqrt{\frac{N}{M}}$$

as an upper bound for R.

Note that if we iterate approximately $\pi\sqrt{N/M}/2$ times, then we have rotated back almost to $-|a\rangle$, and the probability of obtaining a solution is much worse again.

So determining the appropriate number of iterations is a delicate matter.

In the case where $M = 1$ as in Grover's original paper, the number of iterations required is approximately $\pi\sqrt{N}/4$.

If $M \leq N/2$ then $\theta/2 \geq \sin(\theta/2) = \sqrt{M/N}$.

Thus we obtain, in this case,

$$\frac{\pi}{4}\sqrt{\frac{N}{M}}$$

as an upper bound for R.

Note that if we iterate approximately $\pi\sqrt{N/M}/2$ times, then we have rotated back almost to $-|a\rangle$, and the probability of obtaining a solution is much worse again.

So determining the appropriate number of iterations is a delicate matter.

In the case where $M = 1$ as in Grover's original paper, the number of iterations required is approximately $\pi\sqrt{N}/4$.

If $M \leq N/2$ then $\theta/2 \geq \sin(\theta/2) = \sqrt{M/N}$.

Thus we obtain, in this case,

$$\frac{\pi}{4}\sqrt{\frac{N}{M}}$$

as an upper bound for R.

Note that if we iterate approximately $\pi\sqrt{N/M}/2$ times, then we have rotated back almost to $-|a\rangle$, and the probability of obtaining a solution is much worse again.

So determining the appropriate number of iterations is a delicate matter.

In the case where $M = 1$ as in Grover's original paper, the number of iterations required is approximately $\pi\sqrt{N}/4$.

If $M \leq N/2$ then $\theta/2 \geq \sin(\theta/2) = \sqrt{M/N}$.

Thus we obtain, in this case,

$$\frac{\pi}{4}\sqrt{\frac{N}{M}}$$

as an upper bound for R.

Note that if we iterate approximately $\pi\sqrt{N/M}/2$ times, then we have rotated back almost to $-|a\rangle$, and the probability of obtaining a solution is much worse again.

So determining the appropriate number of iterations is a delicate matter.

In the case where $M = 1$ as in Grover's original paper, the number of iterations required is approximately $\pi\sqrt{N}/4$.

If $M \leq N/2$ then $\theta/2 \geq \sin(\theta/2) = \sqrt{M/N}$.

Thus we obtain, in this case,

$$\frac{\pi}{4}\sqrt{\frac{N}{M}}$$

as an upper bound for R.

Note that if we iterate approximately $\pi\sqrt{N/M}/2$ times, then we have rotated back almost to $-|a\rangle$, and the probability of obtaining a solution is much worse again.

So determining the appropriate number of iterations is a delicate matter.

In the case where $M = 1$ as in Grover's original paper, the number of iterations required is approximately $\pi\sqrt{N}/4$.