Quantum Information - Compressed

$$
\begin{aligned}
|\Psi\rangle &= \sum_{k=0}^{d-1} \psi_k |k\rangle \text{ where } \{|k\rangle\} \text{ is an orthonormal basis} \\
|\Phi\rangle &= \sum_{k=0}^{d-1} \phi_k |k\rangle \\
P_\Phi &= |\langle\Phi|\Psi\rangle|^2 \\
\Pi &= |\Psi\rangle\langle\Psi| \quad \text{is a projector so that } \Pi^2 = \Pi \\
\hat{O} &= |\Phi\rangle\langle\Psi| \quad \text{is a linear operator}
\end{aligned}
$$

Measurement & Observables

$$
\begin{aligned}
\hat{O} &= \sum_{k=0}^{d-1} \hat{\lambda}_k |k\rangle\langle k| \quad \text{spectral decomposition} \\
\hat{O}|i\rangle &= \sum_{k=0}^{d-1} \hat{\lambda}_k |k\rangle\langle k|i\rangle = \hat{\lambda}_k \langle k|i\rangle |i\rangle = \hat{\lambda}_{\hat{O},i} |i\rangle \\
\langle\hat{O}\rangle &= \sum_{k=0}^{d-1} \hat{\lambda}_k P_{k,\Phi} = \langle\Psi|\hat{\lambda}|\Psi\rangle
\end{aligned}
$$

Observables for Qubits

$$
\begin{aligned}
\sigma_x = \hat{\sigma}_x &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
\sigma_y = \hat{\sigma}_y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\
\sigma_z = \hat{\sigma}_z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}
\end{aligned}
$$

$$
\begin{aligned}
\sigma_x &\text{ has eigenvalues, eigenvectors } \{1, |0\rangle\,;\ -1, |1\rangle\} \\
\sigma_y &\text{ has eigenvalues, eigenvectors } \{1, |i\rangle\,;\ -1, |-i\rangle\} \\
\sigma_z &\text{ has eigenvalues, eigenvectors } \{1, |+\rangle\,;\ -1, |-\rangle\}
\end{aligned}
$$

The three operators are mutually exclusive, one can not measure in multiple of them simultaneously. To measure $\{\ |0\rangle, |1\rangle\ \}$ use σ_x (the others return random outputs) etc.

Pure, Mixed & Seperable States

$$
\begin{aligned}
|\Psi\rangle \quad & \text{is pure (can be mixed, can be entangled)} \\
\langle \hat{O} \rangle &= \sum_{k=1}^{d-1} p_k \langle \psi_k | \hat{O} | \psi_k \rangle = \sum_{k=1}^{d-1} \mathrm{Tr} \left[\psi_k |\Psi\rangle \langle \Psi| \hat{O} \right] \\
\mathrm{Tr}(\hat{O}) &= \sum_{k=0}^{d-1} \langle k | \hat{O} | k \rangle \\
\hat{O} &= \sum_k p_k \left(|\psi_k\rangle \langle \psi_k| \right) \\
\hat{\rho} &= \sum_k p_k \left(|\psi_k\rangle \langle \psi_k| \right) \quad \text{is an ensemble} \\
\hat{O} &= \mathrm{Tr} \left[\hat{\rho} \hat{O} \right] \\
P_{s_k} &= \langle \Psi | \hat{\rho} | \Psi \rangle \\
\hat{\rho} &= \mathrm{Tr} \left[|\Psi\rangle \langle \Psi| \right] = \sum_k p_k \left| \langle s_k | \Psi \rangle \right|^2
\end{aligned}
$$

$$
\begin{aligned}
\hat{\rho}^2 = \hat{\rho} \quad & \text{means it is a pure state} \\
\hat{\rho} = \sum_k p_k |\psi_k\rangle \langle \psi_k| \quad & \text{mixed}
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{Tr}(\hat{\rho}^2) < 1 \quad & \text{mixed} \\
\mathrm{Tr}(\hat{\rho}) = 1 \quad & \text{pure}
\end{aligned}
$$

An entangled state is not seperable. It can be mixed or pure i.e.

$$
\rho_{A,B} \neq \sum_{p_x=0}^{N} \psi_x \rho_{A,x} \otimes \rho_{B,x}
$$

means the state is entangled (= not seperable). Note, that the concepts mixed and seperable are not opposed. An entangled state can not be separable but it can be mixed. Thus a mixed state can, but must not be separable. A pure state can not be mixed but it can be entangled. Was confusing to me.

Generic Hermitian

$$
\begin{aligned}
\hat{H} &= \frac{1}{2} \left(r_0 \hat{1} + \vec{r} \cdot \vec{\sigma} \right) \\
r = 1 \quad & \text{pure} \\
r < 1 \quad & \text{mixed}
\end{aligned}
$$

Mixed States as Convex Combinations, Ensembles

$$\{p_x, \hat{\rho}_x\}$$

so that

$$\hat{\rho} = \sum_{x=0}^{N} p_x * \hat{\rho}_x$$

with $\sum_{x=0}^{N} p_x = 1$

Multiple Quantum Systems and non-classical correlations

$$|\Psi\rangle_{AB} = \sum_{j=0} \psi_{j,k} |j\rangle_A \otimes |k\rangle_B$$
$$|\Psi\rangle_{AB} = \sum_{j=0} \psi_i |j\rangle_{AB}$$

$$\text{Note:} \quad \left(\sum_j |j\rangle_A \langle j|\right)\left(\sum_k |k\rangle_B \langle k|\right) = \langle j|j\rangle_A |k\rangle_B \langle k|$$

$|\Psi\rangle_{AB} = \sum_{j=0} \psi_{j,k} |j\rangle_A \otimes |k\rangle_B$ is separable and has dimension $2d + 2d - 4$

$|\Psi\rangle_{AB} \neq \sum_{j=0} \psi_{j,k} |j\rangle_A \otimes |k\rangle_B$ is not seperable and has dimension $2(d_A d_B) - 2$

(entangled) Bell states:

$$|\Phi\rangle^{+}_{AB} = \frac{1}{\sqrt{2}} (|01\rangle_{AB} + |10\rangle_{AB})$$
$$|\Psi\rangle^{-}_{AB} = \frac{1}{\sqrt{2}} (|00\rangle_{AB} + |11\rangle_{AB})$$

Note the eigenvalue and eigenvector pairs:

$$\sigma_z \otimes \sigma_z = \{+1 (|00\rangle, |11\rangle); -1 (|10\rangle, |01\rangle)\}$$

Non classical correlations:

$$P_{++} = \langle ++ | \, 01\rangle^2 \frac{1}{4} = P_{+-} = P_{-+} = P_{--}$$

but

$$P_{++} = \left\langle ++ \middle| \, \Phi^{--} \right\rangle^2 = \frac{1}{2} = P_{++} \text{ and } P_{-+} = P_{+-} = 0$$

This is non-classical since Φ^- is a super-position of $|01\rangle$ and $|10\rangle$

1 Instant Collapse

$$\rho = \frac{1}{2} |0\rangle \langle 0| + \frac{1}{2} |1\rangle \langle 1|$$

Consider

$$|\Psi\rangle_{AB}$$

The following measurement results in system A cause the following (instantaneous) collapse in System B. Since the output it still random, this can not be used as faster than light communication:

$$|0\rangle \to |0\rangle_A |0\rangle_B$$
$$|1\rangle \to |1\rangle_A |0\rangle_B$$
$$|+\rangle_\lambda \to |+\rangle_\lambda |-\rangle_B$$
$$|-\rangle_\lambda \to |-\rangle_\lambda |+\rangle_B$$

$$= \frac{1}{\sqrt{2}} |0 \otimes 1\rangle |\Psi\rangle$$

For Ψ^-:

$$\rho_B = \mathrm{Tr}_A [|\Psi\rangle \langle\Psi|] = \frac{1}{2} I_B$$

The substate B is a completely mixed state. For pure entangled states this criterion is enough to determine entanglement. For non-pure (i.e. mixed entangled states):

Entanglement for Mixed States

$$\hat{\rho}_{AB} = \sum_{n=1}^{N} p_n \hat{\rho}_A^n \otimes \hat{\rho}_B^n \text{ mixed seperable state}$$

$$\hat{\rho}_{AB} \neq \sum_{n=1}^{N} p_n \hat{\sigma}_A^n \otimes \hat{\sigma}_B^n \text{ / mixed entangled state}$$

Suppose

$$\hat{\rho}_{AB} = \sum_{n=1}^{N} p_n \hat{\rho}_A^n \otimes \hat{\rho}_B^n$$

and define the partial Trace

$$\hat{\rho}^{T_A} = \sum_{n=1}^{N} p_n \hat{\rho}_A^{nT} \otimes \hat{\rho}_B^n \geq 0$$

In essence, for all separable states, the partial trace is semi-definite positive.

$$\text{If} \quad \mathrm{Tr}\left((\hat{\rho}_{AB})\right) \quad \text{is not} \geq 0 \quad \text{then} \quad \hat{\rho}_{AB} \text{ is entangled.}$$

Werner State

$$\hat{\rho}_{AB} = (1-p)\left|\Psi\right\rangle\left\langle\Psi\right| + p\frac{I}{4}$$

$$= \begin{pmatrix} p & 0 & 0 & 0 \\ 0 & 2-p & 2-p & 0 \\ 0 & 0 & 0 & p \end{pmatrix}$$

$$\left|\Psi\right\rangle \otimes \left|\Psi\right\rangle = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$= \frac{1}{4}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\hat{\rho}_{AB} = \begin{pmatrix} p & 0 & 0 & 0 \\ 0 & 2-p & 2-p & 0 \\ 0 & 2p-2 & 2-p & \\ 0 & 0 & 0 & p \end{pmatrix}$$

$$T^A = \text{transpose each block}$$

$$T^B = \text{transpose blocks}$$

$$\hat{\rho}_{AB} \xrightarrow{T^A} \begin{pmatrix} p & 0 & 0 & 2p-2 \\ 0 & 2-p & 0 & 0 \\ 0 & 0 & 2-p & \\ 2-p & 0 & 0 & p \end{pmatrix}$$

If $p \geq \frac{2}{3}$ then the matrix is semi-definite positive and the state starts to be separable.

Evolution & Krauss Operators

$$i\hbar\frac{d}{dt}\left|\Psi(t)\right\rangle = \hat{H}\left|\Psi(t)\right\rangle$$

$$\hat{H} = \hat{H}^\dagger$$

$$\left|\Psi(t)\right\rangle = e^{-\frac{i}{\hbar}\hat{H}t}\left|\Psi(0)\right\rangle$$

$$e^{\hat{A}} = \sum_{n=0}^{\infty} \frac{\hat{A}^n}{n!} = 1 + \hat{A} + \frac{\hat{A}^2}{2!} + \dots$$

$$\hat{H} \left| E_n \right\rangle = E_n \left| E_n \right\rangle$$

$$\left| \Psi(0) \right\rangle = \left| \Psi_0 \right\rangle = \sum_{k=0}^{d-1} c_k \left| E_k \right\rangle$$

$$\hat{U}(t) \left| \Psi_0 \right\rangle = \sum_n c_n e^{-\frac{i}{\hbar} E_n t} \left| E_n \right\rangle$$

$$= \sum_n c_n e^{-i\omega_n t} \left| E_n \right\rangle$$

Krauss Operators - evolutions of non-isolated systems

$$\hat{\rho}_A = \mathrm{Tr}_E \left[\left| \Phi \right\rangle \left\langle \Phi \right|_{AE} \right]$$

$$\hat{\rho}_A \to \sum_k \hat{E}_k \hat{\rho}_A \hat{E}_k^\dagger$$

$$\sum_k \hat{E}_k^\dagger \hat{E}_k = 1_A$$

$$\hat{E}_k = \sum_{i,j} E_{ij} \left| i \right\rangle \left\langle j \right|$$

Linearity

$$\text{preserves hermiticity} \quad \hat{E}(\rho^\dagger) = \hat{E}(\rho)^\dagger$$

$$\text{trace preserving} \quad \mathrm{Tr}\left[\hat{E}(\rho) \right] = \mathrm{Tr}(\rho)$$

$$\hat{E}_A \otimes \hat{I}_A \geq 0$$

Generalized Measurement

$$P_k = \mathrm{Tr}_A \left[\hat{M}_k^T \hat{M}_k \hat{\rho}_A \right]$$

$$\hat{\rho}_A \to \frac{\hat{M}_k \hat{\rho}_A \hat{M}_k^\dagger}{P_k}$$

$$\{\hat{M}_k\} = \sum_k \hat{M}_k \hat{M}_k^\dagger = 1$$

$$\text{If } \hat{M}_k = \hat{I} \quad \hat{M}_k^\dagger \hat{M}_k = \Pi \quad \text{is a projector.}$$

POVM (positive operater-valued measure):

$$F_k = \hat{M}_k^\dagger \hat{M}_k$$

Small Derivation for the evolution of the subsystem:

$$\hat{\rho}_A = \mathrm{Tr}_E(|\Phi\rangle_{AE} \langle\Phi|_{AE}) = \sum_{k=0}^{N} \langle k| \, |\Phi\rangle_{AE} \langle\Phi|_{AE} \, |k\rangle = \sum_{k=0}^{N} E_k^\dagger \, |\Psi\rangle_A \langle\Psi|_A \, E_k$$

$$U_{AE} \, |\Psi\rangle_A \, |0\rangle_E = \sum_{a}^{d_E-1} \sum_{k}^{d_A-1} \Phi_{a,k} \, |a\rangle \, |k\rangle = \sum_{k}^{d_E-1} |\Phi_k\rangle_A \, |k\rangle_E = \sum_{k}^{d_E-1} E_k \, |\Psi\rangle_A \, |k\rangle_E = |\psi\rangle_{A,E}$$

Quantum Info & Shannon Theory

Number of Required Bits

$$N \sum_k p_k \log_2 \frac{1}{p_k}$$

$$p_k \log_2 \frac{1}{p_k}$$

is the Shannon entropy for a message of k symbols where each symbol has prob. p_k of appearing. It corresponds to the minimal amount of bits required for such a message. Usually p_0 and p_1 for bit 0 and bit 1, since those are the only symbols.

Von Neumann Entropy

$$S(\rho) = -\mathrm{Tr}(\rho \log(\rho))$$

$$= -\mathrm{Tr}\left(\sum_j \lambda_j \log(\lambda_j) \, |j\rangle \langle j| \right)$$

$$= -\sum_j \lambda_j \log(\lambda_j)$$

Von Neumann Entropy for Pure and Mixed States

$$\rho \text{ pure:} \quad \rho = |\Psi\rangle\langle\Psi| \quad S(\rho) = 0$$

$$\rho \text{ mixed:} \quad \rho = \sum_k p_k |\psi_k\rangle\langle\psi_k|$$

$$\rho = \frac{1}{N}\sum_{i=1}^{N} \rho_i \quad \mathrm{Tr}(\rho) = 1 \quad \mathrm{Tr}(\rho^2) \leq 1$$

is a maximally mixed state. Thus

$$S(\rho) = \log_2(N)$$

Properties:

$$S(U\rho U^\dagger) = S(\rho)$$

$$S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B)$$

Accessible Information

Theoretical bound (Holevo Bound) on accessible information

$$I_{acc} = \max_E [H(X) - H(X|Y)] \leq \chi(E)$$

$$\chi(E) = S(\rho_A) - \sum_x p_x S(\rho_x)$$

For a single qubit:

$$\chi \leq S(\rho_A) \leq 1$$

meaning that only one bit is maximally accessible (in 1 single qubit).

$$\chi = S(\rho) - \sum_k p_k S(\rho_k)$$

Quantum Teleportation

Consider the state

$$(\alpha|0\rangle_A + \beta|1\rangle_A) \otimes \frac{1}{\sqrt{2}}(|0\rangle_B|1\rangle_C - |1\rangle_B|0\rangle_C) = \frac{1}{\sqrt{2}}(\alpha|001\rangle - \alpha|010\rangle + \beta|101\rangle - \beta|110\rangle)$$

Now, measure this state in the Bell-state basis

$$\{|\Phi^+\rangle_{AB}, |\Phi^-\rangle_{AB}, |\Psi^+\rangle_{AB}, |\Psi^-\rangle_{AB}\}$$

e.g.

$$\Psi^+ = \frac{1}{\sqrt{(2)}}(|00\rangle_{AB} + |11\rangle_{AB})$$

$$\langle\Psi^+|\,|\Phi_{ABC}\rangle = \frac{1}{2}(\alpha\,|1\rangle_C - \beta\,|0\rangle_C) = \frac{1}{2}\sigma_x\sigma_z(\alpha\,|0\rangle_C - \beta\,|1\rangle_C) = |\Phi\rangle_C$$

This corresponds to the collapsed state in C. Note, that

$$\sigma_x\sigma_z\,|\Phi\rangle_C = \alpha\,|0\rangle_A + \beta\,|1\rangle_A).$$

By applying this unitary on the collapsed state C obtains the state from A. For each of the 4 Bell-states a corresponding unitary can be determined which transforms the collapsed state into the right state. From the classical info of which measurement was obtained to C, the Unitary is selected.

Quantum Fourier Transform

The QFT acts on a quantum state $|x\rangle$ as follows:

$$\mathrm{QFT}\,|x\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{2\pi i\frac{xk}{N}}\,|k\rangle \tag{1}$$

where $N = 2^n$ for an n-qubit quantum register.

Note, that the integer x can be written as $x = \sum_{l=0}^{2^n-1} 2^l x_l$ in binary. Consider the quantum operation

$$H\,|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

. Note that this is a superposition of the values $x = 0$ and $x = 1$. By applying this value to a qubit, we essentially can encode a bit, which is aswell 0 and 1. This is called quantum parallelism.

The QFT can be implemented using a quantum circuit composed of Hadamard gates and controlled phase shift gates. For an n-qubit quantum register $|x_0x_1\ldots x_{n-1}\rangle$, the QFT can be expressed as:

$$\mathrm{QFT}\,|x\rangle = \frac{1}{\sqrt{N}}\sum_{k_0,k_1,\ldots,k_{n-1}} e^{2\pi i(\sum_{l=0}^{N-1} 2^l k_l)(x)}\,|k_0k_1\ldots k_{n-1}\rangle$$

$$= \frac{1}{\sqrt{2}}\sum_{k=0}^{k=1}(e^{2\pi ix2^{(N-1)}k_{N-1}}\,|k_{N-1}\rangle\otimes\frac{1}{\sqrt{2}}\sum_{k=0}^{k=1}(e^{2\pi ix2^{(N-2)}k_{N-2}}\,|k_{N-1}\rangle\otimes\ldots\otimes\frac{1}{\sqrt{2}}\sum_{k=0}^{k=1}(e^{2\pi ix2^0k_0x}\,|k_0\rangle$$

$$= \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle\,e^{2\pi ix_0})\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle\,e^{2\pi i(\frac{x_0}{2}+x_1)})\otimes\ldots\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle\,e^{2\pi i(\frac{x_0}{N-1}+..+x_{N-1})})$$

The corresponding quantum circuit for the QFT is shown below:

ADDD IMAGE

Shors Algorithm

Consists of two parts

1. A classical reduction that converts the factoring problem to finding the period of a function. (Difficult with classical methods)
2. A quantum part that efficiently finds this period using the Quantum Fourier Transform (QFT).

Classical Reduction

Given an integer N to factor:

1. Choose a random integer a such that $1 < a < N$.
2. Compute the greatest common divisor (gcd) of a and N. If $\gcd(a, N) \neq 1$, then we have found a non-trivial factor of N.
3. Define the function $f(x) = a^x \mod N$.
4. The goal is to find the period r of the function $f(x)$, i.e., the smallest positive integer r such that $a^r \equiv 1 \mod N$.
5. If r is even and $a^{r/2} \not\equiv -1 \mod N$, then $\gcd(a^{r/2} - 1, N)$ and $\gcd(a^{r/2} + 1, N)$ are non-trivial factors of N.

1.1 Quantum Period Finding

The quantum part of Shor's Algorithm is used to find the period r of the function $f(x) = a^x \mod N$. This is achieved using a quantum computer and involves the following steps:

The quantum circuit for period finding in Shor's Algorithm is as follows. Start by applying the Hadamard gate to q-qubits:

$$H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

. This creates a superposition of all possible classical bit-strings of length $Q = 2^q$, denoted by

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

The first q-bit corresponds to x_0 and it the superposition of 0 and 1 in the first slot etc.... Consider

$$a^x = a^{x_0} * a^{2x_1} * a^{2^2 x_0} ... a^{2^{N-1} x_{N-1}}$$

. This operation can be implemented by a circuit like: **ADD IMAGE**
resulting in

$$\frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle\,|a^x mod N\rangle = \sum_{b=0}^{r-1}\frac{1}{\sqrt{Q}}\sum_{b=0}^{r-1}\sum_{k=0}^{\frac{Q}{r}-1}|kr+b\rangle\,|a^{kr+b}mod N\rangle$$

$$=\sum_{b=0}^{r-1}\frac{1}{\sqrt{Q}}\sum_{b=0}^{r-1}\sum_{k=0}^{\frac{Q}{r}-1}|kr+b\rangle\,|a^b)mod N\rangle$$

Measure the second register:

$$\Phi_{collapse}=\frac{\sqrt{r}}{\sqrt{Q}}\sum_{k=0}^{\frac{Q}{r}-1}|kr+b_0\rangle\,|a^{b_0})mod N\rangle$$

Consider now only the first register.

$$\frac{\sqrt{r}}{\sqrt{Q}}\sum_{k=0}^{\frac{Q}{r}-1}|kr+b_0\rangle$$

Note that the state is evenly spaced with period r. Perform a Quantum Fourier Transform to determine the period.

$$\mathrm{QFT}(\frac{\sqrt{r}}{\sqrt{Q}}\sum_{k=0}^{\frac{Q}{r}-1}|kr+b_0\rangle)=\frac{\sqrt{r}}{\sqrt{Q}}\sum_{k=0}^{\frac{Q}{r}-1}\mathrm{QFT}(|kr+b_0\rangle)$$

$$=\frac{\sqrt{r}}{Q}\sum_{k=0}^{\frac{Q}{r}-1}\sum_{j=0}^{Q-1}e^{2\frac{\pi}{Q}i(kr+b_0)j}\,|j\rangle=\frac{\sqrt{r}}{Q}\sum_{k=0}^{\frac{Q}{r}-1}e^{2\frac{\pi}{Q}ib_0}\sum_{j=0}^{Q-1}e^{2\frac{\pi}{Q}i(kr)j}\,|j\rangle$$

$$=\frac{\sqrt{r}}{Q}e^{2\frac{\pi}{Q}ib_0 j}\sum_{k=0}^{\frac{Q}{r}-1}\delta_{j,m\frac{Q}{r}}=\frac{\sqrt{r}}{Q}e^{2\frac{\pi}{Q}ib_0}\sum_{m}|m\frac{Q}{r}\rangle$$

Measuring this state yields information on the period.

Phase Estimation

Consider a Unitary operation of the form

$$\hat{O}\,|u\rangle=e^{2\pi\Phi i}\,|u\rangle$$

To estimate Φ use the Phase-estimation algorithm. Prepare a superposition of classical input strings

$$|\Phi\rangle=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle=\frac{1}{\sqrt{N}}(|0\rangle+|1\rangle)\otimes...\otimes(|0\rangle+|1\rangle)$$

Consider the following circuit

ADDD IMAGE

It results in the state

$$|\Phi\rangle = \frac{1}{\sqrt{N}}(|0\rangle + e^{2\pi i\Phi}|1\rangle) \otimes (|0\rangle + e^{2\pi i\Phi 2}|1\rangle) \otimes (|0\rangle + e^{2\pi i\Phi 2^2}|1\rangle) \otimes ... \otimes (|0\rangle + e^{2\pi i\Phi 2^n}|1\rangle)$$

$$= \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{i\Phi x}|x\rangle$$

Perform the inverse Quantum Fourier Transform

$$\text{iQFT}(\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{i\Phi x}|x\rangle) = \frac{1}{N} \sum_{x=0}^{N-1} e^{i\Phi x} \sum_{y=0}^{N-1} e^{-2\pi i \frac{\Phi}{N} xy}|y\rangle = \frac{1}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} e^{-2\pi i \frac{1}{N} x(2^n \Phi y)}|y\rangle$$

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

This Amplitude corresponding to the Wave-function being in state $|y\rangle$ is concentrated at multiples of $N * \Phi$. Measuring y yields Information on the Phase.

Grover algorithm

Grover's algorithm can be used to perform a Database search.

Consider

$$|\Phi\rangle = \sin(\frac{\theta}{2})|\alpha\rangle + \cos(\frac{\theta}{2})|\beta\rangle$$

where $\alpha \in$ A and $\beta \notin$ A. Consider then a Quantum Oracle described by the operator $\hat{O}|x\rangle = -|x\rangle$ if $|x\rangle \in$ A and $\hat{O}|x\rangle = |x\rangle$ if $|x\rangle \notin$ A

Furthermore, consider the Grover-Operator

$$\hat{G} = 2\langle\Phi|\Phi\rangle - I$$

. This performs an inversion around $|\Phi\rangle$.

Prepare a superposition of classical input bits

$$|\Phi\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle = \sin(\frac{\theta}{2})|\alpha\rangle + \cos(\frac{\theta}{2})|\beta\rangle$$

with $\alpha \in$ A and $\beta \notin$ A. Apply the Oracle operation to it, resulting in

$$|\Phi_o\rangle = -\sin(\frac{\theta}{2})|\alpha\rangle + \cos(\frac{\theta}{2})|\beta\rangle$$

Now, application of the Grover Operator results in

$$|\Phi_g\rangle = \sin(\frac{\theta}{2} + \theta)|\alpha\rangle + \cos(\frac{\theta}{2} + \theta)|\beta\rangle$$

Note, that if $\sin(\frac{\theta}{2} = 1$, then the wave function is in a state that is element of the Database A with Probability 1. Assume $|A| = M$ and $|!A| = N - M$, then

$$|\Phi\rangle = \sin(\frac{\theta}{2})\,|\alpha\rangle + \cos(\frac{\theta}{2})\,|\beta\rangle$$

with $\sin(\frac{\theta}{2}) = \sqrt{\frac{M}{N}}$ and $\cos(\frac{\theta}{2}) = \sqrt{\frac{N-M}{N}}$. If $M << N$, then $\frac{\theta}{2} \approx \sin(\frac{\theta}{2}) = \sqrt{\frac{M}{N}}$ and thus $\frac{\theta}{2} + \theta = \frac{\pi}{2}$ leads to k being in the order of $\mathrm{O}(\sqrt{\frac{M}{N}})$. Classical Database searches are in the order of $\mathrm{O}(N)$.

Deutsch Algorithm

Deutsch-Josza Algorithm