Technical Notes on Quantum Computing

Kuljit S. Virk

These notes collect my perspective of the fundamental theoretical basis for quantum computing. There are no new results, but an attempt to put my understanding into a coherent form that I can later use for research.

CONTENTS

I. OVERVIEW

The evolution of a quantum system that can be considered closed at relevant timescales is given completely by a unitary matrix U. In a space of 2^n states, the $2^n \times 2^n$ matrix U can be written as a direct product of 2×2 unitary matrices,

$$U = U_1 \otimes U_2 \otimes \cdots \otimes U_k,$$

where $k = 2^{n-1}(2^n - 1)$ is the number of independent entries of U. Let us denote the 2^n basis states in the vector space as $|m\rangle$ with m being an integer $0 \leq m < 2^n$.

We construct a computational basis in terms of its bit representation $\underline{m} = (m_{n-1}, \ldots m_0)$, such that $m \in \{0, 1\}$, and

$$m = \sum_{j=0}^{n-1} m_j 2^j,$$

The ket is similarly represented as,

$$|\underline{m}\rangle \equiv |m_{n-1}, m_{n-2}, \ldots, m_0\rangle .$$

We now map each m_j to a basis state of a 2-level system or a qubit, so that $|m\rangle$ becomes a direct product of n subsystems,

$$|\underline{m}\rangle = |m_{n-1}\rangle \, |m_{n-2}\rangle \cdots |m_0\rangle .$$

The unitary matrices U_j act non-trivially on only a pair of states, where the pair differs for each j. These are thus transformations of a 2-level system, $|\underline{m}\rangle$ and $|\underline{m}'\rangle = |m'_{n-1} m'_{n-2} \ldots m'_0\rangle$. In general, $m_j \neq m'_j$ for many j, however, we can always apply a permutation P among the basis states such that $P|m\rangle$ and $P|m'\rangle$ differ only in one j or a qubit while all the remaining $n-1$ qubits are in state $|1\rangle$.

We can then apply U_j in this space and then apply P^{-1} to map the computational basis back to the original ordering. As a result, n qubits, ability to do permutation P and the ability to apply a 2×2 unitary operation can effectively apply any arbitrary U to this 2^n-dimensional system. Implementing P can be done with a 2-qubit CNOT operation, and the application of U_j requires the *controlled-U* operation $C^{(n-1)}(U_j)$ on the qubits other than j. The single qubit unitary U_j is also a gate operation, usually in the form of a controlled pulse excitation.

At this stage, it is clear that in principle, any unitary operation can be mapped to a set of gate operations on a quantum state. Since the space of all possible unitaries is exponential in the system size, the number of gates required also becomes exponential. In particular, the dimension of Hilbert space of n qubits is 2^n. There are $O(2^{2n})$ terms in a unitary matrix, and suppose we are able to approximate any unitary within an error of δ, that is, we have covered the Hilbert space with balls of size δ. The number of such balls is,

$$N_{\text{balls}} = \frac{\text{Volume}(U(N))}{\text{Volume(ball)}} \;=\; \left(\frac{C}{\delta}\right)^{2^{2n}},$$

where C is a constant representing the radius of the $U(N)$ group. In gate-based quantum computers, each unitary matrix is implemented by a multiplication of 1 or 2-qubit operators. Each primitive include shuffling and matrix operations with n qubits. Let that be and poly(n) operations. Then the $N_T = (\text{poly}(n))^T$ gates should exceed the total number of balls, and thus

$$T \geq 2^{2n} \frac{\log(C/\delta)}{\log(\text{poly}(n))}. \tag{1}$$

We see from this result that to cover the *entire* unitary group in 2^n-dimensions, the number of gates required is at least 2^{2n}. The more accurate the approximations (smaller δ) requires more gates. This latter scaling with error is logarithmic. The formula does not tell us *how* we can improve error logarithmically. The Solovay-Kitaev theorem provides a procedure that scales as the power 3.97 of the logarithm of error (see II.O on page 20), and algorithms exist to improve this further in some cases. Equation (1) shows that we cannot do better than linear scaling. Nonetheless, it is the fact that gate count scales as polynomial in logarithm of error and not an exponential is what shows that in-principle gate errors do not accumulate, and thus arbitrarily good accuracy can be achieved with imperfect gates.

The Solovay Kitaev theorem shows that given an approximation with error ϵ, such that inverses are contained in the gate set, a combination of 5 gates can be used to improve this error as a power of ϵ. As a result any approximation with low enough ϵ provides a dense covering of the group $U(2^n)$. For a fixed accuracy, this theorem ensures that

there is an upper bound on the gates needed to reach any state within this accuracy. However, the number still grows exponentially with n. The impacct of Solovay Kitaev theorem is that increasing the gate count decreases the error, not increase it, so long as each gate error is below a threshold. Therefore, in principle, below a threshold error, any arbitrary U can be implemented to an arbitrary accuracy.

The threshold error is too small for practical application, but it can be raised significantly using error correction codes. Thus the error correction codes are used to define a logical qubit consisting of thousdands of physical qubits. This is a key enabler in making fault tolerant computing possible, which is what is needed for any practical application.

The essential aspect of quantum computation is that many computational problems can be mapped to such unitary transformations. In particular, the simulation of any physical system is naturally governed by a Hamiltonian from which the unitary matrix follows. Thus any quantum mechanical system whose low energy effective dynamics is restircted to be within N states can be simlated with a system of N qubits.

Since exponentiation of the Hamiltonian is itself a problem for a large system, how is the unitary matrix construced and then applied by decomposition above in a gate based quantum computer? To address this, we first decompose the Hamiltonian into smaller pieces that can be exponentiated,

$$H = \sum_k H_k,$$

When H_k commute with each other, $e^{-iHt} = \otimes_k e^{-iH_k t}$. When they do not, we take small time steps and use the BCH formula

$$\lim_{\Delta t \to 0} e^{i(A+B)\Delta t} = e^{iA\Delta t} e^{B\Delta t} + O(\Delta t^2).$$

This is called the Suzuki-Trotter scheme. Thus a large number of time steps is needed to approximate the dynamics. Nonetheless, the action of any Hamiltonian on a quantum state can be simulated in this manner. We will see how approximation can be improved in some cases.

II. PRIMITIVES

A. Computational Basis States

Computing occurs as a state evolution in a finite dimensional Hilbert space of dimension $N = 2^n$. We denote the N orthogonal basis functions in this space as $|m\rangle$ with m being an integer $0 \leq m < 2^n$. The states $|m\rangle$ enumerate all n-bit integers, and its alternative representation is in the binary representation,

$$\underline{m} = (m_{n-1}, \ldots m_0), \;\; m \in \{0, 1\}, \tag{2}$$

such that,

$$m = \sum_{j=0}^{n-1} m_j 2^j. \tag{3}$$

The state $|m\rangle$ is similarly represented as,

$$|\underline{m}\rangle \equiv |m_{n-1}, m_{n-2}, \ldots, m_0\rangle. \tag{4}$$

This state is then mapped to n physically separate bits, or qubits. Thus $|\underline{m}\rangle$ is a direct product of n 2-level quantum mechanical subsystems,

$$|\underline{m}\rangle = |m_{n-1}\rangle \, |m_{n-2}\rangle \cdots |m_0\rangle. \tag{5}$$

The basis states are ordered in numerically increasing order as described above, and that yields the concrete matrix representation of operators when needed.

It is convenient to define 2×2 unitary matrix basis with,

$$\sigma_1 = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$
$$\sigma_2 = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},$$
$$\sigma_3 = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Note that

$$XY = iZ, \tag{6}$$
$$YZ = iX, \tag{7}$$
$$ZX = iY. \tag{8}$$

B. Pauli Algebra Properties

A simple but useful and powerful identity is the matrix exponential representation in the Pauli basis. Let us take $\boldsymbol{a} = (a_x, a_y, a_z)$, $\boldsymbol{\sigma} = (X, Y, Z)$ and consider,

$$U = \exp\left[t\boldsymbol{a} \cdot \boldsymbol{\sigma}\right].$$

Before expanding the exponential, we note that

$$\left(\boldsymbol{a} \cdot \boldsymbol{\sigma}\right)^2 = \sum_i a_i^2 \sigma_i^2 + \sum_{ij} a_i a_j \left(\sigma_i \sigma_j + \sigma_j \sigma_i\right) \; = \; \left|\boldsymbol{a}\right|^2,$$

since the Pauli matrices anticommute and $\sigma_i^2 = I$. Now expand the exponential letting $a \equiv |\boldsymbol{a}|$,

$$\begin{aligned} \exp\left[t\boldsymbol{a} \cdot \boldsymbol{\sigma}\right] &= I + t\boldsymbol{a} \cdot \boldsymbol{\sigma} + \frac{1}{2!} t^2 \left(\boldsymbol{a} \cdot \boldsymbol{\sigma}\right)^2 + + \frac{1}{2!} t^3 \left(\boldsymbol{a} \cdot \boldsymbol{\sigma}\right)^3 + \ldots \\ &= \left[I + \frac{1}{2!}\left(ta\right)^2 + \frac{1}{4!}\left(ta\right)^4 + \ldots\right] + \frac{\boldsymbol{a} \cdot \boldsymbol{\sigma}}{a}\left[ta + \frac{1}{3!}\left(ta\right)^3 + \frac{1}{5!}\left(ta\right)^5 + \ldots\right]. \end{aligned}$$

Recognizing the terms in the square brackets as the series expansion for cosine and sine respectively,

$$\exp\left[t\boldsymbol{a} \cdot \boldsymbol{\sigma}\right] = \cos\left(\left|\boldsymbol{a}\right| t\right) + \frac{\boldsymbol{a} \cdot \sigma}{|\boldsymbol{a}|} \sin\left(|\boldsymbol{a}| t\right).$$

Furthermore, we have the algebra (6)-(8) from which it follows that

$$[X, Y] = 2iZ,$$
$$[Z, X] = 2iY,$$
$$[Y, Z] = 2iX.$$

From these relations, it also follows that,

$$[\sigma_i, [\sigma_i, \sigma_k]] = 4\sigma_k \delta_{ik}, \;\; i, k \in \{1, 2, 3\}.$$

Thus for two operators, $F = \boldsymbol{f} \cdot \boldsymbol{\sigma}$ and $Q = \boldsymbol{q} \cdot \boldsymbol{\sigma}$ where $\boldsymbol{f}$ and $\boldsymbol{q}$ are complex-valued 3-vectors,

$$\begin{aligned}
[F, Q] &= (f_x q_y - f_y q_x)[X, Y] + (f_x q_z - f_z q_x)[X, Z] + (f_y q_z - f_z q_y)[Y, Z] \\
&= 2i\,(\boldsymbol{f} \times \boldsymbol{q}) \cdot \boldsymbol{\sigma}, \\
[F, [F, Q]] &= -4\,(\boldsymbol{f} \cdot \boldsymbol{q})\,F + 4f^2 Q, \\
[F, [F, [F, Q]]] &= 4f^2\,[F, Q]\,.
\end{aligned}$$

The last identity follows because the first term in the previous identiy vanishes under the commutator with F. Therefore, if we define the n-th commutator as,

$$[(F)^n, Q] = [F, [F, \ldots, [F, Q]]]\,,$$

then from the identity proven above for $n = 3$, we note that

$$\begin{aligned}
\left[(F)^3, Q\right] &= 4f^2\,[F, Q] \\
\left[(F)^4, Q\right] &= 4f^2\,[F, [F, Q]] \\
\left[(F)^5, Q\right] &= \left(4f^2\right)^2 [F, Q]\,.
\end{aligned}$$

From the pattern we observe that for $n = 0, 1, 2, \ldots,$

$$\begin{aligned}
\left[(F)^{3+2n}, Q\right] &= \left(4f^2\right)^{n+1} [F, Q]\,. \\
\left[(F)^{4+2n}, Q\right] &= \left(4f^2\right)^{n+1} [F, [F, Q]]\,.
\end{aligned}$$

From these results, we find a closed form expression for the similarity transformation of Q. For simplicity, let $\alpha = 2f$, then

$$\begin{aligned}
e^{iF} Q e^{-iF} &= Q + i\,[F, Q] - \frac{1}{2!}\,[F, [F, Q]] + \sum_{n=0}^{\infty} \frac{i^{3+2n}}{(3+2n)!} \left[(F)^{3+2n}, Q\right] + \sum_{n=0}^{\infty} \frac{i^{4+2n}}{(4+2n)!} \left[(F)^{4+2n}, Q\right] \\
&= Q + \left(-\frac{1}{2!} + \sum_{n=0}^{\infty} \frac{(-1)^n\,\alpha^{2n+2}}{(4+2n)!}\right) [F, [F, Q]] + \left(i + \sum_{n=0}^{\infty} \frac{i^{2n+3} \alpha^{2n+2}}{(2n+3)!}\right) [F, Q] \\
&= Q + \frac{1}{\alpha^2} \left(-\frac{\alpha^2}{2!} + \sum_{n=0}^{\infty} \frac{(-1)^n\,\alpha^{2n+4}}{(4+2n)!}\right) [F, [F, Q]] + \frac{1}{\alpha} \left(i\alpha + \sum_{n=0}^{\infty} \frac{(i\alpha)^{2n+3}}{(2n+3)!}\right) [F, Q] \\
&= Q + \frac{1}{\alpha^2} \left(\sum_{n=1}^{\infty} \frac{(-1)^n\,\alpha^{2n}}{(2n)!}\right) [F, [F, Q]] + \frac{1}{\alpha} \left(\sum_{n=0}^{\infty} \frac{(i\alpha)^{2n+1}}{(2n+1)!}\right) [F, Q] \\
&= Q + \frac{\cos(\alpha) - 1}{\alpha^2}\,[F, [F, Q]] + \frac{i \sin(\alpha)}{\alpha}\,[F, Q]\,.
\end{aligned}$$

Thus we state the identity as,

$$\begin{aligned}
e^{iF} Q e^{-iF} &= Q + \frac{\cos(2f) - 1}{(2f)^2}\,[F, [F, Q]] + \frac{i \sin(2f)}{2f}\,[F, Q] \\
&\text{where } F = \boldsymbol{f} \cdot \boldsymbol{\sigma}.
\end{aligned}$$

Alternatively, we may also write

$$e^{iF} Q e^{-iF} = \left[\boldsymbol{q} + (\cos(2f) - 1)\left(\hat{\boldsymbol{f}} \times \left(\hat{\boldsymbol{f}} \times \boldsymbol{q}\right)\right) + i \sin(2f)\left(\hat{\boldsymbol{f}} \times \boldsymbol{q}\right)\right] \cdot \boldsymbol{\sigma}.$$

C. Universal representation

As mentioned in the Overview, any unitary matrix in N-dimensions can be represented as a product of simple unitaries, such that each of the simple unitary acts on only 2 states at a time. In this subsection, we show the algorithm to reduce a unitary matrix

$$U = \begin{bmatrix} u_{11} & u_{12} & u_{13} & \cdots & u_{1N} \\ u_{21} & u_{22} & & & \\ & & \ddots & & \\ \vdots & & & & \\ u_{N1} & & & & u_{NN} \end{bmatrix},$$

to a product of $T = N(N-1)/2$ unitaries, each acting on a 2-dimensional subspace,

$$U = U_1 U_2 \dots U_T.$$

Procedure: If $u_{21} = 0$, set $U_1 = I$ where I is the identity matrix in N-dimensional space, otherwise within the state space spanned by $|1\rangle, |2\rangle$, set

$$U_1^\dagger = \begin{bmatrix} \frac{u_{11}^*}{\sqrt{|u_{11}|^2+|u_{21}|^2}} & \frac{u_{21}^*}{\sqrt{|u_{11}|^2+|u_{21}|^2}} & 0 & \cdots & 0 \\ \frac{u_{21}}{\sqrt{|u_{11}|^2+|u_{21}|^2}} & \frac{-u_{11}}{\sqrt{|u_{11}|^2+|u_{21}|^2}} & 0 & \cdots & 0 \\ 0 & 0 & I_{N-2} & & \\ \vdots & \vdots & & & \\ 0 & 0 & & & \end{bmatrix}.$$

Note that

$$U_1^\dagger U = \begin{bmatrix} 1 & u'_{12} & u'_{13} & \cdots & u'_{1N} \\ 0 & u'_{22} & & & \\ & & \ddots & & \\ u'_{31} & & & & \\ \vdots & & & & \\ u'_{N1} & & & & u'_{NN} \end{bmatrix}.$$

Next, continue the procedure with states 1 and 3, and so on until the first column is zeroed out except for 1 in the first entry. This will in general yield N unitary matrices and thus the product $W = U_N^\dagger \cdots U_1^\dagger U$ is also unitary. Since W is unitary, it satisfies $W^\dagger W = I$. In particular, the first column in the product $W^\dagger W$ is $(1, w_{12}^*, \dots, w_{1N}^*)^T$ and since this equals $(1, 0, \dots, 0)$, it follows that the first row of W is also zero. In other words,

$$U_N^\dagger \cdots U_1^\dagger U = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & U^{(N-1)} & \\ 0 & & & \end{bmatrix},$$

where $U^{(N-1)}$ is a unitary in $N-1$ dimensional space. We now repeat the above procedure by reducing $U^{(N-1)}$ to a matrix with 1 in the top left entry, and a unitary matrix in $N-2$ dimensional space. This procedure eventually stops when $T = N(N-1)/2$ many unitaries produce

$$U_T^\dagger \dots U_1^\dagger U = I.$$

With each unitary, we also have 2 associated states that define the 2-dimensional subspace on which the unitary acts. In practice, since gates do not exist between all pairs, qubits are mapped using, for example the Gray code, such that the two states $|\bar{m}\rangle, |\bar{m}'\rangle$ are mapped to

$$|\bar{m}\rangle = |11\cdots10\rangle\,,\ |\bar{m}'\rangle = |11\cdots11\rangle\,,$$

and the remaining states must all have at least one 0 in the first $n-1$ bits. The unitary between these two states is then applied with a $C^{N-1}(U^{(m,m')})$ gate that applies its argument if all other states are 1 and applies identity otherwise. The states are then mapped back to the original ordering of the computational basis. Thus n shuffling operations are needed per unitary.

D. ZY Decomposition of 2×2 Unitary and $C(U)$ Gate

ZY decomposition is a canonical technique to represent any 2×2 unitary matrix.

Theorem: Any matrix in $U(2)$ can be represented with 4 real numbers, $\alpha,\beta,\gamma,\delta$, as follows,

$$U = e^{i\alpha}e^{i\frac{\beta}{2}Z}e^{i\frac{\gamma}{2}Y}e^{i\frac{\delta}{2}Z} = e^{i\alpha}\begin{bmatrix} e^{i\frac{\beta+\delta}{2}}\cos\left(\frac{\gamma}{2}\right) & e^{i\frac{\beta-\delta}{2}}\sin\left(\frac{\gamma}{2}\right) \\ -e^{-i\frac{\beta-\delta}{2}}\sin\left(\frac{\gamma}{2}\right) & e^{-i\frac{\beta+\delta}{2}}\cos\left(\frac{\gamma}{2}\right)\end{bmatrix}. \tag{9}$$

Proof: Any $U(2)$ matrix has the form shown in the second equality.

The following following identities are useful in the algorithm for making a control-U gate,

$$Xe^{i\theta Z}X = e^{-i\theta Z}, \tag{10}$$
$$Xe^{i\theta Y}X = e^{-i\theta Y}, \tag{11}$$
$$Ye^{i\theta Z}Y = e^{-i\theta Z}. \tag{12}$$

Corollary: For any matrix $U\in U(2)$, there exist matrices A,B,C such that

$$ABC = I, \tag{13}$$
$$U = e^{i\alpha}AXBXC. \tag{14}$$

Proof: Write the ZY decomposition in (9) as,

$$\begin{aligned} U &= e^{i\alpha}e^{i\frac{\beta}{2}Z}e^{i\frac{\gamma}{2}Y}e^{i\frac{\delta}{2}Z}, \\ &= e^{i\alpha}e^{i\frac{\beta}{2}Z}e^{i\frac{\gamma}{4}Y}e^{i\frac{\gamma}{4}Y}e^{i\frac{\delta+\beta}{4}Z}e^{i\frac{\delta-\beta}{4}Z}. \end{aligned}$$

Use equations (10) and (11), and the fact that $X^2 = I$ to obtain the following equivalent forms,

$$\begin{aligned} U &= e^{i\alpha}e^{i\frac{\beta}{2}Z}e^{i\frac{\gamma}{4}Y}Xe^{-i\frac{\gamma}{4}Y}XXe^{-i\frac{\delta+\beta}{4}Z}Xe^{i\frac{\delta-\beta}{4}Z} \\ &= e^{i\alpha}e^{i\frac{\beta}{2}Z}e^{i\frac{\gamma}{4}Y}Xe^{-i\frac{\gamma}{4}Y}e^{-i\frac{\delta+\beta}{4}Z}Xe^{i\frac{\delta-\beta}{4}Z}. \end{aligned}$$

Now define

$$A = e^{i\frac{\beta}{2}Z}e^{i\frac{\gamma}{4}Y}, \tag{15}$$
$$B = e^{-i\frac{\gamma}{4}Y}e^{-i\frac{\delta+\beta}{4}Z}, \tag{16}$$
$$C = e^{i\frac{\delta-\beta}{4}Z}. \tag{17}$$

Note that

$$\begin{aligned} ABC &= e^{i\frac{\beta}{2}Z} e^{i\frac{\gamma}{4}Y} e^{-i\frac{\gamma}{4}Y} e^{-i\frac{\delta+\beta}{4}Z} e^{i\frac{\delta-\beta}{4}Z} \\ &= e^{i\frac{\beta}{2}Z} e^{-i\frac{\delta+\beta}{4}Z} e^{i\frac{\delta-\beta}{4}Z} \\ &= I. \end{aligned}$$

Thus we see that equations (13) and (14) hold with the definitions (15)-(17).

How do we make a $C(U)$ gate out of this? We use the fact that CNOT gate effects the operation X on the target bit. Thus we replace both the X in (14) with a CNOT on the target bit, and obtain $C(U)$ as follows:

$$C(U) \left|a\right\rangle_c \left|b\right\rangle_t = e^{i\alpha} A\mathrm{CNOT}\left[B\left[\mathrm{CNOT}\left[\left|a\right\rangle_c \left[C\left|b\right\rangle_t\right]\right]\right]\right].$$

E. Basis Rotation

Another convenient primitive operation is to write the rotation

$$\begin{aligned} A &= e^{i\theta Y} e^{i\alpha Z} e^{-i\theta Y} \\ &= \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} e^{i\alpha} & \\ & e^{-i\alpha} \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \end{aligned}$$

in terms of a vector on a unit sphere. The derivation can be made directly from the multiplying the matrices and using trignometric identities. Here we exploit the properties of Pauli matrices to arrive at the result. We first re-write the exponential as

$$\begin{aligned} A &= \left[I\cos\theta + i\sin\theta Y\right] e^{i\alpha Z} \left[I\cos\theta - i\sin\theta Y\right] \\ &= \cos^2\theta e^{i\alpha Z} + \sin^2\theta Y e^{i\alpha Z} Y + i\sin\theta\cos\theta \left[Y e^{i\alpha Z} - e^{i\alpha Z} Y\right] \\ &= \cos^2\theta e^{i\alpha Z} + \sin^2\theta e^{-i\alpha Z} + i\sin\theta\cos\theta \left(i\sin\alpha\right)\left[YZ - ZY\right] \\ &= \cos^2\theta + \sin^2\theta + \left(\cos^2\theta - \sin^2\theta\right)\left(i\sin\alpha\right) Z + \left(i\sin\theta\cos\theta\right)\left(i\sin\alpha\right)\left(2iX\right) \\ &= I + i\sin\alpha\ \left[\cos 2\theta Z - \sin 2\theta X\right]. \end{aligned}$$

Now define a vector on a unit sphere in $\mathbb{R}^3$,

$$\hat{n}(\theta) = -\sin\theta\hat{x} + \cos\theta\hat{z}\ =\ (\cos\theta\hat{x} + \sin\theta\hat{z}) \times \hat{y}.$$

The expression for A can now be written as

$$A\ =\ e^{i\theta Y} e^{i\alpha Z} e^{-i\theta Y} = I + i\sin\alpha\ \hat{n}(2\theta)\cdot\sigma\ =\ e^{i\alpha\hat{n}(2\theta)\cdot\boldsymbol{\sigma}}.$$

F. Phase Oracle

Suppose we have a function over $x \in \{0, 1\}$ such that

$$f_w(x) = \begin{cases} 0 & x \neq w \\ 1 & x = w \end{cases}.$$

A phase oracle is a unitary operator

$$U_w \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus f(x)\right\rangle,$$

applied to the state $\left|-\right\rangle = (\left|0\right\rangle - \left|1\right\rangle)/\sqrt{2}$, so that

$$U_w \left|x\right\rangle \left|-\right\rangle = (-1)^{f(x)} \left|x\right\rangle \left|-\right\rangle.$$

G. Quantum Fourier Transform

1. Algebraic

The Quantum Fourier Transform (QFT) maps a computational basis state $|\underline{m}\rangle$ to a new state,

$$|\underline{m}\rangle \mapsto \prod_{j=0}^{n-1}\left[\frac{|0\rangle + e^{i2\pi m 2^{j-n}}|1\rangle}{\sqrt{2}}\right] = \frac{\left(|0\rangle + e^{i2\pi m 2^{-1}}|1\rangle\right)_{n-1}\cdots\left(|0\rangle + e^{i2\pi m 2^{1-n}}|1\rangle\right)_{1}\left(|0\rangle + e^{i2\pi m 2^{-n}}|1\rangle\right)_{0}}{2^{n/2}}. \quad (18)$$

The subscripts on the brackets label the subsystems, which is shown explicitly since the phase applied to state $|1\rangle$ depends on the place of the subsystem in the order. Note that the symbol m appearing in the exponents takes integer values corresponding to the binary representation by the bit vector $\underline{m}$,

$$m = \sum_{k=0}^{n-1} m_k 2^k, \;\; m_k \in \{0,1\}.$$

Let us write the exponents more explicitly. For the subsystem j, we have

$$\frac{2\pi m}{2^{j-n}} = 2\pi \sum_{k=0}^{n-1} m_k 2^{k-(n-j)}.$$

The terms $k > n-j$ yield an integer multiple of 2π, and therefore the exponential can be written as,

$$\begin{aligned} e^{i2\pi m 2^{j-n}} &= \exp\left[i2\pi \sum_{k=0}^{n-j-1} \frac{m_k}{2^{n-j-k}}\right] \\ &= \exp\left[i\frac{2\pi m_0}{2^{n-j}}\right]\exp\left[i\frac{2\pi m_1}{2^{n-j-1}}\right]\exp\left[i\frac{2\pi m_2}{2^{n-j-2}}\right]\cdots\exp\left[i\frac{2\pi m_{n-j-1}}{2}\right]. \end{aligned} \quad (19)$$

Thus the subsystem j will involve a rotation that depends on the bit vectors upto $j-1$. We will return to this point shortly to derive a circuit for QFT, but after specifying the mathematical operation of QFT below.

Let us expand the product (18) by writing it as

$$\mathrm{QFT}\,|\underline{m}\rangle = \prod_{j=0}^{n-1}\left(\frac{1}{\sqrt{2}}\sum_{k_j=0}^{1} e^{2\pi i m 2^{j-n}k_j}|k_j\rangle\right), \quad (20)$$

and then fully expand it,

$$\mathrm{QFT}\,|\underline{m}\rangle = \sum_{k_{n-1}=0}^{1}\cdots\sum_{k_0=0}^{1}\left[\exp\left(\frac{i2\pi m}{2^n}\sum_{j=0}^{n-1}2^j k_j\right)|k_{n-1}\rangle\cdots|k_0\rangle\right]. \quad (21)$$

Recalling the definition of computational basis, we now identify a new basis,

$$|\underline{k}\rangle \equiv |k_{n-1}\rangle\cdots|k_0\rangle\,, \quad (22)$$

where the binary representation corresponds to the integer,

$$k = \sum_{j=0}^{2^n-1} 2^j k_j. \quad (23)$$

Thus the QFT transformation is

$$\mathrm{QFT}\,|m\rangle = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{i2\pi mk/2^n}\,|k\rangle\,. \tag{24}$$

Now let us take an arbitrary unit norm state and apply the QFT transformation to it. We let the state be defined as,

$$|x\rangle = \sum_{m=0}^{2^n-1} x_m\,|m\rangle\,. \tag{25}$$

Transforming each $|m\rangle$, we get

$$\mathrm{QFT}\,|x\rangle = \frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1}\sum_{m=0}^{2^n-1} x_m e^{i2\pi mk/2^n}\,|k\rangle = \sum_{j=0}^{2^n-1} y_k\,|k\rangle\,, \tag{26}$$

where the amplitudes y_k are seen as the Fourier transforms of the amplitudes x_m,

$$y_k = \frac{1}{2^{n/2}} \sum_{m=0}^{2^n-1} x_m e^{i2\pi mk/2^n}. \tag{27}$$

2. Circuit

Let us now return to (18) and (19) to determine the circuit for QFT. Prior to QFT operation the basis state $|\underline{m}\rangle$ is a product of $|0\rangle$ and $|1\rangle$ states of the n subsystems. We see from (18) that the QFT operation consists of two fundamental operations on each of the subsystems: Hadamard gate that maps it to the superpositions along with the phase depending on the bit m_j itself, and a rotation that depends on the bits $k = 0, \ldots, n-j-1$. For $n/2 < j < n-1$, the rotation depends only on bits $0, \ldots, j-1$, but for $j < n/2$, this dependnce is both on the bit itself and some of the bits above j. To simplify this, consider a different state in which the phases occur in the reverse order with respect to the order in 18,

$$\begin{aligned}\widetilde{QFT}\,|\underline{m}\rangle = \frac{1}{2^{n/2}} &\left(|0\rangle + e^{i2\pi m 2^{-n}}\,|1\rangle\right)_{n-1} \left(|0\rangle + e^{i2\pi m 2^{-(n-1)}}\,|1\rangle\right)_{n-2} \cdots \\ &\left(|0\rangle + e^{i2\pi m 2^{-2}}\,|1\rangle\right)_{2} \left(|0\rangle + e^{i2\pi m 2^{-2}}\,|1\rangle\right)_{1} \left(|0\rangle + e^{i2\pi m 2^{-1}}\,|1\rangle\right)_{0}.\end{aligned}$$

For this state, the phase on subsystem j is

$$e^{i2\pi m/2^{j+1}} = \exp\left[i\pi \sum_{k=0}^{j} m_k 2^{-(j-k)}\right].$$

The dependence is clearly one sided, i.e., only the bit values $k < j$ enter the rotation angle. Let us now define

$$R_q = \begin{bmatrix} 1 & \\ & \exp\left(2^{-q}\pi i\right) \end{bmatrix}.$$

With this definition, we can write the transformation of subsystem j as,

$$C_j(R_0)C_{j-1}(R_1)\cdots C_1(R_{j-1})C_0(R_j)H\,|m_j\rangle\,,$$

where $C_p(R_k)$ is the controlled-rotation gate in which p is the control bit and j is the target.

Next, we note that if we performed a SWAP operation that reverses the bit order in $\widetilde{QFT}\,|\underline{m}\rangle$, then we clearly obtain the state $QFT\,|\underline{m}\rangle$. We thus have to apply SWAP operations between qubits j and $n-j-1$ on the output of the circuit.

To specify the controlled rotation gate, we follow the ZY decomposition described above. The operator $R = e^{i\pi 2^{-q-1}(I-Z)}$, and so comparing it with

(9), $\alpha = 2^{-q-1}\pi$, $\beta = -2^{-q-1}\pi$, and $\gamma = \delta = 0$. Thus,

$$\begin{aligned} A &= e^{-i\pi/2^{q+2}Z}, \\ B &= e^{-i\pi/2^{q+3}Z}, \\ C &= e^{-i\pi/2^{q+3}Z}. \end{aligned}$$

The operator for controlled rotation is then identity if the control bit is 0. When the control bit is 1,

$$|1\rangle_p\,|m\rangle_j = |1\rangle_p\left[e^{i\pi/2^{q+1}I}e^{-i\pi/2^{q+2}Z}Xe^{-i\pi/2^{q+3}Z}Xe^{-i\pi/2^{q+3}Z}\right]|m\rangle_j\,.$$

H. Phase Estimation

Problem: Given a unitary operator U and an *eigenstate* $|x\rangle$ of this operator with an unknown eigenvalue, $e^{-i2\pi\phi}$, determine ϕ.

Solution: We solve this problem using the QFT transformation. We first attach an n-qubit register initialized to all zeros, and create the state

$$|\psi\rangle = |\underline{0}\rangle\,|x\rangle\,.$$

Next we apply the Hadamard gate to each qubit in the register, creating the state

$$|\psi\rangle = \prod_{j=0}^{n-1}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|x\rangle\,.$$

Apply the operation $C(U^{2^j})$ to the subsystem j, where $|x\rangle$ is the target. Thus, for example

$$\frac{|0\rangle_j\,|x\rangle + |1\rangle_j\,|x\rangle}{\sqrt{2}} \mapsto \left(\frac{|0\rangle_j + e^{-i2^j 2\pi\phi}\,|1\rangle_j}{\sqrt{2}}\right)|x\rangle\,.$$

We see that applying these C-gates to all subsystems, we obtain the following state,

$$|\psi'\rangle = C(U^{2^{n-1}})\cdots C(U^0)\,|\psi\rangle = \prod_{j=0}^{n-1}\left(\frac{|0\rangle + e^{-i2^j 2\pi\phi}\,|1\rangle}{\sqrt{2}}\right)|x\rangle\,.$$

When the expression on the right hand side is expanded, it yields all bit strings of length n and thus all the basis states (4). Furthermore, the phases on subsystem j are given by $e^{-i\phi m_j 2^j}$ since $m_j = 0$ for the state $|0\rangle$. Thus the state,

$$|\psi'\rangle = \frac{1}{2^{n/2}}\sum_{m=0}^{2^n-1} e^{-i2\pi m\phi}\,|m\rangle\,|x\rangle\,.$$

We now apply QFT to this state,

$$\mathrm{QFT}\,|\psi'\rangle = \sum_{m=0}^{2^n-1} f_k\,|k\rangle\,|x\rangle\,,$$

where the amplitudes $f_k$are given by (26),

$$f_k = \frac{1}{2^{n/2}} \sum_{m=0}^{2^n-1} e^{i2\pi m(k-2^n\phi)/2^n}.$$

Finally, we measure the state of the register. The Born principle says that we will get the state $|k\rangle\,|x\rangle$ with probability $F_k = |f_k|^2$. The function F_k has a sharp peak whenever $k = 2^n\phi \mod 2^n$. Thus we recover n-bit representation of the real number ϕ from the measurement outcome k.

I. Period finding

Problem: Given n qubits, a function $f(x)$ such that $f(x+a) = f(x)$, where both $x, a \in \{0, 1, 2, \ldots 2^n - 1\}$, determine a. We are also given a unitary operator U such that $U\,|x\rangle\,|0\rangle = |x\rangle\,|f(x)\rangle$, and an upper bound M such that $M > a$ and $N > M^2$.

Solution: Create a state with equal superposition of all $N = 2^n$ basis states and a second register initialized to $|0\rangle$,

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

Now apply the operator U to $|\psi\rangle$, creating the entangled state,

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

and then perform a projective measurement on the second register. This measurement will yield a specific value $f(x_0)$, and due to the periodicity of f, the resulting state will be,

$$|\psi'\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + ja\rangle\,|f(x_0)\rangle\,.$$

In the above sum, A is unknown since a is to be determined. However, for the known and fixed N, we must have

$$\begin{aligned} &N - a \le x_0 + (A-1)a < N, \\ &\Rightarrow \frac{N}{a} \le A < \frac{N}{a} + 1. \end{aligned}$$

The last inequalities follow because $x_0 \ge 0$. It is clear that A is the least integer greater than N/a or $A = \mathrm{ceil}(N/a)$. We now apply n-qubit QFT operation to the first register, which maps each term in the sum as in (24),

$$|\psi'\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N} y_k\,|k\rangle\,|f(x_0)\rangle\,, \tag{28}$$

$$\text{where, } y_k = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} e^{i2\pi jka/N}. \tag{29}$$

Finally, we perform a projective measurement on the first register, and collapse the state to $|k_0\rangle |f(x_0)\rangle$, with probability

$$P(k_0) = \frac{1}{A} \left| \frac{1 - e^{i2\pi A k_0 a/N}}{1 - e^{i2\pi k_0 a/N}} \right|^2 . \tag{30}$$

At modestly large N, this function shows sharp peaks at points where $2k_0a/N$ is close to an integer. The key observation is that for every multiple of N, denoted lN, there is a multiple of a within a distance $a/2$. To see this, mark the real line with multiples of a, creating subintervals of size a. Any multiple of N must reside in one of these sub-intervals. Thus for any N and a, there are integers l and k such that

$$ka - \frac{a}{2} < lN < ka + \frac{a}{2}.$$

Dividing by Na, we find that for any rational number k/N, there is another rational number l/a within a distance of $1/2N$, and whose denominator is the desired period,

$$\frac{k}{N} - \frac{1}{2N} < \frac{l}{a} < \frac{k}{N} + \frac{1}{2N}.$$

Since our measurement will yield a known value of $k = k_0$, and we know N, the rational number $k/N = k_0/N$ is also known, and we can thus write the above inequality as, a bound on l/a that becomes more precise as N increases,

$$\frac{k_0}{N} - \frac{1}{2N} < \frac{l}{a} < \frac{k_0}{N} + \frac{1}{2N} \tag{31}$$

$$\Rightarrow \frac{l}{a} - \frac{1}{2N} < \frac{k_0}{N} < \frac{l}{a} + \frac{1}{2N} \tag{32}$$

At this point, it becomes important to use the fact that the problem specifies that there is an upper bound on the period, namely $a < M < N$. Thus any rational numbers in the open interval $(l/a - 1/2N, l/a + 1/2N)$ must have denomintor less than M. We already know the existence of l/a as one of these rational numbers. How many rational numbers do we expect besides l/a? The answer is zero.

To see this, note that if there are two rational numbers p_1/q_1 and p_2/q_2 such that $q_1 < M$ and $q_2 < M$, then

$$\left| \frac{p_1}{q_1} - \frac{p_2}{q_2} \right| = \frac{|l_1 q_1 - l_2 q_2|}{q_1 q_2} > \frac{|l_1 q_1 - l_2 q_2|}{M^2} > \frac{1}{M^2} \geq \frac{1}{N}.$$

We see that any two rational numbers with denominators smaller than M are separated by more than $1/M^2$, and since the latter is larger than $1/N$ by choice of N for expected range of a, we can see that no rational number other than l/a can lie in the interval bounded by the known N.

Therefore, the specification that $N > M^2$ ensures that the number of qubits is high enough to uniquely identify this rational number. The bound (31) ensures that there is no other rational number of denominator less than M within the interval of size $1/N$.

To obtain a, we make continued fractions expansion of the number k_0/N. Since $k_0 < N$,

$$\frac{k_0}{N} = 0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots \cfrac{1}{a_{N-1} + \cfrac{1}{a_N}}}}.$$

Given a continued fraction expansion $a_0, \ldots, a_N$, of a number φ, a theorem in number theory gives a sequence of best rational number approximations $\{\varphi_n\}$, that converges to φ. The n-th term in the sequence is p_n/q_n , where q_n form

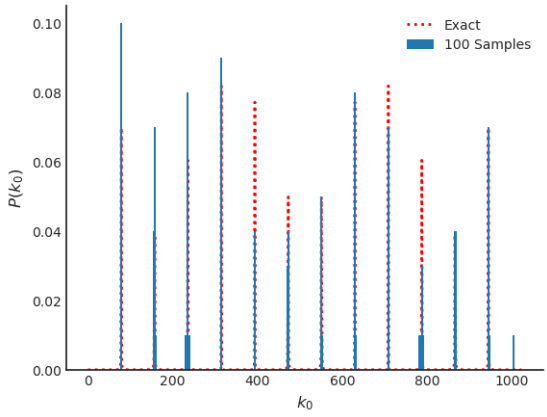

Figure 1 Probability function (30) for $a = 13$ (red) and that from a histogram of 100 samples (blue).

an increasing sequence in n, and p_n and q_n are generated by the recursion,

$$\begin{aligned} p_0 &= a_0, \\ p_1 &= 1 + a_0 a_1, \\ p_n &= a_n p_{n-1} + p_{n-2}, \end{aligned}$$

$$\begin{aligned} q_0 &= 1, \\ q_1 &= a_1, \\ q_n &= a_n q_{n-1} + q_{n-2}. \end{aligned}$$

The theorem states that if s/r is a rational number and $|s/r - \varphi| \leq 1/2r^2$, then s/r is a convergent of the continued fraction for φ [Nielsen Chuang, Theorem 5.1, page 229]. This theorem and the bound (31) thus enable us to identify the period uniquely if k_0 and N are co-prime (no common factors other than 1). The procedure is best illustrated using an Example 1.

If the period is even, and l is even, then there is no way of telling l/a apart from $(l/2)/(a/2)$. In this case, we can just discard the results and perform the experiment again. It is also possible to keep the results and repeat the experiment many times, obtaining a sequence $l_1/s_1, l_2/s_2, l_3/s_3, \ldots$. It can be shown that a is the lowest common multiple of s_i. This is illustrated in Example 2 below [TBD].

Example 1

In this example, we will perform a numerical experiment to illustrate the steps following (30). We will compute $P(k_0)$ with $a = 13$, and draw k_0 from this probability distribution. We let $N = 2^{10} = 1024$. The function $P(k)$ is illustrated in figure 1 for $a = 13$. We draw 100 samples, and see from the figure that the histogram of the counts agrees well with $P(k)$. We discard the values of k_0 that have probability below $1/2$ of the highest probability.

The most probable values of k_0 and the associated continued fraction expansion of k_0/N is shown in the first two columns of table I. The final column shows the difference between each term of the convergent sequence and k_0/N. From (31), we expect that the rational number l/a has a much smaller denominator than N, and that its distance from k_0/N is less than $1/2N$. The smallest n for which $|Np_n/q_n - k_0|$ reaches below 0.5, *and* for which $q_n < M = \sqrt{N}$, provides the best guess for l/a. We see that in each case, the period can be correctly deduced from the denominator q_n of this term in the sequence.

k_0	Continued Fraction of $k_0/1024$	Convergents p_n/q_n	$\lvert Np_n/q_n - k_0\rvert$
79	[0, 12, 1, 25, 3]	{1/12, **1/13**, 26/337, 79/1024}	{6.3, **0.23**, ...}
158	[0, 6, 2, 12, 1, 1, 1]	{1/3, 3/10, **4/13**, 311/1011, 315/1024}	{26.33, 7.80, **0.08**, ...}
315	[0, 3, 3, 1, 77, 1]	{1/2, 1/3, 2/5, **5/13**, 192/499, 197/512}	{118.00, 52.67, 15.60, **0.15**, ... }
473	[0, 2, 6, 15, 1, 1, 1, 1]	{1/2, **6/13**, 91/197, 97/210,188/407, 285/617, 473/1024}	{ 39.00, **0.38**, 0.02, 0.01, ... }

Table I Results of the numerical experiment of Example 1 of section II.I. The nubmers in bold is the first term of the sequence where the bound (31) is satisfied. The third column shows the actual values $|Np_n/q_n - k_0|$ where the corresponding numbers are also in boldface.

J. Order Finding

Problem: Let x be a number co-prime to an n-bit number $0 \leq N < 2^n$. Determine the order r of x such that

$$x^r = 1 \mod N.$$

Solution by Period Finding: We first note that if r is the order of $x \mod N$ as defined above, then $x^r \mod N$ is a periodic function with fundamental period r. Order finding is thus period finding, where we assume that a unitary operator $U_{x,N}$ is defined that maps a state as follows,

$$U_{x,N} |j\rangle |0\rangle = |j\rangle \left|x^j \mod N\right\rangle .$$

As in the period finding case, we form the superposition of all 2^N basis states in the first register, apply $U_{x,N}$ and perform a projective measurement of the second register. Since $x^{j+r} \mod N = x^j$, the resulting state of the first register is,

$$|\psi\rangle = \sum_{m=0}^{A-1} |j_0 + mr\rangle .$$

We then apply a QFT operation on this state, and perform a projective measurement, which would yield a number y/N such that the rational number l/r is within a distance $1/2N$ for some l/r. The resulting r is obtained using continued fraction expansion as illustrated in section II.I.

Solution by Phase Estimation: We can also use phase estimation by noting that due to the (unkown) periodicity r, there exists a transformation of the following form,

$$|y_l\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{i2\pi jl/r} \left|x^j \mod N\right\rangle , \tag{33}$$

$$\Rightarrow \left|x^j \mod N\right\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{-i2\pi jl/r} |y_l\rangle \tag{34}$$

$$\Rightarrow |1\rangle = \frac{1}{\sqrt{r}} \sum_{l} |y_l\rangle . \tag{35}$$

Now assume there is a way to apply the following operator,

$$U_x |y\rangle = U |(xy) \mod N\rangle ,$$

The state (33) is an eigenstate of this operator, in particular,

$$U_x \left|y_l\right\rangle = e^{-i2\pi l/r} \left|y_l\right\rangle . \tag{36}$$

While the state $|y_l\rangle$ cannot be formed since we do not know r in the first place, the state $|1\rangle$ is just a computational basis state, and by (35), it is a superposition of the $|y_l\rangle$ states. This is what the algorithm exploits.

Algorithm: Initialize the following state,

$$\left|\psi\right\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \left|j\right\rangle \left|1\right\rangle \;=\; \frac{1}{2^{n/2}} \prod_{b=0}^{n-1} \left(\left|0\right\rangle_j + \left|1\right\rangle_j\right) \left|1\right\rangle .$$

Recall that the second equality is the explicit representation of the first register in terms of the constituient qubits. Apply the phase estimation algorithm, which applies $C(U^{2^j})$ to the second register with the first as the control. However, before we take that step, we represent the second register as (35) where $r > 0$ is unknown but gurranteed to exist,

$$\begin{aligned} U\left|\psi\right\rangle &= \frac{1}{2^{n/2}} \prod_{b=0}^{n-1} \left(\left|0\right\rangle_j + e^{-i2\pi 2^b l/r} \left|1\right\rangle_j\right) \left|1\right\rangle \\ &= \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} \frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} e^{-i2\pi jl/r} \left|j\right\rangle \left|y_l\right\rangle . \end{aligned}$$

In the second equality, we expanded the product and returned back to the representation in terms of the comptuational basis for the first register. Now take the Fourier transform of the first register,

$$\begin{aligned} QFT\left[U\left|\psi\right\rangle\right] &= \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} f_{k,l} \left|k\right\rangle \left|y_l\right\rangle , \\ f_{k,l} &= \frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} e^{i2\pi j(k-2^n l/r)/2^n} . \end{aligned}$$

Measure the first register. With with probability $\left|f_{k,l}\right|^2$, it will collapse to a state $\left|k\right\rangle \left|y_l\right\rangle$ from which k can be retrieved. From the phase estimation algorithm, the post probable values for k will be such that $k/2^n$ is close to the rational number l/r. Since $r < \sqrt{N}$, we can bound the distance as in the Period finding algorithm and retrieve r from continued fraction expansion of $k/2^n$. In the phase estimation algorithm language, the first register will yield the n-bit representation of the "phase" l/r from which r is retrieved using continued fractions expansion.

K. Discrete Logarithm

Problem: Given integers x, g and p a prime, such that $g^p = 1$, solve for integer a such that,

$$x^a = g \mod p.$$

Solution: The key is to note is that the function,

$$f(\alpha, \beta) = x^\alpha g^{-\beta} \mod p \;=\; g^{a\alpha-\beta} \mod p,$$

has the property that $f(\alpha + m, \beta + am) = f(\alpha, \beta)$. If $p - 1$ is smooth, i.e. it has prime factors smaller than some n, then QFT with $p - 1$ roots of unity is possible in polynomial time. In that case, we initialize a 3-register state as follows,

$$\left|\psi\right\rangle = \frac{1}{p-1} \sum_{\alpha=0}^{p-2} \sum_{\beta=0}^{p-2} \left|\alpha\right\rangle \left|\beta\right\rangle \left|g^{a\alpha-\beta} \mod p\right\rangle . \tag{37}$$

Apply QFT with size $p-1$ to the first two registers,

$$|\psi\rangle = \frac{1}{p-1} \sum_{\alpha,\beta,k,k'=0}^{p-2} |k\rangle\,|k'\rangle\,\left|g^{a\alpha-\beta} \mod p\right\rangle e^{2\pi i(\alpha k+\beta k')/(p-1)}.$$

The probability that the state of the third register is $g^{\mu} \mod p$ involves all pairs α, β such that $g^{a\alpha-\beta} = g^{\mu} \mod p$. Thus for some l,

$$\begin{aligned} & a\alpha - \beta = \mu + lp \\ \Rightarrow\ & a\alpha - \beta = \mu + l + l(p-1) \\ \Rightarrow\ & a\alpha - \beta = \mu + l \mod (p-1). \end{aligned}$$

Since μ is picked arbitrarilty to simply denote a fixed state of the third register, we redefine it to be $\mu+l$ and measure the third register. The resulting state follows the constraint $a\alpha-\beta = \mu \mod (p-1)$, which is equivalent to $\beta = a\alpha-\mu \mod (p-1)$. The modulo $p-1$ is important since it allows us to drop it in the Fourier amplitude. We thus write the state as,

$$\left|\psi'_{\mu}\right\rangle = \frac{1}{p-1} \sum_{k,k'=0}^{p-2} |k\rangle\,|k'\rangle\,e^{-2\pi i\mu/(p-1)} \sum_{\alpha=0}^{p-2} \left[\omega^{k+ak'}\right]^{\alpha}, \tag{38}$$

where $\omega \equiv e^{2\pi i/(p-1)}$.

The summation over α vanishes unless

$$ak' = -k \mod (p-1).$$

This equation can be solved for a by division modulo $p-1$. This case of smooth $p-1$ is not interesting because classical algorithm exists to solve for a in polynomial time. The case where speedup exists is when $p-1$ is not smooth is handled by using QFT with respect to a smooth number q such that $p < q < 2p$. The analysis is very similar to above, but more involved and not fully appreciated by me yet. Shor's original paper discusses this in great detail. I will only sketch out what I think is the crux.

The initialization is still performed to create the state (37). However, the QFT is now done with $\omega_q = e^{2\pi i/q}$. The condition $\beta = a\alpha-\mu \mod (p-1)$ remains since the third register is still written for the order p cyclic group. However, the summation over α in (38) is now,

$$\begin{aligned} & \sum_{\alpha=0}^{p-2} \omega_q^{k\alpha+[\alpha a+\mu \mod (p-1)]k'} \\ = & \sum_{\alpha=0}^{p-2} \omega_q^{k\alpha+\alpha ak'+\mu k'-\left\lfloor \frac{\alpha a+\mu}{p-1} \right\rfloor (p-1)k'}. \end{aligned}$$

This expression can be used to find high probability states, which eventually lead to a continuted fractions expansion solution for a. At my present level of interest in the problem, I did not have the patience to follow that analysis. I will first do some numerical exeperiments to gain my own intuition into the above summation, and then arrive at Shor's analysis myself.

L. Prime Factorization (Shor's Algorithm)

Problem: Given a positive composite number N, find two prime factors of N. Note that it is promised that N is composite so that we expect to find a solution.

Solution: Shor's algorithm reduces factoring to order-finding by making use of two theorems.

Theorem 1 If N is composite and there is a positive integer $y < N$ that solves the constrained system,

$$y^2 = 1 \mod N, \tag{39}$$
$$y \mod N \notin \{-1, 1\}, \tag{40}$$

then either $\gcd(y-1, N)$ or $\gcd(y+1, N)$ or both are factors of N. The non-trivial factor of N can be computed with $O(L^3)$ operations.

Proof That this is so follows because (39) implies that for some positive integer p,

$$y^2 - 1 = pN,$$
$$\Rightarrow \frac{(y-1)(y+1)}{N} = p.$$

Thus N must have a common factor with $x-1$ or $x+1$ or both. Since $y < N$, the common factor cannot be N since in that case $y = N-1$, which violates (40). Therefore, $y - 1 < y + 1 < N$. Euclid's algorithm can be used to find $\gcd(y-1, N)$ and $\gcd(y+1, N)$ to retrieve the non-trivial factors in order $O((\log N)^3)$.

We see that if we find $x < N$ with even order r modulo N, then we can apply Theorem 1 with $y = x^{r/2}$ and obtain the factors smaller than N in $O((\log_2 N)^3)$ steps. The number x is generated randomly, and discarded if its order is not even. However, we have the assurance that a number x with even order can be found with high probability due to the following theorem,

Theorem 2 Suppose N is an odd composite and has the prime factorization, $N = x_1^{\alpha_1} \cdots x_m^{\alpha_m}$. Let x be an integer chosen uniformly at random subject to the conditions, $0 < x < N$ and x is co-prime to N. Then if $x^r \mod N = 1$,

$$P(r \text{ is even and} x^{r/2} \neq -1 \mod N) \geq 1 - \frac{1}{2^m}.$$

Thus the probability is at least 50% of finding a number x that has an even order and satisfies the conditions of Theorem 1. Note that the more prime factors there are (larger m), the higher the probability. The proof of this theorem is based on the Chinese remainder theorem, and is included in the Appendix [TBD].

Euclid's GCD Algorithm

The computation of greatest common divisor plays an essential role in two of the steps in Shor's algorithm. An efficient algorithm for computation of gcd is the Euclid algorithm. To compute the gcd of two numbers (n, m), replace the larger number by its modulus with the smaller. Thus if $m > n$, then $(n, m) \to (n, m \mod n)$. Iterate until the two are equal.

Example: Compute $gcd(252, 105)$. By Euclid algorithm: $(252, 105) \to (42, 105) \to (42, 21) \to (0, 21)$. Thus 21 is the greatest common divisor.

We now have all the ingredients to solve the problem of factorization. The algorithm is as follows.

Shor's Algorithm

Input: A composite number N

Output: One or more factors of N

1. If N is even, return 2.

2. Select an integer $x \in \{1, \ldots, N-1\}$ uniformly at random.
3. If $\gcd(x, N)$ is non-trivial, return $\gcd(x, N)$.
4. Using the quantum order finding algorithm, find the order r of x modulo N.
5. If r is odd, repeat by going to step 2.
6. If r is even,
   (a) If $\gcd(x^{r/2} - 1, N)$ is a factor, return $\gcd(x^{r/2} - 1, N)$.
   (b) If $\gcd(x^{r/2} + 1, N)$ is a factor, return $\gcd(x^{r/2} + 1, N)$.
7. If Step 6 did not return, the algorithm fails.

M. Database search (Grover's algorithm)

Problem: Let there be a database of N items, enumerated as $x = 0, \ldots, N-1$ and suppose we are given an oracle O_w that tests whether an item passes a certain test w or not. Thus the oracle performs the function $f_w(x) = 1$ if x passes the test w and $f_w(x) = 0$ otherwise. The test is provided by a unitary operator U_w such that,

$$U_w |x\rangle |y\rangle = |x\rangle |y \oplus f_w(x)\rangle .$$

Identify all the database items for which $f_w(x) = 1$.

Solution: Initialize the state of equal superposition of all database items,

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle , \tag{41}$$

and repeatedly apply the *Grover operator*

$$U_G = U_s U_w,$$

where

$$U_s = 2 |s\rangle \langle s| - I.$$

Why does this work?

As described in section II.F, the operator U_w can be turned into a phase oracle. Though we do not know what states in the database satisfy w, if we expect at least one solution, we can define a normalized state $|w\rangle$ that contains an equal superposition of all the solution states. Though we have no explicit representation of the oracle, we know that its representation in terms of the unknown $|w\rangle$ is,

$$U_w = I - 2 |w\rangle \langle w| .$$

When operating on any state $|\psi\rangle$, it assigns a phase -1 to the component of $|\psi\rangle$ along $|w\rangle$ and +1 to the orthogonal complement $|w^{\perp}\rangle$. We do not know these components separately, but we are sure that this is the operation of the oracle on a known quantum state. Furthermore, we can also write (41) as,

$$|s\rangle = \sqrt{\frac{M}{N}} |w\rangle + \sqrt{\frac{N-M}{N}} |w^{\perp}\rangle , \tag{42}$$

where M is the number of solutions to the test w, i.e. number of states for which $f_w(x) = 1$. The algorithm does not rely on knowing M, but only that $M \leq N$. The dynamics of this algorithm is best understood by defining an angle θ such that

$$\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}.$$

Then the state (42) can be written as

$$|s\rangle = \sin\frac{\theta}{2}|w\rangle + \cos\frac{\theta}{2}\left|w^{\perp}\right\rangle,$$

and in the space spanned by $|w\rangle$ and $\left|w^{\perp}\right\rangle$, the unitary operator U_s has the representation

$$\begin{aligned} U_s &= \left(2\sin^2\frac{\theta}{2} - 1\right)|w\rangle\langle w| + \left(2\cos^2\frac{\theta}{2} - 1\right)\left|w^{\perp}\right\rangle\left\langle w^{\perp}\right| + 2\sin\frac{\theta}{2}\cos\frac{\theta}{2}\left[|w\rangle\left\langle w^{\perp}\right| + \left|w^{\perp}\right\rangle\langle w|\right] \\ &= -\cos\theta|w\rangle\langle w| + \cos\theta\left|w^{\perp}\right\rangle\left\langle w^{\perp}\right| + \sin\theta\left[|w\rangle\left\langle w^{\perp}\right| + \left|w^{\perp}\right\rangle\langle w|\right]. \end{aligned}$$

Thus for states represented via 2-tuple (α, β) such that,

$$|\psi\rangle = \alpha|w\rangle + \beta\left|w^{\perp}\right\rangle,$$

the operator U_G takes the form of a rotation operator in two dimensions,

$$U_G = \begin{bmatrix} -\cos\theta & \sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}.$$

We now see that at the intialization, the state $|\psi(0)\rangle = |s\rangle$ has only a small component $\sin\theta = \sqrt{M/N}$ with the state we are searching for. With each iteration, the vector (α, β) in this space rotates towards $|w\rangle$. After $O(\sqrt{N})$ iterations, we expect the state to become aligned with $|w\rangle$.

The quantum search is as general as classical search as a fundamental step in many algorithms. We will not discuss those algorithms here as there are separate set of notes on them.

N. Suzuki-Trotter Evolution

O. Improving Approximations

Suppose that we have the ability to generate a group of elements, $\mathcal{G}_\epsilon$ such that for any $U \in SU(N)$, $\exists\tilde{U} \in \mathcal{G}_\epsilon$ such that $\left\|U - \tilde{U}\right\| < \epsilon$. That is, we have the technology to implement $\tilde{U}$ through a set of universal gate operations. Note that $\|\cdot\|$ is a measure of distance through some form of matrix norm. The particular form does not matter in this discussion. The group $\mathcal{G}_\epsilon$ is closed under multiplication and inverse. Let us define a matrix $W \in SU(N)$ such that

$$W = U\tilde{U}^{-1}. \tag{43}$$

Note that, if we knew W, we could construct U exactly by the multiplication $W\tilde{U}$. That is not our aim. Instead, we will show that we can take our existing technology implementing the group $\mathcal{G}_\epsilon$ to construct an *approximation* $\tilde{W}$ *such that* $\|W - \tilde{W}\| < C\epsilon^{3/2}$, where C is some constant independent of ϵ. This procedure lies at the heart of the Solovay-Kitaev theorem, which we will discuss in a separate subsection [TBD]. Here we will focus on the procedure itself.

Procedure: Since W is a special unitary, there is a Hermitian A such that $W = e^{iA}$. Since $\|U\tilde{U}^{-1} - I\| < \epsilon$, we also know that $A \sim O(\epsilon)$. We also know that there exist Hermitian operators B and C such that

$$[B, C] = -iA, \quad B, C \sim O(\epsilon^{1/2}).$$

We can find elements $e^{i\tilde{B}}$ and $e^{i\tilde{C}}$ in $\mathcal{G}_\epsilon$ such that $\left\|B - \tilde{B}\right\| < \epsilon$ and $\left\|C - \tilde{C}\right\| < \epsilon$. Since $\mathcal{G}_\epsilon$ also contains the inverses of all its elements, we can now construct $\tilde{W}$ by the following ordered multiplication of the elements of $\mathcal{G}_\epsilon$,

$$\tilde{W} = e^{i\tilde{B}} e^{i\tilde{C}} e^{-i\tilde{B}} e^{-i\tilde{C}}.$$

By the Baker-Hausdorff-Campbell formula,

$$\begin{aligned}
\tilde{W} &= e^{i(\tilde{B}+\tilde{C}) - \frac{1}{2}[\tilde{B},\tilde{C}] + O\left(\epsilon^{3/2}\right)} e^{-i(\tilde{B}+\tilde{C}) - \frac{1}{2}[\tilde{B},\tilde{C}] + O\left(\epsilon^{3/2}\right)} \\
&= e^{-[\tilde{B},\tilde{C}] + O\left(\epsilon^{3/2}\right)} \\
&= e^{-[B+O(\epsilon), C+O(\epsilon)] + O\left(\epsilon^{3/2}\right)}.
\end{aligned}$$

Since the matrices B, C are both $O(\sqrt{\epsilon})$, it follows that

$$\tilde{W} = e^{iA} + O(\epsilon^{3/2}) \;=\; W + O(\epsilon^{3/2}).$$

Therefore, by picking 5 gate operations available from $\mathcal{G}_\epsilon$: $\tilde{U}$, $e^{\pm i\tilde{B}}, e^{\pm i\tilde{C}}$, we find $\tilde{W}$ that approximates W in (43) within an error of $O(\epsilon^{3/2})$. Since the defining property of W is that it approximates the matrix $U\tilde{U}^{-1}$ with an error of $c\epsilon^{3/2}$, we claim that

$$\left\|U - \tilde{W}\tilde{U}\right\| < (c\epsilon)^{3/2}.$$

We see that when applying the gate $\tilde{U}$, we can also construct and multiply by $\tilde{W}$ to better approximate the exact unitary demanded by our algorithms in simulation of quantum dynamics.

Now suppose we have l_0 gates to approximate U with error ϵ_0. Then $5l_0$ gates will approximate it to $(c\epsilon)^{3/2}$. After k iterations $(5)^k l_0$ gates will approximate the error to

$$\begin{aligned}
\epsilon_k &= (c\epsilon_0)^{(3/2)^k}, \\
\left(\frac{3}{2}\right)^k &= \frac{\log(1/\epsilon)}{\log(c\epsilon_0)} \\
\Rightarrow k \log 5 &= \frac{\log(5)}{\log(3/2)} \log\left[\frac{\log(1/\epsilon)}{\log(c\epsilon_0)}\right] \\
&= 3.97 \log\left[\frac{\log(1/\epsilon)}{\log(c\epsilon_0)}\right].
\end{aligned}$$

Thus the number of gates is

$$N = O(5^k l) \;=\; O\left(\log^{3.97}(1/\epsilon)\right).$$

This shows us that the number of gates required grows slightly less than the 4th power of the logarithm of the *target error.*

III. QUANTUM STATES AND ENTANGLEMENT

A. Density Operator

Suppose that our knowledge of the system is such that with probability p_i the system is in the state $|\psi_i\rangle$ where the states are arbitrary normalizable states of the system. Then the expectation value of an operator W is

$$\left\langle \hat{W} \right\rangle = \sum_i p_i \langle \psi_i | \hat{W} | \psi_i \rangle .$$

We now introduce a set of basis states, $|\alpha\rangle$, and write the above equation in the form

$$\begin{aligned} \left\langle \hat{W} \right\rangle &= \sum_{\alpha,\alpha'} \sum_i p_i \langle \psi_i | \alpha \rangle \langle \alpha | \hat{W} | \alpha' \rangle \langle \alpha' | \psi_i \rangle \\ &= \sum_\alpha \langle \alpha | \left[\hat{W} \sum_i \sum_{\alpha'} | \alpha' \rangle \langle \alpha' | p_i | \psi_i \rangle \langle \psi_i | \right] | \alpha \rangle . \end{aligned}$$

The last line is a trace of a matrix, and we thus have the result,

$$\left\langle \hat{W} \right\rangle = \mathrm{Tr} \left[\hat{W} \hat{\rho} \right],$$

where we define the *density operator,*

$$\hat{\rho} = \sum_i p_i | \psi_i \rangle \langle \psi_i | .$$

Therefore, the density operator represents a mixture of states, defined by a set of (real-valued) probabilities, and the projection operators on those states. Due to the condition that $\sum_i p_i = 1$, and the states have unit norm, the density operator always satisfies the following two conditions,

$$\begin{aligned} \mathrm{Tr} \left[\hat{\rho} \right] &= 1, \\ \mathrm{Tr} \left[\hat{\rho}^2 \right] &\leq 1. \end{aligned}$$

Since $\hat{\rho}$ is Hermitian, its eigenvalues are real and the first condition ensures that its eigenvalues sum to 1. Furthermore, the definition shows that the operator is also positive definite, and therefore the eigenvalues lie in the interval $[0, 1]$. From this, the second condition follows. Finally, a system is in a *pure state* if and only if $p_i = 0$ for all i except one, and equivalently, if and only if $\mathrm{Tr} \left[\hat{\rho}^2 \right] = 1$.

B. Many Body States

Suppose we arbitrarily divide a many particle system into two sub-systems. For example, we may imagine a boundary and define all particles inside that boundary as belonging to system A and those outside to B. With our notation of computational basis states (4), we write a many body state of n particles as follows.

$$| \Psi_n \rangle = \sum_{\underline{m}} \psi(\underline{m}) | m_0 \rangle \dots | m_{n-1} \rangle . \tag{44}$$

Now we arbitrarily define subset A and B of indices such that $A + B = \{ i : 0 \leq i < n \}$. For each vector $\underline{m}$, we also define

$$\begin{aligned} \underline{m}_A &= (m_{i_1}, m_{i_2,\dots}), \quad i_k \in A, \\ \underline{m}_B &= (m_{i_1}, m_{i_2,\dots}), \quad i_k \in B. \end{aligned}$$

Thus, another way to write the state (44) is,

$$|\Psi_n\rangle = \sum_{\underline{m}_A} \sum_{\underline{m}_B} \psi(\underline{m}_A, \underline{m}_B) \, |\underline{m}_A\rangle \, |\underline{m}_B\rangle \, . \tag{45}$$

Reverting back to integer indices, we thus have

$$|\Psi_n\rangle = \sum_{i \in A} \sum_{j \in B} \psi_{ij} \, |i\rangle_A \, |j\rangle_B \, . \tag{46}$$

The coefficients ψ_{ij} define a rectangular matrix since the sizes of the sets A and B are not necessarily the same. We perform singular value decomposition of ψ_{ij},

$$\psi_{ij} = \left[u \sigma v^\dagger\right]_{ij} \; = \; u_{ik} \sigma_{kk} v^*_{jk}. \tag{47}$$

The unit norm of $|\Psi_n\rangle$ ensures that $\mathrm{Tr}\left[\psi^\dagger \psi\right] = 1$. The matrix u is $n_A \times n_A$ unitary matrix where n_A is the number of states in A, and V is $n_B \times n_B$ unitary matrix. The matrix σ is $n_A \times n_B$ with ones along the diagonal and zeros everywhere else. The diagonal entries, or the singular values σ_{kk}, are always real, and thus must satisfy

$$\sum_k \sigma_{kk}^2 = 1.$$

When we substitute (47) into (44), we find that

$$|\Psi_n\rangle = \sum_k \left(\sigma_{kk} \sum_{i \in A} u_{ik} \, |i\rangle_A \sum_{j \in B} v^*_{jk} \, |j\rangle_B \right) .$$

Based on the sums over i and j, we now define a *basis set* for each subystem

$$|a_k\rangle_A = \sum_{i \in A} u_{ik} \, |i\rangle_A \, ,$$
$$|b_k\rangle_B = \sum_{i \in B} v^*_{ik} \, |i\rangle_B \, .$$

The many body state thus takes the equivalent form

$$|\Psi_n\rangle = \sum_k \sigma_{kk} \, |a_k\rangle_A \, |b_k\rangle_B \, .$$

This is called the *Schmidt decomposition* and we have just proven the following theorem.

Schmidt Decomposition

Theorem: Suppose $|\Psi\rangle$ is a pure state of a composition system AB. Then there exist *orthornormal* states $|a_k\rangle_A$ and $|b_k\rangle_B$ such that

$$|\Psi_n\rangle = \sum_k \lambda_k \, |a_k\rangle_A \, |b_k\rangle_B \, ,$$

where λ_k are non-negative real numbers satisfying

$$\sum_k \lambda_k^2 = 1.$$

Clearly, we can further subdivide the systems A and B in a similar manner. Suppose we divided A into A_1 and A_2, then

$$|\Psi_n\rangle = \sum_k \lambda_k \gamma_{kp} \, |\alpha_{kp}\rangle_{A_1} \, |\alpha_{kp}\rangle_{A_2} \, |b_k\rangle_B \, ,$$

where γ_{kp} and α_{kp} define the coefficients of the k^{th} state of the system $A = A_1 \oplus A_2$ in terms of the Schmidt decomposition into A_1, A_2. When this process is iterated recursively, we obtain the so called *Matrix Product States.* We will discuss these in a greater detail and with a more convenient notation in the subesquent notes.