Quantum Computing Primer

Subhayan Roychoudhury
The Molecular Foundry
Lawrence Berkeley National Laboratory

Electronic Structure Theory and the Problem of Scaling

Any general single-particle state $|\phi\rangle$ can be expressed with respect to position vectors (eigenvectors of the position operator) $|\mathbf{r}\rangle$ as

$$\begin{aligned} |\phi\rangle &= \int d\mathbf{r}\, |\mathbf{r}\rangle \langle \mathbf{r}|\phi\rangle \\ &= \int d\mathbf{r}\phi(\mathbf{r})\, |\mathbf{r}\rangle\,, \end{aligned} \tag{1}$$

where we have defined

$$\phi(\mathbf{r}) = \langle \mathbf{r}|\phi\rangle\,. \tag{2}$$

For the sake of computational feasibility, we need to work with a discrete set of points within a real space grid. Then, we need to replace the integral with a sum as

$$|\phi\rangle = \sum_{i=1}^{M} \phi_i\, |\mathbf{r}_i\rangle\,, \tag{3}$$

where M denotes the total number of grid points, $|\mathbf{r}_i\rangle$ is the position-vector associated with the i-th grid point, and

$$\phi_i = \langle \mathbf{r}_i|\phi\rangle\,. \tag{4}$$

Eq. 3 shows that, in this representation, our basis set $\{|\mathbf{r}_1\rangle\,, |\mathbf{r}_2\rangle\,, \ldots, |\mathbf{r}_M\rangle\}$ has M number of basis vectors.

What happens if, instead of a single particle, we need to describe a two-particle state within the same grid. Now our basis set becomes something like

$$\{|\mathbf{r}_1\mathbf{r}_1\rangle\,, |\mathbf{r}_1\mathbf{r}_2\rangle\,, \ldots, |\mathbf{r}_1\mathbf{r}_M\rangle\,, |\mathbf{r}_2\mathbf{r}_1\rangle\,, |\mathbf{r}_2\mathbf{r}_2\rangle\,, \ldots, |\mathbf{r}_2\mathbf{r}_M\rangle\,, \ldots, |\mathbf{r}_M\mathbf{r}_1\rangle\,, |\mathbf{r}_M\mathbf{r}_2\rangle\,, \ldots, |\mathbf{r}_M\mathbf{r}_M\rangle\},$$

where

$$|\mathbf{r}_i\mathbf{r}_j\rangle = |\mathbf{r}_i\rangle \otimes |\mathbf{r}_j\rangle$$

Thus, we now have M^2 basis vectors in out set. Generalizing to an N-particle system, we will need M^N number of basis functions. This is an example of exponential scaling with respect to the number of particles.

Now, if there particles are consideration are electrons then a couple of additional points need to be taken into account.

1. Electrons have an additional *spin* degree of freedom, which, for a single particle requires two basis vectors (we will use $\uparrow$ and $\downarrow$ to denote them). So, the single-electron basis set should be modified to

   $$\{|\mathbf{r}_1^{\uparrow}\rangle\,, |\mathbf{r}_1^{\downarrow}\rangle\,, |\mathbf{r}_2^{\uparrow}\rangle\,, |\mathbf{r}_2^{\downarrow}\rangle\,, \ldots, |\mathbf{r}_M^{\uparrow}\rangle\,, |\mathbf{r}_M^{\downarrow}\rangle\}$$

   This has $2M$ basis vectors. We shall call them spin-orbitals in the position basis. Thus, for N-particles, we will need $(2M)^N$ basis vectors.

2. Electrons are indistinguishable particles with wavefunctions that are antisymmetric with respect to an exchange of any two electrons. This implies, for example, that

$$|\mathbf{r}_i^\alpha \mathbf{r}_j^\beta\rangle = -\,|\mathbf{r}_j^\beta \mathbf{r}_i^\alpha\rangle\,, \tag{5}$$

and therefore, we do not need to consider them separately when we construct our basis set. We can, in fact, combine them into the so-called Slater determinants.

This also implies that

$$|\mathbf{r}_i^\alpha \mathbf{r}_i^\alpha\rangle = -\,|\mathbf{r}_i^\alpha \mathbf{r}_i^\alpha\rangle = |0\rangle\,. \tag{6}$$

Therefore, from our basis set, we can discard any vector in which the same spin-orbital is occupied by multiple electrons. These considerations will reduce the number of vectors required for our N-particle basis set. Any basis vector that we need to include in our new basis set can now be uniquely defined by specifying which spin-orbitals are occupied and which ones are empty (since no spin-orbital can have multiple occupancy and since, thanks to indistinguishability, we do not care which electron is in which orbital). Thus, each basis vector corresponds to choosing N number of occupied orbitals from a total $2M$ number of orbitals. Therefore, instead of $(2M)^N$, now the number of basis-vectors in our set should be ${}_{2M}C_N$ (the binomial coefficient of $2M$ and N).

If there are M number of spin-orbitals, then any such basis vector (Slater determinant) can be written as

$$\text{SD} = |j_{M-1} j_{M-2} \dots j_1 j_0\rangle\,, \tag{7}$$

where for any $i = 0, \dots, M-1$, the value of j_i can be either 0 or 1. In this convention, $j_i = 0$ and $j_i = 1$ will indicate, respectively, that the $(i+1)$-th spin-orbital is empty and occupied. Since each spin-orbital can only have two possible occupancies (0 or 1), the number of possible Slater determinants can not exceed 2^M. However, if the total number of electrons is known to be N, then we know that every Slater determinant must have exactly N number of occupied orbitals. Then, as mentioned earlier, the possible number of Slater determinants boils down to (M *choose* N), which, for any N, can never exceed 2^M.

Let us take a concrete example. If there are 2 electrons in our system (like in a hydrogen molecule), then, the representation of an arbitrary electronic state on a $10\times10\times10$ real space grid will require ${}_{2000}C_2$ i.e, 1999000 basis vectors. Consequently, we need to store 1999000 number of coefficients if we want to store this state (written as a linear combination of the basis vectors) on a computer. Assuming each coefficient requires a byte of storage, we will need slightly less than 2 MB.

If there are 42 electrons in our system (like in a benzene molecule), then the number of basis vectors is ${}_{2000}C_{42}$. This has the order of 10^{87}. Therefore, the number of bytes required to store all the coefficients will exceed the estimated number of atoms in the universe!

For practical computation, this poses a serious problem in terms of scaling. On a conventional computer, the increment in memory is linear with the increment in the number of storage units. If you double the number of bits, you get twice as much memory. However,

for N and M of practical interest, the scaling of $2M$ *choose* N with respect to N is substantially higher. Thus, in practice, if we really want to store all the necessary coefficients on a memory-device, we need a device whose capacity (with respect to the number of storage units) scales *at least* as quickly $2M$ *choose* N. This is exactly where a quantum computer can help.

How, then, can we represent a general many-electron state, written as a linear combination of ${}_MC_N$ Slater determinants like the one shown in Eq. 7, with the help of a quantum computer?

The Qubit

For a quantum computer, the unit of information is a qubit. The state of a single qubit resides in a 2-dimensional vector space. Thus, any state of a single qubit can be written as a linear combination of basis vectors from this 2-dimensional vector space. Naturally, any basis-set of this space contains two basis vectors. Let us choose a set where the two orthogonal basis vectors are denoted by $|0\rangle$ and $|1\rangle$. Thus, any general vector

$$|a\rangle = a_0 |0\rangle + a_1 |1\rangle \tag{8}$$

can be expressed in matrix-form as $\begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$.

Naturally, the basis-vectors $|0\rangle$ and $|1\rangle$ themselves will be written as $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, respectively.

A tensor product of $|a\rangle$ and $|b\rangle = b_0 |0\rangle + b_1 |1\rangle$ is then given by

$$|ab\rangle = |a\rangle \otimes |b\rangle = a_0 b_0 |0\rangle \otimes |0\rangle + a_0 b_1 |0\rangle \otimes |1\rangle + a_1 b_0 |1\rangle \otimes |0\rangle + a_1 b_1 |1\rangle \otimes |1\rangle . \tag{9}$$

$|ab\rangle$ resides in a 4-dimensional space which is the tensor-product space of the two aforementioned vector spaces (i.e., one which hosts $|a\rangle$ and one which hosts $|b\rangle$). If we choose to use $\{|0\rangle \otimes |0\rangle , |0\rangle \otimes |1\rangle , |1\rangle \otimes |0\rangle , |1\rangle \otimes |1\rangle\}$ as the basis-set of this space, then, in matrix form, the vector $|ab\rangle$ can be expressed as $\begin{pmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 b_0 \\ a_1 b_1 \end{pmatrix}$ For example, the two-qubit state $|01\rangle$ can be written as $\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$

This notion can be generalized to more than 2 qubits in a straightforward manner. Continuing the convention introduced in Eq. 8 and 9, for the 2^n dimensional vector space of n qubits, we will choose the basis set

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

Each basis vector contains n terms, each of which can be either 0 or 1. The basis vectors are ordered in such a way that, for each vector, the rightmost term changes between every consecutive vector. The next (to the left) term remains unchanged for two consecutive vectors and then changes. Continuing in this fashion, it is easy to see that the leftmost term remains unchanged at 0 for the first 2^{n-1} basis vectors and then stays fixed at 1 for the rest of the vectors. Such a basis set will be referred to as a computational basis set for n qubits.

Many-electron States : a Qubit-based Representation

From the discussion presented above, we can see that any computational basis-vector of M qubits can be written as

$$|B\rangle = |q_{M-1}q_{M-2}\dots q_1 q_0\rangle\,, \tag{10}$$

where, for any $i = 0, \dots, M-1$, the value of q_i can be either 0 or 1. It is easy to notice the resemblance between Eq. 10, i.e., a basis-vector of the M-qubit Hilbert space and Eq. 7, a basis-vector for a many-electron system with M spin-orbitals. Therefore, in order to represent an arbitrary many-electron state using qubits, we can adopt a convention whereby, the i-th qubit being in state $|1\rangle$ will indicate that the $(i+1)$-th spin-orbital is occupied while the state $|0\rangle$ for the qubit will indicate an unoccupied $(i+1)$-th spin-orbital. Then, any general many-electron state of any number of electrons ($< M$), expressible as a linear-combination of Slater determinants (Eq. 7) composed of M spin-orbitals, can be represented by some general M-qubit state constructed as a linear-combination of the computational basis-vectors (Eq. 10).

Quantum Gates

Let us now dig a little deeper into the details of quantum computation, starting with operators. In the context of quantum-circuits, an N-qubit operator is essentially an N-qubit gate that changes an N-qubit quantum state from some initial state $|I\rangle$ to some final state $|F\rangle$.

Naturally, an operator in an N-dimensional space can be uniquely defined by specifying its actions on the basis functions (which are N in number) of any basis set of that space. Working with the choice of basis set introduced earlier, the Hadamard gate $\hat{H}$ for the 1-qubit space can be defined as

$$\begin{aligned}\hat{H}\,|0\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = |+\rangle \\ \hat{H}\,|1\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) = |-\rangle\end{aligned} \tag{11}$$

The orthonormality of $\{|0\rangle\,, |1\rangle\}$ implies that

$$\langle 0|\hat{H}|0\rangle = \frac{1}{\sqrt{2}}, \qquad \langle 0|\hat{H}|1\rangle = \frac{1}{\sqrt{2}}, \qquad \langle 1|\hat{H}|0\rangle = \frac{1}{\sqrt{2}}, \qquad \langle 1|\hat{H}|1\rangle = -\frac{1}{\sqrt{2}}.$$

Therefore, with respect to the aforementioned basis set, $\hat{H}$ can be written in matrix form as

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \tag{12}$$

Another 1-qubit gate is the Pauli gate $\hat{X}$ whose operations are given by

$$\hat{X}\left|0\right\rangle = \left|1\right\rangle \quad \text{and} \quad \hat{X}\left|1\right\rangle = \left|0\right\rangle,$$

indicating a matrix representation of $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$. A tensor-product of N number of single-qubit operators (each operator associated with a 2-dimensional vector space) is an operator acting on N qubits (associated with a 2^N dimensional vector space). With this in mind, let us construct a simple 2-qubit operator from $\hat{X}$ and $\hat{H}$ such that its operation on the state $|ab\rangle$ (see Eq. 9) follows

$$\hat{XH}\left(\left|ab\right\rangle\right) = \left(\hat{X}\left|a\right\rangle\right) \otimes \left(\hat{H}\left|b\right\rangle\right) \tag{13}$$

$$= \left(a_0\left|1\right\rangle + a_1\left|0\right\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(b_0\left|+\right\rangle + b_1\left|-\right\rangle\right) \tag{14}$$

Note that the final state after operation of $\hat{XH}$ can be written as a simple tensor-product of two single-qubit states. Thus, after the operation, the second qubit will be in the state $\left(a_0\left|1\right\rangle + a_1\left|0\right\rangle\right)$ and the first qubit will be in the state $\frac{1}{\sqrt{2}}\left(b_0\left|+\right\rangle + b_1\left|-\right\rangle\right)$ with a normalization factor of $\frac{1}{\sqrt{2}}$. Thus, the final state is **not entangled**. This is not surprising, given that the 2-qubit operator $\hat{XH}$ itself is a simple tensor-product of 2 single-qubit operators.

Let us see an example where this is no longer true.

A controlled gate acts on a 2-qubit state in such a way that, if the left (control) qubit is in state $|0\rangle$, then it performs an identity operation ($\hat{I}$) on the right (target) qubit. However, if the control qubit is in state $|1\rangle$, then the controlled gate will perform a predefined operation on the target qubit. A controlled NOT (CNOT) gate, for which the predefined operation is a Pauli $\hat{X}$ operation, is a well-known example. Thus,

$$\begin{aligned}
\hat{\text{CNOT}}\left|00\right\rangle &= \left|0\right\rangle \otimes \left(\hat{I}\left|0\right\rangle\right) = \left|00\right\rangle\\
\hat{\text{CNOT}}\left|01\right\rangle &= \left|0\right\rangle \otimes \left(\hat{I}\left|1\right\rangle\right) = \left|01\right\rangle\\
\hat{\text{CNOT}}\left|10\right\rangle &= \left|1\right\rangle \otimes \left(\hat{X}\left|0\right\rangle\right) = \left|11\right\rangle\\
\hat{\text{CNOT}}\left|11\right\rangle &= \left|1\right\rangle \otimes \left(\hat{X}\left|1\right\rangle\right) = \left|10\right\rangle,
\end{aligned}$$

which indicates a matrix form of $\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}$.

Acting on the 2-qubit state $|+0\rangle$, this will produce

$$\begin{aligned}\hat{\text{CNOT}}\,|+0\rangle &= \frac{1}{\sqrt{2}}\hat{\text{CNOT}}\,|00\rangle + \frac{1}{\sqrt{2}}\hat{\text{CNOT}}\,|10\rangle \\ &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right).\end{aligned}$$

This can not be written as a tensor product of 2 single-qubit states. If we measure the state of the first qubit (in this context, when I say "measure the state" of a qubit, what I mean is "measure the observable corresponding to the operator $\hat{Z}$, for which the eigenvectors are $|0\rangle$ and $|1\rangle$) and get, for example, the eigenvalue corresponding to $|1\rangle$, then we know immediately that the entire 2-qubit system must have collapsed to the state $|11\rangle$. Therefore, if we measure the state of the second qubit immediately, we are guaranteed to get $|0\rangle$. Thus, in the state $\hat{\text{CNOT}}\,|0+\rangle$, the two qubits are entangled! Under these circumstances, there is no such thing as "state of the first qubit" or "state of the second qubit".

The controlled rotation CROT gate is another example of a contolled gate. This gate performs a rotation operation $\hat{U}_\theta$ by a predefined angle θ such that

$$\hat{U}_\theta\,|\psi\rangle = e^{i\theta}\,|\psi\rangle$$

on the target qubit, if the control qubit is $|1\rangle$.

Let us operate this on the 2-qubit state

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\otimes|1\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |11\rangle\right)$$

. This should produce

$$\frac{1}{\sqrt{2}}\left(|01\rangle + \exp^{i\theta}|11\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle + \exp^{i\theta}|1\rangle\right)\otimes|1\rangle$$

. Interestingly, the operation has altered the state of the control qubit from $\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$ to $\frac{1}{\sqrt{2}}\left(|0\rangle + \exp^{i\theta}|1\rangle\right)$, leaving the state of the target qubit intact at $|1\rangle$. In other words, a rotation was essentially applied to the control qubit, even though the rotation operator $\hat{U}_\theta$ acted only on the target qubit. The result of the phase-rotation of the target qubit is effectively kicked back onto the control qubit. This effect is called **phase kickback**. Now we will use this effect to construct a quantum circuit that can solve a crucial problem, namely that of finding the discreet Fourier transform.

A periodic function $f(x)$ with a period of l can be written as a linear combination of its Fourier components as

$$f(x) = \frac{1}{\sqrt{l}}\sum_{k=-\infty}^{+\infty}\tilde{f}(k)e^{-2\pi i\frac{kx}{l}}, \tag{15}$$

where $\tilde{f}(k)$ is given by

$$\tilde{f}(k) = \frac{1}{\sqrt{l}}\int_0^l f(x)e^{2\pi i\frac{xk}{l}}dx. \tag{16}$$

Discretizing the problem, the discreet Fourier transform of a sequence of N complex numbers $\{f(0), f(1), \ldots, f(N-1)\}$ (if we assume that the sequence repeats itself after an interval of N, we can compare the elements of this sequence with the values of $f(x)$ from Eq. 15 at a discrete set of points) can be defined as

$$\tilde{f}(k) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} f(j) e^{2\pi i \frac{jk}{N}} \tag{17}$$

We would want the Quantum Fourier Transform (QFT) operator $\hat{U}_{\text{QFT}}$ to transform a vector with expansion-coefficients $\{f(0), f(1), \ldots, f(N-1)\}$ with respect to the computational basis-set into a vector with coefficients $\{\tilde{f}(0), \tilde{f}(1), \ldots, \tilde{f}(N-1)\}$. In mathematical terms:

$$\hat{U}_{\text{QFT}} \left(\sum_{k=0}^{N-1} f(k) \left| k \right\rangle \right) = \sum_{k=0}^{N-1} \tilde{f}(k) \left| k \right\rangle , \tag{18}$$

where $|k\rangle$ is the k-th vectors of the computational basis set. Notably, the basis set contains N number of basis vectors. Therefore, this N-dimensional vector space is associated with $n = log_2(N)$ qubits. Taking inner product of both sides of Eq. 18 with $\langle j|$ and summing over j,

$$\begin{aligned} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} f(k) \langle j | \hat{U}_{\text{QFT}} | k \rangle &= \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} \tilde{f}(k) \delta_{j,k} \\ &= \sum_{j=0}^{N-1} \tilde{f}(j) \\ &= \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \left(\sum_{k=0}^{N-1} f(k) e^{2\pi i \frac{kj}{N}} \right) \end{aligned}$$

where, in the third equality we have used the expansion of $\tilde{f}(j)$ in accordance with Eq. 17. The above equation implies

$$\langle j | \hat{U}_{\text{QFT}} | k \rangle = \frac{1}{\sqrt{N}} e^{2\pi i \frac{kj}{N}},$$

i.e.,

$$\hat{U}_{\text{QFT}} = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \sum_{k=0}^{N-1} e^{2\pi i \frac{kl}{N}} \left| k \right\rangle \langle l |$$

Now, we will try to express

$$\hat{U}_{\text{QFT}} \left| j \right\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j \frac{k}{N}} \left| k \right\rangle . \tag{19}$$

as a tensor-product of n number of single-qubit states. At this point, it is necessary to express the integer k in terms of its binary representation. If k can be written in binary form as

$$k_{n-1}k_{n-2}\ldots k_0 \qquad\qquad \text{where } k_i \in \{0,1\} \forall i = 0,\ldots,n-1,$$

where k_0 is the least significant bit, then

$$k = k_{n-1}2^{n-1} + k_{n-2}2^{n-2} + \ldots + k_0 2^0.$$

Therefore,

$$\frac{k}{N} = \frac{k}{2^n} = \sum_{t=0}^{n-1} \frac{k_t}{2^{n-t}}. \tag{20}$$

Plugging this expression back into Eq. 19, the following equation is obtained:

$$\begin{aligned}
\hat{U}_{\text{QFT}} |j\rangle &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j \left(\sum_{t=0}^{n-1} \frac{k_t}{2^{n-t}}\right)} |k\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \left(\prod_{t=0}^{n-1} e^{2\pi i j \frac{k_t}{2^{n-t}}} \right) |k\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{k_{n-1}=0}^{1} \ldots \sum_{k_1=0}^{1} \sum_{k_0=0}^{1} \left(e^{2\pi i j \frac{k_{n-1}}{2}} |k_{n-1}\rangle \right) \otimes \ldots \otimes \left(e^{2\pi i j \frac{k_1}{2^{n-1}}} |k_1\rangle \right) \otimes \left(e^{2\pi i j \frac{k_0}{2^n}} |k_0\rangle \right) \\
&= \frac{1}{\sqrt{N}} \left(\sum_{k_{n-1}=0}^{1} \left(e^{2\pi i j \frac{k_{n-1}}{2}} |k_{n-1}\rangle \right) \right) \otimes \ldots \otimes \left(\sum_{k_1=0}^{1} e^{2\pi i j \frac{k_1}{2^{n-1}}} |k_1\rangle \right) \otimes \left(\sum_{k_0=0}^{1} e^{2\pi i j \frac{k_0}{2^n}} |k_0\rangle \right) \\
&= \frac{1}{\sqrt{N}} \left(|0\rangle + e^{\frac{2\pi i j}{2}} |1\rangle \right) \otimes \ldots \otimes \left(|0\rangle + e^{\frac{2\pi i j}{2^{n-1}}} |1\rangle \right) \otimes \left(|0\rangle + e^{\frac{2\pi i j}{2^n}} |1\rangle \right)
\end{aligned} \tag{21}$$

where, in the third line, we have expressed the k-th computational basis vectors as a tensor product of single-qubit basis vectors

$$|k\rangle = |k_{n-1}\rangle \otimes \ldots \otimes |k_0\rangle .$$

This lets us express the sum over k (i.e., over all computational basis functions of the 2^n dimensional space) in the second line as individual sums over each constituent qubit (as shown in line 3):

$$\sum_{k=0}^{N-1} \rightarrow \sum_{k_{n-1}=0}^{1} \ldots \sum_{k_0=0}^{1}$$

Now we are ready to show that, if the basis-vector $|j\rangle$ is fed into the input of the quantum circuit shown in Fig. 1 in such a way that the bottommost (topmost) qubit corresponds to the least (most) significant bit, then the transformed state shown in the RHS of Eq. 21 is obtained as the output. This circuit contains the Hadamard gate $\hat{H}$ (see Eq. 11) and the

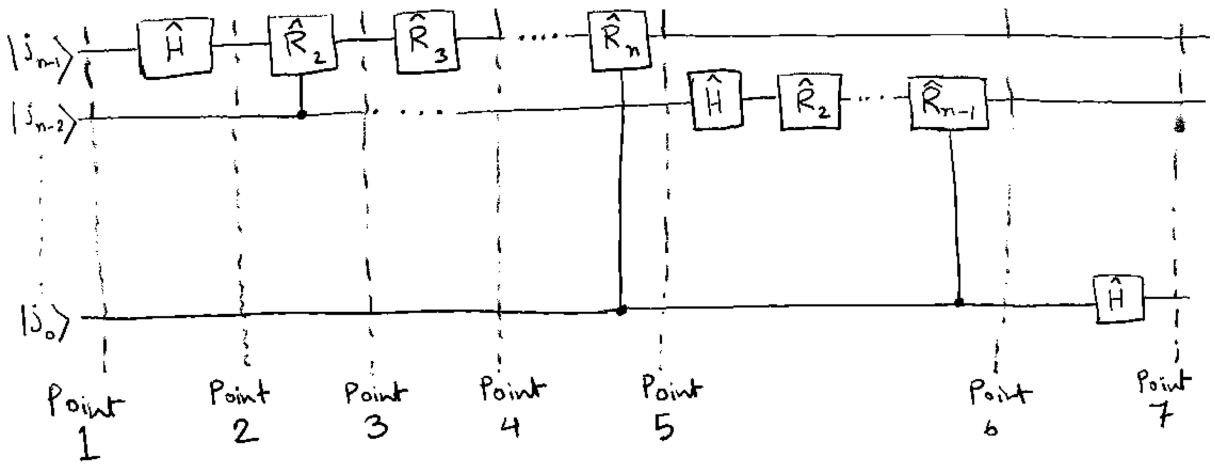

Figure 1: Circuit for performing quantum Fourier transform

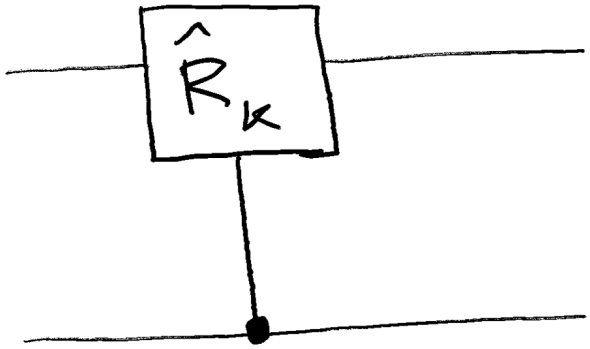

Figure 2: The $\hat{\text{CROT}}_k$ gate

controlled rotation $\hat{\text{CROT}}$ gate which we redefine (in a slightly different way) below. If the control qubit is $|0\rangle$, the $\hat{\text{CROT}}_k$ gate performs, as expected, an identity operation on the target qubit. On the other hand, if the control qubit is $|1\rangle$, then a $\hat{R}_k$ operation is performed on the target qubit $|T\rangle$ such that

$$\hat{R}_k\,|T\rangle = e^{\frac{2\pi i T}{2^k}}\,|T\rangle$$

In our circuit diagram, the two-qubit operation $\hat{\text{CROT}}_k$ is shown by the construction of Fig. 2 where the black dot indicates the operation on the control qubit and the boxed $\hat{R}_k$ indicates the (conditional) rotation operation on the target qubit.

Now let us take a close look at Fig. 1.

1. At the input point (point 1), we have the state

$$|j_{n-1}j_{n-2}\cdots j_1 j_0\rangle\,.$$

Remember that this is the j-th computational basis vector and so the qubits represent the integer j in binary form.

2. Then a Hadamard gate acts on the topmost qubit, leaving the others intact. Consequently, at point 2 we have

$$\left(\hat{H}\left|j_{n-1}\right\rangle\right)\otimes\left|j_{n-2}\ldots j_1j_0\right\rangle=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle+e^{\frac{2\pi ij_{n-1}}{2}}\left|1\right\rangle\right)\otimes\left|j_{n-2}\ldots j_1j_0\right\rangle$$

3. Next a controlled rotation $\hat{\text{CROT}}_2$ is applied on the topmost target qubit with the qubit below it serving as the control qubit. The resulting state at point 3 is

$$\hat{\text{CROT}}_2\left(\left|0\right\rangle\otimes\left|j_{n-2}\right\rangle+e^{\pi ij_{n-1}}\left|1\right\rangle\otimes\left|j_{n-2}\right\rangle\right)\otimes\frac{1}{\sqrt{2}}\left|j_{n-3}\ldots j_0\right\rangle$$

Note from the circuit diagram that, of the two qubits involved in the $\hat{R}_2$ operation, the state $\left|j_{n-2}\right\rangle$ acts as the control qubit. Note that

$$\hat{R}_2\left|0\right\rangle=e^{\frac{2\pi i.0}{2^2}}\left|0\right\rangle=\left|0\right\rangle,$$

and therefore,

$$\hat{\text{CROT}}_2\left(\left|0\right\rangle\otimes\left|j_{n-2}\right\rangle\right)=\left|0\right\rangle\otimes\left|j_{n-2}\right\rangle.$$

What about $\hat{\text{CROT}}_2\left|1\right\rangle\otimes\left|j_{n-2}\right\rangle$? If $\left|j_{n-2}\right\rangle=\left|0\right\rangle$, then obviously the state remains intact:

$$\begin{aligned}\hat{\text{CROT}}_2\left|1\right\rangle\otimes\left|j_{n-2}\right\rangle&=\left|1\right\rangle\otimes\left|j_{n-2}\right\rangle\\&=e^{\frac{2\pi ij_{n-2}}{2^2}}\left|1\right\rangle\otimes\left|j_{n-2}\right\rangle\end{aligned}$$

If $\left|j_{n-2}\right\rangle=\left|1\right\rangle$ then

$$\begin{aligned}\hat{\text{CROT}}_2\left|1\right\rangle\otimes\left|j_{n-2}\right\rangle&=e^{\frac{2\pi i.1}{2^2}}\left|1\right\rangle\otimes\left|j_{n-2}\right\rangle\\&=e^{\frac{2\pi ij_{n-2}}{2^2}}\left|1\right\rangle\otimes\left|j_{n-2}\right\rangle\end{aligned}$$

Then the state at point 3 simplifies to

$$\begin{aligned}&\left(\left|0\right\rangle\otimes\left|j_{n-2}\right\rangle+e^{\pi ij_{n-1}}e^{\frac{2\pi ij_{n-2}}{2^2}}\left|1\right\rangle\otimes\left|j_{n-2}\right\rangle\right)\otimes\frac{1}{\sqrt{2}}\left|j_{n-3}\ldots j_0\right\rangle\\&=\left(\left|0\right\rangle+e^{2\pi i\left(\frac{j_{n-1}}{2^1}+\frac{j_{n-2}}{2^2}\right)}\left|1\right\rangle\right)\otimes\frac{1}{\sqrt{2}}\left|j_{n-2}\ldots j_0\right\rangle\end{aligned}$$

4. In an identical way, it follows that the state at point 4 is

$$\left(\left|0\right\rangle+e^{2\pi i\left(\frac{j_{n-1}}{2^1}+\frac{j_{n-2}}{2^2}+\frac{j_{n-3}}{2^3}\right)}\left|1\right\rangle\right)\otimes\frac{1}{\sqrt{2}}\left|j_{n-2}\ldots j_0\right\rangle$$

5. In this way, the topmost qubits picks up a phase with every controlled rotation upto point 5. At this point the state becomes

$$\begin{aligned}&\left(|0\rangle + e^{2\pi i \sum_{t=0}^{n-1} \frac{j_t}{2^{n-t}}} |1\rangle\right) \otimes \frac{1}{\sqrt{2}} |j_{n-2} \dots j_0\rangle \\ &= \left(|0\rangle + e^{2\pi i \frac{j}{2^n}} |1\rangle\right) \otimes \frac{1}{\sqrt{2}} |j_{n-2} \dots j_0\rangle\end{aligned}$$

where we have used Eq. 20. From now on, the topmost qubit remains unchanged.

6. In a similar manner, beyond point 6, the the next qubit (the one below the topmost qubit) remains unchanged. At this point, the state of the system is

$$\left(|0\rangle + e^{2\pi i \frac{j}{2^n}} |1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i \frac{j}{2^{n-1}}} |1\rangle\right) \otimes \frac{1}{\sqrt{2^2}} |j_{n-2} \dots j_0\rangle$$

7. Finally, at point 7, the state is

$$\frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2\pi i \frac{j}{2^n}} |1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i \frac{j}{2^{n-1}}} |1\rangle\right) \otimes \dots \otimes \left(|0\rangle + e^{\frac{2\pi i j}{2}} |1\rangle\right)$$