Quantum Computation and Extended Church-Turing Thesis

0.1 Extended Church-Turing Thesis

The extended Church-Turing thesis is a foundational principle in computer science. It asserts that any ”reasonable” model of computation can be efficiently simulated on a standard model such as a Turing Machine or a Random Access Machine or a cellular automaton. This thesis forms the foundation of complexity theory — for example ensuring that that the class P (polynomial time) is well defined. But what do we mean by ”reasonable”? In this context, reasonable means ”physically realizable in principle”. One constraint that this places is that the model of computation must be digital. Thus analog computers are not reasonable models of computation, since they assume infinite precision arithmetic. In fact, it can be shown that with suitable infinite precision operations, an analog computer can solve NP-Complete problems in polynomial time. And an infinite precision calculator with operations +, x, =0?, can factor numbers in polynomial time.

We will see that quantum computers are exponentially more powerful than classical computers. But are they a reasonable model of computation. To show this we must show that we can implement (in principle) any quantum circuit on a large number of qubits. There are two issues we must tackle:

1. When we control a spin qubit (as we saw in the last chapter) by a suitable electromagnetic pulse, the spin state changes from spin up to spin down or vice-versa by absorbing/emitting a photon. Surely this entangles the state of the qubit with that of the environment, thus effectively measuring the state of the qubit. This seems to undermine the very feature of quantum systems that gives them exponential computational resources.

2. Are quantum systems digital? At first glance they appear to be analog devices, since a quantum gate is described by a unitary transformation, specified by complex numbers. How robust is the computation to errors in the implementation of each gate? i.e. to what precision must such a transformation be carried out to get the same results.

0.2 Tensor Products

Consider two quantum systems - the first with k distinguishable (classical) states (associated Hilbert space $\mathscr{C}^k$), and the second with l distinguishable states (associated Hilbert space $\mathscr{C}^l$). What is the Hilbert space associated with the composite system? We can answer this question as follows: the number of distinguishable states of the composite system is kl — since for each distinct choice of basis (classical) state $\left|i\right\rangle$ of the first system and basis state $\left|j\right\rangle$ of the second system, we have a distinguishable state of the composite system. Thus the Hilbert space associated with the composite system is $\mathscr{C}^{kl}$.

The tensor product is a general construction that shows how to go from two vector spaces V and W of dimension k and l to a vector space $V \otimes W$ (pronounced “V tensor W”) of dimension kl. Fix bases $|v_1\rangle, \ldots, |v_k\rangle$ and $|w_1\rangle, \ldots, |w_l\rangle$ for V, W respectively. Then a basis for $V \otimes W$ is given by

$$\{|v_i\rangle \otimes |w_j\rangle : 1 \leq i \leq k, 1 \leq j \leq l\},$$

so that $\dim(V \otimes W) = kl$. So a typical element of $V \otimes W$ will be of the form $\sum_{ij} \alpha_{ij}(|v_i\rangle \otimes |w_j\rangle)$. We can define an inner product on $V \otimes W$ by

$$(|v_1\rangle \otimes |w_1\rangle, |v_2\rangle \otimes |w_2\rangle) = (|v_1\rangle, |v_2\rangle) \cdot (|w_1\rangle, |w_2\rangle),$$

which extends uniquely to the whole space $V \otimes W$.

For example, consider $V = \mathscr{C}^2 \otimes \mathscr{C}^2$. V is a Hilbert space of dimension 4, so $V \cong \mathscr{C}^4$. So we can write $|00\rangle$ alternatively as $|0\rangle \otimes |0\rangle$. More generally, for n qubits we have $\mathscr{C}^2 \otimes \cdots$ (n times) $\otimes \cdots \mathscr{C}^2 \cong \mathscr{C}^{2^n}$. A typical element of this space is of the form

$$\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle.$$

A word of caution: Not all elements of $V\otimes W$ can be written as $|v\rangle\otimes|w\rangle$ for $|v\rangle\in V$, $|w\rangle\in W$. As an example, consider the Bell state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$.

0.3 The Significance of Tensor Products

Classically, if we put together a subsystem that stores k bits of information with one that stores l bits of information, the total capacity of the composite system is $k+l$ bits.

From this viewpoint, the situation with quantum systems is extremely paradoxical. We need k complex numbers to describe the state of a k-level quantum system. Now consider a system that consists of a k-level subsystem and an l-level subsystem. To describe the composite system we need kl complex numbers. One might wonder where nature finds the extra storage space when we put these two subsystems together.

An extreme case of this phenomenon occurs when we consider an n qubit quantum system. The Hilbert space associated with this system is the n-fold tensor product of $\mathscr{C}^2 \equiv \mathscr{C}^{2^n}$. Thus nature must "remember" of 2^n complex numbers to keep track of the state of an n qubit system. For modest values of n of a few hundred, 2^n is larger than estimates on the number of elementary particles in the Universe.

This is the fundamental property of quantum systems that is used in quantum information processing.

Finally, note that when we actually a measure an n-qubit quantum state, we see only an n-bit string - so we can recover from the system only n, rather than 2^n, bits of information.

0.4 Tensor product of operators

Suppose $|v\rangle$ and $|w\rangle$ are unentangled states on $\mathscr{C}^m$ and $\mathscr{C}^n$, res pectively. The state of the combined system is $|v\rangle\otimes|w\rangle$ on $\mathscr{C}^{mn}$. If the unitary operator A is applied to the first subsystem, and B to the second subsystem, the combined state becomes $A|v\rangle\otimes B|w\rangle$.

In general, the two subsystems will be entangled with each other, so the combine d state is not a tensor-product state. We can still apply A to the first subs ystem and B to the second subsystem. This gives the operator $A\otimes B$ on the combined system, defined on entangled states by linearly extending its actio n on unentangled states.

(For example, $(A\otimes B)(|0\rangle\otimes|0\rangle) = A|0\rangle\otimes B|0\rangle$. $(A\otimes B)(|1\rangle\otimes|1\rangle) = A|1\rangle\otimes B|1\rangle$. Therefore, we define $(A\otimes B)(\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle)$ to be $\frac{1}{\sqrt{2}}(A\otimes B)|00\rangle+\frac{1}{\sqrt{2}}(A\otimes B)|11\rangle = \frac{1}{\sqrt{2}}\left(A|0\rangle\otimes B|0\rangle + A|1\rangle\otimes B|1\rangle\right)$.)

Let $|e_1\rangle,\dots,|e_m\rangle$ be a basis for the first subsystem, and write $A=\sum_{i,j=1}^m a_{ij}|e_i\rangle\langle e_j|$ (the i,jth element of A is a_{ij}). Let $|f_1\rangle,\dots,|f_n\rangle$ be a basis for the second subsystem , and write $B=\sum_{k,l=1}^n b_{kl}|f_k\rangle\langle f_l|$. Then a basis for t he combined system is $|e_i\rangle\otimes|f_j\rangle$, for $i=1,\dots,m$ and $j=1,\dots,n$. The operator $A\otimes B$ is

$$\begin{aligned} A\otimes B &= \left(\sum_{ij} a_{ij}|e_i\rangle\langle e_j|\right)\otimes\left(\sum_{kl} b_{kl}|f_k\rangle\langle f_l|\right) \\ &= \sum_{ijkl} a_{ij}b_{kl}|e_i\rangle\langle e_j|\otimes|f_k\rangle\langle f_l| \\ &= \sum_{ijkl} a_{ij}b_{kl}(|e_i\rangle\otimes|f_k\rangle)(\langle e_j|\otimes\langle f_l|)\ . \end{aligned}$$

Therefore the $(i,k),(j,l)$th element of $A\otimes B$ is $a_{ij}b_{kl}$. If w e order the basis $|e_i\rangle \otimes |f_j\rangle$ lexicographically, then the matri x for $A\otimes B$ is

$$\begin{pmatrix} a_{11}B & a_{12}B & \cdots \\ a_{21}B & a_{22}B & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \;;$$

in the i,jth subblock, we multiply a_{ij} by the matrix for B.

1 Is Quantum Computation Digital?

There is an issue as to whether or not quantum computing is digital. We need only look at simple gates such as the Hadamard gate or a rotation gate to find real values.

$$H=\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \qquad R_\theta=\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \tag{1}$$

When we implement a gate, how accurate does it need to be? Do we need infinite precision to build this gate properly? A paper by Shamir, “How To Factor On Your Calculator,” shows that if we assume infinite precision arithmetic, then some NP complete problems can be solved in polynomial time. However, we obviously cannot have infinite precision, so we must digitize quantum computation in order to approximate values such as $1/\sqrt{2}$. It turns out that $\log n$ bits of precision are necessary.

Suppose we want to build a gate that rotates the input by θ, but the best accuracy we can actually build is rotation by $\theta \pm \Delta\theta$ (finite precision). Let $U_1,\ldots,U_m$ be a set of ideal gates that implement an exact rotation by θ. Let $V_1,\ldots,V_m$ be a set of actual (constructible) gates that implement rotation by $\theta\pm\Delta\theta$. Let $|\phi\rangle$ be the initial state. Let $|\psi\rangle$ be the ideal output

$$|\psi\rangle = U_1U_2\cdots U_m|\phi\rangle\,, \tag{2}$$

and let $|\psi'\rangle$ be the actual output

$$|\psi'\rangle = V_1V_2\cdots V_m|\phi\rangle\,. \tag{3}$$

The closer $|\psi\rangle$ and $|\psi'\rangle$ are to each other, the better the approximation. If we can approximate each gate to within $\varepsilon = O(1/m)$, then we can approximate the entire circuit with small constant error.

Theorem 0.1: *If $\|U_i - V_i\| \le \frac{\varepsilon}{4m}$ for $1\le i\le m$, then $\||\psi\rangle - |\psi'\rangle\| \le \frac{\varepsilon}{4}$.*

Proof:Consider the two hybrid states

$$\begin{aligned} |\psi_k\rangle &= U_1\cdots U_{k-1}V_k\cdots V_m|\phi\rangle \quad \text{, and} \\ |\psi_{k+1}\rangle &= U_1\cdots U_kV_{k+1}\cdots V_m|\phi\rangle\,. \end{aligned}$$

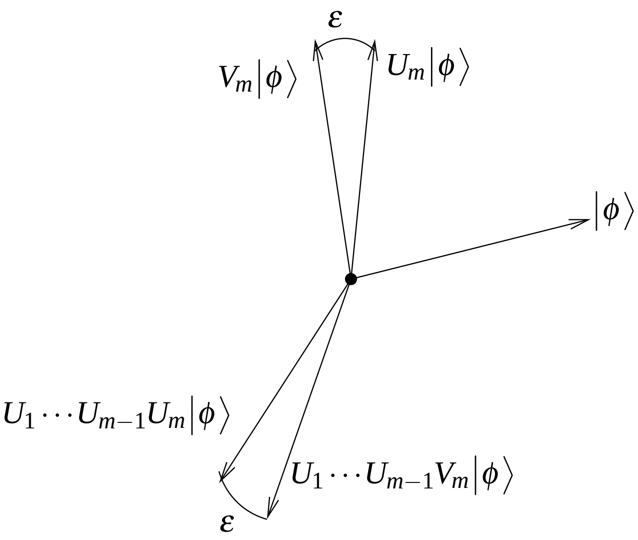
Subtract ϕ_{k+1} from ϕ_k to get

$$|\phi_k\rangle - |\phi_{k+1}\rangle = U_1\cdots U_{k-1}(V_k-U_k)V_{k+1}\cdots V_m|\phi\rangle \tag{4}$$

Since the unitary transformations don’t change the norm of the vector, the only term we need to consider is $U_{k+1}-V_{k+1}$. But we have an upper bound on this, so we can conclude that

$$\||\psi_k\rangle - |\psi_{k+1}\rangle\| \le \frac{\varepsilon}{4m}. \tag{5}$$

Another way to see this is the following picture. Applying unitary transformations to $U_m|\phi\rangle$ and $V_m|\phi\rangle$ preserves the angle between them, which is defined to be the norm.



We use the triangle inequality to finish to proof.

$$\begin{aligned} \| |\psi\rangle - |\psi'\rangle \| &= \| |\psi_0\rangle - |\psi_m\rangle \| \\ &\leq \sum_{i=0}^{m-1} \| |\phi_i\rangle - |\phi_{i+1}\rangle \| \\ &\leq m \cdot \frac{\varepsilon}{4m} \leq \frac{\varepsilon}{4}. \end{aligned}$$