Quantum Computation – Short Notes

Sofia Qvarfort

April 1, 2016

Contents

1 Summary of lectures

Toffoli gate is the CCNOT gate. It is universal for Classical computation.

Classical universal set given by

$$\{H, CNOT\} \tag{1}$$

Quantum universal set is given by

$$\{CNOT, H, R_{\pi/4}\} \tag{2}$$

Solovay-Kitaev's Theorem says that universal sets are equivalent and that a quantum speed-up is robust w.r.t. gate sets.

Proof of the no cloning theorem Pauli, Hadamard, Phase gate and CNOT matrices Deutsch and Deutsch-Josza circuits Grover algorithm circuit Quantum Fourier transform, prove that it's unitary Know how to construct a graph state Compare and constrast different paradigms of computation: gate-based, adiabatic, measurement-based Phase estimation Shor's Algorithm Hidden subgroup problem

2 No-cloning Theorem

Prove this by unitarity or linearity.

3 Quantum Fourier Transform

Definition The QFT is defined as

$$|j\rangle = \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} e^{2\pi ijk/q} |k\rangle \tag{3}$$

It maps $|j\rangle \to |\chi_j\rangle$.

Action What the QFT does is changing the basis of a group. It changes the basis into the irrep basis. That is, given some random basis, we can map the basis onto the computational basis.

Lexographic notation makes it easier to index binary sequences. For a bit

$$|x\rangle = |x_1 x_2 \ldots x_n\rangle \tag{4}$$

We can write

$$x = x_1 2^{n-1} + x_2 2^{n-2} + \ldots + x_n 2^0 \tag{5}$$

Such that for two qubits, we find

$$|00\rangle = |0\rangle \tag{6}$$
$$|01\rangle = |1\rangle \tag{7}$$
$$|10\rangle = |2\rangle \tag{8}$$
$$|11\rangle = |3\rangle \tag{9}$$

Fractional binary notation is an easy way to write sums

$$[0.x_1 \dots x_n] = \sum_{k=1}^{m} \frac{x_k}{2^k} \tag{10}$$

Compact notation of QFT We will here show the derivation of a more compact notation. We know that

$$|j\rangle = \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} e^{2\pi i jk/q} |k\rangle \tag{11}$$

We will work with a two-qubit example. So,

$$\begin{aligned}
\mathcal{F}|x\rangle &= \frac{1}{2}\sum_{k=0}^{3} \omega^{jk} |k\rangle && (12)\\
&= \frac{1}{2}\left(|0\rangle + \omega^{2x_1+x_2}|1\rangle + \omega^{2(2x_1+x_2)}|2\rangle + \omega^{3(2x_1+x_2)}|3\rangle\right) && (13)\\
&= \frac{1}{2}\left(|00\rangle + \omega^{2x_1+x_2}|01\rangle + \omega^{2(2x_1+x_2)}|10\rangle + \omega^{3(2x_1+x_2)}|11\rangle\right) && (14)
\end{aligned}$$

Any $\omega^4 = 1$, which means that we can simplify the above to

$$\begin{aligned}
\mathcal{F}|x\rangle &= \frac{1}{2}\left(|00\rangle + \omega^{2x_1+x_2}|01\rangle + \omega^{2x_2}|10\rangle + \omega^{2x_1+3x_2}|11\rangle\right) && (15)\\
&= \frac{1}{2}\left(|0\rangle + \omega^{2x_2}|1\rangle\right)\left(|0\rangle + \omega^{2x_1+x_2}|1\rangle\right) && (16)\\
&= \frac{1}{2}\left(|0\rangle + e^{2\pi i \frac{x_2}{2}}|1\rangle\right)\left(|0\rangle + e^{2\pi i\left(\frac{x_1}{2}+\frac{x_2}{4}\right)}|1\rangle\right) && (17)\\
&= \frac{1}{2}\left(|0\rangle + e^{2\pi i 0.x_2}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.x_1x_2}|1\rangle\right) && (18)
\end{aligned}$$

This can easily be generalised to more qubits.

4 Pauli, Hadamard, Phase gate and CNOT gate

They are given by

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{19}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{20}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{21}$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{22}$$

5 The Hidden Subgroup Problem

Significance The hidden subgroup problem is important because it is essentially equivalent to Shor's algorithm.

Complexity Some instances of the HS problem belongs in NP. There is no general solution for this problem.

Key idea Lets say that we have a function f that classifies elements in each coset of a subgroup into a certain constant number. Then, given only this function, can we find H such that we find its generators?

Formal statement For a group G and a subgroup $H : |H| < |G|$, we say that a function $f : G \to X$ onto the set X 'hides the group' H if $\forall g_1, g_2 \in G, f(g_1) = f(g_2)$. This is equivalent to $g_1 H = g_2 H$. That is, f is constant within the cosets of H.

The question is:

6 Adiabatic Quantum Computation

Quantum Adiabatic Computation is a class of procedures for solving optimization problems using a quantum computer.

Basic strategy :

- Design a Hamiltonian whose ground state encodes the solutions of an optimisation problem.
- Prepare the known ground state of a simple Hamiltonian.
- Interpolate slowly

Realistic physical Hamiltonians look like

$$H = \sum_{\langle i,j \rangle} H_{ij} \tag{23}$$

where $\langle \cdots \rangle$ denote nearest neighbour.

Construction We can either construct a universal quantum computer that can simulate all Hamiltonians, or we can build a computer specific for the problem.

Adiabatic Theorem Let $H(s)$ be a smoothly varying Hamiltonian for $s \in [0,1]$. Decompose it as

$$H(x) = \sum_{j=0}^{D-1} E_j(x) \left|E_j(x)\right\rangle \left\langle E_j(x)\right| \tag{24}$$

where

$$E_0(s) < E_1(s) \leq E_2(s) \leq \ldots \leq E_{D-1}(s) \tag{25}$$

Let $|\psi_T\rangle = |E_0(0)\rangle$, and thus as $T \to \infty$

$$\left| \langle E_0(1)|\psi_T\rangle \right|^2 \to 1 \tag{26}$$

What this is saying is that measuring the state as $T \to \infty$ makes it increasingly likely to turn out to be the ground state of the new Hamiltonian.

Total run time depends on the gap Δ of the Hamiltonian.

$$\Delta(s) = E_1(s) - E_0(s) \tag{27}$$

A rough estimate suggests,

$$T \gg \frac{\Gamma^2}{\Delta^2} \tag{28}$$

Computing the gap can be done in

$$\geq \frac{1}{Poly(N)} \tag{29}$$

with an efficient quantum algorithm.

Uses
- Unstructured search

- Transverse Ising Model
- Fisher's Problem

Fisher's problem is the problem of interval estimation and hypothesis testing concering the means of two normally distributed populations with unequal variances.

Sources of error
- Unitary control error - the gap may change during the computation, which affects the estimated computation time.
- Error in the final Hamiltonian – we end up in the wrong Hamiltonian (I think)
- Interpolation error – Not sure
- Thermal noise – Probably what it says on the tin...

Open problems include developing fault-tolerance for adiabatic quantum computers, various issues with the gap of the Hamiltonian, working with a constant gap.

7 Graph States

Key idea We wish to come up with a way to easily depict and manipulate cluster states, or states with complicated entanglement connections.

Definition of a graph We write $G = (E, V)$ where G is the graph, E are the edges, and V are the matrices. These are sets.

Interactions We consider some kind of Ising model with interactions between nearest neightbours.

Adjacent vertices When vertices $a, b \in V$ are each the endpoint of an edge, they are adjacent.

Adjacency matrix Γ_G associated with the graph G outlines the connections. If V is the set of all vertices $V = \{a_1, \ldots, a_N\}$ then Γ_G is a symmetric $N \times N$ matrix with elements

$$\Gamma_G = \begin{cases} 1, & \text{if } \{a_i, a_j\} \in E \\ 0 & \text{otherwise} \end{cases} \tag{30}$$

Graph state Every graph $G = (V, E)$ can be associated with a graph state. It is a pure quantum state on a Hilbert space

$$\mathcal{H}_V = (\mathbb{C}^2)^{\otimes V} \tag{31}$$

Each vertex labels a qubit.

Vertex operator To every vertex (qubit) $a \in V$ of the graph $G = (V, E)$ we attach a Hermitian operator

$$K_G^{(a)} = \sigma_x^{(a)} \prod_{b \in N_a} \sigma_z^{(b)} \tag{32}$$

where by N_a we mean the neighbourhood of a – every other vertex directly connected to a. σ_x and σ_z are operators that act on the system.

Using the adjacency matrix, we can express this as

$$K_G^{(a)} = \sigma_x^{(a)} \prod_{b \in V} \left(\sigma_z^{(b)}\right)^{\Gamma_{ab}} \tag{33}$$

That is, when $\Gamma_{ab} = 0$, there is not interaction because the neighbour doesn't exist.

There are $N = |V|$ operators. They all commute. A set of operators $\{K_G^{(a)}\}$ corresponding to all vertices has a common set of eigenvectors. This is the graph state.

Graph state definition given the operators $K_G^{(a)}$, the graph state $|G\rangle$ is defined as

$$K_G^{(a)} |G\rangle = |G\rangle, \forall a \in V \tag{34}$$

Connection to stabilisers The finite Abelian group S is generated by the $K_G^{(a)}$ operators. That is,

$$S = \left\langle \{K_G^{(a)}\}_{a \in V} \right\rangle \tag{35}$$

This is the stabiliser group of the graph state $|G\rangle$.

The empty graph is just the state $|+\rangle^{\otimes n}$.

Initialising graph state The graph state $|G\rangle$ can be obtained by applying a sequence of commuting unitaries acting on two qubits on the empty state. That is,

$$|G\rangle = \prod_{(a,b) \in E} U^{\{a,b\}} |+\rangle^{\otimes V} \tag{36}$$

The unitary $U^{\{a,b\}}$ adds or removes edges! It is a CZ on qubits a and b.

$$U^{\{a,b\}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{37}$$

Entanglement Applying $U^{\{a,b\}}$ onto $|+\rangle |+\rangle$ creates a maximally entangled state.

$$U^{\{a,b\}} |+\rangle |+\rangle = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle - |11\rangle) \tag{38}$$

8 Random Walks

Graph-walk connection We can write down a graph that denotes the degrees of freedom for a particle. That is, if a particle can move one step per time unit, the graph shows us