Quantum algorithms **Monsoon 2007**

Lecture 7

Lecturer: Pranab Sen *Date: August 20*

In the last lecture we saw how to approximate a unitary U on n qubits to within spectral distance ϵ by a product of $(3\pi)^2 4^{2n}\epsilon^{-1}$ unitaries of the form $e^{-i\alpha\vec{P}}$, $\alpha \in \mathbb{R}$ and $\vec{P}$ a generalised Pauli matrix on n qubits. In this lecture, we shall see how to implement $e^{-i\alpha\vec{P}}$ exactly by an $O(n)$-sized circuit consisting of CNOT gates and single qubit gates of the form $e^{-i\beta P}$, $\beta \in \mathbb{R}$ and P a Pauli matrix. After that, we shall see how to approximate $e^{-i\beta P}$ by repeated applications of a basic gate $e^{-i\beta_0 P}$, where β_0 is a fixed irrational multiple of π. Finally, we remark how one can use the *Solovay-Kitaev theorem* for $2^n \times 2^n$ unitaries in order to reduce the overall error incurred in approximating U by circuits composed of gates from our finite universal basis set at the expense of a mild blowup in the circuit size.

1 Implementing $e^{-i\alpha\vec{P}}$ exactly

If $\vec{P} = \mathbb{1}_{2^n}$, then $e^{-i\alpha\vec{P}}$ is just multiplication by the scalar $e^{-i\alpha}$. We can multiply only the first qubit by this scalar, which is a single qubit gate, to achieve the same effect, or we can ignore it because global phases in unitaries have no physical consequence.

Now observe that

$$e^{-i\alpha\vec{P}} = (\cos\alpha)\mathbb{1}_{2^n} - i(\sin\alpha)\vec{P},$$

since $\vec{P}^2 = \mathbb{1}_{2^n}$. So if $\vec{P}$ has $\mathbb{1}_2$ on some qubits, we can pull them out in tensor from the above expression, that is, we do nothing on these qubits and all the action will be on qubits where $\vec{P}$ is non-trivial. For example, if $\vec{P} = X \otimes \mathbb{1}_2$, $e^{-i\alpha\vec{P}} = ((\cos\alpha)\mathbb{1}_2 - i(\sin\alpha)X) \otimes \mathbb{1}_2$. Thus, we can assume that $\vec{P}$ is a tensor product of n non-identity Pauli matrices.

Recall the definitions of the single qubit gates Hadamard and phase:

$$H := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = e^{-i\pi Y/4}\cdot Z = ie^{-i\pi Y/4}e^{-i\pi Z/2}, \quad P := \begin{pmatrix} 1 & \\ & i \end{pmatrix} = e^{i\pi/4}e^{-i\pi Z/4}.$$

Since $HZH = X$ and $(PH)Z(PH)^\dagger = Y$, we can conjugate $e^{-i\alpha\vec{Z}}$, $\vec{Z} := Z^{\otimes n}$ on the qubits where $\vec{P}$ contains X or Y by H or PH respectively, and obtain $e^{-i\alpha\vec{P}}$. For example, if $\vec{P} = Y \otimes Z \otimes X$ and $\vec{Z} = Z \otimes Z \otimes Z$, then $e^{-i\alpha\vec{P}} = ((PH) \otimes \mathbb{1}_2 \otimes H)e^{-i\alpha\vec{Z}}((PH)^\dagger \otimes \mathbb{1}_2 \otimes H)$.

We now show how to implement $e^{-i\alpha\vec{Z}}$ exactly using one ancilla qubit, one $e^{-i\alpha Z}$ gate and $2n$ CNOT gates. It is easy to see that for any computational basis state $|s\rangle$, $s \in \{0,1\}^n$, $e^{-i\alpha\vec{Z}}|s\rangle = e^{-i\alpha(-1)^{|s|}}|s\rangle$, where $|s|$ is defined to be the *Hamming weight* of s i.e. the number of ones in the bit string s. For example, for $\vec{Z} = Z \otimes Z$,

$$e^{-i\alpha\vec{Z}} = \begin{pmatrix} e^{-i\alpha} & & & \\ & e^{i\alpha} & & \\ & & e^{i\alpha} & \\ & & & e^{-i\alpha} \end{pmatrix}$$

Thus, $e^{-i\alpha\vec{Z}}$ just rephases the computational basis states according to whether the Hamming weight is even or odd. Note that, despite its apparent simplicity, $e^{-i\alpha\vec{Z}}$ is still an operation entangled across n qubits. Here is the circuit for $e^{-i\alpha\vec{Z}}$. Note how we seem to act only on the ancilla qubit, but the phase kicks back by the tensor product to the global state. Also observe that we have to uncompute the parity of $|s|$ in the second part of the circuit, in order to return the ancilla qubit to the clean $|0\rangle$ state.

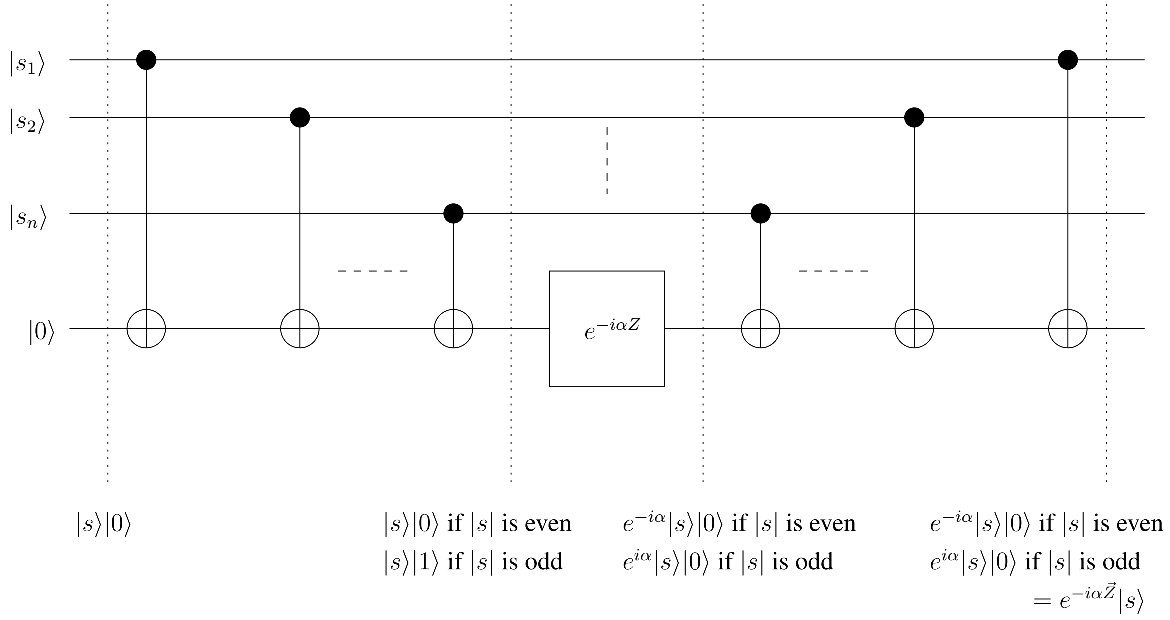
$|s_1\rangle$
$|s_2\rangle$
$|s_n\rangle$
$|0\rangle$
$e^{-i\alpha Z}$
$|s\rangle|0\rangle$
$|s\rangle|0\rangle$ if $|s|$ is even
$|s\rangle|1\rangle$ if $|s|$ is odd
$e^{-i\alpha}|s\rangle|0\rangle$ if $|s|$ is even
$e^{i\alpha}|s\rangle|0\rangle$ if $|s|$ is odd
$e^{-i\alpha}|s\rangle|0\rangle$ if $|s|$ is even
$e^{i\alpha}|s\rangle|0\rangle$ if $|s|$ is odd
$= e^{-i\alpha\vec{Z}}|s\rangle$

Figure 1. Circuit for $e^{-i\alpha\vec{Z}}$

We have thus shown how to implement $e^{-i\alpha\vec{P}}$ exactly using at most $2n$ CNOT gates and $6n+1$ single qubit gates of the form $e^{-i\beta P}$, $\beta \in \mathbb{R}$ and P a non-identity Pauli matrix (at most $6n$ single qubit gates to conjugate Z to Y plus one $e^{-i\alpha Z}$ gate).

2 Using finite basis set of single qubit gates

So far, we have seen how to approximate a unitary U on n qubits to within spectral distance ϵ by a circuit of size at most $(3\pi)^2(8n+1)4^{2n}\epsilon^{-1}$ made up of $CNOT$ and single qubit gates of the form $e^{-i\beta P}$, where $\beta \in \mathbb{R}$ and P is a non-identity Pauli matrix. We now show how we can approximate $e^{-i\beta P}$ by repeated applications of a basic gate $e^{-i\beta_0 P}$, where β_0 is a fixed irrational multiple of π. Thus, CNOT and three single qubit gates $e^{-i\beta_0 P}$, P a non-identity Pauli matrix form a universal set for quantum computation.

Since β_0 is an irrational multiple of 2π, it is easy to see that Euclid's GCD algorithm applied to β_0 and 2π will never terminate. This implies that for all $\delta > 0$, there exists l such that $|\beta_0 l \bmod 2\pi| \leq \delta$. Thus, there exists l' such that $\gamma := |(\alpha - \beta_0 l l') \bmod 2\pi| \leq \delta$, which, using the triangle inequality and submultiplicativity of $\|\cdot\|$, implies for sufficiently small δ that

$$\begin{aligned}
\|e^{-i\alpha P} - e^{-i\beta_0 ll' P}\| &= \|e^{-i\gamma P} - \mathbb{1}_2\| \cdot \|e^{-i\beta_0 ll' P}\| \;=\; \|(1-\cos\gamma)\mathbb{1}_2 - i(\sin\gamma)P\| \\
&\leq |1-\cos\gamma| \cdot \|\mathbb{1}_2\| + |\sin\gamma| \cdot \|P\| \;=\; |1-\cos\gamma| + |\sin\gamma| \\
&\leq 2\gamma \;\leq\; 2\delta.
\end{aligned}$$

In general, in order to get an approximation error of 2δ, we will require $ll' = \Omega(\delta^{-1})$. Taking $\delta := (3\pi)^{-2}(8n+1)^{-1}4^{-2n}\epsilon^2$, we get a circuit of size at most $O(n^2 4^{4n}\epsilon^{-3})$ made up of CNOT and single qubit gates $e^{-i\beta_0 P}$, P non-identity Pauli matrix and β_0 a fixed irrational multiple of π, approximating U to which spectral distance 2ϵ. Once we have shown that CNOT and $e^{-i\beta_0 P}$ generate a dense subset of $2^n \times 2^n$ unitaries, we can appeal to the Solovay-Kitaev theorem to show that it is possible to approximate U to within spectral distance ϵ with circuits of size at most $2^{O(n)} \log^4 \epsilon^{-1}$ made up of the basic gates CNOT and $e^{-i\beta_0 P}$.

We now outline another use of the Solovay-Kitaev theorem. Suppose we have a circuit of size s made up of arbitrary one and two qubit gates. Directly applying our universality proof to replace the one and two qubit gates by circuits made up of CNOT and $e^{-i\beta_0 P}$ gates with an approximation error of at most δ in the spectral distance incurs a size overhead of $O(\delta^{-3})$. Thus, if we want an overall approximation error of at most ϵ, the new circuit will have size $O(s^4/\epsilon^3)$. Instead, by using the Solovay-Kitaev theorem for one and two qubit unitarires, we get a new circuit of size $s \log^4(s/\epsilon)$ made up of CNOT and $e^{-i\beta_0 P}$ gates.