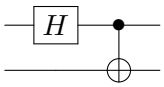
Quantum Circuits and Simulation Solutions

1.



2. Notice that $H^2 = \mathbb{1}$. As a consequence, $e^{-iHt} = \cos(t)\mathbb{1} - i\sin(t)H$. Thus,

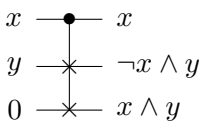
$$e^{-iH\pi/2} = -i \begin{bmatrix} 0 & U \\ U^\dagger & 0 \end{bmatrix}.$$

Thus,

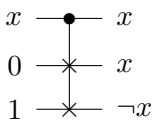
$$e^{-iH\pi/2}|1\rangle|\psi\rangle = -i|0\rangle U|\psi\rangle.$$

The action on the ancilla qubit and the global phase of $-i$ can be ignored. For further reading, see [1, 2].

3. The gate set $\{\text{NOT}, \text{AND}\}$ is universal for classical computation. Thus, we just have to simulate these two gates using Fredkin gates and appropriately initialized ancilla bits. By initializing the control bit to x, and the two target bits to y and 0, one sees that the controlled-swap leaves the bottom bit in the state $x \wedge y$ thus simulating an AND gate.

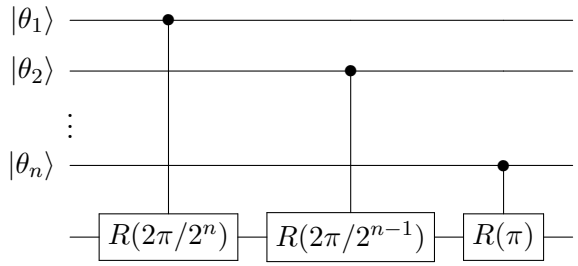


Similarly, by initializing the control bit to x and the two target bits to 0 and 1 one sees that controlled-swap leaves the bottom bit in the state $\neg x$, thus simulating a NOT gate.

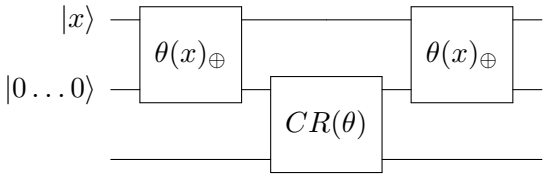


4. (a) Let $\theta_n \dots \theta_1$ be the binary expansion of $\frac{\theta}{2\pi}$ with n bits of precision. Then, we can accomplish our coal with the following type of circuit composed entirely of two-qubit gates, each of which is a controlled-rotation, which rotates the target qubit if the control

qubit is 1, and leaves the target untouched if the control qubit is 0.



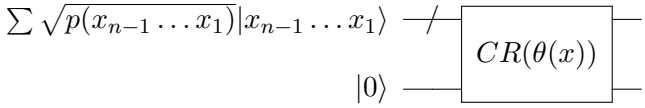
(b) This can be achieved by first computing θ into an ancilla register, then performing the controlled-rotation, then "uncomputing" θ, as follows.



(c) This can be achieved by using the solution to part b by choosing $\theta(x_{n-1}\ldots x_1) = \cos^{-1}\left(\sqrt{p(x_n=0|x_{n-1}\ldots x_1)}\right)$. Then

$$R(\theta(x)) = \begin{bmatrix} \sqrt{p(0|x_{n-1}\ldots x_1)} & -\sqrt{p(1|x_{n-1}\ldots x_1)} \\ \sqrt{p(1|x_{n-1}\ldots x_1)} & \sqrt{p(0|x_{n-1}\ldots x_1)} \end{bmatrix}.$$

Consequently, using the circuit:



the output state from the bottom register will be

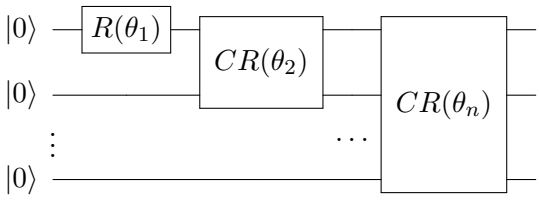
$$\sum_x \sqrt{p(x_{n-1}\ldots x_1)}\sqrt{p(x_n|x_{n-1}\ldots x_1)}|x\rangle = \sum_x \sqrt{p(x_n\ldots x_1)}|x\rangle,$$

as desired.

(d)

$$p(x_n\ldots x_1) = p(x_n|x_{n-1}\ldots x_1)p(x_{n-1}|x_{n-2}\ldots x_1)\ldots p(x_2|x_1)p(x_1).$$

Thus, we can achieve our state preparation task using the following circuit.



where

$$\begin{aligned}
\theta_1 &= \cos^{-1}\left(\sqrt{p(x_1=0)}\right) \\
\theta_2(x_1) &= \cos^{-1}\left(\sqrt{p(x_2=0|x_1)}\right) \\
\theta_3(x_2,x_1) &= \cos^{-1}\left(\sqrt{p(x_3=0|x_2x_1)}\right) \\
&\vdots \\
\theta_n(x_{n-1},\ldots,x_1) &= \cos^{-1}\left(\sqrt{p(x_n=0|x_{n-1}\ldots x_1)}\right).
\end{aligned}$$

This method of state preparation has been independently rediscovered a few times. As far as I am aware, the publication in which this first appeared is [3]. In [4] it is pointed out that the conditional distributions $p(x_j|x_{j-1}\ldots x_1)$ can all be approximated by efficient classical algorithms provided p is a log-concave probability distribution.

5. (a) Each query provides $\log_2 n$ bits of information about a. Thus, classically, one needs at least $n/\log_2 n$ queries to recover all n bits of the secret string a. (It is interesting to think about why such arguments do not apply to quantum queries!) We can show that $2n$ queries suffice to classically solve gues-my-bitstring by exhibiting an explicit algorithm. The following is one example of such an algorithm (not unique). First, query $0\ldots00$ and $0\ldots01$. One will have lower Hamming distance from a than the other, and this is the one that has the correct value a_n of the last bit. Next, query $0\ldots0a_n$ and $0\ldots1a_n$. Again, the string with lower Hamming distance to a has the correct value a_{n-1} of the second-to-last bit. Continuing in this manner, one determines the full string $a_1a_2\ldots a_n$ after $2n$ queries.

   (b) First consider the case $y=a$. Then $|a-x|=|x-y|\equiv f(x)$ for all x. Hence

$$\begin{aligned}
\sum_{x\in\{0,1\}^n}(-i)^{|a-x|}(i)^{|x-y|} &= \sum_{x\in\{0,1\}^n}(-i)^{f(x)}(i)^{f(x)} \\
&= 2^n.
\end{aligned}$$

Next, consider the case $y\neq a$. Let m be the index of a bit on which y and a differ. Let $x',y',a'\in\{0,1\}^{n-1}$ be the strings of the remaining $n-1$ bits of x,y, and a. (That is, $y=y_1y_2\ldots y_n$, $a=a_1a_2\ldots a_n$, $y_m\neq a_m$, $y'=y_1\ldots y_{m-1}y_{m+1}\ldots y_n$, etc.) Then:

$$\begin{aligned}
\sum_{x\in\{0,1\}^n}(-i)^{|a-x|}(i)^{|x-y|} &= \sum_{x'\in\{0,1\}^{n-1}}(-i)^{|a'-x'|}(i)^{|x'-y'|}\sum_{x_m\in\{0,1\}}(-i)^{|a_m-x_m|}(i)^{|x_m-y_m|} \\
&= \sum_{x'\in\{0,1\}^{n-1}}(-i)^{|a'-x'|}(i)^{|x'-y'|}\,(-i+i) \\
&= 0.
\end{aligned}$$

   (c) Initially one has the state $|0\rangle^{\otimes n}$. After applying the Hadamard gates one has the state

$$\left[\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\right]^{\otimes n}=\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$$

After applying the oracle one has the state

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-i)^{|x-a|} |x\rangle.$$

After applying the M gates one has the state

$$\frac{1}{2^n} \sum_{x,y \in \{0,1\}^n} (-i)^{|x-a|} (i)^{|x-y|} |y\rangle.$$

By the result of part b, the amplitude for $y = a$ is one and the amplitude for all other bitstrings y is zero. For further reading see [5, 6].

References

[1] Stephen P. Jordan and Pawel Wocjan. Efficient quantum circuits for arbitrary sparse unitaries. *Physical Review A*, 80:062301, 2009. arXiv:0904.2211.

[2] Dominic W. Berry and Andrew M. Childs. Black-box Hamiltonian simulation and unitary implementation. *Quantum Information and Computation*, 12:29, 2012. arXiv:0910.4157.

[3] Christof Zalka. Efficient simulation of quantum systems by quantum computers. *Proceedings of the Royal Society of London*, A454:313–322, 1998. arXiv:quant-ph/9603026.

[4] Lov Grover and Terry Rudolph. Creating superpositions that correspond to efficiently integrable probability distributions. *arXiv:quant-ph/0208112*, 2002.

[5] Tad Hogg. Highly structured searches with quantum computers. *Physical Review Letters*, 80(11):2473–2476, 1998.

[6] Markus Hunziker and David A. Meyer. Quantum algorithms for highly structured search problems. *Quantum Information Processing*, 1(3):145–154, 2002. `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.95.2249`.