EXERCISES 2

INTRO TO QUANTUM COMPUTING
MAY 2019
TOKYO TECH

NAME

INSTRUCTIONS: Please ask any questions about the exercises in class. The point values indicate the relative difficulty of the problem.

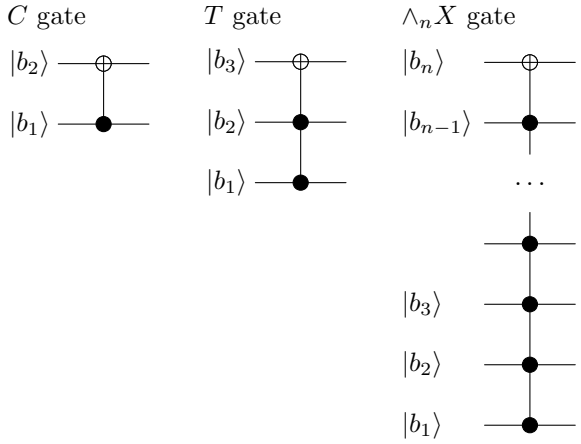
QUOTE: In Nature there are neither rewards nor punishments, there are consequences. ***R.G. Ingersoll***

1 (20 points)

Recall the definitions of the CNOT and Toffoli gates, $C = \wedge X$, and $T = \wedge_2 X$, respectively as $T|b_1b_2b_3\rangle = |b_1b_2(b_3 \oplus (b_1 \wedge b_2))\rangle$ and $C|b_1b_2\rangle = |b_1(b_2 \oplus b_1)\rangle$. Bits b_1 (in the case of C) and b_2 (in the case of T) are usually called the *control bits*.

Recall the definition of the general n-NOT gate $\wedge_n X$ on the $n+1$ qubits as $\wedge_n|b_1 \dots b_n b_{n+1}\rangle = |b_1 \dots b_n(b_{n+1} \oplus (b_1 \wedge \dots \wedge b_n))\rangle$. In other words $\wedge_n X$ 'flips' bit b_{n+1} exclusively when all the bits $b_1, \dots, b_n$ are 1. By analogy with the T and C gates, bits $b_1, \dots, b_n$ are called control bits.

The gates are depicted graphically below. Note that the filled circles represent the control bits while the empty ones represent the bit that is flipped.

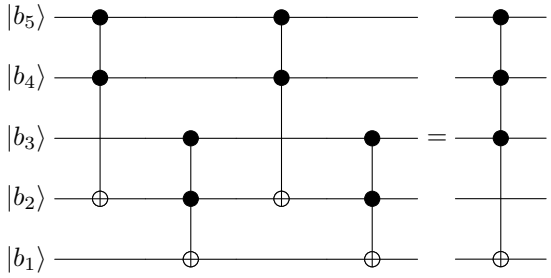


Show (10 points) that the C gate is linear, that is $C|x \oplus y\rangle = C|x\rangle \oplus C|y\rangle$ where $x \oplus y$ is the bitwise $\oplus$. Suppose U is a quantum circuit on n wires composed exclusively of C gates. Conclude that $U|x \oplus y\rangle = U|x\rangle \oplus U|y\rangle$ (i.e. U is linear). Note that a correct mathematical proof of this would involve *induction* on the number of C gates composing U but I will accept an intuitive explanation.

Show (10 points) that T is *not* a linear gate by finding 3-qbit x and y such that $T|x \oplus y\rangle \neq T|x\rangle \oplus T|y\rangle$. Deduce that the T gate cannot be synthesized using exclusively C gates *even with additional temporary storage qubits added*. Bonus (5 points): show that C and X gates are not enough either.

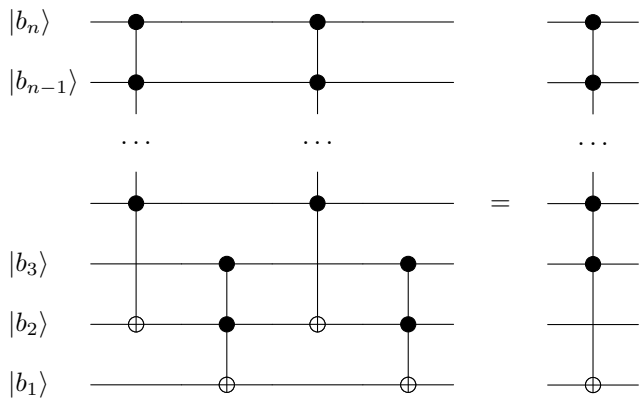
2 (10 points)

Show the following quantum circuit equivalence. Note, in particular, that b_2 is not changed by this circuit and is simply a temporary storage bit. This means that $\wedge_3 X$ can be synthesized using only T gates.



3 20 points

Show the following quantum circuit equivalence. This means that $\wedge_n X$ can be synthesized using only T gates and *one temporary storage qbit*.

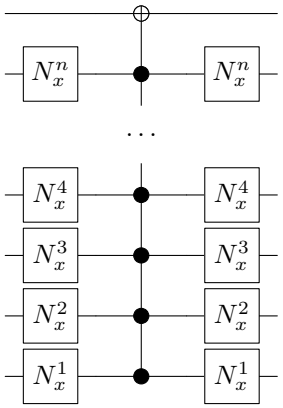


4 10 points

Let $|x\rangle$ be an n-qubit string. Define a single qubit gate N_x^k by

$$N_x^k = \begin{cases} X, & \text{if } x_k = 0 \\ \text{Id}, & \text{otherwise} \end{cases}$$

Here Id is the identity operator, X is the `NOT` gate, and x_k is the k-th bit of $|x\rangle$. Show that the quantum circuit below 'flips' bit b_{n+1} if and only if $|b_1 \dots b_n\rangle = |x\rangle$.



5 20 points

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a boolean map. Use problems 3 and 4 to synthesize a quantum circuit implementing U_f with at most one temporary storage qubit (recall that $U_f|xb\rangle = |x(f(x) \oplus b)\rangle$). Bonus (20 points). Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a one to one map. Modify the construction above to synthesize a quantum circuit implementing U such that $U|x\rangle = |f(x)\rangle$ using at most two temporary qbits. Hint: think of f as a permutation on $\{0, 1, \dots, 2^{n-1}\}$ and represent f as a product of disjoint cycles. Use controlled N_x^k gates to change $|x\rangle$ to $|y\rangle$ where $f(x) = y$.

6 20 points

Bonus. Carefully read paper [1] and explain how the results of that paper imply that $\wedge_n X$ cannot be synthesized with X, C, and T gates without using any temporary storage bits if $n > 2$. Additionally, explain how the results of that paper show that at most *one* temporary qubit is enough to solve problem 5 (none if f has an additional property; which one?).

7 10 points

Bonus. Carefully reread paper [1] and explain why one would still want to use temporary storage bits for most practical problems.

8 15 points

Given a quantum state $|x\rangle = C \sum_{m=0}^{2^n-1} e^{-m2^{k-n+1}\pi i}|m\rangle$, a) determine C (3 points); b) devise a quantum algorithm to determine k (7 points); c) (5 points) devise a procedure to create $|x\rangle$. Hint: you are allowed to use QFT and inverse QFT for this problem.

Additional study.

While quantum algorithms and quantum computing in general is a relatively young area, there is already a great amount of research literature to navigate. This short write-up is a merely an overview of classical introductory papers that go beyond the material presented in class.

Kitayev's paper [4] presents a concise introduction to finite dimensional quantum states and quantum computation. It reviews the concepts of reversible computation necessary for quantum computing, as well. It is also a great introduction to Shor's algorithm (more precisely the quantum portion of it, *the hidden subgroup problem*).

Reversible computation is an important part of quantum algorithm design. Paper [2] is a classic introduction to reversible logic synthesis, both classic and quantum. It is complemented by paper [1] which answers a number of natural questions about reversible logic synthesis. Book [a] by K. Morita is a comprehensive treatment of the theory of reversible computing for various computation models.

Papers [5]–[8] are not directly related to quantum computation but they provide an important relationship between information processing and its physical manifestations. In particular, paper [7] shows that while such connections exists they are more subtle than it might seem at first.

Finally, the matter of quantum entanglement and its exprerimental verification in the form of Bell's inequalities is addressed in [9]. It is worth a careful reading by anyone who wants to understand the nature of entanglement and its physical effects.

References.

[1] Vivek V. Shende et al, *Synthesis of Reversible Logic Circuits*, `http://arxiv.org/abs/quant-ph/0207001v4`

[2] Adriano Barenco et al, *Elementary gates for quantum computation*, `http://arXiv.org/abs/quant-ph/9503016v1`

[3] Patrick J. Coles et al, *Quantum Algorithm Implementations for Beginners*, `http://arxiv.org/abs/1804.03719`

[4] A. Kitaev, *Quantum measurements and the Abelian Stabilizer Problem*, `http://arXiv.org/abs/quant-ph/9511026v1`

[5] R. Landauer, *Irreversibility and Heat Generation in the Computational Process*, IBM Journal of Research and Development, **5**, 3(1961), pp. 183–191

[6] Charles H. Bennett, *Notes on Landauer's principle, reversible computation, and Maxwells Demon*, Studies in History and Philosophy of Modern Physics, 34(2003) pp. 501–510

[7] O. J. E. Maroney, The (absence of a) relationship between thermodynamic and logical reversibility, `http://arXiv.org/abs/physics/0406137v1`

[8] David H. Wolpert, *Extending Landauers Bound from Bit Erasure to Arbitrary Computation*, `https://arxiv.org/pdf/1508.05319v4.pdf`

[9] Alain Aspect, Bell's Theorem: The Naive View of an Experimentalist, `https://arxiv.org/abs/quant-ph/0402001`

[a] Kenichi Morita, *Theory of Reversible Computing*, Monographs in Theoretical Computer Science, an EATCS Series, Springer, **2017**