Exercises in Quantum Computation IV

Wim van Dam
Department of Computer Science, University of California at Santa Barbara, Santa Barbara, CA 93106-5110, USA

Question 1. (Generalized Phase Flip Trick) Define the following superposition $|\varphi_4\rangle$ over the basis states $\mathbb{Z}_4$:

$$|\varphi_4\rangle := \frac{1}{2}(|0\rangle - \mathrm{i}\,|1\rangle - |2\rangle + \mathrm{i}\,|3\rangle).$$

(a) What is the effect of the operation $A_4 : |x\rangle \mapsto |x+1 \bmod 4\rangle$ (for all $x \in \mathbb{Z}_4$) on $|\varphi_4\rangle$?
(b) Let $A^t = A \cdot A \cdots A$ be the t-fold application of A. What is the effect of A^t on $|\varphi_4\rangle$?
(c) For arbitrary $\mathbb{Z}_n$ define the state

$$|\varphi_n\rangle := \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} \mathrm{e}^{-2\pi \mathrm{i} j/n}\,|j\rangle$$

and the operation $A_n : |x\rangle \mapsto |x+1 \bmod n\rangle$ for all $x \in \mathbb{Z}_n$. What is the effect of A_n^t on $|\varphi_n\rangle$?

Question 2. (Fourier-Squared)
(a) Read Handout 4 on the quantum Fourier transformation and Sections 5–5.1 in Nielsen and Chuang's *Quantum Computation and Quantum Information.*
(b) Fix $N \in \mathbb{Z}^+$, what is $\mathrm{Four}_N \cdot \mathrm{Four}_N\,|x\rangle$ for general $x \in \mathbb{Z}_N$?

Question 3. (Factoring 35) Consider the composite number $N = 35$ and the part of the quantum factoring algorithm that is described on Slide 10 of `week6Thurs.pdf`.
(a) Analyze which $x \in \mathbb{Z}_{35}$ are co-prime with 35.
(b) For those x with $\gcd(35,x) = 1$, determine the orders of x mod 35.
(c) Using these orders, determine which $x \in \mathbb{Z}_{35}$ give a non-trivial factor of 35.