Answers to Exercises in Quantum Computation IV

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

Answer 1. (Generalized Phase Flip Trick)
(a) We have $A_4 : |\varphi_4\rangle \mapsto \mathrm{i}\,|\varphi_4\rangle$ as is shown by

$$\begin{aligned} A_4(|\varphi_4\rangle) &= A_4(\tfrac{1}{2}(|0\rangle - \mathrm{i}\,|1\rangle - |2\rangle + \mathrm{i}\,|3\rangle)) \\ &= \tfrac{1}{2}(|1\rangle - \mathrm{i}\,|2\rangle - |3\rangle + \mathrm{i}\,|0\rangle) \\ &= \mathrm{i}\cdot\tfrac{1}{2}(|0\rangle - \mathrm{i}\,|1\rangle - |2\rangle + \mathrm{i}\,|3\rangle). \end{aligned}$$

(b) By applying A_4 t times we get $A_4^t : |\varphi_4\rangle \mapsto (\mathrm{i})^t\,|\varphi_4\rangle$.
(c) It is easy to see that

$$\begin{aligned} A_n(|\varphi_n\rangle) &= \frac{1}{\sqrt{n}}\sum_{j\in\mathbb{Z}_n} \mathrm{e}^{-2\pi\mathrm{i}j/n} A_n(|j\rangle) \\ &= \frac{1}{\sqrt{n}}\sum_{j\in\mathbb{Z}_n} \mathrm{e}^{-2\pi\mathrm{i}j/n}\,|j+1\rangle \\ &= \frac{1}{\sqrt{n}}\sum_{j\in\mathbb{Z}_n} \mathrm{e}^{-2\pi\mathrm{i}(j-1)/n}\,|j\rangle \\ &= \mathrm{e}^{2\pi\mathrm{i}/n}\,|\varphi_n\rangle. \end{aligned}$$

Hence, by repetition, $A_n^t : |\varphi_n\rangle \mapsto \mathrm{e}^{2\pi\mathrm{i}t/n}\,|\varphi_n\rangle$.

Answer 2. (Fourier Squared)
(a) $\mathrm{Four}_N \cdot \mathrm{Four}_N : |x\rangle \mapsto |-x\rangle$, as is shown by

$$\begin{aligned} \mathrm{Four}_N\cdot\mathrm{Four}_N(|x\rangle) &\mapsto \mathrm{Four}_N\left(\frac{1}{\sqrt{N}}\sum_{y\in\mathbb{Z}_N}\zeta_N^{xy}\,|y\rangle\right) \\ &\mapsto \frac{1}{N}\sum_{y,z\in\mathbb{Z}_N}\zeta_N^{xy}\zeta_N^{yz}\,|z\rangle \\ &= \frac{1}{N}\sum_{z\in\mathbb{Z}_N}\left(\sum_{y\in\mathbb{Z}_N}\zeta_N^{y(x+z)}\right)|z\rangle \\ &= |-x\rangle, \end{aligned}$$

for all $x\in\mathbb{Z}_N$ with $\zeta_N := \exp(2\pi\mathrm{i}/N)$, where we used $\sum_y \zeta_N^{y(x+z)} = 0$ if $x+z\neq 0 \bmod N$ and $\sum_y \zeta_N^{y(x+z)} = N$ if $x+z = 0 \bmod N$.

Answer 3. (Factoring 35)
(a) The numbers $x\in\{0,\dots,34\}$ that are co-prime with respect to 35 are all but those that are divisible by 5 or 7, which is the set {1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34}.
(b) For the 24 values $x\in\mathbb{Z}_{35}$ that are co-prime with respect to 35, the orders r are listed in the table below (where order(x) is the smallest positive integer such that $x^r = 1 \bmod 35$).
(c) Of the 21 orders r that are even, the table below lists the values $x^{r/2} \bmod 35$. To find potential non-trivial factors of 35, we calculate for the 21 relevant values x (with even orders r), the greatest common divisors $\mathrm{gcd}_- := \gcd(x^{r/2}-1, 35)$ and $\mathrm{gcd}_+ := \gcd(x^{r/2}+1, 35)$. It turns out that 18 of the gcd cases give the non-trivial factors of 35 (namely 5 and 7). Hence, in total, 18 of the 35 values $x\in\mathbb{Z}_{35}$ (which is $18/35\times 100 \approx 51\%$) are successful in the sense that x is co-prime with 35, the order $r = \mathrm{order}(x)$ is even, and the values $\gcd(x^{r/2}+1, 35)$ and $\gcd(x^{r/2}-1, 35)$ give non-trivial factors of 35.

co-primes x	$r = \mathrm{order}(x)$	$x^{r/2}$	gcd_-	gcd_+	success
1	1	.			
2	12	29	7	5	√
3	12	29	7	5	√
4	6	29	7	5	√
6	2	6	5	7	√
8	4	29	7	5	√
9	6	29	7	5	√
11	3	.			
12	12	29	7	5	√
13	4	29	7	5	√
16	3	.			
17	12	29	7	5	√
18	12	29	7	5	√
19	6	34	1	35	
22	4	29	7	5	√
23	12	29	7	5	√
24	6	34	1	35	
26	6	6	5	7	√
27	4	29	7	5	√
29	2	29	7	5	√
31	6	6	5	7	√
32	12	29	7	5	√
33	12	29	7	5	√
34	2	34	1	35	