Solutions to Exercise Set 5

Solution 5.1 We easily see that

$$U_f\left(|x\rangle \otimes \sum_y \omega_N^y |y\rangle\right) = \sum_y \omega_N^y |x\rangle|y+f(x)\rangle = \sum_y \omega_N^{y-f(x)} |x\rangle|y\rangle = \omega^{-f(x)}\left(|x\rangle \otimes \sum_y \omega_N^y |y\rangle\right),$$

where the second equality is obtained by a simple variable transformation: $y \leftarrow y+f(x)$. Thus, the claimed vector is indeed an eigenvector, and the corresponding eigenvalue is $\omega^{-f(x)}$. This obviously generalizes the phase kickback.

Solution 5.2 Applying F to both wires maps $|0\rangle \otimes |1\rangle$ to

$$\frac{1}{\sqrt{N}} \sum_x |x\rangle \otimes \frac{1}{\sqrt{N}} \sum_y \omega_N^y |y\rangle$$

where x and y both range over all elements in $\mathbb{Z}/N\mathbb{Z}$. Applying U_f maps this to

$$\frac{1}{\sqrt{N}} \sum_x \omega_N^{-f(x)} |x\rangle \otimes \frac{1}{\sqrt{N}} \sum_y \omega_N^y |y\rangle$$

by the observation from Exercise 5.1 above. We can now ignore the second part of the state. Applying F to the first yields

$$\frac{1}{N} \sum_{k,x} \omega_N^{-f(x)} \omega_N^{k\cdot x} |k\rangle = \frac{1}{N} \sum_k \left(\sum_x \omega_N^{kx-f(x)} \right) |k\rangle$$

and so the probability that the measurement outcome is $k=0$ is $p_0 = \left| \sum_x \omega^{-f(x)}/N \right|^2$, which is 1 if f is constant, and 0 if f is surjective. The latter follows from the fact that if f is surjective then it is bijective, and then $\sum_x \omega_N^{f(x)} = \sum_x \omega_N^x = \hat{1}_N(1)\sqrt{N} = 0$.

Solution 5.3 As for the claim of Γ being a group, we argue that $\Gamma = \{\omega_n^j \,|\, 0 \le j < n\}$, where n is the exponent of G, i.e., the smallest positive integer such that $g^n = 1$ for all $g \in G$. Indeed, $\subseteq$ follows from the fact that $\chi(g)^n = \chi(g^n) = \chi(1) = 1$ for all $g \in G$ and $\chi \in \hat{G}$, and $\supseteq$ follows from the observation that we can define a character for a subgoup of order n that maps surjectively into $\{\omega_n^j \,|\, 0 \le j < n\}$, and extend it to a character in $\hat{G}$ by means of Lemma 4.5.

As for the actual question, applying $F_G^\dagger \otimes F_\Gamma^\dagger$ maps $|1_G\rangle \otimes |id_\Gamma\rangle$ to

$$\frac{1}{\sqrt{|G|}} \sum_g |g\rangle \otimes \frac{1}{\sqrt{|\Gamma|}} \sum_\gamma \bar{\gamma} |\gamma\rangle = \frac{1}{\sqrt{|G||\Gamma|}} \sum_{g,\gamma} \bar{\gamma} |g\rangle|\gamma\rangle$$

where g and γ respectively range over $g \in G$ and $\gamma \in \Gamma$. Applying U_f maps this to

$$\begin{aligned} \frac{1}{\sqrt{|G||\Gamma|}} \sum_{g,\gamma} \bar{\gamma}\, |g\rangle|\gamma \cdot f(g)\rangle &= \frac{1}{\sqrt{|G||\Gamma|}} \sum_{g,\gamma} \bar{\gamma} f(g)\, |g\rangle|\gamma\rangle \\ &= \frac{1}{\sqrt{|G|}} \sum_g f(g)|g\rangle \otimes \frac{1}{\sqrt{|\Gamma|}} \sum_\gamma \bar{\gamma}|\gamma\rangle\,, \end{aligned}$$

where the first equality is by substituting the summation variable $\gamma \in \Gamma$ by $\gamma f(g)^{-1}$. We can now ignore the second part of the state. Applying F_G gives

$$\frac{1}{|G|} \sum_{g,\chi} f(g)\chi(g)|\chi\rangle = \frac{1}{|G|} \sum_\chi \sum_g (f\chi)(g)|\chi\rangle = |\bar{f}\rangle\,.$$

Thus, the measurement recovers $\bar{f}$, and hence f, with certainty.

Solution 5.4 The first controlled U maps the state $H|0\rangle \otimes |\varphi\rangle$ of the last two wires to

$$\frac{1}{\sqrt{2}}\big(|0\rangle\otimes|\varphi\rangle + |1\rangle\otimes U|\varphi\rangle\big) = \frac{1}{\sqrt{2}}\big(|0\rangle|\varphi\rangle + e^{2\pi i\mu}|1\rangle|\varphi\rangle\big) = \frac{1}{\sqrt{2}}\big(|0\rangle + e^{2\pi i\mu}|1\rangle\big)\otimes|\varphi\rangle\,.$$

Similarly, the second controlled (power of) U maps the state of the third-to and last wires to

$$\frac{1}{\sqrt{2}}\big(|0\rangle\otimes|\varphi\rangle + |1\rangle\otimes U^2|\varphi\rangle\big) = \frac{1}{\sqrt{2}}\big(|0\rangle + e^{2\pi i\cdot 2\mu}|1\rangle\big)\otimes|\varphi\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + e^{2\pi i[0.m_2\cdots m_n]}|1\rangle\big)\otimes|\varphi\rangle\,,$$

etc. Thus, the state before $F_n^\dagger$ is applied is given by

$$\frac{1}{\sqrt{2^n}}\big(|0\rangle + e^{2\pi i[0.m_n]}|1\rangle\big)\otimes\cdots\otimes\big(|0\rangle + e^{2\pi i[0.m_2\cdots m_n]}|1\rangle\big)\otimes\big(|0\rangle + e^{2\pi i[0.m_1\cdots m_n]}|1\rangle\big)\otimes|\varphi\rangle$$

which equals $F_n|m_1\rangle\cdots|m_n\rangle\otimes|\varphi\rangle$, and so applying $F_n^\dagger$ and measuring the resulting qubits means that $m_1,\ldots,m_n$ is observed with certainty. Thus, (the binary representation of) μ is recovered.

This procedure is referred to as **phase estimation**. If μ does not have a binary representation of length (at most) n then the procedure still works, but then μ is obtained only up to a certain precision and with a certain probability.