5 The quantum Fourier transform and its applications

Exercises: 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10, 5.11, 5.12, 5.13, 5.14, 5.15, 5.16, 5.17, 5.18, 5.19, 5.20, 5.21, 5.22, 5.23, 5.24, 5.25, 5.26, 5.27, 5.28, 5.29.

5.1

The transformation is unitary if and only if the resulting states $|j\rangle$ are such that $\langle j'|j\rangle = \delta_{jj'}$.

$$\begin{aligned}\langle j'|j\rangle &= \left(\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{-2\pi i j'k/N}\,\langle k|\right)\left(\frac{1}{\sqrt{N}}\sum_{l=0}^{N-1} e^{2\pi i jl/N}\,|l\rangle\right)\\ &= \frac{1}{N}\sum_{k=0}^{N-1}\sum_{l=0}^{N-1} e^{2\pi i(jl-j'k)/N}\,\langle k|l\rangle\\ &= \frac{1}{N}\sum_{k=0}^{N-1} e^{2\pi ik(j-j')/N} = \delta_{jj'}.\end{aligned}$$

5.2

$$\begin{aligned}|00\cdots0\rangle \longrightarrow \frac{1}{2^{n/2}}\sum_{k=0}^{2^n-1} e^{2\pi i(k\times0)/2^n}\,|k\rangle\\ = \frac{1}{2^{n/2}}\sum_{k=0}^{2^n-1}|k\rangle\,,\end{aligned}$$

where k inside the *ket* should be written in its binary representation.

5.3

In order to calculate one y_k we need to execute 2^n sum operations, and since there are 2^n different y_k, roughly $2^n \times 2^n = \Theta(2^{2n})$ arithmetic operations are necessary in order to perform the Fourier transform on a classical computer.

The quantum Fourier transform could be calculated more efficiently using the binary fractions, represented by the coefficients $0.j_l j_{l+1}\cdots j_m$. According to Equation (5.4), we need the coefficients from $0.j_n$ up to $0.j_1 j_2 \cdot j_n$. We can calculate them through the iteration

$$\begin{aligned}0.j_n &= \frac{j_n}{2},\\ 0.j_{n-1}j_n &= \frac{j_{n-1}}{2} + \frac{0.j_n}{2},\\ &\vdots\\ 0.j_1 j_2\cdots j_n &= \frac{j_1}{2} + \frac{0.j_2\cdots j_n}{2}.\end{aligned}$$

There are n coefficients and $n-1$ steps, at each step we divide by 2 and add a term, meaning there are two arithmetic operations per step, so we need roughly $2(n-1)$ operations to calculate one of the 2^n different $|j_1,\cdots,j_n\rangle$, resulting in $2(n-1)\times 2^n$ operations, that is, $\Theta(n2^n)$.

5.4

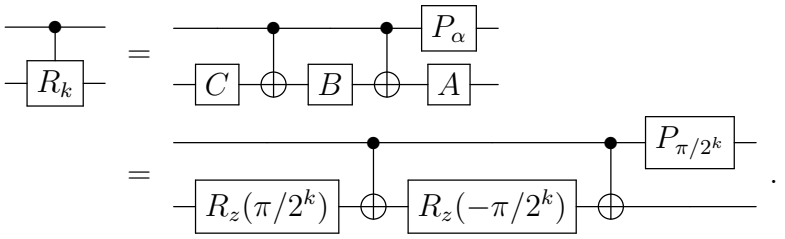
We must find A, B, C and α such that $R_k = e^{i\alpha}AXBXC$ and $ABC = I$ (see Exercise **??**).

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix} = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)}\sin\frac{\gamma}{2} \\ e^{i(\alpha+\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)}\cos\frac{\gamma}{2} \end{bmatrix}$$
$$\implies \alpha = \frac{\pi}{2^k}, \beta = 0, \gamma = 0, \delta = \frac{\pi}{2^{k-1}}.$$

Therefore the operators are given by

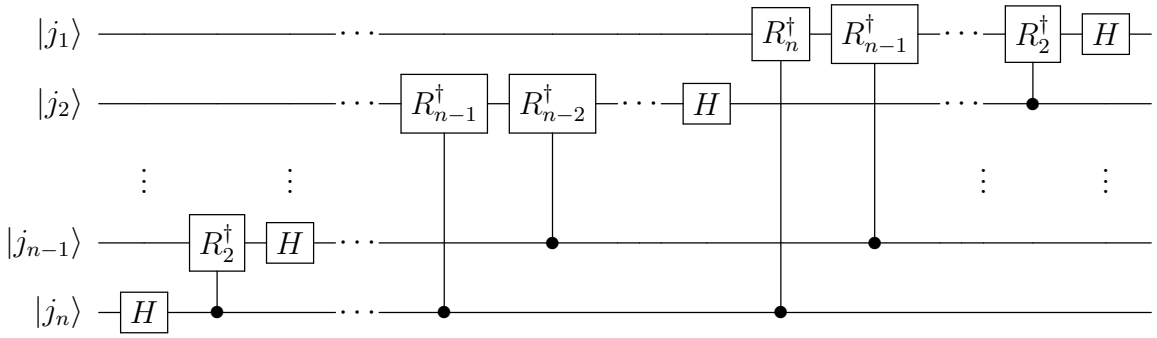
$$\begin{aligned} A &= R_z(\beta)R_y(\gamma/2) = I, \\ B &= R_y(-\gamma/2)R_z(-(\delta+\beta)/2) = R_z(-\pi/2^k), \\ C &= R_z((\delta-\beta)/2) = R_z(\pi/2^k). \end{aligned}$$

And the controlled-R_k gate can thus be decomposed as (see Exercise **??**)



5.5

It is just the inverse circuit of the one shown in Figure 5.1. So omitting the SWAP gates at the start of the circuit, for simplicity, we have



5.6

We can decompose the quantum Fourier transform on n qubits into N gates, where N scales as $\Theta(n^2)$. We are then considering that $U = \prod_{j=1}^{N} U_j$ and $V = \prod_{j=1}^{N} V_j$. The application of each V_j contributes roughly to an error of $E(U_j, V_j)$ that scales as $\Theta(1/p(n))$. This means that there are constants α and β such that $N = \alpha n^2$ and $E(U_j, V_j) = \beta/p(n)$. The error associated with the quantum Fourier transform has a rough upper limit given by

$$E(U, V) \leq NE(U_j, V_j) = \alpha\beta\frac{n^2}{p(n)},$$

meaning that $E(U,V)$ scales as $\Theta(n^2/p(n))$.

5.7

For an arbitrary state $|j\rangle$, we may write it as $|j_0,\cdots,j_{t-1}\rangle$, where each j_k is either 0 or 1. The sequence of controlled-U operations consists in applying the controlled-U^{2^k} using the qubit in state $|j_{t-1-k}\rangle$ as control, from $k=0$ to $k=t-1$. With that, each operation is effectively an unitary $U^{j_{t-1-k}2^k}$ being applied on $|u\rangle$. So the action of the circuit is

$$\begin{aligned}|j\rangle|u\rangle &\longrightarrow |j\rangle U^{j_0 2^{t-1}}\cdots U^{j_{t-1}2^0}|u\rangle \\ &= |j\rangle U^{\sum_{l=0}^{t-1} j_l 2^{t-1-l}}|u\rangle .\end{aligned}$$

But $\sum_{l=0}^{t-1} j_l 2^{t-1-l}$ is precisely the number j decomposed as a sum of its binary digits multiplied by the correspondent powers of two, thus the action of the circuit is effectively

$$|j\rangle|u\rangle \longrightarrow |j\rangle U^j|u\rangle .$$

5.8

If the final state is $\sum_u c_u|\widetilde{\varphi_u}\rangle|u\rangle$ then the probability of measuring $\widetilde{\varphi_u}$, such that $\widetilde{\varphi_u}$ is close to φ to an accuracy of n bits, that is, $e=2^{t-n}-1$, is given by

$$P=|c_u|^2 p(|\widetilde{\varphi_u}-\varphi|>e),$$

where $p(|\widetilde{\varphi_u}-\varphi|>e)$ is the probability that, given that $\widetilde{\varphi_u}$ was measured, it is a value sufficiently close to φ. Since the probability that the condition is not satisfied is upper bounded by $1/(2(e-1))$, the probability of success is such that

$$\begin{aligned}p(|\widetilde{\varphi_u}-\varphi|>e) &\geq 1-\frac{1}{2(e-1)} \\ &= 1-\frac{1}{2(2^{t-n}-2)}.\end{aligned}$$

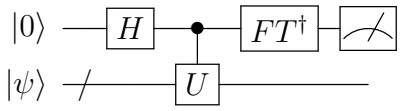
By choosing t according to Equation (5.35) we have

$$\begin{aligned}p(|\widetilde{\varphi_u}-\varphi|>e) &\geq 1-\frac{1}{2\left(2^{\lceil\log\left(2+\frac{1}{2\epsilon}\right)\rceil}-2\right)} \\ &\geq 1-\frac{1}{2\left(2+\frac{1}{2\epsilon}-2\right)} \\ &= 1-\epsilon\end{aligned}$$

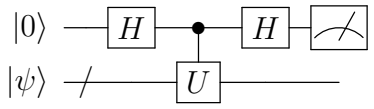
$$\implies \quad P\geq |c_u|^2(1-\epsilon).$$

5.9

Since there are only two possible eigenvalues: ± 1, only one ancilla qubit initialized to $|0\rangle$ is necessary. So the phase estimation algorithm applied to this problem should read



The quantum Fourier transform (as well as its inverse) of a single qubit is just a Hadamard gate, so the circuit is just



This is the exact same circuit as that of Exercise **??**. If the classical register reads 0 then $|\psi\rangle$ collapsed to the eigenspace associated with eigenvalue $+1$ and, on the other hand, if it reads 1 then it collapsed to the other eigenspace.

5.10

$$
\begin{aligned}
5^1 &= 5 \equiv 5 \pmod{21},\\
5^2 &= 25 \equiv 4 \pmod{21},\\
5^3 &= 125 \equiv 20 \pmod{21},\\
5^4 &= 625 \equiv 16 \pmod{21},\\
5^5 &= 3125 \equiv 17 \pmod{21},\\
5^6 &= 15625 \equiv 1 \pmod{21}.
\end{aligned}
$$

5.11

Let us consider the list $\left\{x^0, x^1, \cdots, x^N\right\}$ modulo N. There are at most N different integers in this list, but it contains $N+1$ elements, therefore, at least one of these numbers must appear twice in the list. This means that we always have two numbers a and b, satisfying $a < b$ and $b \leq N$, such that $x^b \equiv x^a \pmod{N}$. Which implies

$$x^{b-a} \equiv 1 \pmod{N}.$$

So the order of x modulo N is some number r such that $r \leq b - a$, and since both, a and b, satisfy $a < N$ and $b \leq N$, we must have $r \leq N$.

5.12

Since U is effectively the identity operator for $N \leq y \leq 2^L - 1$, it is obviously unitary for this case. Now, for $0 \leq y \leq N-1$, U is unitary if and only if $\left\langle y' \left| U^\dagger U \right| y \right\rangle = \delta_{yy'}$.

$$\left\langle y' \left| U^\dagger U \right| y \right\rangle = \langle xy' \pmod N | xy \pmod N \rangle .$$

Since x is co-prime to N then there is an inverse x^{-1} such that $xx^{-1} \equiv 1 \pmod N$. This means that $xy \pmod N \equiv xy$ and $xy' \pmod N \equiv xy'$. Thus

$$\left\langle y' \left| U^\dagger U \right| y \right\rangle = \langle xy' | xy \rangle = \delta_{yy'}.$$

5.13

$$\begin{aligned}
\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle &= \frac{1}{r} \sum_{s=0}^{r-1} \sum_{k=0}^{r-1} \exp\left(-\frac{2\pi i s k}{r}\right) |x^k \pmod N\rangle \\
&= \frac{1}{r} \sum_{k=0}^{r-1} r\delta_{k0} |x^k \pmod N\rangle \\
&= |x^0 \pmod N\rangle = |1\rangle .
\end{aligned}$$

Or equivalently

$$\begin{aligned}
\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \exp\left(\frac{2\pi i s k}{r}\right) |u_s\rangle &= \frac{1}{r} \sum_{s=0}^{r-1} \sum_{l=0}^{r-1} \exp\left(\frac{2\pi i s (k-l)}{r}\right) |x^l \pmod N\rangle \\
&= \sum_{l=0}^{r-1} \delta_{kl} |x^l \pmod N\rangle \\
&= |x^k \pmod N\rangle .
\end{aligned}$$

5.14

If we initialize the second register in the state $|0\rangle$ we get

$$\begin{aligned}
V |j\rangle |0\rangle &= |j\rangle |0 + x^j \pmod N\rangle \\
&= |j\rangle |x^j \pmod N\rangle .
\end{aligned}$$

This is the same result we would get if we had used U^j and initialized the second register in the state $|1\rangle$. **Incomplete...**

5.15

We may write x and y as the product of their prime factors, that is

$$x = q_1^{m_1} q_2^{m2} \cdots ,$$

$$y = q_1^{n_1} q_2^{n_2} \cdots ,$$

where q_i is the i-th prime number. The lcm and gcd of both can be calculated, respectively, as

$$\begin{aligned}\operatorname{lcm}(x,y) &= \prod_i q_i^{\max\{m_i,n_i\}},\\ \gcd(x,y) &= \prod_i q_i^{\min\{m_i,n_i\}}.\end{aligned}$$

Multiplying both quantities gives us

$$\begin{aligned}\operatorname{lcm}(x,y)\times\gcd(x,y) &= \prod_i q_i^{\max\{m_i,n_i\}} \times q_i^{\min\{m_i,n_i\}}\\ &= \prod_i q_i^{\max\{m_i,n_i\}+\min\{m_i,n_i\}}.\end{aligned}$$

But for all i, it is a fact that $\max\{m_i,n_i\}+\min\{m_i,n_i\} = m_i + n_i$, thus

$$\begin{aligned}\operatorname{lcm}(x,y)\times\gcd(x,y) &= \prod_i q_i^{m_i+n_i}\\ &= q_1^{m_1+n_1} q_2^{m_2+n_2}\cdots\\ &= \left(q_1^{m_1} q_2^{m_2}\cdots\right)\left(q_1^{n_1} q_2^{n_2}\cdots\right)\\ &= xy\end{aligned}$$

$$\implies \quad \operatorname{lcm}(x,y) = \frac{xy}{\gcd(x,y)}.$$

The gcd can be computed using Euclid's algorithm. This algorithm involves operations that are no harder than arithmetic multiplication, which can be calculated at a cost of $O(L^2)$ for two L bit numbers, thus the lcm can be computed in $O(L^2)$ operations.

5.16

$$\int_x^{x+1} \frac{1}{y^2}\,\mathrm{d}y = \frac{1}{x^2+x}.$$

It is a fact that $x^2 \geq 2x$ for $x \geq 2$, thus using this condition we have

$$\frac{1}{x^2+x} = \frac{2}{2x^2+2x} \geq \frac{2}{2x^2+x^2} = \frac{2}{3x^2} \quad \implies \quad \int_x^{x+1} \frac{1}{y^2}\,\mathrm{d}y \geq \frac{2}{3x^2} \quad \text{for } x \geq 2.$$

From this result we conclude that

$$\frac{1}{x^2} \leq \frac{3}{2}\int_x^{x+1} \frac{1}{y^2}\,\mathrm{d}y.$$

If we denote the i-th prime number as q_i then this relation is still valid if we substitute x by any prime number since the smallest prime is 2. That is, for all i it is true that

$$\frac{1}{q_i^2} \leq \frac{3}{2}\int_{q_i}^{q_i+1} \frac{1}{y^2}\,\mathrm{d}y \leq \frac{3}{2}\int_{q_i}^{q_{i+1}} \frac{1}{y^2}\,\mathrm{d}y,$$

where in the last inequality we used the fact that $q_{i+1} \geq q_i + 1$ for all prime numbers. Now we must simply sum for all primes on both sides, that is

$$\begin{aligned}\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{5^2} + \cdots &\leq \frac{3}{2}\left(\int_2^3 \frac{1}{y^2}\,\mathrm{d}y + \int_3^5 \frac{1}{y^2}\,\mathrm{d}y + \int_5^7 \frac{1}{y^2}\,\mathrm{d}y + \cdots\right)\\ &\Downarrow\\ \sum_q \frac{1}{q^2} &\leq \frac{3}{2}\int_2^\infty \frac{1}{y^2}\,\mathrm{d}y = \frac{3}{4}.\end{aligned}$$

Now, since

$$1 - \sum_q p(q|s_1')p(q|s_2') \geq 1 - \sum_q \frac{1}{q^2},$$

and $\sum_q 1/q^2 \leq 3/4$, Equation (5.58) follows immediately, that is

$$1 - \sum_q p(q|s_1')p(q|s_2') \geq 1 - \frac{3}{4} = \frac{1}{4}.$$

5.17

(1) If $a > 1$ is ℓ bits long, then a^b will be, at most, $b\ell$ bits long. And since $a^b = N$, which is L bits long, we have $b\ell = L$ and thus $b \leq L$.

(2) **Incomplete...**

5.18

$N = 91$ is not even, so the first step would not return 2, and knowing that 91 is composed of different primes (a little bit of cheating) we can safely say that the second step would return *false*. In step 3 we choose 4, co-prime to 91, then we have

$$\begin{aligned}4^1 &= 4 \equiv 4 \pmod{91},\\ 4^2 &= 16 \equiv 16 \pmod{91},\\ 4^3 &= 64 \equiv 64 \pmod{91},\\ 4^4 &= 256 \equiv 74 \pmod{91},\\ 4^5 &= 1024 \equiv 23 \pmod{91},\\ 4^6 &= 4096 \equiv 1 \pmod{91}.\end{aligned}$$

So we have that $r = 6$ is the order of 4 modulo 91. Now

$$x^{r/2} = 4^3 = 64 \pmod{91} \neq -1 \pmod{91},$$

and as the last step we calculate $\gcd(64 - 1, 91) = 7$, which is indeed a prime factor of 91 since its prime factorization is $91 = 7 \times 13$.

5.19

For the order-finding subroutine to be required, the number must not have 2 as a prime factor, and it must have at least two different prime numbers in its decomposition. So the smallest such number must be the product of the two first primes next to 2, that is $3 \times 5 = 15$.

5.20

**From errata:* $\sqrt{N/r}$ should be N/r.
Since $f(x + r) = f(x)$ we may rewrite

$$\begin{aligned}\hat{f}(\ell) &= \frac{1}{\sqrt{N}} \sum_{k\in\{0,r,\cdots,N-r\}} e^{-2\pi i\ell k/N} f(0) + \cdots + \frac{1}{\sqrt{N}} \sum_{k\in\{r-1,2r-1,\cdots,N-1\}} e^{-2\pi i\ell k/N} f(r-1) \\ &= \frac{1}{\sqrt{N}} \sum_{k\in\{0,r,\cdots,N-r\}} e^{-2\pi i\ell k/N} \left[f(0) + e^{-2\pi i\ell/N} f(1) + \cdots + e^{-2\pi i\ell(r-1)} f(r-1)\right].\end{aligned}$$

To relate this result to Equation (5.63) let us first denote the functions as states, that is, $\hat{f}(\ell) \to |\hat{f}(\ell)\rangle$ and $f(x) \to |f(x)\rangle$. We also have to use the fact that

$$\sum_{k\in\{0,r,\cdots,N-r\}} e^{-2\pi i\ell k/N} = \begin{cases} N/r & ; \text{ if } \ell \text{ is an integer multiple of } N/r \\ 1 & ; \text{ otherwise} \end{cases}.$$

Thus

$$\begin{aligned}|\hat{f}(\ell)\rangle &= \frac{1}{\sqrt{N}} \frac{N}{r} \left[|f(0)\rangle + e^{-2\pi i\ell/N} f(1) + \cdots + e^{-2\pi i\ell(r-1)/N} |f(r-1)\rangle\right] \\ &= \frac{\sqrt{N}}{r} \sum_{x=0}^{r-1} e^{-2\pi i\ell x/N} |f(x)\rangle.\end{aligned}$$

Considering that N is an integer multiple of the period r, the result coincides with Equation (5.63) if we take the case where the proportion relation is just $N = r$.

5.21

(1) Applying U_y to the states $|\hat{f}(\ell)\rangle$ yields

$$U_y |\hat{f}(\ell)\rangle = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i\ell x/r} U_y |f(x)\rangle$$

$$= \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i \ell x/r} \, |f(x+y)\rangle \, .$$

Now, if $x+y < r$ then we may just call it $x' \coloneqq x+y$, otherwise, we may also write it as $x+y = x'+\alpha r$, where α is some positive integer, so in any case, we can always use $f(x+y) \to f(x')$ and perform the variable substitution $x \to x' - y$, yielding

$$\begin{aligned} U_y \, |\hat{f}(\ell)\rangle &= \frac{1}{\sqrt{r}} \sum_{x'=y}^{r+y-1} e^{-2\pi i \ell (x'-y)/r} \, |f(x')\rangle \\ &= e^{2\pi i \ell y/r} \frac{1}{\sqrt{r}} \sum_{x'=y}^{r+y-1} e^{-2\pi i \ell x'/r} \, |f(x')\rangle \, . \end{aligned}$$

Because of the periodicity of $f(x)$, the terms for $x' > r-1$ will be the same as terms for $0 \leq x' < y$ and therefore

$$\begin{aligned} U_y \, |\hat{f}(\ell)\rangle &= e^{2\pi i \ell y/r} \frac{1}{\sqrt{r}} \sum_{x'=0}^{r-1} e^{-2\pi i \ell x'/r} \, |f(x')\rangle \\ &= e^{2\pi i \ell y/r} \, |\hat{f}(\ell)\rangle \, . \end{aligned}$$

(2) U_y will just add an immaterial phase, that will not affect the probability of measurement outcomes. Explicitly we have

$$\begin{aligned} U_y \, |f(x_0)\rangle &= \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{2\pi i x_0 \ell/r} U_y \, |\hat{f}(\ell)\rangle \\ &= \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{2\pi i (x_0+y) \ell/r} U_y \, |\hat{f}(\ell)\rangle \, . \end{aligned}$$

In the period-finding protocol, in step 3, if we were to apply U_y instead of U we would obtain

$$\frac{e^{2\pi i \ell y/r}}{\sqrt{r 2^t}} \sum_{\ell=0}^{r-1} \sum_{x=0}^{2^t-1} e^{2\pi i \ell x/r} \, |x\rangle \, |\hat{f}(\ell)\rangle \, ,$$

and after the $QFT^\dagger$ we would have

$$\frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{2\pi i \ell y/r} \, |\widetilde{\ell/r}\rangle \, |\hat{f}(\ell)\rangle \, .$$

The overall phase does not affect the outcome probabilities, so U_y can be used to realize the black box, which is just as good as U.

5.22

*It seems there is an $1/r$ factor missing in the first equality and an extra $1/\sqrt{r}$ in the second one.

The first step is simply the Fourier transform on two variables:

$$|\hat{f}(\ell_1,\ell_2)\rangle = \sum_{x_1=0}^{r-1}\sum_{x_2=0}^{r-1}\frac{1}{\sqrt{r}}e^{-2\pi i\ell_1 x_1/r}\frac{1}{\sqrt{r}}e^{-2\pi i\ell_2 x_2/r}\,|f(x_1,x_2)\rangle$$
$$= \frac{1}{r}\sum_{x_1=0}^{r-1}\sum_{x_2=0}^{r-1}e^{-2\pi i(\ell_1 x_1+\ell_2 x_2)/r}\,|f(x_1,x_2)\rangle\,.$$

Now we use the periodicity property of the function, that is $f(x_1,x_2)=f(0,x_2+sx_1)$, and get

$$|\hat{f}(\ell_1,\ell_2)\rangle = \frac{1}{r}\sum_{x_1=0}^{r-1}\sum_{x_2=0}^{r-1}e^{-2\pi i(\ell_1 x_1+\ell_2 x_2)/r}\,|f(0,x_2+sx_1)\rangle\,.$$

Making the variable substitution $x_2 \to j - sx_1$ yields

$$|\hat{f}(\ell_1,\ell_2)\rangle = \frac{1}{r}\sum_{x_1=0}^{r-1}\sum_{j=sx_1}^{r-1+sx_1}e^{-2\pi i(\ell_1 x_1+\ell_2 j-\ell_2 s x_1)/r}\,|f(0,j)\rangle$$
$$= \frac{1}{r}\sum_{x_1=0}^{r-1}e^{-2\pi i(\ell_1/s-\ell_2)sx_1/r}\sum_{j=sx_1}^{r-1+sx_1}e^{-2\pi i\ell_2 j/r}\,|f(0,j)\rangle\,.$$

The first sum results in r, and because of the periodicity of $f(x_1,x_2)$, the terms for $j>r-1$ will be the same as terms for $0\le j<sx_1$, so the result is

$$|\hat{f}(\ell_1,\ell_2)\rangle = \sum_{j=0}^{r-1}e^{-2\pi i\ell_2 j/r}\,|f(0,j)\rangle$$

5.23

*Just like in the last exercise, we should remove the $1/\sqrt{r}$ factor from Equation (4.70). Also, there should not be a minus sign in the exponential.

$$\frac{1}{r}\sum_{\ell_1=0}^{r-1}\sum_{\ell_2=0}^{r-1}e^{2\pi i(\ell_1 x_1+\ell_2 x_2)/r}\,|\hat{f}(\ell_2,\ell_2)\rangle = \frac{1}{r}\sum_{\ell_1=0}^{r-1}\sum_{\ell_2=0}^{r-1}\sum_{j=0}^{r-1}e^{2\pi i(\ell_1 x_1+\ell_2 x_2-\ell_2 j)/r}\,|f(0,j)\rangle\,.$$

Using the constraint that $\ell_1/s-\ell_2$ is an integer multiple of r we may write $\ell_1=s(\alpha r+\ell_2)$, where α is an integer. Substituting in the relation yields

$$\frac{1}{r}\sum_{\ell_1=0}^{r-1}\sum_{\ell_2=0}^{r-1}e^{2\pi i(\ell_1 x_1+\ell_2 x_2)/r}\,|\hat{f}(\ell_2,\ell_2)\rangle = \frac{1}{r}\sum_{\ell_2=0}^{r-1}\sum_{j=0}^{r-1}e^{2\pi i(s\alpha r x_1+s\ell_2 x_1+\ell_2 x_2-\ell_2 j)/r}\,|f(0,j)\rangle$$
$$= \frac{1}{r}e^{2\pi i s\alpha r x_1}\sum_{\ell_2=0}^{r-1}\sum_{j=0}^{r-1}e^{2\pi i(sx_1+x_2-j)\ell_2/r}\,|f(0,j)\rangle\,.$$

In this expression, $e^{2\pi i s\alpha r x_1}$ is just an immaterial global phase, and the sum over ℓ_2 can be identified with a Kronecker delta as $\frac{1}{r}\sum_{\ell_2=0}^{r-1} e^{2\pi i(sx_1+x_2-j)\ell_2/r} = \delta_{j,sx_1+x_2}$, thus

$$\begin{aligned}\frac{1}{r}\sum_{\ell_1=0}^{r-1}\sum_{\ell_2=0}^{r-1} e^{2\pi i(\ell_1 x_1+\ell_2 x_2)/r}\,|\hat{f}(\ell_2,\ell_2)\rangle &= \sum_{j=0}^{r-1}\delta_{j,sx_1+x_2}\,|f(0,j)\rangle \\ &= |f(0,sx_1+x_2)\rangle \\ &= |f(x_1,x_2)\rangle\,.\end{aligned}$$

5.24

Applying the continued fractions algorithm to the first and second registers we can obtain, respectively, fractions $a_1/b_1 \approx \widetilde{s\ell_2/r}$ and $a_2/b_2 \approx \widetilde{\ell_2/r}$, so computing $(a_1 b_2)/(b_1 a_2)$ results in s.

5.25

-

5.26

-

5.27

-

5.28

-

5.29

-