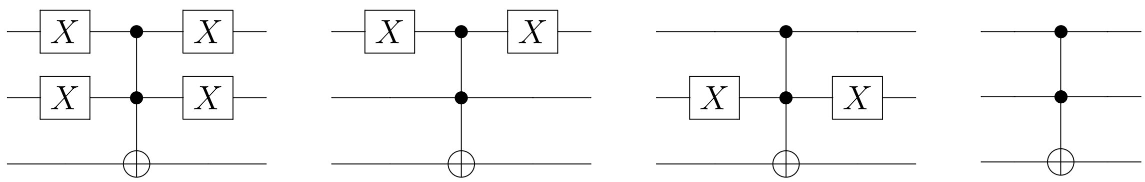
Physics 4481-7681; CS 4812 Solution Set 5

Problem 1: Searching for one of four items

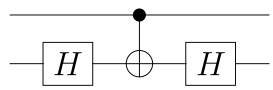
a) The circuit diagrams for the four possibilities for the function $\mathbf{U}_f$ are



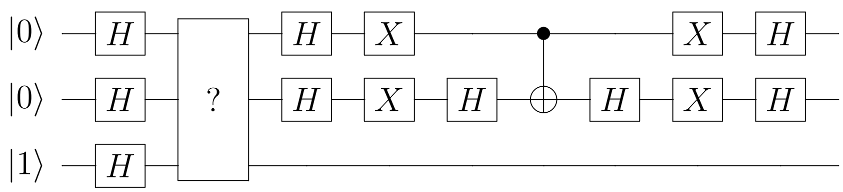
(0) (1) (2) (3)

corresponding to the special number being 00, 01, 10, and 11.

b) A circuit diagram that acts as $\mathbf{1} - 2|11\rangle\langle 11|$ is



c) The circuit diagram for a single Grover iteration applied to $|0\rangle|0\rangle|1\rangle$ is



where the '?' box is a 3-Qbit gate representing any of the four possibilities of part (a).

d) If the $\mathbf{U}_f$ is the Toffoli gate (3) from part a), then the state of the top two Qbits that emerges from $\mathbf{U}_f$ is $|\psi\rangle_0 = \frac{1}{2}\big(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle\big)$.

Since $\mathbf{XH} = \mathbf{HZ}$ and $\mathbf{HXH} = \mathbf{Z}$, the state just prior to the cNOT in the middle of the figure above is

$$
\begin{aligned}
|\psi\rangle_1 &= (\mathbf{H}\otimes\mathbf{1})(\mathbf{Z}\otimes\mathbf{Z})|\psi\rangle_0 = \frac{1}{2}(\mathbf{H}\otimes\mathbf{1})\big(|0\rangle|0\rangle - |0\rangle|1\rangle - |1\rangle|0\rangle - |1\rangle|1\rangle\big) \\
&= \frac{1}{\sqrt{2}}(\mathbf{H}\otimes\mathbf{1})\Big(\frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)|0\rangle - \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)|1\rangle\Big) = \frac{1}{\sqrt{2}}\big(|1\rangle|0\rangle - |0\rangle|1\rangle\big) \ .
\end{aligned}
$$

The cNOT changes this to $|\psi\rangle_2 = \frac{1}{\sqrt{2}}\big(|1\rangle|1\rangle - |0\rangle|1\rangle\big) = -\frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)|1\rangle$.

The final gates after the cNOT are equivalent to acting on $|\psi\rangle_2$ with $\mathbf{ZH}\otimes\mathbf{Z}$. The $\mathbf{H}$ on the upper wire gives

$$
|\psi\rangle_3 = -|1\rangle|1\rangle
$$

and this is invariant under the final $\mathbf{Z}\otimes\mathbf{Z}$. So acting on the oracle associated with 11, the final state is indeed $|1\rangle|1\rangle$ (to within an overall minus sign).

The other three possibilities for the oracle correspond to keeping the box with the question mark a Toffoli gate, but sandwiching it between two $\mathbf{X}$ gates on either the upper wire, the lower wire, or both. Any $\mathbf{X}$ to the left of the Toffoli gate in the above figure can be brought to the left through the $\mathbf{H}$ gate if it is changed to a $\mathbf{Z}$. But $\mathbf{Z}|0\rangle = |0\rangle$, so the extra $\mathbf{X}$ gates on the left can be ignored. Any $\mathbf{X}$ to the right of the Toffoli gate in the figure above can be brought to the right through the $\mathbf{H}$ gate if it is converted to a $\mathbf{Z}$ gate. The $\mathbf{Z}$ gate can be brought to the right through the next $\mathbf{X}$ gate if a factor of -1 is introduced. A $\mathbf{Z}$ on the upper wire can be brought to the right through the cNOT gate (because the computational basis states that determine whether NOT acts are eigenstates of $\mathbf{Z}$) and a $\mathbf{Z}$ on the lower wire can be brought to the right through the $\mathbf{H}$ gate if it is converted back to an $\mathbf{X}$ which also commutes with the cNOT gate, and can be converted back to the $\mathbf{Z}$ gate by being brought through the $\mathbf{H}$ gate on the other side of the cNOT gate. So now we have one or two $\mathbf{Z}$ gates to the left of the final two $\mathbf{X}$ gates. Either or both $\mathbf{Z}$ gates can be brought to the right through the $\mathbf{X}$ gates producing more minus signs that cancel the earlier ones. Finally either or both $\mathbf{Z}$ gates can be brought through the $\mathbf{H}$ gates converting them back to $\mathbf{X}$ gates.

In short, the effect of sandwiching the Toffoli gate on the left of the above figure between one or two pairs of $\mathbf{X}$ gates left is to leave the circuit unchanged except for one or two final $\mathbf{X}$ gates on the extreme right on the same wire(s) as the original pair(s) of $\mathbf{X}$ gates. These have the effect of converting the $-|1\rangle|1\rangle$ that would be produced by the unsandwiched Toffoli gate into either $-|0\rangle|1\rangle$, $-|1\rangle|0\rangle$, or $-|0\rangle|0\rangle$, corresponding precisely to whether the sandwiched Toffoli gates were taken from parts (2), (1), or (0) of part a).

Problem 2: Quantum Zeno

Let $\mathbf{V}|x\rangle = (-1)^{f(x)}|x\rangle$, $|\phi\rangle = \mathbf{H}^{\otimes n}|0\rangle_n = \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle$ and $\mathbf{W} = 2|\phi\rangle\langle\phi| - \mathbf{1}$.

a) Setting $|\text{yes}\rangle = \frac{1}{m^{1/2}}\sum_{x|f(x)=1}|x\rangle$ and $|\text{no}\rangle = \frac{1}{(2^n-m)^{1/2}}\sum_{x|f(x)=0}|x\rangle$, we can write

$$|\phi\rangle = \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle = \cos\theta|\text{no}\rangle + \sin\theta|\text{yes}\rangle \ ,$$

where $\sin\theta = \sqrt{m/2^n}$ and $\cos\theta = \sqrt{1-m/2^n}$. The matrix elements of $\mathbf{V}$ in the $|\text{no}\rangle, |\text{yes}\rangle$ basis are

$$\mathbf{V} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \ .$$

Using

$$\begin{aligned}
\langle\text{no}|\mathbf{W}|\text{no}\rangle &= \langle\text{no}|\big(2|\phi\rangle\langle\phi| - \mathbf{1}\big)|\text{no}\rangle = 2\langle\text{no}|\phi\rangle\langle\phi|\text{no}\rangle - 1 = 2\cos^2\theta - 1 = \cos 2\theta \\
\langle\text{yes}|\mathbf{W}|\text{yes}\rangle &= \langle\text{yes}|\big(2|\phi\rangle\langle\phi| - \mathbf{1}\big)|\text{yes}\rangle = 2\langle\text{yes}|\phi\rangle\langle\phi|\text{yes}\rangle - 1 = 2\sin^2\theta - 1 = -\cos 2\theta \\
\langle\text{no}|\mathbf{W}|\text{yes}\rangle &= \langle\text{no}|\big(2|\phi\rangle\langle\phi| - \mathbf{1}\big)|\text{yes}\rangle = 2\langle\text{no}|\phi\rangle\langle\phi|\text{yes}\rangle = 2\cos\theta\sin\theta = \sin 2\theta \\
\langle\text{yes}|\mathbf{W}|\text{no}\rangle &= \langle\text{yes}|\big(2|\phi\rangle\langle\phi| - \mathbf{1}\big)|\text{no}\rangle = 2\langle\text{yes}|\phi\rangle\langle\phi|\text{no}\rangle = 2\sin\theta\cos\theta = \sin 2\theta
\end{aligned}$$

we find that the matrix elements of $\mathbf{W}$ are

$$\mathbf{W} = \begin{pmatrix} \langle \text{no}|\mathbf{W}|\text{no}\rangle & \langle \text{no}|\mathbf{W}|\text{yes}\rangle \\ \langle \text{yes}|\mathbf{W}|\text{no}\rangle & \langle \text{yes}|\mathbf{W}|\text{yes}\rangle \end{pmatrix} = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix} ,$$

so that $\mathbf{WV} = \begin{pmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix}$ is a rotation by 2θ (counterclockwise from the $|\text{no}\rangle$ towards the $|\text{yes}\rangle$ axis).

The explicit form for the quantum state after k iterations is thus

$$(\mathbf{WV})^k|\phi\rangle = \cos\big((2k+1)\theta\big)|\text{no}\rangle + \sin\big((2k+1)\theta\big)|\text{yes}\rangle \ .$$

If $m \ll 2^n$, then $\theta \approx \sqrt{m/2^n}$. The above state is first close to $|\text{yes}\rangle$ when $(2k+1)\theta \approx \pi/2$, or $k \approx \pi/(4\theta) \approx (\pi/4)\sqrt{2^n/m}$, as in eq. (4.22).

b) We implement $\mathbf{U}_f$ in the standard way, so that $\mathbf{U}_f|x\rangle_n|0\rangle = |x\rangle_n|f(x)\rangle$. Applying $\mathbf{U}_f$ to the initial state gives

$$\mathbf{U}_f|\phi\rangle|0\rangle = \cos\theta|\text{no}\rangle|0\rangle + \sin\theta|\text{yes}\rangle|1\rangle \ .$$

Measuring the output Qbit gives 0 with probability $\cos^2\theta = 1 - m/2^n$ and 1 with probability $\sin^2\theta = m/2^n \ll 1$. If we measure 0, then the state of the input bits is left as $|\text{no}\rangle$. Applying $\mathbf{WV}$ to $|\text{no}\rangle$ and measuring again gives

$$\mathbf{U}_f(\mathbf{WV}|\text{no}\rangle)|0\rangle = \cos 2\theta|\text{no}\rangle|0\rangle + \sin 2\theta|\text{yes}\rangle|1\rangle \ .$$

Measuring the output Qbit gives 0 with probability $\cos^2 2\theta \approx 1 - 4m/2^n$, and 1 with probability $\sin^2 2\theta \approx 4m/2^n \ll 1$. Again if we measure 0, then the state is left as $|\text{no}\rangle$, and so on. (If instead we had reset the state to $|\phi\rangle$ before applying $\mathbf{WV}$, then the state would instead have 3θ in the above, and the probability of measuring 0 would be $\cos^2 3\theta \approx 1 - 9m/2^n$.)

If the probability of finding a solution in a given step is $p = 4m/2^n$, and not finding a solution is $q = 1-p$, then the probability of finding a solution on the k^{th} step is $q^{k-1}(1-q)$. The average value of the number of steps is thus

$$\sum_{k=1}^{\infty} kq^{k-1}(1-q) = (1-q)\frac{\partial}{\partial q}\sum_{k=0}^{\infty} q^k = (1-q)\frac{\partial}{\partial q}\frac{1}{1-q} = (1-q)\frac{1}{(1-q)^2} = \frac{1}{1-q} = 1/p \ ,$$

so on average it takes $1/p = 2^n/4m$ iterations (or $2^n/9m$ using a protocol in which the state is reset to $|\phi\rangle$ before each iteration). The number of steps grows as $2^n/m$ rather than as $\sqrt{2^n/m}$. [Hence "the watched quantum pot takes longer to boil."]

Problem 3: Modified Grover

a) For $M/N = 4$, we have $\sin\theta = \sqrt{M/N} = 1/2$, i.e., $\theta = \pi/3$. This reduces to the case $N = 4$, $M = 1$ considered in problem 1, in which a single application of $\mathbf{WV}$ rotates $|\phi\rangle$ by $2\theta = 2\pi/3$. Hence $\mathbf{WV}\phi = |\text{yes}\rangle$, and measurement will result in finding one of the marked states with probability 1.

b) To simplify the algebra, use the abbreviated notation $|\phi\rangle = \cos\theta|\text{no}\rangle + \sin\theta|\text{yes}\rangle = c|n\rangle + s|y\rangle$, so that $\mathbf{V}_\alpha|\phi\rangle = \cos\theta|\text{no}\rangle + \mathrm{e}^{i\alpha}\sin\theta|\text{yes}\rangle = c|n\rangle + ps|y\rangle$, where $p = \mathrm{e}^{i\alpha}$, $c = \cos\theta$, $s = \sin\theta$. Then $\mathbf{W}_\alpha\mathbf{V}_\alpha|\phi\rangle = (1-p)c\langle\phi|n\rangle|\phi\rangle + (1-p)ps\langle\phi|y\rangle|\phi\rangle - c|n\rangle - ps|y\rangle$.

Using $\langle\phi|n\rangle = c$, $\langle\phi|y\rangle = s$, and expanding $|\phi\rangle = c|n\rangle + s|y\rangle$, we extract the component in the $|n\rangle$ direction:

$$\begin{aligned}\big[(1-p)c^3 + (1-p)ps^2c - c\big]|n\rangle &= c\big[(-p^2s^2 + c^2 - 1 + ps^2 - pc^2\big]|n\rangle \\ &= cp\big[-s^2(p+p^{-1}) + s^2 - c^2\big]|n\rangle = cp\big[-2s^2\cos\alpha + s^2 - c^2\big]|n\rangle\ .\end{aligned}$$

Setting this to zero requires $\cos\alpha = (s^2 - c^2)/2s^2$, and there's a solution for α if $|s^2 - c^2)/2s^2| \le 1$. Substituting $s = \sqrt{M/N}$, $c = \sqrt{(N-M)/N}$, then $s^2 - c^2 = (2M-N)/N$, and the condition $|(2M-N)/2M| \le 1$ implies $M \ge N/4$.

c) The modified Grover only works starting from $\sin\theta' \ge 1/2$, i.e., $\theta' \ge \pi/6$, and starting from some smaller θ we would iterate the standard Grover ℓ times until $(2\ell+1)\theta \ge \pi/6$, and then use the modified Grover. For $M \ll N$ and $\theta \approx \sqrt{M/N}$, that would mean $\ell \approx (\pi/12)\sqrt{N/M}$ standard Grover iterations followed by a single modified Grover. In particular, $M = 1$ gives a total of $\ell \approx (\pi/12)\sqrt{N} + 1$, including the final modified Grover.

Problem 4: Grover plus period finding

a) The algorithm begins with a uniform superposition over all counter values and all input values $|\Phi\rangle = \frac{1}{\sqrt{T}}\sum_{t=0}^{T-1}|t\rangle \otimes \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$. We apply $\mathbf{G}$ to obtain the state

$$\mathbf{G}|\Phi\rangle = \frac{1}{\sqrt{T}}\sum_{t=0}^{T-1}|t\rangle \otimes \big(\cos(2t+1)\theta|\text{no}\rangle + \sin(2t+1)\theta|\text{yes}\rangle\big)$$

since the initial state $|\phi\rangle = \cos\theta|\text{no}\rangle + \sin\theta|\text{yes}\rangle$, $\sin\theta = \sqrt{\frac{m}{N}}$, and each Grover iteration rotates $|\phi\rangle$ closer to $|\text{yes}\rangle$ by an angle 2θ. Finally we apply the QFT on the counter register and then measure in the computation basis. Applying the QFT on $\mathbf{G}|\Phi\rangle$ produces

$$\begin{aligned}|\Phi\rangle_{\text{QFT}} &= \frac{1}{T}\sum_{t=0}^{T-1}\sum_{\ell=0}^{T-1}\mathrm{e}^{2\pi i\ell t/T}|\ell\rangle \otimes \big(\cos(2t+1)\theta|\text{no}\rangle + \sin(2t+1)\theta|\text{yes}\rangle\big) \\ &= \frac{1}{T}\sum_{t=0}^{T-1}|\ell\rangle \otimes \big(\frac{a_\ell + b_\ell}{2}|\text{no}\rangle + \frac{a_\ell - b_\ell}{2i}|\text{yes}\rangle\big)\end{aligned}$$

where $a_\ell = \sum_{t=0}^{T-1} \mathrm{e}^{2\pi i(\ell+T\theta/\pi)t/T+i\theta}$, $b_\ell = \sum_{t=0}^{T-1} \mathrm{e}^{2\pi i(\ell-T\theta/\pi)t/T-i\theta}$. Therefore, the probability of measuring the outcome ℓ is given by

$$P(\ell) = \frac{1}{4T^2}\left(|a_\ell + b_\ell|^2 + |a_\ell - b_\ell|^2\right) = \frac{1}{2T^2}\left(|a_\ell|^2 + |b_\ell|^2\right)$$

Since a_ℓ and b_ℓ are invariant under $\ell \to \ell + T$, we consider ℓ to be defined mod$T$.

b) (i) When $T\theta/\pi$ is an integer, all a_ℓ and b_ℓ vanish except for $\ell = \pm T\theta/\pi$, for which $|a_{\ell=-T\theta/\pi}| = |b_{\ell=T\theta/\pi}| = T$. Measuring the counter gives either $T\theta/\pi$ or $T - T\theta/\pi$ with equal probability 1/2, and either determines θ to accuracy $O(1/T)$.

(ii) When $T\theta/\pi$ is not an integer, there are a few cases to consider. First recall that $|a_\ell|^2$ and $|b_\ell|^2$ are given respectively by

$$\Big|\sum_{t=0}^{T-1} \mathrm{e}^{2\pi i(\ell\pm T\theta/\pi)t/T\pm i\theta}\Big|^2 = \Big|\frac{1-\mathrm{e}^{2\pi i(\ell\pm T\theta/\pi)}}{1-\mathrm{e}^{2\pi i(\ell\pm T\theta/\pi)/T}}\mathrm{e}^{\pm i\theta}\Big|^2 = \Big|\frac{\sin\pi(\ell\pm T\theta/\pi)}{\sin\pi(\ell\pm T\theta/\pi)/T}\Big|^2 .$$

Letting δ equal the smaller of $\ell \pm T\theta/\pi$, note that whenever $0 < \delta < 1/2$, we use $\sin x \geq 2x/\pi$ $(0 \leq x \leq \pi/2)$, and $\sin\varepsilon \leq \varepsilon$ for $0 < \varepsilon \ll 1$, to bound

$$\Big|\frac{\sin\pi\delta}{\sin\pi\delta/T}\Big|^2 \geq \Big|\frac{2\delta}{\pi\delta/T}\Big|^2 = T^2\frac{4}{\pi^2} .$$

That means that when $\ell + T\theta/\pi < 1/2$, we have $|a_\ell|^2 \geq T^2(4/\pi^2)$, and when $\ell - T\theta/\pi < 1/2$, we have $|b_\ell|^2 \geq T^2(4/\pi^2)$.

When $0 < T\theta/\pi \leq 1/2$, success means measuring $\ell = 0$ (the closest integer to $T\theta/\pi$), and we have

$$P(\ell = 0) = \frac{1}{2T^2}\left(|a_{\ell=0}|^2 + |b_{\ell=0}|^2\right) \geq \frac{1}{2T^2}\Big(T^2(4/\pi^2) + T^2(4/\pi^2)\Big) = \frac{4}{\pi^2} .$$

When $1/2 < T\theta/\pi < 1$, success means measuring $\ell = \pm 1$ (i.e., $\ell = 1$ or $\ell = T-1 = -1$ (mod$T$), since 1 is now the closest integer to $T\theta/\pi$, and

$$P(\ell = -1) + P(\ell = 1) \geq \frac{1}{2T^2}\left(|a_{\ell=-1}|^2 + |b_{\ell=1}|^2\right) \geq \frac{1}{2T^2}\Big(T^2(4/\pi^2) + T^2(4/\pi^2)\Big) = \frac{4}{\pi^2} .$$

When $1 < T\theta/\pi < T/2 - 1$, success means measuring $\ell = \pm j$, where j is the closest integer to $T\theta/\pi$, within 1/2 of $T\theta/\pi$ above or below, so that

$$P(\ell = -j) + P(\ell = j) \geq \frac{1}{2T^2}\left(|a_{\ell=-j}|^2 + |b_{\ell=j}|^2\right) \geq \frac{1}{2T^2}\Big(T^2(4/\pi^2) + T^2(4/\pi^2)\Big) = \frac{4}{\pi^2} .$$

When $T/2 - 1 < T\theta/\pi < T/2 - 1/2$ (though note that θ will never be this large for $m \ll N$), success means $\ell = \pm(T/2 - 1)$ (i.e., $\ell = T/2 - 1$ or $\ell = T/2 + 1$), and

$$\begin{aligned} P(\ell = -T/2+1) + P(\ell = T/2-1) &\geq \frac{1}{2T^2}\left(|a_{\ell=-T/2+1}|^2 + |b_{\ell=T/2-1}|^2\right) \\ &\geq \frac{1}{2T^2}\Big(T^2(4/\pi^2) + T^2(4/\pi^2)\Big) = \frac{4}{\pi^2} . \end{aligned}$$

When $T/2 - 1/2 \le T\theta/\pi < T/2$, success means $\ell = T/2$, and

$$P(\ell = T/2) = \frac{1}{2T^2}\left(|a_{\ell=T/2}|^2 + |b_{\ell=T/2}|^2\right) \ge \frac{1}{2T^2}\Big(T^2(4/\pi^2) + T^2(4/\pi^2)\Big) = \frac{4}{\pi^2}\ .$$

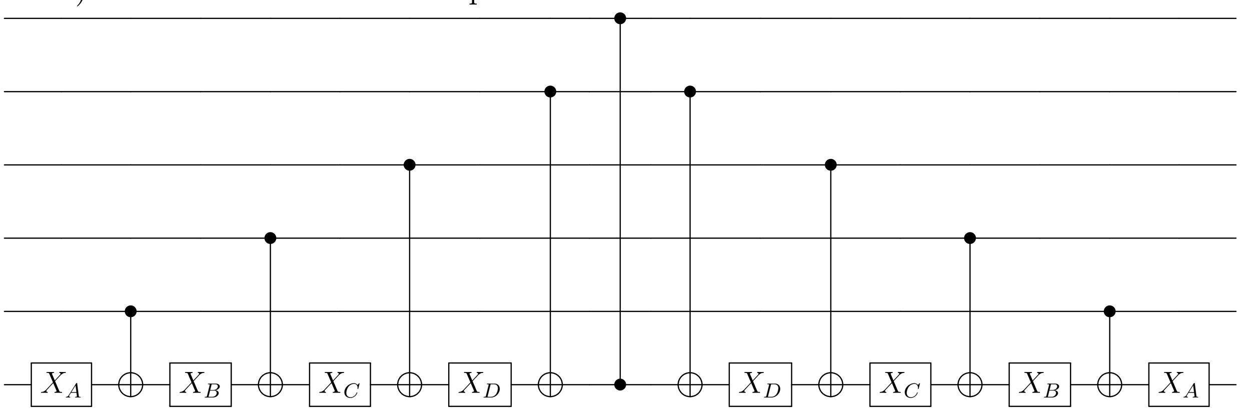
For all cases, measuring the counter reveals the closest integer to $T\theta/\pi$ with constant probabability of success at least $4/\pi^2$, and θ is determined with $O(1/T)$ accuracy.

c) Since $\theta \approx \sqrt{m/N}$, we have $\delta m \approx 2\sqrt{mN}\delta\theta$. To have m determined with high probability to within $\delta m \approx 1$, given that $\delta\theta = O(1/T)$, it follows that $T = O(\sqrt{mN})$ queries are required. (One of those m special values can then be found with an additional $O(\sqrt{N/m})$ queries by the standard Grover iteration.)

Classically it takes $O(N)$ queries to determine m (and it takes $O(N/m)$ queries to have a high probability of finding a special value).

Problem 5: qudits

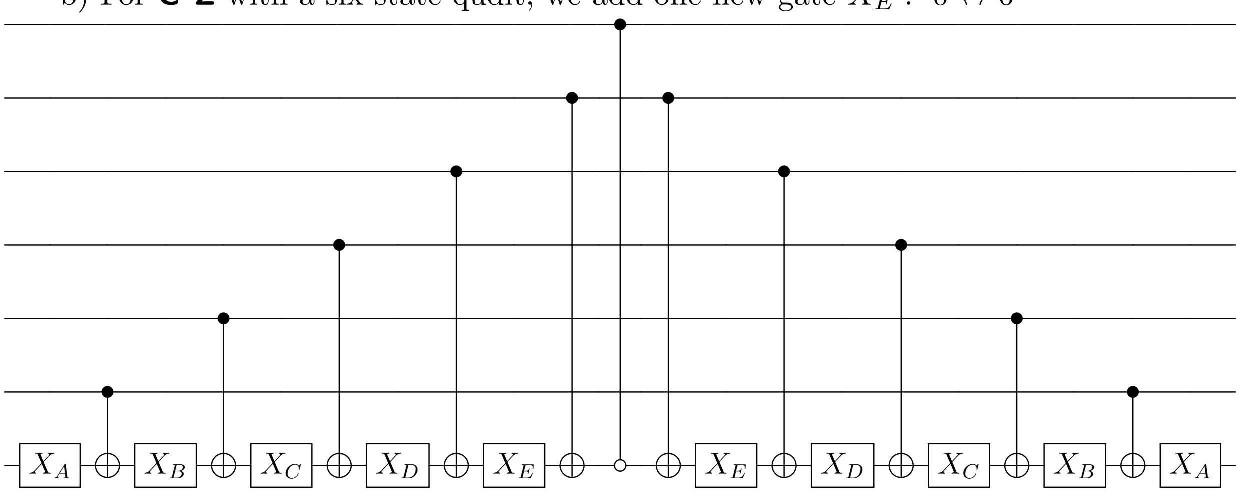
a) For $\mathbf{C}^5\mathbf{Z}$ with a five-state qudit



where $X_A:\ 0 \leftrightarrow 2$, $X_B:\ 1 \leftrightarrow 3$, $X_C:\ 0 \leftrightarrow 4$, $X_D:\ 1 \leftrightarrow 5$, and there is a total of eight cNOTS, one c$\mathbf{Z}$, and eight 1-Qbit gates.

The circuit in fig. 4.5 has ten Toffoli gates ($\mathbf{c}^2\mathbf{X}$) and two double-controlled $\mathbf{Z}$s ($\mathbf{c}^2\mathbf{Z}$). Each Toffoli and the double-controlled $\mathbf{Z}$s can be made with six cNOT gates (fig. 2.13 in the text), for a total of 72 cNOT gates.

b) For $\mathbf{C}^6\mathbf{Z}$ with a six-state qudit, we add one new gate $X_E:\ 0 \leftrightarrow 6$



so there are now a total of ten cNOTS, one c$\mathbf{Z}$, and ten 1-Qbit gates.

The circuit in fig. 4.7 of the text has two $\mathbf{c}^4\mathbf{Z}$ and two $\mathbf{c}^3\mathbf{X}$ gates. According to fig. 4.5, a $\mathbf{c}^3\mathbf{X}$ gate can be built with two Toffolis and two $\mathbf{c}^2\mathbf{Z}$s, and a $\mathbf{c}^4\mathbf{Z}$ can be built with six Toffolis and two $\mathbf{c}^2\mathbf{Z}$s, so the total is $(2(6+2)+2(2+2))6 = 24\cdot 6 = 144$ cNOT gates. (We see that the number of cNOT gates increases much less quickly if a single reliable qudit is available.)

Problem 6: GHZ

a) For the circuit at left, after the 1-Qbit gates act we have $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) = \frac{1}{2}(|00\rangle+|01\rangle+|10\rangle+|11\rangle$. The $\mathbf{cZ}$ gate takes this to $\frac{1}{2}(|0\rangle(|0\rangle+|1\rangle)+|1\rangle(|1\rangle-|0\rangle))$, and the final 1-Qbit gate then has the effect $\to \frac{1}{2\sqrt{2}}\big((|0\rangle+|1\rangle)(|0\rangle+|1\rangle)+(|1\rangle-|0\rangle)(|1\rangle-|0\rangle)\big) = \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$

Although the circuits agree on the state $|00\rangle$, they do not agree on any of the other computational basis states, as can be easily checked explicitly on any of $|10\rangle$, $|01\rangle$, $|11\rangle$. Alternatively, in python (or similarly in matlab) we can define

```
I=eye(2)
X=array([[0,1],[1,0]])
Y=array([[0,-1j],[1j,0]])
Z=array([[1,0],[0,-1]])
H=(X+Z)/sqrt(2)
Ym=(I-1j*Y)/sqrt(2)
cNOT=kron((1+Z)/2,I)+kron((1-Z)/2,X)
cZ10=diag([1,1,-1,1])
```

Then we see that

kron(Ym,I).dot(cZ10).dot(kron(Ym,Ym))= $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1 & 0 & 0\\ 0 & 0 & -1 & -1\\ 0 & 0 & -1 & 1\\ 1 & 1 & 0 & 0\end{pmatrix}$

cNOT.dot(kron(H,I))= $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 0 & 1 & 0 & -1\\ 1 & 0 & -1 & 0\end{pmatrix}$

and the two only agree on the first column (for $|00\rangle$).

b) Now we have

$$
\begin{aligned}
&\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\\
&\qquad\to\frac{1}{2\sqrt{2}}(|000\rangle-|001\rangle+|010\rangle+|011\rangle-|100\rangle+|101\rangle+|110\rangle+|111\rangle)\\
&\qquad=\frac{1}{2\sqrt{2}}\big(|0\rangle((|0\rangle+|1\rangle)|0\rangle+(-|0\rangle+|1\rangle)|1\rangle)+|1\rangle((-|0\rangle+|1\rangle)|0\rangle+(|0\rangle+|1\rangle)|1\rangle)\big)\\
&\qquad\to\frac{1}{2\sqrt{2}}\big((|0\rangle+|1\rangle)((|0\rangle+|1\rangle)(|0\rangle+|1\rangle)+(-|0\rangle+|1\rangle)(|1\rangle-|0\rangle))\\
&\qquad\qquad\quad+(|1\rangle-|0\rangle)((-|0\rangle+|1\rangle)(|0\rangle+|1\rangle)+(|0\rangle+|1\rangle)(|1\rangle-|0\rangle))\big)\\
&\qquad=\frac{1}{\sqrt{2}}\big(|000\rangle+|111\rangle\big)
\end{aligned}
$$

Once again, if we check any state other than $|000\rangle$, we find that the result is different for the two circuits. Or more comprehensively, we use the definitions from part a) plus the additional

cZ01=diag([1,-1,1,1])

def p(A,B,C): return kron(A,kron(B,C))

to find

p(Ym,I,Ym).dot(kron(I,cZ01)).dot(kron(cZ10,I)).dot(p(Ym,Ym,Ym))

$$
=\tfrac{1}{\sqrt{2}}\begin{pmatrix}1&0&-1&0&0&0&0&0\\0&-1&0&1&0&0&0&0\\0&0&0&0&0&1&0&1\\0&0&0&0&-1&0&-1&0\\0&0&0&0&-1&0&1&0\\0&0&0&0&0&1&0&-1\\0&-1&0&-1&0&0&0&0\\1&0&1&0&0&0&0&0\end{pmatrix},\text{ and}
$$

kron(I,cNOT).dot(kron(cNOT,I)).dot(p(H,I,I)) $= \tfrac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&0&1&0&0&0\\0&1&0&0&0&1&0&0\\0&0&0&1&0&0&0&1\\0&0&1&0&0&0&1&0\\0&0&1&0&0&0&-1&0\\0&0&0&1&0&0&0&-1\\0&1&0&0&0&-1&0&0\\1&0&0&0&-1&0&0&0\end{pmatrix}$,

and again the two only agree on the first column (for $|000\rangle$).

c) The operator $\mathbf{S}_{01}=(\mathbf{X}_0\mathbf{X}_1+\mathbf{Y}_0\mathbf{Y}_1)/2$ exchanges the states $|01\rangle$ and $|10\rangle$, and vanishes on the states $|00\rangle$ and $|11\rangle$. Thus $\exp(i\alpha\mathbf{S}_{01})$ is the identity on $|00\rangle$ and $|11\rangle$, and since $\mathbf{S}_{01}^2$ acts as the identity on $|00\rangle$ and $|11\rangle$, we have $\exp(i\alpha\mathbf{S}_{01})=\cos\alpha\mathbf{1}+i\mathbf{S}_{01}\sin\alpha$

on those states.[†] For $\alpha = -i\pi/2$, that gives the iSWAP: $|01\rangle \to -i|10\rangle$, $|10\rangle \to -i|01\rangle$.

d) Now we have

$$
\begin{aligned}
&\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
&\qquad \to \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle - i|100\rangle - i|101\rangle - i|010\rangle - i|011\rangle + |110\rangle + |111\rangle) \\
&\qquad \to \frac{1}{2\sqrt{2}}(|000\rangle - i|010\rangle - i|100\rangle - |110\rangle - |001\rangle - i|011\rangle - i|101\rangle + |111\rangle) \\
&\qquad = \frac{1}{2\sqrt{2}}(|00\rangle(|0\rangle - |1\rangle) - i|01\rangle(|0\rangle + |1\rangle) - i|10\rangle(|0\rangle + |1\rangle) - |11\rangle(|0\rangle + |1\rangle)) \\
&\qquad \to \frac{1}{4}((|0\rangle - i|1\rangle)(|0\rangle - i|1\rangle)(|0\rangle - |1\rangle) - i(|0\rangle - i|1\rangle)(-i|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \\
&\qquad\qquad - i(-i|0\rangle + |1\rangle)(|0\rangle - i|1\rangle)(|0\rangle + |1\rangle) - (-i|0\rangle + |1\rangle)(-i|0\rangle + |1\rangle)(|0\rangle + |1\rangle)) \\
&\qquad = \frac{1}{\sqrt{2}}\big(|000\rangle + |111\rangle\big)
\end{aligned}
$$

And again if we check any state other than $|000\rangle$, we find that the result is different for this and either of the other two circuits. Or more comprehensively, we use the definitions from parts a,b) plus the additional

Xp=(I+1j*X)/sqrt(2)

iSWAP = (kron(I,I)+kron(Z,Z))/2 - 1j*(kron(X,X)+kron(Y,Y))/2

to find

p(Xp,Xp,I).dot(kron(I,iSWAP)).dot(kron(iSWAP,I)).dot(p(Ym,Ym,Ym)

$$
= \frac{1}{\sqrt{2}}\begin{pmatrix}
1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 \\
0 & -i & 0 & 0 & 0 & i & 0 & 0 \\
0 & 0 & i & 0 & 0 & 0 & i & 0 \\
0 & 0 & -i & 0 & 0 & 0 & i & 0 \\
0 & i & 0 & 0 & 0 & i & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0
\end{pmatrix}
$$

which agrees with the other two circuits only on the first column (for $|000\rangle$).

[†] Formally, $\mathbf{S}_{01}$ satisfies $\mathbf{S}_{01}^2 = \mathbf{P}$, where $\mathbf{P} = (\mathbf{1} - \mathbf{Z}_0\mathbf{Z}_1)/2$ is the projection on the states $|01\rangle$, $|10\rangle$, so $\exp(i\alpha\mathbf{S}_{01}) = (\mathbf{1} - \mathbf{P}) + (\cos\alpha\mathbf{1} + i\mathbf{S}_{01}\sin\alpha)\mathbf{P}$.

Problem 7: 3-qubit state tomography for GHZ

a) The value of $\vec{p}$ for the state $|0\rangle$ is $(1,0,0,1)$, for the state $(|0\rangle+|1\rangle)/\sqrt{2}$ is $(1,1,0,0)$.

To estimate the expectation the value of $\mathbf{Z}$, we measure the state in the computational basis and calculate $(N_0 - N_1)/N$, where $N_{0,1}$ is the number of times 0,1 respectively are measured and $N = N_0 + N_1$ is the total number of measurements.

To estimate the expectation value of $\mathbf{X}$ in any state, recall that $R_y^{\pi/2} = (\mathbf{1} - i\mathbf{Y})/\sqrt{2}$, so that $R_y^{-\pi/2}\mathbf{Z}R_y^{\pi/2} = \mathbf{Z}(-i\mathbf{Y}) = -\mathbf{X}$, so that $\langle\psi|\mathbf{X}|\psi\rangle = -\langle\psi|R_y^{-\pi/2}\mathbf{Z}R_y^{\pi/2}|\psi\rangle$. That means we apply the operator $R_y^{\pi/2}$ to the state, then measure, and $-(N_0 - N_1)/N$ will give an estimate for $\langle\psi|\mathbf{X}|\psi\rangle$, where again $N_{0,1}$ is the number of times 0,1 respectively are measured.

To estimate the expectation value of $\mathbf{Y}$, then since $R_x^{\pi/2} = (\mathbf{1} - i\mathbf{X})/\sqrt{2}$, we have $R_x^{-\pi/2}\mathbf{Z}R_x^{\pi/2} = \mathbf{Z}(-i\mathbf{X}) = \mathbf{Y}$, so that $\langle\psi|\mathbf{Y}|\psi\rangle = \langle\psi|R_x^{-\pi/2}\mathbf{Z}R_x^{\pi/2}|\psi\rangle$. That means we apply the operator $R_x^{\pi/2}$ to the state, then measure, and $(N_0 - N_1)/N$ will give an estimate for $\langle\psi|\mathbf{Y}|\psi\rangle$, where again $N_{0,1}$ is the number of times 0,1 respectively are measured.

The general result is to apply $R_y^{\pi/2}$ or $R_x^{\pi/2}$, resp., for the expectation value of $\mathbf{X}$ or $\mathbf{Y}$, and otherwise the identity, then measure in the computational basis and calculate $(-1)^{|\mathbf{X}|}\sum_x (-1)^x N_x/N$ where N_x is the number of times the result x is measured in $N = \sum_{x=0}^{1} N_x$ trials, and $|\mathbf{X}|$ is the number of $\mathbf{X}$ operators (0 or 1 in this case).

b) With $\vec{\mathbf{P}}_{(2)}$ ordered as (II IX IY IZ XI YI ZI XX XY XZ YX YY YZ ZX ZY ZZ), the ideal values of $\vec{p}$ for $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ are $(1\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ {-1}\ 0\ 0\ 0\ 1)$, i.e., the four non-zero values are $p_{\rm II} = p_{\rm XX} = -p_{\rm YY} = p_{\rm ZZ} = 1$.

To estimate the expectation value of any element of $\vec{\mathbf{P}}_{(2)}$ for a 2-Qbit state, we apply $R_y^{\pi/2}$ or $R_x^{\pi/2}$, resp., for any Qbit that corresponds to an $\mathbf{X}$ or $\mathbf{Y}$ in the element of interest of $\vec{\mathbf{P}}_{(2)}$, and then measure in the computational basis. The expectation value is given by $(-1)^{|\mathbf{X}|}\sum_{x,y}(-1)^{x+y}N_{xy}/N$, where N_{xy} is the number of times the result xy is measured in a total of $N = \sum_{x,y=0}^{1} N_{xy}$ trials, and $|\mathbf{X}|$ is the number of $\mathbf{X}$ operators in the element of $\vec{\mathbf{P}}_{(2)}$.

c) The eight non-zero ideal values of $\vec{p}$ for $|\psi\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$ are[†]
$p_{\rm III} = p_{\rm IZZ} = p_{\rm XXX} = -p_{\rm XYY} = -p_{\rm YXY} = -p_{\rm YYX} = p_{\rm ZIZ} = p_{\rm ZZI} = 1$.

To estimate the expectation value of any element of $\vec{\mathbf{P}}_{(3)}$ for a 3-Qbit state, we apply $R_y^{\pi/2}$ or $R_x^{\pi/2}$, resp., for any Qbit that corresponds to an $\mathbf{X}$ or $\mathbf{Y}$ in the element of interest of $\vec{\mathbf{P}}_{(3)}$, and then measure in the computational basis. The expectation value is given by $(-1)^{|\mathbf{X}|}\sum_{x,y,z}(-1)^{x+y+z}N_{xyz}/N$, where N_{xyz} is the number of times the result xyz is measured in a total of $N = \sum_{x,y,z=0}^{1} N_{xyz}$ trials, and $|\mathbf{X}|$ is the number of $\mathbf{X}$ operators in the element of $\vec{\mathbf{P}}_{(3)}$.

[†] Note that the experimental values for these expectation values are given in Fig.S9 of arXiv:1402.4848 for the $N = 2$ Bell state (part a) above) and for the $N = 3,4,5$ GHZ states (only $N = 3$ asked in part c) here).

Problem 8: Quantum cakes

Work with the state

$$|\Psi\rangle = \alpha|\mathrm{BB}\rangle + \beta|\mathrm{BG}\rangle + \gamma|\mathrm{GB}\rangle + \delta|\mathrm{GG}\rangle \ .$$

where

$$|\mathrm{B}\rangle = c|\mathrm{F}\rangle + s|\mathrm{R}\rangle \ , \qquad |\mathrm{G}\rangle = -s|\mathrm{F}\rangle + c|\mathrm{R}\rangle \ ,$$

a) $|\Psi\rangle$ symmetric in the two Qbits implies that $\beta = \gamma$.

b) $\langle \mathrm{GG}|\Psi\rangle = 0$ implies that $\delta = 0$, and hence $|\Psi\rangle = \alpha|\mathrm{BB}\rangle + \beta\big(|\mathrm{BG}\rangle + |\mathrm{GB}\rangle\big)$. A relative phase rotation on the two Qbits permits taking α and β both real, and the normalization of $|\Psi\rangle$ implies that $\alpha^2 + 2\beta^2 = 1$.

[Note also that a more general rotation $U = \mathrm{e}^{i(\theta/2)\hat{n}\cdot\vec{\sigma}}$ between the $|\mathrm{F}\rangle, |\mathrm{R}\rangle$ and $|\mathrm{B}\rangle, |\mathrm{G}\rangle$ bases would give no additional degrees of freedom, since a simultaneous transformation by V on each of the basis sets induces $U \to V^\dagger U V$, and V can always be chosen to rotate $\hat{n}$ to $\hat{y}$, so that U takes the (orthogonal) form given above, in terms of real $c = \cos(\theta/2)$ and $s = \sin(\theta/2)$.]

c) $0 = \langle \mathrm{BR}|\Psi\rangle = \langle \mathrm{RB}|\Psi\rangle = \alpha\langle \mathrm{R}|\mathrm{B}\rangle + \beta\langle \mathrm{R}|\mathrm{G}\rangle = \alpha s + \beta c$

So the problem is to maximize $|\langle \mathrm{RR}|\Psi\rangle|^2 = (\alpha s^2 + 2\beta s c)^2$, subject to the constraints $\alpha s + \beta c = 0$, $\alpha^2 + 2\beta^2 = 1$, and $c^2 + s^2 = 1$. Solving those constraints gives $\alpha^2 = (1 - s^2)/(1 + s^2)$, and hence $|\langle \mathrm{RR}|\Psi\rangle|^2 = |\alpha s^2 + 2\beta s c|^2 = |-\alpha s^2|^2 = s^4(1 - s^2)/(1 + s^2)$. Setting the derivative of this quantity to zero gives the equation $s^4 + s^2 - 1 = 0$, with positive solution $s^2 = (-1 + \sqrt{5})/2$. For this value of s^2, we have

$$|\langle \mathrm{RR}|\Psi\rangle|^2 = (1 - s^2)^2/(1 + s^2) = (5\sqrt{5} - 11)/2 \approx .09017 \ .$$

(This maximum value of the violation of local causality is only slightly larger than the value $|\langle \mathrm{RR}|\Psi\rangle|^2 = .09$ for the specific state given in class. The value $\sin^2\theta = (-1 + \sqrt{5})/2$ corresponds to $\theta \approx .90456$ radians $\approx 51.83°$.)