ECE 595: Introduction to Quantum Computing
Homework 06

Warren D. (Hoss) Craft

Mon 4/6/2020

Note: References throughout the homework to "Mermin" refer to Mermin's (2007) *Quantum Computer Science: An Introduction* [1] and further bracketed citations are omitted.

(1) (10 points) In class, we argued that the probability of measuring a bit string $y_j = j2^n/r + \delta_j$ at the end of the period-finding algorithm was $\geq (4/\pi^2)/r$.

(*a*) Starting from $p(y) = \frac{1}{2^n m}\left|\sum_{k=0}^{m-1} e^{2\pi ikry/2^n}\right|^2$, show that $p(y_j) = \frac{1}{2^n m}\frac{\sin^2(\pi\delta_j mr/2^n)}{\sin^2(\pi\delta_j r/2^n)}$.

Solution. Letting $y = y_j = j2^n/r + \delta_j$, we have:

$$p(y_j) = \frac{1}{2^n m}\left|\sum_{k=0}^{m-1} e^{2\pi ikr(j2^n/r+\delta_j)/2^n}\right|^2 \tag{1}$$

where the operand for the summation can be rewritten as:

$$\begin{aligned}
e^{2\pi ikr(j2^n/r+\delta_j)/2^n} &= e^{(2\pi ijk)+(2\pi ikr)\delta_j/2^n} && (2)\\
&= e^{(2\pi ijk)}e^{(2\pi ikr)\delta_j/2^n} && (3)\\
&= [\cos(2\pi ijk) + i\sin(2\pi ijk)]e^{(2\pi ikr)\delta_j/2^n} && (4)\\
&= [1+0]e^{(2\pi ikr)\delta_j/2^n} && (5)\\
&= e^{(2\pi ikr)\delta_j/2^n} && (6)
\end{aligned}$$

where the sin and cos reduce in that way because $(2\pi ijk)$ is an integer multiple of π. Thus the summation can be rewritten as:

$$\begin{aligned}
S &= \sum_{k=0}^{m-1} e^{2\pi ikr(j2^n/r+\delta_j)/2^n} && (7)\\
&= \sum_{k=0}^{m-1} e^{2\pi ikr\delta_j/2^n} && (8)\\
&= \sum_{k=0}^{m-1} (e^{2\pi ir\delta_j/2^n})^k && (9)
\end{aligned}$$

which is a geometric sum of the form $\sum_{k=0}^{m-1} ab^k$ with $a = 1$ and $b = e^{2\pi ir\delta_j/2^n}$. Thus

$$\begin{aligned}
S &= \frac{1-(e^{2\pi ir\delta_j/2^n})^m}{1-(e^{2\pi ir\delta_j/2^n})} && (10)\\
&= \frac{1-(e^{2\pi imr\delta_j/2^n})}{1-(e^{2\pi ir\delta_j/2^n})} && (11)\\
&= \frac{1-(e^{imx})}{1-(e^{ix})} && (12)
\end{aligned}$$

where we let $x = 2\pi r\delta_j/2^n$. We can then manipulate the expression as follows (thanks, Tameem!):

$$\begin{aligned}
S &= \frac{\frac{e^{imx/2}}{e^{imx/2}} - (e^{imx/2}\, e^{imx/2})}{\frac{e^{ix/2}}{e^{ix/2}} - (e^{ix/2}\, e^{ix/2})} && (13)\\
&= \left(\frac{e^{imx/2}}{e^{ix/2}}\right) \frac{e^{-imx/2} - (e^{imx/2})}{e^{-ix/2} - (e^{ix/2})} && (14)\\
&= \left(\frac{e^{imx/2}}{e^{ix/2}}\right) \frac{(\cos(mx/2) - i\sin(mx/2)) - (\cos(mx/2) + i\sin(mx/2))}{(\cos(x/2) - i\sin(x/2)) - (\cos(x/2) + i\sin(x/2))} && (15)\\
&= \left(\frac{e^{imx/2}}{e^{ix/2}}\right) \frac{-2i\sin(mx/2)}{-2i\sin(x/2)} && (16)\\
&= \left(\frac{e^{imx/2}}{e^{ix/2}}\right) \frac{\sin(mx/2)}{\sin(x/2)} && (17)
\end{aligned}$$

The squared modulus is then:

$$\begin{aligned}
|S|^2 &= \left|\left(\frac{e^{imx/2}}{e^{ix/2}}\right) \frac{\sin(mx/2)}{\sin(x/2)}\right|^2 && (18)\\
&= \frac{\sin^2(mx/2)}{\sin^2(x/2)} \left|\left(\frac{e^{imx/2}}{e^{ix/2}}\right)\right|^2 && (19)\\
&= \frac{\sin^2(mx/2)}{\sin^2(x/2)} && (20)
\end{aligned}$$

Substituting back into Eq (1) and substituting back in for x and rearranging a bit, we have:

$$\begin{aligned}
p(y_j) &= \frac{1}{2^n m} \frac{\sin^2(m(2\pi r\delta_j/2^n)/2)}{\sin^2((2\pi r\delta_j/2^n)/2)} && (21)\\
&= \frac{1}{2^n m} \frac{\sin^2(\pi\delta_j mr/2^n)}{\sin^2(\pi\delta_j r/2^n)} && (22)
\end{aligned}$$

(b) Recall that our definition for m was the smallest integer for which $mr + x_0 \geq 2^n$, where x_0 is the smallest integer satisfying $f(x_0) = f_0$, where f_0 was the measurement result of our output register. Therefore, $mr/2^n \geq 1 - x_0/2^n$. Let us now assume that $x_0/2^n \ll 1$ and $2^n \gg 1$. Show that the dominant contribution to $p(y_j)$ is

$$p(y_j) = \frac{1}{r}\left(\frac{\sin(\pi\delta_j)}{\pi\delta_j}\right)^2 + \epsilon, \tag{23}$$

where ϵ is of the order $1/2^{2n}$.

Solution. From Mermin's Eq (3.17), we have

$$m = \left\lfloor \frac{2^n}{r} \right\rfloor \text{ or } m = \left\lfloor \frac{2^n}{r} \right\rfloor + 1 \tag{24}$$

meaning that m is within 1 unit (actually probably within $\frac{1}{2}$ unit) of $\frac{2^n}{r}$, and thus when $\frac{2^n}{r}$ is large (as Mermin points out, in fact $\frac{2^n}{r} \geq \frac{N^2}{r} > N = pq$) we have $\frac{m}{(2^n)/r} = \frac{mr}{2^n} \approx 1$. Thus the numerator in Eq (22) can be well approximated by $\sin^2(\pi\delta_j mr/2^n) \approx \sin^2(\pi\delta_j(1)) = \sin^2(\pi\delta_j)$. On the other hand, with $2^n = 2^{2n_0} \geq N^2 = p^2q^2$, 2^n is quite large and thus the operand of the trig function in the denominator of Eq (22) is quite small, so the sine term in the denominator can be replaced using $\sin(\theta) \approx \theta$. Combining these approximations then, from Eq (22) we get:

$$
\begin{aligned}
p(y_j) &= \frac{1}{2^n m} \frac{\sin^2(\pi\delta_j mr/2^n)}{\sin^2(\pi\delta_j r/2^n)} && (25) \\
&\approx \frac{1}{2^n m} \frac{\sin^2(\pi\delta_j)}{(\pi\delta_j r/2^n)^2} && (26) \\
&= \frac{(2^n)^2}{2^n mr^2} \frac{\sin^2(\pi\delta_j)}{(\pi\delta_j)^2} && (27) \\
&= \frac{2^n}{mr^2} \frac{\sin^2(\pi\delta_j)}{(\pi\delta_j)^2} && (28) \\
&\approx \frac{r}{r^2} \frac{\sin^2(\pi\delta_j)}{(\pi\delta_j)^2} && (29) \\
&= \frac{1}{r} \frac{\sin^2(\pi\delta_j)}{(\pi\delta_j)^2} && (30) \\
&= \frac{1}{r} \left(\frac{\sin(\pi\delta_j)}{\pi\delta_j} \right)^2 && (31)
\end{aligned}
$$

Thus we find that $p(y_j) = \frac{1}{r}\left(\frac{\sin(\pi\delta_j)}{\pi\delta_j}\right)^2 + \epsilon$. Now let's look more carefully at estimating the resulting error term ϵ.

Consider $\lambda = \frac{r}{2^n}$ as a small-valued parameter and consider $F(\lambda) = m\lambda = m(\frac{r}{2^n})$. The Taylor series for $F(\lambda)$ about 0 gives:

$$
\begin{aligned}
F(\lambda) &= F(0) + F'(0)\lambda + F''(0)\lambda^2 + \dots && (32) \\
&= 1 + f_1\lambda + f_2\lambda^2 + \dots && (33)
\end{aligned}
$$

where we take $F(0) = \lim_{\lambda\to 0}(m\lambda) = 1$ (because $m \to 1/\lambda$ as $\lambda \to 0$) and f_1, f_2, *etc.*, are constants. Then we can expand the sin function in the numerator of Eq (22) as:

$$
\begin{aligned}
\sin(\pi\delta_j(mr/2^n)) &= \sin(\pi\delta_j) + (\pi\delta_j\cos(\pi\delta_j))m\lambda - \frac{((\pi\delta_j)^2\sin(\pi\delta_j))}{2!}m^2\lambda^2 - \dots && (34) \\
&= \sin(\pi\delta_j) + g_1\lambda - g_2\lambda^2 - \dots && (35)
\end{aligned}
$$

where g_1, g_2, *etc.*, are constants.

Similarly, we can expand the sin function in the denominator of Eq (22) as:

$$
\begin{aligned}
\sin(\pi\delta_j(r/2^n)) &= \sin(0) + (\pi\delta_j\cos(0))\lambda - \frac{((\pi\delta_j)^2\sin(0))}{2!}\lambda^2 - \frac{((\pi\delta_j)^3\cos(0))}{3!}\lambda^3 + \dots && (36) \\
&= \pi\delta_j\lambda - h_1\lambda^3 + \dots && (37)
\end{aligned}
$$

where h_1 is a constant.

From Eq (22) then we have that

$$
p(y_j) = \frac{1}{2^n m}\left(\frac{\sin(\pi\delta_j) + g_1\lambda - g_2\lambda^2 - \dots}{\pi\delta_j\lambda - h_1\lambda^3 + \dots}\right)^2 \tag{38}
$$

which gives us the same estimate as before when using just the first terms in the numerator and denominator. Pulling out λ^2 from the denominator and then limiting ourselves to the just the first two terms in the expansions in the numerator and denominator, we have:

$$
\begin{aligned}
p(y_j) &= \frac{1}{2^n m\lambda^2}\left(\frac{\sin(\pi\delta_j) + g_1\lambda - g_2\lambda^2 - \dots}{\pi\delta_j - h_1\lambda^2 + \dots}\right)^2 && (39)\\
&\approx \frac{1}{r}\left(\frac{\sin(\pi\delta_j) + g_1\lambda}{\pi\delta_j - h_1\lambda^2}\right)^2 && (40)\\
&= \frac{1}{r}\left(\frac{\sin(\pi\delta_j)}{\pi\delta_j} + g_1\lambda - \frac{\sin(\pi\delta_j)}{\pi\delta_j}h_1\lambda^2\right)^2 && (41)\\
&= \frac{1}{r}\left(\left(\frac{\sin(\pi\delta_j)}{\pi\delta_j}\right)^2 + k\lambda + \dots\right) && (42)\\
&\approx \frac{1}{r}\left(\frac{\sin(\pi\delta_j)}{\pi\delta_j}\right)^2 + \frac{1}{r}k\lambda && (43)\\
&\approx \frac{1}{r}\left(\frac{\sin(\pi\delta_j)}{\pi\delta_j}\right)^2 + \frac{m}{2^n}k\frac{r}{2^n} && (44)\\
&\approx \frac{1}{r}\left(\frac{\sin(\pi\delta_j)}{\pi\delta_j}\right)^2 + \frac{c}{2^{2n}} && (45)\\
& && (46)
\end{aligned}
$$

Thus for small λ, we have ϵ on the order of $1/2^{2n}$. (OK — sorry, Tameem, despite your best effort to educate me there, it's clear I still don't have a good grasp on how to do that analysis. I am eager to do better and have you teach me more in that direction.)

(c) Using that $\frac{x}{\frac{1}{2}\pi} \leq \sin x$ for $0 \leq x \leq \pi/2$, show that $p(y_j) \geq (4/\pi^2)/r$. (Notice that $4/\pi^2) \approx 0.4053$.)

Solution. Since $0 \leq \delta_j \leq \frac{1}{2}$, we have $0 \leq \pi\delta_j \leq \frac{\pi}{2}$. As illustrated in Figure (1), we also know that $\sin(x) \geq \frac{2}{\pi}x$ for $0 \leq x \leq \frac{\pi}{2}$.

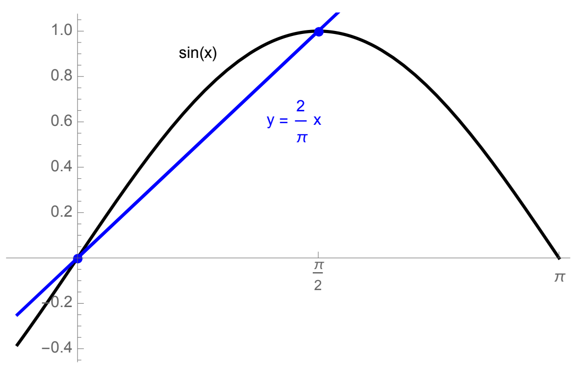

Figure 1: Illustration of the inequality $\sin(x) \geq \frac{2}{\pi}x$ for $0 \leq x \leq \frac{\pi}{2}$.

Thus from Eq (31), we have:

$$p(y_j) \approx \frac{1}{r}\left(\frac{\sin(\pi\delta_j)}{\pi\delta_j}\right)^2 \geq \frac{1}{r}\left(\frac{\frac{2}{\pi}(\pi\delta_j)}{\pi\delta_j}\right)^2 = \frac{1}{r}\left(\frac{2}{\pi}\right)^2 = \frac{4/\pi^2}{r} \approx \frac{0.4053}{r} \tag{47}$$

As Mermin points out (pg 81), since there are at least $r-1$ different values of j, and r is a large number, then the probability of getting *some* y_j value is at least $p = \frac{4/\pi^2}{r}(r-1) \approx 4/\pi^2 \approx 0.4$.

(2) Let us restrict ourselves to the very unlikely case that the period r is a power of 2, *i.e.*, $r = 2^\alpha$, where α is a positive integer.

(a) Following the same arguments in class, the most likely outcomes of measuring the input register will be $y_j = j2^{n-\alpha}$. Show that the probability of this outcome is $p(y_j) = \frac{m}{2^n} = \frac{1}{r} + \epsilon$, where ϵ is again on the order of $1/2^{2n}$.

Solution. Letting $y = y_j = j2^{n-\alpha}$, we have essentially let $\delta_j = 0$. Recalling that $\lim_{x\to 0} \frac{\sin(x)}{x} = 1$, Eq (31) gives us:

$$p(y_j) = \frac{1}{r}\left(\frac{\sin(\pi\delta_j)}{\pi\delta_j}\right)^2 = \frac{1}{r} + \epsilon = \frac{m}{2^n} + \epsilon \tag{48}$$

with the analysis of ϵ being roughly the same as before so that ϵ is once again on the order of $\frac{1}{2^{2n}}$.

(b) In this case, what is the probability of measuring any bit string that is a multiple of $2^n/r$? What is this probability if r is very large?

Solution. Notice that the number of such multiples of $2^n/r$ is $\frac{2^n-1}{2^{n-\alpha}} = 2^\alpha - 2^{\alpha-n} = r - \frac{r}{2^n}$, and thus the probability of measuring *any* of the bit strings that are multiples of $2^n/r$ is $p = \frac{1}{r}(r - \frac{r}{2^n}) = 1 - \frac{1}{2^n} \approx 1$. For r very large, the overall probability remains the same at essentially 1, but with the probability $p(y_j)$ of encountering any single specific y_j being very small (based on Eq (48)).

(c) For the case of $r = 2^\alpha$, why would it be okay to only use n_0 qubits for the input register?

Solution. Recall from part(b) above that the probability of measuring *some* bit string that is a multiple of $2^n/r$ was $p = 1 - \frac{1}{2^n} = 1 - \frac{1}{2^{2n_0}}$, which for large n_0 will still give $p \approx 1$ even if $n = n_0$ instead of $n = 2n_0$.

(d) Since r divides $(p-1)(q-1)$ if $N = pq < 2^{n_0}$, what must the form of p and q be if $r = 2^\alpha$? What are the first 3 smallest primes that satisfy this?

Solution. Let $r = 2^\alpha$ for some positive integer α. Since r divides $(p-1)(q-1)$ we know that $2^\alpha \mid (p-1)(q-1)$ and thus both $(p-1)$ and $(q-1)$ are powers of 2. Thus $p = 2^i + 1$ and $q = 2^j + 1$ for some positive integers i, j. Plugging in successive small integer values for i in the formula $2^i + 1$ gives 3 (a prime), 5 (a prime), 9 (non-prime), 17 (a prime), etc. Thus the first 3 smallest such primes are 3, 5, and 17.

References

[1] N. David Mermin. *Quantum Computer Science: An Introduction.* New York, NY: Cambridge University Press, 2007.