An example of period finding

Peter Young

(Dated: June 29, 2018)

When computers we build become quantum,
Then spies of all factions will want 'em.
Our codes will all fail,
And they'll hack our email,
But crypto that's quantum will daunt 'em.

This is a slightly modified version of a limerick by Peter and Jennifer Shor. (The original version is printed in the book by Nielsen and Chuang.) Continuing in a literary vein, on p. 453 of Nielsen and Chuang is a very well-crafted (Shakespearean) sonnet by Daniel Gottesman on error correction. It seems that quantum computing brings out latent literary qualities in scientists who work on it.

Back to the matter in hand. In this handout, we consider a simple but generic example of using period finding to factor an integer into its two prime factors. We take

$$N = pq = 91, \quad \text{with factors } p = 13, q = 7. \tag{1}$$

Choosing a random integer b which has no factors in common with 91 we take $b = 4$. First we determine the period r, which is the smallest integer such that $b^r \equiv 1 \bmod pq$. We have

$$\begin{aligned}
b &= 4 \\
b^2 &= 16 \\
b^3 &= 64 \\
b^4 &\equiv 74 \bmod pq \qquad (\text{since } 64 \times 4 = 2 \times 91 + 74) \\
b^5 &\equiv 23 \bmod pq \qquad (\text{since } 74 \times 4 = 3 \times 91 + 23) \\
b^6 &\equiv 1 \bmod pq \qquad (\text{since } 23 \times 4 = 1 \times 91 + 1)
\end{aligned} \tag{2}$$

so the period is

$$r = 6\,. \tag{3}$$

Fortunately this is even. Also fortunately $b^{r/2} + 1 = 65$ is not equivalent to 0 mod pq so one of the factors, either p or q, is the greatest common divisor of their product, N (= 91) and $b^{r/2}+1$ (= 65). The other factor of N is the greatest common divisor of N and $b^{r/2} - 1$ (= 63).

The greatest common divisor (GCD) can be determined from Euclid's algorithm as follows. Suppose we want the GCD of a_0 and b_0, say, with $a_0 > b_0$. We iterate the following expressions:

$$a_{n+1} = b_n, \tag{4a}$$

$$b_{n+1} = a_n - [a_n/b_n]\, b_n, \tag{4b}$$

for $n = 1, 2, \cdots$, where $[x]$ means the greatest integer less than or equal to x. The values of the a_n decrease, as do those of the b_n, with always $a_n > b_n$. Common factors of both numbers are preserved by this process. At some point, the smaller number b_n will have been reduced to the common factor itself so $[a_n/b_n]$ is an integer and hence $b_{n+1} = 0$. Thus, the GCD is the value of b at the iteration before it becomes zero.

Let's go through this with $a_0 = 91, b_0 = 65$:

$$\begin{aligned} a_1 &= 65, \\ b_1 &= 91 - [91/65]\, 65 = 91 - 65 = 26, \\ a_2 &= 26, \\ b_2 &= 65 - [65/26]\, 25 = 65 - 52 = 13, \\ a_3 &= 13, \\ b_3 &= 26 - [26/13]\, 13 = 26 - 26 = 0. \end{aligned} \tag{5}$$

Hence the GCD is $b_2 = 13$, which is indeed one of the factors of 91. By the same process the GCD of 63 and 91 is found to be 7, the other factor of 91.

In Shor's algorithm the period is found by Fourier transforming the function

$$f(x) = b^x \bmod pq \tag{6}$$

evaluated for $x = 0, 1, 2, \cdots, 2^n - 1$. What do we take for n? For our choice of $N = 91$, N can be represented in $n_0 = 7$ bits. According to Mermin, one should take $n = 2n_0$, to ensure that one has at least N periods in the data. (In our example we will actually have *very many* more than N periods, so we are doing a bit of an overkill.) Anyway we follow Mermin and take $n = 14$.

Now the period $r = 6$ is not a power of 2, so $2^n = 16384$ is *not* a multiple of r. Hence our range of x does not cover an exact integer number of periods. This is the usual situation. However, as explained by Mermin, if both p and q are both primes of the form $2^\ell + 1$ (an example being the commonly studied case of $N = 15$), the period *is* a power of 2, so the function to be Fourier transformed will contain an *exact* integer number of periods. In these special cases the application

of the Fourier transform to find the period is *much simpler* than the general case. Here we consider a *generic* example, where the application of the Fourier transform to find the period requires a bit more thought.

As discussed in the lecture, a measurement is made of the output register, obtaining some value for $f(x)$, say f_0. The input register will then contain a superposition of those basis states for which $f(x) = f_0$. Since $f(x)$ is periodic with period r, the possible values of x are of the form $x_0 + kr$, so, after the measurement on the output register, the state of the input register becomes

$$|\psi\rangle = \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} |x_0 + kr\rangle. \tag{7}$$

Here $x_0 < r$, $x_0 + kr < 2^n$ and the number states in the sum is

$$Q = \left[\frac{2^n}{r}\right] . \tag{8}$$

order (m)	peak position ($m\,2^n/r$)	nearest integer (y_m)	$P(y_m)$
0	0	0	0.167
1	2730.67	2731	0.114
2	5461.33	5461	0.114
3	8192	8192	0.167
4	10922.67	10923	0.114
5	13653.33	13653	0.114

TABLE I: The peak positions in the Fourier transform for the example discussed in this handout. The output is at integer values of y and the nearest integers to the peaks are shown along with the probability at those nearest integer values. Neglecting the zeroth order peak at $y = 0$, which doesn't give useful information, the sum of the other probabilities at the nearest integers is 0.623, so we have a greater than 60% probability of obtaining the nearest integer to a non-zero multiple of $2^n/r$ from which there are techniques for obtaining r.

If we were to measure $|\psi\rangle$ we would just get one value of $x_0 + kr$, which, because of the dependence on the unknown quantity x_0, does not give any information from which we might be able to determine the period r. Therefore, in order to extract information on r, we Fourier transform $|\psi\rangle$, obtaining

$$\sum_{y=0}^{2^n-1} \left(\frac{1}{\sqrt{2^n Q}} \sum_{k=0}^{Q-1} e^{2\pi i (x_0+kr) y/2^n} \right) |y\rangle \, . \tag{9}$$

The probability of getting a particular state y is given by the square of the absolute value of a term in the brackets in Eq. (9), i.e.

$$P(y) = \frac{1}{2^n Q} \left| \sum_{k=0}^{Q-1} e^{2\pi i k r y / 2^n} \right|^2 . \tag{10}$$

Note that the troublesome dependence on x_0, which gives information on the possible values of x when measuring $|\psi\rangle$, only appears as an unimportant phase factor in the Fourier transform, and this will drop out when we take the square of the absolute value to get the probabilities. If y could take real values, the exponentials would add up precisely in phase (and so there would be a peak in the probability for y), at for

$$y_m = m \frac{2^n}{r}, \tag{11}$$

where m is an integer. We emphasize that y_m is not an integer in general, but the measured values of y *are* are integers, so there will be peaks in $P(y)$ at integer values close to the y_m in Eq. (11).

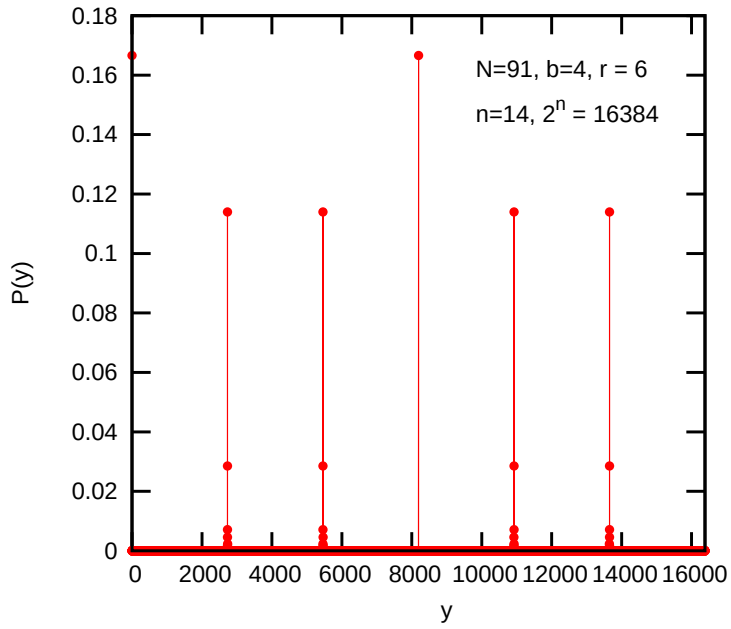

FIG. 1: Probabilities for the different components of the Fourier transformed state. There are six sharp peaks. The one at $y = 0$ doesn't give useful information. However, the probability of hitting the highest point of one of the other five peaks, i.e. the nearest integer to a non-zero multiple of $2^n/r$, is greater than 60%, see Table I. If the measurement gives one of these results, it can then be used to determine the period r, as discussed in the appendix.

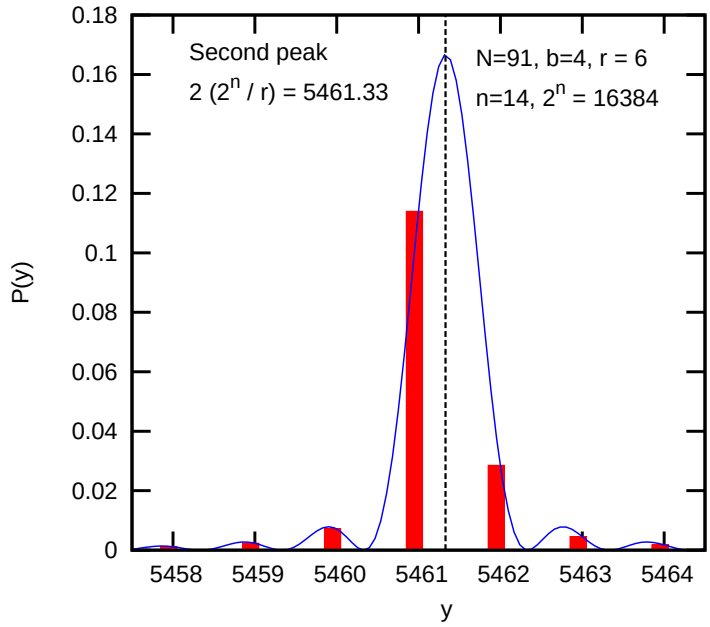

FIG. 2: A blowup of the region around the $m = 2$ peak in Fig. 1 (see also Table I). The histogram is obtained from numerical evaluation of Eq. (10). The probability is dominated by the biggest peak, the one where y is the nearest integer to $y_2 = 2 \times (2^n/r) = 5461.33$ (indicated by the vertical dashed line). The solid curve is the expression shown in Eq. (14) (with y considered to be a continuous variable).

For the example we are studying, $N = 91, r = 6, n = 14$, we have

$$\frac{2^n}{r} = 2730.67 \tag{12}$$

so

$$Q = 2730\,. \tag{13}$$

Hence there are 2730 (and a third) periods in our data. The peaks in the Fourier transform, which are at integers next to multiples of $2^n/r$ as discussed above, are shown in Table I.

I have evaluated $P(y)$ numerically from Eq. (10) and the results are shown in Fig. 1. There are $r = 6$ peaks. There is a trivial one at $y = 0$ but this can not give any useful information about the period r. The other five peaks are around integer multiples (m) of $2^n/r$. However, since the values of y are integers, one has a set of discrete values around each peak, as shown in the histogram in Fig. 2 which blows up the region around the $m = 2$ peak.

As discussed in the lecture, the sum in Eq. (10), can be evaluated, and gives, in the region of a peak, when the number of periods is large,

$$P(y) = \frac{1}{r}\left(\frac{\sin \pi\delta}{\pi\delta}\right)^2, \tag{14}$$

where

$$y = y_m + \delta \tag{15}$$

where y_m is the real number given by Eq. (11) that indicates the peak position. (Recall that y itself is an integer.) The function in Eq. (14) is plotted for continuous y as the solid curve in Fig. 2. When evaluated at integer y, it agrees very well with the values numerically computed from Eq. (10) which are shown as the histogram in Fig. 2.

Note that δ in Eq. (15) can be written as

$$\delta = \epsilon + \ell \tag{16}$$

where ℓ is an integer and $|\epsilon| < 0.5$. Note too that

$$\sum_{\ell=-\infty}^{\infty} \left(\frac{\sin(\pi(\epsilon+\ell))}{\pi(\epsilon+\ell)} \right)^2 = 1, \tag{17}$$

for arbitrary ϵ (Mathematica finds this numerically but does not seem to know it analytically). Hence, according to Eq. (14), the weight around each of the peaks in Fig. 1 is equal to $1/r$ ($= 1/6$ here). Since there are 6 peaks, the sum of all the probabilities is 1 as required. Referring to Fig. 2, the weight in the largest histogram is 0.114 which is 68% of 1/6, the total weight in all the histograms for this peak.

Appendix A: Continued Fractions

Here we discuss, using continued fractions, how to estimate the period r when the Fourier transform gives value of the integer closest to $m2^n/r$ for some integer m. We call this measured integer value y, and determined the continued fraction representation of $x = y/2^n$, which is close to m/r, where r, the period, is what we want to determine.

The continued fraction representation of x is obtained as follows. If there is an integer part of x call this c_0. Subtract c_0 from x and call the inverse of the remainder x_1, so

$$x = c_0 + \frac{1}{x_1}. \tag{A1}$$

Let the integer part of x_1 be c_1. Subtract c_1 from x_1 and call the inverse of the remainder x_2.

Continuing in the same way for c_2 and x_3 etc. we get

$$x = c_0 + \cfrac{1}{c_1 + \cfrac{1}{x_2}} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{x_3}}} \cdots = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cdots}}}. \tag{A2}$$

If x is a rational number (ratio of two integers) the continued fraction will eventually terminate. If x is irrational (like π) the continued fraction will go on for ever.

There is a theorem, see Mermin, that the best guess for x is partial sum having the largest denominator less than N. Assume that we measure the value $y = 5461$, the highest histogram for the peak in Fig. 2. Then we determine the continued fraction representation for $x = 5461/16384$. Since this is a rational fraction the continued fraction terminates and has only the following denominators

$$c_0 = 0,\ c_1 = 3,\ c_2 = 5461. \tag{A3}$$

The partial sums are $1/3$ and $5461/16384$. The latter has a denominator bigger than N $(= 91)$ so we neglect it and conclude that

$$\frac{m}{r} = \frac{1}{3}, \qquad \text{so } r = 3m\,. \tag{A4}$$

We try some small values for m, and deduce that $m = 2$ gives the period $(r = 6)$. In our case, we already know that $m = 2$ is the correct value because we chose, by hand, the $m = 2$ peak in Fig. 1, see also Fig. 2. Knowing that the period is $r = 6$, we can determine the factors of N $(= 91)$, as shown at the beginning of this handout.