Quantum Fourier transform and Shor's algorithm

August 12, 2018

1 The discrete Fourier transform

Let us start with a short summary of the definition and some of the properties of the classical discrete Fourier transform. Given an integer N, the discrete Fourier transform is usually defined to be a mapping from the space of complex sequences with N elements to itself. To simplify our notation a bit, we will denote the i-th element of a sequence of N complex numbers as $x[i]$ instead of x_i and let the index i start at zero, so that such a sequence is given by the N complex numbers $x[0], x[1], \ldots, x[N-1]$. We combine these numbers into a vector $x \in \mathbb{C}^N$.

Given such a sequence x, the discrete Fourier transform of x is defined to be the sequence X with elements

$$X[k] = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{-\frac{2\pi i}{N} jk} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \eta^{-jk}$$

where we denote by $\eta = e^{\frac{2\pi i}{N}}$ the standard N-th root of unity. Mapping vectors to vectors, we can think of the Fourier transform as a mapping

$$\mathcal{F} \colon \mathbb{C}^N \to \mathbb{C}^N$$

which is clearly linear. We will now show that this mapping is in fact unitary. For this purpose, consider the vectors u_k which are defined as follows.

$$u_k[i] = \frac{1}{\sqrt{N}} \eta^{ik}$$

Clearly, the complex conjugates of these vectors are the image of the standard basis under the discrete Fourier transform. In fact, if we consider the vector e_k defined by $e_k[j] = \delta_{jk}$, then the j-th component of the Fourier transform of this vector is

$$\begin{aligned} \mathcal{F}(e_k)[j] &= \frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} e_k[s] \eta^{-sj} \\ &= \frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} \delta_{sk} \eta^{-sj} \\ &= \frac{1}{\sqrt{N}} \eta^{jk} = u_k[j]^* \end{aligned}$$

Let us now show that the vectors u_k form an orthonormal basis of $\mathbb{C}^N$. For given k and k', we can compute the hermitian product

$$\begin{aligned}\langle u_k, u_{k'}\rangle &= \sum_{s=0}^{N-1} u_k[s]u_{k'}^*[s] \\ &= \frac{1}{N}\sum_{s=0}^{N-1} \eta^{-sk}\eta^{sk'} = \frac{1}{N}\sum_{s=0}^{N-1}\eta^{s(k'-k)}\end{aligned}$$

Now this is a geometric series with $q = \eta^{k-k'}$. If $k = k'$, then $q = 1$ and the series sums up to N, so that the hermitian product is one. If, however, $k \neq k'$, then the sum gives

$$\frac{1-q^N}{1-q}$$

according to the summation formula for a geometric series. However, as η is an N-th root of unity, $q^N = 1$ and the series sums up to zero. This proves our claim that the u_k form an orthonormal basis and at the same time demonstrates that the mapping given by the Fourier transform $\mathcal{F}$ is a unitary matrix. Also note that the Fourier coefficient $X[k]$ can be written as

$$X[k] = \sum_s x[s]u_k^*[s] = \langle x, u_k\rangle$$

Using the properties of the vectors u_k, it is also easy to find a formula for the inverse of the Fourier transform. In fact, given a vector x, we can expand x in the basis u_k and obtain

$$\begin{aligned}x &= \sum_k \langle x, u_k\rangle u_k \\ &= \sum_k X[k]u_k \\ &= \sum_k X[k]\sum_s u_k[s]e_s = \frac{1}{\sqrt{N}}\sum_k(\sum_s X[s]\eta^{sk})e_k\end{aligned}$$

where we have renamed the indices in the last line. From this result, we can immediately read off that the formula for the cofficients $x[k]$ in terms of the $X[k]$, i.e. the formula for the inverse Fourier transform, is given by

$$x[k] = \frac{1}{\sqrt{N}}\sum_s X[s]\eta^{sk}$$

This is very similar to the formula for the Fourier transform itself, up to the sign in the exponent. It is worth mentioning that some authors use this as the definition of the Fourier transform, not its inverse, but it should be clear that this is merely a convention.

2 Quantum Fourier transform

Let us now jump right back into the world of quantum computing. Imagine that we have a quantum computer with n qubits. The states of this quantum computer are then described by rays in a Hilbert space with $N = 2^n$ dimensions, namely the n-fold tensor product of the one-qubit Hilbert space. With respect to the usual standard basis labeled by the vectors $|x\rangle$, with x ranging from 0 to N-1, we can then consider any vector as a sequence, using the identification

$$x = \sum_k x[k]|x\rangle$$

To this sequence, we can apply the Fourier transform. This will give us a unitary transformation $\mathcal{F}$, described by

$$\mathcal{F}(\sum_k x[k]|k\rangle) = \sum_k X[k]|k\rangle = \frac{1}{\sqrt{N}} \sum_{s,k} x[s]\eta^{-sk}|k\rangle$$

As any unitary transformation, this transformation can be realized by a quantum circuit. In fact, one can show (see [2] and the references therein) that this can be done with a number of quantum gates that scales as $\mathrm{O}(n^2)$.

3 The quantum part of Shor's algorithm

Shor's factoring algorithm consists of classical parts and quantum parts. In this section, we take a look at the heart of the algorithm - the quantum part. Essentially, this part is about finding the period of a unit modulo M.

Suppose we are given a large number M and an element x in $\mathbb{Z}_M$, or, in other words, an integer $x \in \{0, 1, \ldots, M-1\}$. If x and M are co-prime, we know that x is a unit modulo m, thus a certain power of x will be one modulo M. The purpose of the period-finding algorithm is to find the smallest number r such that

$$x^r \equiv 1 \mod M$$

We call this number the *period* of x. To find the value of the period, we first find a power of two, i.e. some $N = 2^n$, such that $M^2 \leq N \leq 2M^2$ (in other words, n is the smallest number such that M^2 can be represented as an n-bit number). Next, we prepare a register of n+n qubits in the usual superposition

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle|0\rangle$$

which can be done by starting with the fiducial state that is zero in all qubits and then applying the Hadamard-Walsh operator.

In the next step called *modular exponentation*, we apply the operator U_f to this superposition, where f is the function $f(a) = x^a$. We know on general grounds that this can be done, and Shor demonstrates in [2] that this can be done with $\mathrm{O}(n^3)$ gates and O(n) qubits and refers to further results improving this to $\mathrm{O}(n^2 \log n \log\log n)$ gates at the cost of increasing the required space slightly.

After applying this step to our quantum state, we end up with the state $|\psi\rangle$ given by the expression

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle |x^k \mod M\rangle$$

Now there are different ways to proceed. As in the expositions given in [3] and [4], we add a measurement step to the algorithm that simplifies the arguments a bit (but is actually not needed and not done in [2])). In fact, at this point of the algorithm, we perform a measurement of the second register. Let us call the measured value y. As measuring amounts to the projection onto the eigenstates, only those components of the state $|\psi\rangle$ survice the measurement for which, in the expression above, $x^k \equiv y \mod M$. Let us denote the smallest such number by x_0. Then, after the measurement, our state will be

$$\frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle |y\rangle$$

where A is the largest number such that $x_0 + (A-1)r < N$. In particular, it follows that from $x_0 \geq 0$ and $x_0 \leq r$ that $(A-1)r < N$ and $(A+1)r > N$. At this point, we ignore the second register and focus on the first one and apply the inverse of a quantum Fourier transform to it. The resulting state will be

$$\frac{1}{\sqrt{AN}} \sum_{j=0}^{A-1} \sum_{s=0}^{N-1} \eta^{(x_0+jr)s} |s\rangle$$

Let us now reorganize this term a bit. First, we can collect all terms that contribute to the amplitude for a given value of s and find that the coefficient of $|s\rangle$ is given by

$$\frac{1}{\sqrt{AN}} \eta^{x_0 s} \left[\sum_{j=0}^{A-1} \eta^{jrs} \right]$$

Thus, if we now perform a measurement of the first register, we obtain the value s with the probability

$$P(s) = \frac{1}{AN} \left| \sum_{j=0}^{A-1} \eta^{jrs} \right|^2$$

Now, the sum can again be simplified by recognizing it as a geometric series with coefficient $q = \eta^{rs}$. If $q = 1$, which will happen exactly if s is a multiple of $\frac{N}{r}$, we find that the probability is $\frac{A}{N}$. We now claim that in general, the probability distribution given by $P(s)$ is peaked at those values of s for which $\frac{sr}{N}$ is close to an integer.

We have already seen that in case this number is exactly an integer, which happens if and only if $q = 1$, the probability is $\frac{A}{N}$. For the general case, we can therefore assume that q is not one and sum the geometric series to obtain

$$P(s) = \frac{A}{N} \left| \frac{1}{A} \frac{1 - q^A}{1 - q} \right|^2$$

We want to show that this distribution has a peak in the range of those s where $s \cdot r$ is close to a multiple of N. If we denote, for a given integer x, by $\{x\}_N$ the residual modulo N in the range between $-\frac{N}{2}$ and $\frac{N}{2}$, we can express this condition more formal as

$$-\frac{r}{2} \leq \{sr\}_N \leq \frac{r}{2}$$

How many values of s do exist that fulfill this condition? We claim that there are precisely r such values. In fact, let us follow the argument in [4] and draw the grids of integers spanned by the numbers r and N, as done in figure 1.

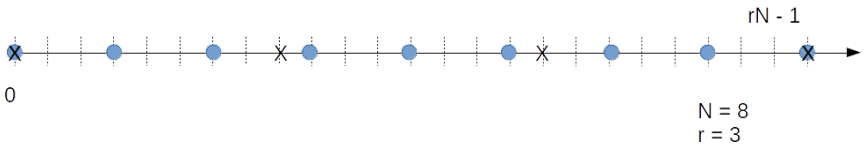

Figure 1

Here the blue bubbles mark multiples or r, i.e. points of the form sr, and the crosses mark multiples of N, i.e. points of the form kN. Now each such multiple of N is located in a stripe between two consecutive blue bubbles, and one of the bubbles will be closer than $\frac{r}{2}$ to it. Thus we can select, for each kN, a number rs such that $|rs - kN| \leq \frac{r}{2}$. Now we let k run over the r values from 0 to r - 1. This will select r corresponding values of s, and these are exactly the values for which our condition holds (if you wanted to formally prove that no s is selected twice using this procedure, you would once more need that $r \ll N$).

We will now estimate the probability P(s) in this range, using the argument given in [4]. The argument is based on the elementary geometrical observations - for which we will give proofs in the appendix - that

$$|1 - e^{i\Phi}| \geq \frac{2|\Phi|}{\pi}$$

for $\Phi \in [-\pi, \pi]$ and

$$|1 - e^{i\Phi}| \leq |\Phi|$$

for all values of Φ. Let us first try to use this to derive a lower bound for $|1 - q^A|$. We can write this as

$$|1 - q^A| = |1 - e^{2\pi i \frac{rsA}{N}}|$$

and try to apply the above estimate with $\Phi = 2\pi\frac{\{rs\}_N A}{N}$. If $\{rs\}_N$ is in the range between $-\frac{r}{2}$ and $\frac{r}{2}$, then the absolute value of this angle is at most $\pi\frac{rA}{N}$. We know that $(A-1)r \leq N$, but not necessarily that $Ar \leq N$, so we cannot apply the above bound directly.

However, there is a little trick. Let $\Phi = 2\pi\frac{\{rs\}_N}{N}$. We can then apply the estimates for the numerator and the denominator to see that

$$|\frac{1-q^{A-1}}{1-q}| \geq \frac{2(A-1)|\Phi|}{\pi}\frac{1}{|\Phi|} = \frac{2(A-1)}{\pi}$$

Using this and the reversed triangle inequality $|x+y| \geq |x| - |y|$ we can now write

$$\begin{aligned}
|\frac{1-q^{A}}{1-q}| &= |\frac{1-q^{A-1}}{1-q} + q^{A-1}| \\
&\geq |\frac{1-q^{A-1}}{1-q}| - |q^{A-1}| \\
&= |\frac{1-q^{A-1}}{1-q}| - 1 \\
&\geq \frac{2(A-1)}{\pi} - 1 = \frac{2A}{\pi} - (1+\frac{\pi}{2})
\end{aligned}$$

Squaring this, we thus find that for the values of s in the specified range, we have

$$P(s) \geq \frac{4A}{\pi^2 N} - \frac{4(1+\frac{\pi}{2})}{\pi N}$$

Now we know that $rA \approx N$, so the first term is approximately $\frac{4}{\pi^2 r}$. Further, we know that $r \leq M \ll N$ by our choice of N, so the second term is negligible. We have therefore found an approximate lower bound

$$P(s) \geq (\frac{4}{\pi^2})\frac{1}{r} - \epsilon$$

for all values of s for which $\{rs\}_N \in [-\frac{r}{2}, \frac{r}{2}]$. To obtain an estimate for s to be in that range, we need to use the fact shown above that there are precisely r values of s so that the residual falls into this range. By summing up the probabilities, we now see that with probability bounded below by $\frac{4}{\pi^2} \approx 0.4$, the measured value s will be such that $\{rs\}_N$ is in that range. This condition simply means that with probability at least 0.4, the measured value of s will be within an interval of length $\frac{1}{2}$ around an integer times $\frac{N}{r}$.

4 Finding the period

In the previous section, we have seen that with high probability, our measurement after applying the quantum Fourier transform will yield a value which is an integral multiple of $\frac{r}{N}$. Let us now see why this helps us to find the period r.

What we have shown is that with reasonable probability, our measurement will give us a value s such that there exists an integer d with

$$-\frac{r}{2} \leq rs - dN \leq \frac{r}{2}$$

Dividing this by rN gives

$$|\frac{s}{N} - \frac{d}{r}| \leq \frac{1}{2N}$$

We know the the fraction $\frac{s}{N}$, as we know s (from our measurement) and N (which we have chosen). We do not know d and r yet. However, this equation tells us that it is located in a strip of width $\frac{1}{N}$ around the known $\frac{s}{N}$.

Now two rational numbers $\frac{a}{b}$ and $\frac{c}{d}$ whose denominator is bounded by M need to have a distance of at most $\frac{1}{M^2}$ (which is an immediate consequence of the familiar formula)

$$\frac{a}{b} - cd = \frac{ad - bc}{bd}$$

As the order r we are looking for can be at least M, and $M^2 \leq N$, this shows that there is at most one fraction of the form $\frac{d}{r}$ in the region of size $\frac{1}{N}$ around $\frac{s}{N}$. As Shor points out in [2], we can therefore obtain the unknown fraction $\frac{d}{r}$ from the known fraction $\frac{s}{N}$ by looking for the nearest fraction that has denominator at most M. The situation is visualized in diagram 2.

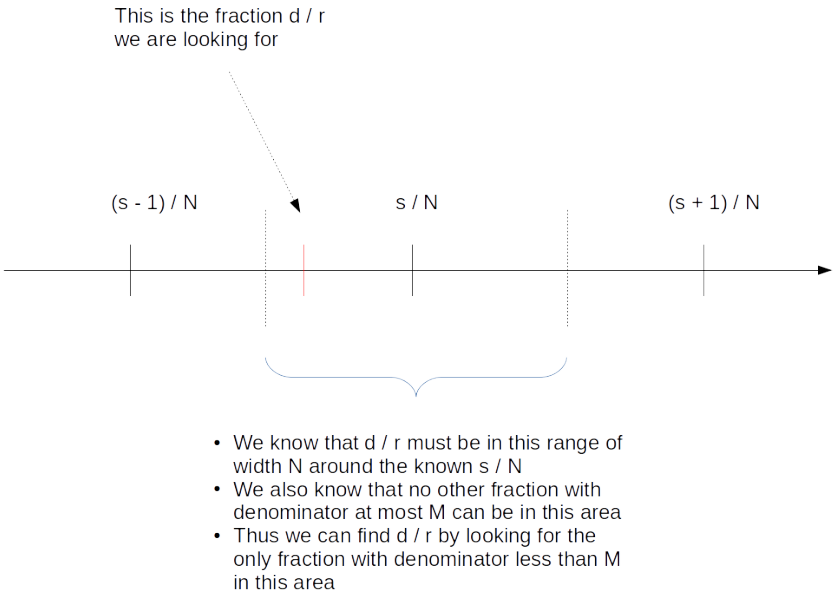

Figure 2

Now luckily, the theory of continued fractions (see [6] chapter 10 or the short summary in the appendix) provides a mechanism to calculate that approximation. In fact, we simply have to expand the number $\frac{s}{N}$ as a continued fraction and take the last convergent which has denominator smaller than M. This will then be our fraction $\frac{d}{r}$ and consequently its denominator will be the number r we are looking for.

Once we have that fraction, we can be lucky and d and r are relatively prime. If this happens, we can extract r and are done. If not, we can run our quantum algorithm once more. Shor argues in [2] that the overall success probability for the algorithm is bounded below so that a reasonably small number of iterations will succeed with a very high probability.

With these considerations, we can now summarize the algorithm for finding the period of an element x modulo M, assuming that x and M are relatively prime.

1. Choose the number n such that $N = 2^n$ is between M^2 and $2M^2$, i.e. such that M^2 can be represented with n bits.
2. Initialize the system in the state $\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle|0\rangle$
3. Apply the transform U_f with $f(x) = x^k \mod M$ to obtain the state $\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle|x^k \mod M\rangle$
4. Perform a measurement of the second register
5. Apply an inverse quantum Fourier transform to the first register
6. Measure the value of the first register and call the result s.
7. Expand the rational number $\frac{r}{N}$ into a continued fraction and find the last convergent $\frac{c}{r}$ for which the denominator r is smaller than M
8. Test whether r is the period of x. If not, start over with a new iteration

5 Omitting the intermediate measurement

Let us now see why the intermediate measurement that we have introduced before applying the quantum Fourier transform is actually not needed. Consider the state

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle|x^k \mod M\rangle$$

that our system has immediately before doing this measurement. Let us now skip this measurement and apply the quantum Fourier transform directly. This will leave our system in the state

$$\frac{1}{N} \sum_{k,s} \eta^{sk} |s\rangle|x^k \mod M\rangle$$

We now analyze the probability to find the system in the state $|s\rangle|y = x^k \mod M\rangle$ after measuring both registers. Let us denote this probability by $P(s, y)$. Arguing as before, we find that

$$P(s, y) = \frac{1}{N^2} \Big| \sum_{j=1} 1^{A-1} \eta^{sjr} \Big|^2 \Big|$$

where the symbol A has the same meaning as before - note that this now depends on y. Now, this is again a geometric series, and using arguments very similar to our previous considerations, we find that asymptotically, we can estimate this from below by

$$\frac{A^2}{N^2} \frac{4}{\pi^2}$$

given that $|rs_N| \leq \frac{r}{2}$. Note that at this point, A still depends on y. However, we also know that approximately,

$$\frac{A}{N} \approx \frac{1}{r}$$

so that, again asymptotically, we can replace our estimate by

$$\frac{4}{\pi^2}\frac{1}{r^2}$$

which is the same result that Shor obtains in [2] on page 18. Now, as the period of x is r, there are exactly r different values that x^k can take. Thus, if we want to obtain a lower bound for the probability to obtain s if we measure the first register, we need to multiply this bound by r. Again, we thus find that for all s for which $|rs_N| \leq \frac{r}{2}$, the probability to obtain s as measurement of the first register is asymptotically bounded below by

$$r \cdot \frac{4}{\pi^2}\frac{1}{r^2} = \frac{4}{\pi^2}\frac{1}{r}$$

As there are again r values of s that satisfy this condition on $\{rs\}_N$, we again obtain that with probability at least $\frac{4}{\pi^2}$, our measured value of s will be close to a multiple of $\frac{r}{N}$.

This shows that the intermediate measurement is not really needed, and we are now ready to write down the final version of Shor's algorithm for finding the period.

1. Choose the number n such that $N = 2^n$ is between M^2 and $2M^2$, i.e. such that M^2 can be represented with n bits.
2. Initialize the system in the state $\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}|k\rangle|0\rangle$
3. Apply the transform U_f with $f(x) = x^k \mod M$ to obtain the state $\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}|k\rangle|x^k \mod M\rangle$
4. Apply an inverse quantum Fourier transform to the first register
5. Measure the value of the first register and call the result s.
6. Expand the rational number $\frac{r}{N}$ into a continued fraction and find the last convergent $\frac{c}{r}$ for which the denominator r is smaller than M
7. Test whether r is the period of x. If not, start over with a new iteration

6 Factoring large numbers

We have now seen how the quantum part of Shor's algorithm can be used to obtain the period of an integer x modulo M. How would this help us to find a prime factor?

Again, we need some number theory. We claim that given a period r which is even, the greatest common divisor

$$\gcd(x^{\frac{r}{2}} - 1, M)$$

is a factor of M unless $x^{\frac{r}{2}} \equiv -1 \mod M$.

To see why this is true, let us assume the contrary, i.e. that the greatest common divisor is one, that r is even and that $x^{\frac{r}{2}} \not\equiv -1 \mod M$. We again start with the equation

$$x^r - 1 \equiv 0 \mod M$$

Assuming for a moment that the period is even, this is equivalent to

$$(x^{\frac{r}{2}} - 1)(x^{\frac{r}{2}} + 1) \equiv 0 \mod M$$

In other words, we can find an integer t such that

$$(x^{\frac{r}{2}} - 1)(x^{\frac{r}{2}} + 1) = tM$$

If now p^s is any prime power dividing M, it divides the right hand side of the equation and therefore the left hand side of the equation. As we did assume that $\gcd(x^{\frac{r}{2}} - 1, M)$ is one, no power of p does divide the first number, and therefore we obtain that p^k divides $x^{\frac{r}{2}} + 1$. As this is true for all p, we can conclude that in fact, M divides $x^{\frac{r}{2}} + 1$, a contradiction.

Thus, we can, in most cases, find a divisor of M by taking the greatest common divisor of M and $x^{\frac{r}{2}} - 1$. However, there are a few things that can go wrong. First, it might happen that r is odd, in which case this approach does not work. Second, it might be that we do in fact have that $x^{\frac{r}{2}} \equiv -1 \mod M$, so that our argument breaks down. In [2], Shor again shows that for sufficiently large values of M, a random choice of x will result in a period r for which none of these exceptions applies, i.e. that repeating the algorithm several times will give us a factor with very high probability, unless M is a prime power or M itself is even. This is not a major restriction, as there are efficient classical methods to determine factors if M is a prime power.

Having gone through this exercise, we are now finally in a position to write down the full factoring algorithm.

1. Verify that M is odd and M is not a prime power
2. Randomly pick a number x
3. If $\gcd(x, M) > 1$, we have found a factor of M. Otherwise proceed.
4. Apply the period finding algorithm detailed in the last section to find the multiplicative period r of x modulo M
5. If r is odd, start over with a new iteration using a different value of x
6. Calculate the greatest common divisor $\gcd(x^{\frac{r}{2}} - 1, M)$ and verify that this is a factor of M.

7 An example

Let us take a look at an example to see the algorithm in action. Assume that we wanted to factor the number $M = 42$. As $M^2 = 1764$, we will need 11 qubits and $N = 2048$. Now we pick our random number x, let us assume that $x = 11$ (which in fact has period six).

Using a numerical library that offers an efficient way to run a discrete Fourier transform (for instance the numpy.fft Python package), it is not difficult to calculate the probability distribution $P(s)$ to measure a value s directly by building the initial state and running a Fourier transform on it. Diagram 3 shows the result for $N = 2048, M = 42$ and $x = 11$.

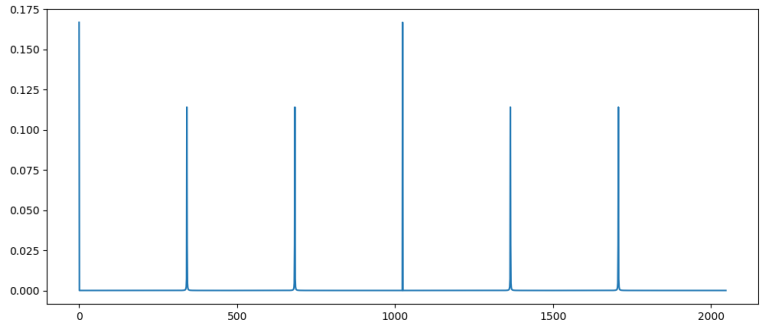

Figure 3

In this case, x actually has period 6, thus we expect peaks at multiples of $\frac{2048}{6} = 341.333$. The diagram clearly shows these peaks, located at approximately 341, 683, 1024, 1365 and 1706.

Suppose first that we measure 1365. Building the continued fraction expansion of $\frac{1365}{2048}$, we find the convergents

$$\frac{0}{1}, \frac{1}{1}, \frac{1}{2}, \frac{2}{3}, \frac{1365}{2048}$$

So our guess for the period would be $r = 3$ instead of $r = 6$. This is an example where the algorithm fails because we measure

$$1365 \approx 4 \cdot \frac{2048}{6}$$

but the fraction $\frac{4}{6}$ is not in lowest terms. However, if we measure 1707, then our continued fraction expansion will be

$$\frac{0}{1}, \frac{1}{1}, \frac{5}{6}, \frac{851}{1021}, \frac{1707}{2048}$$

The last convergent with denominator less than M now gives the correct value $r = 6$. This is even, so we can compute the greatest common divisor

$$\gcd(x^3 - 1 \mod M, M) = \gcd(28, 42) = 14$$

which yields the factor 14 of M.

Finally, let us look at a different example with a slightly larger value of M, e.g. $M = 95$. Diagram 4 shows the probability distribution for $x = 71$.

Now we already need 14 qubits, i.e. $N = 2^{14} = 16384$. Here, we again see clear peaks. If we measure, for instance, s=11833, which is the peak corresponding to $c = 13$, we obtain the continued fraction expansion

$$\frac{0}{1}, \frac{1}{1}, \frac{2}{3}, \frac{3}{4}, \frac{5}{7}, \frac{8}{11}, \frac{13}{18}, \frac{5910}{8183}, \frac{11833}{16384}$$

and $r = 18$. This is again even, and we find

$$x^9 - 1 \equiv 55 \mod M$$

which gives us the greatest common divisor 5.

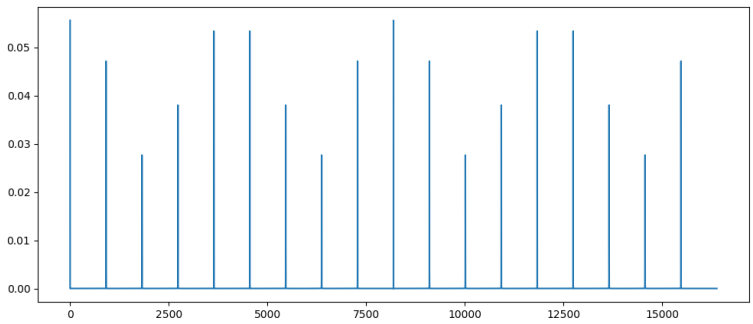

Figure 4

A Estimates for points on the circle

Here we will take a closer look at the estimates for $1 - e^{i\Phi}$ used before. First, let us try to find a bound from above. The absolute value $|1 - e^{i\Phi}|$ is the length of the straight line connecting the point 1 and the point $e^{i\Phi}$, as shown in diagram 5.

Intuitively, it is clear that this path is shorter than going around, i.e. that

$$|1 - e^{\Phi}| \leq |\Phi|$$

for all angles Φ. Formally, this can be seen as follows. First, using the Euler identities, a short calculation shows that for all angles,

$$|1 - e^{i\Phi}|^2 = 2(1 - \cos\Phi)$$

Now consider the two functions f and g given by $f(\Phi) = 2(1 - \cos\Phi)$ and $g(\Phi) = \Phi^2$. At the origin, both functions are zero. Their derivatives are both zero at the origin as well, and for their second derivatives, we have $f'' \leq g''$ for all values. As furthermore both functions are symmetric around the origin, we can conclude that $f \leq g$ everyhwere. This proves our inequality.

Next, let us try to apply a similar argument to prove our second inequality. First, we rewrite our expression for $|1 - e^{i\Phi}|$ a bit. By the additional theorem for the cosine, we have

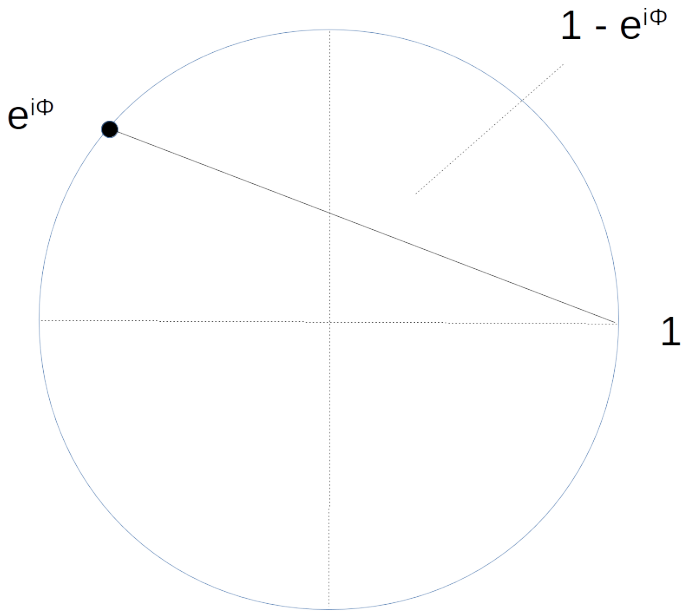

Figure 5

$$1 - \cos\Phi = 2\sin^2\frac{\Phi}{2}$$

so that we obtain the simple expression

$$|1 - e^{i\Phi}| = 2\sin\frac{\Phi}{2}$$

whenever the right hand side is non-negative. To use this to derive a lower bound, we therefore need a lower bound for the sine. So let us now consider the function F given by

$$F(x) = \sin x - \frac{2x}{\pi}$$

Clearly, this function has zeros at $x = 0$ and $x = \frac{\pi}{2}$. We claim that it does not have any zeros between these two points. There are several ways to see this. One possible argument is that the function represents the difference between the function cos and the straight line from the origin to the value of cos at $\frac{\pi}{2}$. As the cosine is concave in this region, this line is always below the graph of the cosine and does not intersect it in any other points within this interval. Thus we have shown that for $x \in [0, \frac{\pi}{2}]$, the inequality

$$\sin x \geq \frac{2x}{\pi}$$

holds. Consequently, we immediately find that for $\Phi \in [0, \pi]$, we have the inequality

$$|1 - e^{i\Phi}| = 2 \sin \frac{\Phi}{2} \geq 2 \frac{\Phi}{\pi}$$

Using the symmetry of the right hand side with respect to reflexion at the origin, we therefore finally obtain that for all $\Phi \in [-\pi, \pi]$, we have the inequality

$$|1 - e^{i\Phi}| \geq 2 \frac{|\Phi|}{\pi}$$

B Continued fractions

In this section, we briefly summarize some of the key facts about continuous fractions. The standard reference for this is still [6], chapter 10 or even the classical source [5].

For a sequence of symbols $a_0, a_1, \ldots, a_N$, we can define the continued fraction given by that sequence as the function

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

of the variables $a_0, a_1, \ldots, a_N$, which is typically abbreviated using the notation

$$[a_0; a_1, \ldots, a_N]$$

To make the notation clear, let us look at a few examples. Obviously, a continued fraction of length one is simply given by

$$[a_0] = a_0$$

A continued fraction of length two is given by

$$[a_0; a_1] = a_0 + \frac{1}{a - 1}$$

and a continued fraction of length three is given by

$$[a_0; a_1, a_2] = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{1}{a_1 a_2 + 1} = \frac{a_0 + a_2 + a_0 a_1 a_2}{a 1 a_2 + 1}$$

Given a continued fraction $[a_0; a_1, a_2, \ldots, a_N]$, we can of course, for any $m < N$, consider the continued fraction defined by taking only the first m elements of the sequence, i.e. $[a_0; a_1, a_2, \ldots, a_m]$. This expression is called the m-th *convergent* of the continued fraction. Obviously, as it is the case for the full continued fraction, each convergent is a rational function in the a_i. As such, it can be expressed as

$$[a_0; a_1, \ldots, a_m] = \frac{p_m}{q_m}$$

with polynomials p_m, q_m in the a_i. It is not difficult to write down a recurison formula for these polynomials (see Theorem 149 in [**?**]):

$$\begin{aligned} p_0 &= a_0 \\ q_0 &= 1 \\ p_1 &= a_1 a_0 + 1 \\ q_1 &= a_0 \\ p_n &= a_n p_{n-1} + p_{n-2} \quad \text{for} \quad 2 \leq n \\ q_n &= a_n q_{n-1} + q_{n-2} \quad \text{for} \quad 2 \leq n \end{aligned}$$

In case the coefficients a_i are non-negative and non-zero numbers, it is clear that this formula implies that the numbers p_m and q_m form two strictly increasing sequences. As shown in [6], the convergents behave as follows.

- The convergents $\frac{p_n}{q_n}$ with even n increase strictly
- The convergents $\frac{p_n}{q_n}$ with odd n decrease strictly
- The even convergents are bounded above by the value of the full continued fraction
- The odd convergents are bounded below by the value of the full continued fraction
- The convergents are in their lowest term

Thus, the convergents approximate the value of the full continued fraction, and the approximation gets better with increasing m.

Now suppose we start with an arbitrary rational number $\frac{p}{q}$. We can then expand this number into a continued fraction, using the Euclidian algorithm. In fact, if we write

$$p = qs + r$$

with integers s and r, we see that

$$\frac{p}{q} = s + \cfrac{1}{\cfrac{q}{r}}$$

and $r < q$. We can now proceed like this with q in place of p and r in place of q. As the remainder r gets smaller with every step and eventually reaches 1, the algorithm terminates and we obtain our desired continuous fraction expansion. This is maybe best explained using an example. Suppose we wanted to expand $\frac{5}{3}$. We would then first write

$$5 = 1 \cdot 3 + 2$$

so that

$$\frac{5}{3} = 1 + \cfrac{1}{\cfrac{3}{2}}$$

Now we do the same with $\frac{3}{2}$. We have

$$3 = 1 \cdot 2 + 1$$

so that

$$\frac{3}{2} = 1 + \frac{1}{2}$$

We thus find that

$$\frac{5}{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2}} = [1, 1, 2]$$

and the algorithm terminates.

Now given any rational number $x = \frac{p}{q}$, we can form the convergents of the (finite) continued fraction expansion of x. The convergents then give us a sequence $\frac{p_n}{q_n}$ of rational numbers with strictly increasing denominator. Thus if we wanted to find an approximation of x by a fraction $\frac{p'}{q'}$ with a denominator smaller than some number b, we could form the n-th convergents until $q_{n+1} \geq b$ and use $\frac{p_n}{q_n}$ as an approximation. In fact, as shown in [6] (Theorem 181), this approximation is in some sense the best possible approximation to x with that constraint for the denominator.

References

[1] M.A. Nielsen, I.L. Chaung, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2010

[2] P. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J.Sci.Statist.Comput. Vol. 26 Issue 5 (1997), pp 1484–1509, available as arXiv:quant-ph/9508027v2

[3] R. Jozsa, *Quantum Algorithms and the Fourier Transform*, arXiv:quant-ph/9707033

[4] J. Preskill, *Quantum computation*, Lecture notes (PH229), chapter 6, available online at `http://www.theory.caltech.edu/people/preskill/ph229/`

[5] O. Perron, *Die Lehre von den Kettenbrüchen*, Teubner Verlag, Leipzig, 1913, available online at `https://archive.org/details/dielehrevondenk00perrgoog`

[6] G.H. Hardy, E.M. Wright, *An introduction to the theory of numbers*, Oxford University Press, Oxford, 1975