F. THE QUANTUM FOURIER TRANSFORMATION AND SHOR'S ALGORITHM

F1

Die Quanten-Fouriertransformation.

$m \in \mathbb{N}_0$, $q = 2^m$. Die QFT ist durch ihre Wirkung auf die Basis $\mathcal{B} = \{ |x\rangle_m : x \in \{0, \dots, q-1\}\}$ festgelegt*):

$$\mathcal{F} |x\rangle_m = \frac{1}{\sqrt{q}} \sum_{y=0}^{q-1} e^{2\pi i \frac{xy}{q}} |y\rangle_m$$

Es gilt ~~∀x,x'~~ $\forall x, x' \in \{0, \dots, q-1\}$ $\langle \mathcal{F} x | \mathcal{F} x' \rangle = \langle x | x' \rangle$, also ist $\mathcal{F}$ unitär.

*) (und durch die Forderung der Linearität)

$m=1$:

$$\mathcal{F}|x\rangle_1 = \frac{1}{\sqrt{2}}\sum_{y=0}^{1} e^{2\pi i \frac{xy}{2}} |y\rangle_1 = \frac{1}{\sqrt{2}}\sum_{y=0}^{1} (-1)^{xy} |y\rangle_1$$

$$= H|x\rangle_1 \qquad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ Hadamardgatter.}$$

$m=2$

$$\mathcal{F}|x\rangle_2 = \frac{1}{2}\sum_{y=0}^{3} e^{2\pi i \frac{xy}{4}} |y\rangle_2$$

$$\left.\begin{array}{l} x = x_0 + 2x_1 \\ y = y_0 + 2y_1 \end{array}\right\} \quad xy = x_0y_0 + 2(x_1y_0 + x_0y_1) + 4x_1y_1$$

$$\frac{xy}{4} = y_0 \cdot \left(\frac{x_1}{2} + \frac{x_0}{4}\right) + y_1 \cdot \frac{x_0}{2} + x_1y_1$$

$$e^{2\pi i \frac{xy}{4}} = e^{2\pi i \, y_0(x_1 2^{-1} + x_0 2^{-2})} \, e^{2\pi i \, y_1 \cdot x_0 \cdot 2^{-1}} \qquad \left(e^{2\pi i x_1 y_1} = 1\right)$$

Notation: $x_1 2^{-1} + x_0 2^{-2} = 0.x_1x_0$

$x_0 \cdot 2^{-1} = 0.x_0$

Die Summation $y \in \{0,1,2,3\}$ entspricht einer Summation über $y_0, y_1 \in \{0,1\}$, und $|y\rangle_2 = |y_1\rangle_1 \otimes |y_0\rangle_1$. Also ist

$$\mathcal{F}|x_1x_0\rangle_2 = \frac{1}{2} \cdot \sum_{y_0=0}^{1} \sum_{y_1=0}^{1} e^{2\pi i y_0 \cdot 0.x_1x_0} \, e^{2\pi i y_1 \cdot 0.x_0} \, |y_1\rangle_1 \otimes |y_0\rangle_1$$

$$= \frac{1}{\sqrt{2}} \sum_{y_1=0}^{1} e^{2\pi i y_1 \cdot 0.x_0} \, |y_1\rangle_1 \otimes \frac{1}{\sqrt{2}} \sum_{y_0=0}^{1} e^{2\pi i y_0 \, 0.x_1x_0} |y_0\rangle_1$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i \, 0.x_0} \, |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i \, 0.x_1x_0} |1\rangle\right)$$

Allgemein ist

$$2^{-m} xy = y \cdot \frac{x}{2^m} = \underbrace{y}_{y_0 + 2y_1 + \dots + 2^{m-1} y_{m-1}} \cdot (0.x_{m-1} \dots x_2 x_1 x_0)$$

$$= y_0 (0.x_{m-1} \dots x_0) + y_1 (x_{m-1}.x_{m-2} \dots x_0) + \dots + y_{m-1} \cdot (x_{m-1} \dots x_1 . x_0)$$

$$e^{2\pi i} = 1 \Rightarrow e^{2\pi i \frac{xy}{2^m}} = e^{2\pi i \left[y_0 \cdot (0.x_{m-1} \dots x_0) + y_1 \cdot (0.x_{m-2} \dots x_0) + \dots + y_{m-1} (0.x_0) \right]}$$

$$= e^{2\pi i \sum_{k=0}^{m-1} y_k \cdot (0.x_{m-1-k} \dots x_0)}$$

also

$$\mathcal{F} |x\rangle_m = 2^{-\frac{m}{2}} \sum_{y_0, \dots y_{m-1} = 0}^{1} e^{2\pi i \sum_{k=0}^{m-1} y_k \cdot (0.x_{m-1-k} \dots x_0)} |y_0\rangle \otimes \dots \otimes |y_{m-1}\rangle$$

$$= \bigotimes_{k=0}^{m-1} \frac{1}{\sqrt{2}} \sum_{y_k=0}^{1} e^{2\pi i \, y_k \cdot (0.x_{m-1-k} \dots x_0)} |y_k\rangle$$

$$= \bigotimes_{k=0}^{m-1} \frac{1}{\sqrt{2}} \left[|0\rangle + e^{2\pi i \cdot (0.x_{m-1-k} \dots x_0)} |1\rangle \right]$$

F5

$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\, 0.x_1x_0}\,|1\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle + \underbrace{e^{i\pi x_1}}_{(-1)^{x_1}} \cdot e^{i\frac{\pi}{2}x_0}\,|1\rangle\right)$$

<u>$x_0 = 0$:</u> $$\frac{1}{\sqrt{2}}\cdot\left(|0\rangle + (-1)^{x_1}|1\rangle\right) = \left\{\begin{array}{ll} \frac{|0\rangle+|1\rangle}{\sqrt{2}} & x_1 = 0 \\ \frac{|0\rangle-|1\rangle}{\sqrt{2}} & x_1 = 1 \end{array}\right\} = H|x_1\rangle$$

$x_0 = 1$ $$\frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_1}\cdot \underbrace{e^{i\frac{\pi}{2}}}_{i}\,|1\rangle\right)$$

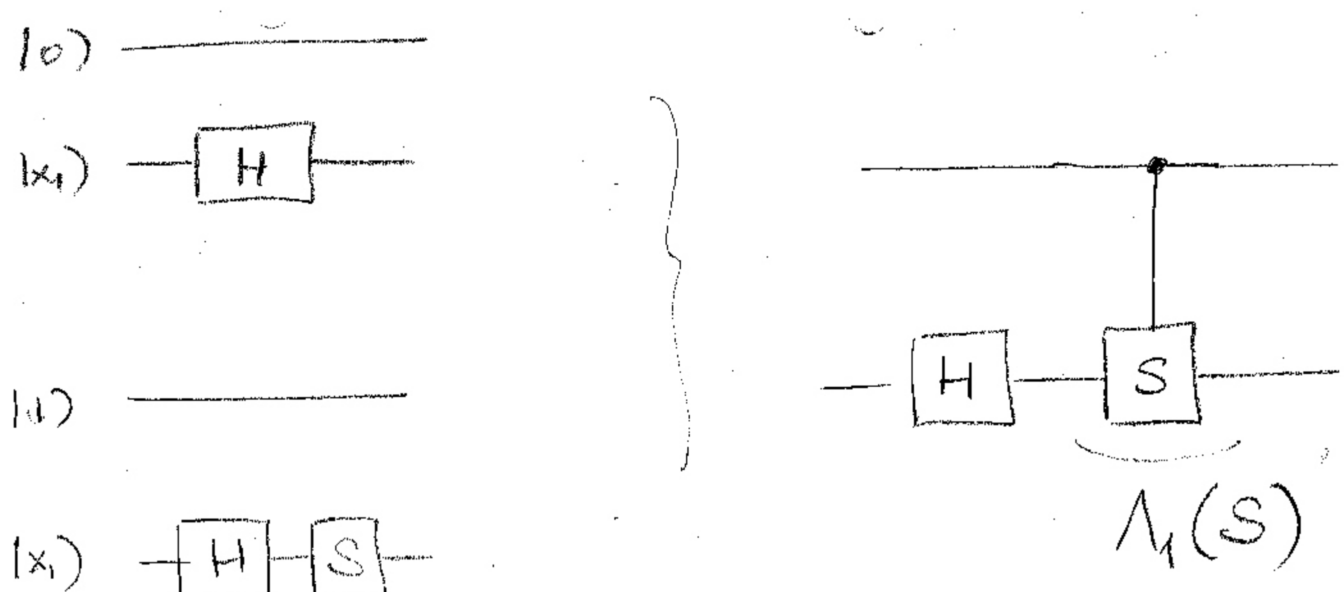
$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad S|y\rangle = \begin{cases} |y\rangle & y=0 \\ i|y\rangle & y=1 \end{cases}$$

$$SH|x_1\rangle = S\frac{1}{\sqrt{2}}\sum_{y=0}^{1}(-1)^{x_1y}|y\rangle = S\,\frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_1}|1\rangle\right)$$

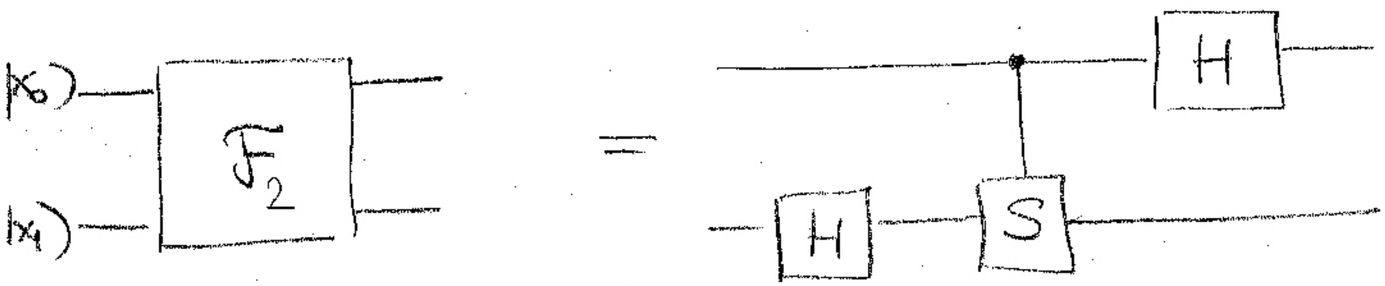
$$= \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_1}\cdot i\,|1\rangle\right)$$

$x_0 = 0$:

$x_0 = 1$



Also



F.2 Some Elementary Number Theory.

$a, b \in \mathbb{N}$. If $\gcd(a,b) = d$, then there are $v, w \in \mathbb{Z}$ such that

$$d = va + w \cdot b$$

In particular,

$$bw \equiv d \bmod a.$$

This is proven using Euclid's algorithm (see homework 10.4).
Euclid's algorithm is fast, i.e. polynomial in the number of bits of a and b.

Special case: if $\gcd(m,n) = 1$ [this is usually written as $(m,n) = 1$]

then there is $k \in \mathbb{N}$ with $k \cdot m \equiv 1 \bmod n$.

For $n \in \mathbb{N}$, Euler's Φ-function is defined as

$$\Phi(n) = |T_n| \quad \text{where} \quad T_n = \{ m \in \{1, \dots, n-1\} : (m,n) = 1 \}.$$

Theorem (Euler): $n, b \in \mathbb{N}$, $(n, b) = 1$. Then

$$b^{\Phi(n)} \equiv 1 \mod n$$

Definition: $n, b \in \mathbb{N}$, $(n, b) = 1$. The smallest number $r \in \mathbb{N}$ with

$$b^r \equiv 1 \mod n$$

is called the period of b modulo n.

Let $p, q \in \mathbb{P}$, $p \neq q$, and $N = pq$

Let $c \in \mathbb{N}$ with $(c, (p-1)(q-1)) = 1$ and $d \in \mathbb{N}$ with $cd \equiv 1 \mod (p-1)(q-1)$

Let $(b, N) = 1$ and r be the period of b.

Lemma 1. (a) $\forall a \in \mathbb{N}, \ell \in \mathbb{Z}: \; a^{1+\ell(p-1)(q-1)} \equiv a \mod (pq)$

(b) $(c, r) = 1$, i.e. $\exists d \in \mathbb{N}: \; cd \equiv 1 \mod r$.

Theorem 1 For $N = pq$, $p, q \in \mathbb{P}$, $p \neq q$

$$\liminf_{N \to \infty} \frac{\Phi(N)}{\frac{N}{\log \log N}} = e^{-\gamma}$$

where $\gamma = 0.5772\ldots$ is the Euler-Mascheroni constant

$$\gamma = -\int_0^1 \ln|\ln x|\, dx.$$

Corollary. For large enough $N = pq$, $(p \neq q)$

$$\frac{\Phi(N)}{N} \geq \frac{0.5}{\log \log N}$$

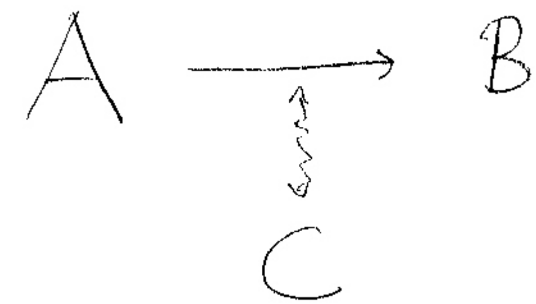
In other words: for any $y \in \{1, \dots, N-1\}$, the probability that $(y, N) = 1$ is at least $\frac{0.5}{\log \log N}$.

(so even for $N \sim 2^{(10^6)}$, this probability is $> \frac{1}{15}$)

Hence: given $N = pq$, $p, q \in \mathbb{P}$, $p \neq q$, a number $y \in \{1, \dots, N\}$ with $(y, N) = 1$ can be found very quickly

F.3 RSA Encryption

Public key cryptography: to receive messages from anyone, B just keeps two keys, a public and a private one.



B picks two large primes p and q, ~~sets~~ $N = pq$, and chooses a large number c with $(c, (p-1)(q-1)) = 1$, then calculates d with $cd \equiv 1 \mod (p-1)(q-1)$.

B publishes c and N but keeps p, q, and d secret.

To send the message $a \in \{0, \ldots, N-1\}$ encrypted to B, A calculates $b = a^c \bmod N$ and publishes b. *)

B decrypts this message by taking $b^d = a^{cd} \equiv a \mod N$

*) calculating $b = a^c \bmod N$ can also be done fast.

Reason: $cd = 1 + \ell \cdot (p-1)(q-1)$ with $\ell \in \mathbb{Z}$, so

$$a^{cd} = a^{1+\ell(p-1)(q-1)} \equiv a \bmod N$$

by Lemma 1.(a).

C can attempt to find p and q from $N = pq$ but this takes a long time, even with the best current algorithms.

But: if C manages to find the period r of b modulo N, then, by Lemma 1(b), $(c, r) = 1$, so there is $d' \in \mathbb{N}$ with $cd' \equiv 1 \bmod r$, i.e. $cd' = 1 + r \cdot \ell'$, $\ell' \in \mathbb{Z}$, and

$$b^{d'} = a^{cd'} = a^{1+r\ell'} = a \cdot (a^r)^{\ell'} \equiv a \bmod N$$

so C has then cracked RSA. [Here we also used that b and a have the same period mod N]

F.4 Shor's algorithm.

Task: given $N \in \mathbb{N}$ (large) and $b \in \mathbb{N}$ (large) with $(b, N) = 1$,
find r such that $b^r \equiv 1 \mod N$, r minimal. (certainly, $r \leq N-1$)

"large" here means a large number of bits, $N \sim 2^\beta$
In today's RSA, $\beta \gtrsim 10^3$.

Let $f(x) = b^x \mod N$. $(x \in \{1, \ldots, N-1\})$. $f(r) = 1$.

f can be calculated fast on a classical computer, hence also on a quantum computer.

Step 0: (remove small r) Calculate $f(x)$ for $x \in \{1, \ldots, 1000\}$ (say).
This will find r if $r \leq 1000$.

Because N is so large, going on by this method will take an exponentially long time in the number of bits β.

Step 1. (Preparation)

Choose $m \in \mathbb{N}$ such that $q = 2^m > N^2$ (i.e. $m > 2\beta$).

Let U_f be the unitary implementing f, i.e.

$$U_f(|x\rangle_m \otimes |y\rangle_m) = |x\rangle_m \otimes |y \oplus_2 f(x)\rangle_m.$$

Prepare the $2m$ qbits in the state $|0\rangle_m \otimes |0\rangle_m$, and calculate

$$U_f\left[\left(H^{\otimes m}|0\rangle_m\right) \otimes |0\rangle_m\right] = \frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} |x\rangle_m \otimes |f(x)\rangle_m.$$

Do a measurement on the second register.

It returns a random value f_0

There is $x_0 \in \{0, \dots, r-1\}$ with $f_0 = f(x_0)$.

Because f is periodic, there are many more x with $f_0 = f(x)$,

namely

$$x = x_0 + k \cdot r \quad , \quad k \in \{0, \dots, n-1\}$$

where $n = \max\{k \in \mathbb{N}_0 : x_0 + kr < 2^m - 1\}$ (thus $n = \left[\frac{q}{r}\right]$ or $\left[\frac{q}{r}\right] + 1$)

After this measurement, the state is

$$\frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} |x_0 + k \cdot r\rangle_m \otimes |f_0\rangle_m =: |\Psi\rangle_m \otimes |f_0\rangle_m$$

the state gets a new normalization after measurement (conditional probabilities!)

$|x\rangle \otimes |f_0\rangle$ and $|x'\rangle \otimes |f_0\rangle$ are orthonormal for $x \neq x'$

Because the result for f_0 is random, there is no obvious way of getting r by taking differences of several measurements, because also the "offset" x_0 is random.

But periods of a function are easily detected using the Fourier transform, irrespective of x_0

Step 2. (Quantum Fourier transform)

Apply the Q.F.T. : $\mathcal{F}_m |\Psi\rangle_m$ and do a measurement.

The result is a number $y \in \{0, \dots, q-1\}$.

Then, with probability $\geq \frac{1}{5}$,

$$\frac{y}{q} = \frac{j}{r}$$

where $j \in \mathbb{N}$ satisfies $(j, r) = 1$.

Thus, after cancelling common factors in the numerator and denominator of the fraction $\frac{y}{q}$, the denominator is r, with probability $\geq \frac{1}{5}$.

Check if r is the period. If not, run the algorithm again.

The probability to fail t times is $\left(\frac{4}{5}\right)^t \xrightarrow[t \to \infty]{} 0$.

Explanation of Step 2.

We had $|\Psi\rangle_m = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} |x_0 + kr\rangle_m$

(we omit the factor $|f_0\rangle_m$ because it plays no role any more)

$$F_m |\Psi\rangle_m = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} F_m |x_0 + kr\rangle_m \qquad (q = 2^m)$$

$$= \frac{1}{\sqrt{nq}} \sum_{k=0}^{n-1} \sum_{y=0}^{q-1} e^{2\pi i \frac{(x_0+kr)\cdot y}{q}} |y\rangle_m$$

$$= \frac{1}{\sqrt{q}} \sum_{y=0}^{q-1} e^{\frac{2\pi i x_0 y}{q}} |y\rangle_m \cdot \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} e^{2\pi i \frac{kry}{q}}$$

$$= \sum_{y=0}^{q-1} a_y \cdot |y\rangle_m$$

with $a_y \in \mathbb{C}$, $|a_y|^2 = p_y$ the probability of finding y when measuring.

Note that x_0 already appears only in the phase of a_y, hence drops out in P_y.

$2\pi \frac{ry}{q} =: \alpha \quad \Rightarrow$ the inner sum is a geometric series

$$g_n(\alpha) = \sum_{k=0}^{n-1} e^{i\alpha k} = \begin{cases} n & \alpha \text{ a multiple of } 2\pi \\ \dfrac{e^{i\alpha n} - 1}{e^{i\alpha} - 1} & \text{otherwise.} \end{cases}$$

Thus

$$|g_n(\alpha)|^2 = \left| \frac{\sin \frac{\alpha n}{2}}{\sin \frac{\alpha}{2}} \right|^2$$

Therefore, when measuring, find y with probability

$$P_y = \frac{1}{n \cdot q} \frac{\sin^2\left(n\pi \frac{ry}{q}\right)}{\sin^2\left(\pi \frac{ry}{q}\right)}$$

Lemma 2. Let $\mathcal{Y} = \{ y \in \{0, \dots, q-1\} : \exists j \in \mathbb{N}_0,\ \delta \in [-\tfrac{1}{2}, \tfrac{1}{2}] :$
$y = \frac{q}{r} j + \delta \}$

Then $|\mathcal{Y}| \geq r-1$, and the probability to find $y \in \mathcal{Y}$ satisfies

$$P_y \geq \frac{1}{r} \left(\frac{2}{\pi}\right)^2 \geq \frac{0.405}{r}$$

Hence, with probability $p(\mathcal{Y}) \geq 0.4$, the measured value is in $\mathcal{Y}$.

Proof.

Suppose $y = j\frac{q}{r} + \delta_j$ (since $y \in \mathbb{N}_0$, $\delta_j \neq 0$ in general.
$\delta_j = \frac{ry}{q} - \left[\frac{ry}{q}\right] \in \left[-\frac{1}{2}, \frac{1}{2}\right)$).

Then $\sin\left(n\pi \frac{r}{q} y\right) = \sin\left(n\pi + n\pi \frac{r}{q}\delta_j\right)$

$= (-1)^{n\pi} \sin\left(n\pi \frac{r}{q}\delta_j\right)$

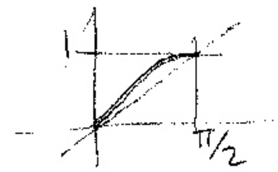
so $$p_y = \frac{1}{nq} \frac{\sin^2\left(n\pi \frac{r}{q}\delta_j\right)}{\sin^2\left(\pi \frac{r}{q}\delta_j\right)}$$

Because $q > N^2$, $\pi \frac{r}{q}\delta_j \leq \frac{\pi}{2} \cdot \frac{r}{q} \overset{r \leq N}{\leq} \frac{\pi}{2} \frac{1}{N} \ll \frac{\pi}{2}$.

Because $|\sin x| \leq |x|$,

$$p_y \geq \frac{1}{nq} \cdot \frac{\sin^2\left(n\pi \frac{r}{q}\delta_j\right)}{\left(\pi \frac{r}{q}\delta_j\right)^2}$$

For $|x| \le \frac{\pi}{2}$, $|\sin x| \geqslant \frac{2}{\pi}|x|$



$$p_y \geqslant \frac{1}{nq} \frac{\left(n\pi \frac{r}{q}\delta_j\right)^2}{\left(\pi \frac{r}{q}\delta_j\right)^2} \left(\frac{2}{\pi}\right)^2 \quad \text{because} \quad \left|n\pi \frac{r}{q}\delta_j\right| \le \frac{\pi}{2}\left|\frac{nr}{q}\right| \le \frac{\pi}{2}.$$

$$\geqslant \frac{n}{q}\cdot\left(\frac{2}{\pi}\right)^2$$

Recall $\quad \frac{q}{r} - 1 \le n \le \frac{q}{r} + 1$

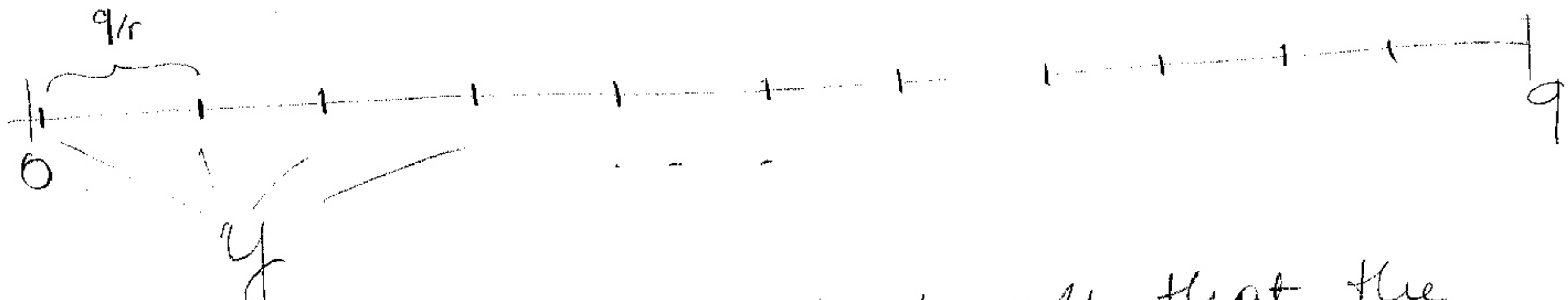
Thus $\quad 1 - \frac{r}{q} \le \frac{n \cdot r}{q} \le 1 + \frac{r}{q} \quad$ and $\quad \frac{n}{q} \geq \frac{1}{r}$

hence $\quad \frac{n}{q} \geqslant \frac{1}{r}\left(1 - \frac{r}{q}\right) \geqslant \frac{1}{r}\left(1 - \frac{1}{r}\right) \quad$ since $\quad q > N^2 \geq r^2$

So, for $r \geqslant 100$, $\frac{n}{q} \geqslant 0.99\frac{1}{r}$ and thus $p_y \geqslant \frac{1}{r}\cdot 0.405 \cdot 0.99 \geqq \frac{0.4}{r}$.

The fact that $|Y| \geqq r-1$ is obvious. $\blacksquare$

Lemma 2 can be visualized as follows



The Q.F.T. is so strongly peaked at $y \in Y$ that the probability of finding $y \in Y$ in the measurement is $\geq \frac{2}{5}$.

The picture also makes $|Y| \geq r-1$ clear.

The rest of the argument for step 2 is now simple:

$$\frac{y}{q} - \frac{j}{r} = \frac{\delta_j}{q}, \text{ so } \left|\frac{y}{q} - \frac{j}{r}\right| \leq \frac{1}{2q}$$

but if the two were different, then

$$\left|\frac{y}{q} - \frac{j}{r}\right| = \left|\frac{yr - jq}{qr}\right| \geq \frac{1}{qr} \underset{r \geq 1}{\geq} \frac{1}{q}$$

Thus $\frac{y}{q} = \frac{j}{r}$. It remains to see how likely it is to have $(r,j) = 1$.

Lemma 3

$$\text{Prob}\left((j,r) = 1 \right) \geq \frac{1}{2}.$$

Proof. $\mathrm{Prob}(2 \mid r) = \frac{1}{2}$ and $\mathrm{Prob}(2 \mid j) = \frac{1}{2}$

$$\Rightarrow \mathrm{Prob}(2 \nmid r \text{ or } 2 \nmid j) = 1 - \mathrm{Prob}(2 \mid r \text{ and } 2 \mid j) = 1 - \frac{1}{2^2} = \frac{3}{4}$$

$$\mathrm{Prob}(3 \nmid r \text{ or } 3 \nmid j) = 1 - \mathrm{Prob}(3 \mid r \text{ and } 3 \mid j) = 1 - \frac{1}{3^2} = \frac{8}{9}.$$

$$\mathrm{Prob}(\text{no common prime factors } p \leq P) = \prod_{\substack{p \in \mathbb{P} \\ p \leq P}} \left(1 - \frac{1}{p^2}\right) \geqslant \underbrace{\prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^2}\right)}_{\text{convergent infinite product}}$$

$$= \frac{6}{\pi^2} = 0.6079\ldots > 0.5. \qquad \square$$

Thus in summary

$$\mathrm{Prob}(\text{success for Shor}) \geq \frac{2}{5} \cdot \frac{1}{2} = \frac{1}{5}.$$