Quantum Computation (484)

Mario Berta, Herbert Wiklicky

m.berta@imperial.ac.uk
Autumn 2018

The Function $f_{a,N}$

We are interested in the following function

$$f_{a,N}(x) = a^x \bmod N$$

more precisely its so-called **period**.

We are interested in the smallest r such that

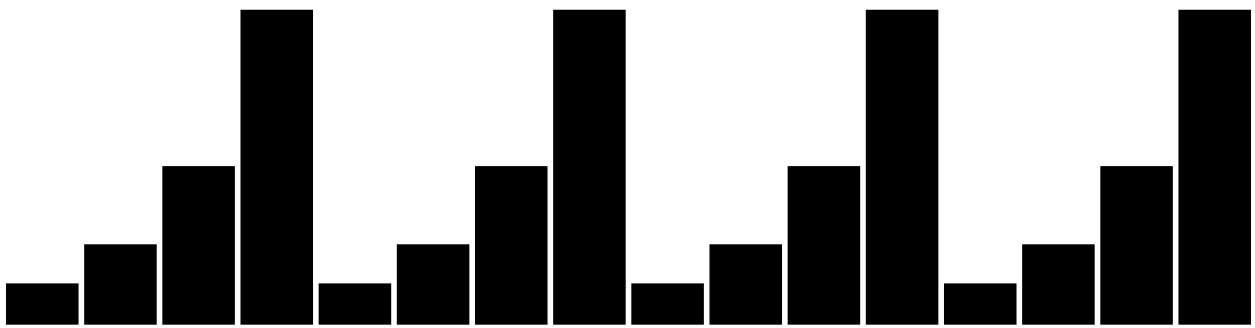
$$f_{a,N}(r) = a^r \bmod N = 1$$

From Number Theory: If a and N are **co-prime** – i.e. the greatest common divisor $GCD(a, N) = 1$ – then $r \leq N$ and we know

$$f_{a,N}(r + s) = f_{a,N}(s)$$

Example: $f_{2,15}$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	...
$f_{2,15}$	1	2	4	8	1	2	4	8	1	2	4	8	1	...

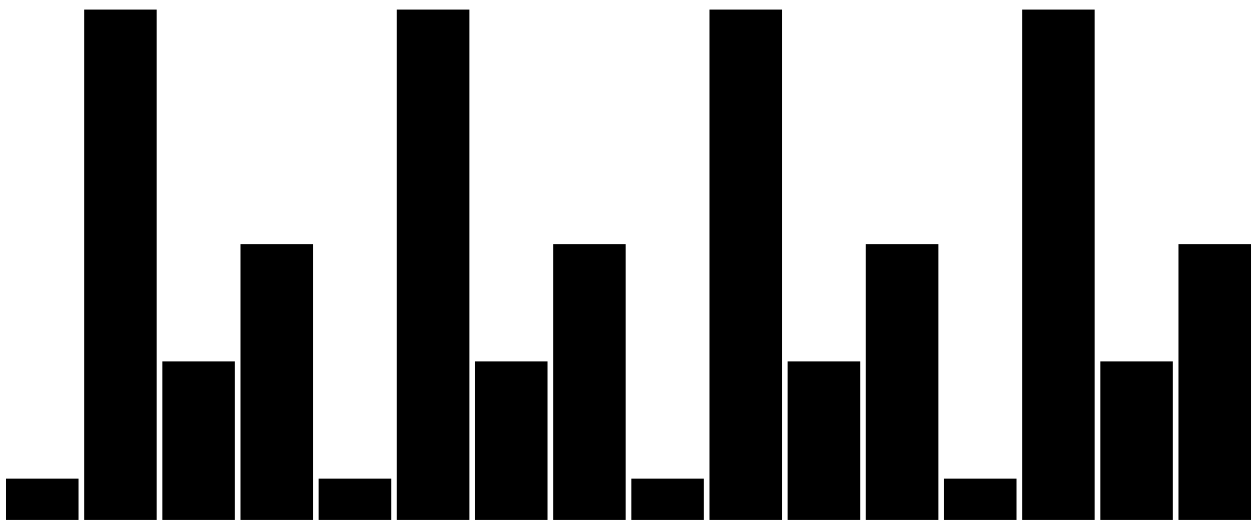


Example: $f_{4,15}$

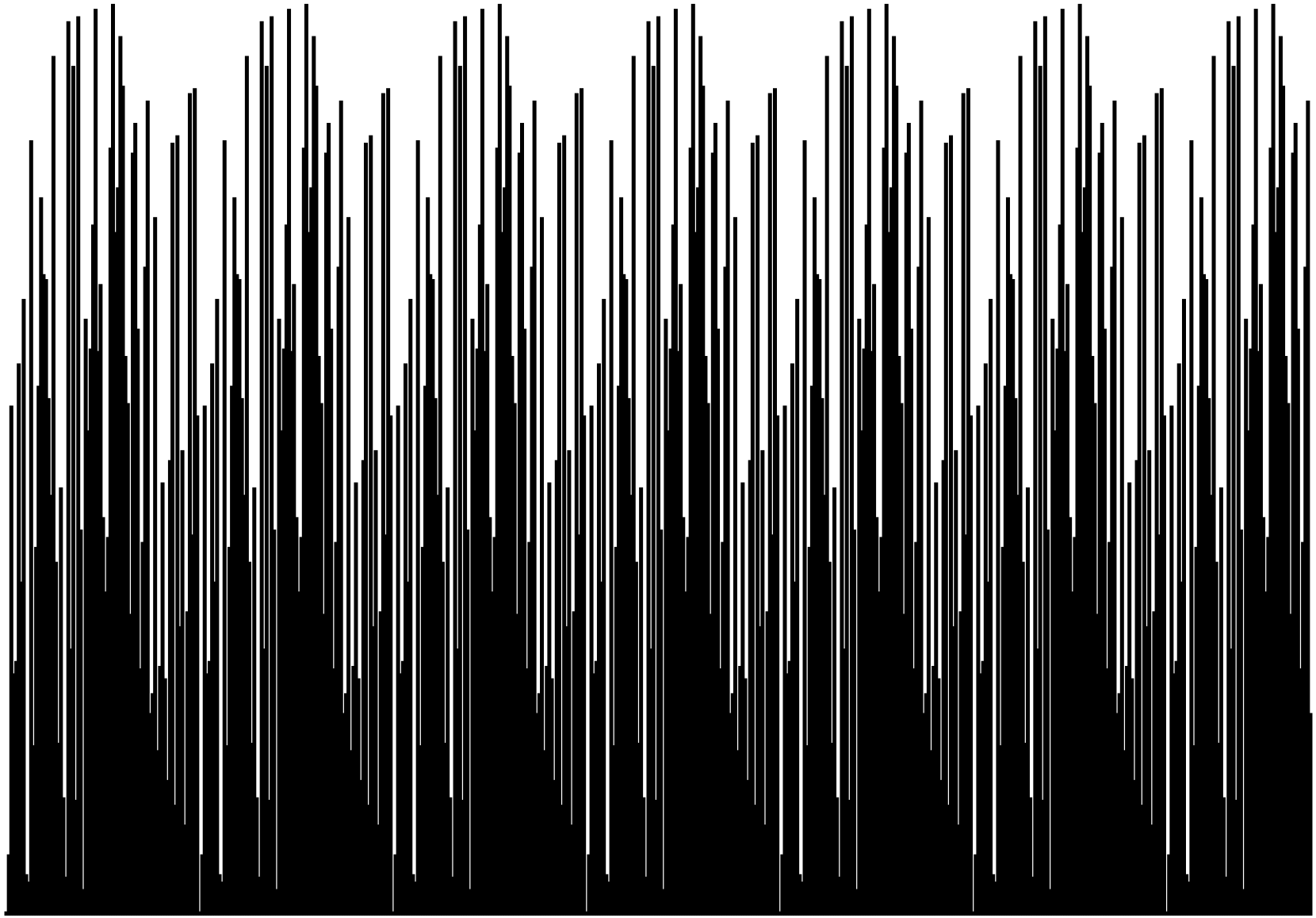
x	0	1	2	3	4	5	6	7	8	9	10	11	12	...
$f_{4,15}$	1	4	1	4	1	4	1	4	1	4	1	4	1	...

Example: $f_{13,15}$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	...
$f_{13,15}$	1	13	4	7	1	13	4	7	1	13	4	7	1	...

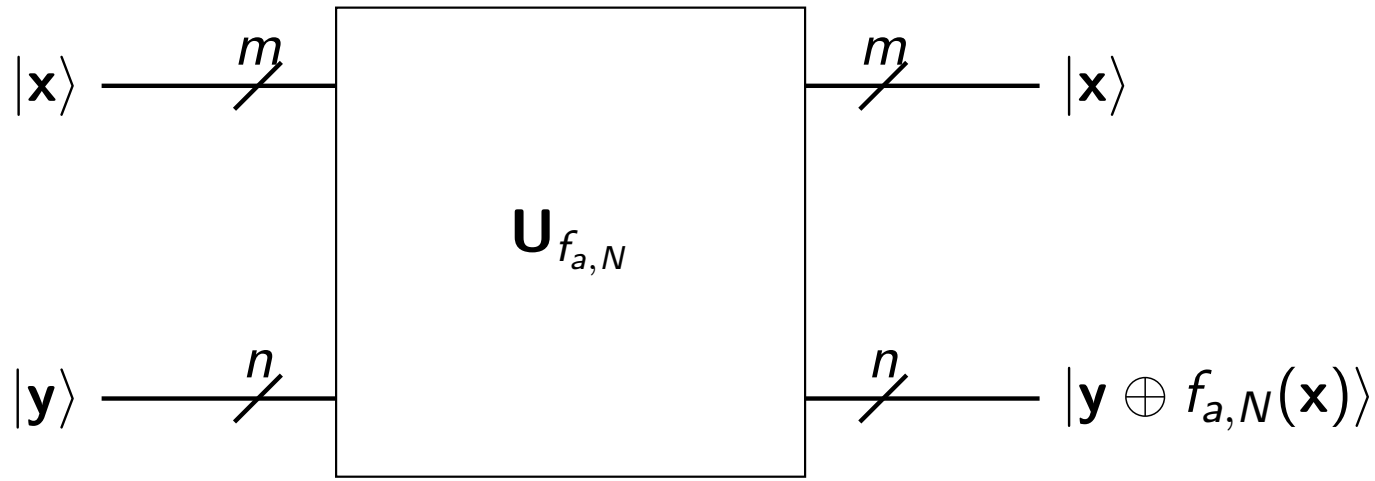


Example: $f_{24,371}$



Implementing $f_{a,N}$

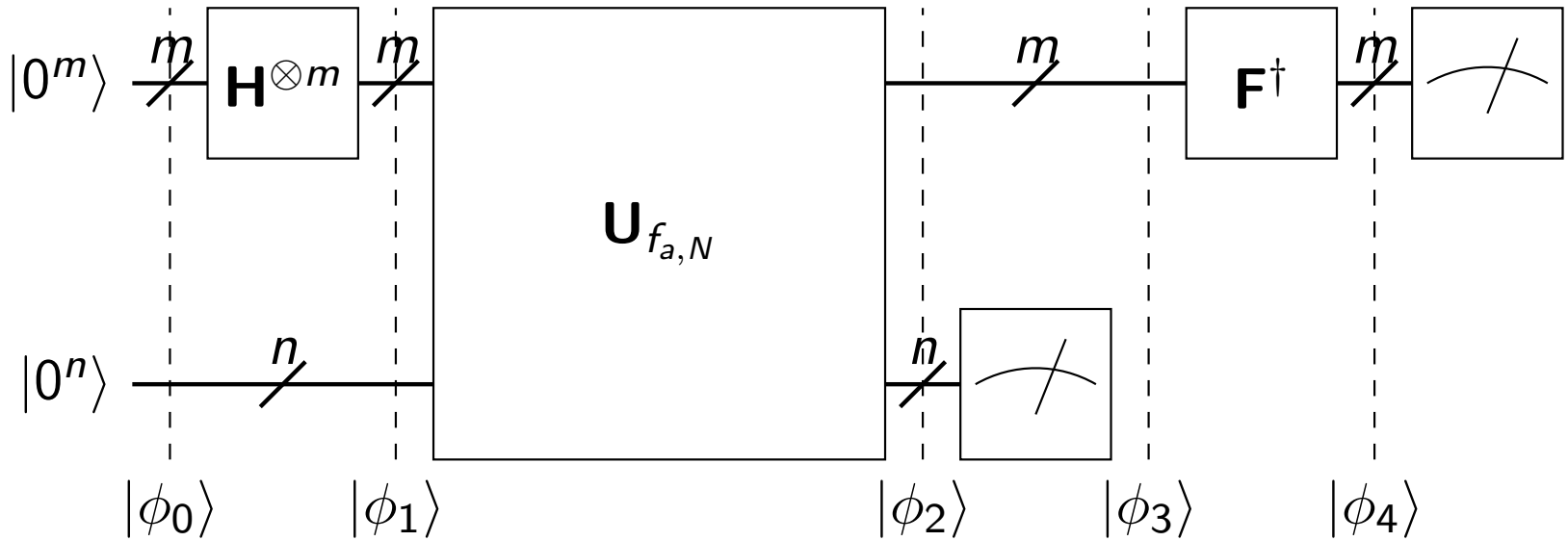
As usual we represent the function $f_{a,N}$ as a unitary operator.



In order deal with N (the maximal) outputs we need $n = \log_2 N$ lower qubits. We need to investigate the first N^2 values of x, so we need $m = log_2 N^2 = 2 \log_2 N = 2n$ upper qubits.

Period Finding for $f_{a,N}$

The quantum circuit which allows us to determine the period of $f_{a,N}$ makes use of the inverse QFT box $\mathbf{F}^\dagger$.



$$|\phi_0\rangle = |0^m 0^n\rangle = |0^m\rangle\,|0^n\rangle$$

$$|\phi_1\rangle = \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x}\in\{0,1\}^m} |\mathbf{x}\rangle\,|0^n\rangle$$

All Values of $f_{a,N}$

Due to quantum parallelism we get a values of $f_{a,N}$ for the first 2^m inputs.

$$|\phi_2\rangle = \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x}\in\{0,1\}^m} |\mathbf{x}\rangle\, |f_{a,N}(\mathbf{x})\rangle$$

Example: Consider $f_{a,15}$, i.e. for $N = 15$ we need $n = 4$ and $m = 8$. If we take $a = 13$, which is (co)prime with N, then

$$\phi_2 = \frac{1}{\sqrt{256}} \left(|0,1\rangle + |1,13\rangle + |2,4\rangle + \ldots + |254,4\rangle + |255,7\rangle\right)$$

Measuring the Lower Qubits

If we now measure the lower qubits, one of the possible values v of $f_{a,N}$ is observed. The collapsed state is a linear combination of all $|\mathbf{x}, f_{a,N}(\mathbf{x}) = v\rangle$.

If $\bar{\mathbf{x}}$ is the smallest one such that $f_{a,N}(\bar{\mathbf{x}}) = v$. As $f_{a,N}$ repeats itself with period r also $x = \bar{\mathbf{x}} + jr$ gives $f_{a,N}(\bar{\mathbf{x}} + jr) = v$.

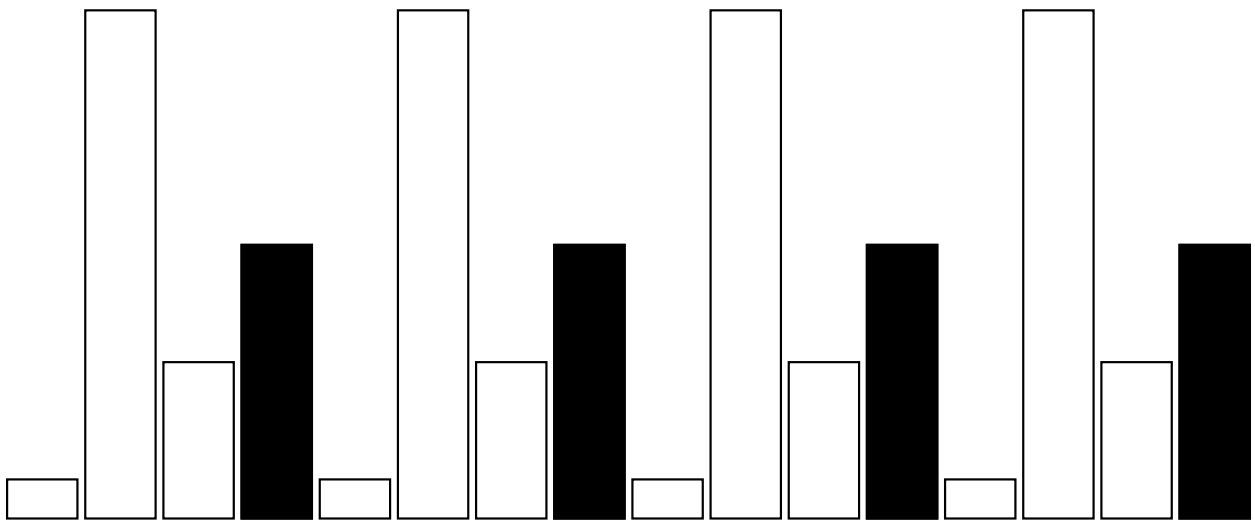
For 2^m initial inputs our function $f_{a,N}$ will repeat itself $\left\lfloor \frac{2^m}{r} \right\rfloor$ times.

$$|\phi_3\rangle = \frac{1}{\left\lfloor \frac{2^m}{r} \right\rfloor} \sum_{\mathbf{x}=\bar{\mathbf{x}}+jr} |\mathbf{x}\rangle \, |f_{a,N}(\bar{\mathbf{x}})\rangle = \frac{1}{\left\lfloor \frac{2^m}{r} \right\rfloor} \sum_{j=0}^{\left\lfloor \frac{2^m}{r} \right\rfloor - 1} |\bar{\mathbf{x}} + jr\rangle \, |f_{a,N}(\bar{\mathbf{x}})\rangle$$

Example $f_{13,15}$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	...
$f_{13,15}$	1	13	4	7	1	13	4	7	1	13	4	7	1	...

$$\phi_3 = \frac{1}{\left\lfloor \frac{256}{4} \right\rfloor} \left(|3,7\rangle + |7,7\rangle + |11,7\rangle + |15,7\rangle + \ldots + |251,7\rangle + |255,7\rangle \right)$$



Analysing the Period in ϕ_3

If QFT as a way to evaluate polynomial of rotations then $\text{QFT}^\dagger$ decompose a vector into rotations or repetitions.

If we have a vector with period r, like ϕ_3, then $\mathbf{F}^\dagger$ eliminates the **offset** $\bar{\mathbf{x}}$ and changes the period length from r to $\frac{2^m}{r}$.

Measuring the top qubits of ϕ_4 will return one of the possible repetitions which happen with period $\frac{2^m}{r}$, i.e. we will measure

$$x = \lambda \frac{2^m}{r}$$

Assuming $2^m \bmod r = 0$ (w.l.o.g.) then we have

$$\frac{x}{2^m} = \frac{2^m \lambda}{2^m r} = \frac{\lambda}{r}$$

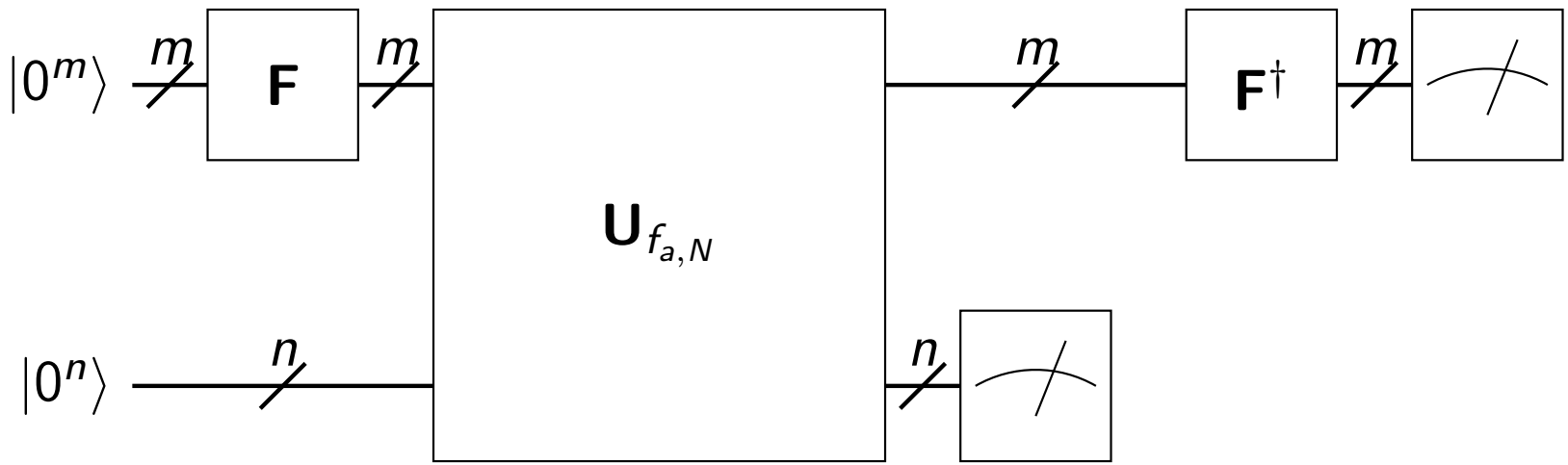
If we turn this into an irreducible fraction we obtain r.

Fourier and Hadamard

Since $e^{\pi i} = -1$ the Hadamard can be expressed similar as $\mathbf{F}$

$$\mathbf{H}^{\otimes n} |\mathbf{x}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{y}=0}^{2^n-1} e^{\pi i [\mathbf{x},\mathbf{y}]} |\mathbf{y}\rangle$$

An alternative circuit for period finding uses $\mathbf{F}$ instead of $\mathbf{H}$.



Period Estimation

Once we have determined the period r of $f_{a,N}$ we can exploit the fact

$$a^r = 1 \bmod N \quad \text{or, equivalent} \quad a^r - 1 = 0 \bmod N$$

Thus

$$N \mid (a^r - 1) \quad \text{or} \quad N \mid (a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1)$$

For this we need to assume that r is even. If this is the case, any factor of N is also a factor of $a^{\frac{r}{2}} + 1$ or $a^{\frac{r}{2}} - 1$.
We then compute, using the classical Euclid's algorithm, the GCD's

$$GCD(a^{\frac{r}{2}} + 1, N) \quad \text{and} \quad GCD(a^{\frac{r}{2}} - 1, N)$$

which give us a factor of N, provided $a^{\frac{r}{2}} \neq -1 \bmod N$. This is unlikely, but if this happens we have to restart with a different a.

Euclid's Algorithm

Find $GCD(a, b)$ w.l.o.g. assume that $a < b$.

```
Euclid(a,b) =
  if (b==0)
    then return a;
    else Euclid(b, a mod b);
```

The run time complexity is $O((\log a)(\log b))$ bit operations.

Example: The period of $f_{2,15}$ is $r = 4$; i.e. $2^4 = 1 \bmod 15$.
Therefore, $15 \mid (2^2 + 1)(2^2 - 1) = 3 \cdot 5$.
Hence, $GCD(5, 15) = 5$ or $GCD(3, 15) = 3$ is a factor of $N = 15$.

Shor's Algorithm

Input: A positive integer N. **Output:** A factor of N

Step 1. Use a (classical) polynomial algorithm to determine whether N is a power of a prime, if so exit.

Step 2. Randomly choose an integer a with $1 < a < N$. Use Euclid's algorithm to determine $GCD(a, N)$. If $GCD(a, N) \neq 1$ return it and exit.

Step 3. Use quantum circuit to determine period r of $f_{a,N}$.

Step 4. If r is odd or $a^r = -1 \bmod N$ then restart from Step 2 (choose a new integer a).

Step 5. Use Euclid's algorithm to determine $GCD(a^{\frac{r}{2}} + 1, N)$ and $GCD(a^{\frac{r}{2}} - 1, N)$. Return (nontrivial) solution(s) as factor of N.

Further Issues and Resources

More details on **Grover's Algorithm** can be found in:

Phillip Kaye, Raymond Laflamme, Michael Mosca: An Introduction to Quantum Computing, Oxford University Press, 2007

More details on **Shor's Algorithm** – in particular on quantum algorithms for **Phase Estimation** and **Period Finding** – are also in the cited book or in:

N. David Mermin: Quantum Computer Science, Cambridge University Press, 2007

There are a number of other quantum algorithms which are often collectively seen as instances of the **Hidden Subgroup Problem** (as, e.g., **Simon's Algorithm**).