Quantum computation: lecture 10 (Ruediger)

Shor's algorithm: summary

Task: given N, non-prime, find a non-trivial factor of N

We assume: · 2 does not divide N

· $N \neq p^e$, p prime

(as these cases are easily solvable)

<u>Algorithm:</u> • Pick $a \in \{2..N-1\}$ unif. at random

• Compute $\gcd(a, N) = d$ with Euclid's algo

• if $d \neq 1$, we have found a non-trivial factor of N

• if $d = 1$, compute the multiplicative order of $a^x \bmod N$, call it r (NB: r is the smallest value s.t. $a^r \bmod N = 1$) → Shor

• if r is odd, then declare failure

• if r is even, write $a^r - 1 = (a^{r/2} - 1) \cdot (a^{r/2} + 1)$

- if N divides $a^{\frac{r}{2}}+1$, then declare failure
- otherwise, compute $\gcd(N, a^{\frac{r}{2}}-1)$ and $\gcd(N, a^{\frac{r}{2}}+1)$: both must be non-trivial: <u>done</u>

<u>Analysis</u> $\longrightarrow$ $\mathbb{P}(\text{failure}) \leq \frac{1}{4}$ (repeat the algo in this case)

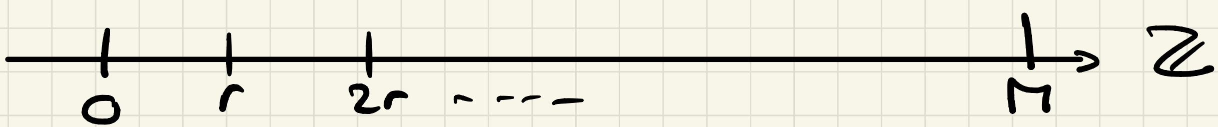
Take now $M = 2^m \sim N^2$ $(r < N)$.

We wish to compute the period of $f : \mathbb{Z} \to \mathbb{Z}$

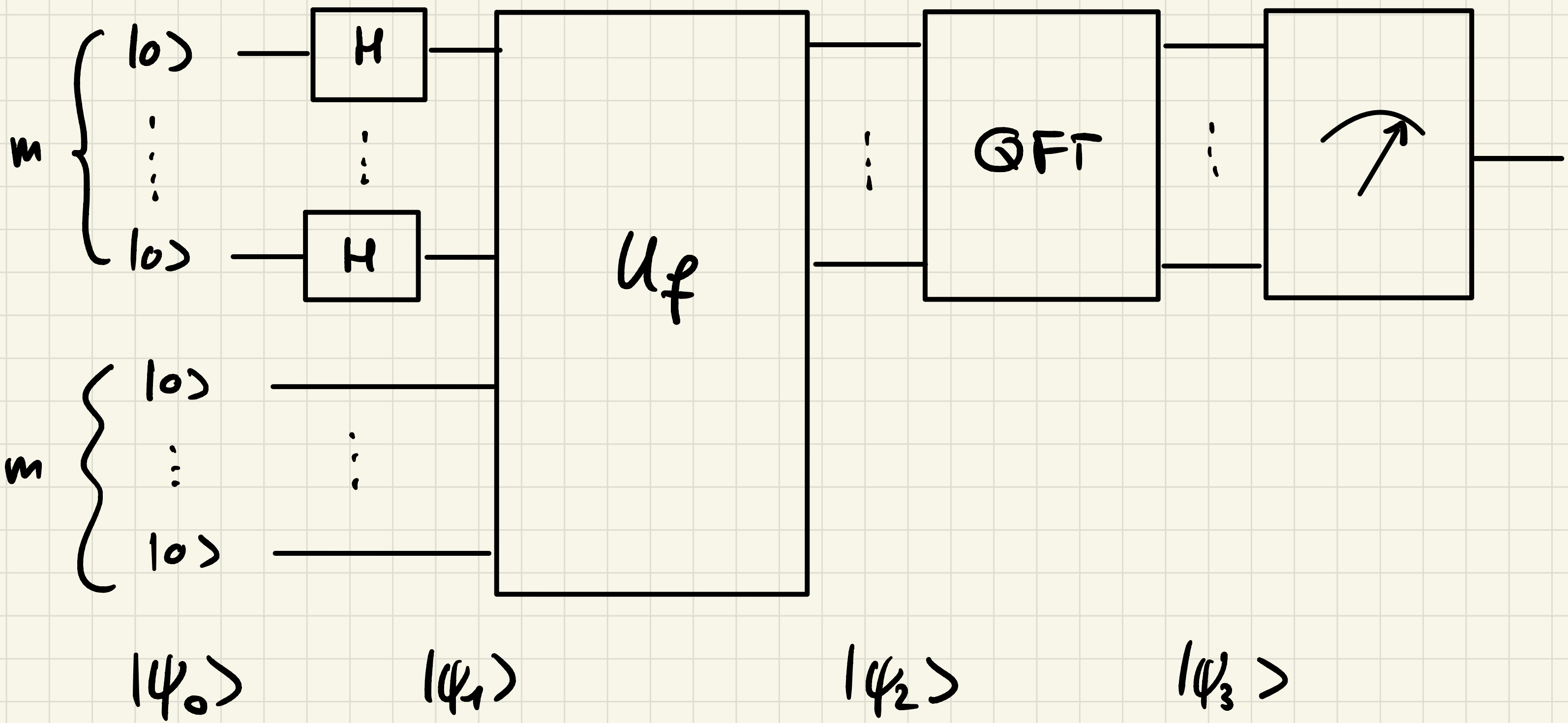
defined as $f_{a,N}(x) = a^x \mod N$

f is r-periodic : $f(x+r) = f(x)$ $\forall x \in \mathbb{Z}$

Look at f on $\{0 .. M-1\}$



Consider now the following quantum circuit :



m
|0⟩
|0⟩
m
|0⟩
|0⟩
H
H
U_f
QFT
$|\psi_0\rangle$
$|\psi_1\rangle$
$|\psi_2\rangle$
$|\psi_3\rangle$

$$|\psi_0\rangle = |\overbrace{0..0}^{m}\rangle \otimes |\overbrace{0..0}^{m}\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \otimes |0..0\rangle$$

$$|\psi_2\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \otimes |f(x)\rangle$$

[Assume r divides M] $$= \frac{1}{\sqrt{M}} \sum_{x_0=0}^{r-1} \sum_{j=0}^{\frac{M}{r}-1} |x_0+jr\rangle \otimes |\underbrace{f(x_0+jr)}_{=f(x_0)}\rangle$$

$$|\psi_3\rangle = \frac{1}{M} \sum_{x_0=0}^{r-1} \sum_{y=0}^{M-1} e^{\frac{2\pi i x_0 y}{M}} \sum_{j=0}^{\frac{M}{r}-1} e^{\frac{2\pi i j y}{M/r}} |y\rangle \otimes |f(x_0)\rangle$$

Measurement: $P_y = |y\rangle\langle y| \otimes I_m$

Outcome:

If r divides M, then $P(y) = \frac{1}{M^2} \sum_{x_0=0}^{r-1} \left| \sum_{j=0}^{\frac{M}{r}-1} e^{\frac{2\pi i j y}{M/r}} \right|^2$

So $y = k \cdot \frac{M}{r}$ with $k \in \{0 .. r-1\}$ uniformly dist.

Now, if r does not divide M, the formula becomes:

$$P(y) = \frac{1}{M^2} \sum_{x_0=0}^{r-1} \left| \sum_{j=0}^{A(x_0)-1} e^{\frac{2\pi i j y}{M/r}} \right|^2 \text{ where } A(x_0) = \begin{cases} \text{either } \lceil \frac{M}{r} \rceil \\ \text{or } \lceil \frac{M}{r} - 1 \rceil \end{cases}$$

In this second case, it can be shown that

$$\mathbb{P}\left(\exists\, 0 \le k \le r-1 \text{ s.t. } \left|y - k \cdot \frac{M}{r}\right| \le \frac{1}{2}\right) \ge \frac{2}{5}$$

i.e. $\left|\frac{y}{M} - \frac{k}{r}\right| \le \frac{1}{2M} \le \frac{1}{2r^2}$ in case of success.

Assume now $\gcd(k,r) = 1$ (this happens with probability $\ge \frac{1}{4 \ln \ln r}$).

Systematiz way to find r:

Compute all convergents of $\frac{y}{M}$ (continued fraction)

$\Longrightarrow$ look at all the denominators:

each of these denominators is a candidate

for the period r: check if $a^r \bmod N = 1$

#