Quantum computation : lecture 7 (Rüdiger)

Factorization: $N \in \mathbb{N} = \prod_i p_i^{e_i}$ $\quad p_i$ primes

e_i natural numbers

$\text{size}(N) = \log_2 N = \#$ bits required to represent N

To multiply requires $O(\text{size}(N)^2)$ operations (or less)

To factorize requires $O(e^{\text{size}(N)^{1/3}})$ operations, classically

Task: Given N, find a non-trivial factor of N

Classical algorithm:

- Pick $a \in \{2, \ldots, N-1\}$ uniformly at random
- Compute $d = \gcd(a, N)$ with Euclid's algo.
- If $d > 1$, return d ✓
- If $d = 1$, find the multiplicative order of a modulo N, i.e. (see next page)

find the smallest natural number r such that $a^r = 1 \mod N$.

<u>Aside</u>: if $\gcd(a, N) = 1$, then $\exists\, \alpha \in \{2 .. N-1\}$ s.t. $a \cdot \alpha = 1 \mod N$ (multiplicative inverse)

<u>Example</u>: $N = 5$, $a = 2$, $\gcd(a, N) = 1 \Rightarrow \alpha = 3$

<u>Proof</u>: extended Euclid's algo gives (α, v) s.t.

$a \cdot \alpha + N \cdot v = 1$ i.e. $a \cdot \alpha = 1 \mod N$ #

Given a and N s.t. $\gcd(a,N)=1$, could it be that $a^r = 0 \mod N$ for some r?

<u>Claim</u>: This cannot happen: $1 = a \cdot \alpha = (a \cdot \alpha)^r$

$= a^r \cdot \alpha^r \mod N$ so $a^r \neq 0 \mod N$

So $a, a^2, a^3, a^4, \ldots$ is never 0

So $\exists\, r_1 \neq r_2$ s.t. $a^{r_1} = a^{r_2} \mod N$ (there are only $N-1$ non zero elements).

Say $r_1 > r_2$: $\quad a^{r_1} - a^{r_2} = 0 \mod N$

so $\quad a^{r_2} \cdot \left(a^{r_1 - r_2} - 1 \right) = 0 \mod N$

so $\quad \underbrace{\alpha^{r_2} \cdot a^{r_2}} \cdot \left(a^{r_1 - r_2} - 1 \right) = 0 \mod N$

$\quad = (\alpha \cdot a)^{r_2} = 1 \mod N$ (so not 0)

so $\quad a^{r_1 - r_2} - 1 = 0 \mod N$

so $\quad \exists\, r > 0$ s.t. $a^r = 1 \mod N$

(and <u>finite</u>)

(r = "<u>order</u>" of a mod N)

Back to the factoring algorithm:

Let r be the smallest natural number such that $a^r = 1 \mod N$.

(**NB**: this is the difficult part, where the classical algorithm is slow)

- If r is odd, then declare failure & restart
- If r is even, then write $a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1)$

- Can it be that $a^{r/2} - 1 = 0 \mod N$?

No, because we assumed that r is the smallest value s.t. $a^r - 1 = 0 \mod N$.

- So $\underbrace{a^r - 1}_{\text{multiple of } N} = \underbrace{(a^{r/2} - 1)}_{\text{not a multiple of } N} \cdot (a^{r/2} + 1)$:

$\begin{cases} \text{either } a^{r/2}+1 \text{ is a multiple of } N : \text{declare failure} \\ \text{or } \gcd(a^{r/2}-1, N) \text{ \underline{and} } \gcd(a^{r/2}+1, N) \\ \quad \text{are non-trivial} \longrightarrow \text{we are done} \end{cases}$

Claim: $\mathbb{P}$(failure of the algo) $\leq \frac{1}{4}$

(without proof)

We will see next how to compute r efficiently with a quantum algorithm.

(We know that $1 \leq r \leq N-1$, so checking all the possible values of r is prohibitive; classically, we can do a bit better than that.)

<u>Note</u>: There are easy numbers to factorize:

- N even
- N multiple of 3
- N multiple of 5 ...
- $N = p^e$ (try all the roots)

The hardest numbers to factorize are:

$N = p \cdot q$ with $p \neq q$ large primes

<u>Task</u>: find the multiplicative order of $a \bmod N$

i.e. the smallest value of $r > 0$ s.t. $a^r = 1 \bmod N$

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

$$f_{a,N} : \mathbb{Z} \longrightarrow \mathbb{Z}$$

Then $f_{a,N}(x+r) = f_{a,N}(x) \quad \forall x \in \mathbb{Z}$

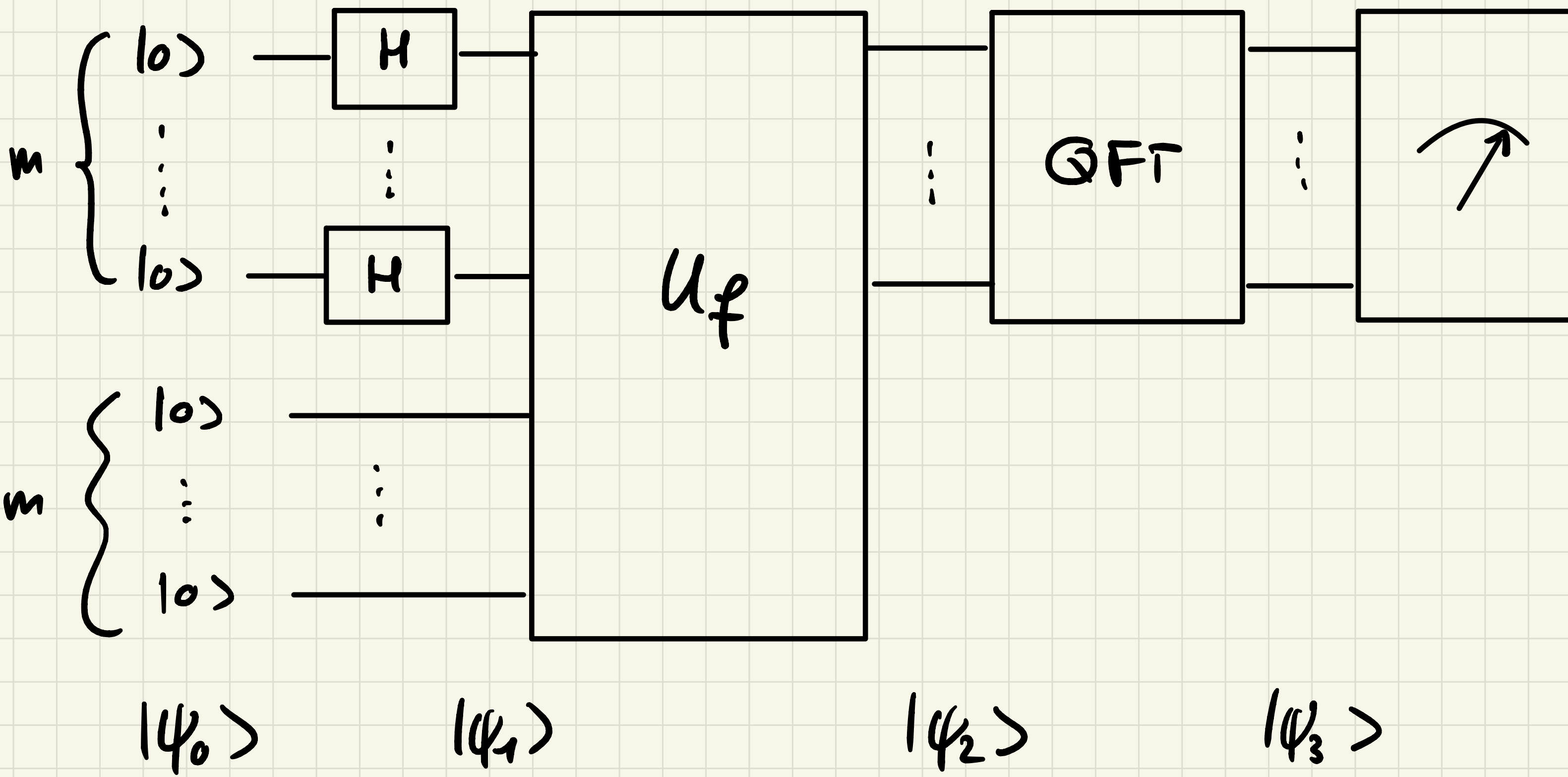
So r is also the period of $f_{a,N}$

⚠ $|\mathbb{Z}| = \infty$, but Simon's algo was operating on a finite domain

Solution: Pick $M \gg r$ (typically $M \sim N^2$)
and $f: \{0..M-1\} \longrightarrow \{0..M-1\}$

For now, assume for simplicity $M = 2^m$ for some $m \geq 1$ and $M = k \cdot r$ for some $k \geq 1$.

Quantum circuit:



$$|\psi_0\rangle = |\underbrace{0\ldots0}_{m}\rangle \otimes |\underbrace{0\ldots0}_{m}\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \otimes |0\ldots0\rangle$$

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

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

Quantum Fourier transform

$$\mathrm{QFT}\,|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \exp\left(\frac{2\pi i x y}{M}\right) |y\rangle$$

= unitary operation

State $|\varphi_3\rangle$, measurement $\Longrightarrow$ next week!

(and some more details...)