

# Quantum computation : lecture 6 (Rüdiger)

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

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  $a \in \{2, \dots, N-1\}$  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  $a^r = 1 \pmod{N}$ .

Aside: if  $\gcd(a, N) = 1$ , then  $\exists \alpha \in \{2 \dots N-1\}$   
s.t.  $a \cdot \alpha = 1 \pmod{N}$  (multiplicative inverse)

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

Proof: extended Euclid's algo gives  $(\alpha, v)$  s.t.

$$a \cdot \alpha + N \cdot v = 1 \quad \text{i.e.} \quad a \cdot \alpha = 1 \pmod{N} \#$$

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

Claim: This cannot happen:  $1 = a \cdot \alpha = (a \cdot \alpha)^r$   
 $= a^r \cdot \alpha^r \pmod N$  so  $a^r \neq 0 \pmod N$

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

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

$$\text{Say } r_1 > r_2 : a^{r_1} - a^{r_2} = 0 \pmod{N}$$

$$\text{so } a^{r_2} \cdot (a^{r_1 - r_2} - 1) = 0 \pmod{N}$$

$$\text{so } \underbrace{a^{r_2} \cdot a^{r_2}}_{= (a \cdot a)^{r_2}} \cdot (a^{r_1 - r_2} - 1) = 0 \pmod{N}$$
$$= (a \cdot a)^{r_2} = 1 \pmod{N} \text{ (so not 0)}$$

$$\text{so } a^{r_1 - r_2} - 1 = 0 \pmod{N}$$

$$\text{so } \exists r > 0 \quad \text{s.t.} \quad a^r = 1 \pmod{N}$$

(and finite)  $\left( r = \underline{\text{"order"}}$  of  $a \pmod{N} \right)$

## Back to the factoring algorithm:

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

(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  $a^{r/2} - 1 = 0 \pmod N$ ?

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

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

{ either  $a^{r/2} + 1$  is a multiple of  $N$ : declare failure  
or  $\gcd(a^{r/2} - 1, N)$  and  $\gcd(a^{r/2} + 1, N)$   
are non-trivial  $\rightarrow$  we are done

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

(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.)



Note: 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:

$$N = p \cdot q \quad \text{with } p \neq q \text{ large primes}$$

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

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

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

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

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

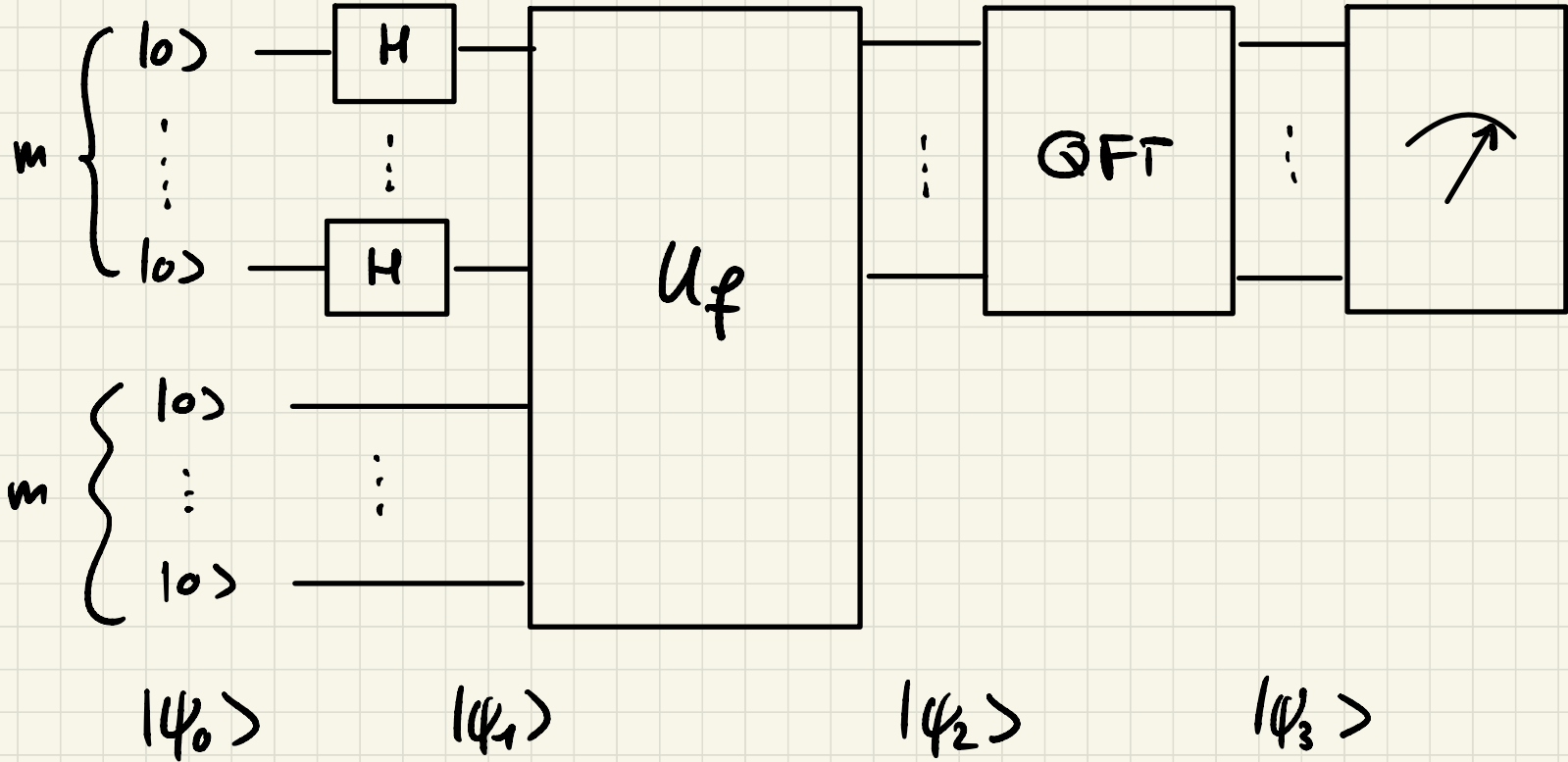
⚠  $|\mathbb{Z}| = \infty$ , but Simon's algo was operating on  
a finite domain

Solution: Pick  $M \gg r$  (typically  $M \sim N^2$ )

and  $f: \{0..M-1\} \rightarrow \{0..M-1\}$

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:



$$|\psi_0\rangle = \underbrace{|0 \dots 0\rangle}_m \otimes \underbrace{|0 \dots 0\rangle}_m$$

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

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

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

# Quantum Fourier transform

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

= unitary operation

State  $|\psi_3\rangle$ , measurement  $\Rightarrow$  next week!

(and some more details...)