Order finding

Friday, 21 May 2021 16:31

specific unitary U

$$U|y\rangle = |xy \bmod N\rangle$$

↑ computational basis state

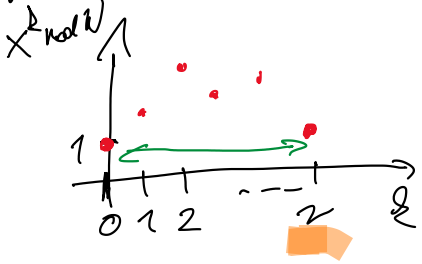
N integer
x integer
(y of course an integer)

operator U: depends on x and N as parameters

related to the formula that defines what an "order" is

r is the "order" of x with respect to N:

$$x^r = 1 \bmod N$$



relation of U (above) to the "order" r:

$$|u_s\rangle := \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k/r} |x^k \bmod N\rangle$$

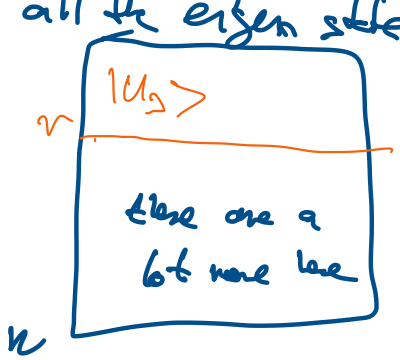
$$U|u_s\rangle = e^{-2\pi i s/r} |u_s\rangle$$

↑ "basis": $\{|u_s\rangle \mid s = 0, 1, \ldots, r-1\}$

r number of "basis" states

part of the eigenstate basis!

more eigenstates that we know nothing about



$n \approx \lceil \log N \rceil$

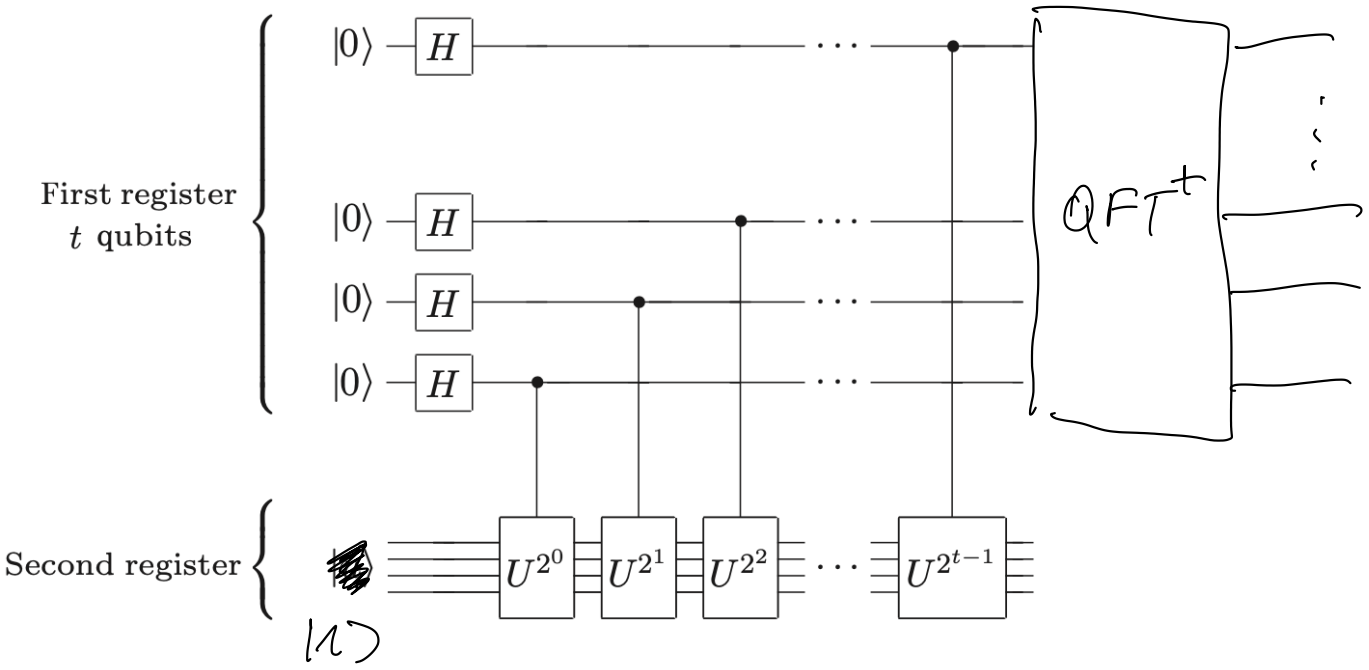
$$|1\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle$$

what's cool about this?

i) contains only the eigenstates we know about

ii) simplest superposition

we can imagine



$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle$$

output distribution