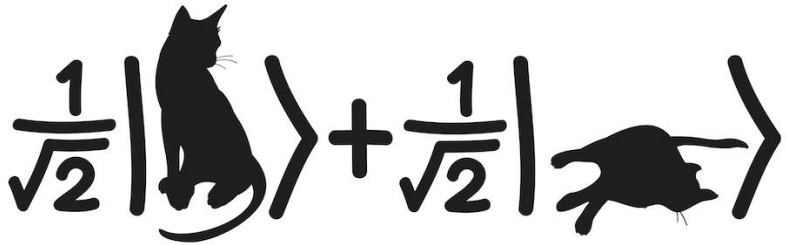
Quantum Mechanics & Quantum Computation



Umesh V. Vazirani
University of California, Berkeley

Lecture 13: Quantum Fourier Transform

Definition & Properties

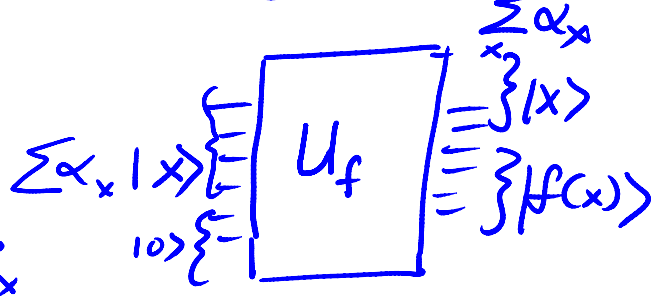
Period finding: $f: \{0, 1, \ldots, N-1\} \to S$

f is periodic with period r ← secret.

$\forall x \quad f(x) = f(x + r \pmod N)$

$x \not\equiv y \bmod r$ then $f(x) \neq f(y)$

Challenge: Find r.

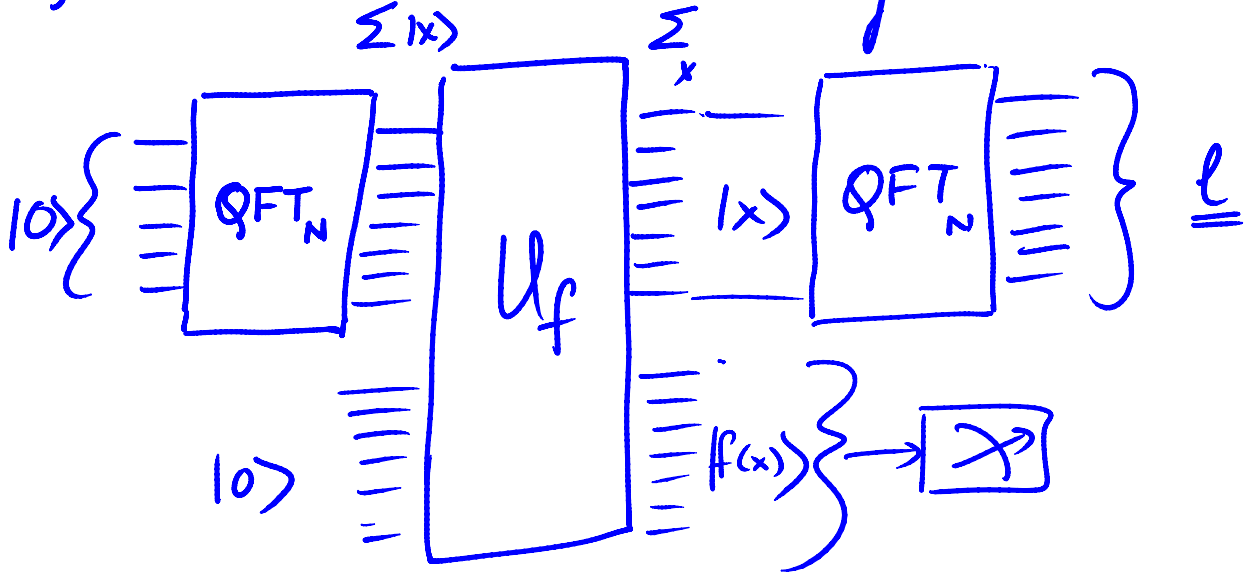


trials $\approx r$

$r = 5$

Quantum Algorithm $O(\log N)$

Quantum Period Finding:



Claim $\frac{\ell}{N} \approx \frac{k}{r}$

If $N \gg r$ can efficiently reconstruct r.

Special Case:

$$f : \{0, \ldots, N-1\} \to S$$

$$\forall x \quad f(x) = f(x + r \pmod N)$$

$$r \mid N$$