Scott Aaronson's Motivation

Shor's Algo for factoring

$\{2^k\}_{k=1}^{\infty} = \{2, 4, 8, 16, 32, 64, 128, 256, \ldots\}$

$\{2^k\}_{k=1}^{\infty} \bmod 15$

$= \{\overline{2, 4, 8, 1}, \overline{2, 4, 8, 1}, 2, 4, \ldots\}$

period = 4

$\{2^k\}_{k=1}^{\infty} \bmod 21$

$= \{\overline{2, 4, 8, 16, 11, 1}, 2, 4, 8, 16 \ldots\}$

period = 6

Is there a general rule to predict the period?

Euler (1760's): $n = p \times q$ ($p \neq q$ prime nos)

Consider $\{x^k\}_{k=1}^{\infty} \bmod n$ if x is not divisible by p or q

then above seq. will repeat with some period that evenly $|$ $(p-1)(q-1)$

(divides)

Ex. $n = 15 \Rightarrow p = 3 \neq q = 5 \Rightarrow (p-1)(q-1) = 2 \times 4 = 8$

$\Rightarrow$ the period is $\frac{8}{2} = 4$

$n = 21 \Rightarrow p = 3 \neq q = 7 \Rightarrow (p-1)(q-1) = 12$

$\Rightarrow$ the period is $\frac{12}{2} = 6$

Observation If we can find a period of $\{x^k\}_{k=1}^{\infty} \bmod n$, then we can learn a divisor of $(p-1)(q-1)$.

+++ If we could learn several (for eg, random divisors of $(p-1)(q-1)$ (by trying different random values of x) then with high prob. we could put those divisors together to learn $(p-1)(q-1)$ itself.

Obs ② If we knew $(p-1)(q-1)$ using some more tricks recover p & q.

Task

① Using a quantum computer, can we quickly create a superposition over $x \pmod n$, $x^2 \pmod n$, $x^3 \pmod n$, ... & so on?

② After creating a superposition how do we find the period.

Given r, how do we find quickly $\{x^r \pmod n\}$

Suppose $n=17$, $x=3$ & $r=14$

$$r = 14 = 2^3 + 2^2 + 2^1$$

$$x^r = 3^{14} = 3^{2^3 + 2^2 + 2^1} = 3^{2^3} \cdot 3^{2^2} \cdot 3^{2^1}$$

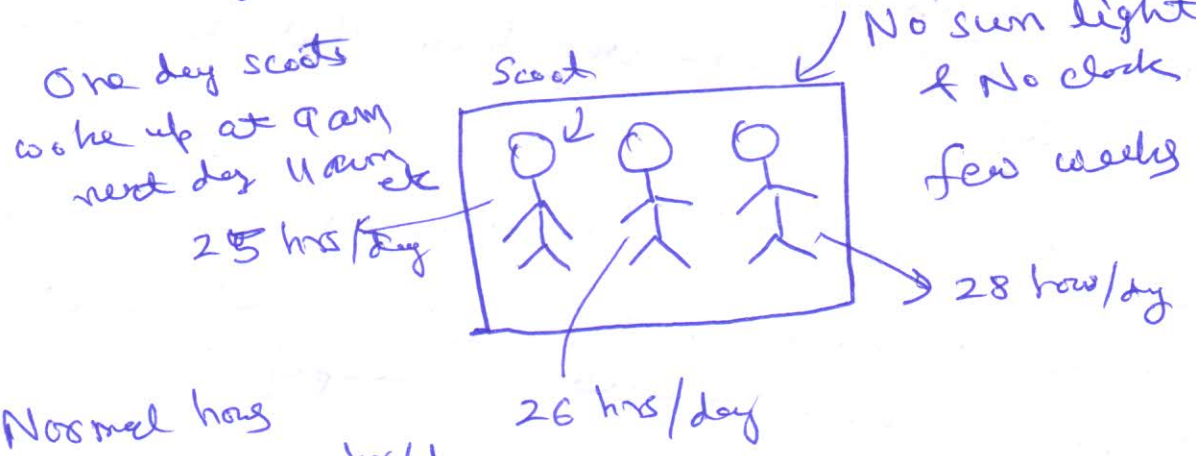
$$= ((3^2)^2)^2 \cdot (3^2)^2 \cdot 3^2$$

$$\Rightarrow 3^{14} \pmod{17} = 2$$

∴ We can create a quantum superposition over all pairs of integers of the form $(r, x^r \pmod n)$ $1 \le r \le n$

Now How to extract period?

— Using Quantum Fourier transform. (QFT)

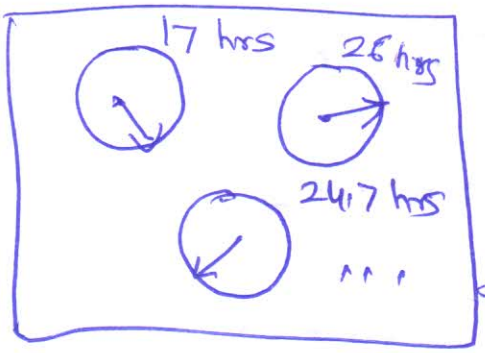


Normal hoos schedule 24 hrs/day

Q: Scoot tells you he woke up at 5:00 pm can you tell how long is his day (25 hrs/day 28 hrs/day etc.?)

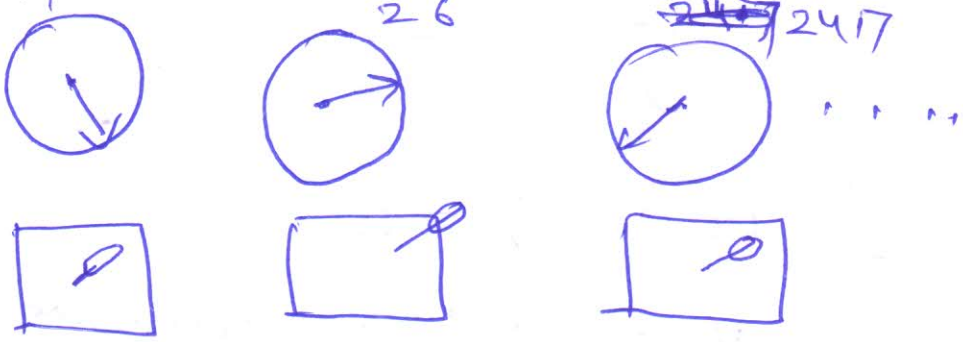
A: Not much!

full revolution eg 17 hrs & so on



for any # of hrs.

Simplicity: only hr. hand & no minute hand



Posterboard with a thumbtack

— When scott moves in the room each thumbtack was in the middle of its respective board.

— Where scoot wakes up in the morn the first thing he will do is to move each thumbtacks exactly 1 inch in the direction that the clock is pointing

New Q: By examining the thumbtacks in his room is it possible to figure out what sort of schedule scott is keeping

Ans: It is possible.

Eg. Suppose scott is keeping 26-hr day then what would happen to the thumbtack below the 24 hrs clock?

— it will go periodic motion, it would drift around a bit, but after every 12-days it would return to the middle where it started.

Now assumption of 26-hr day sch.

Q: What will happen below 26-hr day clock

Scott will wake up same time every

Morn this clock will be pointy in the same dr^n as it was last time after 1 inch movement it will not be on poster board at all.

⇒ Just by looking which thumbtack travelled the fastest from its starty pt. one can figure out the schedule.

⇒ you could infer the period of the scott's life. and that is Q.F.T.

Q.F.T. $\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} \longrightarrow \begin{pmatrix} c_1' \\ c_2 \\ \vdots \\ c_n' \end{pmatrix}$ $c_i, c_i' \in \mathbb{C}$

↓ Inulpt V^r has a non zero entry whenever scott woke up & zero elsewhere.

↓ output V^r Records the positions of the thumbtacks on the poster board (pts in complex plane)

⟹ we get a L.T.^n that maps a quantum state encoding a periodic seq. to a quantum state encoding the period of the seq.

— In terms of interference

Note: Prob. are always ≥ 0 (classical Prob. Theory)
amplitudes in quantum mechanics can be +ve, -ve or even complex nos.

⇒ The amplitudes correspond to different ways of getting a particular ans. can interfere destructively & cancel each other out.

⇒ In Shor's algo, every "real universe" corresponds to an element of the sq. contributes some amplitude to every real universe corresponds to a possible period of the sq.

— The catch is ~~that~~ ∀ periods other than the true one those contributions point in different $dr^n(s)$ & ∴ cancel each other. Only for the true period do the contributions from diff. universes ∀ all pt. in the same dr^n.

∴ after measurement we will find true period with high prob.