

# A Javnt Through the Complexity Zoo

## Agenda:

1. Languages, Turing Machines, and the Church-Turing Thesis
2. Some Classical Creatures:  $P$ ,  $NP$ ,  $PSPACE$
3. A relativistic aside:  $P$  v.  $PSPACE$
4. Efficient classical computation:  $BPP$
5. Efficient quantum computation:  $BQP$
6.  $BQP \subseteq PSPACE$
7. "Clifford circuits"  $\subseteq BPP$  (Gottesman-Knill)

## Primary References:

- Nielsen-Chuang
- Atiya-Barak
- Aaronson-Watrous : 0808.2669
- Gottesman : quant-Ph/9807006
- Cuffaro : 1310.0938
- Jozsa-Linden : quant-Ph/0001143 (entanglement paper)

1.

- One question at the heart of this talk is:

Q: Which Yes/No questions are answerable by physical devices?

- Formally, a Yes/No question is called a "language".

Def: A language  $L \subseteq \{0, 1\}^* := \{\text{all finite binary strings}\}$ .

Write

$$L(x) := \begin{cases} 1 & \text{if } x \in L \\ 0 & \text{otherwise} \end{cases} \quad (\text{"indicator func."})$$

- Ex:
- $\text{PRIMES} = \{\text{binary}(n) \mid n \text{ prime}\}$
  - $\text{CONN} = \{\text{binary}(G) \mid G \text{ connected graph}\}$
  - $\text{SUBSET-SUM} = \{\text{binary}(S) \mid \exists T \subseteq S, \sum_{t \in T} t = 0\}$
  - $\text{HALT} = \{\text{binary}(A) \mid A \text{ algorithm that always halts}\}$ .
- Food for thought: neural networks suggest follows an outcome
- {Does or not, grammatically correct sentence or not, etc...}

Def: A language  $L$  is decidable iff  $\exists$  "reasonably effective procedure"  $A_L: \{0,1\}^* \rightarrow \{0,1\}$  s.t.

$$\forall x \in \{0,1\}^*: A_L(x) = L(x).$$

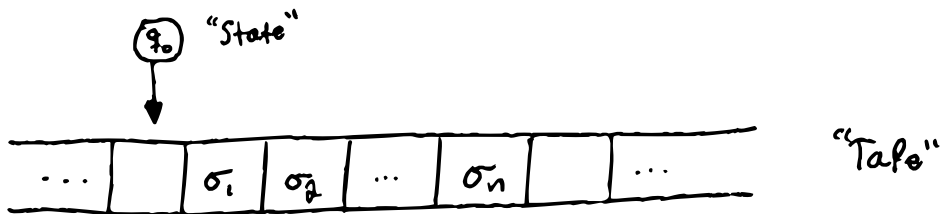
- One is left wondering what constitutes a "reasonably effective procedure".

Turing's Idea:

- Human working by rote w/ unlimited Pens and Paper



Turing Machine



$$\text{Input} = \sigma_1 \sigma_2 \dots \sigma_n \in \{0,1\}^n.$$

## Church-Turing Thesis:

A "reasonably effective procedure"



A Computable on Turing Machine

- Later, Deutsch and others proposed

A "REP"



A Physically Realizable



A Turing machine

- No physical system can "compute more" than TM.

Q: Which Yes/No questions are efficiently answerable by physical devices?



2.

Def. A (language) Complexity Class is any collection of languages.

Ex:

- $P := \left\{ L \mid \begin{array}{l} \exists \text{ Poly-time TM } A \text{ s.t.} \\ \forall x \in \{0,1\}^*: A(x) = L(x) \end{array} \right\}$
- $PSPACE := \left\{ L \mid \begin{array}{l} \exists \text{ Poly-space TM } A \text{ s.t.} \\ \forall x \in \{0,1\}^*: A(x) = L(x) \end{array} \right\}$
- $NP := \left\{ L \mid \begin{array}{l} \exists \text{ Poly-time TM } A, \text{ Polynomial } P \text{ s.t.} \\ \forall x \in L, \exists c \in \{0,1\}^{P(|x|)} : A(x, c) = 1 \end{array} \right\}$

Q:  $P \stackrel{?}{=} NP$  (literally 1 Million \$ Question!)

Thm:  $P \subseteq NP \subseteq PSPACE$  (Why?)

3.

- A Physicist might think  $P = PSPACE$  because, well, "time and space are morally the same", according to relativity. But then  $P = NP$ , which only diehard contrarians believe. What gives?!

- The difference lies in the re-usability of space, but not of time.
- How could one "re-use" time?
- CTCs!

Def.  $P_{CTC} = "P \text{ w/ CTC}"$ .

Thm. (Adleman-Watrous):  $P_{CTC} = PSPACE$

- Complexity a function of where you are in spacetime?!

4.

- Include randomness in computation
- Can only increase power, because non-random is special case of random.

Def.  $BPP = \left\{ L \mid \begin{array}{l} \exists \text{ poly-time TM } A, \text{ function } p \text{ s.t.} \\ \forall x \in \{0,1\}^+, \text{ if } r \sim U(\{0,1\}^{p(|x|)}), \\ \Pr[A(x,r) = L(x)] \geq 2/3. \end{array} \right\}$

- Extended-Church-Turing thesis.

- Quantum Computer, it is said, threatens this idea (e.g. Shor's algorithm).

5. • What is good comp. model for quantum computing?

Def. An  $n$ -qubit quantum circuit  $Q_n$  (over gate set  $G$ ) is

$$Q_n = U_d \dots U_1, \quad U_i = \bigotimes_{j \in I_i} g_j, \quad g_j \in G.$$

Q: Given  $n+1$  qubit state  $|\psi\rangle$ , how to act  $Q_n$  on  $|\psi\rangle$ ?

A: Nonsense!

• Really, when we talk about "circuits" we mean "families of circuits".

Def.  $Q = (Q_n)_{n \in \mathbb{N}}$  is a family of circuits.

• Not just any family is valid!

→

Consider the language  $\swarrow$  nht TM

$$L = \{1^n \mid X_n \text{ halts}\}$$

• Many halting problem. (Uncomputable)

Let

$$Q_n := \begin{cases} X^{\otimes n} & 1^n \in L \\ I^{\otimes n} & 1^n \notin L \end{cases}$$

Then

$$Q_n | 0 \rangle^{\otimes n} = \begin{cases} |1\rangle^{\otimes n} & 1^n \in L \\ |0\rangle^{\otimes n} & 1^n \notin L \end{cases}$$

• So, measuring first qubit we decide halting problem!

• Need uniform circuit.

Def. A family  $Q = (Q_n)_{n \in \mathbb{N}}$  is uniformly generated if  $n \mapsto Q_n$  is computable by poly-time TM.

Def:  $L \in \text{BQP}$  iff  $\exists$  uniform, poly-size family  $(Q_n)_{n \in \mathbb{N}}$  st.  $\forall x \in \{0,1\}^*$ ,

$P_r(\text{first qubit of } Q_n | x \rangle \text{ is } |L(x)\rangle) \geq 2/3.$

• Physical extended Church-Turing Thesis.

Shor's Algorithm:

$\text{FACTORING} = \{ \langle (N, k) \rangle \mid \exists d \in \{2, \dots, k\} : d \mid N \}$

$\in \text{BQP}$

but  $\stackrel{?}{\in} \text{BPP}.$

Q:  $\text{BPP} \stackrel{?}{=} \text{BQP}$  ("quantum cannot match the classical")

The question of quantum complexity theory.

b.

- What can we say about the power of a BQP computation?

Naive approach:

$$U \sim 2^n \times 2^n = O(2^n) \text{ Params.}$$

$$|\Psi\rangle \sim 2^n = \mathcal{O}(2^n) \quad \text{params.}$$

ans BQF evanton Seamp to return  $O(2^n)$  form.

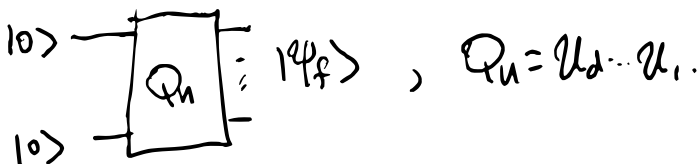
Thus,

$$\text{BQP} \subseteq \text{EXPSPACE}$$

- Can he do better?

Thm:  $BQP \subseteq PSPACE$

Proof Sketch: (Feynman Path Integral):



Then,

$$|\psi_f\rangle = \sum_{x \in \{0,1\}^n} \beta_x |x\rangle = U_d \dots U_1 |0\rangle^{\otimes n}.$$

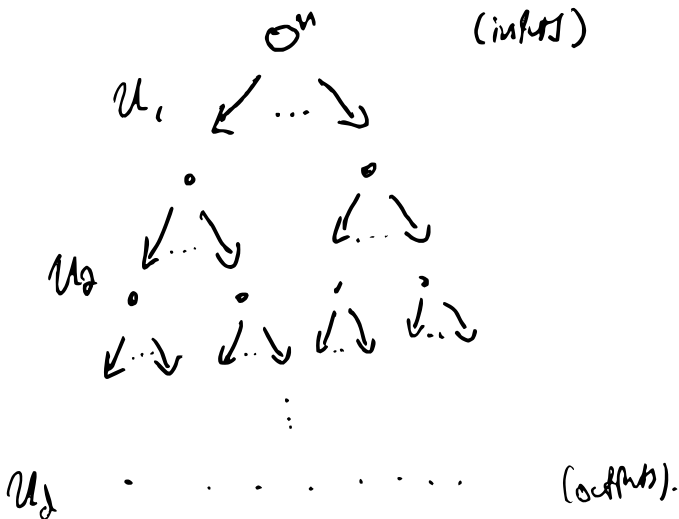
Now, for matrices  $A, B$ ,

$$(AB)_{ij} = \sum_k A_{ik} B_{kj}.$$

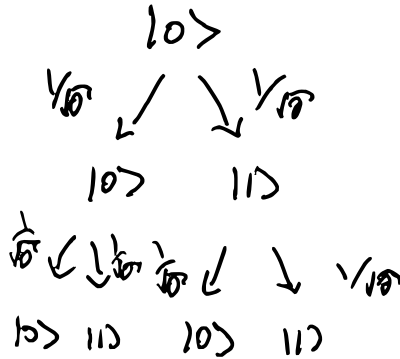
So,

$$\beta_x = \sum_{i_1 \in \{0,1\}^n} (U_d)_{x i_1} \dots (U_1)_{i_1 0^n}$$

Physical interpretation: Sum of histories input strings and take:



Eg.



• Note: for each path, can compute the answer efficiently.

• If gate set has bounded fan-out  $k$ , then  
 $\# \text{ of paths} \leq k^n$ .

• So,

$$\beta_x = \sum_{\substack{\text{Paths } p \\ \text{ending in } x}} \alpha_p, \quad \alpha_p = \text{product along path.}$$

$$= \sum_{\text{exp}} \text{poly-time computable thing.}$$

exp-time,  
 but not space!

$\Rightarrow \text{BQP} \subseteq \text{PSPACE. QED.}$

• Stronger bounds are known, e.g.  $BQP \subseteq PP$ .

• Still, ultimate question is if  $BPP \stackrel{?}{=} BQP$ .

7:

Q: If  $BPP \neq BQP$ , then why?

• Entanglement? Necessary, maybe, but sufficient?

• No!

Def. The order-n Pauli group is

$$\mathcal{P}_n := \{n\text{-fold tensor prod. of Pauli matrices}\} \times \{\pm 1, \pm i\}.$$

The order-n Clifford group is

↗  
to make it  
a group.

$$C_n = \{U \in U(2^n) \mid U \mathcal{P}_n U^\dagger = \mathcal{P}_n\} \quad (\text{normalizer}).$$

Thm (GKW): Let  $(\Gamma_n)_{n \in \mathbb{N}}$  be a uniform family of Clifford circuits. Then,  $\exists$  BPP-algorithm  $A$  s.t.  $\forall x \in \{0,1\}^+$  and  $y \in \{0,1\}^{|x|}$ ,

$$Pr[A(x) = y] = |\gamma_y(x)|^2,$$

where

$$\Gamma_{|x|} |x\rangle = \sum_{y \in \{0,1\}^{|x|}} \gamma_y(x) |y\rangle.$$

Proof sketch:

- Naively, one needs to store all  $2^{|x|}$  amplitudes to simulate. But can make use of the group structure.

For input  $|0\rangle^{\otimes n}$  (similar for others),

$$Z_i |0\rangle^{\otimes n} = |0\rangle^{\otimes n} \quad (Z_i \text{ is } Z \text{ on } i\text{th qubit}).$$

- Also  $|0\rangle^{\otimes n}$  is unique state w/ this property. (modulo phase)
- So, can describe  $|0\rangle^{\otimes n}$  w/  $Z_i$  (generates of the stabilizer of the state).
- Then, perform  $U$ , w/  $|0\rangle^{\otimes n}$  stabilized by  $M$

$$U| \psi \rangle = U M | \psi \rangle = (U M U^\dagger) U | \psi \rangle.$$

- Thus, similar update stabilizer  $M$ , not  $|\psi\rangle$  itself.

• Since  $U$  is Clifford  $M_i$  Pauli,  $UM_iU$  is also Pauli.

• Description needs

• 2 bits for each  $n$  Pauli ( $I, X, Y, Z$ )

• 2 bits for overall phase ( $\pm 1, \pm i$ ).

$\Rightarrow$  Full description of state needs  $O(n^2)$  bits.

• Updating each  $M_i$  takes constant time ( $2 \times 2$  matrix)

$\Rightarrow$  Simulate takes  $O(n)$  time (constant for each region).

• Measure qubit at end is trickier, which I refer you to Gottesman's paper.

• CNOT:

• Since  $CNOT P_N CNOT^\dagger = P_N$ , so CNOT is Clifford, entangled states are classically simulable!

$\Rightarrow$  Entanglement not sufficient for quantum advantage!

Q: Is it necessary? (open!)

//