BRICS Mini-course on Quantum Computation

A. Berthiaume
C.W.I.

Session II: Complexity (I)

Reference:

Oracle Quantum Computing
By A. Berthiaume & G. Brassard
In Journal of Modern Optics
Vol 41, Numb. 12, 1994

HTTP://www.cwi.nl/~berthiau/
Seminar.html

Comparing QC and TM:

1) TM $\overset{P}{\Longrightarrow}$ QC

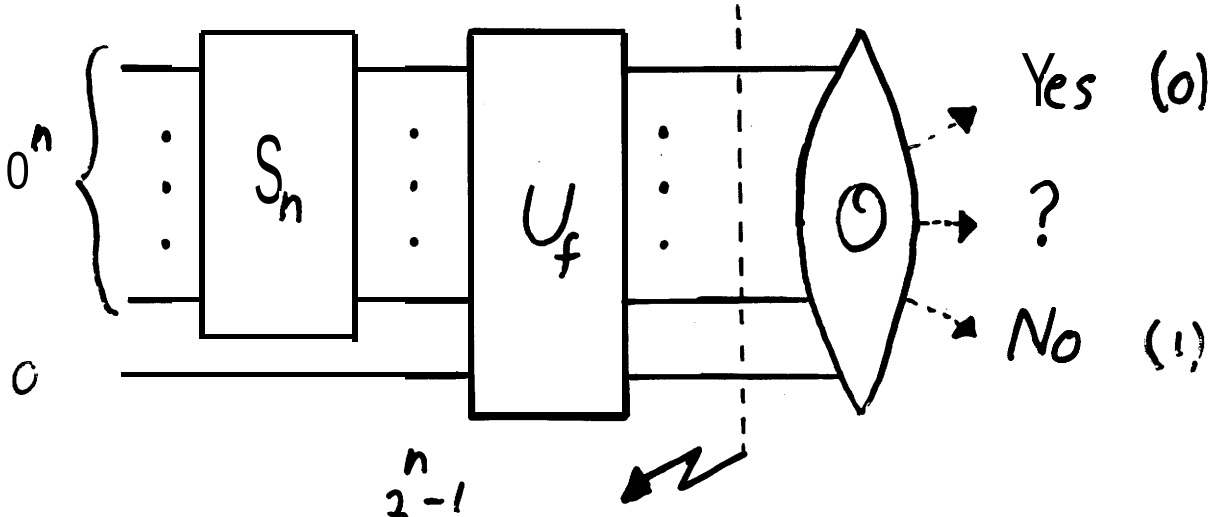
(Lecerf / Bennett)

2) CQP à la Jozsa

3) DJ problem

"Quantum Parallelism" Jozsa 91:

Let $F_n = \{ f \mid f : \{0,1\}^n \to \{0,1\} \}$
and $G : F_n \to \{0,1\}$. Consider



$$\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i, f(i)\rangle$$

➤ Which G's can be "implemented" as an <u>observable</u> $\mathcal{O}$?

1) $G_0 \equiv 0$

2) $G_i \equiv f(i)$

3) $G_{ij} \equiv f(i) \oplus f(j)$

Complexity Classes:

P ≡ decision Problems Solvable on a TM in Poly-Time.

EQP ≡ decision Problems Solvable on a QC (exactly) in Poly-Time <u>worst-case</u>.

We know that

$$P \subseteq EQP$$

but $P \subsetneq EQP$?

Compromising:

$$P \subseteq EQP \subseteq PSPACE$$

$\subsetneq$

is unknown

So, we change the problem...

PSPACE = decision problems in poly-space on TMs

Oracle Machines:

An oracle: $X \subseteq \Sigma^*$

$\Sigma = \{0,1\}$

An oracle machine:

let M be a $\begin{cases} \text{TM} \\ \text{PTM} \\ \text{QC}^* \end{cases}$

etc...

then

$M^X(x)$ may "ask" questions of the form

"is $b \in X$?"

Cost: $|b|$ (writing)

Answer: Y/N (instantaneous)

New Question:

We have $\forall X \subseteq \Sigma^*$

$$P^X \subseteq EQP^X$$

but $\overset{?}{\exists} X \subseteq \Sigma^*$ s.t.

$$P^X \subsetneq EQP^X \ ?$$

Notation & Definition :

- $B(X)$: A predicate: $X \subseteq \Sigma^*$

  True iff $\forall_{n \geq 1}$

  $$\#(X \cap \Sigma^n) = \begin{cases} 0 \\ 2^{n-1} \end{cases}$$

- S_X : A Language

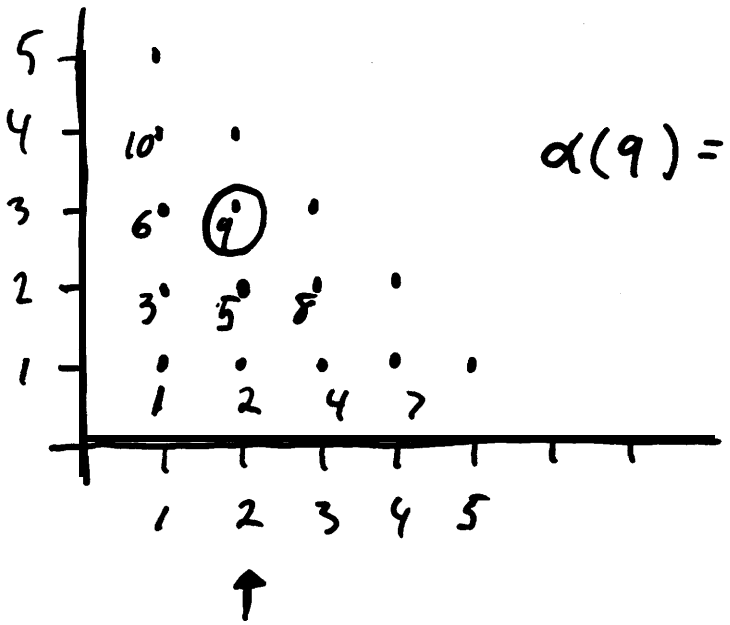
  $$\{1^n \mid X \cap \Sigma^n = \emptyset\}$$

Definitions:

- $\alpha : \mathbb{N} \to \mathbb{N}$ s.t. $\forall i \in \mathbb{N}$

$$\overset{\infty}{\exists} n \in \mathbb{N} \quad \alpha(n) = i$$

ex:



$\alpha(9) = 2$

- $$p(n) = \begin{cases} 1 & \text{if } n = 1 \\ 2^{p(n-1)} & \text{if } n > 1 \end{cases}$$

$$p(k) = \underbrace{2^{2^{2^{2^{\cdot^{\cdot^{\cdot}}}}}}}_{k \text{ times}}$$

<u>Thm:</u> for all $X \subseteq \Sigma^*$,

if $B(X)$ is true then

$$S_X \in EQP^X$$

Proof: immediate by DIP.

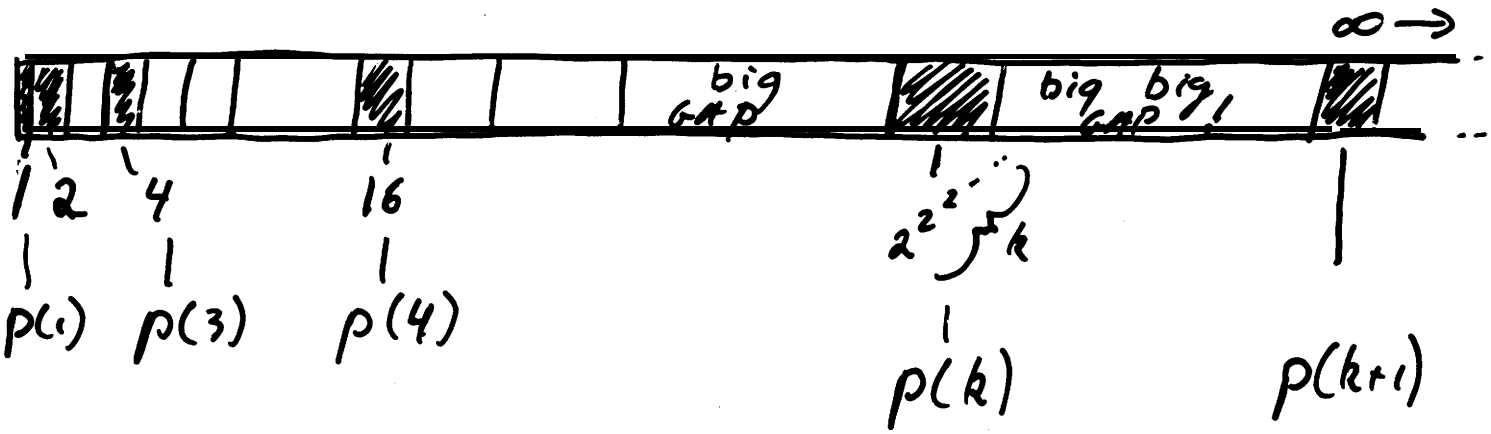
Therefore; to prove $P^X \subsetneq EQP^X$ We Need X s.t. $B(X)$ holds yet it won't be of use to TMs.

<u>Thm:</u> $\exists\, X \subseteq \Sigma^*$ s.t. $B(X)$ and any TM M recognizing S_X (using X as an Oracle) Will take expo. time on infinitely many inputs.

<u>Cor:</u> $\exists\, X \subseteq \Sigma^*$ s.t. $P^X \subsetneq EQP^X$

Proof:

View of Σ^* (not to scale)



In Stages:

- $X_1 = \emptyset$
- $\forall n \geq 1$ do:
  - run $M^{X_n}_{\alpha(n)}(1^{p(n)})$ for $2^{p(n)-1}$ steps
  - $X_{n+1} = \begin{cases} X_n \\ \underline{OR} \\ X_n \cup \{1/2 \text{ of } \Sigma^{p(n)-1}\} \end{cases}$
- $X = \lim_{n \to \infty} X_n$

Deciding what to add:

Key: forcing $M^{X_n}_{\alpha(n)}(1^{p(n)})$ to either make a mistake about S_X or take too much time to answer.

Recall: $S_X = \{ 1^k \mid X \cap \Sigma^k = \emptyset \}$

Run $M_{\alpha(n)}^{X_n}(1^{p(n)})$ for $2^{p(n)-1}$ steps.

<u>3 outcomes</u>:

1) M has not stopped

2) M rejects

$\rightarrow$ set $X_{n+1} = X_n$

3) M accepts

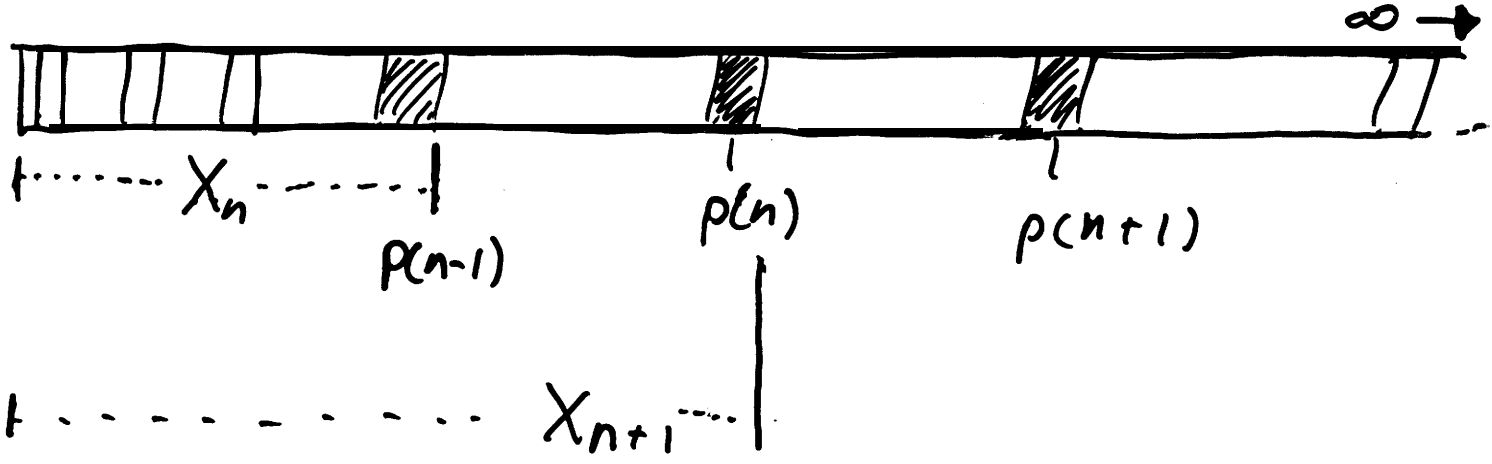
$\rightarrow$ set $X_{n+1} = X_n \cup \{ \frac{1}{2} \text{ of } \Sigma'^{p(n)} \}$

but which half?

Which half of $\Sigma^{p(n)}$?

$M^{X_n}_{\alpha(n)}(1^{p(n)})$ accepts within $2^{p(n)-1}$ steps

Consider Σ^*



Let $Q_n = \{$ questions asked by M during the run $\}$

$$|Q_n| < 2^{p(n)-1}$$

So $\exists\, R_n \subseteq \Sigma^{p(n)}$ s.t. $R_n \cap Q_n = \emptyset$

And $|R_n| = \dfrac{2^{p(n)}}{2}$

Set $X_{n+1} = X_n \cup R_n$

Showing that $X = \lim_{n \to \infty} X_n$ works

- By construction, $B(X)$ holds
- Lemma: if M_i recognizes S_X using X, then $\forall n$ s.t. $\alpha(n) = i$ $M_i^X(1^{p(n)})$ accepts in more than $2^{p(n)-1}$ steps.

Proving the lemma:

if M_i^X rec. S_X then

1) $\forall n$ s.t. $\alpha(n) = i$ $\quad 1^{p(n)} \in S_X$

by contradiction:

$$1^{p(n)} \notin S_X \iff X \cap \Sigma^{p(n)} \neq \emptyset$$

$$\iff M_i^{X_n}(1^{p(n)}) \text{ accepts}$$

but, to M_i, $X \equiv X_n$

so

$$\iff M_i^X(1^{p(n)}) \text{ accepts}$$

$$\iff 1^{p(n)} \in S_X$$

<u>Second Part:</u>

M_i^X accepts $1^{P(n)}$ in $\geq 2^{P(n)-1}$ steps

by contradiction: Suppose

$M_i^X(1^{P(n)})$ accepts $< 2^{P(n)-1}$ steps

then $1^{P(n)} \in S_X$

$\Leftrightarrow X \cap \Sigma^{P(n)} = \emptyset$

but <u>TO M_i</u> $X \equiv X_n$

$\Leftrightarrow M_i^{X_n}(1^{P(n)})$ also accepts

$\Leftrightarrow \exists R_n \subset \Sigma^{P(n)}$ s.t.

$\# R_n = 2^{P(n)}/2$

and $X \cap \Sigma^{P(n)} = R_n$

$\Leftrightarrow 1^{P(n)} \notin S_X$

$\rightarrow\leftarrow$

Conclusions

- $\exists X \subseteq \Sigma^* \quad P^X \subsetneq EPQ^X$

- (See paper)
  $\exists Y \subseteq \Sigma^* \quad EQP^Y \not\subseteq NP^Y$

But $S_X, S_Y \in BPP^{X(Y)}$

Next Time:

Beyond BPP^X!