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 $\xrightarrow{P} QC$
   (Lecerf / Bennett)

2) CQP à la Jozsa

3) DJ problem
"Quantum Parallelism" Joza 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 observable \( \mathcal{O} \)?

1) \( G_0 \equiv 0 \)
2) \( G_i \equiv f(i) \)
3) \( G_{ij} \equiv f(i) \oplus f(j) \)
**Complexity Classes:**

\[ P \equiv \text{decision Problems Solvable on a TM in Poly-Time.} \]

\[ EQP \equiv \text{decision Problems Solvable on a QC (exactly) in Poly-Time worst-case.} \]

We know that

\[ P \subseteq EQP \]

but \[ P \not\subseteq EQP \]?
Compromising:

\[ P \leq \text{EQP} \leq \text{PSPACE} \]

\( C \uparrow \)

is unknown

So, we change the problem...

\[ \text{PSPACE} = \text{decision problems in poly-space on TMs} \]
Oracle Machines:

An oracle: \( X \subseteq \Sigma^* \rightarrow \Sigma = \{0, 1\} \)

An oracle machine:

let \( M \) be a \( \begin{cases} \text{TM} \\ \text{PTM} \\ \text{QC}^* \\ \text{etc...} \end{cases} \)

then \( M^X(x) \) may "ask" questions of the form "is \( b \in X \) ?"

Cost: 1b! (writing)

Answer: Y/N (instantaneous)
New Question:

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

$P^x \subseteq \text{EQP}^x$

but $\exists X \in \Sigma^*$ s.t.

$P^x \notin \text{EQP}^x$?
Notation & Definition:

- $B(X)$: A predicate: $X \subseteq \Sigma^*$
  
  True iff $\forall n \geq 1$

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

- $S_x$: A language

  $$\{i^n \mid X \cap \Sigma^n = \emptyset\}$$
Definitions:

- $\alpha: \mathbb{N} \rightarrow \mathbb{N}$ s.t. $\forall i \in \mathbb{N}$
  $\exists n \in \mathbb{N}$ $\alpha(n) = i$

ex: $\alpha(9) = 2$

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

$p(k) = \underbrace{2^2}_2 \underbrace{2^2}_2 \ldots \underbrace{2^2}_2^{k \text{ times}}$
Thm: for all $X \in \Sigma^*$, if $B(X)$ is true then $S_x \in EQP^*$

Proof: immediate by DIP.

Therefore, to prove $P^*_x \subseteq EQP^*$ we need $X$ s.t. $B(X)$ holds yet it won't be of use to TMs.
**Thm:** \( \exists X \in \Sigma^* \) s.t. \( B(X) \)
and any TM \( M \) recognizing \( S_x \) (using \( X \) as an Oracle)
Will take expo. time on infinitely many inputs.

**Cor:** \( \exists X \in \Sigma^* \) s.t. \( P^x \in \text{EQP}^x \)
Proof:

View of $\Sigma^*$ (not to scale)

In Stages:

- $X_i = \emptyset$

- $\forall n \geq 1$ do:
  - run $M_{d(n)}(\{p(n)\})$ for $2^{p(n)} - 1$ steps
  - $X_{n+1} = \begin{cases} X_n & \text{OR} \\ X_n \cup \{\frac{1}{2} \text{ of } \sum_{i=1}^{p(n)}\} \end{cases}$

- $X = \lim_{n \to \infty} X_n$
Deciding what to add:

Key: forcing $M_{\Delta(n)}^{X_n}(1^{P(n)})$ 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 \( M_{a(n)}(1^{p(n)}) \) for \( 2^{p(n)} - 1 \) steps.

3 outcomes:

1) \( M \) has not stopped

2) \( M \) rejects

   \[ \rightarrow \text{ set } X_{n+1} = X_n \]

3) \( M \) accepts

   \[ \rightarrow \text{ set } X_{n+1} = X_n \cup \{\frac{1}{2} \text{ of } \Sigma_{p(n)}^n\} \]

   but which half?
Which half of $\sum_{i=1}^{\rho(n)}$?

$M_{\alpha(n)}(1^{\rho(n)})$ accepts within $2^{\rho(n)}$ steps.

Consider $\sum^*$

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

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

So $\exists R_n \subseteq \sum^\rho(n)$ s.t. $R_n \cap Q_n = \emptyset$ and $|R_n| = \frac{2^{\rho(n)}}{2}$

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. $x(n) = i$, $M_i^X(1^{P(n)})$ accepts in more than $2^{P(n)} - 1$ steps.
Proving the lemma:

if \( M_i^X \) rec. \( S_x \) then

1) \( \forall n \ s.t. \ d(n) = i \quad 1^{P(n)} \in S_x \)

by contradiction:

\[ 1^{P(n)} \notin S_x \iff X \cap \sum^{P(n)} \neq \emptyset \]

\[ \iff M_i^{X_n}(1^{P(n)}) \text{ accepts} \]

but, to \( M_i \), \( X \equiv X_n \)

So

\[ \iff M_i^X(1^{P(n)}) \text{ accepts} \]

\[ \iff 1^{P(n)} \in S_x \]
Second Part:

$M_i^x$ 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 $1^{P(n)} \in S^x_x$

$\iff \exists X \cap \sum P(n) = \emptyset$

but to $M_i \quad X \equiv X_n$

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

$\iff \exists R_n \subset \sum P(n)$ s.t.

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

and $X \cap \sum P(n) = R_n$

$\iff 1^{P(n)} \notin S^x_x$
Conclusions

- $\exists X \subseteq \Sigma^* \quad \mathbb{P}^x \neq \mathbb{EPQ}^x$

- (See paper)
  $\exists Y \subseteq \Sigma^* \quad \mathbb{EQP}^y \neq \mathbb{NP}^y$

But $S_x, S_y \in \mathbb{BPP}^x(y)$

Next Time:

Beyond $\mathbb{BPP}^x$!