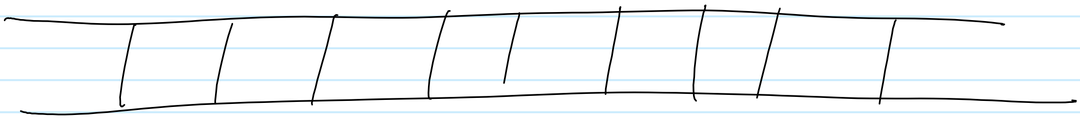
Scott Aaronson: Quantum Complexity and Quantum Optics

December-30-13 2:37 AM

See also http://quantumrio.wordpress.com/, problem sets at https://www.dropbox.com/sh/cazr7ep5n6f14ya/eCaZnKXX1B

1. ECT & complexity
2. Linear optics & Boson sampling.
3. Postselection KLM, Approximate Boson sampling. (KLM: Knill, Laflamme, Milburn, http://arxiv.org/abs/quantph/0006088)
4. Scalability & verification of Boson sampling devices.

Turing Machine



The Physical Church-Thesis: Anything that can be physically computed can be computed by a Turing machine.

Beyond Turing:

1. "Zeno Computer" - fails as at 10^43 Hz the energy needed to cool the computer will turn it into a black hole.
2. "Special Relativity Computer" - will need an exponential amount of energy to accelerate.

A definition of the class "P".

ECT: "Extended Church-Turing Thesis": P is always the same, and the physical P is the CS P.

A definition of "NP". $P = NP$? Conjecture: $P \neq NP$.

Def L is "NP hard" if $NP \subseteq P^L$

P w/ oracle for L.

Def L is is "NP-complete" if it is NP-hard & in NP.

$P \subseteq NP \subseteq PSPACE \subseteq EXP$

Conj: All inclusions are strict.
Thm: $P \neq EXP$.

Lecture II

A difference between factorization & all known NP-complete problem: In factorization there is uniqueness of solutions.

Claim factorization $\in NP \cap (\text{co-}NP)$.

Claim If $\exists L \in NP \cap (\text{co-}NP)$ s.t. L is NP complete, then $NP = \text{co-}NP$.

But, conjecture $NP \neq coNP$.

The "polynomial Hierarchy" (PH)

0th level : P
1st level : NP, coNP
2nd level: NP^{NP}, $coNP^{NP}$
3rd level: $NP^{(NP^{NP})}$ etc.

Conjecture: This is non-degenerate.

http://en.wikipedia.org/wiki/Polynomial_hierarchy

This whole hierarchy is contained in P-Space.

Thm If graph isomorphism is NP-complete, Then PH collapses to NP^{NP}

#P : count # of sol'ns of P problems.

Example The matching problem in a bi-partite graph is P, yet the corresponding counting problem is #P-complete.

The permanent of a matrix A:

$$per(A) = \sum_{\sigma \in S_n} \prod_i a_{i\sigma(i)}$$

For the V-V adjacency matrix of a bipartite graph, per counts matchings, so per is #P - complete.

$NP \subseteq PH \subseteq P^{\#P} \subset PSPACE$

Toda 1991 $PH \subset P^{\#P}$

BPP: Bounded-error Probabilistic Poly time:

The class of all $L \subseteq \{0,1\}^*$ s.t. $\exists$ poly-time Turing machine s.t.

random string, uniform distribution, poly length

* $x \in L \Rightarrow Pr[M(x, r) \text{ accepts}] \geq \frac{2}{3}$
* $x \notin L \Rightarrow Pr[M(x, r) \text{ accepts}] \leq \frac{1}{3}$

[The only needed property of $\alpha = \frac{1}{3}$ & $\beta = \frac{2}{3}$ is $0 < \alpha < \beta < 1$]

PP: Same as BPP, but with $\alpha = \beta$.

Claim $P \subset BPP \subset PP \subset P^{\#P} \subset PSPACE$

$BPP \subset NP$ unknown.

Thm (Sipster-...) $BPP \subset NP^{NP}$ ◻

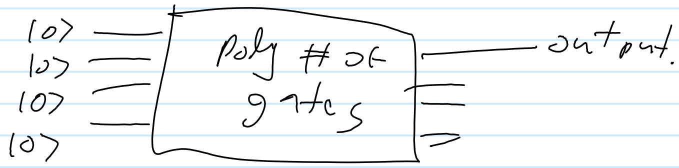
$NP \subset BPP$ unknown

Thm $NP \subset BPP \Rightarrow PH = NP^{NP}$

BQP The class of $L \subset \{0,1\}^*$ s.t. $\exists$ classical poly-time turing machine M s.t. $\forall x \in \{0,1\}^*$ M outputs a quantum circuit C_x s.t.

$x \in L \Rightarrow C_x$ accepts w/ prob $\geq 2/3$

$x \notin L \Rightarrow C_x$ —"— $\leq 1/3$



claim $P \subset BPP \subset BQP \subset PSPACE \subset EXP$

$$BQP \subset PP \subset P^{\#P} = PSPACE$$

The relationship between NP & BQP is unknown

Conjecture $P = BPP \subsetneq BQP$

Follows from the existance of a good enough pseudo-random number generator