<전산학특강 기말고사 답안>

2018320161 컴퓨터학과 송대선

-Problem1-

만일 P = NP이면, 다음과 같은 구조적 특징을 가집니다.

1. P = NP = NP-Complete가 됩니다.
   NP-Complete는 NP에 속하고, 모든 NP의 문제들이 그 문제로 reduction이 efficient하게 이루어지는 문제들의 집합입니다.
   따라서 당연히 NP-Complete ⊂ NP입니다.
   그런데 NP = P이면, NP-Complete ⊂ P이고,
   그러면 NP-Complete에 속하는 문제들은 efficient하게 solvable합니다.
   그런데 NP = P이므로, NP에 속하는 문제들 역시 efficient하게 solvable합니다.
   즉, reduction으로 인해 NP = NPC가 되어 P = NP = NP-Complete가 되는 것입니다.

2. P = NP = coNP가 됩니다.
   P의 Complement는 역시 P에 속합니다.
   그런데 P = NP임으로, NP의 Complement역시 NP=P에 속함으로,
   P = NP = coNP가 성립합니다.
   (coNP는 NP의 Complement입니다.)

3. P = NP = PH가 됩니다.
   P = NP($\Sigma_1 P$) = coNP($\Pi_1 P$)인데, 이는 곧
   P = $\Sigma_1 P = \Pi_1 P = \Sigma_2 P = \Pi_2 P = \Sigma_3 P = \Pi_3 P = \cdots$의 형태가 무한히 같아집니다.
   즉, entire hierarchy가 P로 무너지는 것입니다.

-Problem2-

만일 P $\neq$ NP이면, 다음과 같은 구조적 특징을 가집니다.

1. NP - P $\neq \phi$이다.
   우리는 P ⊂ NP이라는 것을 trivial한 사실로 받아드립니다.
   그런데 P $\neq$ NP이 성립하려면 NP $\not\subset$ P이어야 합니다.
   따라서 NP - P $\neq \phi$이 성립합니다.
   이는 verification은 efficient하게 할 수 있으나,
   solve는 efficient하게 할 수 없는 문제들이 존재한다는 것을 의미합니다.

2. P $\neq$ NP-Complete
   NP-Complete는 NP에 속하면서,
   NP의 모든 문제들이 NP-Complete로 efficiently reduce되는 문제들의 집합입니다.
   즉, NP-Complete는 Hardest Problems of NP입니다.
   그런데, Problem2-1에서 제가 보였듯이, NP에는 P에 속하지 않는 문제들이 있습니다.
   즉, 쉽게 solve되지 않는 문제들이 있다는 것입니다.
   이런 상황에서 NP-Complete가 P에 속해버리면 가장 어려운 문제가 쉽게 solve된다는 의미로, 이는 모순입니다. 따라서 P $\neq$ NP-Complete입니다.

3. NP $\neq$ p-selective

우리는 다음과 같은 Theorem을 수업시간에서 배웠습니다.

“if each member of NP is P-selective, then P = NP”

또한 p→q이 참이면, 대우명제인 ~q → ~p 역시 참입니다.

따라서, “if P $\neq$ NP,

then there exist a member of NP that is not P-selective“ 역시 성립합니다.

따라서 NP $\neq$ P-selective입니다.

-Problem3-

P $\neq$ NP라고 증명을 해보겠습니다.

우리는 다음 두 가지 Theorem을 배웠습니다.

Theorem 1 : P $\subset$ BQP

Theorem 2 : if SAT is not in P, then P $\neq$ NP

위 두 가지 Theorem을 결합하면, “if SAT is not in BQP, then P $\neq$ NP”이 됩니다.

우리는 Deutsch`s algorithm이라는 quantum algorithm을 배웠고,
이 알고리즘은 function f가 balanced function인지 constant function인지의
여부를 가립니다.
그러나 이 알고리즘 만으로는 SAT를 효율적으로 해결 할 수가 없습니다.
balanced function은 not gate의 기능을 하고,
constant function은 constant의 기능을 합니다.
이 두 가지만으로는 SAT에 들어가는 and, or gate의 역할을 해낼 수 없습니다.
따라서 SAT를 다항시간 내에 해결하는 quantum 알고리즘은 존재하지 않습니다.
SAT는 BQP에 속하지 않으며, 그로 인해 SAT는 P에 속하지 않으며,
이로 인해, P $\neq$ NP이 됩니다.

이렇게 P $\neq$ NP라는 것을 증명하였습니다.