Intermediate Complexity

Peter Mayr

Computability Theory, April 26, 2021

Recall

Polytime reductions $\leq_m^p$ induce an equivalence relation on problems in NP:

$$A \text{ and } B \text{ are equivalent if } A \leq_m^p B \text{ and } B \leq_m^p A.$$

Then

- P …equivalence class of the easiest problems in NP
- NP-complete …class of the hardest problems in NP

Question

Is there anything in between (assuming P $\neq$ NP)?

Ladner's Theorem (1975)

Assume $\mathrm{P} \neq \mathrm{NP}$. Then there exists $A \in \mathrm{NP}$ that is neither in P nor NP-complete.

Proof.

Consider DTMs over $\Sigma = \{0, 1\}$.

- Let M_1, M_2,... be an enumeration of DTMs deciding the languages in P such that M_i runs in time n^i.
- Let $f_1, f_2, \ldots$ be an enumeration of functions such that $f_i(x)$ is computable in time $|x|^i$.

Blowing holes in SAT:

Define A using a function $f : \mathbb{N} \to \mathbb{N}$ as

$$A := \{x \ : \ x \in \mathrm{SAT} \text{ and } f(|x|) \text{ is even}\}.$$

Definition of f by DTM M

On input n in unary, compute $f(n)$ inductively using 2 stages.
Each stage takes n steps.
Initialize $f(0) = f(1) := 2$.

- **Stage 1:** Compute $f(0), f(1), \ldots$ until n steps are over.
- Suppose the last value M computed was $f(m) = k$.
- **Stage 2:**
- If $k = 2i$, search for $x \in \{0,1\}^*$ in lexicographical order witnessing $L(M_i) \neq A$, i.e.,
  1. M_i accepts x and ($x \notin$ SAT or $f(|x|)$ is odd), or
  2. M_i rejects x and ($x \in$ SAT and $f(|x|)$ is even).

  If M finds such x in $\leq n$ steps, $f(n) := k + 1$; else $f(n) := k$.
- If $k = 2i + 1$, search for $x \in \{0,1\}^*$ in lexicographical order witnessing f_i does not reduce SAT to A, i.e.
  1. $x \in$ SAT and ($f_i(x) \notin$ SAT or $f(|f_i(x)|)$ is odd), or
  2. $x \notin$ SAT and ($f_i(x) \in$ SAT and $f(|f_i(x)|)$ is even).

  If such x is found in $\leq n$ steps, $f(n) := k + 1$; else $f(n) := k$.

Runtime of M

- By construction $f(n)$ is computed in time $O(n)$ (in Stage 2, $x \in \text{SAT}$ is checked by a DTM that takes $\leq n$ steps).
- The time counter adds a factor $\log(n)$ (cf. Time Hierarchy Theorem).

Overall M computes $f(n)$ in polynomial time in n.

Thus $A = \{x \ : \ x \in \text{SAT and } f(|x|) \text{ is even}\}$ is in NP.

Claim: $A \notin \text{P}$

- Suppose otherwise that $i \in \mathbb{N}$ is minimal such that $A = L(\text{M}_i)$.
- Then for $k = 2i$ Stage 2 of M never finds x witnessing $L(M_i) \neq A$.
- Hence f is eventually constant $2i$.
- Since $f(n)$ is odd for only finitely many $n \in \mathbb{N}$, $A = L(\text{M}_i)$ and SAT differ only in a finite initial segment.
- Then SAT $\in P$ contradicts the assumption P $\neq$ NP.

Claim: A is not NP-complete

- Suppose otherwise that $i \in \mathbb{N}$ is minimal such that f_i reduces SAT to A.
- Then for $k = 2i + 1$ Stage 2 of M never finds x witnessing $x \in$ SAT but $f_i(x) \notin A$ (or conversely).
- Hence f is eventually constant $2i + 1$.
- Since $f(n)$ is even for only finitely many $n \in \mathbb{N}$, A is finite and in P.
- Then SAT $\in P$ contradicts the assumption P $\neq$ NP.

$\square$

Note

- Ladner's Theorem extends to yield an infinite hierarchy of intermediate problems between P and NP-complete.
- No "natural" problems of intermediate complexity are known.
- Fixed template **Constraint Satisfaction Problems** (CSP) form a large natural subclass of NP with P/NP-complete dichotomy (Bulatov, Zhuk 2017).

  CSP(H) for a fixed digraph H:
  Input: digraph G
  Question: Is there a homomorphism $G \to H$?

Possibly NP-intermediate problems

Factoring (decision version)

Given $m < n$, does n have a factor d with $1 < d < m$?

- in NP: yes-instances are certified by such a factor d
- in co-NP: no-instances are certified by prime factorization of n
- in BQP (bounded-error quantum polynomial time): solvable by a quantum computer in polynomial time with an error probability of at most $1/3$ (Shor 1994)

Discrete Logarithm (decision version)

Given prime p, generator $a \in \mathbb{Z}_p^*$, $b \in \mathbb{Z}_p^*$ and $m \in \mathbb{N}$, is there $x \leq m$ such that

$$a^x = b \text{ in } \mathbb{Z}_p$$

Graph Isomorphism

Given graphs G, H, are they isomorphic?

- quasi-polynomial algorithm $2^{O((\log n)^k)}$ (Babai 2015)