P, NP, and Beyond

Hengfeng Wei

hfwei@nju.edu.cn

May 01 $\sim$ May 04, 2017

P, NP, and Beyond

P

$$\mathsf{P} = \bigcup_{c>0} \mathsf{DTIME}(n^c)$$

TC 34.1–5

$$f(n) = O(n^c) \qquad t(n) = O(n^d)$$

$$\cancel{T(n) = kf(n) + t(n)}$$

$$T_k(n) = \sum_{i=1}^{k} f^{(i)}(n) + t(n)$$

$$k = O(1) \textit{ vs. } k = \Theta(n^{O(1)}) \qquad O \textit{ vs. } \Theta, \Omega$$

NP

Definition (NP)

$L \in \mathsf{NP}$ if $\exists$ polynomial-time *verifier* $V(x, c)$ such that $\forall x \in \{0,1\}^*$,

$$x \in L \iff \exists c \in \{0,1\}^*, V(x, c) = 1.$$

NP-problems has short certificates that are easy to verify.

TC 34.2–6

$$\text{HAM-PATH} \in \text{NP}$$

NP

TC 34.2–4

NP is closed under $\cup, \cap, \cdot, *$.

$$L_1 \in \text{NP}, L_2 \in \text{NP} \implies L = L_1 \circ L_2 \in \text{NP}$$

Question:

Is NP-complete closed under $\cup, \cap, \cdot, *$?

NP

Theorem

NP is closed under "$*$".

$$c = c_1 \# c_2 \# \dots \# c_k \# m_1 \& m_2 \& \dots \& m_{k-1}$$

$A^*(x, y) : \forall 1 \le k \le |x|$

$$c = c_1 \# c_2 \# \dots \# c_k \# m_1 \& m_2 \& \dots \& m_{k-1}$$
$$\bigwedge \wedge_{i=1}^{i=k} A(x_i, c_i)$$

$$x \in L^* \iff \exists c, A(x, c) = 1$$

Reference

http://www.dei.unipd.it/~geppo/AA/DOCS/NPC.pdf

coNP

$$L \in \mathsf{NP} \overset{?}{\Longrightarrow} \overline{L} \in \mathsf{NP}$$

$$\overline{\mathsf{SAT}} = \{\phi : \phi \text{ is not satisfiable}\}$$

$$\mathsf{TAUT} = \{\phi : \phi \text{ is a tautology}\}$$

$$\mathsf{coNP} = \{L : \bar{L} \in \mathsf{NP}\}$$

Definition (coNP)

$L \in$ coNP if $\exists$ polynomial-time *verifier* $V(x, c)$ such that $\forall x \in \{0,1\}^*$,

$$x \in L \iff \forall c \in \{0,1\}^*, V(x,c) = 1.$$

NP *vs.* coNP

$$\text{coNP} \neq \{0,1\}^* \setminus \text{NP}$$

$$\text{P} \subseteq \text{NP} \cap \text{coNP}$$

$$\text{P} = \text{NP} \implies \text{NP} = \text{coNP}$$

$$\text{NP} \neq \text{coNP} \implies \text{P} \neq \text{NP}$$

NP-hard and NP-complete

$$\forall L \in \mathsf{NP}, L \le_p L' \implies L' \text{ is NP-hard}$$

$$\text{NP-complete} = \mathsf{NP} \cap \text{NP-hard}$$

NP-hard and NP-complete

TC 34.5–6

HAM-PATH is NP-complete.

$$\text{HAM-CYCLE} \leq_p \text{HAM-PATH}$$

$\leq_p$: split v into v_1, v_2; add $s, t, (s, v_1), (v_2, t)$

Question:

$$\text{HAM-PATH} \leq_p \text{HAM-CYCLE}$$

$\leq_p$: add v'; $(v', v), \forall v \in V$

P *vs.* NP

solve *vs.* verify

exhaustive search avoidable?

$$\mathsf{P} \neq \mathsf{NP} \implies \mathsf{P} \neq \mathsf{NP}\text{-complete}$$

Theorem (NP-intermediate: Ladner's theorem, 1975)

$$\mathsf{P} \neq \mathsf{NP} \implies \exists L \in \mathsf{NP} \setminus \mathsf{P} \land L \notin \mathsf{NP}\text{-complete}$$

Factoring, Graph (group) isomorphism (*vs. Subgraph isomorphism*)

EXP

$$\mathsf{EXP} = \bigcup_{c>0} \mathsf{DTIME}(2^{n^c})$$

$$\mathsf{P} \subseteq \mathsf{NP} \subseteq \mathsf{EXP}$$

Time Hierarchy Theorem

$$\mathsf{P} \subsetneq \mathsf{EXP}$$

Theorem (Time Hierarchy Theorem, 1965)

$$f(n) \log f(n) = o(g(n)) \implies \mathsf{DTIME}(f(n)) \subsetneq \mathsf{DTIME}(g(n))$$

R

$$\mathsf{R} = \mathsf{DTIME}(< \infty)$$

$$\#\text{undecidable} \gg \#\text{decidable}$$

$$\#\text{algs} = \mathbb{N}$$
$$\#\text{problems} = 2^{\mathbb{N}} = \mathbb{R}$$

PSPACE

$$\text{PSPACE} = \bigcup_{c>0} \text{SPACE}(n^c)$$

$$\text{P} \subseteq \text{PSPACE}$$

$$\text{NP} \subseteq \text{PSPACE} \subseteq \text{EXP}$$

PSPACE-complete

Definition (QBF: Quantified Boolean Formula)

$$Q_1 x_1 Q_2 x_2 \cdots Q_n x_n \varphi(x_1, x_2, \ldots, x_n)$$

$$Q_i : \forall, \exists$$

$$\text{TQBF} = \{\text{True QBF}\} \in \text{PSPACE-complete}$$

$$\text{SAT} : \phi = \exists x_1, \ldots, x_n \varphi(x_1, x_2, \ldots, x_n) \in \text{NP-complete}$$

$$\text{TAUT} : \phi = \forall x_1, \ldots, x_n \varphi(x_1, x_2, \ldots, x_n) \in \text{coNP-complete}$$

PSPACE-complete

The QBF game

$$\varphi(x_1, x_2, \ldots, x_{2n})$$

Player 1 wins $\iff$ $\varphi(x_1, x_2, \ldots, x_{2n})$ is true.

Does player 1 has a *winning strategy*?

$$\exists x_1 \forall x_2 \exists x_3 \forall x_4 \cdots \forall x_{2n} \varphi(x_1, x_2, \ldots, x_{2n})$$

NP *vs.* PSPACE

$$\mathsf{NP} \stackrel{?}{=} \mathsf{PSPACE}$$

Short certificate for winning strategy?

PH

Definition (Polynomial Hierarchy)

$L \in \sum_i^p$ if $\exists$ polynomial-time decidable *relation* $R(x, u_1, u_2, \ldots, u_i)$ such that $\forall x \in \{0,1\}^*$,

$$x \in L \iff \exists u_1 \in \{0,1\} \forall u_2 \in \{0,1\} \cdots Q_i u_i \in \{0,1\}$$
$$R(x, u_1, u_2, \ldots, u_i) = 1$$

$$\prod_1^p = \text{co} \sum_1^p$$

$$\sum_1^p = \text{NP} \qquad \prod_1^p = \text{coNP}$$

$$\text{PH} = \bigcup_i \sum_i^p$$

$$\text{Unique-SAT} \in \sum_2^p$$

Summary

$$\mathsf{P} \subseteq \mathsf{NP} \subseteq \mathsf{PH} \subseteq \mathsf{PSPACE} \subseteq \mathsf{EXP}$$

$$\mathsf{P} \subsetneq \mathsf{EXP}$$

References

- "Computational Complexity — A Modern Approach" by Arora and Barak (the first 5 chapters)
- "Computer and Intractability — A Guide to the Theory of NP-Completeness" by Garey and Johnson

If HAM-CYCLE $\in$ P

TC 34.2–3

$$\text{HAM-CYCLE} \in \text{P} \implies \text{HAM-CYCLE-LIST} \in \text{P}$$

1. starting from v
2. removing each edge e on v
3. checking $G \setminus e$
4. restoring and marking the critical edge $e = (v, u)$
5. $v = u$

Reference

http://www.cs.wustl.edu/~pless/441/hw3soln.pdf

Question

remove $e \in E$ in arbitrary order if $(G \setminus e) \in$ HAM-CYCLE?

$G^3 \in$ HAM-CYCLE

TC 34.2–11 (Karaganis, 1968)

$$G^3 \in \text{HAM-CYCLE}$$

References

- "On the Cube of a Graph" by Jerome J. Karaganis, 1968
- "The Cube of Every Connected Graph is 1-Hamiltonian" by Gary Chartrand and S. F. Kapoor, 1968
- http://www.aco.gatech.edu/sites/default/files/documents/comp-fa14sol.pdf

$G^3 \in$ HAM-CYCLE

Theorem ($T^3 \in$ HAM-CYCLE)

Let $T = (V, E)$ be a tree. For any edge $e \in E$, there is a Hamilton cycle on T^3 that contains e.

Proof.

By induction on subtrees obtained by removing any edge $e = (u, v)$. □

Question

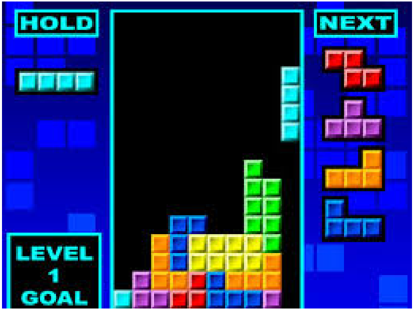
In I.S., choose edge $e = (u, v)$ with u or v being a leaf?

Tetris is NP-complete

References

- "6.890 Algorithmic Lower Bounds: Fun with Hardness Proofs", by Prof. Erik Demaine, Fall 2014 (Lecture 03, from 00:51:00)
- "Tetris is Hard, Made Easy" by Ron Breukelaar, Hendrik Jan Hoogeboom, and Walter A. Kosters, 2003

Tetris



TETRIS

Definition (TETRIS: The Tetris Problem)

$$\text{TETRIS} \in \text{NP}$$

3-PARTITION

Definition (3-PARTITION)

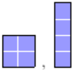
3-PARTITION $\leq_p$ TETRIS: the initial board

3-PARTITION $\leq_p$ TETRIS: the piece sequence

1. First for every $a_i \in A$ the sequence (in this order):

   
   'begin'

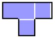
   followed by a_i times (),
   'middle'

   followed by ()
   'end'

2. Then to fill the top of all the s buckets the 'subset fillers':

   s times 

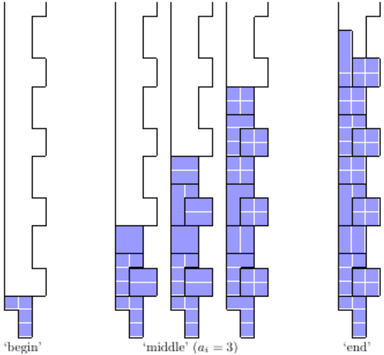
3. Then the T-shape to unlock the 'lock':

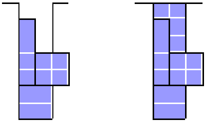
   

4. And to clear the whole board by filling the 'fill area':

   $5T + 16$ times 

3-PARTITION $\leq_p$ TETRIS: " $\Longrightarrow$ "





3-PARTITION $\leq_p$ TETRIS: " $\Longleftarrow$ "


THANK YOU