Algorithms and Complexity

- IA Algorithm I,II
- IB Complexity, Computation

Language and Automata

$L \subseteq \Sigma^\star$, $\forall x \in L$, the length $n = |x|$

Reference: Formal Language and Automata

Reduction

Reduction of $L_1 \to L_2$ is a computable function $f : \Sigma_1^\star \to \Sigma_2^\star$ s.t.

- $\forall x \in \Sigma_1^\star . f(x) \in L_2 \Leftrightarrow x \in L_1$.
- every string in L_1 is only mapped by f to a string in L_2.

Polynomial time reducible $L_1 \leq_P L_2$.

- the string $f(x)$ produced by the reduction f on input x
- must be bounded in length by $p(n)$.
- transitive as $g \circ f$ is polynomial reduction $L_1 \to L_3$
- g is polynomial function $L_2 \to L_3$

Usage,

- L_2 is decidable $\to L_1$ is decidable
- by $f(x) \in / \notin L_2$
- L_1 is not decidable $\to L_2$ is not decidable
- L_1: Halting problem

Complexity Class

Polynomial p is of form n^k, k is a constant.

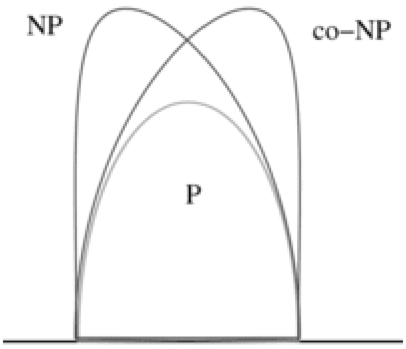
$L \in \mathcal{P} = \bigcup_{k=1}^{\infty} TIME(n^k)$

$L \in \mathcal{NP} = \bigcup_{k=1}^{\infty} NTIME(n^k)$

- Prover $M : x \in L \to certificate\ c$ and $|c| < p(|x|)$
- solvable by a nondeterministic TM M within $p(|x|)$
- Verifier V
- $\exists c.(x, c)$ is accepted by V running in polynomial time
- verifiable by a deterministic TM V in polynomial time
- polynomially satisfiable / certificate of membership (L)

Complement: $L \in \text{co-}\mathcal{NP}$

- $\forall c.(x, c)$ are all not accepted by V in polynomial time
- polynomially falsifiable / certificates of disqualification
- Relationship with $\mathcal{NP}, \mathcal{P}$: Unknown.



$L \in \mathcal{NP}\text{-hard}$

- if $\forall A \in \mathcal{NP}, A \leq_P L$.

$L \in \mathcal{NP}\text{-complete}$

- if $L \in \mathcal{NP}$ and $\mathcal{NP}\text{-hard}.$

Lists of Algorithms

- IA Algorithm I,II
- IB Complexity
- II Randomized Algorithm, BioInfo

Decision problem: output starts with ?.

- Negation of decision problem swaps the accept/reject state in TM
  - $SAT = rej, S\bar{A}T = acc$

Optimization problem: output starts with max / min.

Number Theory

$input \in \mathbb{N}$, $n := \#(bits\mathbb{B})$

Algorithm	Input	Output	Complexity	Note
Euclid's algo	(x, y)	$?x = 1$	$O(\log x + \log y)$	in #bits
Prime/COMPosite	$1\{0,1\}^\star$	Prime or Factor	$O(\sqrt{x})$	in #bits
Knapsack	$I = (v_i, w_i), W_M, V_m$	$?\exists I' \subseteq I.W \leq W_M$ $\wedge V \geq V_m$	$\mathcal{NP}$-complete	$X3C <_p it$
Schedule	/	/	$\mathcal{NP}$-complete	$Knapsack <_p it$

Boolean / nCNF

Variables $X = \{x_1, x_2, ...\}$

Expression $\phi : X$,

- CNF $\phi \equiv C_1 \wedge ... \wedge C_m$
- 3CNF ϕ'
    - each clause C_i is ≤ 3 literals disjunction
    - ϕ conversion to ϕ' in P.

Assignment $T : X \to \mathbb{B}$

- CVP, $l : X \to \mathbb{B} \cup \{\wedge, \vee, \neg\}$

Algorithm	Input	Output	Complexity	Note
Evaluation	ϕ, T	$?\mathbb{T}.$	$O(n^2)$	$each\ rule\ O(n)$ remove one variable
SAT	ϕ	$?\exists T.T(X) = \mathbb{T}$	$O(2^n n^2)$	$(\# T); \mathcal{NP}\text{-complete}$
VAL	ϕ	$?\forall T.T(X) = \mathbb{T}$	$O(2^n n^2)$	$\neg\phi_{S\bar{A}T}$ [negate both IO]
CVP	DiG	$Circuit\ Value\ \mathbb{B}$	$\mathcal{P}$	linear T by topological sort
CNF-SAT	ϕ_{CNF}	Same as SAT	$\mathcal{NP}\text{-complete}$	$SAT <_p it$
3SAT	ϕ_{3CNF}	Same as SAT	$\mathcal{NP}\text{-complete}$	$\text{CNF-SAT} <_p it$

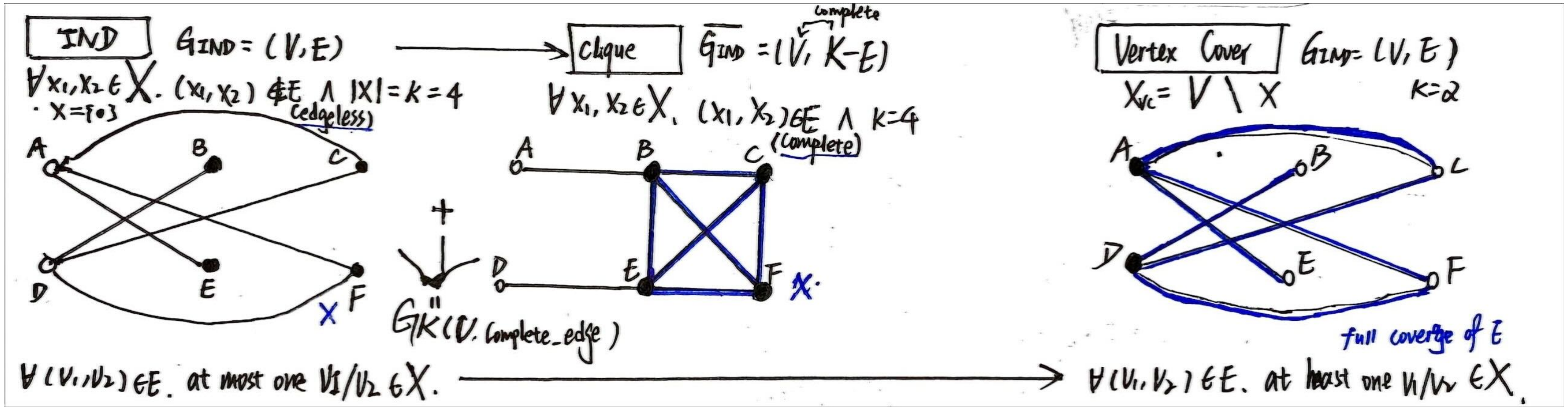
Graph Theory

$G : (V, E)$, Directed Acyclic Graph $DiAG$, Undirected Graph UnG,

Node / Vertex $v \in V$, the number of nodes $n = |V|$

Algorithm	Input	Output	Complexity	Note
Reachability	DiG, v_1, v_2	$?\exists p.path(v_1 \to v_2).$	$O(n^2); S(n)$	marked V, neighbours
HAMiltonian	G	$?\exists cycle.path(v_1 \to all!v_i \to v_1)$	$O(n!)$ $\mathcal{NP}\text{-complete}$	$3SAT <_p it$

Algorithm	Input	Output	Complexity	Note
TSP	$G, C: V \times V \to N$	order/enum for V HAM with min Cost	$O(n!)/O(2^n n^2)$ $\mathcal{NP}$-complete	$\Omega(n \log n)$ $HAM <_p it$
Isomorphism	G_1, G_2	$?\exists f.(v_1, v_2) \in E_1 \Leftrightarrow$ $f(v_1), f(v_2) \in E_2$	$O(n!)$	all possible bijections
k-colourability	G	assignment of colours	$k = 2, \mathcal{P}$ $\mathcal{NP}$-complete	 $3SAT <_p k = 3$
INDependent Set	$UnG, k = \|X\|$	$?\exists X \subseteq V.\forall x_i.(x_1, x_2) \notin E$ $or\ \forall(v_1, v_2) \in E.$ $v_1, v_2\ at\ most\ one \in X.$	$\mathcal{NP}$-complete	$3SAT <_p it$
Clique	$UnG, k = \|X\|$	$?\exists X \subseteq V.\forall x_i.(x_1, x_2) \in E$	$\mathcal{NP}$-complete	$\bar{G}_{IND}, X_{IND}$
Vertex Cover	$UnG, k = \|X\|$	$?\exists X \subseteq V.\forall(v_1, v_2) \in E.$ $v_1 \in X \vee v_2 \in X (at\ least\ 1)$	$\mathcal{NP}$-complete	$G_{IND}, V - X_{IND}$



Set Theory

Algorithm	Input	Output	Complexity	Note
Bipartite	$B, G, M \subseteq B \times G$	? $\exists M'.\forall b \in B, g \in G.(b,g) \in M'$ and pairwise disjoint	$\mathcal{P}$	
3D Matching	X, Y, Z, M	similar as above	$\mathcal{NP}$-complete	$3SAT <_p it$
eXact Cover by 3-Sets	$U(3n), S(3) \subset \mathbb{P}(U)$	?$\exists S^*$ pairwise disjoint and full coverage	$\mathcal{NP}$-complete	$U =_{3DM} X \cup Y \cup Z$
Set Cover	$U, S \subset \mathbb{P}(U), n$	?$\exists S^*$ full coverage	$\mathcal{NP}$-complete	$(U_{X3C}, S_{X3C}, \frac{\lvert U_{X3C} \rvert}{3})$ $E(G_{VC}), E(v_i) \lvert deg(v) > 0$