TCS HW4

1

下将 $\mathrm{VERTEX-COVER}$, $\mathrm{DONIMATING-SET}$ 分别简记为 VC, DS.

先证明 $\mathrm{DS} \in \mathbf{NP}$. 只需非确定性地猜测支配集中的 k 个顶点, 并验证该集合是支配集即可. 显然这可在多项式时间内完成.

再证明 $\mathrm{VC} \leq_p \mathrm{DS}$.

不妨只考虑连通图, 否则逐个考察连通分支即可.

如下构造 $f : \langle G, k\rangle \mapsto \langle G', k\rangle$:

- 若 $k > |V(G)|$, 则显然 $\langle G, k\rangle \notin \mathrm{VC}$, 取 $G' = G$ 即可, 此时 $\langle G, k\rangle \notin \mathrm{DS}$.
- 若 $k \leq |V(G)|$, 对图 G 中的每个 $e_i = (u_i, v_i) \in E(G)$, 添加点 w_i 和边 $(u_i, w_i), (v_i, w_i)$, 如此得到 G'. 显然这可在多项式时间完成.

下证明 f 是 VC 到 DS 的归约, 即证 $\langle G, k\rangle \in \mathrm{VC} \iff \langle G', k\rangle \in \mathrm{DS}$. 显然只需考虑 $k \leq V(G)$ 时.

$(\Longrightarrow)$

我们断言: G 的点覆盖 S 就是 G' 的支配集.

这是因为, $\forall w \in V(G') - V(S)$,

- 若 $w \in V(G)$, 任取 G 中与 w 关联的一条边 e, e 的另一个端点 u 必在点覆盖 S 中, 从而 w 被支配.
- 若 $w \in V(G') - V(G)$, 由 G' 的构造方式知, $\exists u, v \in V(G)$, $(u, v) \in E(G)$, $(u, w), (v, w) \in E(G')$. 由于 S 是点覆盖, 必有 $u \in S \vee v \in S$, 从而 w 被支配.

$(\Longleftarrow)$

设 G' 有支配集 S.

对于 $\forall e = (u, v) \in E(G)$:

- 若 $u \in S \vee v \in S$, 则 e 被覆盖.
- 若 $u \notin S \wedge v \notin S$, 由于在构造 G' 时为 e 添加的那个点 w 未被支配, 必有 $w \in S$, 从而 $S \leftarrow (S - \{w\}) \cup \{u\}$ 覆盖 e.

对每个 $e \in E(G)$ 都如是操作, 所得 S 覆盖了 G 的所有边. 令 $S' = \{v | v \in S \cap V(G)\}$, 显然 S' 是 G 的一个点覆盖, $|S'| \leq k \leq |V(G)|$, 再向 S' 中加入一些 $V(G) - S'$ 中的点, 使 $|S'| = k$, 就得到了 G 的 k 元点覆盖.

至此, 我们证明了 $\mathrm{VC} \leq_p \mathrm{DS}$, 再由 $\leq_p$ 的传递性, 立刻得到 $\mathrm{DS} \in \mathbf{NPC}$.

2

设一元语言 $L \in \mathbf{NPC}$, 故存在多项式时间归约 $f : \Sigma^* \to \Sigma^*, w \in \mathrm{SAT} \iff f(w) \in L$.

设 f 在 n^c 时间内运行.

我们称一个 CNF 的集合是可满足的, 如果其中存在一个 CNF 是可满足的.

先证明一个引理.

引理: 对于一个 CNF 集合 $S, \forall w \in S, |w| \le n, |S| > n^c$, 可以在 $n|S|$ 的多项式时间内找到 $S' \subset S$, $|S'| \le n^c$, 使得 S' 与 S 的可满足性相同.

- 首先, 我们计算出所有 $f(w), w \in S$, 然后删去 $f(w) \notin 1^+$ 的那些 w. 这是因为 $f(w) \notin L$, 必有 $f \notin \mathrm{SAT}$.
- 如果此时仍有 $|S| > n^c$, 注意到 f 在 n^c 时间内运行, 故必有 $f(w) \in \{1^k | 1 \le k \le n^c\}$, 由鸽巢原理, $\exists w_1, w_2 \in S$, $w_1 \ne w_2$, $f(w_1) = f(w_2)$. 这样一来, $w_1 \in \mathrm{SAT} \iff w_2 \in \mathrm{SAT}$, 故可删去所有这样的 w_2, 直到 $|S| \le n^c$.
- 至此, 我们得到了所需 S'. 由于所有操作只涉及计算 $f(\cdot)$ 和字符串比较, 易知整个过程在 $n|S|$ 的多项式时间完成.

回到该题, 我们给出 SAT 的一个多项式时间判定算法, 从而说明 $\mathbf{P} = \mathbf{NP}$.

对于一个给定的CNF $\phi(x_1, x_2, \cdots, x_k)$, $|\phi| = n$.

$$\{\phi(x_1, x_2, \cdots, x_k)\}$$

的可满足性等价于

$$\{\phi(0, x_2, \cdots, x_k), \phi(1, x_2, \cdots, x_k)\}$$

的可满足性, 又等价于

$$\{\phi(0, 0, x_3, \dots, x_k), \phi(0, 1, x_3, \dots, x_k), \phi(1, 0, x_3, \cdots, x_k), \phi(1, 1, x_3, \cdots, x_k)\}$$

的可满足性.

如是展开 k 轮, 在每一轮展开后, 一旦集合的规模超过了 n^c (此时集合中至多有 n^{2c} 个元素), 就使用引理缩小集合规模. 最终, 我们得到了至多 n^c 个不含变量的 CNF, 每一个的可满足性都可在 $O(n)$ 时间内判定, 然后一一判定即可.

不难发现, 以上过程的每一步都能在多项式时间内完成, 因此我们得到了一个多项式时间的 SAT 判定算法, 故 $\mathbf{P} = \mathbf{NP}$.

3

先证明 $\mathrm{SPACETM} \in \mathbf{PSPACE}$.

构造图灵机 $M =$ "对于输入 $\langle M, w, 1^n \rangle$, 模拟 $M(w)$, 一旦某一步使用了 n 格纸带以外的空间, 直接拒绝. 运行结束后, 输出 $M(w)$ 的结果."

显然 M 在多项式空间内判定 $\mathrm{SPACETM}$, 故 $\mathrm{SPACETM} \in \mathbf{PSPACE}$.

再证明 $\forall L \in \mathbf{PSPACE}, L \le_p \mathrm{SPACETM}$.

存在图灵机 M 和常数 c, M 在 n^c 空间内判定 L. 故 $w \in L \iff \langle M, w, 1^{n^c} \rangle \in \mathrm{SPACETM}$.

这个归约 $f : w \mapsto \langle M, w, 1^{n^c} \rangle$ 显然可在多项式时间完成.

综上, $\mathrm{SPACETM}$ 是 $\mathbf{PSPACE}$ 完全的.

4

以下将 $\mathrm{EXACT\ INDSET}$ 简记为 EI.

(1)

注意到

$$\langle G,k\rangle \in \mathrm{EI} \iff \langle G,k\rangle \in \mathrm{INDSET} \wedge \langle G,k+1\rangle \notin \mathrm{INDESET}.$$

并且我们知道 $\mathrm{INDESET} \in \mathbf{NP}$.

故取

$$\begin{aligned} L_1 &= \mathrm{INDSET}, \\ L_2 &= \{\langle G,k\rangle | \langle G,k+1\rangle \notin \mathrm{INDSET}\}. \end{aligned}$$

即有 $\mathrm{EI} = L_1 \cap L_2$, $L_1 \in \mathbf{NP}$, $L_2 \in \mathbf{coNP}$.

(2)

首先, 为了得到更强的结果, 我们需要改造传统的 $3\mathrm{SAT}$ 到 INDSET 的归约. 我们仍将 k 元 3CNF 的每个子句映射成 7 个点, 分别对应子句的七种可满足赋值, 并对子句间和子句内矛盾的赋值连边. 在此基础上, 我们增加 $k-1$ 个点, 并从这 $k-1$ 个点到所有其它点连边.

同时, 记 $EI(G)$ 为 G 的最大独立集中的顶点数, 即 $EI(G)=k \iff \langle G,k\rangle \in \mathrm{EI}$.

在这种归约 h 下, 不难证明, 对于 k 元 3CNF ϕ:

$$\begin{aligned} \phi \in \mathrm{SAT} &\iff EI(h(\phi)) = k, \\ \phi \notin \mathrm{SAT} &\iff EI(h(\phi)) = k-1. \end{aligned}$$

然后, 我们给出一个后面将用到的引理: 若 $EI(G_1)=k_1, EI(G_2)=k_2$, 则它们的积图 $G_1 \times G_2$ 满足 $EI(G_1 \times G_2) = k_1 k_2$.

这个引理很容易证明, 并不是本题的重点, 因此不再赘述.

回到本题, 我们证明 $\forall L = L_1 \cap L_2 \in \mathrm{DP}$, 其中 $L_1 \in \mathbf{NP}$, $L_2 \in \mathbf{coNP}$, 都满足 $L \leq_p \mathrm{EI}$.

我们知道 SAT 是 $\mathbf{NP}$ 完全的, $\overline{\mathrm{SAT}}$ 是 $\mathbf{coNP}$ 完全的, 故存在多项式时间归约 f, g, 满足

$$\begin{aligned} w \in L_1 &\iff f(w) \in \mathrm{SAT}, \\ w \in L_2 &\iff g(w) \notin \mathrm{SAT}. \end{aligned}$$

于是有

$$w \in L \iff f(w) \in \mathrm{SAT} \wedge g(w) \notin \mathrm{SAT}.$$

设 $f(w)$ 是 k_1 元 3CNF, $g(w)$ 是 k_2 元 3CNF. 由于总是可以添加由新变元构成的子句, 不妨设 $k_1 \neq k_2, k_1 > 0, k_2 > 0$.

记 $G_1 = h(f(w)), G_2 = h(g(w))$, 接下来我们证明

$$w \in L \iff \langle G_1 \times G_2, k_1(k_2-1)\rangle \in \mathrm{EI}. \, (*)$$

$(\Longrightarrow)$

$$\begin{aligned} w \in L &\Longrightarrow f(w) \in \mathrm{SAT} \wedge g(w) \notin \mathrm{SAT} \\ &\Longrightarrow EI(G_1) = k_1 \wedge EI(G_2) = k_2 - 1 \\ &\Longrightarrow EI(G_1 \times G_2) = k_1(k_2-1). \end{aligned}$$

$(\Longleftarrow)$

我们去证明逆否命题, 即

$$w \notin L \implies \langle G_1 \times G_2, k_1(k_2-1)\rangle \notin \mathrm{EI}.$$

由于

$$w \notin L \Longrightarrow \neg(f(w) \in \mathrm{SAT} \wedge g(w) \notin \mathrm{SAT}),$$

且有

$$\begin{aligned} \neg(f(w) \in \mathrm{SAT} \wedge g(w) \notin \mathrm{SAT}) \vdash & (f(w) \in \mathrm{SAT} \wedge g(w) \in \mathrm{SAT}) \\ & \vee(f(w) \notin \mathrm{SAT} \wedge g(w) \notin \mathrm{SAT}) \\ & \vee(f(w) \notin \mathrm{SAT} \wedge g(w) \in \mathrm{SAT}), \end{aligned}$$

我们可以分三种情况讨论:

- $f(w) \in \mathrm{SAT} \wedge g(w) \in \mathrm{SAT}$: $EI(G_1 \times G_2) = k_1k_2 \neq k_1(k_2-1)$.
- $f(w) \notin \mathrm{SAT} \wedge g(w) \notin \mathrm{SAT}$: $EI(G_1 \times G_2) = (k_1-1)(k_2-1) \neq k_1(k_2-1)$.
- $f(w) \notin \mathrm{SAT} \wedge g(w) \in \mathrm{SAT}$: $EI(G_1 \times G_2) = (k_1-1)k_2 \neq k_1(k_2-1)$.

至此, 我们证明了 $(*)$, 也就得到了 L 到 EI 的一个多项式归约.

5

将该语言记为 A.

先证明 $A \in \mathbf{NL}$. 由于 $\mathbf{NL} = \mathbf{coNL}$, 只需证 $\overline{A} \in \mathbf{NL}$.

构造非确定性图灵机 $M =$"对于输入 $\langle G\rangle$, 非确定性选择一对顶点 $\langle s,t\rangle$, 模拟运行 $\mathrm{PATH}(\langle G,s,t\rangle)$, 并反转其输出."

显然 M 在对数空间内判定 $\overline{A}$, 故 $A \in \mathbf{NL}$.

再证 A 是 $\mathbf{NL}$ 完全的. 只需证 $\mathrm{PATH} \leq_l A$.

对于给定的 $\langle G,s,t\rangle$ 中的每个 $v \in V(G)$, 增加边 $\langle t,v\rangle, \langle v,s\rangle$, 得到 G'. 由于只需要修改邻接矩阵 (或边的其它编码), 显然 G' 的每一位都可在对数空间计算出.

下证明 $f : \langle G,s,t\rangle \mapsto \langle G'\rangle$ 是 PATH 到 A 的归约, 即证 $\langle G,s,t\rangle \in \mathrm{PATH} \iff \langle G'\rangle \in A$.

$(\Longrightarrow)$ 若在 G 中 s 可达 t, 那么在 G' 中, $\forall u,v \in V(G')$, 都存在路径 $u \to s \to t \to v$, 因此 G' 是强连通图.

$(\Longleftarrow)$ 若 G' 是强连通图, 则存在 s 到 t 的路径 C, 其中除端点外不出现 s,t. 显然, C 中没有形如 $\langle t,v\rangle, \langle v,s\rangle$ 的边, 因此这 C 也是 G 中的一条路径, 即 G 中 s 可达 t.

综上, A 是 $\mathbf{NL}$ 完全的.

6

将该语言类记为 C.

先证明 $C \subseteq \mathbf{NP}$. 我们知道 $\mathrm{NSPACE}(f) \subseteq \mathrm{DTIME}(2^{O(f)})$, 故对数空间验证机也是一个多项式时间验证机, 自然就有 $C \subseteq \mathbf{NP}$.

再证明 $\mathbf{NP} \subseteq C$.

$\forall A \in \mathbf{NP}$, 存在非确定性图灵机 M 和常数 c, M 在 n^c 时间内判定 A.

那么, M 的每个格局可用 $O(n^c)$ 位编码.

构造验证机 $M' =$ "对于输入 $\langle w, u\rangle$, 将 u 看作 M 运行 w 的格局序列, 检查 u 是否是合法的接受格局序列, 若是则接受, 否则拒绝."

显然 M' 在对数空间内运行, 且一个接受格局序列的长度是 $O(n^{2c})$ 的.

由于 $w \in A$ 等价于存在 M 接受 w 的格局序列, 故 M' 确实判定了 A, 于是得到 $\mathbf{NP} \subseteq C$.

综上, $C = \mathbf{NP}$.