Lecture 13

1765331700 GMT0

Access available at: https://archive.tmysam.top/notebookw14.pdf

Review

假设 $P \neq NP$，则存在 $NP \cap NPH = NPC$

L 是 NPC 的，当

1. $L \in NP$
2. $(\forall k \in NP)(k \leq_P L)$

规约：（最坏情况）

$SAT \to_P 3SAT$

$SAT \to_P INTEGERPROG$

$3SAT \to_P INDSET$

$3SAT \to_P ExactOneSAT$

$ExactOneSAT \to_P SubsetSum$

$INDSET \to_P CLIQUE$

$INDSET \to_P VERTEXCOVER$

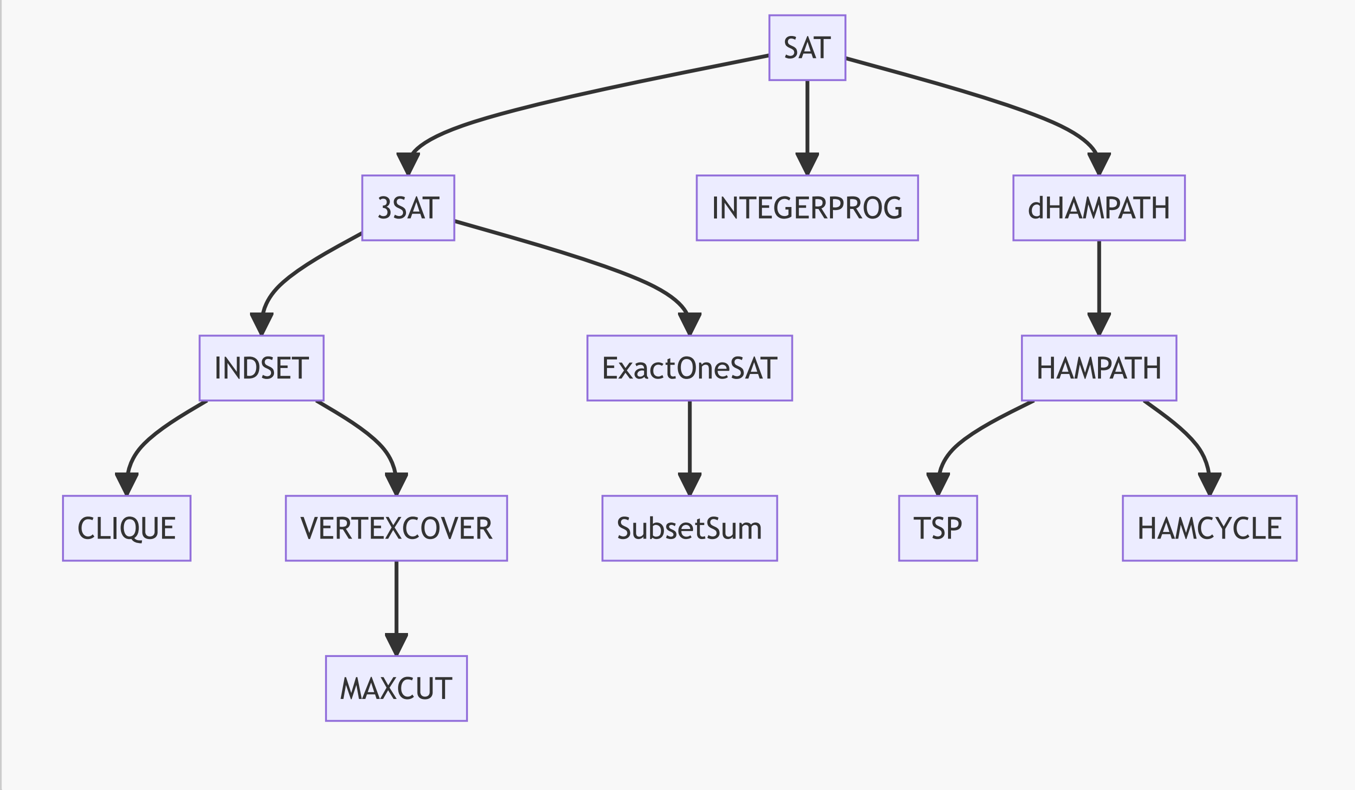
$VERTEXCOVER \to_P MAXCUT$

$SAT \to_P dHAMPATH$

$dHAMPATH \to_P HAMPATH$

$HAMPATH \to_P TSP$

$HAMPATH \to_P HAMCYCLE$



一个问题的 Hard 体现在某些实例上，但是这些实例可能不好找

对于 平均情况，知之甚少。

一方面知道一些问题是 NPH，但另一方面这些问题可能也可以比较快地使用启发式算法找到一个近似解。

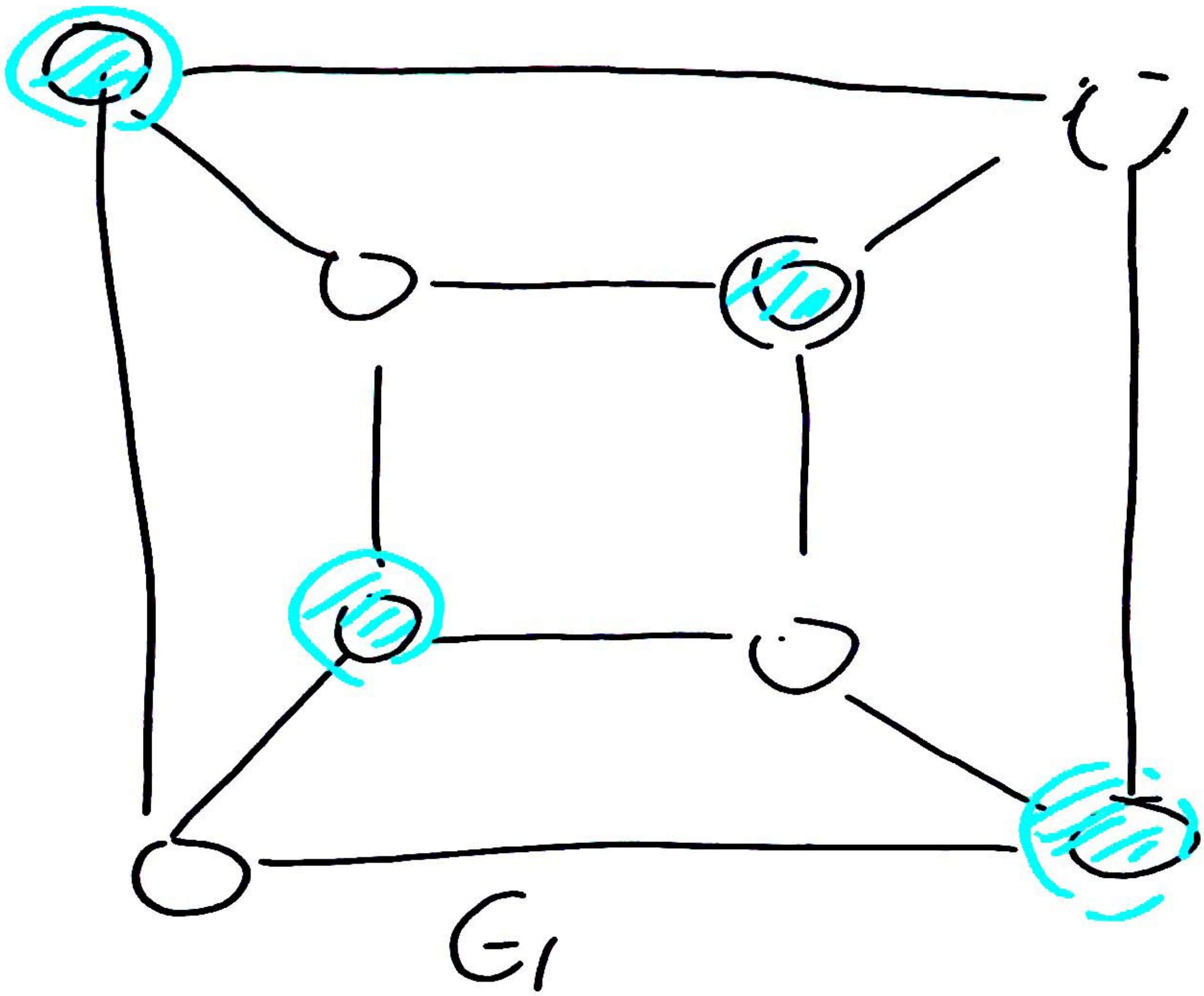
继续证明 INDSET 是 NPH

$INDSET = \{< G, k >: G\text{有一个大小为}k\text{的独立集}\}$

用邻接矩阵表示图 G

$|V(G)| = v$，$| < G > | = O(v^2)$（邻接表会产生一些麻烦）

独立集：一些顶点，使得这些顶点之间没有边相连



对于以上的图：

$< G, 4 >\in INDSET$

$< G, 5 >\notin INDSET$

> 定理5.28：INDSET 是 NPC。

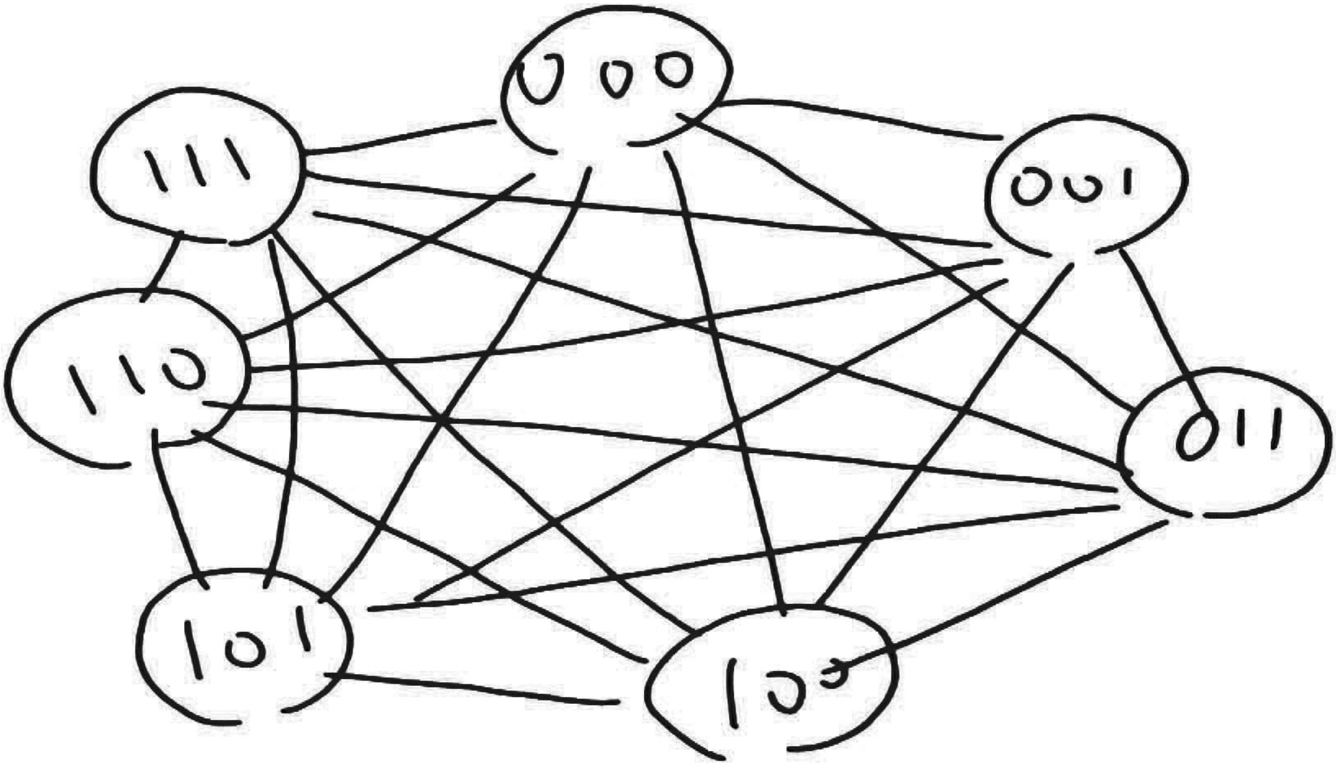
$3SAT \leq_P INDSET$

给定任意的 3CNF φ，其中有 m 个子句，可以构造一个图 G，使得其中有 $\leq 8m$ 个顶点，则：

1. $\varphi \in SAT \implies < G, m >\in INDSET$
2. $\varphi \notin SAT \implies < G, m >\notin INDSET$

对于每一个子句，都制造一个簇，包含 ≤ 8 个满足条件的赋值。将这 ≤ 8 个点之间连边。

例如对于：$C = x_1 \vee \bar{x}_2 \vee x_3$，则除了$(0,1,0)$ 之外的 7 个赋值都满足该子句。



（也就是在这个团里至多选一个）

对于不同的子句，当赋值有矛盾的时候，将这些点之间连边。

例如子句 $x_1 \vee \bar{x}_2 \vee x_5$ 的一个赋值 $(0,0,1)$ 和子句 $x_2 \vee x_3 \vee \bar{x}_5$ 的一个赋值 $(1,0,1)$ 之间有矛盾（对于 x_2 的赋值不同，不能同时出现），因此将这两个点之间连边。

规约是可以在多项式时间内完成的。（最多有 $8m$ 个顶点，边的数量也是多项式级别的）

∎

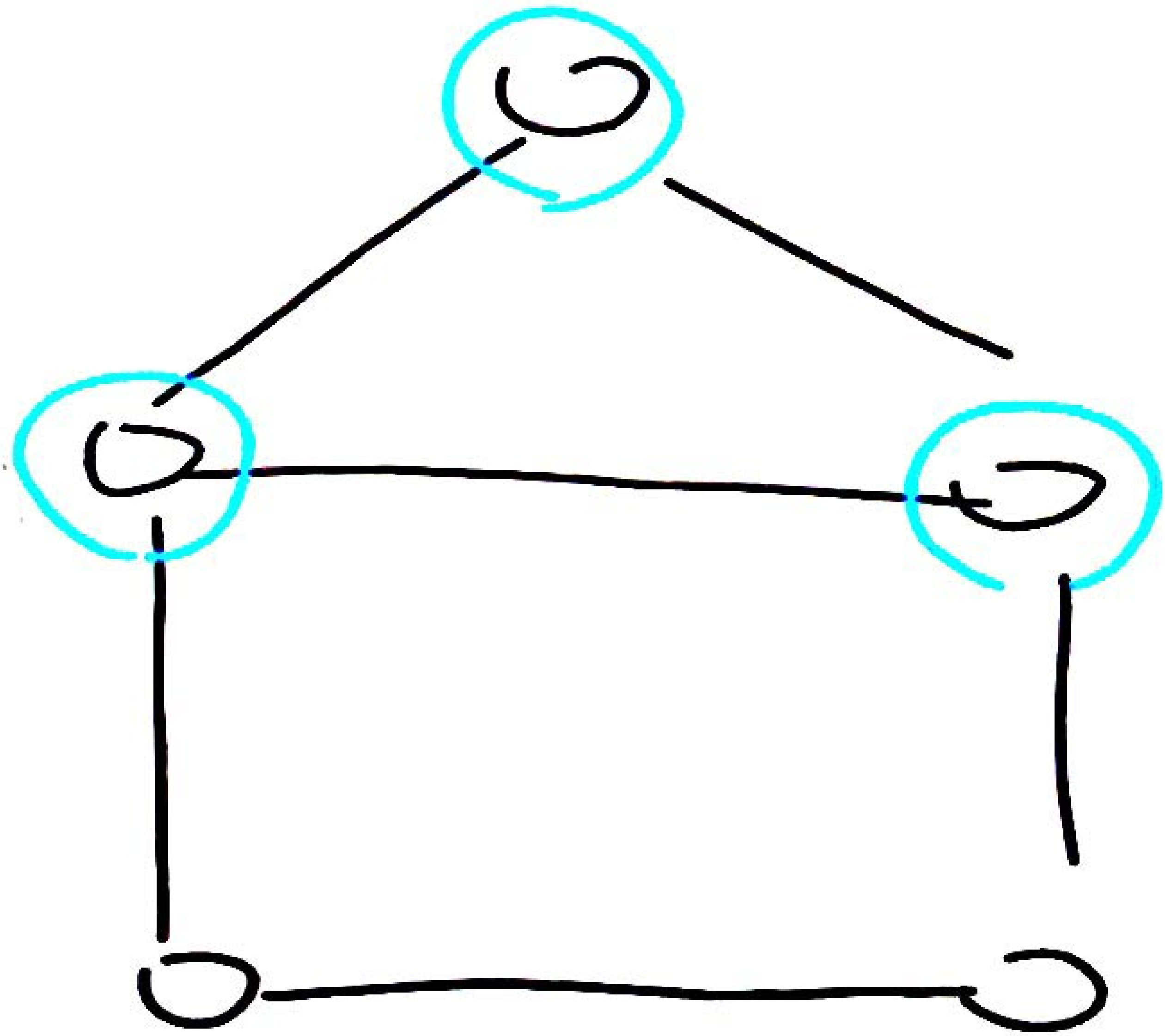
（反方向也是可以规约的，则独立集与 SAT 等价）

φ 是可以满足的 $\iff$ G 有独立集，大小为 m。

Clique 问题

$CLIQUE = \{< G, k >: G\text{有一个大小为}k\text{的团}\}$

团：一个子图，为完全图



$< G, 3 > \in CLIQUE$，则存在 3 个顶点，两两之间都有边相连。

$< G, 4 > \notin CLIQUE$，则不存在 4 个顶点，两两之间都有边相连。

> 定理5.29：CLIQUE 是 NPC。

证书 是一个包含 k 个顶点的集合。

验证器 检查这些顶点之间是否两两相连。

证明 $INDSET \leq_P CLIQUE$。

给定图 G，与整数 k。

$< G, k > \in INDSET \iff < \bar{G}, k > \in CLIQUE$

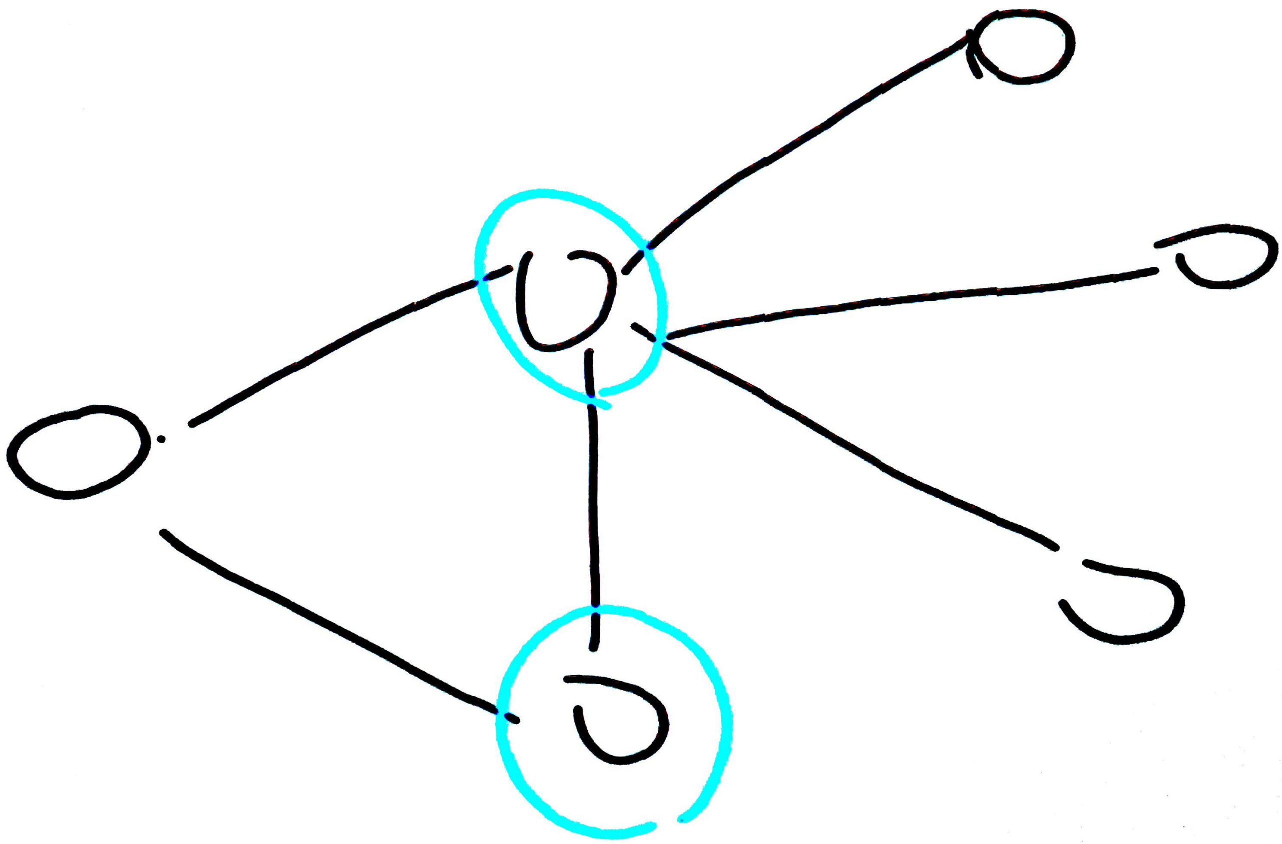
∎

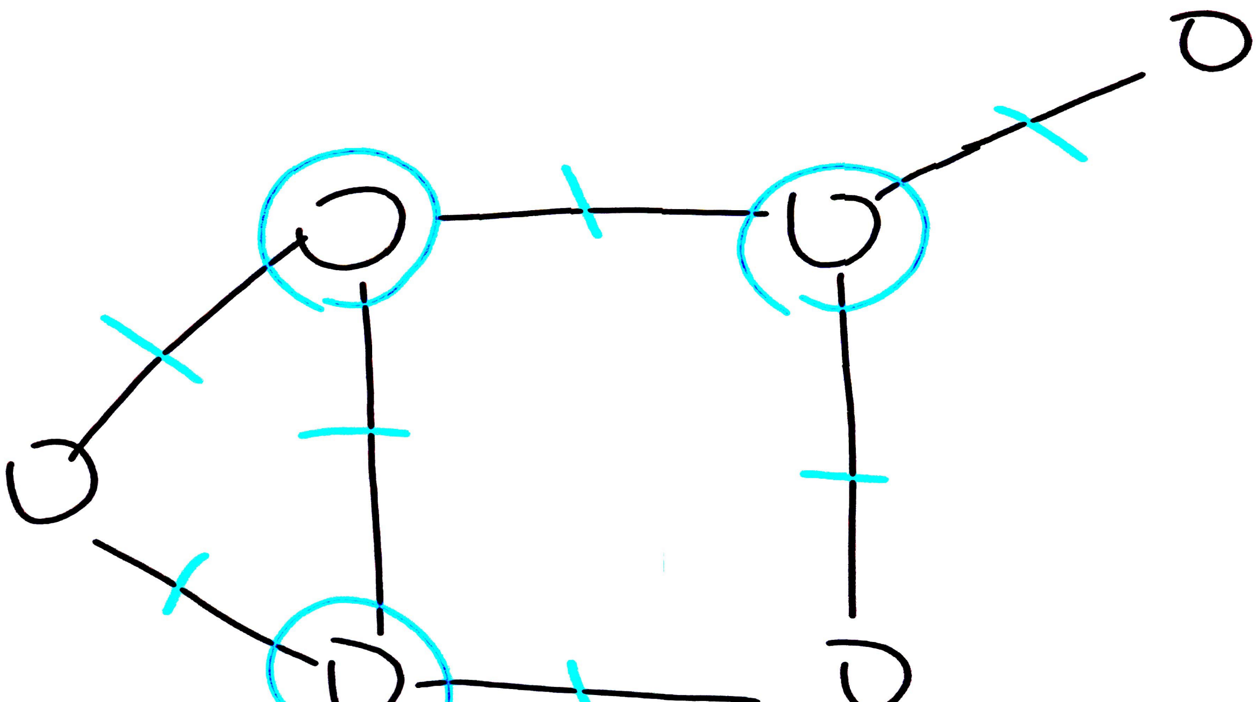
Vertex Cover 问题

$VERTEXCOVER = \{< G, k >: G\text{有一个大小为}k\text{的顶点覆盖}\}$

顶点覆盖：图 G 的一个顶点子集 S，使得图 G 的每一条边至少有一个端点在 S 中。

最小覆盖：找到最小的顶点覆盖。





> 定理5.30：VERTEXCOVER 是 NPC。

顶点是顶点覆盖 $\iff$ 剩下的顶点是独立集

证书 是一个包含 k 个顶点的集合。

验证器 检查这些顶点是否覆盖了图 G 的所有边。

证明 $INDSET \leq_P VERTEXCOVER$。

令 $G=(V,E)$，其中 $W \subseteq V$，W 是 G 的一个顶点覆盖 $\iff$ $V-W$ 是 G 的一个独立集。

$< G,k > \in INDSET \iff < G,|V(G)|-k > \in VERTEXCOVER$

∎

dHAMPATH 问题

$dHAMPATH = \{< G,s,t >: \text{有向图}G\text{有一条从 } s \text{ 到 } t \text{ 的 Hamilton 路径}\}$

> 定理5.31：dHAMPATH 是 NPC。

证书 是一条从 s 到 t 的 Hamilton 路径。

验证器 检查路径是否合法，并且经过了图 G 的每一个顶点恰好一次。

证明 $3SAT \leq_P dHAMPATH$。

给定一个 3CNF φ，可以构造一个有向图 G，使得：

- s 和 t 是图 G 的两个特殊顶点
- 令 φ 可满足 $\iff$ $< G,s,t > \in dHAMPATH$

由 s 出发，依次经过每一个变量的“片段”（variable gadget），每一个变量的“片段“有两条路径，分别对应该变量取真或取假。

假设 φ 有 n 个变量，m 个子句。

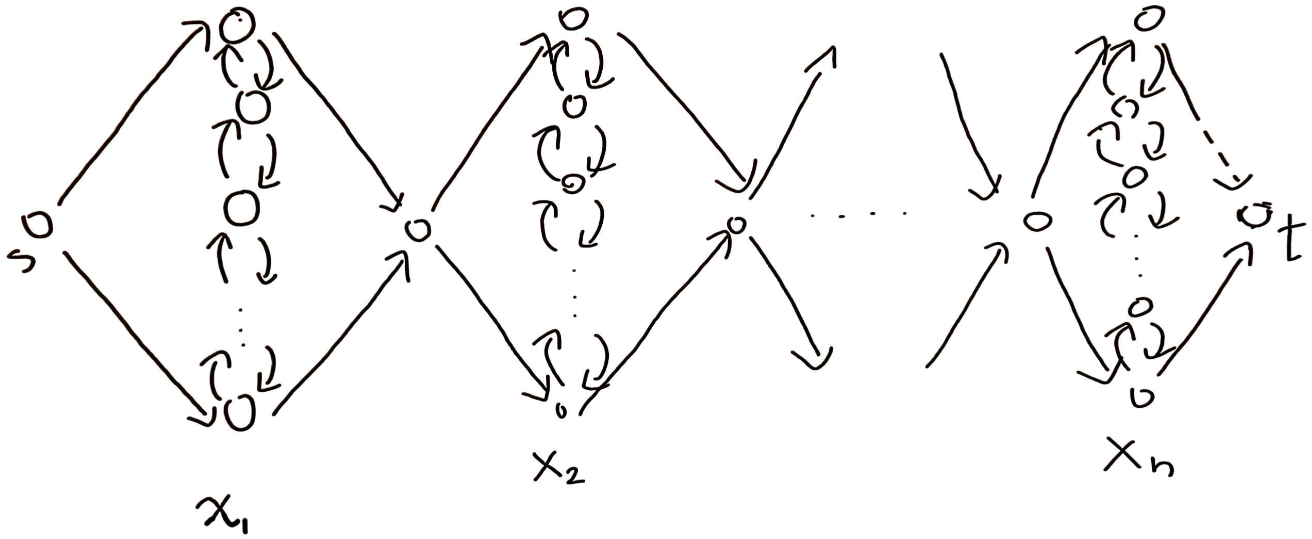
> 下面部分加的点的数量与课内讲述有所不同，但逻辑相同。

先构造图：包含 s 和 t，以及 $x_{i,j}$ （$i=1,2,...,n$，$j=0,1,2,...,m$），x_i （$i=0,1,2,...,n$，$x_0=s$，$x_n=t$）。

加边：

- $x_i \to x_{i+1,0}$，$x_i \to x_{i+1,m}$
- $x_{i+1,0} \to x_{i+1}$，$x_{i+1,m} \to x_{i+1}$
- $x_{i,j} \to x_{i,j-1}$，$x_{i,j} \to x_{i,j+1}$

这就保证每个“菱形”可且只可从两个方向之一（真或假）遍历。

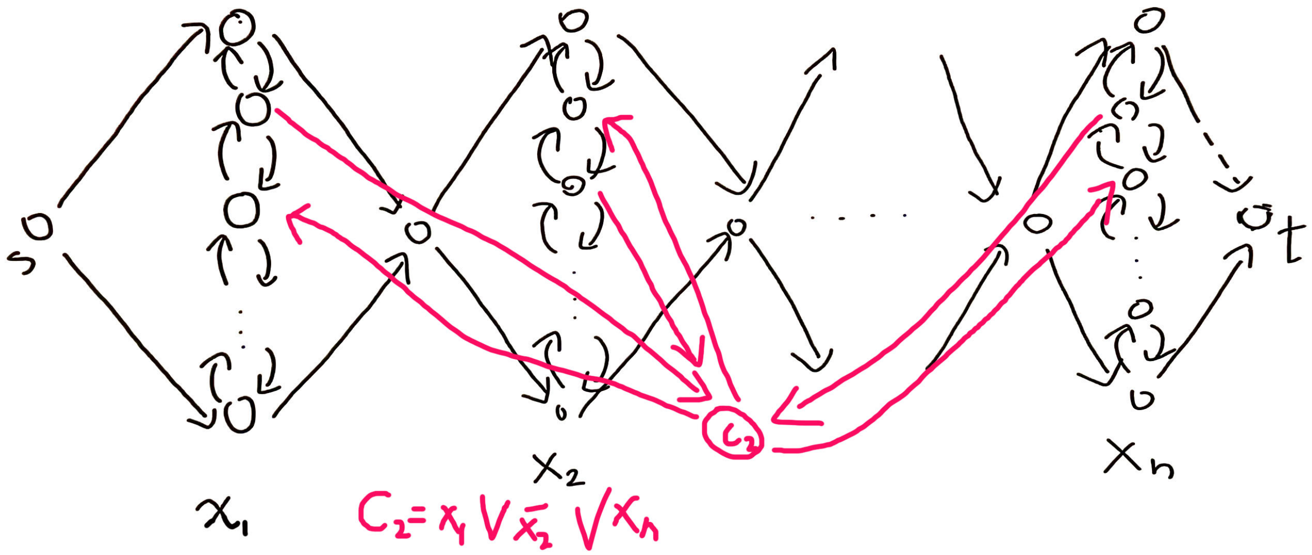


然后增加一些顶点 c_j，代表各个子句。

当有变量 x_k 出现在子句 c_j 中时：

- 如果 x_k 是正出现的，则增加边 $x_{k,j-1} \to c_j$ 和 $c_j \to x_{k,j}$
- 如果 x_k 是反出现的，则增加边 $x_{k,j} \to c_j$ 和 $c_j \to x_{k,j-1}$

这就要求，当经过某个"菱形"时，如果选择了某个变量的赋值为真（或假），则可以"顺路"访问该变量所满足的子句顶点。



这样如果 φ 可满足，则可以构造一条从 s 到 t 的 Hamilton 路径，反之亦然。

∎

HAMPATH 问题

$HAMPATH = \{< G, s, t >\text{: 无向图}G\text{有一条从 } s \text{ 到 } t \text{ 的 Hamilton 路径}\}$

显然有 $HAMPATH \leq_P dHAMPATH$。只需对每一条无向边 (u, v)，变为两条有向边 $u \to v$ 和 $v \to u$ 即可。

> 定理5.32：HAMPATH 是 NPC。

证书 是一条从 s 到 t 的 Hamilton 路径。

验证器 检查路径是否合法，并且经过了图 G 的每一个顶点恰好一次。

证明 $dHAMPATH \leq_P HAMPATH$。

给定任意有向图 $G(V, E)$，以及顶点 $s, t \in V(G)$。考虑构造无向图 $G'(V', E')$，$s', t' \in V(G')$，使得:

- G 中存在一条从 s 到 t 的 Hamilton 路径 $\iff$ G' 中存在一条从 s' 到 t' 的 Hamilton 路径

对任意 $v \in V(G) \setminus \{s, t\}$，在 G' 中创建三个顶点 v_{in}, v_{mid}, v_{out}。有边 (v_{in}, v_{mid}) 和 (v_{mid}, v_{out})。

对边 $(u, v) \in E(G)(u \neq s, v \neq t)$，在 G' 中创建无向边 (u_{out}, v_{in})。

对边 $(s, v) \in E(G)$，在 G' 中创建无向边 (s', v_{in})。

对边 $(u, t) \in E(G)$，在 G' 中创建无向边 (u_{out}, t')。

因为

- 一旦从 s' 出发，下一个一定访问到某个 u_{in}
- 一旦某个 u_{in} 被访问到，下一个一定是 u_{mid} （否则以后就无法访问到 u_{mid} 了）
- 一旦某个 u_{mid} 被访问到，下一个一定是 u_{out}
- 一旦某个 u_{out} 被访问到，下一个只能是某个 v_{in} 或 t'
- 最终必须到达 t'

$\blacksquare$

通过有向图的 Hamilton 路径转换为转换后的无向图给出的 Hamilton 路径是简单且显然的，读者自证不难。

通过转换后的无向图给出的 Hamilton 路径转换为有向图的 Hamilton 路径是简单且显然的，读者自证不难。

问题

是否有问题 L 满足 $L \in NP$，但 $L \notin P$ 且 $L \notin NPC$?

假设 $P \neq NP$。

猜想:

- 大整数分解问题
- 图同构问题

> 定理5.33：**假设** $P \neq NP$，则存在 $L \in NP$，且 $L \notin P$。

通过 "padding" 对输入变长（塞垃圾）

输入 x $|x| = n$，构造 $x' = x\#2^n$

时间分层定理、时空关系

$\mathrm{DTIME}(n) \subsetneq \mathrm{DTIME}(n^2) \subsetneq \mathrm{DTIME}(n^3) \ldots$

$P \subsetneq E \subsetneq EXP$