§5.6 基本NP完全问题的证明

- 定理1 三可满足问题(3SAT)是NP完全问题。

(证) 整个证明过程分成两步，

先证 $3SAT \in NP$，

再证明$SAT \propto 3SAT$.

$3SAT \in NP$是显然的，因为很容易构造一不确定算法，

该算法第一阶段猜一个函数

f： U→{真, 假}。

- 然后，第二阶段检测公式**F**的值，
- 这只需将公式**F**中的所有因子**u**及¬**u**分别用**f(u)**和**f(u)**的补替代，
- 即用“真”或“假”替代，
- 再对逻辑式求值。
- 容易看出，第二阶段所需时间是**m**和**n**的多项式
- 其中**m**是集合**U**的逻辑变量的个数，
- **n**是公式**F**的项的个数。

- **SAT** $\propto$ **3SAT**就不那末明显了。
- 先构造映射

  $$g: \mathbf{SAT} \rightarrow \mathbf{3SAT}$$

- 其中**SAT**表示可满足性问题的实例之集合
- **3SAT**表示三可满足性问题的实例的集合。
- 然后再证明**g**是多项式转换。
- **SAT**的实例为
- ①集合$\mathbf{U} = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m\}$
- ②公式$\mathbf{F} = \{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n\}$，
- 其中$\mathbf{c}_i$ $(\mathbf{i} = \mathbf{1}, \mathbf{2}, \ldots, \mathbf{n})$是项。
- 以**U**及**F**为输入，**g**为**3SAT**构造实例**U'**及**F'**如下所述:

- $U' = U \cup U'_1 \cup U'_2 \cup \ldots \cup U'_n$
- $F' = C'_1 \cup C'_2 \cup \ldots \cup C'_n$
- 其中C'_j是项的集合，且每一项含三个因子
- 因此**F′**也是项的集合，所以**F′**是公式。
- 由上两式可见:
- 逻辑变量集合**U**增加一些变量,
- 再改写公式**F**的每一项为项集合,
- 就得到三可满足问题的实例。
- 还需证明**F′**是可满足的充分必要条件为
- **F**是可满足的。

- 为定义映射g，只须说明如何构造C'_j及U'_j.
- 公式F的项C_j是因子的集合

$$C_j = \{Z_1, Z_2, \ldots, Z_K\}$$

即$|C_j| = K$，C_j由K个因子组成。

C'_j及U'_j的构成按K的值

分四种情况讨论。

- $K=1$， $C_j = \{z_1\}$， 则U'_j及C'_j构造为

  $U'_j = \{y_{j1}, y_{j2}\}$

  增加两个逻辑变量而已

$C'_j = \{\{z_1, y_{j1}, \neg y_{j2}\}, \{z_1, \neg y_{j1}, y_{j2}\}, \{z_1, y_{j1}, y_{j2}\},$

$\{z_1, \neg y_{j1}, \neg y_{j2}\}\}$

即C'_j含四个项。

将C_j一个项替换为四个项.

注意: 这四个项穷尽两个逻辑变量y_{j1}, y_{j2}

的四种情况

$K=2$， $C_j=\{z_1, z_2\}$，则

$U'_j = \{y_j\}$

仅仅增加一个逻辑变量

$C'_j = \{\{z_1, z_2, y_j\}, \{z_1, z_2, \neg y_j\}\}$

即C'_j含两项。

将C_j一个项替换为两个项.

注意: 这两个项穷尽一个逻辑变量y_j

的两种情况

$K = 3$， $C_j = \{z_1, z_2, z_3\}$，则

$U'_j = \Phi$

不增加逻辑变量

$C'_j = \{\{z_1, z_2, z_3\}\}$

即C'_j含一项。

- K>3， $C_j = \{z_1, z_2, \ldots, z_k\}$， 则
- $U'_j = \{y_{j1}, y_{j2}, \ldots, y_{jk-3}\}$, 增加K - 3个逻辑变量
- $C'_j = \{ \{z_1, z_2, y_{j1}\},$

$\{z_3, \neg y_{j1}, y_{j2}\},$

$\{z_4, \neg y_{j2}, y_{j3}\}, \ldots,$

$\{z_{i-1}, \neg y_{ji-3}, y_{ji-2}\},$

$\{z_i, \neg y_{ji-2}, y_{ji-1}\},$

$\{z_{i+1}, \neg y_{ji-1}, y_{ji}\}, \ldots,$

$\{z_{k-2}, \neg y_{jk-4}, y_{jk-3}\},$

$\{z_{k-1}, z_k, \neg y_{jk-3}\}\}$

若K=4, 则增一个变量

第一项和最后一项各含两个z(原变量)和一个y(新增变量).

其余各项含一个z和两个y(其中一个是因子的非)

- 即C'_j含(K—2)项, 比$|U'_j|$大1。
- 若K=4, 则含两项.

- 显然，映射g为3SAT问题计算一个实例所需时间为m和n的多项式。
- 要增加n个变量集合, 对应F中的n个项.
- 每个集合至多含m-3个变量, m为U中因子的个数

- 要把n个项改写为n个 项集合
- 每个集合至多含m-2个项, 每项有三个因子.

- 现在证明如**F**可满足, 则**F′**也可满足. 设
- $\mathbf{f}$： $\mathbf{U} \to$ {真, 假}
- 能使**F**值为真。
- 因**U**是**U′**的子集, 只须证明**f**可以扩展为
- $\mathbf{f'}$： $\mathbf{U'} \to$ {真, 假}
- 并使公式**F′**为真；
- 从而只要给诸$\mathbf{U'}_j$的各逻辑变量赋值
- 保持**U**的逻辑变量的赋值不变,
- 并使**F′**为真即可

- 因集合
- $(U' - U)$
- 中的逻辑变量被划分为集合U'_j，
- U'_j中的逻辑变量仅出现在相应的C'_j中,
- 因此只须证明,
- 映射f'可以逐次扩展到各集合U'_j,
- 每次扩展使C'_j中的项的值都为真.

- 同样分四种情况，
- ①$\mathbf{K=1}$，
- 用数理逻辑的方法很容易证明$\mathbf{C'_j}$和$\mathbf{C_j}$恒等，(P7)
- 即$\mathbf{C'_j}$的值只与$\mathbf{z_1}$有关，
- 因$\mathbf{f}$已经满足$\mathbf{C_j}$，
- 则$\mathbf{f'}$不论给$\mathbf{y_{j1}}$, $\mathbf{y_{j2}}$赋什么值都能使$\mathbf{C'_j}$满足。

- ②**K=2**，同样可用数理逻辑
- 证明$\mathbf{C'_j}$和$\mathbf{C_j}$恒等，
- 即$\mathbf{C'_j}$的值只与$\mathbf{z_1}$，$\mathbf{z_2}$有关，
- 因**f**已经满足$\mathbf{C_j}$，
- 则不论**f**给$\mathbf{y_j}$赋什么值, 都可使$\mathbf{C'_j}$满足

- ③**K=3**，(P9)
- $\mathbf{U'_j}$为空，
- 且$\mathbf{C'_j}$只含一个项, 就是$\mathbf{C_j}$, 已被**f**满足。
- $\mathbf{C_j}$已经含三个因子, 被**f**赋值，
- 因此**f**, 不用给任何新逻辑变量赋值。

- ④**K>3**，
- $C_j = \{z_1, z_2, \ldots, z_k\}$，因f已满足$C_j$，
- 此即C_j的K个因子中至少一个为真，
- 设z_i为真，
- 按i的值分三种情况,
- 讨论如何扩展映射f

- (i) **i**为**1**或**2**，则令
- $y_{j1}=y_{j2}=\ldots=y_{jK-3}=$假
- 这使C'_j的每一项都为真。
- (ii)如**i**为**K－4**或**K－3**，则令
- $y_{j1}=y_{j2}=\ldots=y_{jK-3}=$ 真
- 这也使C'_j的每一项都为真。
- (iii)如**2<i<K－4**，则令
- $y_{j1}=y_{j2}=\ldots=y_{ji-2}=$ 真
- $y_{ji-1}=y_{ji}=\ldots=y_{jK-3}=$ 假
- 这又使C'_j的每一项都为真。

- 这就证明了公式F'中所有的C'_j都被满足，
- 也就证明了公式F'被我们构造的映射f'满足。

- 现在证明如F'可满足，则F亦可满足。
- 设存在映射
- f'： $U' \to \{$真, 假$\}$
- 使公式F'值为真.
- 如何定义映射 f ?

- 定义映射
- **f**：**U** →{真，假}
- 为
- **f(u)**＝ **f′(u)** **(u∈U)**
- **U**是**U′**的子集，如**u∈U**，则**u∈U′**

- 现在证明**f**满足公式**F**，即**f**使公式**F**的值为真。

- 此即, C'_j 被满足, 要证明C_j也能被满足
- ① $K = l$, C'_j有四项 (P7)
- 这四个项穷尽两个逻辑变量y_{j1}, y_{j2}的四种情况

不论给y_{j1}, y_{j2}赋什么值,

一定有某个项的后两个因子值均假,

这就是说z_1必定为真.

所以, C_j被满足了.

- ② $K = 2$， C'_j有两项
- 这两个项穷尽逻辑变量y_{j1}的两种情况

不论给y_{j1}赋什么值,

必有一项的最后一个因子为假,

这就是说z_1和z_2必定有一个为真.

所以, C_j被满足了.

- ③ **K = 3**,
- C'_j只含有一项, 与C_j相同
- 既然C'_j满足了, 当然C_j也满足了.

- ④ **K>3**,
- **f′**满足**C′**$_j$，则只须证明**f′**使
- z_1，z_2，…，z_k
- 中至少有一个的值为真。用反证法.
- 令
- $z_1, z_2, \ldots, z_k$
- 皆假, 用“假”替代**C′**$_j$中的诸**z**，再简化**C′**$_j$
- 则**C′**$_j$等价为

- $C'_j = \{ \{y_{j1}\},$

  $\{\neg y_{j1}, y_{j2}\},$

  $\{\neg y_{j2}, y_{j3}\}, \cdots,$

  $\{\neg y_{ji-3}, y_{ji-2}\},$

  $\{\neg y_{ji-2}, y_{ji-1}\},$

  $\{\neg y_{ji-1}, y_{ji}\}, \cdots,$

  $\{\neg y_{jk-4}, y_{jk-3}\},$

  $\{\neg y_{jk-3}\}\}$
- 因C'_j被满足，则其各项之值皆“真”。
- 第一项之值为真，则必有
- $f'(y_{j1}) =$ 真

- 第二项$\{\neg y_{j1}, y_{j2}\}$等价于$\{y_{j2}\}$，其值为真，则必有
- $f'(y_{j2}) = $ 真
- 以此类推，由Cj的倒数第二项为“真”知，必有
- $f'(y_{jK-3}) = $ 真
- 但是由此确定的映射没能满足C'_j
- 因为C'_j的最后一项
- $\{\neg y_{jk-3}\}$
- 必定为假，从而使C'_j值为假，即公式F′值为假，这与f′满足F′的假设矛盾。

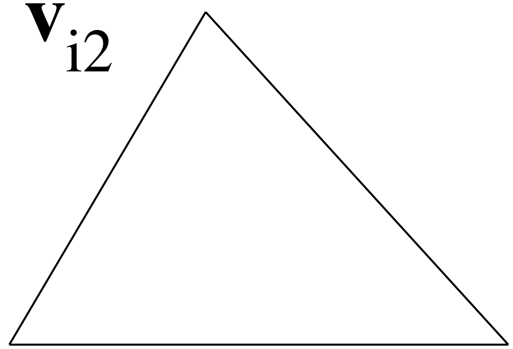
- 这反证了C_j中诸因子
- $z_1, z_2, \ldots, z_k$
- 至少有一个为真，这使C_j值为真. 因此映射f使公式F满足。证毕。

- 定理2 顶点覆盖问题(VC)是NP完全问题。
- 证明过程梗概
- 先定义3SAT $\propto$ VC的多项式转换f.
- 3SAT问题的实例为两个集合
- $U = \{u_1, u_2, \ldots, u_n\}$
- $F = \{C_1, C_2, \ldots, C_m\}$
- 其中C_i(i=1，2，…，m)为含三个因子的项

- 由**3SAT**的实例, 映射**g**构造**VC**问题的实例有以下四步骤。
- ①对每一个逻辑变量$\mathbf{u}_i \in \mathbf{U}$，构造子图

- 该子图由两个节点$\mathbf{u}_i$，$\neg\mathbf{u}_i$ 及一条边组成。

- ②对每一项$\mathbf{C}_i \in \mathbf{F}$构造子图
- $\mathbf{v}_{i2}$



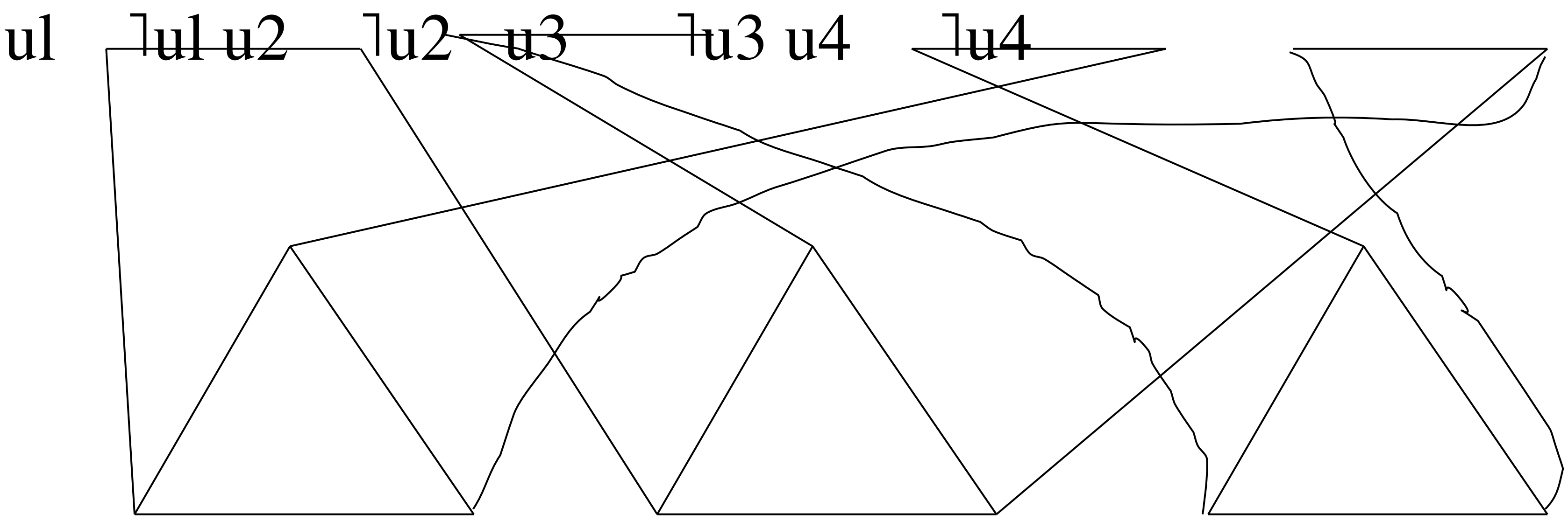
- $\mathbf{v}_{i1}$ $\mathbf{v}_{i3}$
- 以$\mathbf{C}_i$的三个因子为顶点,
- 建造一个三角形(有三条边)

- ③对项$C_i = \{v_{i1}, v_{i2}, v_{i3}\}$中每个因子
- $v_{ij}(j = 1, 2, 3)$,
- 如$v_{ij} = u$ $(u \in U)$,
- 则连接节点**u**(由①构造)和节点v_{ij}(由②构造)
- 如$v_{ij} = \neg u$,
- 则连接节点$\neg u$和节点v_{ij}
- 由以上三步得到VC实例的图。
- ④令K=n+2m, n=|U| m=|F|

- 证明之前, 给一个例子.

- 设3SAT问题有如下实例
- U = {u1, u2, u3, u4}
- F = {{ul, ¬u3, ¬u4}, {¬ul, u2, ¬u4},
  {u2, u3, u4}}

真 真 假 假



K=10

显然实例是可满足的，f如上所示。

为证明本定理,须证明两件事.

1. $VC \in NP$

- 设VC问题的实例$G = (V, E)$
- 构造一不确定算法，该算法第一阶段猜一个$V' \subset V$(V'是V的子集,且$|V'|=K$)
- 第二阶段检测V'是否为G的K覆盖.
- 这阶段的时间复杂度是多项式的.

所以VC问题可由多项式时间不确定算法解决

因此,$VC \in NP$

2. 前面定义的映射g是从3SAT到VC的多项式转换。

- g的四步骤的时间复杂度都是多项式的
- 所以g的复杂度也是多项式的

- 下面证明3SAT的实例可满足的充分必要条件是:
- 它在VC的像实例有K覆盖.

- 先设**3SAT**问题的实例可满足,欲证明其在**VC**的像实例有**K**覆盖
- 存在映射**f**, 给逻辑变量集合**U**的各个**u**赋值, 使得**F**的所有项
- $\mathbf{C}_1,\mathbf{C}_{\mathbf{2}},\ldots,\mathbf{C}_m$
- 的值均为真.
- 构造**VC**的像实例的**K**覆盖如下.

- 考虑每一个逻辑变量**u**,
- 若映射**f**给**u**的赋值为真, 则将①构造的线段的左侧端点选入覆盖
- 否则, 把右侧端点选入覆盖
- 入选的有**n**个结点
- 它们覆盖了①构造的**n**条线段

- 又因为②的构造方法, 每个项
- $C_i = \{v_{i1}, v_{i2}, v_{i3}\}$
- 的三个因子至少一个(记作v)的值为真.
- v对应着②构造的子图中的一个结点,
- 除去它,将另两个结点选入覆盖,
- 它们覆盖了三角形的三条边
- 共选入了2m个结点
- (该项对应着②构造的子图——三角形)

- v是三角形中的一个结点，
- 它和①的线段的一端相连接.

- 总共选入了n+2m个结点.
- 将证明这构成了VC实例的K覆盖.

- 由①构造的n条线段和②构造的三角形的3m条边已经被它们覆盖
- 下面证明③连接的3m条边也被覆盖
- 每个三角形有两个结点被选入, 相应的两条边被覆盖
- 第三个结点(v)没有被选入,但是与之相连的、在①的线段里的端点被选入.
- 所以, 第三条边也被覆盖了.

- 充分性得证, 下面证明必要性

- 先设其在VC的像实例有K覆盖,
- 欲证明3SAT问题的实例可满足

- 注意到K=n+2m
- 考虑由①建造的线段，
- 每条线段的两端点必有一端在K覆盖,否则该线段无法覆盖
- 共n个结点
- 由此定义映射f(u)如下:
- 若与u对应的线段的左侧结点在覆盖则
-   f(u)=真
- 否则f(u)=假

- 考虑由②建造的三角形,
- 为覆盖这三边, 必有两个顶点在K覆盖, 共2m个结点.
- 注意: 已经有了n+2m=K个结点.
- 考虑由③添加的三条线段,
- 三角形有两个顶点在K覆盖, 与之相连的两线段则被覆盖,
- 第三个顶点v没有入选K覆盖,

- 所以由③添加的第三条线段的覆盖责任,必定由不在三角形的端点u承担
- 这个端点u必定就是前一页的入选端点,
- 若这个端点是线段的左侧结点则
- 该结点对应的逻辑变量赋值为真
- 第三顶点v的赋值为真;
- 若这个端点是线段的右侧结点则
- 该结点对应的逻辑变量赋值为假
- 第三顶点v的赋值也为真

- 所以, 三角形对应的项的逻辑值因而为真
- 所以公式**F**的值也就是真
- 所以**3SAT**的实例可满足.
- 证毕

- 定义 图G＝(V, E)的独立集合V′是V的子集
- 且如u、$v \in V'$，则(u，v) $\notin$ E，
- 即V′中的任两个节点之间不存在边。
- 如|V′|＝K，则V，称为G的K独立集合。
-
- 独立集合问题(简称IS)
- 实例：图G＝(V，E)及正整数J≤|V|
- 问：G是否有独立集合V′且|V′|≥J

- 引理 图**G＝(V，E)**， **V′**是**V**的子集**V′ ⊂V.**
- 下述三命题是等价的:
- **1. V′**是**G**的覆盖
- **2. (V—V′)**是**G**的独立集合
- **3. (V—V′)**是**G**的补图**G′ ＝(V，E′)**的集团, 其中

- $E' = \{(u, v) \mid u、v \in V，(u，v) \notin E\}$

- 引理通过独立集合将覆盖与集团联系起来

- 证 引理可以分三步来证明
- ① ② ③
- $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$
- ①$1 \Rightarrow 2$, 使用反证法
- 设$(V—V')$不是G的独立集合
- 则存在两点u、$v \in (V—V')$, 但是
- $(u, v) \in E$
- 因为u、$v \in (V—V')$,所以
- u、$v \notin V'$
- 这与"V'是G的覆盖"矛盾(V'没有覆盖边(u, v))

- ②**2** $\Rightarrow$ **3**
- **(V—V′)**是**G**的独立集合
- 任意两点**u**、**v** $\in$ **(V—V′),**
- 则**(u, v)** $\notin$ E
- 根据补图的定义, 有**(u, v)** $\in$ E′**,**
- 所以**, (V—V′)**是**G**的补图**G′** ＝**(V**，**E′)**的集团

- ③ **3 $\Rightarrow$ 1**
- **(V—V′)是G的补图G′ = (V，E′)的集团,**
- 用反证法证明**V′**是**G**的覆盖。
- 设**V′**不是**G**的覆盖，则
- **G**中存在边**(u，v)** $\in$ **E**，但是
- $\mathbf{u} \notin \mathbf{V'}$，$\mathbf{v} \notin \mathbf{V'}$，
- 则必有
- $\mathbf{u} \in \mathbf{V—V'}$, $\mathbf{v} \in \mathbf{V—V'}$，
- 因**(V—V′)**是**G′**的集团，则
- $\mathbf{(u，v)} \in \mathbf{E'}$
- 由补图定义知
- $\mathbf{(u，v)} \notin \mathbf{E}$
- 这与前面假设矛盾。定理证毕.

- 引理告诉我们, 覆盖、独立集合、集团三者只是同一个问题的不同叙述。
- 上述引理提供了极为简单的方法,
- 可将一个问题转换为其它两个问题。譬如,
- 欲将顶点覆盖问题转换为集团问题，只需映射
- **f**：**VC → CL**
- 由**VC**的实例：**G = (V, E)**及正整数**K**，映射**f**构造**CL**的实例：图**G′**(**G**的补图)和
- 正整数**J = |V|—K**.

- 因此只要证这三个问题中一个是**NP**完全问题
- 就证明了三个问题都是**NP**完全问题**.**
- 由定理**2**可证得定理**3**。

- 定理**3** 集团问题**(CL)**和独立集合问题**(IS)**是**NP**完全问题

- 定理**4** 哈密尔顿回路问题**(HC)**是**NP**完全问题
- 下一节**§5-8**给出定理的完整证明

- 先用定理**4**的结论证明巡回售货员问题**(TS)**
- 是**NP**完全问题。

- 定理**5** 巡回售货员问题**(TS)**是**NP**完全问题
- 定理**5**的证明很简单，本章第四节的例子已经证明
- $$\mathbf{HC} \propto \mathbf{TS}$$
- 又$\mathbf{TS} \in \mathbf{NP}$是明显的，
- 定理**4**结论为
- 哈密尔顿问题**(HC)**是**NP**完全问题，
- 所以**TS**问题是**NP**完全问题