

Lovász 局部引理

从存在性到随机化构造

小概率坏事件、局部依赖与局部修复

即使并合界无法给出有用结论，大量局部约束仍可能同时满足。局部引理利用 局部依赖证明解的存在；重采样将存在性转化为算法。见证树与可逆执行记录 则从两个角度解释：反复进行局部修复，为什么能够很快结束？

高级算法课程教学团队

南京大学

第六讲 · 随机算法与随机化技术

学习目标与阅读建议

本讲研究两个紧密相关的问题：大量局部约束为什么能够同时满足？怎样高效地找到满足它们的赋值？读完本讲，应当能够：

1. 构造依赖图，并区分对整个事件族的独立性与两两独立；
2. 用对称局部引理分析可满足性及超图染色，并证明非对称局部引理；
3. 实现局部重采样，区分重采样次数、变量抽样次数和事件检查开销；
4. 利用重采样表、见证树与分枝过程证明 Moser–Tardos 定理；
5. 通过编码和恢复长执行所消耗的随机比特，分析递归修复算法。

第一次阅读可沿第 1 节的可满足性例子，进入第 2 节的局部引理及其应用，再学习第 3 节的条件概率证明。第 4 节先介绍重采样算法及其保证，第 5 节再用见证树完成分析。第 6 节给出另一条独立的算法分析路线：递归修复与熵压缩。两种构造性证明使用的对象不同，一个是从历史中提取的见证树，另一个是实际递归过程的记录。

记号与计算假设在使用时引入。全文中， n 为变量数， m 为约束或坏事件数， d 为每个事件至多相邻的其他事件数。 $\Gamma(A)$ 表示开邻域， $\Gamma^+(A) = \Gamma(A) \cup \{A\}$ 表示含自身的邻域。记 $[n] = \{1, \dots, n\}$ ； $\ln$ 为自然对数， $\log_2$ 用于计算比特数；空乘积为 1。概率和期望均针对明确指定的随机实验，而非满足赋值上的任意分布。

目录

学习目标与阅读建议	i
1 局部约束与概率方法	1
2 局部引理及其应用	2
3 局部引理为什么成立	4
4 通过局部重采样找到一个解	6
5 重采样为何终止：表与见证树	7
6 递归修复与熵压缩	11
7 三个阶段分别建立了什么	14
8 习题	15
A 证明中用到的初等工具	16
文献说明	17

1 局部约束与概率方法

1.1 贯穿全讲的例子：可满足性

布尔变量取值于 $\{0,1\}$ ，其中 1 表示真。文字是变量或其否定，子句是若干文字的析取；合取范式（CNF）公式是若干子句的合取。例如，

$$\Phi = (x_1 \vee \neg x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee x_4) \wedge (x_3 \vee \neg x_4 \vee \neg x_5).$$

一个赋值满足 Φ ，当且仅当它满足所有子句。本讲约定， k -CNF 的每个子句恰好包含 k 个不同变量，每个变量只出现一个文字；特别地，子句不是永真式。因此，每个子句在其 k 个变量上恰好有一个违反它的赋值。

k -SAT 与结构化的搜索问题

给定 n 个变量上的 k -CNF 公式 $\Phi = C_1 \wedge \cdots \wedge C_m$ ， k -SAT 问它是否可满足。对固定 $k \geq 3$ ，不加限制的该问题是 NP 完全的。本讲寻找一个由子句相交程度决定的充分条件：既保证满足赋值存在，又能通过高效随机算法构造这样的赋值。

一般可满足性的计算困难，促使我们研究具有额外结构的实例；它并不排除受限实例上的高效算法。NP 完全性的背景来自 Cook-Levin 理论，参见文献说明及 [7]。

如果各子句使用的变量集合互不相交，就可以分别满足它们。另一个简单情形来自不同的思路：独立、均匀地选择 $X_1, \dots, X_n \in \{0,1\}$ ，令 A_i 为子句 C_i 被违反的坏事件。于是

$$\mathbb{P}(A_i) = 2^{-k}, \quad \mathbb{P}\left(\bigcup_{i=1}^m A_i\right) \leq \sum_{i=1}^m \mathbb{P}(A_i) = m2^{-k}. \quad (1)$$

概率 2^{-k} 来自唯一的违反比特模式，而不来自子句之间的独立性。我们只假设输入变量相互独立。因此，只要 $m < 2^k$ ，全部子句同时满足的概率就为正。

概率方法

为了证明具有某种性质的对象存在，可以先设计一个概率空间，再证明目标事件具有正概率。该事件中必定包含一个满足要求的对象。但正概率本身既不提供高效搜索算法，也不保证一次随机试验很容易成功。

1.2 为什么约束总数未必是正确参数

当子句的变量集合互不相交时，坏事件相互独立，故

$$\mathbb{P}\left(\bigcap_{i=1}^m \overline{A_i}\right) = (1 - 2^{-k})^m > 0 \quad (2)$$

对任意有限 m 都成立。此时，并合界给出的限制 $m < 2^k$ 完全没有必要。另一方面，对固定 k ，式 (2) 中的成功概率随 m 指数下降。即使各子句能够独立修复，不断重新抽取整个赋值仍可能很慢。

在互不相交与任意相交之间，还有有限依赖的情形。将共享变量的两个子句连边，假设每个子句至多与 d 个其他子句相交。我们希望用局部参数 d ，而不是总数 m ，来控制可满足性。局部引理给出一个这样的充分条件：

$$e(d+1)2^{-k} \leq 1. \quad (3)$$

这个条件允许任意多的约束。它不是对每个顶点的邻域分别使用并合界；其证明必须回答：在给定其他约束已经满足后，一个坏事件的条件概率会增加多少？

1.3 约束满足问题的统一视角

有限域约束满足问题（CSP）由变量 $x_j \in \Omega_j$ 和局部谓词 C_i 组成，每个谓词只依赖指定的变量子集。使所有谓词为真的赋值就是一个解。可满足性和超图染色是其中的两个例子。许多图论与集合系统问题也能写成约束形式，但写出约束本身，并不等于验证了局部引理条件，更不等于得到了高效的事件检查方法。

为变量选择相互独立的分布，再令 A_i 表示约束 C_i 失败。一次局部引理应用包含三个独立的建模任务：选择概率空间，估计每个坏事件的概率，以及描述事件之间的依赖。概率空间是证明设计的一部分；均匀选择适合本讲的例子，但不是局部引理的必要假设。

2 局部引理及其应用

2.1 依赖图究竟表达什么

设 $\mathcal{A} = \{A_1, \dots, A_m\}$ 是同一概率空间中的事件。事件 A, B 独立，指 $\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$ 。等价地，当 $\mathbb{P}(B) > 0$ 时，以 B 为条件不会改变 A 的概率。

定义 2.1 (依赖图)。 以 $\mathcal{A}$ 为顶点集的简单无向图称为依赖图，如果每个 A_i 都与 $\Gamma^+(A_i)$ 之外的整个事件族独立。具体而言，对任意通过指定一些非邻居事件发生或不发生而得到的事件 B ，均有

$$\mathbb{P}(A_i \cap B) = \mathbb{P}(A_i)\mathbb{P}(B). \quad (4)$$

也就是说， A_i 与非邻居们共同确定的信息独立，而不只是分别与每个非邻居独立。

依赖图不必唯一，也不必最小。添加边不会破坏定义，但可能削弱最后的数值界。非邻居事件族必须排除事件 A_i 自身。

对于独立变量 $X_1, \dots, X_n$ ，记 $\text{vbl}(A_i) \subseteq [n]$ 为确定 A_i 的一个给定变量指标集。变量相交图的邻域定义为

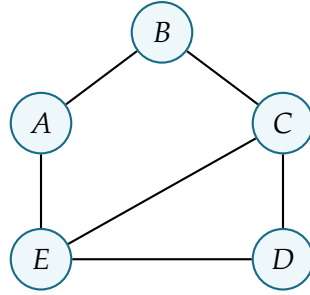
$$\Gamma(A_i) = \{A_j \neq A_i : \text{vbl}(A_i) \cap \text{vbl}(A_j) \neq \emptyset\}. \quad (5)$$

每个不在 $\Gamma^+(A_i)$ 中的事件，都只由 $\text{vbl}(A_i)$ 之外的变量确定；这些事件共同确定的信息也是如此。底层变量块的独立性说明，该图确实是依赖图。

例 2.2 (一个小的变量相交图)。 考虑如下作用域的事件：

$$A(X_1, X_2), \quad B(X_2, X_3), \quad C(X_3, X_4), \quad D(X_4), \quad E(X_1, X_4).$$

相交图的边为 AB, AE, BC, CD, CE, DE 。特别地， A 与 (C, D) 联合独立，而 C, D 彼此之间不必独立。



仅有两两独立并不够

令 U, V 为独立公平比特, 取 $A_1 = \{U = 0\}$ 、 $A_2 = \{V = 0\}$ 、 $A_3 = \{U \oplus V = 0\}$ 。三个事件两两独立, 但避免前两个事件会迫使 $U = V = 1$, 从而第三个事件发生。因此, 空图不是这组事件的依赖图。两两概率计算不能替代定义 2.1 中的联合独立条件。

2.2 先陈述对称引理, 再看两个应用

定理 2.3 (对称 Lovász 局部引理)。 设对每个 i 都有 $\mathbb{P}(A_i) \leq p$, 且事件族有一个最大度至多为 d 的依赖图。如果

$$ep(d+1) \leq 1, \quad (6)$$

则 $\mathbb{P}(\bigcap_i \overline{A_i}) > 0$ 。当 $d \geq 1$ 时, 另一个充分条件是 $4pd \leq 1$ 。当 $d = 0$ 时, 各事件相互独立, 只要每个 $\mathbb{P}(A_i) < 1$, 结论就成立。

我们先应用这个定理, 再由非对称版本推导两个数值条件。它同时使用两种信息: 单个坏事件不太可能发生, 以及整个事件族的局部依赖有限。没有依赖控制时, 仅有较小的边缘概率并不足够。

推论 2.4 (稀疏 k -CNF 的可满足性)。 若一个 k -CNF 公式中每个子句至多与 d 个其他子句共享变量, 且 $e(d+1) \leq 2^k$, 则该公式可满足。当 $d \geq 1$ 时, $d \leq 2^{k-2}$ 是另一个充分条件。

证明。 选择独立公平比特。每个子句违反事件的概率为 $p = 2^{-k}$, 子句相交图就是变量相交图。应用定理 2.3; 其另一种条件为 $4d2^{-k} \leq 1$ 。□

如果每个变量至多出现在 L 个子句中, 则 $d \leq k(L-1)$: 一个子句的每个变量至多把它连接到 $L-1$ 个其他子句。同一对相交子句可能被重复计数, 但求上界时这没有影响。

定义 2.5 (超图染色)。 k -一致超图 $H = (V, E)$ 的每条超边都是 V 的一个 k 元子集。顶点 v 的度为包含它的超边数, 最大度记为 Δ 。一个正常 q -染色为每个顶点指定 $[q]$ 中的一种颜色, 并要求没有超边为单色。

定理 2.6 (稀疏一致超图的染色)。 对 $k, q \geq 2$, 最大度为 Δ 的 k -一致超图, 只要满足

$$\Delta \leq \frac{q^{k-1}}{ek}, \quad (7)$$

就能够正常 q -染色。

证明。 独立、均匀地为每个顶点选择颜色。对超边 e , 令 A_e 表示其所有顶点同色。在 q^k 种局部赋值中, 单色赋值有 q 种, 因此 $\mathbb{P}(A_e) = q^{1-k}$ 。将相交超边连边, 每条超边至多与 $k(\Delta-1)$ 条其他超边相交。若 E 非空, 则 $\Delta \geq 1$, 并且

$$ep(d+1) \leq eq^{1-k}(k(\Delta-1)+1) \leq eq^{1-k}k\Delta \leq 1.$$

对称局部引理适用。没有超边时，染色结论显然成立。 $\square$

对固定 q 及充分大的 Δ ，取 $k \geq \log_q \Delta + \log_q \log_q \Delta + O_q(1)$ 即可达到上述条件，额外的对数用于补偿因子 k 。有限参数下的精确保证是式 (7)。注意，变量的度 Δ 与坏事件的依赖度 d 是不同参数。

2.3 非对称概率与局部预算

对称引理只使用最大的坏事件概率和最大的依赖度。当各事件的这些参数差异很大时，分别选择参数通常能保留更多信息。

定理 2.7 (非对称 Lovász 局部引理)。 设事件族 $\mathcal{A} = \{A_1, \dots, A_m\}$ 有一个依赖图。如果存在 $\alpha_i \in [0, 1]$ ，使得

$$\mathbb{P}(A_i) \leq \alpha_i \prod_{A_j \in \Gamma(A_i)} (1 - \alpha_j) \quad \text{对每个 } i, \quad (8)$$

则

$$\mathbb{P}\left(\bigcap_{i=1}^m \overline{A_i}\right) \geq \prod_{i=1}^m (1 - \alpha_i) > 0. \quad (9)$$

参数 α_i 是验证不等式的证书，不是算法的重采样概率，也不一定等于 A_i 的真实概率。证明会给出它们的含义：即使已经知道另一些坏事件没有发生， A_i 的条件概率仍然至多为 α_i 。

导出对称条件。 当 $d \geq 1$ 时，取所有 $\alpha_i = 1/(d+1)$ 。每个事件的邻居至多有 d 个，故

$$\alpha_i \prod_{A_j \in \Gamma(A_i)} (1 - \alpha_j) \geq \frac{1}{d+1} \left(\frac{d}{d+1}\right)^d \geq \frac{1}{e(d+1)}.$$

最后一个不等式等价于 $(1 + 1/d)^d \leq e$ 。因此，式 (6) 蕴含式 (8)。另取 $\alpha_i = 1/(2d)$ ，利用 Bernoulli 不等式可得

$$\frac{1}{2d} \left(1 - \frac{1}{2d}\right)^d \geq \frac{1}{2d} \left(1 - \frac{d}{2d}\right) = \frac{1}{4d}.$$

当 $d = 0$ 时，应改取 $\alpha_i = \mathbb{P}(A_i) < 1$ ，既不能除以 d ，也不能使用不合法的参数 $1/(d+1) = 1$ 。这里的初等估计在附录 A 中给出证明。

3 局部引理为什么成立

3.1 证明一个更强的条件概率结论

对 $S \subseteq [m]$ ，记 $E_S = \bigcap_{j \in S} \overline{A_j}$ 。为了估计避开全部坏事件的概率，链式法则提示我们写成

$$\mathbb{P}(E_{[m]}) = \prod_{i=1}^m (1 - \mathbb{P}(A_i \mid E_{\{1, \dots, i-1\}})).$$

但是，每个条件概率只有在条件事件具有正概率时才有定义。下面的归纳同时建立正概率和条件概率上界。

引理 3.1 (条件避免概率界)。 在式 (8) 的条件下, 对每个 $S \subseteq [m]$, 事件 E_S 均有正概率。而且, 对每个 $i \notin S$,

$$\mathbb{P}(A_i | E_S) \leq \alpha_i. \quad (10)$$

证明. 对 $s = |S|$ 归纳。当 $s = 0$ 时, $E_\emptyset$ 的概率为 1, 局部引理条件给出 $\mathbb{P}(A_i) \leq \alpha_i$ 。

设两个结论对更小的集合都成立。先证明大小为 $s \geq 1$ 的集合 S 对应的事件具有正概率。任取 $j \in S$, 由归纳假设,

$$\mathbb{P}(E_S) = \mathbb{P}(E_{S \setminus \{j\}})(1 - \mathbb{P}(A_j | E_{S \setminus \{j\}})) \geq \mathbb{P}(E_{S \setminus \{j\}})(1 - \alpha_j) > 0.$$

接着固定 $i \notin S$, 把 S 分为 i 的邻居与非邻居两部分:

$$S_1 = \{j \in S : A_j \in \Gamma(A_i)\}, \quad S_2 = S \setminus S_1.$$

如果 $S_1 = \emptyset$, 由联合独立性, $\mathbb{P}(A_i | E_S) = \mathbb{P}(A_i) \leq \alpha_i$ 。否则, 记 $S_1 = \{j_1, \dots, j_\ell\}$, 其中 $\ell \geq 1$ 。由条件概率定义,

$$\mathbb{P}(A_i | E_S) = \frac{\mathbb{P}(A_i \cap E_{S_1} | E_{S_2})}{\mathbb{P}(E_{S_1} | E_{S_2})} \leq \frac{\mathbb{P}(A_i)}{\mathbb{P}(E_{S_1} | E_{S_2})}. \quad (11)$$

分子至多为 $\mathbb{P}(A_i | E_{S_2}) = \mathbb{P}(A_i)$ 。这一步正是整个非邻居事件族与 A_i 独立的用途。

对分母使用链式法则:

$$\begin{aligned} \mathbb{P}(E_{S_1} | E_{S_2}) &= \prod_{r=1}^{\ell} \left(1 - \mathbb{P}(A_{j_r} | E_{S_2 \cup \{j_1, \dots, j_{r-1}\}})\right) \\ &\geq \prod_{r=1}^{\ell} (1 - \alpha_{j_r}). \end{aligned}$$

这里每个条件集合至多含 $s - 1$ 个元素, 因此都能使用归纳假设。代入式 (11), 再使用局部引理条件, 得到

$$\mathbb{P}(A_i | E_S) \leq \frac{\alpha_i \prod_{A_j \in \Gamma(A_i)} (1 - \alpha_j)}{\prod_{j \in S_1} (1 - \alpha_j)} = \alpha_i \prod_{\substack{A_j \in \Gamma(A_i) \\ j \notin S_1}} (1 - \alpha_j) \leq \alpha_i.$$

两个归纳结论均得到证明。 □

3.2 从条件概率界回到整体概率

定理 2.7 的证明. 引理 3.1 保证链式法则中的每个因子都有定义, 且至少为 $1 - \alpha_i$ 。所以

$$\mathbb{P}(E_{[m]}) = \prod_{i=1}^m \mathbb{P}(\overline{A_i} | E_{\{1, \dots, i-1\}}) \geq \prod_{i=1}^m (1 - \alpha_i) > 0. \quad \square$$

从局部到整体的机制

给定非邻居事件的状态, 不会改变 A_i 的概率。给定邻居都不发生, 可能使其概率上升; 但归纳能够控制分母中的邻居避免概率。假设中的因子 $(1 - \alpha_j)$ 正好补偿这一增长。这比两两独立更强, 也不是对各个邻域分别应用并合界。

证明只使用了坏事件概率和依赖图。它没有说明事件如何表示、怎样抽取一个随机对象, 或怎样找到当前被违反的约束。这些是算法化局部引理需要额外处理的问题。

4 通过局部重采样找到一个解

4.1 变量框架与算法

设 $X_1, \dots, X_n$ 为相互独立、分布给定的随机变量, $\mathcal{A} = \{A_1, \dots, A_m\}$ 为坏事件族, 其作用域 $\text{vbl}(A_i)$ 已给定。具体算法先在有限域上描述, 并删去变量域中零概率的取值。每次抽样使用变量自身的给定分布, 不要求均匀。假设能够独立抽样变量、检查一个给定坏事件是否发生, 并访问各作用域及其关联关系。我们先统计这些操作次数, 再转换为实现时间。

使用式 (5) 中的变量相交图。边更少的统计依赖图可能足以证明存在性, 但不能自动替代重采样分析中的这个图: 两个统计上独立的事件仍可能共享变量, 而一次修复会改变该变量。

Moser-Tardos 重采样算法

1. 按照各变量的给定分布, 独立抽取所有 X_j 。
2. 只要还有坏事件发生, 就选择一个这样的 A_i , 独立重新抽取所有 $j \in \text{vbl}(A_i)$ 对应的 X_j , 其他变量保持不变。
3. 没有坏事件发生时, 返回当前赋值。

为被违反事件固定一个确定的优先次序就足够了。更一般地, 选择可以依赖已经揭示的执行历史, 但不能查看未来的随机样本。下文的一次重采样指一个事件的整批重采样, 其中可能重新抽取多个变量。被选择的事件必须在这次重采样之前确实发生。

定理 4.1 (Moser-Tardos)。 假设式 (8) 对变量相交图成立。令 R_i 为事件 A_i 的总重采样次数, $R = \sum_i R_i$, 则

$$\mathbb{E}R_i \leq \frac{\alpha_i}{1 - \alpha_i}, \quad \mathbb{E}R \leq \sum_{i=1}^m \frac{\alpha_i}{1 - \alpha_i}. \quad (12)$$

算法几乎必然终止, 并返回避开所有坏事件的赋值。

第 5 节将利用见证树证明该定理 [2]。分析不假设当前坏事件数单调下降, 也不假设执行中的赋值始终保持初始乘积分布; 这两个断言一般都不成立。

4.2 在证明之前先看结论

当 $d \geq 1$ 且 $ep(d+1) \leq 1$ 时, 取 $\alpha_i = 1/(d+1)$ 可得

$$\mathbb{E}R_i \leq \frac{1}{d}, \quad \mathbb{E}R \leq \frac{m}{d}. \quad (13)$$

当 $4pd \leq 1$ 时, 改取 $\alpha_i = 1/(2d)$, 得到 $\mathbb{E}R \leq m/(2d-1)$ 。因此, 可满足性和超图染色的应用都成为构造性的: 找到违反的子句就重采样其变量; 找到单色超边就重新为其所有顶点染色。

当 $d = 0$ 时, 各事件的变量作用域互不相交。反复重采样 A_i 直到它不发生, 所需重采样批数的期望为 $p_i/(1-p_i)$, 其中 $p_i = \mathbb{P}(A_i) < 1$; 初始样本已满足约束时, 批数为零。因此 $\mathbb{E}R = \sum_i p_i/(1-p_i)$, 也就是在式 (12) 中取 $\alpha_i = p_i$ 。这个情形不需要使用 m/d 。

局部修复与拒绝采样有什么不同。 在互不相交的子句例子中, 整赋值拒绝采样要求全部 m 个子句一次同时成功, 其概率为式 (2)。局部重采样则保留所有已经成功的子句中的变量, 只修复失败的部分。其修复次数期望为 $m2^{-k}/(1-2^{-k})$ 。一般定理说明, 即使有限的相交使修复能够在附近产生新失败, 这种局部策略仍然有效。

4.3 从重采样次数到计算开销

记 $s_i = |\text{vbl}(A_i)|$ 、 $d_i = |\Gamma(A_i)|$ 。初始化时检查所有 m 个事件，并维护当前被违反的事件集合。重采样 A_i 后，只有 $\Gamma^+(A_i)$ 中的事件可能改变状态，因此只需重新检查这些事件并更新集合。维护的不变量是：记录的事件状态与实际当前赋值一致。

这样实现时，变量抽样次数与事件检查次数分别满足

$$N_{\text{draw}} = n + \sum_i s_i R_i, \quad N_{\text{test}} \leq m + \sum_i (d_i + 1) R_i. \quad (14)$$

对定理 4.1 的界取期望，可得

$$\begin{aligned} \mathbb{E} N_{\text{draw}} &\leq n + \sum_i s_i \frac{\alpha_i}{1 - \alpha_i}, \\ \mathbb{E} N_{\text{test}} &\leq m + \sum_i (d_i + 1) \frac{\alpha_i}{1 - \alpha_i}. \end{aligned} \quad (15)$$

这些是访问操作次数，不包括构造相交图的开销。转换为实际时间时，需要计入每次抽样和检查的成本，以及选择、更新被违反事件的管理成本。

例如，在 $d \geq 1$ 的对称条件下，若 $s_i \leq k$ ，事件检查次数的期望为 $O(m)$ ，变量抽样次数的期望至多为 $n + km/d$ 。直接检查一个 k -子句需要 $O(k)$ 次比特访问。显式保存所有邻域的表本身可能有 $\Theta(md)$ 个条目；后续检查次数为 $O(m)$ ，并不意味着这些预处理和存储成本可以忽略。

期望界不是对每次执行的确定性限制。如果 $B > 0$ 是 $\mathbb{E}R$ 的上界，Markov 不等式给出 $\mathbb{P}(R > 2B) \leq 1/2$ 。独立重新启动 r 次，每次至多执行 $\lceil 2B \rceil$ 批重采样，那么所有尝试都未能结束的概率至多为 2^{-r} 。这是重启算法的保证，不是原始单次执行的指数尾界。

5 重采样为何终止：表与见证树

5.1 将全部随机选择组织成一张表

可以预先抽取一张无限的独立随机表，而不是在执行时才产生随机性。对每个变量 X_j ，令

$$X_j^{(0)}, X_j^{(1)}, X_j^{(2)}, \dots$$

为来自其给定分布的独立样本。不同变量和不同下标对应的所有表项相互独立。初始化使用每个变量的第 0 项。每次重采样一个事件，就将其涉及变量的计数器分别增加一。算法其他部分不变，也可以在需要时才揭示对应表项来模拟这个过程。

令 $\Lambda = (\Lambda_1, \Lambda_2, \dots)$ 为执行日志，其中 $\Lambda_t \in \mathcal{A}$ 记录第 t 步重采样的事件。在第 t 步之前，变量 j 的值为

$$X_j^{(h_j(t))}, \quad h_j(t) = |\{s < t : j \in \text{vbl}(\Lambda_s)\}|. \quad (16)$$

事件 Λ_t 在这些取值上发生，之后相关计数器才增加。区分检查时刻与重采样时刻，才能正确对应表项下标。

一条固定的长日志可能描述一个很罕见的执行，但对所有 m^t 种日志直接求和，无法利用局部性。见证树只保留足以证明某一次重采样发生的那部分历史。

5.2 从过去构造一个见证

定义 5.1 (合法见证树 (proper witness tree))。合法见证树是一棵有限有根树，每个结点 u 带有事件标签 $A[u] \in \mathcal{A}$ ，每个孩子的标签都属于父结点标签的 Γ^+ ，且同胞结点的标签互不相同。以 A 为根标签的所有此类树组成集合 $\mathcal{T}_A$ 。根的深度为 0。

这些是带标签的有根树，不一定是算法实际的调用树。无须额外记录孩子顺序：由于同胞标签不同，可以按一个固定的规范次序排列。

反向构造 $T(\Lambda, t)$

先建立一个标签为 Λ_t 的根。依次扫描 $s = t-1, t-2, \dots, 1$ 。若已建树中有结点 u 满足 $\Lambda_s \in \Gamma^+(A[u])$ ，就在所有这样的结点中选择一个最深的结点，为它添加标签为 Λ_s 的孩子。并列时使用固定规则。若不存在这样的结点，则略过 Λ_s 。最后得到的树记为 $T(\Lambda, t)$ 。

选择最深的相容结点非常重要。假如同一个结点的两个孩子标签相同，后加入的那个本来可以接到已经存在的同标签孩子下面，与“最深”矛盾。因此，构造出的树是合法见证树。

引理 5.2 (深度与重复标签)。反向构造得到的树具有以下性质。

1. 如果被纳入的两个日志位置 $s < r$ 的标签共享变量，则位置 s 的结点严格深于位置 r 的结点。特别地，同一深度的标签使用互不相交的变量集合。
2. 若根对应日志中事件 A 的第 r 次出现，则树中恰有 r 个标签为 A 的结点。因此，不同重采样步骤产生不同的见证树。

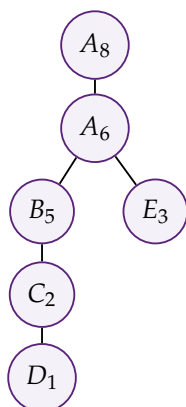
证明。 处理位置 s 时，位置 r 的结点已经存在。由于标签相交，所选连接点的深度至少为位置 r 的结点深度，新结点再深一层。对第二个结论，根标签的每次更早出现都会被纳入，因为它始终与根相容。这些恰好是截至根时刻的全部 A 标签。若两棵树根标签不同，它们显然不同；若根标签相同，则在不同出现次数处，该标签的结点数不同。 $\square$

5.3 一个具体见证及其使用的表项

使用例 2.2 中的五个作用域，考虑日志前缀

$$\Lambda = D, C, E, D, B, A, C, A.$$

第 8 步的根为 A 。反向扫描纳入位置 6, 5, 3, 2, 1，略过位置 7, 4。处理位置 2 时若有并列，选择标签为 B 的结点作为父结点。下图中的下标记日志位置，不表示不同的事件类型。



结点	检查该事件所用的表项
D_1	$X_4^{(0)}$
C_2	$X_3^{(0)}, X_4^{(1)}$
E_3	$X_1^{(0)}, X_4^{(2)}$
B_5	$X_2^{(0)}, X_3^{(1)}$
A_6	$X_1^{(1)}, X_2^{(1)}$
A_8	$X_1^{(2)}, X_2^{(2)}$

不同结点分配到的表项互不相交。注意, E_3 与 C_2 共享变量 X_4 , 却位于不同分枝上。共享变量不意味着两个见证结点之间必定具有祖先关系; 正确的顺序性质是它们的深度不同。这里构造的是给定日志对应的见证, 不是断言具有这些作用域的任意谓词都能够产生该日志。

5.4 见证树的概率界

引理 5.3 (见证树引理)。 对每棵固定的合法见证树 τ ,

$$\mathbb{P}(\exists t : T(\Lambda, t) = \tau) \leq \prod_{u \in \tau} \mathbb{P}(A[u]). \quad (17)$$

证明。 如果同一深度存在两个变量作用域相交的结点, 引理 5.2 说明该树不可能出现, 结论显然。否则, 对每个 $j \in \text{vbl}(A[u])$ 定义

$$r_\tau(u, j) = |\{v \in \tau : \text{depth}(v) > \text{depth}(u), j \in \text{vbl}(A[v])\}|. \quad (18)$$

用随机表中的元组 $(X_j^{(r_\tau(u, j))})_{j \in \text{vbl}(A[u])}$ 来检查 $A[u]$ 。这个检查由一棵固定的树确定, 不是算法在随机选取的执行时刻自适应进行的检查。

固定一个变量 j , 所有使用它的结点具有不同深度。从最深到最浅排列, 它们分别使用下标 $0, 1, \dots$ 的表项。因此, 不同结点的检查不共享表项。全部表项的独立性说明, 各结点检查相互独立, 且每个检查具有该标签事件的原始概率。于是

$$\mathbb{P}(\tau \text{ 的所有检查都成功}) = \prod_{u \in \tau} \mathbb{P}(A[u]). \quad (19)$$

还需证明: 在同一张随机表上, τ 的实际出现必定使这些检查全部成功。设 $\tau = T(\Lambda, t)$, 结点 u 对应日志位置 s 。固定其标签使用的变量 j 。所有涉及 j 的更早位置 $r < s$ 都会被纳入树中, 因为扫描到 r 时, 结点 u 已经存在, 提供了相容的连接点。这些结点都严格深于 u 。反之, 涉及 j 的被纳入的更晚位置, 由引理 5.2 必定浅于 u 。因此

$$r_\tau(u, j) = |\{r < s : j \in \text{vbl}(\Lambda_r)\}| = h_j(s).$$

固定树检查使用的取值, 恰好就是 Λ_s 在被重采样前发生时的取值。所以每个结点检查都成功。这个事件包含关系与式 (19) 结合, 就证明了对所有可能出现时刻 t 取并之后的概率界。 $\square$

独立性在哪里重新出现

连续发生的重采样事件不必独立; 在给定执行历史后, 其条件概率也不必等于原始概率。真正独立的是: 对一棵固定见证树, 用互不相交的随机表项进行的检查。局部依赖限制了可能的见证形状, 新鲜随机性则使每个固定见证的出现付出相应的概率代价。

5.5 用分枝过程对所有见证求和

由产生的见证树互不相同,

$$R_i = \sum_{\tau \in \mathcal{T}_{A_i}} \mathbf{1}\{\exists t : T(\Lambda, t) = \tau\}, \quad \mathbb{E}R_i \leq \sum_{\tau \in \mathcal{T}_{A_i}} \prod_{u \in \tau} \mathbb{P}(A[u]). \quad (20)$$

这些等式和不等式在尚未证明终止时也有意义: 各项非负, 先有限截断再取单调极限, 就能合法交换求和与期望。现在需要控制的是一个可能包含无穷多项的树权重和。

先设所有相关的 α_i 都为正, 定义

$$w(A_i) = \alpha_i \prod_{A_j \in \Gamma(A_i)} (1 - \alpha_j). \quad (21)$$

局部引理假设即为 $\mathbb{P}(A_i) \leq w(A_i)$ 。

根标签为 A_i 的辅助分枝过程

确定地建立一个标签为 A_i 的根。对每个已建结点 u , 对每个 $B \in \Gamma^+(A[u])$ 独立进行试验: 以概率 α_B 添加一个标签为 B 的孩子, 否则不添加该标签的孩子。对新结点重复这一操作。所得 T_{A_i} 可能有限, 也可能无限。

这是一个多类型 Galton–Watson 分枝过程, 类型就是事件标签。它生成合法见证树, 但能生成的树不必全都能由实际执行产生。加入这些额外的树, 只会使所求上界更大。

引理 5.4 (分枝概率)。 对根标签为 A_i 的有限合法见证树 τ ,

$$\mathbb{P}(T_{A_i} = \tau) = \frac{1 - \alpha_i}{\alpha_i} \prod_{u \in \tau} w(A[u]). \quad (22)$$

证明. 令 $C(u)$ 为结点 u 的孩子标签集合。每个非根结点贡献其产生概率 $\alpha_{A[u]}$, 每个缺失的潜在孩子贡献不产生的概率。因此

$$\mathbb{P}(T_{A_i} = \tau) = \prod_{u \neq \text{根}} \alpha_{A[u]} \prod_{u \in \tau} \prod_{B \in \Gamma^+(A[u]) \setminus C(u)} (1 - \alpha_B). \quad (23)$$

也可以先在每个结点放入所有潜在孩子的不产生因子, 再对实际产生的孩子, 将对应因子替换为产生因子。式 (23) 因而等于

$$\left(\prod_{u \in \tau} \prod_{B \in \Gamma^+(A[u])} (1 - \alpha_B) \right) \left(\prod_{u \neq \text{根}} \frac{\alpha_{A[u]}}{1 - \alpha_{A[u]}} \right).$$

补入缺失的根比值, 并乘以 $(1 - \alpha_i)/\alpha_i$ 补偿。此后每个结点对应的自身标签因子约去, 留下 $\alpha_{A[u]} \prod_{B \in \Gamma(A[u])} (1 - \alpha_B) = w(A[u])$ 。□

定理 4.1 的证明. 结合式 (20)、局部引理条件及引理 5.4, 得到

$$\begin{aligned} \mathbb{E}R_i &\leq \sum_{\tau \in \mathcal{T}_{A_i}} \prod_{u \in \tau} \mathbb{P}(A[u]) \\ &\leq \sum_{\tau \in \mathcal{T}_{A_i}} \prod_{u \in \tau} w(A[u]) \\ &= \frac{\alpha_i}{1 - \alpha_i} \sum_{\tau \in \mathcal{T}_{A_i}} \mathbb{P}(T_{A_i} = \tau) \leq \frac{\alpha_i}{1 - \alpha_i}. \end{aligned}$$

最后的概率和至多为 1, 因为分枝过程可能生成无限树。这里不需要证明它几乎必然灭绝。

如果 $\alpha_i = 0$, 假设迫使 $\mathbb{P}(A_i) = 0$ 。在各变量域中的取值均具有正边缘概率的有限域模型下, 这种事件不可能发生, 可以删除, 也从不会被重采样。从邻域中删去它, 只是删去了一个值为 1 的因子。对剩余事件应用前面的证明即可。因此, 定理允许参数位于 $[0, 1)$, 而不会出现除以零的问题。

对 i 求和得到有限的 $\mathbb{E}R$ 上界。非负扩展随机变量如果期望有限, 就几乎必然取有限值, 因此算法几乎必然终止。停止条件保证, 返回时所有约束都得到满足。□

这个证明完成了什么。一个可能很长的自适应执行，被替换为可数个有限证书。每个证书的概率至多为其局部事件概率的乘积；另一个随机树过程负责核算全部证书的权重。辅助随机树用于求和，不是算法的实际轨迹，也不是满足赋值的分布。

6 递归修复与熵压缩

6.1 Moser 的递归 Fix-It 算法

回到 k -CNF 公式，固定子句次序以及每个含自身邻域的次序。可以用递归方式调度重采样：修复一个子句后，检查它自身以及可能被它直接影响的所有邻居。

Moser 递归算法

主过程。抽取 n 个独立公平比特。只要还有违反的子句，就选取次序中的第一个这样的子句 C ，调用 $\text{Fix}(C)$ 。全部子句满足时返回赋值。

过程 $\text{Fix}(C)$ 。

1. 用新鲜独立公平比特重新抽取 C 的 k 个变量。
2. 只要 $\Gamma^+(C)$ 中还有违反的子句 D ，就选择次序中的第一个这样的 D 并调用 $\text{Fix}(D)$ 。
3. 当 $\Gamma^+(C)$ 中全部子句满足时返回。

含自身的邻域必须包含 C ：一次重采样之后，同一个子句仍可能违反。每次调用开始时，其子句必定被违反；调用首先抽取一批 k 个新比特，再进行零次或多次递归调用。按时间排列的这些批次是一个合法的 Moser-Tardos 执行，因此，只要满足该定理的条件，定理 4.1 已经适用。下面在一个稍强但简洁的数值条件下给出独立证明，目的是展示另一种机制，而不是改进 Moser-Tardos 的阈值。

引理 6.1 (返回时刻的保持性质)。 如果一次 $\text{Fix}(C)$ 调用返回，则在它进入时已经满足的每个子句，在返回时仍然满足；而且，返回时 $\Gamma^+(C)$ 中的全部子句都满足。因此，主过程启动的顶层调用至多有 m 次，包括可能的最后一次尚未完成的调用。

证明。 第一个结论只讨论一次有限、已经完成的递归。可以对其中的调用总数归纳，无须预先假设每次调用都终止。首次重采样只改变 C 的变量，因此不会影响 $\Gamma^+(C)$ 之外的子句。由归纳假设，每个已经返回的递归孩子都保持其进入时已满足的所有子句。因此，进入父调用时已经满足、且位于 $\Gamma^+(C)$ 之外的子句，在父调用返回时仍然满足。父调用的停止条件又使 $\Gamma^+(C)$ 内的全部子句都满足，从而证明保持性质。

每次顶层调用完成时，之前已经满足的子句全部恢复满足，且原本违反的根子句变得满足。因此，在各次顶层调用的边界处，已满足子句集合严格增加。后续顶层调用的根不可能是之前修复过的根，所以最多启动 m 次顶层调用。□

不变量针对返回时刻

早先顶层调用修复过的子句，在后续递归修复的内部，可能暂时再次被违反。保持性质只保证后续调用返回后它仍然满足，不保证每次中间重采样后都满足。论证限制的是互不重复的顶层根，并不是断言每个子句只被重采样一次。

6.2 为什么长执行能够描述自身的随机性

在重采样一个违反的 k -子句之前，它的 k 个变量取值已经由子句标签唯一确定：所有文字都为假。因此，重采样是用 k 个新随机比特覆盖一个已知的局部赋值。如果记录了重采样子句的标签，那么最终赋值就足以让我们撤销全部覆盖，逐步恢复随机比特。

直接记录每次子句标签，需要每次 $\lceil \log_2 m \rceil$ 比特。递归改变了这个成本：非根调用的子句属于其父调用的含自身邻域，因此只需记录至多 $d+1$ 种选择中的一个名次。全局标签只在至多 m 个顶层根处需要。如果每次调用消耗的随机比特，多于记录该调用所需的比特，长执行就会把许多均匀随机比特变为一个更短、却可完全恢复的描述。

引理 6.2 (有限不可压缩性)。 设 $\mathcal{B} \subseteq \{0,1\}^N$ 。如果一个编码在 $\mathcal{B}$ 上是单射，且每个编码串长度至多为 L ，则

$$\frac{|\mathcal{B}|}{2^N} < 2^{L+1-N}. \quad (24)$$

如果所有编码串长度恰好为 L ，则有更强的 $|\mathcal{B}|/2^N \leq 2^{L-N}$ 。特别地，均匀 N 比特串能通过单射编码得到至多 $N - \ell$ 比特描述的概率，小于 $2^{1-\ell}$ 。

证明。 长度至多为 L 的二进制串共有 $\sum_{r=0}^L 2^r = 2^{L+1} - 1$ 个；长度恰好为 L 的则有 2^L 个。由单射性， $|\mathcal{B}|$ 不超过相应数目，再除以等可能输入的总数 2^N 即可。 $\square$

引理不禁止某个特定串被压缩，而是说：不可能让大量均匀随机串都得到短很多、且彼此不同的描述。这里除了这个初等计数事实，不需要使用 Kolmogorov 复杂性的其他工具。

6.3 在固定的重采样次数后冻结

在选择随机性之前，固定公式及整数参数 n, m, k, t ，其中 $m \geq 1$ 、 $t \geq 1$ 。向算法提供长度为

$$N = n + tk \quad (25)$$

的均匀随机带。前 n 比特初始化赋值，此后每一块 k 比特供一次调用使用，子句内部的变量顺序预先固定。如果执行到达第 t 次调用，就在这次调用的首次重采样刚完成时立刻停止，此时随机带恰好全部用完。如果算法更早终止，这条随机带就不属于我们将要编码的长执行集合 $\mathcal{B}_t$ 。

每次调用打开递归树的一个结点，孩子按调用时刻排列。已完成的顶层调用构成森林，而最后一棵树可能还带有未完成的调用栈。记录冻结前真正发生的进入和返回，再为仍然打开的栈补上闭括号，就得到一片恰有 t 个结点的完整有序森林。补上的闭括号只是在完成记录，不表示这些调用实际上已经返回。

记

$$a = \lceil \log_2 m \rceil, \quad b = \lceil \log_2(d+1) \rceil. \quad (26)$$

下面的定长编码明确划分字段，从而避免部分递归记录在哪里结束的歧义。

编码前 t 次调用及当前赋值

记录四个字段，其长度均由 n, m, d, t 预先确定：

1. **森林形状**： $2t$ 比特。按深度优先顺序，进入结点记为 1，离开结点记为 0。
2. **根标签**： m 个长度为 a 的槽位。依次写入根标签，未使用槽位补零。
3. **非根标签**： t 个长度为 b 的槽位。按先序写入每个非根在其父标签含自身邻域中的名次，未使用槽位补零。
4. **当前赋值**：第 t 次重采样之后的 n 比特赋值。

标签和名次均从零开始编号，以固定宽度的二进制表示。宽度为零时，唯一可能的选择无需任何比特。

根数和非根结点数都由森林形状确定，因此解码器知道哪些槽位是补零。由引理 6.1，森林至多有 m 个根。总编码长度为

$$L = n + ma + t(b + 2). \quad (27)$$

公式和参数不是传输记录的一部分，因为在这个计数论证中，它们是所有随机带共有的固定辅助信息。长度核算已经包括森林的完整二进制形状，而不只是子句标签。

6.4 反向撤销覆盖，恢复随机带

森林及其标签确定了按时间排序的子句序列 $C_{i_1}, \dots, C_{i_t}$ 。这是因为每次调用一进入就重采样，所以调用的先序就是重采样顺序。最后的赋值提供反向处理该序列的起点。

恢复随机带

从记录的赋值开始，对 $s = t, t-1, \dots, 1$ 依次执行：

1. 按预定次序读取 C_{i_s} 作用域上的当前比特，保存为第 s 次调用消耗的 k 个随机比特。
2. 将这些变量改为唯一违反 C_{i_s} 的赋值，其他变量保持不变。

撤销全部 t 次重采样后，当前赋值就是初始的 n 比特。输出它，再按 $1, \dots, t$ 的次序输出恢复的各比特块。

引理 6.3 (可逆性)。 对 $\mathcal{B}_t$ 中的每条随机带，上述解码过程能够恢复其全部 $n + tk$ 个比特。因此，编码在 $\mathcal{B}_t$ 上是单射。

证明。 对 s 反向归纳。撤销第 s 次调用之前，更晚的重采样已经全部撤销，所以当前维护的赋值恰好是该次重采样刚完成时的状态。其作用域上的取值，正是这次抽到的新随机比特块。调用之前该子句被违反，因而其作用域上的旧值被唯一确定。将作用域恢复为该违反模式，就得到前一状态。如此逐步恢复初始赋值，并找回每一块随机比特。 $\square$

例如，若 $C = x_1 \vee \neg x_2 \vee x_3$ ，其作用域上的前驱取值必定为 $(0, 1, 0)$ 。撤销后续修改后，当前作用域上的三个比特揭示了当时用来覆盖该模式的新随机比特。不同子句共享变量不会妨碍恢复，因为更晚发生的覆盖先被撤销。

6.5 由计数得到尾界

令 R 为递归算法的调用总数，也就是其重采样批数。定义每次调用的比特盈余

$$\gamma = k - b - 2. \quad (28)$$

减去的两项分别是局部标签成本和每个结点的森林形状成本。结合式 (25)、式 (27) 及引理 6.3，由定长不可压缩性得到

$$\mathbb{P}(R \geq t) = \frac{|\mathcal{B}_t|}{2^{n+tk}} \leq \min\{1, 2^{ma-\gamma t}\}. \quad (29)$$

等式使用的是未加条件的均匀随机带。我们没有假设在给定长执行之后，随机带仍然均匀。只对长执行对应的子集进行编码，而计数引理本来就允许定义域是这样的子集。

定理 6.4 (递归修复的熵压缩界)。 设 $k \geq 3$ ，每个子句至多与 d 个其他子句相交，且 $d < 2^{k-3}$ 。对任意 $0 < \delta < 1$ ，递归算法以至少 $1 - \delta$ 的概率，在重采样调用次数达到

$$t_\delta = \lceil m \lceil \log_2 m \rceil + \log_2(1/\delta) \rceil \quad (30)$$

之前返回满足赋值。特别地，对 $n \geq 2$ ，以至少 $1 - 1/n$ 的概率，调用次数为 $O(m \log(2m) + \log n)$ 。

证明。 由于 d 为整数且 $k \geq 3$ ， $d < 2^{k-3}$ 蕴含 $d + 1 \leq 2^{k-3}$ ，因此 $b \leq k - 3$ 、 $\gamma \geq 1$ 。式 (29) 给出 $\mathbb{P}(R \geq t_\delta) \leq \delta$ 。其尾概率趋于零，因而独立于 Moser–Tardos 定理地证明了几乎必然终止。终止时，主循环的条件保证所有子句满足。取 $\delta = 1/n$ 即得最后的结论；使用 $\log(2m)$ 使 $m = 1$ 时表述仍有意义。□

更一般地，只要 $\gamma > 0$ ，阈值 $\lceil (ma + \log_2(1/\delta))/\gamma \rceil$ 就足够。定理中的条件保证每次调用至少节省一个比特。当 $d = 0$ 时，对任意 $k \geq 1$ 都能直接处理互不相交的子句，不必要求这套特定编码产生比特盈余。

该界统计的是全部调用，而不只是顶层调用，也不是单个变量的赋值次数。每次调用抽取 k 比特。实现时可以沿用第 4.3 节的局部更新来维护被违反事件的状态，再加上递归栈和寻找违反邻居的管理成本。若作用域和邻域有限且显式给出，这些开销都关于输入长度和调用次数为多项式。有固定执行预算时，递归栈长度也不超过该预算。

两种树，两种核算方式

Moser–Tardos 见证树从日志中反向提取，用来证明一次重采样确实发生；其概率通过独立随机表项控制。递归调用树记录算法实际发生的嵌套调用，和最终赋值共同恢复随机带。前者支持见证概率求和，后者支持对长执行的单射编码。

7 三个阶段分别建立了什么

局部引理把局部失败与整体可行性联系起来。Moser–Tardos 定理进一步加入可访问的变量表示和局部修复规则。熵压缩则从另一个角度解释修复为何高效：过多的失败，将会泄露过多关于随机选择的信息。

方法	所需结构	本讲证明的结论
经典局部引理	依赖图与坏事件概率	全部避免的概率为正；没有搜索时间保证。
Moser–Tardos	独立变量作用域、新鲜抽样及事件检查	重采样次数期望至多为 $\sum_i \alpha_i / (1 - \alpha_i)$ 。
递归熵压缩证明	k -子句具有唯一违反赋值；递归邻居名次	在 $d < 2^{k-3}$ 时给出明确的高概率调用次数界。

进一步的方向

条件 $ep(d+1) \leq 1$ 是便于使用的充分条件，不是每个依赖图的精确刻画。Shearer 的工作给出了由依赖图和事件概率决定的紧刻画 [4]。如果掌握超出图结构的事件信息，还可能得到不同或更强的论证。本讲各定理都不依赖这些进一步结果。

在非乘积概率空间中，可能没有一个可以直接重新独立抽取的变量块。重采样预言机框架用其他局部修复操作来替代 [5]，但必须验证相应的假设；抽象依赖图本身并不提供高效的修复操作。

最后，找到一个满足赋值与从满足赋值上的指定分布中抽样，是不同的任务。对乘积测度 μ 以及 $\mathcal{S} = \bigcap_i \overline{A_i}$ ，自然的条件抽样目标是

$$\mu(\sigma \mid \mathcal{S}) = \frac{\mu(\sigma) \mathbf{1}\{\sigma \in \mathcal{S}\}}{\mu(\mathcal{S})}.$$

前面的终止证明只说明输出位于 $\mathcal{S}$ ，并没有证明它服从这个分布。Moser–Tardos 输出的分布性质需要额外分析 [6]；不能将其期望时间定理直接理解成精确抽样定理。

8 习题

依赖建模与局部引理的应用

- 并合界的阈值。**在 k 个变量上，构造含 2^k 个子句的不可满足 k -CNF。为什么它不与推论 2.4 矛盾？在子句作用域互不相交时，比较整赋值拒绝采样与局部修复。
- 联合独立与两两独立。**验证三个公平比特事件例子中的全部两两独立关系。找出一个由其中两个事件的指示变量共同确定、却不与第三个事件独立的事件。
- 变量出现次数。**如果每个变量至多出现在 L 个子句中，推导一个关于 k, L 的可满足性充分条件。对超图染色，比较精确条件 $eq^{1-k}(k(\Delta-1)+1) \leq 1$ 与式 (7)。
- 不相同的预算。**设依赖图为星形，中心事件概率为 p_0 ， r 个叶子事件概率为 $p_1, \dots, p_r$ 。给定中心参数 $a \in (0, 1)$ ，在每个叶子取 $\alpha_j = p_j / (1 - a)$ 。写出所得充分条件，包括 $\alpha_j < 1$ 。为什么只保留最大概率的对称界可能丢失有用信息？

重采样与见证树

- 条件事件的正概率。**在引理 3.1 中，标出归纳假设的每个使用位置及其条件集合大小。为什么必须在写式 (11) 之前先证明正概率？

6. **构造下一棵见证树。**在第 5.3 节的日志后增加第九个标签 D 。固定最深父结点并列时的规则，构造 $T(\Lambda, 9)$ 。哪些位置被略过？验证每个被纳入结点使用的表项下标。
7. **合法树与实际生成的树。**给出一棵合法见证树，使某一深度的两个标签共享变量，并解释它为什么不能由反向扫描产生。分枝过程求和时，为什么仍然可以包括这棵树？
8. **成本与置信度。**允许每个事件具有不同的抽样和检查成本，推导式 (15) 的相应版本。再由已知的期望批数界导出高置信度的重启保证，说明它与一次不间断执行的尾界有何区别。

递归修复与可逆信息

9. **返回时刻的保持性质。**对已完成的递归树归纳，证明引理 6.1。为什么这个归纳不需要假设算法几乎必然终止？为什么暂时出现的违反不影响顶层根数至多为 m 的结论？
10. **检查编码的每个字段。**为第 6.3 节的四个字段写出解码过程，解释如何识别根、补零以及名次宽度。为什么可以在记录的形状中关闭未完成调用，而不真正继续执行它们？
11. **多个禁止局部赋值。**假设每个坏约束涉及 k 个公平比特，且至多有 $s \geq 1$ 个禁止赋值。保持相同的递归修复方式，并为每次调用添加一个名次，指明重采样前是哪一个禁止赋值。证明：对应熵论证的一个充分比特盈余条件为 $k > b + 2 + \lceil \log_2 s \rceil$ 。说明解码器和尾界如何改变。
12. **比较两种构造性分析。**取 $k = 10$ 、 $d = 100$ 、 $p = 2^{-k}$ ，判断 $ep(d+1) \leq 1$ 、 $4pd \leq 1$ 和 $d < 2^{k-3}$ 中哪些成立。比较两个证明对重采样次数、置信度和输出分布分别提供了什么信息。

A 证明中用到的初等工具

A.1 乘积、对数与重复试验

对 $u > -1$ ， $\ln(1+u) \leq u$ ，因为 $u - \ln(1+u)$ 在零点取得最小值。因此，对 $d \geq 1$ ， $(1 + 1/d)^d \leq e$ 。对 $0 \leq x \leq 1$ 和整数 $d \geq 1$ ，Bernoulli 不等式 $(1-x)^d \geq 1-dx$ 可由归纳得到：将 d 时的下界乘以 $1-x$ ，得到 $1 - (d+1)x + dx^2 \geq 1 - (d+1)x$ 。

如果每次试验独立地以概率 $p < 1$ 失败，一直重复到首次成功，则失败次数的期望为

$$\sum_{r \geq 1} p^r = \frac{p}{1-p}.$$

初始试验的计数方式很重要：当初始赋值也可能成功时，这里计算的是重采样次数，而非全部独立求值次数；后者的期望是 $1/(1-p)$ 。

A.2 非负计数与几乎必然终止

对可能取无穷的非负整数值随机变量 R ，

$$R = \sum_{t \geq 1} \mathbf{1}\{R \geq t\}, \quad \mathbb{E}R = \sum_{t \geq 1} \mathbb{P}(R \geq t).$$

先对有限项求和，再增加截断长度，就得到这两个恒等式。同样的论证允许交换期望与可数个非负见证指示变量的求和。若 $\mathbb{E}R < \infty$ ，则 $\mathbb{P}(R = \infty) = 0$ ，因为对每个整数 T 都有 $\mathbb{E}R \geq T\mathbb{P}(R = \infty)$ 。

对 $a > 0$ ，由 $R \geq a\mathbf{1}\{R \geq a\}$ 得到 Markov 不等式 $\mathbb{P}(R \geq a) \leq \mathbb{E}R/a$ ，这正是第 4.3 节重启分析的依据。对于式 (29) 在 $\gamma \geq 1$ 时给出的更强几何尾界，求和还得到 $\mathbb{E}R \leq ma + 2$ 。这是显式编码的另一个推论，与更强、更一般的 Moser–Tardos 期望界是不同的结论。

A.3 为什么算法证明能推广到非有限域

随机表证明只使用相互独立的新鲜样本、可测的事件检查和有限作用域。因此，只要这些操作有定义，同一证明也适用于其他变量分布。对一个零概率坏事件，每个固定的表项下标元组使该事件发生的概率都是零。有限元组的选择只有可数多个，事件也只有有限多个；对这些零概率事件取可数并可数，几乎必然没有任何表项组合实现零概率坏事件。这样就能替代有限支撑情形中的删除论证，而不改变证明主体。

文献说明

局部引理起源于 Erdős 与 Lovász 的工作 [1]。它的条件概率证明以及局部约束应用，构成本讲第一阶段。Moser 的构造性工作 [3] 与一般的 Moser–Tardos 定理 [2] 提供算法化阶段。第 6 节给出递归修复的初等熵压缩分析，使用明确的定长森林编码，得到定理 6.4 中的高概率界。第 7 节的研究方向提供进一步阅读线索；其中更强的结果不是理解本讲的前提。

参考文献

- [1] Paul Erdős and László Lovász. Problems and Results on 3-Chromatic Hypergraphs and Some Related Questions. In *Infinite and Finite Sets*, Vol. II, Colloquia Mathematica Societatis János Bolyai 10, pages 609–627. North-Holland, 1975. [原始论文](#)。
- [2] Robin A. Moser and Gábor Tardos. A Constructive Proof of the General Lovász Local Lemma. *Journal of the ACM*, 57(2), Article 11, 1–15, 2010. [作者稿](#); [doi:10.1145/1667053.1667060](#)。
- [3] Robin A. Moser. A Constructive Proof of the Lovász Local Lemma. In *Proceedings of STOC*, pages 343–350, 2009. [较早的作者稿](#)。
- [4] James B. Shearer. On a Problem of Spencer. *Combinatorica*, 5:241–245, 1985. [doi:10.1007/BF02579368](#)。
- [5] Nicholas J. A. Harvey and Jan Vondrák. An Algorithmic Proof of the Lovász Local Lemma via Resampling Oracles. *SIAM Journal on Computing*, 49(2):394–428, 2020. [doi:10.1137/18M1167176](#)。
- [6] Bernhard Haeupler, Barna Saha, and Aravind Srinivasan. New Constructive Aspects of the Lovász Local Lemma. [作者稿](#), [arXiv:1001.1231](#), 2010.
- [7] Stephen A. Cook. The Complexity of Theorem-Proving Procedures. In *Proceedings of STOC*, pages 151–158, 1971. [doi:10.1145/800157.805047](#)。