中国科学: 信息科学 2020 年 第 50 卷 第 11 期: 1680–1696
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
评述

洛瓦兹局部引理的新变种及其应用

何昆[1,2*], 孙晓明[3,4]

1. 深圳大学计算机与软件学院, 深圳 518061
2. 深圳计算科学研究院, 深圳 518109
3. 中国科学院计算技术研究所, 北京 100190
4. 中国科学院大学, 北京 100049
* 通信作者. E-mail: hekun.threebody@foxmail.com

收稿日期: 2019–12–26; 修回日期: 2020–02–21; 接受日期: 2020–02–26; 网络出版日期: 2020–10–19

国家自然学基金 (批准号: 61433014, 61832003, 61761136014, 61872334, 61801459)、中国科学院战略性先导科技专项 (B 类) (批准号: XDB28000000) 和中国科学院王宽诚率先人才计划卢嘉锡国际团队项目资助

摘要 洛瓦兹局部引理是组合数学和概率论中的重要工具, 其最主要的用途之一是证明当约束之间"弱相关" 时, 满足复杂约束的组合对象存在. 自从 1975 年 Erdős 和 Lovász 提出洛瓦兹局部引理以来, 局部引理在组合数学、理论计算机和物理学等领域已经有了很多应用. 近年来, 为了扩展局部引理的应用范围, 人们提出了很多新版的局部引理, 尤其是在构造版本局部引理上取得了重大的突破. 本文将综述局部引理近年来最新的研究进展, 包括几种最主要的局部引理变种以及它们在计算机科学和物理学中的应用. 特别的, 我们将给出抽象版本、Lopsided 版本、变量版本和量子版本局部引理紧的条件, 并讨论抽象版本紧的条件同统计物理、量子版本紧的条件同量子物理之间的联系. 同时, 我们还将以布尔可满足性问题和量子可满足性问题为例, 说明局部引理在证明问题有解、找到问题的解以及对问题的解进行计数和采样等方面的应用.

关键词 洛瓦兹局部引理, 变量版本局部引理, 量子版本局部引理, 构造版本局部引理, Shearer 界

1 引言

1975 年, 著名数学家 Erdős 和 Lovász 提出了洛瓦兹局部引理 [1]. 该引理一经提出之后, 就成为了最重要的概率方法之一 [2]. 最初的洛瓦兹局部引理关心的是如下问题, 给定一组坏事件之间的依赖关系, 当这些坏事件的概率满足什么条件时, 可以保证所有的坏事件均不发生. 近年来, 人们发展了各种新版本的局部引理, 如 Lopsided 版本、变量版本、量子版本和构造版本, 并且发现了它们在计算机和物理学等领域的很多新应用 [3]. 本文将综述近年来洛瓦兹局部引理的新变种及其应用.

引用格式: 何昆, 孙晓明. 洛瓦兹局部引理的新变种及其应用. 中国科学: 信息科学, 2020, 50: 1680–1696, doi: 10.1360/SSI-2019-0287
He K, Sun X M. New versions of Lovász Local Lemma and their applications (in Chinese). Sci Sin Inform, 2020, 50: 1680–1696, doi: 10.1360/SSI-2019-0287

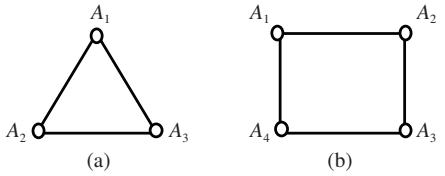

图 1 依赖图的例子. (a) 3 个事件; (b) 4 个事件

Figure 1 Examples of the dependency graph. (a) Three events; (b) four events

2 抽象版本局部引理

给定概率空间中的一组坏事件 $\mathcal{A}=\{A_1,\ldots,A_m\}$, 假定这些事件的概率依次为 $p_1,\ldots,p_m$. 局部引理关心当这组事件的概率向量 $\boldsymbol{p}=(p_1,\ldots,p_m)$ 满足什么条件时, 可以保证所有的坏事件都不发生. 我们首先来考虑两种极端情况, 即所有事件全独立和所有事件全相关. 当这组事件全独立时, 只要每个事件的概率均小于 1, 即可保证所有的坏事件不发生. 当这组事件全相关时, 只有所有事件的概率之和小于 1, 才能保证所有的坏事件不发生. 对于一般情况, 事件集 $\mathcal{A}$ 中坏事件的依赖关系可以由一个无向图 $G_D=([m],E)$ 刻画, 其中 G_D 的每个顶点 $i\in[m]$ 对应一个坏事件 A_i, 并且 A_i 同所有的 $\{A_j: j\neq i,(i,j)\notin E\}$ 相互独立. 我们称 G_D 为事件集 $\mathcal{A}$ 的依赖图, 并用 Γ_i 表示顶点 i 在 G_D 中的邻居. 例如, 图 1(a) 所示的 3 个事件全相关, 图 1(b) 所示的 4 个事件, A_1 与 A_3 独立, A_2 与 A_4 独立. 局部引理关心给定依赖图, 当事件的概率满足什么条件时能同时避开所有的坏事件, 也就是要刻画依赖图的抽象内部.

定义1 (图的抽象内部) 图 G_D 的抽象内部, $\mathcal{I}(G_D)$, 定义为

$$\mathcal{I}(G_D)=\Big\{\boldsymbol{p}:\text{对于任意的依赖图为 } G_D \text{ 的事件集 } \mathcal{A}, \text{若其概率向量为 } \boldsymbol{p},\\ \text{则 } \Pr\left(\cap_{A\in\mathcal{A}}\overline{A}\right)>0 \text{ 始终成立}\Big\}.$$

因为依赖图只给定了事件之间的依赖关系, 对事件的形式没有任何其他的要求, 因此, 我们称相关局部引理为抽象版本局部引理 (abstract LLL). 容易验证, 图 1(a) 中所示的依赖图 G_D 对应的抽象内部为 $\mathcal{I}(G_D)=\{\boldsymbol{p}:p_1+p_2+p_3<1\}$, 即图 2(b) 中三角形以下所有的概率向量都属于 $\mathcal{I}(G_D)$.

2.1 最常用的局部引理及其在 k-SAT 上的应用

最简单的局部引理形式如下.

定理1 [4,5] 给定图 $G_D=([m],E)$ 和 $p\in(0,1)$, 令 d 为 G_D 中顶点的最大度. 如果 $e\cdot p\cdot d\leqslant 1$, 则 $\boldsymbol{p}=(p,\ldots,p)\in\mathcal{I}(G_D)$.

下面我们来看一看定理 1 在 k-SAT 问题上的应用. 如果一个合取范式的每个子句都恰好包含 k 个文字, 我们称该合取范式为一个 k-SAT 实例. 如 $\Phi=(x_1\vee\overline{x}_2)\wedge(x_2\vee\overline{x}_3)\wedge(x_3\vee\overline{x}_1)$ 就是一个 2-SAT 实例. 由定理 1, 我们可以证明如下推论.

推论1 [2] 给定一个 k-SAT 的实例 Φ, 如果其每个子句最多同其他 $\lfloor 2^k/e\rfloor$ 个子句共用变量, 则 Φ 是可满足的.

证明 我们把 Φ 涉及的所有变量看作是独立随机变量, 每个随机变量以 1/2 的概率取值为 0, 以 1/2 的概率取值为 1. 对 Φ 的每个字句定义一个坏事件, 其中 A_i 发生当且仅当第 i 个子句不被满足. 由 Φ 是一个合取范式, 容易验证, 任何一个坏事件发生的概率均为 $1/2^k$, 且 Φ 可满足当且仅当所有的

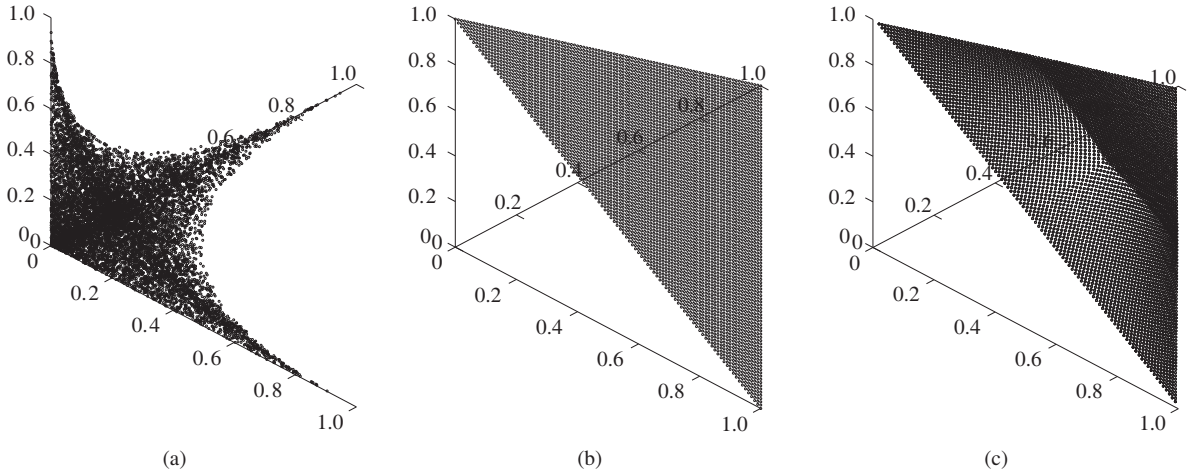

图 2　不同版本局部引理所刻画的概率向量. (a) 定理 3; (b) 定理 4; (c) 定理 9

Figure 2　The probability vectors characterized by different LLLs. (a) Theorem 3; (b) Theorem 4; (c) Theorem 9

坏事件均不发生. 令 G_D 为这些坏事件对应的依赖图, 其中顶点 i 与 j 之间连一条边, 当且仅当第 i 个子句与第 j 个子句共用变量. 因为 Φ 的每个子句最多同其他 $\lfloor 2^k/e \rfloor$ 个子句共用变量, 则 G_D 中任何一个顶点的度均不超过 $\lfloor 2^k/e \rfloor$. 由 $e \cdot 1/2^k \cdot \lfloor 2^k/e \rfloor \leqslant 1$, 结合定理 1, 本推论成立.

事实上, 推论 1 在渐进意义下是紧的. 2016 年, Gebauer 等 [6] 证明了如下定理.

定理2 [6]　存在常数 c, 使得对于任意的正整数 k, 均存在一个不可满足的 k-SAT 的实例 Φ, 其每个子句最多同其他 $\lfloor 2^k(1/e + c/\sqrt{k}) \rfloor$ 个子句共用变量.

如定理 1 所示, 最初的局部引理中所有坏事件的概率是相等的. 1977 年, Spencer [4] 将局部引理推广到了坏事件的概率不同的情况.

定理3 [4]　给定图 $G_D = ([m], E)$ 和向量 $\boldsymbol{p} \in (0,1)^m$, 如果存在实数 $x_1, \ldots, x_m \in (0,1)$ 使得 $p_i \leqslant x_i \prod_{j \in \Gamma_i}(1 - x_j)$ 对任意的 $i \in [m]$ 均成立, 则 $\boldsymbol{p} \in \mathcal{I}(G_D)$.

对于绝大多数依赖图, 定理 3 所刻画的概率向量依然只是抽象内部的真子集. 以图 1(a) 所示的依赖图为例, 定理 3 所刻画的概率向量如图 2(a) 所示. 而如之前所述, 图 2(b) 中三角形以下所有的概率向量都属于该依赖图的抽象内部.

定理 1 和 3 是使用得最广的局部引理. 除了应用到 k-SAT 问题之外, 其他应用还包括超图染色 [7]、拉姆塞数 [4] 等. 更多应用可以参见文献 [2].

2.2　抽象版本紧的条件及其物理内涵

定理 1 和 3 所刻画的概率向量都只是抽象内部的真子集. 1985, Shearer [5] 首先给出了抽象内部的精确刻画. 给定图 $G_D = ([m], E)$, 令 $\mathrm{Ind}(G_D)$ 表示由 G_D 的独立集构成的集合. 对于任意的长为 m 的向量 $\boldsymbol{\lambda}$, 令 $I(G_D, \boldsymbol{\lambda}) = \sum_{S \in \mathrm{Ind}(G_D)} \prod_{i \in S} \lambda_i$. 对于 G_D 任意的诱导子图 G, 令 $\boldsymbol{\lambda}(G)$ 为 G 中的顶点对应的 $\boldsymbol{\lambda}$ 的元素组成的向量. 则有如下定理.

定理4 [5]　给定图 $G_D = ([m], E)$ 和概率向量 $\boldsymbol{p} \in (0,1)^m$, $\boldsymbol{p} \in \mathcal{I}(G_D)$ 当且仅当对于 G_D 任意的诱导子图 G, $I(G, -\boldsymbol{p}(G)) > 0$ 始终成立. 如果 $\boldsymbol{p} \in \mathcal{I}(G_D)$, 则对于任意依赖图为 G_D, 概率向量为 $\boldsymbol{p}$ 的事件集 $\mathcal{A}$ 均有 $\Pr\left(\cap_{A \in \mathcal{A}} \overline{A}\right) \geqslant I(G_D, -\boldsymbol{p})$, 且存在事件集使等号成立.

以图 1(a) 中的依赖图为例, 容易验证定理 4 所刻画的抽象内部为 $\{\boldsymbol{p}: p_1+p_2+p_3<1\}$, 即恰好包含图 2(b) 中三角形以下所有的概率向量. $I(G_D,\boldsymbol{\lambda})$ 被称为 G_D 的独立集多项式, 是被研究的最多的图多项式之一, 在组合数学和计算机科学中有很多应用. $I(G_D,\boldsymbol{\lambda})$ 也是统计物理中硬核晶格气模型的配分函数, 其中 $\boldsymbol{\lambda}\in\mathbb{C}^m$. 物理学家们尤其关心 $I(G_D,\boldsymbol{\lambda})=0$ 对哪些 $\boldsymbol{\lambda}$ 成立. 他们很早就注意到了局部引理和硬核晶格气模型之间的联系 [8~10]. 除了形式上的一致之外, 这种联系还体现在如下两个方面. 第 1, 若 p 是由 Shearer 界算出的使得 $I(G_D,-p^m)=0$ 成立的最小概率, 则 $-p$ 恰好也是硬核晶格气模型配分函数的第 1 个负的逸度零点 (fugacity zero), 在该零点, 一些热力学量会展现出非平凡的属性. 第 2, 若 $\boldsymbol{p}\in\mathcal{I}(G_D)$ 且 $|\lambda_i|\leqslant p_i$ 对于任意的 $i\in[m]$ 成立, 则 $I(G_D,\boldsymbol{\lambda})\neq 0$ [11]. 借助局部引理与硬核晶格气模型配分函数之间的联系以及统计物理中配分函数研究的新进展, 人们发现了新的局部引理, 即团展开局部引理, 并利用该引理改进了一些组合问题的界 [12]. 关于独立集多项式研究的最新进展, 可参见文献 [13, 14].

2.3 其他的中间版本与应用

尽管 Shearer 界对抽象版本局部引理是紧的, 但判定一个概率向量是否落在 Shearer 界之内却是 #P 难的 [13]. 因此, 人们发展了一系列比定理 3 的界更好同时又相对容易计算的局部引理, 如团局部引理 [15]、团展开局部引理 [12], 并将它们应用到了 k-SAT、特定类型的图染色和拉丁排列 (Latin transversals) 等问题. 相关工作可以参见 Szegedy 的综述 [3].

3 Lopsided 版本局部引理

本节将介绍抽象版本局部引理的一种有趣的推广, 即 Lopsided 版本局部引理 (Lopsided LLL). 在抽象版本局部引理中, 事件集 $\mathcal{A}$ 中坏事件的依赖关系由依赖图 $G_D=([m],E)$ 刻画, 其中每个坏事件 A_i 同所有的 $\{A_j: j\neq i, j\notin\Gamma_i\}$ 相互独立. 在 Lopsided 版本局部引理中, 事件集 $\mathcal{A}$ 中坏事件的依赖关系由负依赖图刻画 [16], 无向图 G_D 为事件集 $\mathcal{A}$ 的负依赖图, 当且仅当 G_D 的每个顶点 i 对应一个坏事件 A_i, 且对于任意的顶点 $i\in[m]$ 和任意顶点集 $K\subseteq[m]\setminus(\Gamma_i\cup\{i\})$, $\Pr(A_i|\bigcup_{k\in K}A_j)\geqslant\Pr(A_i)$ 成立. 也就是说, A_i 同其在 G_D 中的非邻居倾向于同时发生. 换句话说, G_D 中的边刻画的是事件之间倾向于不同时发生的依赖关系, 因此, 我们称 G_D 为 "负" 依赖图. 容易验证, 对于任意一个事件集 $\mathcal{A}$, 如果 G_D 是事件集 $\mathcal{A}$ 的依赖图, 则 G_D 一定也是 $\mathcal{A}$ 的负依赖图.

在一些应用中, 坏事件集合对应的依赖图很稠密, 而负依赖图却很稀疏. 因此, 抽象版本局部引理的条件无法满足, 而应用 Lopsided 版本局部引理却可以算出很好的界. 我们考虑 Lopsided 版本局部引理的一个重要应用, 即证明满足一定条件的排列的存在性 [16~19]. 假设我们希望证明存在 $\{1,2,\ldots,n\}$ 的一个排列, 满足对于任意的 $i\in[n]$, 数 i 不落在排列的第 i 个位置. 由此, 我们可以定义 n 个坏事件, $\{A_1,A_2,\ldots,A_n\}$, 其中 A_i 表示数 i 落在排列的第 i 个位置. 容易验证, 这 n 个事件的依赖图是一个大小为 n 的团, 因为所有的事件都相关. 而这 n 个事件的一个负依赖图却是一个大小为 n 的独立集, 因为所有的坏事件是正相关的.

Lopsided 版本局部引理关心给定负依赖图, 当事件的概率满足什么条件时能同时避开所有的坏事件, 也就是要刻画负依赖图的 Lopsided 内部.

定义2 (图的 Lopsided 内部) 图 G_D 的 Lopsided 内部, $\mathcal{LI}(G_D)$, 定义为

$$\mathcal{LI}(G_D)=\Big\{\boldsymbol{p}: \text{对于任意的负依赖图为 } G_D \text{ 的事件集 } \mathcal{A}, \text{若其概率向量为 } \boldsymbol{p},$$

$$\text{则 } \Pr\left(\cap_{A\in\mathcal{A}}\overline{A}\right)>0 \text{ 始终成立}\Big\}.$$

下面的两个定理是定理 1 和 3 向负依赖图的推广.

定理5 给定图 $G_D=([m],E)$ 和 $p\in(0,1)$, 令 d 为 G_D 中顶点的最大度. 如果 $e\cdot p\cdot d\leqslant 1$, 则 $\boldsymbol{p}=(p,\ldots,p)\in\mathcal{LI}(G_D)$.

定理6 给定图 $G_D=([m],E)$ 和向量 $\boldsymbol{p}\in(0,1)^m$, 如果存在实数 $x_1,\ldots,x_m\in(0,1)$ 使得 $p_i\leqslant x_i\prod_{j\in\Gamma_i}(1-x_j)$ 对任意的 $i\in[m]$ 均成立, 则 $\boldsymbol{p}\in\mathcal{LI}(G_D)$.

可以证明, Shearer 界对 Lopsided 版本局部引理依然是紧的, 即有如下定理.

定理7 [5] 给定图 $G_D=([m],E)$ 和向量 $\boldsymbol{p}\in(0,1)^m$, $\boldsymbol{p}\in\mathcal{LI}(G_D)$ 当且仅当对于 G_D 任意的诱导子图 G, $I(G,-\boldsymbol{p}(G))>0$ 成立. 如果 $\boldsymbol{p}\in\mathcal{LI}(G_D)$, 则对于任意负依赖图为 G_D, 概率向量为 $\boldsymbol{p}$ 的事件集 $\mathcal{A}$ 均有 $\Pr\left(\cap_{A\in\mathcal{A}}\overline{A}\right)\geqslant I(G_D,-\boldsymbol{p})$, 且存在事件集使等号成立.

下面介绍 Lopsided 版本局部引理在 k-SAT 问题上的应用. 2016 年, Gebauer 等 [6] 运用定理 6 证明了如下推论.

推论2 [6] 给定一个 k-SAT 的实例 Φ, 如果其每个变量最多被 $\lfloor 2^{k+1}/(e(k+1))\rfloor$ 个子句共用, 则 Φ 是可满足的.

事实上, 推论 2 在渐进意义下也是紧的, 因为有如下定理.

定理8 [6] 存在常数 c, 使得对于任意的 k, 均存在一个不可满足的 k-SAT 的实例 Φ, 其每个变量最多被 $\lfloor(2/e+c/\sqrt{k})2^k/k\rfloor$ 个子句共用.

Lopsided 版本局部引理在组合数学和理论计算机中还有其他很多有趣的应用, 比如拉丁排列 [12,16,18]、超图上的匹配 [20]、特定类型的图染色 [19]、纠错码的存在性证明 [21] 等. 关于 Lopsided 版本局部引理的应用的详细介绍可参见文献 [20,22].

4 变量版本局部引理

在抽象版本局部引理中, 依赖图只给出了事件之间是否存在依赖关系, 却没有刻画它们如何相互依赖. 我们考虑如下提供了更丰富的事件结构的刻画. 设事件集 $\mathcal{A}=\{A_1,\ldots,A_m\}$ 由集合 $\mathcal{X}=\{X_1,\ldots,X_n\}$ 中的随机变量决定. 这里, 每个 X_i 既可以是连续变量, 也可以是离散变量, 且集合 $\mathcal{X}$ 中所有的随机变量相互独立. 对任意的 $i\in[m]$, 令 $\mathcal{X}_i\subseteq\mathcal{X}$ 表示 A_i 所依赖的所有随机变量构成的集合. 则这些事件和变量之间的依赖关系可以完全由一个二部图 $G_B=([m],[n],E)$ 刻画, 其中, 对于任意的 $(i,j)\in[m]\times[n]$, $(i,j)\in E$ 当且仅当 $X_j\in\mathcal{X}_i$. 我们称 $\mathcal{A}$ 是由变量集 $\mathcal{X}$ 生成的事件系统, 称 G_B 为 $\mathcal{A}$ 对应的事件 – 变量图.

考虑 2-SAT 实例 $\Phi=(x_1\vee\overline{x}_2)\wedge(x_2\vee\overline{x}_3)\wedge(x_3\vee\overline{x}_1)$. 对于任意的 $i\in\{1,2,3\}$, 定义随机变量 X_i, 其中 $X_i=0$ 表示 x_i 取值为 0, $X_i=1$ 表示 x_i 取值为 1, 且令 $\Pr(X_i=0)=\Pr(X_i=1)=1/2$. 对于任意的 $j\in\{1,2,3\}$, 定义坏事件 A_j 为 Φ 的第 j 个子句不被满足. 容易验证事件集 $\mathcal{A}=\{A_1,A_2,A_3\}$ 的事件 – 变量图如图 3(a) 所示.

事件 – 变量图是对坏事件集合的一种很自然的刻画. 在局部引理的绝大多数应用中, 坏事件都是由一系列独立的随机变量决定的, 如超图染色 [7]、可满足性问题 [6,23,24]、无环图的边染色 [25] 等. 近年来, 构造版本局部引理上的重大突破也是基于变量模型的 [26,27].

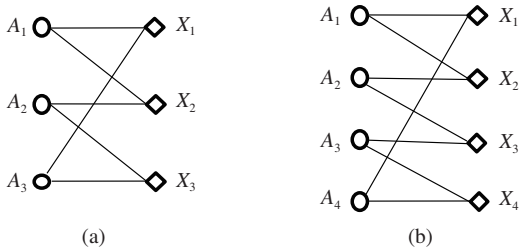

图 3 事件 – 变量图的例子. (a) 3 个事件; (b) 4 个事件

Figure 3 Examples of the event-variable graph. (a) Three events; (b) four events

变量版本局部引理 (variable LLL) 关心给定事件 – 变量图, 当事件的概率满足什么条件时能同时避开所有的坏事件, 也就是要刻画事件 – 变量图的变量内部.

定义3 (二部图的变量内部) 二部图 G_B 的变量内部, $\mathcal{VI}(G_B)$, 定义为

$$\mathcal{VI}(G_B)=\Big\{\boldsymbol{p}:\text{对于任意的事件 – 变量图为 } G_B \text{ 的事件集 } \mathcal{A}, \text{若其概率向量为 } \boldsymbol{p},\\ \text{则 } \Pr\left(\cap_{A\in\mathcal{A}}\overline{A}\right)>0 \text{ 始终成立}\Big\}.$$

给定二部图 $G_B=([m],[n],E)$, 我们称 $[m]$ 中的顶点为左顶点, $[n]$ 中的顶点为右顶点, 并按如下方式定义 G_B 的基图.

定义4 (二部图的基图) 二部图 $G_B=([m],[n],E)$ 的基图为 $G_D(G_B)=([m],E')$, 其中 $E'=\{(v_1,v_2):v_1,v_2 \text{ 均为左顶点且 } v_1,v_2 \text{ 同时与某个右顶点相邻}\}$.

容易验证, 若 G_B 是事件系统 $\mathcal{A}$ 的事件 – 变量图, 则 $G_D(G_B)$ 是 $\mathcal{A}$ 的一个依赖图. 以之前为 2-SAT 实例 $\Phi=(x_1\vee\overline{x}_2)\wedge(x_2\vee\overline{x}_3)\wedge(x_3\vee\overline{x}_1)$ 定义的事件集 $\mathcal{A}=\{A_1,A_2,A_3\}$ 为例. 图 3(a) 是 $\mathcal{A}$ 的事件 – 变量图, 容易验证图 3(a) 的基图即是图 1(a), 而图 1(a) 则是 $\mathcal{A}$ 的依赖图.

对于任意的概率向量 $\boldsymbol{p}$, 如果 $\boldsymbol{p}\notin\mathcal{VI}(G_B)$, 则由 $\mathcal{VI}(G_B)$ 的定义有存在事件 – 变量图为 G_B 概率向量为 $\boldsymbol{p}$ 的事件集 $\mathcal{A}$ 使得 $\Pr\left(\cap_{A\in\mathcal{A}}\overline{A}\right)=0$. 因为 $\mathcal{A}$ 也是一个依赖图为 $G_D(G_B)$ 的事件集, 我们有 $\boldsymbol{p}\notin\mathcal{I}(G_D(G_B))$. 因此, 对于任意的二部图 G_B, $\mathcal{I}(G_D(G_B))\subseteq\mathcal{VI}(G_B)$. 如果 $\mathcal{I}(G_D(G_B))\neq\mathcal{VI}(G_B)$, 我们称 Shearer 界对 G_B 不紧, 或 G_B 变量版本与抽象版本有差异. 人们猜测, Shearer 界对很多二部图都不紧. 但在很长一段时间里, 人们仅知道唯一一个 Shearer 界不紧的二部图, 即图 3(b) [28], 对二部图的变量内部也没有超出 Shearer 界的刻画. 在对由变量生成的事件系统应用局部引理时, 人们通常直接忽略掉变量信息, 将事件之间的依赖关系抽象为依赖图, 并使用抽象版本局部引理. 因为 Shearer 界对抽象版本局部引理是紧的, 这样找到的条件不可能超出 Shearer 界.

4.1 变量版本紧的条件

2017 年, 何昆等 [29] 刻画了变量版本局部引理紧的条件, 并找到了一系列变量版本与抽象版本有差异的二部图. 本小节给出这一条件.

如果一个二部图不连通, 则此二部图的变量内部即是其连通分量的变量内部的直积. 因此, 我们只需考虑那些连通的二部图. 我们首先定义二部图的变量边界.

定义5 (二部图的变量边界) 二部图 G_B 的变量边界, $\mathcal{V}\partial(G_B)$, 定义为

$$\mathcal{V}\partial(G_B)=\Big\{\boldsymbol{p}:(1-\epsilon)\boldsymbol{p}\in\mathcal{VI}(G_B) \text{ 和 } (1+\epsilon)\boldsymbol{p}\notin\mathcal{VI}(G_B) \text{ 对任意的 } \epsilon\in(0,1) \text{ 成立}\Big\}.$$

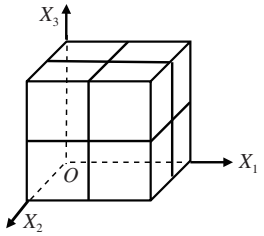

图 4　定理 9 中规划的直观含义

Figure 4　Intuition of the programme in Theorem 9

我们称 $\boldsymbol{p} \in \mathcal{V}\partial(G_B)$ 为 G_B 的变量边界向量.

刻画二部图的变量内部等价于刻画其变量边界. 2017 年, 何昆等 [29] 提出了一个数学规划来刻画二部图的变量边界.

定理9 [29]　给定二部图 $G_B = ([m], [n], E)$ 和向量 $\boldsymbol{p} \in (0,1)^m$, 令 $\boldsymbol{d} = (d_1, \ldots, d_n)$, 其中 d_j 是 G_B 的右顶点 j 的度. 则 $\lambda\boldsymbol{p}$ 是 G_B 的变量边界向量当且仅当 λ 是如下规划的最优解:

$$
\begin{aligned}
&\min \lambda\\
&\text{s.t. (1) 对于任意的 } k_1 \in [d_1], \ldots, k_n \in [d_n], \sum_{i\in[m]} C_{i,k_1,k_2,\ldots,k_n} \geqslant 1;\\
&\quad\text{(2) 对于任意的 } (i,j) \in ([m]\times[n]) \setminus E,\ C_{i,k_1,k_2,\ldots,k_n} \text{不依赖于} k_j;\\
&\quad\text{(3) 对于任意的 } i \in [m], \sum_{k_1\in[d_1],\ldots,k_n\in[d_n]} \left(\prod_{j\in[n]} x_{jk_j}\right) C_{i,k_1,k_2,\ldots,k_n} = \lambda p_i;\\
&\quad\text{(4) 对于任意的 } j \in [n], \sum_{k\in[d_j]} x_{jk} = 1;\\
&\quad\text{(5) 对于任意的 } j \in [n], k \in [d_j],\ x_{jk} \in [0,1];\\
&\quad\text{(6) 对于任意的 } i \in [m], k_1 \in [d_1], \ldots, k_n \in [d_n],\ C_{i,k_1,k_2,\ldots,k_n} \in \{0,1\}.
\end{aligned}
$$

以图 3(a) 中的二部图为例, 具体说明定理 9 中规划的直观含义. 对图 3(a) 中的二部图, 有 $m = n = 3$. 我们把事件 A_1, A_2, A_3 看成是三维坐标空间中的柱体. A_1 事件只同 X_1, X_2 有关, 同 X_3 无关. 因此, A_1 可以看作是底面在 X_1OX_2 平面的柱体. 类似地, A_2 可以看作是底面在 X_2OX_3 平面的柱体, A_3 可以看作是底面在 X_1OX_3 平面的柱体. 上述规划本质上是说, 三维单位立方体被划分成了 8 个小立方体, A_1, A_2, A_3 中的每个柱体都是若干个小立方体的并, 如图 4 所示.

具体的, 上述规划的第 5 条约束限定了 X_j 坐标轴上的区间被划分成了 d_j 段, 其中第 k 段的长度为 x_{jk}. 因为图 3(a) 满足 $d_1 = d_2 = d_3 = 2$, 所以三维立方体被划分成了 8 个小立方体. 设这 8 块小立方体的编号分别为 111, 112, 121, 122, 211, 212, 221, 222. 其中, 第 $k_1k_2k_3$ 号小立方体的长宽高分别由 x_{1k_1}, x_{2k_2} 和 x_{3k_3} 表示. 因此, 第 $k_1k_2k_3$ 号小立方体的体积是 $\prod_{j\in[3]} x_{jk_j}$.

上述规划的第 4 条约束限定我们考虑单位立方体, 即整个大立方体的长宽高都是 1.

柱体 A_i 是否包含第 $k_1k_2k_3$ 号小立方体由 C_{i,k_1,k_2,k_3} 表示. 如果 $C_{i,k_1,k_2,k_3} = 1$, 则柱体 A_i 包含第 $k_1k_2k_3$ 号小立方体; 否则 $C_{i,k_1,k_2,k_3} = 0$, 柱体 A_i 不包含第 $k_1k_2k_3$ 号小立方体. 上述规划的第 6 条约束限定了 C_{i,k_1,k_2,k_3} 的取值只能是 0 和 1, 因此, 任何一个小立方体 $k_1k_2k_3$ 要么被包含在柱体 A_i 之中, 要么和柱体 A_i 的交为空.

容易验证, 柱体 A_i 的体积是 $\sum_{k_1\in[d_1],\ldots,k_n\in[d_n]}(\prod_{j\in[n]}x_{jk_j})C_{i,k_1,k_2,\ldots,k_n}$. 因此, 上述规划的第 3 条约束限定了柱体集满足体积要求, 即柱体 A_i 的体积恰好为事件 A_i 的概率 λq_i.

上述规划的第 2 条约束限定了 A_1,A_2,A_3 符合图 3(a) 中事件和变量的依赖关系. 如对于任意的 k_1,k_2,k_3, C_{1,k_1,k_2,k_3} 不依赖于 k_3, 即事件 A_1 不依赖于变量 X_3.

上述规划的第 1 条约束限定了这 8 个小立方体中的每一个一定被某个柱体包含, 因而, 整个单位立方体被柱体 A_1,A_2,A_3 的并撑满, 即 $\Pr\left(\cap_i\overline{A_i}\right)=0$.

4.2 圈二部图的变量边界

本小节给出圈二部图的变量边界. 圈二部图是一类很重要的二部图, 人们所知的第一个变量版本与抽象版本有差异的例子, 就是图 3(b) 所示的圈二部图.

定义6 (圈二部图) 对于任意的 $n\geqslant 4$, 如果一个二部图的基图是长为 n 的圈, 我们称该二部图为长为 n 的圈二部图. 如果一个二部图的基图是长为 3 的圈, 且此二部图中不存在一个右顶点同时与所有的左顶点相邻, 我们称该二部图为长为 3 的圈二部图. 长为 n 的圈二部图也简称为圈二部图.

在考察长为 n 的圈二部图时, 为了表达的简洁性, 有时我们会把标号 $i\in[n]$ 记为 $n+i$. 例如 p_{n+1} 是指 p_1.

令 $G_n=([n],[n],E_n)$, 其中 $E_n=\{(i,i),(i,(i+1)):i\in[n]\}$. 例如, G_3 和 G_4 分别如图 3(a) 和 (b) 所示. 不难验证, 任何一个长为 n 的圈二部图的变量边界都和 G_n 的变量边界相同. 因此, 我们只需要考虑 G_n. 基于定理 9, 何昆等 [29] 给出了 G_n 变量边界的精确刻画.

定理10 [29] 给定向量 $\boldsymbol{p}\in(0,1)^n$, 对于任意的 $i\in[n]$, 令 λ_i 为如下方程组的最小正数解: $b_1=\lambda p_i$, 对任意的 $2\leqslant k\leqslant n-1$, $b_k=\frac{\lambda p_{k+i-1}}{1-b_{k-1}}$, $b_{n-1}=1-\lambda p_{i-1}$. 令 $\lambda_0=\min_{i\in[n]}\lambda_i$. 则 $\lambda_0\boldsymbol{p}$ 是 G_n 的变量边界向量.

由定理 10, 我们可以得到最简单的圈二部图 G_3 的变量边界向量.

例1 [29] 设向量 $\boldsymbol{p}\in(0,1)^3$ 满足 $p_1+p_2+p_3=1$. 由定理 10 有, 对于任意的 $i\in\{1,2,3\}$, $\lambda_i=\frac{1-\sqrt{1-4p_ip_{i+2}}}{2p_ip_{i+2}}$. 因为函数 $\frac{1-\sqrt{1-2x}}{x}$ 在 $x>0$ 时随 x 单调递增, 则 $\lambda_0=\min_{i\in[3]}\lambda_i=\lambda_j$, 其中 j 满足 p_ip_{i+2} 在 $i=j$ 时取得最小值. 例如, 如果 $p_1\geqslant p_2$ 且 $p_1\geqslant p_3$, 则 $\lambda_3\boldsymbol{p}=\frac{1-\sqrt{1-4p_2p_3}}{2p_2p_3}\boldsymbol{p}$ 是 G_3 的变量边界向量.

图 2(c) 所示的就是 G_3 的变量边界. 可以看到, G_3 的变量边界同图 2(b) 所示的 $G_D(G_3)$ 的抽象内部的边界不同. 也就是说, G_3 的变量内部超出了 Shearer 界.

5 量子版本局部引理

物理学家感兴趣的绝大多数系统都可以由局域哈密尔顿量 $H=\sum_i H_i$ 刻画, 其中每个局域的项 H_i 非平凡地作用在 H 的部分 qudit 上. 如果 H_i 非平凡地作用在不超过 k 个 qudit 上, 我们称其为 k- 局域的. 如果 H 的基态同时也是每个 H_i 的基态, 我们称 H 是无忧的 (frustration free). 无忧的局域哈密尔顿量有零能量的基态, 在物理学中有很多应用 [30,31].

在计算机科学中, 无忧的局域哈密尔顿量被称为可满足的, 判定一个给定的局域哈密尔顿量是否是无忧的被称为量子可满足性问题 (quantum SAT), 简称 QSAT. 人们已经证明, QSAT 是 QMA_1- 完全的 [32], 而 QMA_1- 完全问题是难解的, 人们普遍相信这类问题即使在量子图灵机模型下也没有多项

表 1 向量空间的相对维度与独立性 [33]

Table 1 Relative dimension and independence of vector space [33]

Probability space Ω	$\rightarrow$	Vector space V
Event $A \subseteq \Omega$	$\rightarrow$	Subspace $A \subseteq V$
Probability $\Pr(A)$	$\rightarrow$	Relative dimension $R(A) := \frac{\dim(A)}{\dim(V)}$
Conjunction $A \wedge B$	$\rightarrow$	$A \cap B$
Disjunction $A \vee B$	$\rightarrow$	$A + B = \{a + b \mid a \in A, b \in B\}$
Complement $\overline{A} = \Omega \backslash A$	$\rightarrow$	Orthogonal subspace $A^{\perp}$
Conditional probability $\Pr(A\|B) := \frac{\Pr(A \wedge B)}{\Pr(B)}$	$\rightarrow$	$R(A\|B) := \frac{R(A \cap B)}{R(B)}$
Independence $\Pr(A \wedge B) = P(A) \cdot P(B)$	$\rightarrow$	$R(A \cap B) = R(A) \cdot R(B)$

式时间算法. 类似于 SAT 是经典复杂性理论的核心问题, QSAT 也是量子复杂性理论的核心问题. 量子版本局部引理 (quantum LLL) 正是求解 QSAT 的有力工具.

给定局域哈密尔顿量 $H = \sum_i H_i$, 令 $\Pi = \sum \Pi_i$, 其中 Π_i 为向 H_i 的激发态上投影的投影算符. 容易验证, H 是无忧的当且仅当 Π 是无忧的. 因此, 本文中我们只关心那些所有局域的项均是投影算符的局域哈密尔顿量. 同时, 为了陈述得简单, 我们将无差别地使用哈密尔顿量、子空间和到子空间的投影算符.

5.1 第一个量子版本局部引理及其在 k-QSAT 上的应用

2009 年, Ambainis 等 [33] 将概率和独立性等概念推广到了向量空间, 提出了基于依赖图的量子版本局部引理. 相关概念如表 1 [33] 所示.

考虑局域哈密尔顿量 $\Pi = \sum \Pi_i$. 类似于经典的情况, 这些子空间 $\{\Pi_i\}$ 间的依赖关系可以由一个无向图 $G_D = ([m], E)$ 刻画, 其中 G_D 的每个顶点 $i \in [m]$ 对应一个子空间 Π_i, 并且 Π_i 同所有的 $\{A_j : j \neq i, j \notin \Gamma_i\}$ 不共用 qudit. 我们称 G_D 为局域哈密尔顿量 $\Pi = \sum \Pi_i$ 的依赖图.

以下的量子版本局部引理是定理 1 向子空间的推广.

定理11 [33,34] 设子空间 $A_1, A_2, \ldots, A_m$ 的依赖图为 $G_D = ([m], E)$, 其中 G_D 的所有顶点的度均不超过 d. 若 $e \cdot d \cdot R(A_i) \leqslant 1$ 对任意的 $i \in [m]$ 均成立, 则有 $R(\bigcup_i A_i) < 1$.

以下的量子版本局部引理是定理 3 向子空间的推广.

定理12 [33] 设子空间 $A_1, A_2, \ldots, A_m$ 的依赖图为 $G_D = ([m], E)$. 若存在实数 $x_1, \ldots, x_m \in (0, 1)$ 使得 $R(A_i) \leqslant x_i \prod_{j \in \Gamma_i}(1 - x_j)$ 对任意的 $i \in [m]$ 均成立, 则 $R(\bigcup_i A_i) < 1$.

量子版本局部引理的一个典型应用是求解 QSAT. k-QSAT 问题是对 k-SAT 问题的自然推广. 考虑局域哈密尔顿量 $\Pi = \sum \Pi_i$, 若其中每个 Π_i 都是 k- 局域的, 我们称 Π 是一个 k-QSAT 实例. 利用定理 11, Ambainis 等 [33] 将推论 1 推广到了 k-QSAT.

推论3 [33] 给定一个 k-QSAT 实例 $\Pi = \sum \Pi_i$, 其中每个 Π_i 的秩均为 1. 如果每个 Π_i 最多同其他 $\lfloor 2^k/e \rfloor$ 个子空间共用 qudit, 则 Π 可满足.

任何一个经典的 k-SAT 实例都可以被看作一个 k-QSAT 实例, 只不过 k-SAT 实例涉及的子空间一定可以由标准计算基张成. 结合定理 2, 我们有推论 3 在渐进意义下也是紧的.

利用定理 11, Ambainis 等 [33] 还将随机 k-QSAT 问题临界密度的下界从 $\Omega(1)$ 改进到了 $\Omega(2^k/k^2)$, 几乎匹配上了临界密度的上界 $O(2^k)$ [35].

5.2 量子版本紧的条件及其物理内涵

最近, Sattath 等 [36] 针对相互作用图推广了量子版本局部引理. 相互作用图 $G_B=([m],[n],E)$ 是一个二部图, 其中 $[m]$ 中的顶点表示哈密尔顿量, $[n]$ 中的顶点表示 qudit, 当一个哈密尔顿量非平凡地作用在另一个 qudit 上时, 相应的顶点之间连一条边. 相互作用图是对局域哈密尔顿量的一种自然刻画, 是经典情形下事件 – 变量图的量子对应.

事件 – 变量图的量子内部定义如下.

定义7 (二部图的量子内部) 二部图 G_B 的量子内部, $\mathcal{QI}(G_B)$, 定义为

$$\mathcal{QI}(G_B)=\Big\{\boldsymbol{r}:\text{存在与 }\boldsymbol{r}\text{ 等长的有理向量 }\boldsymbol{r}',\text{其每一维都不小于 }\boldsymbol{r},\text{且满足任意相互作用图为 }G_B,\text{相对维度向量为 }\boldsymbol{r}'\text{ 的局域哈密尔顿量都是无忧的}\Big\}.$$

由上述定义容易验证, 给定二部图 G_B 和有理向量 $\boldsymbol{r}$, 任意相互作用图为 G_B 相对维度向量为 $\boldsymbol{r}$ 的局域哈密尔顿量都是无忧的当且仅当 $\boldsymbol{r}\in\mathcal{QI}(G_B)$. 量子版本局部引理关心给定相互作用图, 当局域哈密尔顿量的相对维度向量满足什么条件时能保证该局域哈密尔顿量是无忧的, 也就是要刻画相互作用图的量子内部.

2016 年, Sattath 等 [36] 证明了 Shearer 界对量子版本局部引理依然是充分的, 即有如下定理.

定理13 [36] 对于任意的二部图 G_B, $\mathcal{I}(G_D(G_B))\subseteq\mathcal{QI}(G_B)$.

如第 2.2 小节所述, 由 Shearer 界算出的概率阈值的相反数恰好是硬核晶格气模型配分函数的第一个负的逸度零点, 在经典统计力学中已经被反复研究过. 结合经典统计力学中的工具和定理 13, Sattath 等 [36] 计算了多种晶格的无忧临界阈值的下界.

与变量版本局部引理超出 Shearer 界不同, Sattath 等 [36] 猜测 Shearer 界对量子版本局部引理是紧的. 这一猜测具有重要的物理意义.

首先, 这一猜测成立意味着硬核晶格气模型配分函数的第一个负的逸度零点恰好也是局域哈密尔顿量无忧的临界阈值的相反数. 同时, 几何化定理 [37] 说明了几乎所有 qudit 维数足够大的局域哈密尔顿量, 其核的相对维度都能取得理论上的极小值. 因此, 如果 Shearer 界对量子版本局部引理是紧的, 结合几何化定理, 我们有对于几乎所有 qudit 维数足够大的局域哈密尔顿量, 硬核晶格气模型的配分函数提供了其量子可满足性问题的完整刻画, 且晶格气的临界指数可以用来计算无忧哈密尔顿量的基态熵. 也就是说, 经典统计力学中的相关结论可以直接迁移到量子复杂性领域 [36].

其次, Gilyén 和 Sattath [38] 提出了一个量子重采样算法. 当局域哈密尔顿量的一致差异 (uniform gap) 足够大, 且其相对维度向量落在 Shearer 界之内时, 该算法可以高效地制备一个无忧的量子态. 如果 Shearer 界对量子版本局部引理是紧的, 则该量子重采样算法的收敛条件也是紧的.

2019 年, 何昆等 [34] 证明了这一猜测, 即有如下定理.

定理14 [34] 对于任意给定的二部图 G_B, $\mathcal{I}(G_D(G_B))=\mathcal{QI}(G_B)$.

6 构造版本局部引理

之前所讨论的局部引理只能用来证明问题的解的存在性. 本节将讨论构造版本局部引理 (constructive LLL), 除了证明解存在, 此类局部引理还会给出能快速找到问题的解的构造性算法.

1991 年, Beck [39] 提出了一个寻找满足所有约束的赋值的确定性算法. 当依赖图 $G_D=([m],E)$ 中顶点的最大度不超过 $2^{m/48}$ 时, 该算法是多项式的. 这是第一个构造版本局部引理. 之后, 人们做了

一系列改进弱化构造版本局部引理的条件 [40~43]. 这些构造版本局部引理都依赖于原来的非构造版本局部引理, 并且它们的条件离定理 1 中的条件还有较大差距.

2009 年, Moser [26] 提出了一个新的构造版本局部引理, 在 k-SAT 问题上几乎达到了推论 1 所刻画的界. 之后, Moser 和 Tardos [27] 一起改进了该结果, 他们在由变量生成的事件系统这一模型下, 提出了一个新的构造版本局部引理, 达到了定理 3 中的界. Moser [26] 及 Moser 和 Tardos [27] 的结果是局部引理研究中里程碑式的工作. 他们的结果既没有基于以前的构造版本局部引理, 也没有利用非构造版本局部引理的证明. 他们提出了一个简单的构造算法, 并给出了对算法收敛性的优雅的证明. 利用 Moser 和 Tardos 提供的构造性算法, 绝大多数非构造版本局部引理保证有解的问题都可以被快速地求解.

6.1 变量版本的构造算法及其在求解 k-SAT 上的应用

Moser 和 Tardos [27] 针对变量模型, 提出了一个简单的重采样算法, 即算法 1.

算法 1 Resample

1: Sample $X_1, \ldots, X_n$ uniformly at random;
2: **while** $\exists i \in [m]$ such that A_i holds **do**
3: Choose an arbitrary such i and resample all variables used by A_i;
4: **end while**
5: Return the current assignments of all variables.

显然, 当算法 1 停止时, 输出的对所有随机变量的赋值可以避开所有的坏事件. 并且, 人们还找到了一系列优雅的保证算法 1 停止的条件, 即定理 15, 17 和 19.

在变量模型下, 事件集 $\mathcal{A} = \{A_1, \ldots, A_m\}$ 的依赖图一般是指其二部图的基图. 对于依赖图, 有如下定理.

定理15 [27] 假设由变量生成的事件集 $\mathcal{A} = \{A_1, \ldots, A_m\}$ 的依赖图为 $G_D = ([m], E)$, 概率向量为 $\boldsymbol{p} \in (0,1)^m$. 如果存在实数 $x_1, \ldots, x_m \in (0,1)$ 使得 $p_i \leqslant x_i \prod_{j \in \Gamma_i}(1 - x_j)$ 对任意的 $i \in [m]$ 均成立, 则算法 1 对事件进行重采样的期望次数不超过 $\sum_{i \in [m]} \frac{x_i}{1-x_i}$.

利用定理 15, 绝大多数非构造版本局部引理保证有解的问题都可以被快速地求解. 这里以求解 k-SAT 为例进行说明.

定理16 [26, 44] 给定一个 k-SAT 实例 Φ, 如果其每个子句最多同其他 $\lfloor (2^k - 1)/e \rfloor$ 个子句共用变量, 则算法 1 可以找到一组使 Φ 为真的赋值, 且重采样的期望次数为 $O(m)$, 其中 m 是 Φ 的子句数.

结合定理 2 可知, 从渐进意义而言, 定理 16 对 k-SAT 问题是紧的.

在变量模型下, 事件集 $\mathcal{A} = \{A_1, \ldots, A_m\}$ 的负依赖图一般是指无向图 $G_D = ([m], E)$, 其中 G_D 的每个顶点 $i \in [m]$ 对应一个坏事件 A_i, 并且 $(i, j) \in E$ 当且仅当在 A_i, A_j 中只有一个事件发生时, 通过重采样该事件的变量可能导致另一个事件发生. 对于负依赖图, 有如下定理.

定理17 [27] 假设由变量生成的事件集 $\mathcal{A} = \{A_1, \ldots, A_m\}$ 的负依赖图为 $G_D = ([m], E)$, 概率向量为 $\boldsymbol{p} \in (0,1)^m$. 如果存在实数 $x_1, \ldots, x_m \in (0,1)$ 使得 $p_i \leqslant x_i \prod_{j \in \Gamma_i}(1 - x_j)$ 对任意的 $i \in [m]$ 均成立, 则算法 1 对事件进行重采样的期望次数不超过 $\sum_{i \in [m]} \frac{x_i}{1-x_i}$.

也就是说, 在变量模型下, Lopsided 版本局部引理也可以一定程度地算法化. 定理 17 是定理 15 向负依赖图的扩展. 利用定理 17, 可以证明如下结论.

定理18 [6,26] 给定一个 k-SAT 实例 Φ, 如果其每个变量最多被 $\lfloor 2^{k+1}/(e(k+1))\rfloor$ 个子句共用, 则算法 1 可以找到一组使 Φ 为真的赋值, 且重采样的期望次数为 $O(m)$, 其中 m 是 Φ 的子句数.

结合定理 8 可知, 从渐进意义而言, 定理 18 对 k-SAT 问题也是紧的.

Moser 和 Tardos 只能证明在定理 3 的条件下重采样算法快速收敛. 2011 年, Kolipaka 和 Szegedy [28] 进一步证明了重采样算法在 Shearer 界之内都快速收敛. 即有如下定理.

定理19 [28] 假设由变量生成的事件集 $\mathcal{A}=\{A_1,\ldots,A_m\}$ 的依赖图为 $G_D=([m],E)$, 概率向量为 $\boldsymbol{p}\in(0,1)^m$. 如果存在 $\epsilon>0$ 使得 $(1+\epsilon)\boldsymbol{p}\in\mathcal{I}(G_D)$, 则算法 1 对事件进行重采样的期望次数不超过 m/ϵ.

由第 4 节, 我们知道变量版本局部引理紧的条件超出了 Shearer 界. 因此, 重采样算法的收敛条件有可能进一步扩展. 2017 年, Catarata 等 [45] 发现实际执行时重采样算法对于很多超出 Shearer 界的实例依然是高效的. 一个重要开放问题是在变量模型下构造版本局部引理紧的条件是什么.

为了在非变量模型下快速找到问题的解, 除了变量模型, 人们还研究了其他模型下的构造版本局部引理. 2014 年, Harris 和 Srinivasan [17] 提出了针对排列的构造版本局部引理, 之后 Harvey 和 Vondrák [46] 进一步把构造版本局部引理扩展到了存在 resampling oracles 的情况. 2014 年, Achlioptas 和 Iliopoulos [47] 提出了基于随机游走的构造版本局部引理, 之后 Achlioptas 等 [48,49] 进一步把构造版本局部引理扩展成了一个集中的随机局部搜索的算法框架. 文献 [46,48] 中坏事件的选取规则是确定的. 2016 年, Kolmogorov [50] 证明了, 只要满足某种对易条件, 任意选取坏事件的规则都是可行的. 除了基于重采样的构造算法, 另一类重要的构造算法是基于回溯的 [26]. 最近, Achlioptas 等 [51] 提出了一个新的框架, 统一了基于重采样的算法和基于回溯的算法. 很多构造版本局部引理的算法, 如重采样, 都是随机的串行算法. 有一系列工作研究构造版本局部引理的去随机化和并行化 [27,52~54]. 最近, Harris [55] 给出了一个在 Shearer 界之内都快速收敛的确定性算法.

6.2 变量版本的构造算法及其在计数和采样上的应用

除了找到问题的解, 计算机科学还关心如何对问题的解计数, 以及如何对问题的解随机均匀采样. 本节讨论构造版本局部引理在计数与采样中的应用.

2017 年, 郭珩等 [56] 证明了在相关的坏事件互斥这一 "极端" 情况下, 算法 1 输出的不仅仅是问题的解, 还是对问题的解的随机均匀采样. 基于算法 1, 郭珩等提出了一种新的采样算法, 即部分拒绝性采样, 得到了该算法在 "极端" 情况下精确的期望运行时间, 并将其应用到了 k-SAT 和独立集的采样. 后来, 郭珩和 Jerrum [57] 又基于对部分拒绝性采样运行时间的分析, 找到了网络所有终端可靠性问题 (all-terminal network reliability) 的第一个完全多项式时间随机近似框架 (fully polynomial-time randomized approximation scheme). 之后, 郭珩和何昆 [58] 进一步扩展了相关结果, 得到了一系列 popping 算法精确的期望运行时间. 郭珩和 Jerrum [59] 还将相关技术应用到了有向环拟阵的计数.

2017 年, 结合构造版本局部引理, Moitra [24] 提出了一种新的算法框架, 对合取范式的可行解进行计数和采样. 2019 年, 凤维明等 [60] 利用局部引理, 绕开了传统马尔可夫链无法对不连通的样本空间进行采样的障碍, 从而改进了 Moitra 的结果. 郭珩等 [61] 还将相关算法框架推广到了超图染色的计数和采样. 最近, Galanis 等 [62] 又将相关算法框架推广到了随机 k-SAT 解的计数.

这里, 我们还是以 SAT 问题为例, 来看看局部引理在计数与采样上的应用.

定理20 [24] 令 Φ 为一个关于 n 个变量的合取范式, 其每个子句包含 k 到 $2k$ 个文字, 并且每个变量最多被 d 个子句共用. 如果 $k\geqslant 60\log d$, 则存在着一个确定性的多项式算法对 Φ 可满足的赋值

表 2　不同晶格的临界阈值 [34]

Table 2　Summary of the critical thresholds for various lattices [34]

Lattice	Quantum	Lower bound of the difference (between the classical and quantum thresholds)
Triangular	$\frac{5\sqrt{5}-11}{2}$ [10, 67, 68]	6.199×10^{-8}
Square	0.1193 [10, 69]	5.943×10^{-8}
Hexagonal	0.1547 [10]	1.211×10^{-7}
Simple cubic	0.0744 [67]	9.533×10^{-10}

进行近似计数, 其误差不超过真实值的 $1/n^c$. 且存在着一个随机的多项式时间算法对 Φ 可满足的赋值进行近似采样, 采样的分布与真实分布的总变化距离 (total variation distance) 不超过 $1/n^c$.

在一定的计算复杂性假设下, 定理 20 中 k 和 d 的关系在量阶上是紧的, 因为可以证明如下定理.

定理21 [63]　令 Φ 为一个关于 n 个变量的合取范式, 其每个子句包含 k 到 $2k$ 个文字, 并且每个变量最多被 d 个子句共用. 如果 $k \leqslant 2\log d - O(1)$, 则以 $1/n^c$ 的误差对 Φ 可满足的赋值进行近似计数和采样都是 NP- 难的.

6.3　量子版本的构造算法及其在求解 QSAT 上的应用

Ambainis 等 [33] 提出了量子版本局部引理之后, 人们试图给出量子版本局部引理的构造算法. 有一系列工作研究给定对易的局域哈密尔顿量, 如何高效地制备一个无忧的量子态 [64~66]. 2017 年, Gilyén 和 Sattath [38] 设计了一个适用于一般的局域哈密尔顿量的量子重采样算法. 在局域哈密尔顿量的一致差异足够大, 且其相对维度向量落在 Shearer 界之内时, 该算法可以高效地制备一个无忧的量子态. 该算法的一个直接应用就是求解落在 Shearer 界之内的 QSAT 实例.

7　经典变量与量子的能力差异及晶格的临界阈值

如第 4.1 和 5.2 小节所述, Shearer 界对量子版本局部引理是紧的, 而变量版本局部引理紧的条件超出了 Shearer 界. 这从局部引理角度展现了量子和经典的能力差异. 相比于任意的图, 物理学家们更关心无限大的图, 尤其是晶格. 本节将比较晶格上局域哈密尔顿量无忧的临界阈值和由变量生成的事件系统的临界阈值, 以研究晶格上量子和经典的能力差异.

晶格上硬核晶格气模型配分函数的第 1 个负的逸度零点恰好是其硬核奇点 (hard-core singularity). 如第 5.2 小节所述, 该零点恰好也是局域哈密尔顿量无忧的临界阈值的相反数. 因此, 我们可以由统计物理中反复研究过的硬核奇点直接得到局域哈密尔顿量无忧的临界阈值. 接下来, 我们考虑晶格上由变量生成的事件系统的临界阈值. 虽然我们已经知道变量版本局部引理紧的条件, 即定理 9, 但定理 9 中的数学规划很难求解, 要直接计算晶格上变量版本的临界阈值是非常困难的. 2019 年, 何昆等 [34] 考虑了晶格上的事件系统. 他们借助变量版本、量子版本以及 Lopsided 版本局部引理紧的条件, 即定理 9, 14 和 7, 给出了事件系统与局域哈密尔顿量临界阈值之差的下界, 见表 2 [10, 34, 67~69]. 在表 2 中, 晶格上的点表示局域哈密尔顿量或者经典的事件, 边表示 qudit 或者变量. 相关结果展现了晶格上量子和经典的能力差异, 同时, 也首次给出了在无穷大的图上变量版本紧的条件超出 Shearer 界的例子.

8 总结与展望

洛瓦兹局部引理是最重要的概率方法之一, 是组合数学和理论计算机中的重要工具. 除了抽象版本局部引理之外, 局部引理还有很多其他的变种, 比如 Lopsided 版本以及近年来发现的变量版本、量子版本和构造版本局部引理. 本文主要以 SAT 问题和 QSAT 问题为例, 介绍了这些不同版本的局部引理的应用, 包括 SAT 问题是否有解、如何快速找到 SAT 问题的解、如何对 SAT 问题的解进行计数和采样、QSAT 问题是否有解以及如何快速找到 QSAT 问题的解. 在这些应用中, 由局部引理得到的界要么渐进意义上是紧的, 要么量阶是紧的. 利用局部引理还可以给出一些晶格上事件系统与局域哈密尔顿量临界阈值之差的下界.

对于很多版本的局部引理, 如抽象版本、Lopsided 版本、变量版本和量子版本, 人们已经知道其紧的条件. 其中, Shearer 界对抽象版本、Lopsided 版本和量子版本局部引理都是紧的, 这将统计物理中硬核晶格气模型的配分函数、量子物理中局域哈密尔顿量无忧的临界阈值和洛瓦兹局部引理联系了起来. 而变量版本局部引理紧的条件可以超出 Shearer 界, 这从局部引理角度展现了量子与经典的能力差异.

构造版本局部引理是当前局部引理领域研究的热点. 扩展构造版本局部引理的应用范围以及构造版本局部引理的并行化和去随机化是未来重要的研究方向. 关于构造版本的一个重要的开放问题是, 重采样算法是否在变量版本局部引理的范围内都收敛. 求解这一问题, 将为重采样算法及相关算法的分析提供新的工具.

参考文献

1 Erdös P, Lovász L. Problems and results on 3-chromatic hypergraphs and some related questions. Infinite Finite Sets, 1975, 10: 609–627
2 Alon N, Spencer J H. The Probabilistic Method. 4th ed. Hoboken: John Wiley & Sons, 2016
3 Szegedy M. The Lovász Local Lemma – a survey. In: Proceedings of International Computer Science Symposium in Russia, Berlin, 2013. 1–11
4 Spencer J. Asymptotic lower bounds for Ramsey functions. Discrete Math, 1977, 20: 69–76
5 Shearer J B. On a problem of spencer. Combinatorica, 1985, 5: 241–245
6 Gebauer H, Szabó T, Tardos G. The local lemma is asymptotically tight for SAT. J ACM, 2016, 63: 43
7 Mcdiarmid C. Hypergraph colouring and the Lovász Local Lemma. Discrete Math, 1997, 167: 481–486
8 Wood D W. The exact location of partition function zeros, a new method for statistical mechanics. J Phys A-Math Gen, 1985, 18: L917–L921
9 Guttmann A J. Comment on 'The exact location of partition function zeros, a new method for statistical mechanics'. J Phys A-Math Gen, 1987, 20: 511–512
10 Todo S. Transfer-matrix study of negative-fugacity singularity of hard-core lattice gas. Int J Mod Phys C, 1999, 10: 517–529
11 Scott A D, Sokal A D. On dependency graphs and the lattice gas. Combin Probab Comput, 2006, 15: 253–279
12 Bissacot R, Fernández R, Procacci A, et al. An improvement of the Lovász Local Lemma via cluster expansion. Combinator Probab Comp, 2011, 20: 709–719
13 Harvey N J, Srivastava P, Vondrák J. Computing the independence polynomial: from the tree threshold down to the roots. In: Proceedings of the 29th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), New Orleans, 2018. 1557–1576
14 Bezáková I, Galanis A, Goldberg L A, et al. Inapproximability of the independent set polynomial in the complex plane. In: Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing (STOC), Los Angeles, 2018. 1234–1240

15 Kolipaka K, Szegedy M, Xu Y. A sharper local lemma with improved applications. In: Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques. Berlin: Springer, 2012. 603–614
16 Erdős P, Spencer J. Lopsided Lovász Local Lemma and Latin transversals. Discrete Appl Math, 1991, 30: 151–154
17 Harris D G, Srinivasan A. A constructive Lovász Local Lemma for permutations. Theory Comput, 2017, 13: 1–41
18 Szabó S. Transversals of rectangular arrays. Acta Math Univ Comenianae, 2008, 77: 279
19 BÖttcher J, Kohayakawa Y, Procacci A. Properly coloured copies and rainbow copies of large graphs with small maximum degree. Random Struct Algorithms, 2012, 40: 425–436
20 Mohr A T. Applications of the lopsided Lovász Local Lemma regarding hypergraphs. Dissertation for Ph.D. Degree. Carolina: University of South Carolina, 2013
21 Keevash P, Ku C Y. A random construction for permutation codes and the covering radius. Des Codes Crypt, 2006, 41: 79–86
22 Lu L, Mohr A, Székely L. Quest for negative dependency graphs. In: Recent Advances in Harmonic Analysis and Applications. Berlin: Springer, 2012. 243–258
23 Gebauer H, Moser R A, Scheder D, et al. The Lovász Local Lemma and satisfiability. In: Efficient Algorithms. Berlin: Springer, 2009. 30–54
24 Moitra A. Approximate counting, the Lovász Local Lemma, and inference in graphical models. J ACM, 2019, 66: 10
25 Giotis I, Kirousis L, Psaromiligkos K I, et al. Acyclic edge coloring through the Lovász Local Lemma. Theor Comput Sci, 2017, 665: 40–50
26 Moser R A. A constructive proof of the Lovász Local Lemma. In: Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC), Bethesda, 2009. 343–350
27 Moser R A, Tardos G. A constructive proof of the general Lovász Local Lemma. J ACM, 2010, 57: 11
28 Kolipaka K B R, Szegedy M. Moser and Tardos meet Lovász. In: Proceedings of the 43rd Annual ACM Symposium on Theory of Computing (STOC), California, 2011. 235–244
29 He K, Li L, Liu X, et al. Variable-version Lovász Local Lemma: beyond shearer's bound. In: Proceedings of the 58th IEEE Annual Symposium on Foundations of Computer Science (FOCS), Berkeley, 2017. 451–462
30 Rokhsar D S, Kivelson S A. Superconductivity and the quantum hard-core dimer gas. Phys Rev Lett, 1988, 61: 2376–2379
31 Castelnovo C, Chamon C, Mudry C, et al. From quantum mechanics to classical statistical physics: generalized Rokhsar-Kivelson Hamiltonians and the "stochastic matrix form" decomposition. Ann Phys, 2005, 318: 316–344
32 Bravyi S. Efficient algorithm for a quantum analogue of 2-sat. Contemp Math, 2011, 536: 33–48
33 Ambainis A, Kempe J, Sattath O. A quantum Lovász Local Lemma. J ACM, 2012, 59: 24
34 He K, Li Q, Sun X, et al. Quantum Lovász Local Lemma: Shearer's bound is tight. In: Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing (STOC), Phoenix, 2019. 461–472
35 Laumann C R, Läuchli A M, Moessner R, et al. On product, generic and random generic quantum satisfiability. Phys Rev A, 2010, 81: 359–366
36 Sattath O, Morampudi S C, Laumann C R, et al. When a local Hamiltonian must be frustration-free. Proc Natl Acad Sci USA, 2016, 113: 6433–6437
37 Laumann C, Moessner R, Scardicchio A, et al. Phase transitions in random quantum satisfiability. Bull Am Phys Soc, 2009, 54
38 Gilyén A, Sattath O. On preparing ground states of gapped hamiltonians: an efficient quantum Lovász Local Lemma. In: Proceedings of the 58th IEEE Annual Symposium on Foundations of Computer Science (FOCS), Berkeley, 2017. 439–450
39 Beck J. An algorithmic approach to the Lovász Local Lemma. Random Struct Algor, 1991, 2: 343–365
40 Czumaj A, Scheideler C. A new algorithm approach to the general Lovász Local Lemma with applications to scheduling and satisfiability problems. In: Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (STOC), Portland, 2000. 38–47
41 Molloy M, Reed B. Further algorithmic aspects of the local lemma. In: Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC), Dallas, 1998. 524–529
42 Radhakrishnan J, Srinivasan A. Improved bounds and algorithms for hypergraph 2-coloring. Random Struct Algor, 2000, 16: 4–32

43 Salavatipour M R. A $(1+\epsilon)$-approximation algorithm for partitioning hypergraphs using a new algorithmic version of the Lovász Local Lemma. Random Struct Algor, 2004, 25: 68–90

44 Messner J, Thierauf T. A Kolmogorov complexity proof of the Lovász Local Lemma for satisfiability. Theor Comput Sci, 2012, 461: 55–64

45 Catarata J D, Corbett S, Stern H, et al. The Moser-Tardos resample algorithm: where is the limit? (an experimental inquiry). In: Proceedings of the 19th Workshop on Algorithm Engineering and Experiments (ALENEX), Barcelona, 2017. 159–171

46 Harvey N J, Vondrák J. An algorithmic proof of the Lovász Local Lemma via resampling oracles. In: Proceedings of the 56th Annual Symposium on Foundations of Computer Science (FOCS), Berkeley, 2015. 1327–1346

47 Achlioptas D, Iliopoulos F. Random walks that find perfect objects and the Lovász Local Lemma. J ACM, 2016, 63: 22

48 Achlioptas D, Iliopoulos F. Focused stochastic local search and the Lovász Local Lemma. In: Proceedings of the 27th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), Arlington, 2016. 2024–2038

49 Achlioptas D, Iliopoulos F, Kolmogorov V. A local lemma for focused stochastic algorithms. ArXiv: 1809.01537

50 Kolmogorov V. Commutativity in the algorithmic Lovász Local Lemma. SIAM J Comput, 2018, 47: 2029–2056

51 Achlioptas D, Iliopoulos F, Sinclair A. Beyond the Lovász Local Lemma: point to set correlations and their algorithmic applications. In: Proceedings of IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS), Baltimore, 2019. 725–744

52 Harris D G. Deterministic parallel algorithms for fooling polylogarithmic Juntas and the Lovász Local Lemma. ACM Trans Algor, 2018, 14: 47

53 Chandrasekaran K, Goyal N, Haeupler B. Deterministic algorithms for the Lovász Local Lemma. SIAM J Comput, 2013, 42: 2132–2155

54 Haeupler B, Harris D G. Parallel algorithms and concentration bounds for the Lovász Local Lemma via witness dags. ACM Trans Algor, 2017, 13: 53

55 Harris D G. Deterministic algorithms for the Lovász Local Lemma: simpler, more general, and more parallel. 2019. ArXiv: 1909.08065

56 Guo H, Jerrum M, Liu J. Uniform sampling through the Lovász Local Lemma. J ACM, 2019, 66: 18

57 Guo H, Jerrum M. A polynomial-time approximation algorithm for all-terminal network reliability. SIAM J Comput, 2019, 48: 964–978

58 Guo H, He K. Tight bounds for popping algorithms. 2018. ArXiv: 1807.01680

59 Guo H, Jerrum M. Approximately counting bases of bicircular matroids. 2020. ArXiv: 1808.09548

60 Feng W, Guo H, Yin Y, et al. Fast sampling and counting k-sat solutions in the local lemma regime. 2019. ArXiv: 1911.01319

61 Guo H, Liao C, Lu P, et al. Counting hypergraph colorings in the local lemma regime. SIAM J Comput, 2019, 48: 1397–1424

62 Galanis A, Goldberg L A, Guo H, et al. Counting solutions to random cnf formulas. 2020. ArXiv: 1911.07020

63 Bezáková I, Galanis A, Goldberg L A, et al. Approximation via correlation decay when strong spatial mixing fails. SIAM J Comput, 2019, 48: 279–349

64 Cubitt T S, Schwarz M. A constructive commutative quantum Lovász Local Lemma, and beyond. 2011. ArXiv: 1112.1413

65 Schwarz M, Cubitt T S, Verstraete F. An information-theoretic proof of the constructive commutative quantum Lovász Local Lemma. 2013. ArXiv:1311.6474

66 Sattath O, Arad I. A constructive quantum Lovász Local Lemma for commuting projectors. Quantum Inf Comput, 2015, 15: 987–996

67 Gaunt D S. Hard-sphere lattice gases. II. plane-traingular and three-dimensional lattices. J Chem Phys, 1967, 46: 3237–3259

68 Baxter R J. Hard hexagons: exact solution. J Phys A-Math Gen, 1980, 13: 61–70

69 Gaunt D S, Fisher M E. Hard-sphere lattice gases. I. plane-square lattice. J Chem Phys, 1965, 43: 2840–2863

New versions of Lovász Local Lemma and their applications

Kun HE[1,2*] & Xiaoming SUN[3,4]

1. *School of Computer and Software, Shenzhen University, Shenzhen* 518061*, China*;
2. *Shenzhen Institute of Computing Sciences, Shenzhen* 518109*, China*;
3. *Institute of Computing Technology, Chinese Academy of Sciences, Beijing* 100190*, China*;
4. *University of Chinese Academy of Sciences, Beijing* 100049*, China*
* Corresponding author. E-mail: hekun.threebody@foxmail.com

Abstract Lovász Local Lemma (LLL) is an important tool in combinatorics and probability theory. It can be used to show the existence of combinatorial objects meeting a collection of criteria as long as the criteria are weakly dependent. It was first proposed by Erdős and Lovász in 1975. Since then, many applications of LLL have been found in combinatorics, theoretical computer science, and physics. Recently, several new versions of LLL have been proposed. Constructive LLL is an especially big breakthrough in theoretical computer science that has attracted lots of attention. In this paper, we will review recent progress in LLL research, including new versions of LLL and their applications. We will precisely define and differentiate among abstract LLL, lopsided LLL, variable LLL, and quantum LLL. We will also provide connections between abstract LLL and statistical physics, as well as between quantum LLL and quantum physics. LLL can be used to prove the existence of solutions, find solutions efficiently, count the number of solutions, and sample a solution uniformly at random. We will also illustrate these applications of LLL with the SAT problem and the quantum SAT problem.

Keywords Lovász Local Lemma, variable LLL, quantum LLL, constructive LLL, Shearer's bound

Kun HE received his Ph.D. degree from the Institute of Computing Technology, Chinese Academy of Sciences in 2019. He is currently a postdoctoral researcher at Shenzhen University. His research interests lie in theoretical computer science, with an emphasis on probabilistic methods and sampling.

Xiaoming SUN received his B.S. and Ph.D. degrees in Computer Science from Tsinghua University, Beijing, China, in 2001 and 2005, respectively. Currently he is a professor at the Institute of Computing Technology, Chinese Academy of Sciences. His current research interests include quantum computing, decision tree complexity, and computational complexity.