arXiv:2601.02811v1 [math.ST] 6 Jan 2026

网络模型的决策理论稳健性

Marios Papamichalis* Regina Ruane† Sim´on Lunag´omez‡ Swati Chandna§

2026年1月7日

摘要

神经科学、流行病学和社会科学中的网络数据，通常使用贝叶斯网络模型进行分析，例如 Erd˝os-R´enyi 图、随机区块模型、随机点积图和图子先验。在此类应用中，这些模型都只是近似，而真实网络往往稀疏且异质，并呈现任何单一模型设定都无法完全捕捉的高阶依赖关系。这引出了一个问题：当假定模型存在轻微设定错误时，基于网络的决策、模型选择、函数汇总和政策建议有多稳定？我们采用局部决策理论稳健性框架来回答这一问题：允许后验分布在一个较小的库尔贝克–莱布勒邻域内变化，并选择使最坏情况下的后验期望损失最小的动作。该框架在可交换网络模型中的专门应用，得益于低维网络泛函的存在。首先，我们借助图子极限，将决策理论稳健性拓展至可交换图，并推导出稳健后验风险的精确小半径展开。对于平方损失，我们证明，主导的膨胀项由损失的后验方差控制。对于在渗流和碎裂阈值处发散的稳健性指标，我们得到一个普适临界指数，用以描述临界性附近决策层面不确定性如何急剧增大。其次，我们针对稀疏 Erd˝os– R´enyi 模型与随机块模型之间的决策论稳健模型选择，建立了非参数极小极大理论。对于配置模型和稀疏图子类中的渗流型稳健性泛函，结果表明，在这些类别上，无论是贝叶斯方法还是频率学派方法，都无法统一地改进由此得到的决策理论鲁棒性误差指数。第三，我们提出一种实用的稳健网络分析算法，该算法基于对后验样本或变分样本进行熵倾斜，并展示其在功能性脑连接和卡纳塔克邦村庄社会网络分析中的应用。综上，这些结果为贝叶斯网络分析提供了一种决策论稳健性概念，补充了经典的网络对象层面韧性概念。

1 引言

网络数据来源广泛，涵盖功能性脑连接、传染病传播、村庄社会网络以及在线平台等。贝叶斯网络模型已成为分析此类数据的核心工具，为学习潜在结构、比较相互竞争的表示形式，以及将不确定性传播至预测和政策决策提供了一个统一框架。常见选择包括 Erd˝os–R´enyi（Erdős–Rényi模型）图、

*Human Nature Lab，耶鲁大学，纽黑克，CT 06511，marios.papamichalis@yale.edu
†统计与数据科学系，宾夕法尼亚大学沃顿商学院，3733 Spruce Street，费城，PA 19104-6340，ruanej@wharton.upenn.edu
‡统计系，ITAM，墨西哥，simon.lunagomez@itam.mx§伦敦大学伯贝克学院，s.chandna@bbk.ac.uk

随机块模型（随机块模型）、潜在空间模型和随机点积图模型，以及非参数图子先验。

在实践中，这些模型都只是近似。经验网络通常较为稀疏且高度异质，任何单一设定都只能部分刻画其中的社区、枢纽节点、度变异性和高阶依赖。然而，在进行模型选择时，选择社区表示还是潜在空间表示，意味着要根据干预的预期影响对其排序，或比较不同网络的稳健性指标。通常，人们会报告这些结果，却没有系统评估其对模型设定错误的敏感性。本文的核心问题是：

当假定的贝叶斯网络模型仅近似正确时，基于网络的决策质量会如何下降？

我们采用Watson和Holmes [2016]提出的局部决策论稳健性框架来回答这一问题。在这一视角下，贝叶斯分析被表述为一个决策问题：选择动作以最小化后验期望损失，并通过允许后验分布在工作模型的一个小Kullback–Leibler（KL）（或更一般的 ϕ–散度）邻域内移动来评估稳健性。随后，对该邻域内的最坏情形后验风险进行评估 [Watson和Holmes, 2016, Watson 等人，2017]。风险的增幅量化了贝叶斯决策对似然或先验分布的局部模型设定错误有多脆弱。这一方法拓展了稳健贝叶斯分析中的经典思想，例如 Γ–极小极大规则和ε–污染 [Berger和Berliner, 1986, Vidakovic，2000], ，并且与经济学中对模糊厌恶偏好的变分表示 [Maccheroni et al., 2006, Hansen and Sargent，2008]以及近期为缓解模型设定错误而对后验分布进行温度调整或粗化的提议 [Miller and Dunson, 2019, Avella Medina et al.，2022]密切相关。我们的目标是将这种决策层面的稳健性视角引入可交换网络模型，并将其与图极限理论以及基于渗流和韧性的经典网络稳健性概念联系起来。

对象层面与决策层面的鲁棒性。 网络科学领域的大量文献讨论了如何通过扰动图本身来研究对象层面的鲁棒性。针对随机图模型的渗流分析量化了移除节点或边时巨型连通分量如何崩溃。Callaway等人 [2000] 和Cohen等人 [2000]证明，Erdős–Rényi模型网络在相对有限的随机故障下就可能失去全局连通性，而具有重尾度分布的网络（如无标度网络或配置模型）则表现出显著的韧性。研究者还利用配置模型中的标度极限和临界指数进一步完善了这些结果 [Janssen等人，2014年，van der Hofstad，2017]。近期综述强调，此类现象在各个领域普遍存在[Artime等人，2024年，Kawasumi和Hasegawa，2024]。一些变体研究了结构化或对抗性扰动，包括重尾空间网络；即使在任意节点移除的情况下，这类网络也可能保留巨型连通分量 [Jacob和M¨orters，2017], 以及优先连接网络；在考虑度基线后，这类网络即使遭受定向攻击，仍可能保持连通[Hasheminezhad和Brandes，2023]。

另一条互补的研究路线探讨了推断程序对观测图扰动的鲁棒性。例如，当潜在的随机块模型受到几何随机图或其他边扰动的破坏时，谱社区检测的稳定性 [P´ech´和

Perchet，2020年，Stephan和Massouli´e， 2019], 以及在部分节点或边遭到对抗性破坏时估计图参数的极小极大速率 [Acharya等人， 2023]。这些研究成果量化了结构噪声或对抗性修改邻接矩阵如何影响网络拓扑或特定算法。

相比之下，我们关注的是决策层面的贝叶斯意义上的鲁棒性。我们不对观测图进行调整，而是研究模型参数的后验分布，以及由此得出的决策或预测，如何响应与假定数据生成机制之间的微小偏差。这一视角可追溯至Wald决策理论 [Wald、 1950] 以及稳健贝叶斯表述；这类表述旨在寻找在某个假定模型的邻域内表现良好的程序[Berger和Berliner，1986年、Vidakovic、 2000]。在此，我们将Watson和Holmes [2016] 提出的决策论稳健性框架专门应用于网络模型，并将其与图极限理论相结合；后者通过图子表示节点可交换随机图 [Diaconis和Janson，2009年、Lov´asz、2012年、Aldous、 1981]。这种表示方法使我们能够在网络生成分布空间中构造局部KL邻域，并研究后验扰动如何传递至我们感兴趣的网络汇总量。

网络泛函、临界行为与决策层面不确定性。在许多应用中，研究对象并非完整网络或其参数向量，而是一个低维网络泛函，用于概括某些行为特征。例如，图子上的易感者–感染者–易感者（SIS）动力学中的流行病阈值和稳态感染流行率[Vizuete等人， 2020]；基于节点移除时最大连通分量规模构造的基于渗流的稳健性指标 [Callaway等人，2000年，Artime等人， 2024]；以及决定网络上扩散与共识动力学的谱量，例如代数连通度和共识相干性 [Zhang等人， 2017]。这些情境的一个共同特征是存在临界阈值——渗流阈值或再生阈值——在这些阈值处，网络的连通性或动力学行为会发生定性变化。接近此类阈值时，稳健性指标往往会发散，并对模型参数的微小变化变得极其敏感。

我们的首要目标是理解，这些泛函中的决策层面不确定性在后验分布的局部决策论稳健性扰动下如何变化。对于一大类碎裂型指标，包括易感性、Erdős–Rényi模型和配置模型中的基于最大连通分量的指标，我们证明稳健后验风险存在精确的小半径展开。对于平方损失，半径为 C 的KL球上的最坏情况风险在一阶近似下按 C的平方根增长，其系数由损失的后验方差决定。此外，当底层网络趋近渗流或碎裂阈值时，稳健风险的主导项以普适临界指数发散：决策层面不确定性按距临界点的距离的逆函数的四次方膨胀，增幅比泛函本身更为剧烈。这将随机图中的经典相变 [van derHofstad， 2017]与关于基于网络的决策脆弱性的定量结论联系起来。

我们的第二个目标是刻画在相互竞争的网络模型中进行决策论稳健模型选择的基本极限。我们关注稀疏 ER 图与双块随机块模型之间的比较，既考察带标签形式，也考察其稀疏图子表示。对于这一双点实验，我们推导出显式的逐顶点 Kullback–Leibler 和切尔诺夫信息指标 $I(\lambda)$及 $J(\lambda)$，其中 λ是信噪参数，并证明 $J(\lambda)$起到决策论稳健性“

噪声指标”的作用，它决定了稳健贝叶斯因子检验。接着，我们将这对模型嵌入稀疏图的广泛非参数类中，包括配置模型和稀疏图子，并证明，无论是估计量还是经过稳健化的模型后验分布，都无法在这些类上统一实现优于 $J(\lambda)$的决策论稳健性错误指数。对于配置模型中近临界的基于渗流的稳健性指标，也存在类似的极小极大现象。因此，我们所识别的决策理论鲁棒性指数是底层网络问题固有的，而非特定建模选择所造成的假象。

在计算方面，我们将决策论稳健性视为一个模块化层，构建在给定网络模型的现有近似后验之上。实践中，我们使用随机块模型和随机点积图的变分后验、基于谱嵌入或度矩等方法得到的谱伪后验或基于矩的伪后验；对于较小的图，则使用传统的马尔可夫链蒙特卡罗采样器。随后，通过对后验抽样或变分抽样进行熵倾斜来求解 KL 散度球优化问题，并在权重空间中采用镜像下降对抗算法，以处理更一般的 ϕ 散度球。这些方法只需能够在后验抽样上评估损失，且只会给现有推断流程带来适度的额外开销。

我们通过两个实质性案例来展示这一方法。在一个功能性脑连接网络中，我们比较社团表示与潜在空间表示，并评估基于连通性的摘要统计量的决策论稳健性。在来自卡纳塔克邦村庄的社交网络中，我们重新审视了Banerjee 等人开展的实验。 [2013]并研究在对不同网络模型和先验分布施加决策论稳健性扰动后，关于扩散路径和干预目标选择的结论如何变化。在这两个案例中，敏感性分析显示，当看似有力的网络结论依赖于脆弱的建模假设时，决策论稳健性便显得尤为重要。

本文通过图子极限，将可交换网络模型的决策论稳健贝叶斯决策形式化，并推导出稳健后验风险在小半径下的精确展开。此外，本文还识别了碎裂阈值附近渗流型稳健性指标的普适临界指数；针对稀疏 ER 图与随机块模型之间的决策论稳健模型选择，以及配置模型和稀疏图子图类中的稳健性泛函，发展了完整的非参数极小极大理论；确立了相关决策论稳健性噪声指数的最优性；并提出了一种稳健网络分析的计算策略，该策略基于对后验分布样本和变分样本进行熵倾斜，并针对一般 ϕ散度球采用镜像下降对抗算法。我们展示了该策略在脑连接网络以及 Banerjee 等人研究的卡纳塔克邦村庄社会网络中的应用。Banerjee 等人 [2013]。

本文其余部分安排如下。第2 节回顾可交换随机图、图子以及示例中使用的贝叶斯网络模型。第3.1 节构建网络泛函的一般决策论稳健性理论，并确立碎裂型指标的临界指数。第4 节介绍稀疏 ER 图与随机块模型的非参数决策论稳健性极小极大理论；第5 节研究配置模型和基于渗流的稳健性指标。第6 节介绍基于熵倾斜和镜像下降的计算方案。第7节报告关于功能性脑连接和卡纳塔克邦村庄网络的实证研究。第8 节讨论其影响及未来工作的方向。

2 背景与设定

本节回顾全文所用的可交换网络框架，具体介绍我们如何围绕工作模型构造 Kullback–Leibler（KL）邻域，并概述用于决策论稳健性分析的贝叶斯网络模型和后验近似。

2.1 可交换网络模型与图极限

设 G_n 是顶点集 $[n] = \{1, \ldots, n\}$ 上的简单无向图，其邻接矩阵为 $A^{(n)} = (A_{ij})_{1 \le i,\ j \le n}$。若对每个 n 以及 $[n]$ 的每个置换 σ，均有……，则称 $(G_n)_{n \ge 1}$（或 $(A^{(n)})_{n \ge 1}$）是节点可交换的。

$$\left(A_{ij}^{(n)}\right)_{1 \le i < j \le n} \overset{d}{=} \left(A_{\sigma(i)\sigma(j)}^{(n)}\right)_{1 \le i < j \le n}.$$

根据 Aldous–Hoover表示，任何这样的稠密节点可交换序列都可以（在保测变换意义下）表示为一个图子 $W:\ [0,1]^2 \to [0,1]$，以及相互独立同分布的潜在位置 $U_1,\ U_2,\ \cdots \sim$，服从 $\mathrm{Unif}[0,1]$:

$$A_{ij} \,\big|\, U_{1:n} \ \sim\ \mathrm{Bernoulli}\big(W(U_i, U_j)\big), \qquad 1 \le i < j \le n, \tag{1}$$

在无序对 $(i,\ j)$ 上相互独立，其中 $U_{1:n} = (U_1,\ \ldots\ldots,\ U_n)$。许多常见的稠密模型都有自然的graphon表示:

- Erd˝os–R´enyi（Erdős–Rényi模型）图，其中 $W(x,\ y) \equiv p$ 为常数;
- 随机区块模型（随机块模型），其中 W 是在 $[0,1]$有限划分上的阶梯函数;
- 具有有界潜在位置的随机点积图（随机点积图），其中 $W(x,\ y) = \langle \xi(x),\ \xi(y) \rangle$ 对应于潜在特征映射 ξ。

反过来，任意图子 W 都可以用阶梯函数在割范数下近似，因此随机块模型构成了一个便于理论研究和计算的有限维近似类。

图子KL邻域。对于图子 W 和固定的 n，令 $\mathcal{G}(W$表示由 G_n根据（1）生成的分布。给定一个工作图子 $W^\star$及其对应的图分布 $\mathcal{G}^\star :\ = \mathcal{G}(W^\star)$，在对象层面考虑KL球是自然的

$$\Gamma_C(\mathcal{G}^\star) := \big\{ \mathcal{G}(W) : \mathrm{KL}\big(\mathcal{G}(W) \,\|\, \mathcal{G}^\star\big) \le C \big\}, \qquad C > 0, \tag{2}$$

其中，散度是对大小为 n的邻接矩阵诱导分布计算的。在稠密模拟中，我们使用（2）来可视化拟合模型的局部邻域，并探究图子层面的扰动如何传递到网络泛函。

在实践中，我们用固定网格上的阶梯函数随机块模型来近似 $W^\star$ 和候选 W。将 $[0,1]$ 划分为 K 个区间，并将每个区间视为一个块，再用块均值矩阵替代 W。由此得到有限维参数化 $P \in [0,1]^{K \times K}$，以及定义在 $[n]$上的相应随机图分布。随后可以通过对潜在位置进行蒙特卡洛抽样，估计 KL 散度 $\mathrm{KL}(\mathcal{G}(W) \,\|\, \mathcal{G}^\star)$:

$$\mathrm{KL}\big(\mathcal{G}(W) \,\|\, \mathcal{G}(W^\star)\big) \approx \frac{1}{M} \sum_{m=1}^{M} \sum_{1 \le i < j \le n} \mathrm{kl}\Big(W\big(U_i^{(m)}, U_j^{(m)}\big), W^\star\big(U_i^{(m)}, U_j^{(m)}\big) \Big),$$

其中，($U_1^{(m)}$、……、$U_{(m)n}$) 是来自 Unif$[0,1]$ 的独立同分布抽样。等价地，在连续层面上，也可以使用单位边图子图散度

$$\mathrm{KL}(W\|W^\star) := \int_{[0,1]^2} \mathrm{kl}\big(W(x,y), W^\star(x,y)\big)\,\mathrm{d}x\,\mathrm{d}y, \tag{3}$$

其中，kl(p，q) 表示伯努利 Kullback–Leibler 散度。

KL 球内的局部扰动。研究拟合的稠密模型在对象层面 的鲁棒性时，在球内生成邻近的可交换图子是一种有效方法 $\Gamma_C(\mathcal{G}^\star)$。对于随机块模型和随机点积图的阶梯图子图近似，将区块边概率集合视为定义在 K^2 个单元上的单个概率向量，并通过狄利克雷（广义贝叶斯自助法）抽样和简单的重缩放移动来扰动该向量，会更为方便。

形式上，这些扰动会在$\Gamma_C(\mathcal{G}^\star)$ 内的 K区块随机块模型空间上诱导出一条马尔可夫链。在补充材料中，我们证明:

- 狄利克雷扰动与工作模型之间的期望 KL 散度具有简单的闭式解（命题 S.1）；并且
- 诱导出的马尔可夫链在 KL 球内部是 ψ不可约且非周期的，因此，KL 球 $\Gamma_C(\mathcal{G}^\star)$内的任意可交换阶梯图子模型都以正概率可达（定理 S.1）。

这些结果仅用于探索性稠密模拟；我们所有的决策层面的稳健性计算6则基于后验样本的熵倾斜以及在权重空间中的镜像下降。

在本文余下部分，我们主要对稠密节点可交换模型使用图子图表示，并将其作为定义和可视化工作模型局部邻域的便捷方式。对于稀疏网络，我们则使用显式的参数模型或非参数模型（稀疏 Erdős–Rényi 模型、随机块模型、配置模型、空间模型），并直接在其有限规模的n 概率律层面推导决策论稳健性性质。

2.2 网络的贝叶斯建模

现在简要介绍支撑我们的决策问题和决策论稳健性分析的贝叶斯网络模型。在所有情形中，参数 $\theta \in \Theta$ 索引一族随机图定律 $\{P_\theta^{(n)} : \theta \in \Theta\}$ 这些图有 n 个顶点 G_n，并且在 Θ上设定先验分布 Π。

参数模型。对于稀疏网络，我们考虑:

- 稀疏 *Erd˝os–R´enyi*（*ER*）模型，其中 $\theta = p_n$ 控制边概率（通常满足$p_n \asymp c/n$）；
- 随机区块模型（随机块模型），其参数为（π，B），分别表示块比例和区块内部/之间的边概率，既有带标签形式，也有无标签（图子）形式;
- 配置模型，由度分布 μ 参数化，为基于渗流的稳健性指标提供了一个灵活的基准。

对于稠密网络（例如第 7 节中的脑连通性示例），我们采用 Erdős–Rényi模型、随机块模型和低秩潜在位置模型，这些模型都具有 graphon表示。

非参数先验和图子先验。 为捕捉更多复杂结构，我们考虑图子上的非参数先验，例如随机块模型的有限或无限混合，以及基于平滑核的先验。这些先验定义在对称可测函数W构成的空间上：$[0,1]^2 \to [0,1]$并对保测变换取商，再通过（1）诱导出可交换随机图定律。在稀疏区域，我们按照Watson和Holmes [2016],Watson 等人 [2017]的做法，将这些先验与重缩放方案或度校正构造相结合。

基线后验分布与伪后验推断。 对于网络模型，精确的贝叶斯推断在中等或大型 n规模下通常难以实现，因此我们采用可扩展的近似方法：

- 适用于随机块模型、潜在空间模型和随机点积图的变分后验；
- 将谱估计量或矩估计法估计量置于伪贝叶斯框架中，其中近似似然与显式先验共同产生可处理的伪后验；
- 仅在小型网络中，使用传统的马尔可夫链蒙特卡罗采样器（吉布斯采样、HMC）作为基线比较。

在所有情况下，第3.1节和第6节中的决策论稳健性机制都将所得的后验分布或伪后验分布$\Pi_{0,\,n}(\cdot \mid G_n)$视为基线分布。稳健性通过允许$\Pi_{0,\,n}$在散度球内变化，并按照第6节所述，通过熵倾斜和镜像下降计算最坏情况下的后验风险来定义。

在此背景下，我们将转向网络泛函的一般决策论稳健性理论，以及支配其稳健后验风险的临界指数。

3 网络泛函的一般决策论稳健性理论

3.1 网络泛函的决策论稳健性

在许多网络应用中，最终决策取决于复杂随机图模型的低维泛函：例如流行病阈值、稳健性指数、共识相干性或谱间隙。决策论稳健性关注的是，当模型参数的后验分布发生微小的局部模型设定错误时，此类决策会受到多大影响，其中影响程度以 Kullback–Leibler（KL）散度衡量。遵循Watson和Holmes [2016],Watson 等人 [2017], 的做法，我们通过考察工作后验的 KL邻域内最坏情况下的后验期望损失，定义一种局部决策论稳健性准则。我们将其称为 决策论稳健性。

3.1.1 由网络泛函驱动的决策问题

设 $\Theta \subset \mathbb{R}^p$ 为一个参数空间，用于索引一族网络定律 $\{P_\theta^{(n)} : \theta \in \Theta\}$，这些网络定律定义在具有 n 个顶点的图 G_n上。典型示例如下：

- 稀疏或稠密的 Erd˝os–R´enyi 图以及随机块模型（SBM）；
- 具有预设度或社团结构的配置模型和图子；
- 几何图和空间无标度模型。

令 $R(\theta) \in \mathbb{R}$ 为一个感兴趣的网络泛函，例如：

- 图子上的极限 SIS 噪声指数 Vizuete等人 [2020];
- 一种基于渗流的稳健性指数（例如最大连通分量曲线下的面积），如Artime等人 [2024];
- 空间晶格或随机图上的渐近共识相干性 [Zhang等人， 2017]。

给定关于 Θ 的先验分布 Π 和观测图 $G_n \sim P_{\theta_0}^{(n)}$，令$\Pi_{0,\,n}(\cdot \mid G_n)$表示 θ上的一个（可能是伪）后验分布。对于平方损失 $L(a,\ \theta) = (a - R(\theta)),\ ^2$, 贝叶斯行动为

$$a_n^\star := \int R(\theta)\, \Pi_{0,n}(\mathrm{d}\theta),$$

其基准后验风险为

$$\rho_{0,n} := \int \big(a_n^\star - R(\theta)\big)^2\, \Pi_{0,n}(\mathrm{d}\theta) = \mathrm{Var}_{\Pi_{0,n}}\big(R(\theta)\big).$$

为了研究Watson和Holmes [2016], 意义下的局部模型设定错误，我们考虑后验KL球

$$\mathcal{U}_C\big(\Pi_{0,n}\big) := \big\{\widetilde{\Pi} : \mathrm{KL}\big(\widetilde{\Pi} \| \Pi_{0,n}\big) \le C\big\},$$

并定义相应的稳健后验风险

$$\rho_{\mathrm{rob},n}(C) := \sup_{\widetilde{\Pi} \in \mathcal{U}_C(\Pi_{0,n})} \int \big(a_n^\star - R(\theta)\big)^2\, \widetilde{\Pi}(\mathrm{d}\theta).$$

差值 $\rho_{\mathrm{rob},n}(C) - \rho_{0,n}$ 衡量在半径为 C 的局部后验KL扰动下，最坏情况下的后验期望损失可能膨胀的程度。

3.1.2 碎裂型指标的通用临界指数

网络中的许多鲁棒性和韧性指标会在碎裂阈值处发散，这通常由一个标量负载参数控制，例如分枝因子或谱半径。示例包括：

- 稀疏 Erdős–Rényi 模型或配置模型中的易感性或期望连通分量大小，例如[van derHofstad, 2017];
- 基于渗流的稳健性指标，这类指标根据节点移除后的最大连通分量构建，例如 [Artime等人, 2024];

我们将这种行为抽象如下。设 ρ: $\Theta \to \mathbb{R}$ 为一个光滑的负载参数 （例如有效分枝因子或谱半径），并定义距临界点的距离

$$\Delta(\theta) := 1 - \rho(\theta).$$

假设 3.1 （临界鲁棒性泛函）。 存在一个真实参数 $\theta_0 \in \Theta$、 θ_0 的邻域 $\mathcal{N}$、一个常数 $c_0 > 0$ 和一个函数 H: $\Theta \to \mathbb{R}$，使得：

1. $\Delta(\theta_0) = \Delta_0 > 0$ 和 $\nabla_\theta \rho(\theta_0) \neq 0$;
2. 对所有 $\theta \in \mathcal{N}$,

$$R(\theta) = \frac{c_0}{\Delta(\theta)} + H(\theta);$$

3. H 在 $\mathcal{N}$ 上是 C^2 且有界，并且当 $\Delta_0 \downarrow 0$ 时， $\|\nabla_\theta R(\theta_0)\| \asymp \Delta_0^{-2}$。

假设 3.1 描述了这样一种情形：当网络接近碎裂阈值时，鲁棒性泛函 $R(\theta)$ 按如下形式发散 $1/\Delta(\theta)$，其梯度则以如下形式急剧增大$\Delta(\theta)^{-2}$。

我们还假设后验分布具有局部伯恩斯坦–冯·米塞斯行为。

假设 3.2 （局部后验渐近）。 存在一个缩放因子 $r_n \downarrow 0$和一个正定矩阵 Σ，使得对于每个有界连续的 φ: $\mathbb{R}^p \to \mathbb{R}$,

$$\int \varphi\Big(\frac{\theta-\theta_0}{r_n}\Big)\,\Pi_{0,n}(\mathrm{d}\theta) \xrightarrow[n\to\infty]{P_{\theta_0}^{(n)}} \int \varphi(z)\,\phi_\Sigma(\mathrm{d}z),$$

其中， ϕ_Σ服从 $N(0,\ \Sigma)$ 分布。等价地，在 $\Pi_{0,\ n}$下，

$$\theta = \theta_0 + r_n Z_n, \qquad Z_n \Rightarrow Z \sim N(0,\Sigma)$$

依 $P_{\theta_0}^{(n)}$ –概率。

下　　该定理概述了此类稳健性指标临界指数的一般行为。

定理 3.3 (碎裂型指标的鲁棒临界指数)。 假设 *3.1*和 *3.2* 成立。设 $\Delta_0 := \Delta(\theta_0) > 0$ 表示真实网络到碎裂阈值的距离，并允许 $\Delta_0 = \Delta_0^{(n)} \downarrow 0$ 满足 $\Delta_0^{(n)} \gg r_n$ 当 $n \to \infty$时成立。此外，假设:

1. 假设 *3.1* 中的分解意味着 $\|\nabla_\theta R(\theta_0)\| \asymp \Delta_0^{-2}$当 $\Delta_0 \downarrow 0$时成立;

2. 在假设*3.2*下， Z_n 的概率律具有一致有界的二阶和四阶矩（关于 $P_{\theta_0}^{(n)}$ –概率）；

3. 定理 *S.2*中的指数矩条件对归一化损失$L_n/\rho_{0,n}$ 一致成立（因此，该定理中的 $o(\sqrt{C})$ 余项可以选取得对小的C在 n 上一致）。

于是:

1. 基准后验风险。 存在 $V_0 \in (0、\ \infty)$ 使得

$$\rho_{0,n} = \mathrm{Var}_{\Pi_{0,n}}\big(R(\theta)\big) = \frac{V_0\, r_n^2}{\Delta_0^4}\,\big(1 + o_{P_{\theta_0}^{(n)}}(1)\big). \tag{4}$$

特别地，当接近碎裂阈值时， $R(\theta)$ 的后验均方误差按 Δ_0^{-4} 的量级变化。

2. 急剧膨胀。 对于任意确定性序列 $\mathcal{C}_n \downarrow 0$,

$$\rho_{\mathrm{rob},n}(\mathcal{C}_n) = \rho_{0,n} + 2\,\rho_{0,n}\sqrt{\mathcal{C}_n} + o_{P_{\theta_0}^{(n)}}\big(\rho_{0,n}\sqrt{\mathcal{C}_n}\big). \tag{5}$$

等价地,

$$\frac{\rho_{\mathrm{rob},n}(\mathcal{C}_n) - \rho_{0,n}}{\rho_{0,n}\sqrt{\mathcal{C}_n}} \xrightarrow[n\to\infty]{P_{\theta_0}^{(n)}} 2.$$

3. 锐度。 对于任意 $k < 2$， 存在一个（确定性）序列 $\mathcal{C}_n \downarrow 0$， 使得对于所有充分大的 n,

$$\rho_{\mathrm{rob},n}(\mathcal{C}_n) > \rho_{0,n} + k\,\rho_{0,n}\sqrt{\mathcal{C}_n}$$

其中 $P_{\theta_0}^{(n)}$概率趋于 1。因此， 系数 2 在 (5) 渐近最优　　*l.*

解释。 对象级鲁棒性指标（如易感性或基于最大连通分量的度量）通常会以 $1/\Delta(\theta)$ 或 $1/\Delta(\theta)^2$ 的速度发散，因为网络正接近碎裂阈值 [vanderHofstad, 2017]。定理3.3 表明，一旦将此类指标嵌入决策理论框架，指标中的不确定性便会以更快的速度膨胀，在 Δ_0^{-1}中具有普适指数 4，并呈现普适的 $\sqrt{\mathcal{C}_n}$ 半径依赖关系 $\mathcal{C}_n$，且常数为 2。

在接下来的网络章节中，我们将针对具体的鲁棒性指标（例如稀疏 Erdős–Rényi 模型和配置模型的易感性 3.1 ）验证假设，并推导出相匹配的决策理论鲁棒性极小极大下界。

3.2 推广至一般的 ϕ–散度球

最后指出，只需进行简单的重新缩放，我们所有局部决策论稳健性结果都可以从 KL 球推广到一般的 ϕ–散度球。

定义 3.4 （ϕ–散度与 ϕ–球）。 设 ϕ: $[0,\infty) \to \mathbb{R}$ 为凸函数，满足 $\phi(1) = \phi'(1) = 0$且 $0 < \phi''(1) < \infty$。对于满足 $Q \ll P$ 的概率测度 Q 和 P，我们定义 ϕ–散度

$$D_\phi(Q\|P) := \int \phi\left(\frac{\mathrm{d}Q}{\mathrm{d}P}\right) \mathrm{d}P,$$

以及相应的半径为 $C > 0$ 、以 P 为中心的 ϕ–散度球，

$$\mathcal{B}_\phi(P; C) := \{Q \ll P : D_\phi(Q\|P) \le C\}.$$

注 3.5 （KL与 ϕ球的局部等价性）。 根据 Csisz´ar 的二次近似 ，

$$D_\phi(Q\|P) = \frac{\phi''(1)}{2}\,\chi^2(Q,P) + o\big(\chi^2(Q,P)\big) \qquad \text{as } Q \to P,$$

对于 Kullback–Leibler 散度 KL($Q\|P$)，也有类似的展开。特别是，当半径 C较小时， ϕ球 $\mathcal{B}_\phi$(P; C) 在局部等价于半径为 $C_{\mathrm{KL}} = C/\phi''(1)$ 的 KL 球，误差至多为 $o(C)$ 阶项。

注 3.6 （决策理论鲁棒性指数的推广）。 由于我们所有的局部决策论稳健性风险展开和极小极大指数，都只通过散度半径在 $\chi^2(Q,P)$ 中的二次行为依赖于该半径，因此，为 KL 球证明的结果经过缩放 $C \mapsto C/\phi''(1)$ 后，可原样推广至 ϕ球。等价地，若某个模型在 KL 散度下具有决策理论鲁棒性噪声指数 J，且其局部决策论稳健性风险展开涉及 $\sqrt{C}$，那么同一模型在 $\mathcal{B}_\phi$(P; C) 下的决策论稳健性指数为 $J/\sqrt{\phi''(1)}$，且具有相同的 $\sqrt{C}$缩放，误差至多为 $o(\sqrt{C})$ 阶项。因此，我们所有的指数 4 现象和极小极大界，都推广至一般的 ϕ散度球，散度半径中只需乘以一个通用因子 $\phi''(1)^{-1/2}$。

4 稀疏 Erdős–Rényi 模型与随机块模型之间的非参数极小极大理论

现在，我们将该框架专门用于稀疏 Erd˝os–R´enyi 模型与稀疏双块随机块模型之间的模型选择，并证明：

1. 每个顶点的 Kullback–Leibler 信息和切尔诺夫信息分别具有显式极限 $I(\lambda)$ 和 $J(\lambda)$；2. 将无标签随机块模型视为稀疏图子时，这些极限仍然成立；3. 即使采用稳健化，任何估计量或后验分布都无法在广泛的非参数类上一致地突破切尔诺夫指数 $J(\lambda)$。

4.1 带标签的稀疏 ER 与随机块模型的显式信息指数

设 n 为偶数。固定 $c > 0$ 和信号参数 $\lambda \in (0, c)$，并令

$$p_n := \frac{c}{n}, \qquad p_n^{\text{in}} := \frac{c+\lambda}{n}, \qquad p_n^{\text{out}} := \frac{c-\lambda}{n}.$$

令 $\mathcal{V}_n = \{1, \dots, n\}$，并固定一个平衡划分 $\sigma\colon \mathcal{V}_n \to \{+1, -1\}$，其中每个社团有 $n/2$ 个节点。

- 在 H_0 （稀疏 Erdős–Rényi 模型）下，邻接矩阵 $A = (A_{ij})_{1 \le i < j \le n}$ 的各项相互独立，服从伯努利分布(p_n)。记其分布为 $P_{(n)\,0}$。
- 在 H_1 （已知标签的平衡二块随机块模型）下，各条边相互独立，且

$$A_{ij} \sim \begin{cases} \text{Bernoulli}(p_n^{\text{in}}), & \sigma(i) = \sigma(j), \\ \text{Bernoulli}(p_n^{\text{out}}), & \sigma(i) \neq \sigma(j), \end{cases}$$

并记其分布为 $P_1^{(n)}$。

令 $N_n = \binom{n}{2}$ 表示边数，并令 $N_{\text{in}n}, N_n^{\text{out}}$ 表示块内/块间边数；容易验证 $N_n^{\text{in}} = 2\binom{n/2}{2} = n($ $n-2)/4$，且 $N_{\text{out}_n} = n^2/4$。

引理 4.1 （KL 散度与每顶点信息）。令 $P_0^{(n)}$ 表示边概率为 $p_n = c/n$ 的 *Erd˝os–R´enyi* 模型，令 $P_1^{(n)}$ 表示社团规模相等且边概率为

$$p_n^{\text{in}} = \frac{c+\lambda}{n}, \qquad p_n^{\text{out}} = \frac{c-\lambda}{n},$$

其中 $c > 0$和 $|\lambda| < c$为固定值（因此对于所有充分大的 n， $p_n^{\text{in}}, p_n^{\text{out}} \in$ （0, 1））。令 $D_n :=$ $\text{KL}\big(P_{(n)\,1} \,\|P_{(0}{}_n^{\,})\big)$，并令 N_n^{in}和 $N_{\text{out}n}$分别表示块内和块间无序顶点对的数量。则

$$D_n = N_n^{\text{in}}\,\text{KL}\big(\text{Bern}(p_n^{\text{in}}) \| \text{Bern}(p_n)\big) + N_n^{\text{out}}\,\text{KL}\big(\text{Bern}(p_n^{\text{out}}) \| \text{Bern}(p_n)\big).$$

此外，

$$\frac{D_n}{n} \xrightarrow[n\to\infty]{} I(\lambda) := \frac{1}{4}\left[(c+\lambda)\log\frac{c+\lambda}{c} + (c-\lambda)\log\frac{c-\lambda}{c}\right],$$

因此，特别地 $D_{\ n} = I$（λ） $n + o$（n），当 $n \to \infty$ 时。最后，对 λ 在 0 附近作泰勒展开，得到

$$I(\lambda) = \frac{\lambda^2}{4c} + O\left(\frac{\lambda^4}{c^3}\right), \qquad \lambda \to 0.$$

引理 4.2 （切尔诺夫信息与错误指数）。令

$$\mathcal{C}_n := \sup_{0 \le t \le 1} -\log \sum_A P_0^{(n)}(A)^{1-t} P_1^{(n)}(A)^t$$

为 $P_0^{(n)}$和 $P_{(n)\,1}$之间的切尔诺夫信息。假设处于稀疏区域 $p_n = c/n$且

$$p_n^{\text{in}} = \frac{c+\lambda}{n}, \qquad p_n^{\text{out}} = \frac{c-\lambda}{n}, \qquad |\lambda| < c,$$

包含两个大小均为 $n/2$ 的块，因此

$$N_n^{\text{in}} = 2\binom{n/2}{2} = \frac{n^2}{4} - \frac{n}{2}, \qquad N_n^{\text{out}} = \left(\frac{n}{2}\right)^2 = \frac{n^2}{4}.$$

Then

$$\frac{\mathcal{C}_n}{n} \xrightarrow[n\to\infty]{} J(\lambda) := \sup_{0\le t\le 1} \frac{1}{4}\Big[2c - c^{1-t}\big((c+\lambda)^t + (c-\lambda)^t\big)\Big].$$

此外，当 $\lambda \to 0$ 时，

$$J(\lambda) = \frac{\lambda^2}{16c} + O\left(\frac{\lambda^4}{c^3}\right),$$

因此，特别是 $\mathcal{C}_n = J(\lambda)\ n + o(n)$ 且

$$J(\lambda) = \tfrac{1}{4} I(\lambda) + O\left(\frac{\lambda^4}{c^3}\right),$$

其中 $I(\lambda)$ 是引理 *4.1* 中每个顶点的 *KL* 信息。

注释 4.3 (小信号信息指数)。 在第 4.1 节的稀疏双块 Erdős–Rényi模型 与随机块模型实验中，令 $I(\lambda)$ 和 $J(\lambda)$ 分别表示引理 4.1–4.2 中精确的每顶点 Kullback–Leibler 信息指数和 Chernoff 信息指数。在 $\lambda = 0$ 附近进行泰勒展开可得

$$I(\lambda) = \frac{\lambda^2}{4c} + O\left(\frac{\lambda^4}{c^3}\right), \qquad J(\lambda) = \frac{\lambda^2}{16c} + O\left(\frac{\lambda^4}{c^3}\right), \qquad \lambda \to 0.$$

特别是，在主导阶上，可以使用以下近似

$$I(\lambda) \ \approx\ \frac{\lambda^2}{4c}, \qquad J(\lambda) \ \approx\ \frac{\lambda^2}{16c},$$

并且 Chernoff 指数渐近地等于 KL 指数的四分之一：

$$J(\lambda) \ \approx\ \tfrac{1}{4}\, I(\lambda) \qquad \text{as } \lambda/c \to 0.$$

因此，对于带标签的稀疏 ER 与随机块模型，假设检验和贝叶斯因子模型选择的最优指数误差率由显式的 Chernoff 指数 $J(\lambda)$ 决定。

4.1.1 未标记 随机块模型与图子决策论稳健极小极大检验

现在，我们直接在图子层面表述 ER 与随机块模型的决策论稳健性极小极大问题。设 $K \ge 2$，令 $\pi = (\pi_1, \ldots, \pi_K)$ 为定义在各块上的概率向量，并令P_0、$P_\lambda \in [0,1]^{K\times K}$ 分别表示 H_0 和 H_1 下的边概率矩阵，其中 P_0对应 Erd˝os–R´enyi 基线（无社区），而 P_λ 对应社区备择。照例，我们将顶点集 $[n]$ 上参数为 $(\pi,\ P_0)$ 或 $(\pi,\ P_\lambda)$ 的带标签随机块模型序列记为 $(G_n)_{n\ge1}$，并将对应的概率律记为 $\big(\mathbb{P}_0^{(n)}\big)_{n\ge1}$ 和 $\big(\mathbb{P}_\lambda^{(n)}\big)_{n\ge1}$。

令 $W_0, W_\lambda\colon [0,1]^2 \to [0,1]$ 为按通常方式与 (π, P_0) 和 (π, P_λ) 相关联的阶梯函数图子：将单位区间划分为 K 个长度为 π_k的子区间；当 x 位于第 k 个区块且 y 位于第 ℓ个区块时，$W_\lambda(x,y) = P_\lambda(k,\ell)$。对于 $W \in \{W_0, W_\lambda\}$，我们用 $\widetilde{\mathbb{P}}_W^{(n)}$ 表示通过抽取 $U_1, \ldots, U_n \overset{\text{i.i.d.}}{\sim} \text{Unif}[0,1]$，然后 $G_n \mid U_{1:n} \sim \mathcal{G}(W)$得到的可交换随机图的分布，即标准的图函数抽样方案。

回顾一下，$I(\lambda)$ 和 $J(\lambda)$ 分别表示第 4.1 节中针对带标签的随机块模型实验 引入的每顶点信息和决策理论鲁棒性噪声指数。$\big(\mathbb{P}_0^{(n)},\ \mathbb{P}_\lambda^{(n)}\big)_{n\ge1}$。

引理 4.4 (图子表示下的信息与决策理论鲁棒性噪声指数**)**。 固定 λ ，并考虑带标签的随机块模型实验 $\big(\mathbb{P}_0^{(n)}$ 、 $\mathbb{P}_\lambda^{(n)}\big)_{n\geq 1}$ 以及无标签图子实验 $\big(\widetilde{\mathbb{P}}_{W_0}^{(n)}$ 、 $\widetilde{\mathbb{P}}_{W_\lambda}^{(n)}\big)_{n\geq 1}$。那么，每顶点信息和决策理论鲁棒性噪声指数相同：

$$I(\lambda) \;=\; \lim_{n\to\infty}\frac{1}{n}\,D\big(\mathbb{P}_\lambda^{(n)}\big\|\mathbb{P}_0^{(n)}\big) \;=\; \lim_{n\to\infty}\frac{1}{n}\,D\big(\widetilde{\mathbb{P}}_{W_\lambda}^{(n)}\big\|\widetilde{\mathbb{P}}_{W_0}^{(n)}\big),$$

并且，对于任意决策理论鲁棒性半径序列 $\mathcal{C}_n = o(n)$，

$$J(\lambda) \;=\; \lim_{n\to\infty}\frac{1}{n}\,J_n\big(\mathbb{P}_\lambda^{(n)},\mathbb{P}_0^{(n)};\mathcal{C}_n\big) \;=\; \lim_{n\to\infty}\frac{1}{n}\,J_n\big(\widetilde{\mathbb{P}}_{W_\lambda}^{(n)},\widetilde{\mathbb{P}}_{W_0}^{(n)};\mathcal{C}_n\big),$$

其中 $D(\cdot\|\cdot)$ 表示 ***Kullback–Leibler***散度，而 $J_n(\cdot,\cdot;\mathcal{C}_n)$ 是有限的n 决策理论鲁棒性噪声指数，定义见第 *4.3*节。

现在我们考虑两个固定图子之间的假设检验。

定理 4.5 （图子的决策理论鲁棒贝叶斯因子检验）。 考虑检验

$$H_0\colon W = W_0 \qquad \textit{versus} \qquad H_1\colon W = W_\lambda,$$

基于 $G_n \sim \widetilde{\mathbb{P}}_W^{(n)}$，先验概率为 $\pi_0,\pi_1 \in (0,1)$。令

$$\mathrm{BF}_n(G_n) := \frac{\pi_1}{\pi_0}\,\frac{\mathrm{d}\widetilde{\mathbb{P}}_{W_\lambda}^{(n)}}{\mathrm{d}\widetilde{\mathbb{P}}_{W_0}^{(n)}}(G_n)$$

表示贝叶斯因子，并令 φ_n^{BF}为贝叶斯因子检验，当 $\mathrm{BF}_n(G_n)\geq 1$ 时拒绝 H_0 。对于决策理论鲁棒性半径序列 $\mathcal{C}_n = o(n)$，令 $R_n^{\mathrm{WH}}(\varphi_n^{\mathrm{BF}};\mathcal{C}_n)$ 表示 φ_n^{BF} 在以 $\widetilde{\mathbb{P}}_{W_0}^{(n)}$ 和 $\widetilde{\mathbb{P}}_{W_\lambda}^{(n)}$ 为中心、半径为 $\mathcal{C}_n$ 的 ***KL*** 球上的相应决策理论鲁棒贝叶斯风险。那么

$$-\lim_{n\to\infty}\frac{1}{n}\log R_n^{\mathrm{WH}}(\varphi_n^{\mathrm{BF}};\mathcal{C}_n) \;=\; J(\lambda),$$

其中 $J(\lambda)$ 是引理 *4.4*中的决策理论鲁棒性噪声指数 .

我们最终将决策论稳健极小极大刻画从带标签随机块模型推广到非参数图子类。

定理 4.6 (非参数图子的决策理论鲁棒极小极大检验**)**。 设 $(\mathcal{W}_n)_{n\geq 1}$是一个图子类序列，满足 W_0，$W_\lambda \in \mathcal{W}_n$ 对所有 n均成立，并假设诱导实验$\big\{\widetilde{\mathbb{P}}_W^{(n)} : \; W \in \mathcal{W}_n\big\}$ 满足与第 *4.1*节相同的局部渐近正态性和正则性假设，其信息指数为 $I(\lambda)$，决策理论鲁棒性噪声指数为 $J(\lambda)$。

对于任意检验序列 φ_n 以及任意决策理论鲁棒性半径 $\mathcal{C}_n = o(n)$，定义检验 W_0 对 W_λ 的图子决策论稳健极小极大风险为

$$R_{n,\mathcal{W}_n}^{\mathrm{WH}}(\varphi_n;\mathcal{C}_n) := R_n^{\mathrm{WH}}\big(\varphi_n;W_0,W_\lambda,\mathcal{C}_n\big),$$

其中 $R_n^{\mathrm{WH}}(\cdot)$ 是第*4.3*节中的决策理论鲁棒检验风险。于是

$$\liminf_{n\to\infty}\frac{1}{n}\log\inf_{\varphi_n} R_{n,\mathcal{W}_n}^{\mathrm{WH}}(\varphi_n;\mathcal{C}_n) \;\geq\; -J(\lambda),$$

而定理*4.5* 中的贝叶斯因子检验 φ_n^{BF}达到了相匹配的错误指数

$$-\lim_{n\to\infty}\frac{1}{n}\log R_{n,\mathcal{W}_n}^{\mathrm{WH}}\big(\varphi_n^{\mathrm{BF}};\mathcal{C}_n\big) \;=\; J(\lambda).$$

特别地， J（λ） 是图子类 $\mathcal{W}_n$ 内检验 W_0 与 W_λ 时的非参数决策理论稳健性极小极大错误指数。

4.2 无标记随机块模型与稀疏图子图类

接下来考虑 r 表示无标签图子图表示。令 W_0 为常数稀疏图子 n

$$W_0^{(n)}(x,y) \equiv \frac{c}{n},$$

并令 W_λ 为双块阶梯图元

$$W_\lambda(x,y) := \begin{cases} \dfrac{c+\lambda}{n}, & x,y \in [0,1/2) \text{ or } x,y \in [1/2,1], \\ \dfrac{c-\lambda}{n}, & \text{otherwise.} \end{cases}$$

对于 $W \in \{W_0, W_\lambda\}$，通过对潜在位置 $U_i \sim$ 进行独立同分布的 Unif$[0,1]$ 抽样，并独立地对边 $A_{ij} \mid U_i, U_j \sim$ 按伯努利分布$(W(U_i,U_j))$ 抽样，定义 G_n。令 $P_{(n)\,0,\text{无标记}}$ 和 $P_{1}^{(n)}{}_{,\text{无标记}}$ 表示相应的图分布。

等价地，在 W_λ 下，我们可以引入独立同分布的潜在标签 $Z_i \in \{\pm 1\}$，其分布为 $\mathbb{P}(Z_i = 1) = 1/2$, 并且

$$\mathbb{P}(A_{ij} = 1 \mid Z) = \begin{cases} \dfrac{c+\lambda}{n}, & Z_i = Z_j, \\ \dfrac{c-\lambda}{n}, & Z_i \neq Z_j. \end{cases}$$

引理 4.7 (无标记随机块模型信息指数)。令 $D_n^{\text{unlab}} := \mathrm{KL}\big(P_{(n)\,1,\text{无标记}} \| P_0^{(n)}{}_{,\text{无标记}}\big)$，并令 $\mathcal{C}_n^{\text{unlab}}$ 为 $P_0^{(n)}{}_{,\text{无标记}}$ 与 $P_{(n)\,1,\text{无标记}}$之间的切尔诺夫信息。那么，在稀疏区域 $p_n = c/n$ 中，

$$\frac{D_n^{\text{unlab}}}{n} \to I(\lambda), \qquad \frac{\mathcal{C}_n^{\text{unlab}}}{n} \to J(\lambda),$$

因此 $D_n^{\text{unlab}} = I(\lambda)\ n + o(n)$ 且 $\mathcal{C}_n^{\text{unlab}} = J(\lambda)\ n + o(n)$。特别是，从带标签随机块模型转为无标签随机块模型（通过稀疏图子表示）不会改变每顶点信息指数。

在 W_0 与 W_λ 之间进行贝叶斯因子模型选择，可达到切尔诺夫速率：

定理 *4.8*（无标签随机块模型与 *Erdős–Rényi*模型之间的稳健贝叶斯因子）。考虑两个模型的贝叶斯实验 $M \in \{0,1\}$，其先验为 $\Pi(M=0) = \Pi(M=1) = 1/2$，似然函数为 $P_0^{(n)}$*,unlab (Erdős–Rényi*模型*)* 和 $P_1^{(n)}$*,unlab (* 随机块模型 *)*。令 $\Pi_n(M \mid G_n)$ 为后验分布，并令 δ_n 为贝叶斯判别器 $\delta_n(G_n) = \mathbb{1}\{\Pi_n(M=1 \mid G_n) \geq 1/2\}$，即在 $P_0^{(n)}$*,unlab* 与 $P_{(n)}$ *1,unlab* 之间进行似然比（贝叶斯因子）检验。

对于 $m \in \{0,1\}$，记

$$R_{n,m} := \mathbb{P}_{P_{m,\text{unlab}}^{(n)}}\big(\delta_n(G_n) \neq m\big)$$

为模型 m 下的（非稳健）误分类概率，并注意到 $R_{n,\,0}$ 和$R_{n,\,1}$ 具有相同的指数速率。于是：

1. Chernoff 最优性。贝叶斯因子检验渐近地达到 *Chernoff* 最优性：

$$-\frac{1}{n}\log R_{n,m} \longrightarrow J(\lambda), \qquad m = 0,1,$$

其中 $J(\lambda)$ 是引理 *4.7*中的逐顶点 *Chernoff* 指数。

2. 稳健贝叶斯风险。 对于任意满足 $\mathcal{C}_n \downarrow 0\, \mathcal{C}_n = o\big(R_{n,m}^2\big)$ （等价地， $\sqrt{\mathcal{C}_n} = o(R_{n,m})$）的序列，稳健贝叶斯误分类概率

$$\mathcal{R}_n^{\mathrm{WH}}(m;\mathcal{C}_n) := \mathbb{E}_{P_{m,\mathrm{unlab}}^{(n)}}\Big[\sup_{Q:\,\mathrm{KL}(Q\|\Pi_n(\cdot|G_n))\le\mathcal{C}_n} \mathbb{E}_Q\big[\mathbb{1}\{\delta_n(G_n)\neq M\}\big]\Big]$$

满足 $\mathcal{R}_n^{\mathrm{WH}}(m;\mathcal{C}_n) = R_{n,\ m}\big(1+o(1)\big)$，因此

$$-\frac{1}{n}\log \mathcal{R}_n^{\mathrm{WH}}(m;\mathcal{C}_n) \;\longrightarrow\; J(\lambda), \qquad m=0,1.$$

因此，对于指数尺度上足够小的衰减半径 $\mathcal{C}_n$ ，决策理论上的稳健化不会改变信息论检测率。

4.3 模型选择的非参数极小极大下界

现在，我们将 ER 与随机块模型（SBM）的检验问题置于一个广义的非参数模型类中。设 $\mathcal{P}_n$是任意一组图分布，使得对于所有足够大的 n ，

$$P_{0,\mathrm{unlab}}^{(n)},\ P_{1,\mathrm{unlab}}^{(n)} \in \mathcal{P}_n.$$

（可能随机化的）选择器 δ_n 将图映射到 $\{0,1\}$，并为每个 $P \in \mathcal{P}_n$关联一个标签 $M(P) \in \{0,1\}$，其中 $M\big(P_{(n)\,0,\ \mathrm{unlab}}\big) = 0$且 $M\big(P_{(n)\,1,\ \mathrm{unlab}}\big) = 1$。令 $\Pi_n(\cdot \mid G_n)$ 为 $\{0,1\}$上的任意（可能依赖于数据的）后验分布或伪后验，并定义稳健后验误分类概率

$$e_n^{\mathrm{rob}}(C;G_n) := \sup_{Q:\,\mathrm{KL}(Q\|\Pi_n(\cdot|G_n))\le C} \mathbb{E}_Q\big[\mathbb{1}\{\delta_n(G_n)\neq M\}\big].$$

相应的非参数极小极大稳健风险为

$$\mathfrak{R}_n^\star(C) := \inf_{\delta_n,\Pi_n}\sup_{P\in\mathcal{P}_n} \mathbb{E}_P\big[e_n^{\mathrm{rob}}(C;G_n)\big].$$

定理 4.9 （稀疏 Erdős–Rényi 模型与随机块模型的非参数极小极大下界）。 令 $\mathcal{P}_n$ 为任意一个包含 $P_{(n)\ 0,\ \text{无标号}}$ 以及 $P_{1,\ \text{无标号}}^{(n)}$ 的模型类，其中 n 足够大。令 $\mathcal{C}_n \downarrow 0$ 为任意序列。则

$$\limsup_{n\to\infty}\frac{1}{n}\log\frac{1}{\mathfrak{R}_n^\star(\mathcal{C}_n)} \;\le\; J(\lambda) \;=\; \frac{\lambda^2}{16c} + O\!\left(\frac{\lambda^4}{c^3}\right) \qquad as\ \lambda\to 0. \tag{6}$$

特别地，对于 $\mathcal{P}_n$ 中的所有模型，任何估计量/后验分布对以及任何半径选择，都无法达到优于 $J(\lambda)$ 的指数误差率。

如果进一步将范围限制为包含 W_0 和 W_λ 的图子类 $\mathcal{W}_n$ ，并令 $\mathcal{P}_n = \{P_W^{(n)} :\ W \in \mathcal{W}_n\}$，我们将得到匹配的上界。

定理 4.10 （稀疏图子类上的极小极大刻画）。 令 $\mathcal{W}_n$ 为任意图子类，满足 W_0、$W_\lambda \in \mathcal{W}_n$，并令 $P_W^{(n)}$ 表示由 W生成的随机图的分布。对于每个 n 和稳健半径 $\mathcal{C}_n > 0$，定义两点图子决策论稳健极小极大风险为

$$\mathfrak{R}_{n,\mathcal{W}_n}^{\mathrm{WH}}(\mathcal{C}_n) := \inf_{\delta_n,\Pi_n}\max_{m\in\{0,1\}} \mathbb{E}_{P_{W_m}^{(n)}}\big[e_n^{\mathrm{rob}}(\mathcal{C}_n;G_n)\big],$$

其中 W_0 和 W_λ 分别对应 *ER* 和双块随机块模型的图子，而 $e_n^{\mathrm{rob}}(\mathcal{C}_n;\ G_n)$ 是第 *4.3*节中的鲁棒化后验误分类概率，其中 $M \in \{0,1\}$ 表示模型。

设 R_n 为在 W_0 与 W_λ 之间、对 $M \in \{0,1\}$赋予相等先验概率时，贝叶斯因子检验的（非稳健）贝叶斯误分类概率，如定理 *4.8* (*i*) 所示。设 $\mathcal{C}_n \downarrow 0$满足 $\mathcal{C}_n = o(R_n^2)$；特别地，只需假设

$$\mathcal{C}_n = o\big(\exp\{-2J(\lambda)n\}\big), \qquad \textit{equivalently} \qquad \sqrt{\mathcal{C}_n} = o\big(\exp\{-J(\lambda)n\}\big),$$

因为 $R_n = \exp\{-J(\lambda)n + o(n)\}$。于是

$$\lim_{n\to\infty} \frac{1}{n} \log \frac{1}{\mathfrak{R}^{\mathrm{WH}}_{n,\mathcal{W}_n}(\mathcal{C}_n)} = J(\lambda).$$

特别地，对于嵌入模型类 $\mathcal{W}_n$中的二点图子检验问题 $W = W_0$ 与$W = W_\lambda$， W_0 与 W_λ 之间的贝叶斯因子检验在 ***Chernoff*** 指数 $J(\lambda)$ 下是决策论稳健极小极大最优的。

这些结果表明，即使在非常大的非参数模型类中，稳健化也不会改善或降低稀疏 ER 与随机块模型的最优检测指数。

5 基于渗流的网络稳健性指标的鲁棒性

现在我们将定理 3.3 专门应用于配置模型和基于渗流的稳健性指标，并推导出一个关于距碎裂阈值距离的、具有临界指数 4 的非参数极小极大下界。

5.1 配置模型与临界稳健性指标

我们聚焦于度数独立同分布的配置模型，并考虑由连通分量大小导出的稳健性指标。设 $G_n \sim \mathrm{CM}_n(\mu)$ 是定义在 n 个顶点上的配置模型，其度数独立同分布 $D_i \sim \mu$ 且三阶矩有限，为 $\mathbb{E}_\mu[D^3] < \infty$；令 $P_\mu^{(n)}$ 表示 G_n 的分布。记

$$\theta(\mu) := \frac{\mathbb{E}_\mu[D(D-1)]}{\mathbb{E}_\mu[D]}$$

为分枝因子。在次临界区间 $\theta(\mu) < 1$中，包含一个均匀随机选取顶点的连通簇的期望有限；在超临界状态 $\theta(\mu) > 1$下，存在一个巨型连通分量[van der Hofstad, 2017]。

我们采用易感性作为具体的稳健性指标：对于 $G_n \sim \mathrm{CM}_n(\mu)$ 和一个均匀随机选取的顶点 V_n,

$$S_n(\mu) := \mathbb{E}_\mu\big[|C(V_n)|\big],$$

其中 $C(V_n)$ 是 V_n 所在的连通分量。对于满足 $\theta(\mu) < 1$ 的 μ，标准的分枝过程耦合可得

$$S_n(\mu) \xrightarrow[n\to\infty]{} R(\mu) := \frac{1}{1-\theta(\mu)}.$$

命题 5.1（配置模型中易感性的临界行为）。设 μ 为配置模型的度分布，并令

$$\theta(\mu) := \frac{\mathbb{E}_\mu[D(D-1)]}{\mathbb{E}_\mu[D]}$$

表示其分枝因子。将易感性指数定义为

$$R(\mu) := \frac{1}{1-\theta(\mu)}, \qquad \Delta(\mu) := 1-\theta(\mu).$$

那么，对于 $\{\mu : \theta(\mu) < 1\}$ 的任意紧子集， $R(\mu)$ 是光滑的，并且具有如下表示

$$R(\mu) = \frac{c_0}{\Delta(\mu)} + H(\mu), \qquad c_0 = 1,\ H(\mu) \equiv 0.$$

此外，假设度分布族 μ由有限维参数 ϑ 参数化， $\vartheta \mapsto \mu_\vartheta$，并设 $\vartheta_\star$ 为满足以下条件的临界参数

$$\theta(\mu_{\vartheta_\star}) = 1, \qquad \nabla_\vartheta \theta(\mu_{\vartheta_\star}) \neq 0$$

（以非退化方式趋近临界性）。那么，当 $\vartheta \to \vartheta_\star$ 从亚临界侧趋近 $\{\vartheta : \theta(\mu_\vartheta) < 1\}$ 时，也就是说，当 $\Delta(\mu_\vartheta) \downarrow 0$ 时，

$$\left\|\nabla_\vartheta R(\mu_\vartheta)\right\| \asymp \Delta(\mu_\vartheta)^{-2}.$$

特别是，在任何此类有限维参数化中， R 满足假设*3.1* ，其中$\rho(\mu) = \theta(\mu)$ 以及 $\Delta(\mu) = 1-\theta(\mu)$。

因此，配置模型的易感性提供了一个具体示例：它是一种基于渗流的稳健性指数，具有定理3.3所要求的 $1/\Delta$ 发散性。更复杂的鲁棒性泛函，例如节点移除过程中最大连通分量曲线下的面积 [Artime等人， 2024], 表现出相同的主导 $1/\Delta$ 行为和相同的临界指数。

5.2 临界指数与极小极大下界

现在，我们将定理3.3 专门应用于易感性 $R(\mu)$，并在包含配置模型族的一般模型类上推导非参数极小极大下界。

固定一个序列 $\Delta_n \downarrow 0$，满足 $\Delta_n \gg n^{-1/2}$，并考虑满足 $\Delta(\mu) = 1-\theta(\mu) \in [\Delta_n, 2\Delta_n]$的度分布 μ。令 $\mathcal{P}_n$ 为任意一个模型类，其中包含该切片中所有 μ 对应的配置模型 $\mathrm{CM}_n(\mu)$。对于 $R(\mu)$ 的估计量 $a_n(G_n)$，定义在 μ处的稳健风险，

$$\widetilde{\mathcal{R}}_n(a_n, \Pi_n; \mu; \mathcal{C}_n) := \mathbb{E}_{P_\mu^{(n)}}\left[\sup_{\widetilde{\Pi}:\, \mathrm{KL}(\widetilde{\Pi}\|\Pi_n) \le \mathcal{C}_n} \int \big(a_n(G_n) - R(\mu')\big)^2\, \widetilde{\Pi}(\mathrm{d}\mu')\right],$$

其中 $\Pi_n = \Pi_n(\cdot \mid G_n)$ 是 μ 上任意的数据依赖后验分布， $\mathcal{C}_n \ge 0$ 是一个半径。切片 $\{\mu : \Delta(\mu) \in [\Delta_n, 2\Delta_n]\}$ 上的非参数极小极大稳健风险为

$$\mathfrak{R}_n^{\mathrm{WH}}(\Delta_n, \mathcal{C}_n) := \inf_{(a_n, \Pi_n)} \sup\Big\{\widetilde{\mathcal{R}}_n(a_n, \Pi_n; \mu; \mathcal{C}_n) : P_\mu^{(n)} \in \mathcal{P}_n,\ \Delta(\mu) \in [\Delta_n, 2\Delta_n]\Big\}.$$

定理 5.2 （临近临界曲面的非参数极小极大下界）。 假设 $\mathcal{P}_n$包含配置模型族 $\{\mathrm{CM}_n(\mu) : \mu \in (\underline{\mu},\ \overline{\mu})\}$ 其中存在某个 $0 < \underline{\mu} < \overline{\mu} < \infty$，并令

$$\theta(\mu) := \frac{\mathbb{E}_\mu[D(D-1)]}{\mathbb{E}_\mu[D]}, \qquad \Delta(\mu) := 1-\theta(\mu),$$

表示分枝因子及其亏损。假设存在一个临界点 $\mu_\star \in (\underline{\mu}, \overline{\mu})$，使得 $\Delta(\mu_\star) = 0$ 且 $\nabla_{\underline{\mu}}\theta(\mu_\star) \neq 0$ （以非退化方式趋近临界性）。令 $\Delta_n \downarrow 0$ 满足

$\Delta_n \gg n^{-1/2}$，并假设对于所有足够大的 n，近临界切片 $\{\mu:\ \Delta(\mu) \in [\Delta_n, 2\Delta_n]\}$均非空。

定义此切片上的经典非参数极小极大风险为

$$\mathfrak{R}_n^{\mathrm{class}}(\Delta_n) := \inf_{a_n} \sup \Big\{ \mathbb{E}_{P_\mu^{(n)}} \big[\big(a_n(G_n) - R(\mu) \big)^2 \big] : P_\mu^{(n)} \in \mathcal{P}_n,\ \Delta(\mu) \in [\Delta_n, 2\Delta_n] \Big\},$$

其中 $R(\mu) = (1-\theta(\mu))^{-1}$ 是次临界区间内配置模型的易感性$\Delta(\mu) > 0$。于是，存在一个 $c > 0$，它仅取决于(μ, μ) 以及$\mu_\star$附近的局部参数化，使得

$$\mathfrak{R}_n^{\mathrm{class}}(\Delta_n) \ \geq\ \frac{c}{n\,\Delta_n^4} \qquad \textit{for all } n \textit{ large enough.} \tag{7}$$

等价地，

$$\liminf_{n\to\infty} n\,\Delta_n^4\,\mathfrak{R}_n^{\mathrm{class}}(\Delta_n) \ \geq\ c.$$

特别地，任何逐点支配经典平方误差风险的稳健化极小极大风险泛函 $\mathfrak{R}_n^{\mathrm{WH}}(\Delta_n, \mathcal{C}_n)$，

$$\widetilde{\mathcal{R}}_n(a_n, \Pi_n; \mu; \mathcal{C}_n) \ \geq\ \mathbb{E}_{P_\mu^{(n)}} \big[\big(a_n(G_n) - R(\mu) \big)^2 \big] \quad \textit{for all } (a_n, \Pi_n) \textit{ and } \mu,$$

必然满足相同的下界：$\mathfrak{R}_n^{\mathrm{WH}}(\Delta_n, \mathcal{C}_n) \geq \mathfrak{R}_n^{\mathrm{class}}(\Delta_n) \gtrsim 1/(n\Delta_n^4)$。

结合定理 5.2 与定理 3.3（应用于 $R(\mu)$，其后验分布以速率$r_n \asymp n^{-1/2}$收缩）可得：

- 在临界点附近状态下，易感性的基线后验均方误差按 $1/(n\Delta_n^4)$ 的量级缩放；
- 在 Δ_n^{-1} 中，稳健均方误差具有相同的临界指数 4，并会以$1 + 2\sqrt{\mathcal{C}_n}$ 的量级因子显著膨胀；
- 对于包含配置模型的大型模型类，不存在任何稳健程序能够在统一意义下改善这一缩放关系。

特别是，当网络接近其渗流阈值时，即使允许任意非参数模型以及对后验分布进行任意稳健化，对于基于渗流的稳健性指标的决策层面不确定性，也不可避免地至少以 Δ_n^{-4} 的速度爆炸。

6 网络模型的决策理论稳健决策计算

我们的理论将决策论稳健性抽象为：在基线后验分布 Π_0 周围的散度球 $\mathcal{B}_\phi(\Pi_0; C)$ 上进行优化。在实际应用中，Π_0 只能通过网络模型（随机块模型、图子、随机点积图、配置模型）的近似后验抽样获得，因此我们必须近似最不利扰动。本节将说明如何通过两个模块化步骤实现这一过程：

1. **基线推断**。拟合网络模型，并使用变分推断或谱方法／矩方法，在伪贝叶斯层的封装下，获得近似后验或伪后验 $\Pi_0(\mathrm{d}\theta \mid G_n)$。

2. **稳健化**。给定后验样本 $\{(\theta^s,\ w_s)\}_{s=1}^S$ 和损失 $L(a,\ \theta)$，通过对权重进行熵倾斜，计算散度球 $\mathcal{B}_\phi(\Pi_0; C)$ 上的最坏情况后验风险；对于一般的 ϕ–球，则在权重空间中使用镜像下降。

这种解耦意味着，现有针对随机块模型、图子和潜在位置模型的可扩展推断流程都可以原样使用：决策论鲁棒层会叠加在它们生成的任意近似后验样本之上。

完整的计算细节，包括 KL 散度球熵倾斜程序以及针对一般 ϕ–散度球的镜像下降对抗算法的显式伪代码，均收录于补充材料中。

6.1 网络模型的基线近似后验

对于第 2.2 节中的每个网络模型，我们假设可以获得近似后验抽样

$$\{(\theta^s, w_s) : s = 1, \dots, S\}, \qquad \sum_{s=1}^{S} w_s = 1,$$

来自基线后验或伪后验 Π_0 在 Θ上的结果。典型选择包括：

- **变分后验** 适用于随机块模型和随机点积图，其中 $q_\lambda(\theta)$ 是通过最大化证据下界拟合的均值场或结构化变分近似。我们对$\theta^s \sim q_\lambda$ 进行抽样，并设定 $w_s = 1/S$。

- **谱／矩伪后验**，其中点估计量 $\theta(G_n)$（例如谱嵌入、度矩、Hill尾指数）具有由随机矩阵理论或参数自助法推导出的近似高斯抽样分布。随后，我们将此高斯分布视为基线伪后验，并从中抽样。

决策论稳健化步骤将 $\{(\theta^s,\ w_s)\}$ 视为 Π_0 的经验近似，而不论这些抽样是如何获得的。

6.2 通过熵倾斜进行 KL 散度球优化

固定一个动作 a 和损失 $L(a,\ \theta)$。令 $L_s := L(a,\ \theta^s) \in \mathbb{R}$ 表示在后验抽样 θ^s处计算的损失，并令

$$\boldsymbol{w} = (w_1, \dots, w_S), \qquad \boldsymbol{q} = (q_1, \dots, q_S)$$

表示基线和扰动后的后验权重。对于以 Π_0 为中心、半径为 $C > 0$ 的 Kullback–Leibler 球，我们采用离散近似

$$\mathcal{U}_C(\boldsymbol{w}) := \Big\{\boldsymbol{q} :\ q_s \geq 0,\ \sum_s q_s = 1,\ \mathrm{KL}(\boldsymbol{q}\|\boldsymbol{w}) \leq C\Big\}, \qquad \mathrm{KL}(\boldsymbol{q}\|\boldsymbol{w}) := \sum_{s=1}^{S} q_s \log \frac{q_s}{w_s}.$$

a 的决策理论鲁棒后验风险为

$$\rho_{\mathrm{rob}}(a; C) \approx \sup_{\boldsymbol{q} \in \mathcal{U}_C(\boldsymbol{w})} \sum_{s=1}^{S} q_s L_s.$$

对于 KL 球，借助 Donsker–Varadhan变分公式，这个有限维问题可以转化为一个一维对偶问题。定义

$$\psi(\lambda) := \frac{C + \log \sum_{s=1}^{S} w_s \exp\{\lambda L_s\}}{\lambda}, \qquad \lambda > 0. \tag{8}$$

Then

$$\sup_{\boldsymbol{q} \in \mathcal{U}_C(\boldsymbol{w})} \sum_{s=1}^{S} q_s L_s = \inf_{\lambda > 0} \psi(\lambda), \tag{9}$$

且最不利权重具有熵倾斜 形式

$$q_s^\star(\lambda) \propto w_s \, \exp\{\lambda L_s\}, \qquad \lambda = \arg\min_{\lambda > 0} \psi(\lambda). \tag{10}$$

使用 MCMC 抽样实现。 在实践中， Π_0 由通过 MCMC 或变分推断获得的后验分布或伪后验抽样 $\{(\theta^s,\ w_s)\}_{s=1}^S$ 表示。对于固定动作 a ，我们计算 $L_s = L(a,\ \theta^s)$，并求解一维对偶问题 $\lambda^\star = \arg\min_{\lambda>0} \psi(\lambda)$。该离散支撑集上的最不利后验分布具有倾斜权重

$$q_s^\star \ \propto \ w_s \exp\{\lambda^\star L_s\}, \qquad s = 1, \ldots, S,$$

对于任意泛函 f，稳健后验期望可近似为 $\sum_s q_s^\star f(\theta^s)$。完整的数值方案（包括用于求解 $\lambda^\star$ 的简单二分搜索）见补充材料中的算法1 。

在实践中，我们按以下步骤进行：

1. 在后验分布或伪后验抽样上计算 $L_s = L(a,\ \theta^s)$。
2. 使用 log-sum-exp 稳定化方法计算 $\psi(\lambda)$及其导数。
3. 使用简单的一维方法（牛顿法、二分法或网格搜索）最小化 $\psi(\lambda)$，求解 $\lambda > 0$ 。
4. 构造倾斜权重 $q_s^\star(\lambda)$，在（10）中，并通过以下方式近似最不利后验分布下的稳健期望：$\sum_s q_s^\star(\lambda) f(\theta^s)$，其中泛函 f为任意感兴趣的泛函。

这为 KL 散度球稳健化提供了一种快速的对抗算法；除能够计算 $L(a, \theta^s)$ 外，无需针对具体模型进行额外推导。

镜像下降对抗算法 对于一般的 ϕ 散度球 $\mathcal{B}_\phi(\Pi_0; C)$，我们在后验抽样构成的离散权重空间中运行镜像下降对抗算法。令 $\boldsymbol{w} = (w_1, \ldots, w_S)$ 表示基准权重， $L_s = L(a, \theta^s)$，我们维护对数倾斜量 $u_s^{(t)} = \log(q_s^{(t)}/w_s)$，并进行如下更新：

$$u_s^{(t+1)} \ = \ u_s^{(t)} + \eta \left\{ L_s - \bar{L}^{(t)} \right\}, \qquad \bar{L}^{(t)} := \sum_{r=1}^{S} q_r^{(t)} L_r,$$

接着将 $\boldsymbol{q}^{(t+1)}$ 投影回 ϕ球 $\{D_\phi(\boldsymbol{q} \| \boldsymbol{w}) \ \le C\}$。对于 Kullback–Leibler 球，这个投影有闭式解；对于一般的 ϕ ，它可归结为单纯形上的一个小型凸规划。补充材料中的算法2 给出了完整的伪代码实现。

6.3 散度半径的实际校准

散度半径 C 表示我们愿意从工作后验 Π_0偏离多远。我们关于网络泛函的局部理论表明，在平方损失下，稳健后验风险具有一个尖锐的展开式

$$\rho_{\mathrm{rob}}(C) = \rho_0 + 2\,\rho_0\sqrt{C} + o\big(\rho_0\sqrt{C}\big),$$

其中， ρ_0 是基准后验风险（等价地说，是损失的后验方差）。在实践中，我们采用三种互补的校准策略:

- **决策论敏感性路径**。 对于给定的决策或网络泛函（谱间隙、巨型连通分量大小、希尔指数、流行病阈值），我们在一系列半径上计算$\rho_{\mathrm{rob}}(C)$，并绘制$\rho_{\mathrm{rob}}(C)$关于$\sqrt{C}$的曲线。理论预测该曲线起初呈线性，斜率为 $\approx 2\rho_0$；曲线上明显的折点表明，最不利后验分布已进入参数空间中性质截然不同的区域（例如越过渗流或检测阈值）。

- **随网络规模的缩放**。 由于 KL 散度会在边或顶点上累加，随着 n 增大，固定的 C代表每条边上的扰动更小。对于具有 $O(n)$个有效观测的稀疏模型（例如具有 $p_n \sim c/n$的稀疏ER/SBM），采用每顶点预算 $\mathcal{C}_n = c_\star/n$是很自然的选择，这样总 KL 扰动的量级就是一个常数。在稠密情形下，按边设定预算 $\mathcal{C}_n = c_{\star\star}/n^2$ 可能更合适。针对稀疏 ER 与随机块模型以及配置模型得出的非参数极小极大结果，可为特定问题提供指导，说明 $\mathcal{C}_n$ 在多大之前，稳健性膨胀才会主导基准风险。

- **应用特定容忍度**。 可以根据风险可容忍的膨胀程度反推出 C 。例如，要求 $\rho_{\mathrm{rob}}(C) \le (1+\delta)\,\rho_0$，便得到启发式约束 $\sqrt{C} \lesssim \delta/2$。在流行病学或渗流应用中，更自然的做法可能是约束最不利图在有效再生数或分枝因子等关键量上的偏移幅度，并利用早期理论中的利普希茨界将其转换为半径。

在我们的实验中，我们报告决策论稳健性敏感性曲线，并采用一个默认C ，其对应于后验风险大约膨胀 10–20%；除非领域知识表明应采用更严格或更宽松的容忍度。

7 实验

本节通过两个真实数据集，说明所提出的针对网络模型的决策论稳健性框架。在这两种情况下，我们都指定简单的工作模型（Erd˝os–R´enyi 和随机区块模型），定义具有科学研究意义的低维网络泛函，并按照 Watson和Holmes 的含义，研究相应贝叶斯决策的局部鲁棒性。第一个示例使用一个功能性脑连接网络总体；第二个示例使用来自印度卡纳塔克邦村庄的第 1 波社交网络。

7.1 合成实验验证 1：Erdős–Rényi模型与随机块模型及配置模型渗流

尽管我们的重点是放在真实数据应用（第7.2–7.3节）上，但纳入一项小型合成数据研究，以数值检验我们框架的两个关键理论预测是有益的:

（i）稳健后验风险关于小半径 $\sqrt{C}$ 的展开，以及（ii）碎片化型泛函的临界指数 4。下面的实验有意设计得尽可能简洁，可以在补充材料中报告。

合成实验 A：Erdős–Rényi模型与随机块模型在检测阈值附近的比较。我们首先考虑第″节中的稀疏Erd´os–Renyi模型与双块随机块模型的检验问题。固定 $c > 0$ 并取信号参数 $\lambda \in (0,\ c)$，我们取

$$p_n \;=\; \frac{c}{n}, \qquad p_n^{\mathrm{in}} \;=\; \frac{c+\lambda}{n}, \qquad p_n^{\mathrm{out}} \;=\; \frac{c-\lambda}{n},$$

并模拟图 G_n，分别来自 H_0（边概率为 p_n的稀疏 Erdős–Rényi 模型）和 H_1（标签已知、类间平衡的双块随机块模型，块内/块间概率为 p_n^{in}、p_n^{out}），如第 4 节所述。对于每个模拟得到的 G_n，我们在 $M \in \{0,1\}$ 上计算精确的两点后验分布 $\Pi_n(M \mid G_n)$，先验分布 H_0、H_1相等，并考虑模型选择决策$a(G_n) \in \{0,1\}$的 0–1 损失 $L(a,M) = \mathbb{1}\{a \neq M\}$。基线后验误分类概率为

$$e_{0,n}(G_n) \;=\; \min\bigl\{\Pi_n(M=0 \mid G_n),\, \Pi_n(M=1 \mid G_n)\bigr\},$$

对于一组较小半径 $C > 0$，我们计算 Watson–Holmes 稳健后验误分类概率

$$e_{\mathrm{rob},n}(C; G_n) \;=\; \sup_{Q:\,\mathrm{KL}(Q\|\Pi_n)\le C} \mathbb{E}_Q\bigl[\mathbb{1}\{a(G_n) \neq M\}\bigr]$$

按照第6节的方法，通过对两个后验权重进行熵倾斜。对蒙特卡洛重复试验中的$e_{0,n}(G_n)$和$e_{\mathrm{rob},n}(C;$ $G_n)$取平均，得到经验基线风险和稳健风险$R_{0,n} \;=\; \mathbb{E}[e_{0,n}(G_n)]$以及$R_{\mathrm{rob},n}(C) \;=\mathbb{E}[e_{\mathrm{rob},n}(C; G_n)]$。

定理 S.2 给出的通用小半径展开式，对于有界损失，有

$$R_{\mathrm{rob},n}(C) \;\approx\; R_{0,n} + \sqrt{2\,\mathrm{Var}_{\Pi_n}\bigl(L(a(G_n),M)\bigr)}\,\sqrt{C}, \qquad C \downarrow 0.$$

在两点检验中，该方差等于$R_{0,n}(1 - R_{0,n})$，因此首项$\sqrt{C}$ 系数与$\sqrt{R_{0,n}(1 - R_{0,n})}$成正比。为直观展示这一点，我们将稳健超额误分类概率归一化为

$$C \;\longmapsto\; \frac{R_{\mathrm{rob},n}(C) - R_{0,n}}{\sqrt{2\,R_{0,n}(1-R_{0,n})}\,\sqrt{C}},$$

对于较小的 C，该值应近似保持平坦，其水平由一个依赖于(n, λ)的有限常数给出。

合成实验 B：配置模型中的渗流与指数 4。为说明定理 3.3中确立的碎裂型指标的临界指数 4，我们考虑第 $_n(\mu)$ 节中的配置模型 CM5.1，其度分布为 μ，选择该分布使得分枝因子

$$\theta(\mu) \;=\; \frac{\mathbb{E}_\mu[D(D-1)]}{\mathbb{E}_\mu[D]}$$

满足 $0 < \Delta(\mu) := 1 - \theta(\mu) \ll 1$。具体而言，我们取泊松族 (μ_Δ)，其中$D_i \sim$ Poisson$(1-\Delta)$，因此 $\theta(\mu_\Delta) = 1-\Delta$ 且 $\Delta(\mu_\Delta) = \Delta$。对于每个 (n,Δ)，我们模拟图 $G_n \sim \mathrm{CM}_n(\mu_\Delta)$，并对泊松均值赋予 Gamma(1,1) 先验分布；在 G_n 条件化后

并截断至亚临界区域 $\{\lambda < 1\}$，得到共轭伪后验 $\Pi_n(\mu \mid G_n)$，我们用蒙特卡洛抽样对其进行近似。我们聚焦于易感性泛函

$$R(\mu) \;=\; \frac{1}{1-\theta(\mu)},$$

它在碎裂阈值附近按 $1/\Delta(\mu)$ 发散，并满足假设 3.1。在平方损失下，$L(a,\ \mu) = (a - R(\mu))^2$, 我们计算贝叶斯估计量 $a_n^\star = \mathbb{E}_{\Pi_n}[R(\mu)]$, 基准后验风险 $\rho_{0,\ n} = \mathbb{E}_{\Pi_n}[(a_n^\star - R(\mu))^2]$, 以及相应的 Watson–Holmes 稳健风险

$$\rho_{\mathrm{rob},n}(C) \;=\; \sup_{\tilde{\Pi}:\,\mathrm{KL}(\tilde{\Pi}\|\Pi_n)\le C} \mathbb{E}_{\tilde{\Pi}}\big[(a_n^\star - R(\mu))^2\big].$$

定理3.3 预示，在近临界区域且 C 较小时，

$$\rho_{0,n} \;\asymp\; \frac{1}{n\,\Delta(\mu)^4}, \qquad \rho_{\mathrm{rob},n}(C) - \rho_{0,n} \;\asymp\; \frac{\sqrt{C}}{n\,\Delta(\mu)^4}.$$

数值实现与结果。在实验 A 中，我们固定 $c = 3$，并考虑具有较弱社区信号 $\lambda = 0.4$ 的稀疏区域 $p_n = c/n$。我们在双点实验 H_0（稀疏 Erdős–Rényi 模型）与 H_1（具有已知标签、组内/组间连接概率分别为 $p_n^{\mathrm{in}} = (c+\lambda)/n$ 和 $p_n^{\mathrm{out}} = (c-\lambda)/n$ 的平衡二块随机块模型）下模拟规模为 $n = 400$ 的图。我们进行 $N_{\mathrm{rep}} = 1000$ 次蒙特卡洛重复试验，并采用半径 $C \in [10^{-4}, 10^{-2}]$ 的对数网格。对于每次重复试验，我们计算 $\{H_0, H_1\}$ 上的精确后验分布、0–1 损失下的贝叶斯规则，以及基线和稳健误分类概率 $e_{0,\ n}(G_n)$ 和 $e_{\mathrm{rob},\ n}(C; G_n)$，其中稳健误分类概率通过对两个后验权重进行熵倾斜得到。对重复试验取平均后得到$R_{0,\ n}$ 以及 $R_{\mathrm{rob},\ n}(C)$。根据上述归一化过程，可得经验稳健性敏感度曲线

$$C \;\longmapsto\; \frac{R_{\mathrm{rob},n}(C) - R_{0,n}}{\sqrt{2\,R_{0,n}(1-R_{0,n})}\,\sqrt{C}}.$$

图 1 的 (a) 面板将该量绘制为 $\sqrt{C}$的函数。在 $C \in [10^{-4}, 10^{-2}]$范围内，该曲线基本平坦，取值约在 3。7 到 4。2 之间。这证实了稳健误分类风险按预测的$\sqrt{C}$ 标度变化，且水平几乎恒定，并为这一稀疏 ER 与随机块模型检验问题提供了首要$\sqrt{C}$ 系数的有限样本估计。

在实验 B 中，我们固定 $n = 5000$，并考虑均值为$1 - \Delta$ 的泊松配置模型，其中 $\Delta \in \{0.40, 0.30, 0.25, 0.20, 0.17, 0.15\}$。对于每个 Δ，我们模拟 $N_{\mathrm{rep}} = 200$ 个图，通过 $S_{\mathrm{post}} = 2000$ 次抽样近似均值的截断伽马后验分布，并计算$\rho_{0、\ n}$ 以及 $\rho_{\mathrm{rob},\ n}(C)$（使用相同的网格 $C \in [10^{-4}, 10^{-1}]$）。图 1 的 (b) 面板绘出了归一化稳健性敏感性曲线

$$C \;\longmapsto\; \frac{\rho_{\mathrm{rob},n}(C) - \rho_{0,n}}{\rho_{0,n}\sqrt{C}}$$

对于（n，Δ）=（5000，0。2）。对于较小的半径，在 C的范围内，该曲线再次接近水平，取值约在 2。2 到 2。9 之间，这与定理 3.3 中平方损失展开的理论系数 2 高度一致，也说明了在距临界点的距离固定时，易感性风险会按预测发生 $\sqrt{C}$ 膨胀。

为探究 Δ^{-1}中的指数 4，我们固定一个较小的半径 $C \approx 10^{-3}$，并对每个 Δ考察双对数图

$$-\log \Delta \longmapsto \log\bigl(n\,\rho_{0,n}\bigr), \qquad -\log \Delta \longmapsto \log\Bigl(\tfrac{n\,(\rho_{\mathrm{rob},n}(C)-\rho_{0,n})}{\sqrt{C}}\Bigr).$$

图2 显示　出了得到的回归线及相应的最小二乘斜率

$$\widehat{\kappa}_{\mathrm{base}} \approx 4.49, \qquad \widehat{\kappa}_{\mathrm{rob}} \approx 4.65,$$

并且也报告于表 1中。两条斜率都与定理 3.3所预测的理论指数 4 极为接近。在蒙特卡罗误差的范围内，基线指数与稳健指数在数值上无法区分。结合小半径敏感性曲线，这些合成实验为以下两点提供了受控的数值检验：(i) $\sqrt{C}$ 决策理论稳健风险的展开，以及 (ii) 渗流型泛函在碎裂阈值附近按指数 4 爆发。

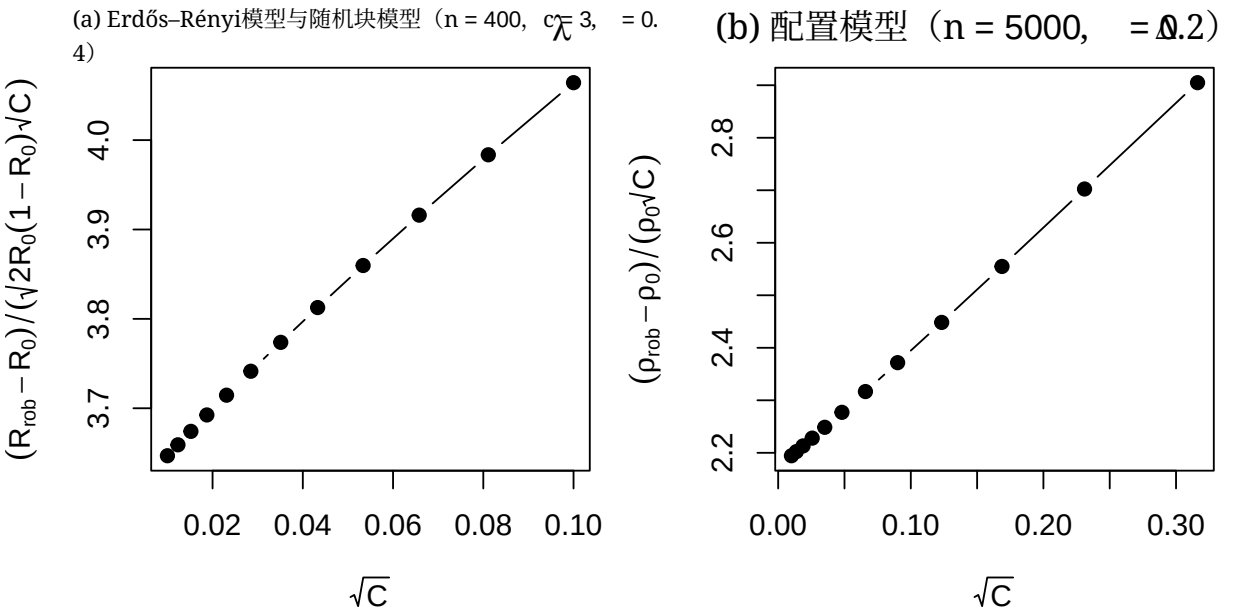

图 1：合成小半径稳健性敏感性曲线。(a) Erdős–Rényi模型与双块随机块模型测试，参数为 $n = 400$, $c = 3$, $\lambda = 0.4$：归一化超额稳健分类错误概率 $(R_{\mathrm{rob},\,n}(C) - R_{0,\,n})/(\sqrt{2R_{0,\,n}(1 - R_{0,\,n})}\sqrt{C})$ 随 $\sqrt{C}$ 的变化。(b) 平均度为 $1 - \Delta$ ($n = 5000$, $\Delta = 0.2$) 的泊松度配置模型：归一化超额稳健易感性 $(\rho_{\mathrm{rob},\,n}(C) - \rho_{0,\,n})/(\rho_{0,\,n}\sqrt{C})$ 随 $\sqrt{C}$的变化。虚水平线标示定理 S.2（面板 a）和定理 3.3（面板 b）所预测的首项系数对应的参考水平。

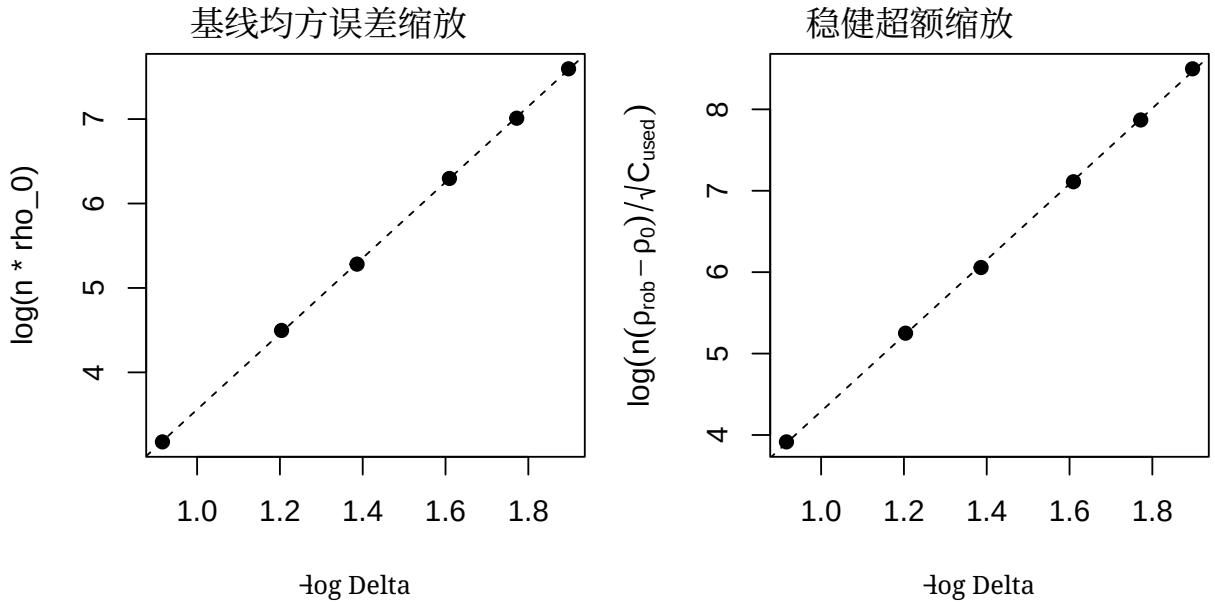

图2：配置模型易感性：距临界点的距离的对数–对数缩放。左图：$-\log\,\Delta \mapsto \log(n\,\rho_{0,n})$及拟合的最小二乘直线（虚线）；右图：$-\log\,\Delta \mapsto \log\big(n(\rho_{\mathrm{rob},n}(C)\,-\rho_{0,n})/\sqrt{C}\big)$ 在 $C \approx 10^{-3}$处。回归斜率 $\widehat{\kappa}_{\mathrm{base}} \approx 4.49$ 和 $\widehat{\kappa}_{\mathrm{rob}} \approx 4.65$ 接近定理 3.3中的理论指数4。

	基线指数	稳健指数
配置模型易感性（$n = 5000$）	4.49	4.65

表1：在配置模型实验中，对 $-\log\,\Delta \mapsto \log(n\,\rho_{0,n})$和 $-\log\,\Delta \mapsto \log\big(n(\rho_{\mathrm{rob},n}(C) - \rho_{0,n})/\sqrt{C}\big)$的估计斜率，针对 $\Delta \in \{0.40, 0.30, 0.25, 0.20, 0.17, 0.15\}$ 和 $C \approx 10^{-3}$。理论预测二者具有共同指数4；经验估计值 $\widehat{\kappa}_{\mathrm{base}}$ 和 $\widehat{\kappa}_{\mathrm{rob}}$ 接近这一数值。

合成实验 C：模型错设压力测试（真实模型为度修正随机块模型，工作模型为随机块模型）。我们基于度修正随机块模型（DCSBM）生成了网络，该模型具有温和的社区结构但存在强烈的度异质性，随后拟合了一个设定错误的普通随机块模型。我们聚焦于主特征值 λ_1（以及相关的流行病阈值代理指标），并通过对后验抽样进行指数倾斜来实施 KL散度球稳健化。

为了在非平凡情形下校准阈值决策 Intervene$\{\mathbb{P}(\lambda_1 > \tau) > p_\star\}$，我们通过试点程序设定 τ，将其限制在工作后验支持集内：$\tau = \min\{q_{0.60}(\lambda_{1,\,\mathrm{true}})\;\; q_{0.98}(\lambda_{1,\,\mathrm{work}})\}$。在试点中，真实的超越概率很大，而工作后验基本将其排除在外，这表明存在严重的模型设定错误。由于 KL 倾斜只能对工作模型抽样重新加权，因此无法在基线后验分配（近乎）零概率的地方创造支撑；试点上限缓解了这种退化问题。

表 2：试点校准展示了事件 $\{\lambda_1 > \tau\}$ 的模型设定错误。

量	值	解释
$\tau_{\text{truth}} = q_{0.60}(\lambda_{1,\ \text{true}})$	10.274	目标非平凡真实情形
$\tau_{\text{cap}} = q_{0.98}(\lambda_{1,\ \text{work}})$	10.041	截断至工作后验支持集
选定的 $\tau = \min(\tau_{\text{truth}},\ \tau_{\text{cap}})$	10.041	决策中使用的阈值
$P_{\text{true}}(\lambda_1 > \tau)$（试点）	0.67	度修正随机块模型下的频繁超越
P_{work}（$\lambda_1 > \tau$）（试点）	0.02	工作随机块模型几乎排除了超阈值事件
$p_\star$ =成本$_{\text{int}}$/成本$_{\text{out}}$	0.20	决策概率阈值

图 3 显示，增大 KL 半径 C 会使鲁棒化后验向 λ_1 较大的取值移动，并且相较于度修正随机块模型的真实值，显著降低均方误差（MSE），这与随机块模型后验因忽略度异质性而产生向下偏差的情况一致。对于阈值策略，稳健化在半径适中的情况下可降低遗憾，因为它对模型设定错误的工作后验所导致的假阴性进行防范。

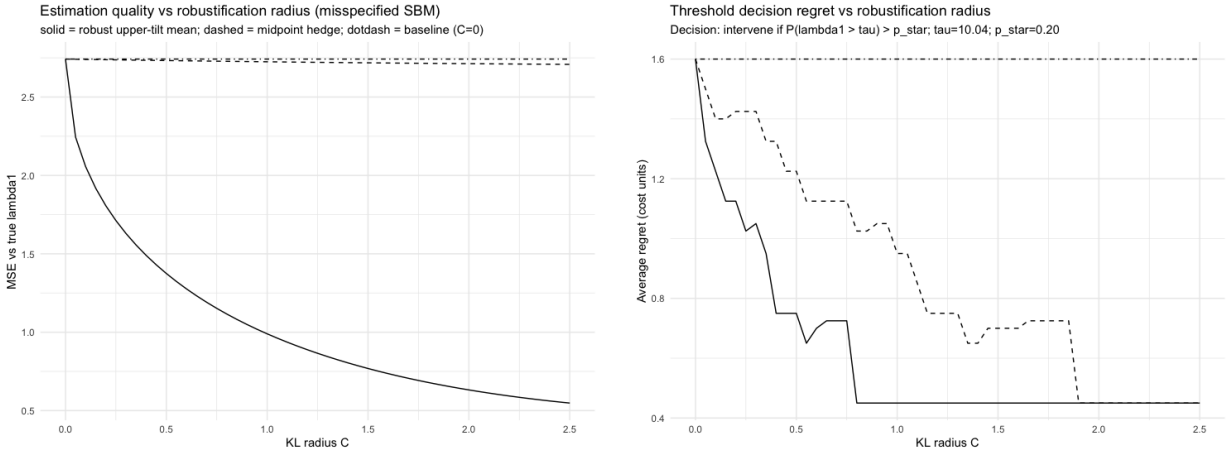

图3：**模型错设压力测试（真实模型为度修正随机块模型，工作模型为随机块模型）**。通过在工作后验抽样周围的 KL 球内进行指数倾斜来实现稳健化，KL球的半径为 C。左图：对于 λ_1，估计性能（均方误差）随 KL 半径 C 的变化。右图：阈值决策遗憾随 KL 半径 C 的变化；稳健化通过防范随机块模型设定错误下的假阴性来降低遗憾。

合成实验D：半径路径与误差指数（Erdős–Rényi模型与随机块模型）。我们针对带标签的稀疏 Erd˝os–R´enyi 模型与双块随机块模型的检验，提供更多数值证据，以支持第 4 节的信息论结论：只有在 KL 半径确实局部取值时，稳健化风险才满足局部小半径展开，而半径路径 $\mathcal{C}_n$ 决定了鲁棒性会保留还是破坏指数级错误衰减。

对于每个 n 和信号强度 λ，我们在 H_0（ER）和 H_1（$p_{\text{in}} = (c+\lambda)/n$ 和 $p_{\text{out}} = (c-\lambda)/n$的平衡两块随机块模型）下模拟带标签稀疏图，采用等先验下的贝叶斯决策规则，并记录后验误分类概率 $e_0(G_n)$。随后，我们在半径为 C 的KL球内对后验分布进行鲁棒化，并计算相应的最坏情况误分类概率 $e_{\text{rob}}(C;\ G_n)$（双点情形；通过伯努利KL约束精确求解）。

局部小半径区域（面板 *a*）。面板 (a) 报告重复归一化量

$$\mathbb{E}\left[\frac{e_{\mathrm{rob}}(C;G_n)-e_0(G_n)}{\sqrt{2\,e_0(G_n)\big(1-e_0(G_n)\big)}\,\sqrt{C}}\right],$$

在局部 $\sqrt{C}$ 展开下，对于每个固定的（$n,\ \lambda$），它等于 $1+o(1)$，其中 $\overline{C}\downarrow 0$。对于中等信号（$\lambda=0.2$），在图示的最小半径范围内，归一化因子仍接近 1：对于 $n=200$，它在 $\sqrt{C}\in[0.002,0.03]$ 上介于 1。0006 和 1。0087 之间；对于 $n=800$，介于 1。0035 和 1。0488 之间；对于 $n=1600$，在图示网格范围内则低于 1。28。相比之下，对于更强的信号和更大的 n，同一 $\sqrt{C}$ 网格相对于后验分布变得非局部：对于 $\lambda=0.4$，该比值在 $n=200$ 时约为 1。00–1。05，在 $n=400$ 时增至 1。02–1。29，在 $n=800$ 时增至 1。63–6。95，随后在 $n=1600$ 时飙升至 1.2×10^{3}–1.4×10^{4}。这是稀有错误区域，此时 $e_0(G_n)$ 已经极小，因此要使局部展开在决策层面适用，“小半径”必须随着 n（以及信号）而缩小。

错误指数与半径路径（*B–C* 面板）。面板 (B) 绘出了经验指数估计 $-\log(R)/n$，其中 $R=\mathbb{E}[e(G_n)]$，分别对应基准贝叶斯风险和指数收缩半径路径 $\mathcal{C}_n=\exp(-2\alpha n)$。从定量结果看，对于 $\lambda=0.2$，当 n较大时，基线指数与指数半径鲁棒指数基本无法区分：在 $n=6400$ 处，二者分别为 0。0012021（基线）和 0。0012008（稳健）；在 $n=12800$处，分别为 0。0014373523（基线）和 0。0014372875（稳健）。对于 $\lambda=0.1$，在 $n=12800$处，较大-n 时对应的数值分别为 3.568×10^{-4}（基线）和 3.430×10^{-4}（稳健），相对差距约为 4%。对于 $\lambda=0.3$，基线与稳健结果在 $n=6400$ 之前都十分接近（二者均为 $\approx2.654\times10^{-3}$）；而在最大的 n处，基线指数估计的波动明显增大（例如在 $n=12800$处为 0。00448），这与风险极小时出现的有限样本/蒙特卡洛不稳定性相符；稳健指数则保持稳定，约为 2.69×10^{-3}。在所有 λ中，稳健指数都不超过基线指数，这与第 4 节所预测的稳健化无法提升信息指数这一事实一致。

图（C）比较了 $\lambda=0.2$下的几种半径缩放。指数小半径保留了指数衰减：在 $n=12800$时，基线具有 $R\approx5.40\times10^{-9}$，速率为 0。0014873；而$\mathcal{C}_n=\exp(-2\alpha n)$得到 $R\approx5.41\times10^{-9}$，速率为 0。0014872（指数的有效数字前四位一致）。相比之下，多项式/常数半径会产生次指数行为，并导致每节点指数趋于零：在 $n=12800$时，常数半径区域具有 $R\approx1.93\times10^{-3}$，速率为 4.88×10^{-4}；而 κ/n 区域具有 $R\approx4.02\times10^{-6}$，速率为 9.71×10^{-4}。区域 $\mathcal{C}_n\propto n$会使 KL 预算达到饱和，并得到 $R_{\mathrm{rob}}\approx1$（速率为 0），可作为合理性检查。

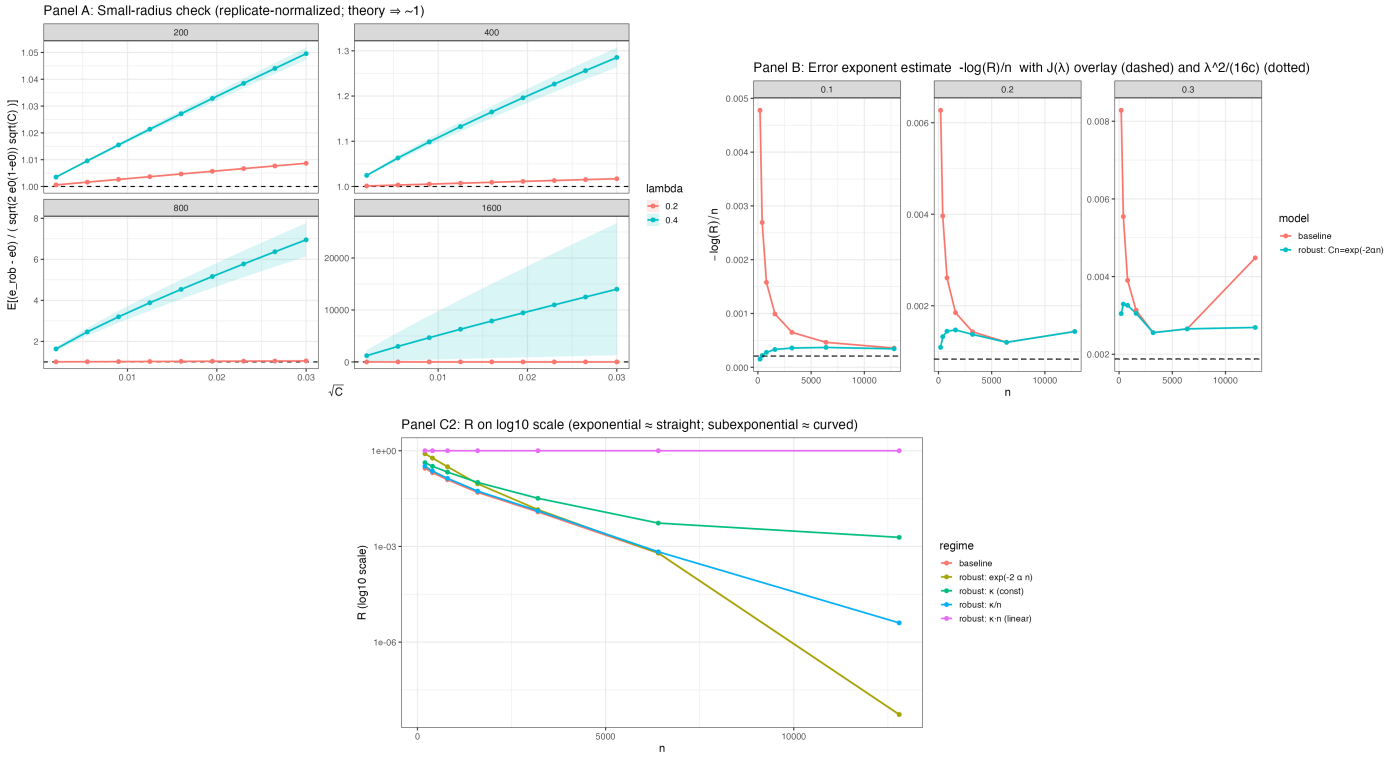

图 4：A）左上：局部 $\sqrt{C}$ 归一化。较大的 n和较强的 λ处出现偏差，表明半径网格并非局部。B）右上：基线和 $\mathcal{C}_n = \exp(-2\alpha n)$的指数估计 $-\log(R)/n$ 与 n 的关系。C）下方：不同半径缩放下的有效指数（多项式/常数半径下指数坍缩）。合成 ER 与随机块模型对局部性及指数行为的验证，采用后验 KL散度稳健化。关键的定性预测是，指数收缩半径可以保留指数速率，而多项式/常数半径会破坏该指数。

7.2 实验 2：脑连接网络中的鲁棒网络泛函与模型选择

数据与工作模型。 我们考虑一个病例对照研究中的静息态功能连接网络群体。对于 n_{subj} 名个体，我们观测到 m次扫描；每次扫描均表示为一个无向无权图，图中包含一组共同的 p 个脑区（节点），这些图通过对区域时间序列之间的绝对成对相关性进行阈值化而得到。

对于每次扫描, 我们比较两个密切相关的随机块模型 （SBM）工作模型,

$$\mathcal{M}_1 = \text{SBM}(K_1), \qquad \mathcal{M}_2 = \text{SBM}(K_2),$$

分别具有 $K_1 = 2$ 和 $K_2 = 3$ 个块。模型 $\mathcal{M}_k$ 的参数为 $\theta_k = (\pi^{(k)}, B^{(k)})$，其中 $\pi^{(k)}$ 为社区比例， $B^{(k)}$ 为一个表示社团内及社团间边概率的 $K_k \times K_k$ 矩阵。我们为每个 k 的 $(\pi^{(k)}, B^{(k)})$ 赋予简单的共轭先验，并通过贝叶斯信息准则近似计算 $\mathcal{M}_k$ 的边际似然。

为避免两个随机块模型的拟合效果几乎相同时后验权重退化，我们采用基于温度化贝叶斯信息准则的伪后验,

$$w_k \propto \exp\Big\{-\tfrac{1}{2}\,\tau\,\text{BIC}(\mathcal{M}_k)\Big\}, \qquad k = 1, 2,$$

温度为 $\tau = 0.25$。对 $\boldsymbol{w} = (w_1,\ w_2)$ 进行归一化，可得到基线后验模型概率 $p_k = \Pi_0(M = \mathcal{M}_k \mid \text{扫描})$，$k = 1,\ 2$。

网络泛函与决策。对于每次扫描和每个模型 $\mathcal{M}_k$，我们考虑网络泛函向量

$$R_k(\theta_k) = \big(C_k(\theta_k),\, L_k(\theta_k),\, S_k(\theta_k),\, \lambda_{1,k}(\theta_k)\big),$$

其中

- $C_k(\theta_k)$ 是全局聚类系数，
- $L_k(\theta_k)$ 是平均最短路径长度，
- $S_k(\theta_k)$ 是小世界指数，例如 $S_k = (C_k/C_{\text{随机}})/(L_k/L_{\text{随机}})$，其中 $(C_{\text{随机}}\ L_{\text{随机}})$ 是根据简单随机参考图计算得出的，并且
- $\lambda_{1,\ k}(\theta_k)$ 是期望邻接矩阵的主特征值。

我们研究两个决策：

1. 一个 模型选择决策 $a \in \{\text{SBM}(K_1),\text{SBM}(K_2)\}$，采用 0–1 损失，其中基线贝叶斯行动选择温度化后验权重较大的 SBM p_k；以及

2. 一个 泛函分类决策，例如判断 $S_k(\theta_k) > S_0$ 是否超过预先指定的阈值 S_0，并将其解释为小世界结构的证据。

对于每次扫描，我们使用 (M, θ_M) 上的联合基线后验 Π_0，并计算上述决策对应的后验风险 $\rho_0(a)$。

鲁棒性设置。对于脑部实验，我们将注意力限制在Π_0的 KL邻域内。对于给定的 KL半径 $C > 0$，我们考虑不确定集

$$\mathcal{U}_C(\Pi_0) = \big\{\tilde{\Pi} : \mathrm{KL}(\tilde{\Pi} \,\|\, \Pi_0) \le C\big\},$$

˜并针对每个动作 a计算最不利的熵倾斜 Π_C。由此得到稳健后验风险

$$\rho_{\text{rob}}(C, a) = \sup_{\tilde{\Pi} \in \mathcal{U}_C(\Pi_0)} \mathbb{E}_{\tilde{\Pi}}\big[L(a, \theta_M, M)\big].$$

对于模型选择决策，我们记录贝叶斯选择在 Erdős–Rényi模型(K_1) 和 Erdős–Rényi模型(K_2) 之间发生变化时的切换半径 $C^\star$，以及归一化的小半径敏感性曲线 $C \mapsto \{\rho_{\text{rob}}(C,\ a) - \rho_0(a)\}/\sqrt{C}$。

在 $n_{\text{scan}} = 124$ 次扫描中，观测到的网络呈现出显著的小世界结构（表 3）。聚类系数较高（中位数 $C = 0.381$），平均路径长度较短（中位数 $L = 1.850$），小世界指数 S 通常约为 1。6。邻接矩阵的主特征值也相当大，中位数为 $\lambda_1 \approx 56$。

更灵活的随机块模型(K_2)模型所占的温度化后验概率质量相当可观，但并未达到极端程度：温度化概率中位数为$p_{\text{SBM}(K_2)\ \tau} = 0.724$，四分位距为 $[0.683,\ 0.788]$。稳健模型选择则更为微妙。切换半径 $C^\star$ 的中位数为0.112，四分位距为 $[0.072,\ 0.201]$，这意味着大约一半的扫描中，只需对

pos后验分布（按 KL 距离衡量）进行相对较小的扰动，就足以改变首选的块数 .

图 5 （左）展示了一个代表性扫描的归一化稳健性敏感性曲线。在一定范围的 C内，该曲线接近理论上的小半径斜率，表明在此示例中，局部渐近理论提供了良好的近似。图 5 右侧面板绘出了观测到的小世界指数 S 与三块 SBM 的温度化后验概率之间的关系；小世界行为更极端（ S 值更大）的扫描往往在 SBM(3) 上具有更高的后验质量，尽管变异不可忽略。

图 6 通过绘制每个网络的（C、 L）来概括扫描层面的小世界性质，并依据首选随机块模型（K_1 与 K_2）进行着色。几乎所有扫描结果都位于聚类程度高且路径较短的区域，并且两个随机块模型生成的网络在整体函数方面大体相似。因此，稳健性计算所探究的是一个微妙的模型选择问题——除了两块划分之外，究竟还需要多少额外结构才能解释连通性数据——而不是对 SBM 模型族的明显不匹配。

表3：脑连接实验：网络泛函、温度化模型概率及跨 $n_{\mathrm{scan}} = 124$ 次扫描的鲁棒性摘要。各项数值为扫描间的中位数 [第一四分位数、第三四分位数]。

数量	中位数 [Q1、Q3]
全局聚类 C	0.381 [0.357, 0.412]
平均路径长度 L	1.850 [1.821, 1.872]
小世界指数 S	1.645 [1.547, 1.710]
主特征值 λ_1	56.1 [50.9, 63.6]
温和的 $p_{\mathrm{SBM}(K_2)\,\tau}$	0.724 [0.683, 0.788]
切换半径 $C^{\star}$	0.112 [0.072, 0.201]

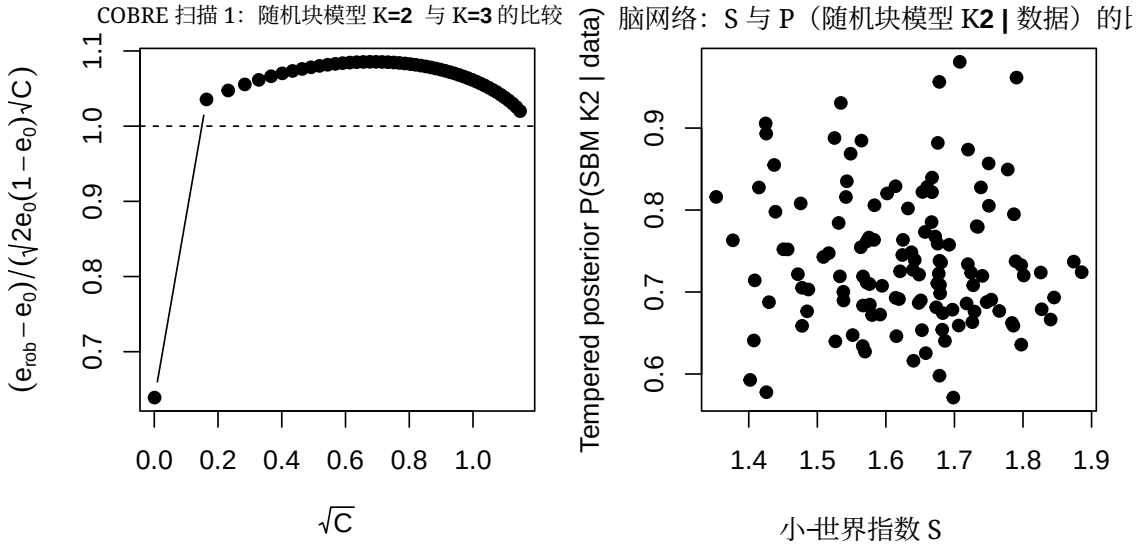

图5：脑连接实验，随机块模型(K_1)与随机块模型(K_2)。左侧：代表性扫描中模型选择决策的归一化稳健风险增量（$\rho_{\mathrm{rob}}(C)-\rho_0$）$/\sqrt{C}$，绘制为相对于$\sqrt{C}$的变化。右侧：观测到的小世界指数 S 与温度化后验概率$p_{\mathrm{SBM}(K_2)\,\tau}$ 在各次扫描中的关系。

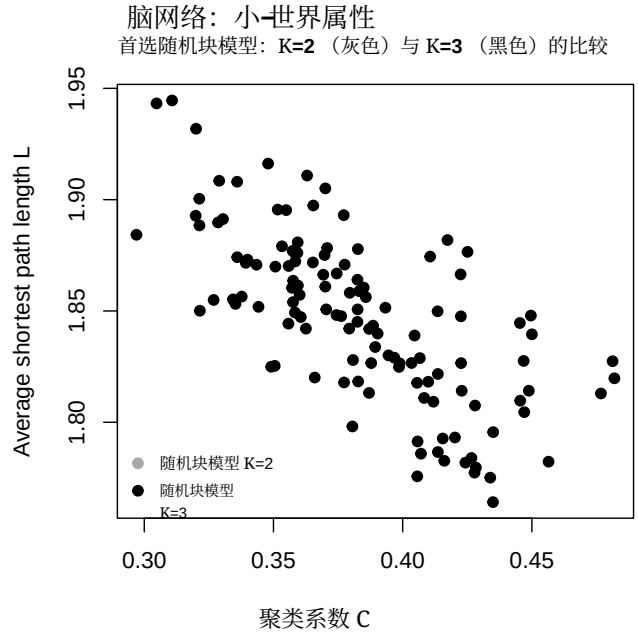

图6：脑连接实验：所有扫描的全局聚类 C 与平均路径长度 L 。数据点按温度化后验分布下的首选随机块模型着色（较浅的点偏向随机块模型(K_1)，较深的点偏向随机块模型(K_2)）。

随机块模型与潜在空间随机点积图模型的比较。 为了检验这些结论并非仅仅依赖于对关系密切的随机块模型进行比较，我们还将三块 SBM 与一个

潜在维度为 $d = 3$ 的随机点积图（RDPG）工作模型，其维度与随机块模型区块的数量相匹配。对于每次扫描，我们在其上计算基于温度化贝叶斯信息准则的伪后验

$$\{M = \mathrm{SBM}(K = 3),\ M = \mathrm{RDPG}(d = 3)\},$$

采用与上文相同的温度调整方案，然后构造 0–1 损失模型选择风险 $\rho_0(a)$及其 KL 鲁棒化。与模棱两可的 SBM(2) 与 SBM(3) 对比不同，潜在空间模型明显处于劣势：在全部 124 次扫描中，随机内积图模型的温度化后验概率质量在数值上几乎为零（$p_{\mathrm{RDPG}} \ll 10^{-40}$，通常会下溢至零），因此，以机器精度计算，三块 SBM 被选中的概率为 1。由于每次扫描中的基线误分类风险实际上都为零，相应的切换半径 $C^\star$ 均取相同的值 $C^\star \approx 6.21$，即根据闭式表达式，将伯努利风险从 $e_0 = 10^{-6}$ 变为 $1/2$ 所需的 KL 距离 $C^\star(e_0) = \mathrm{KL}(\mathrm{Bern}(1/2) \,\|\, \mathrm{Bern}(e_0))$。换言之，必须大幅偏离基线后验分布（远远超出我们理论所考虑的局部模型错设范围），随机内积图模型才可能成为最优选择。图 7左图显示，代表性扫描的归一化鲁棒性曲线基本上平坦且为零，反映出这种近乎退化的模型选择；右图则证实，即便对于小世界行为最显著的扫描，随机内积图模型的后验质量仍接近于零。图 8 还显示，按首选模型（SBM 或随机内积图模型）对点着色时，(C, L)点云几乎没有变化，进一步说明 SBM 模型族已经能够捕捉这些网络的全局功能结构。加入潜在空间并不能在边际似然或稳健风险方面带来有竞争力的替代模型。

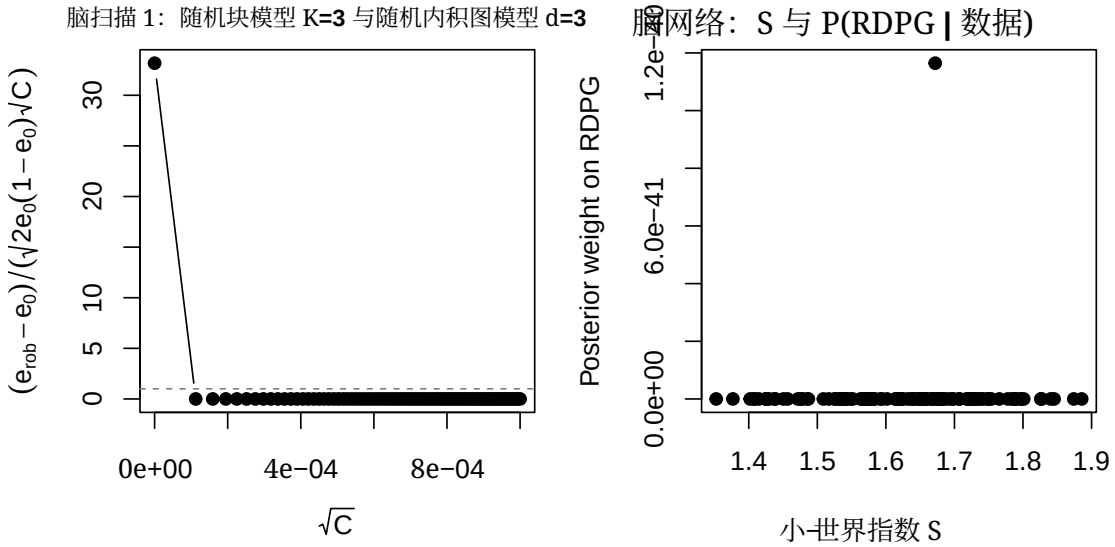

图 7：脑连接实验，SBM(3) 与 RDPG($d = 3$)。左：代表性扫描中模型选择决策的归一化稳健风险增量，绘制为相对于 $\sqrt{C}$ 的函数。该曲线基本平坦于零，反映出基线误分类风险趋于消失。右：跨扫描的观测小世界指数 S 与温度化后验概率 p_{RDPG}；对于所有网络，RDPG 上的后验质量在数值上都可以忽略不计。

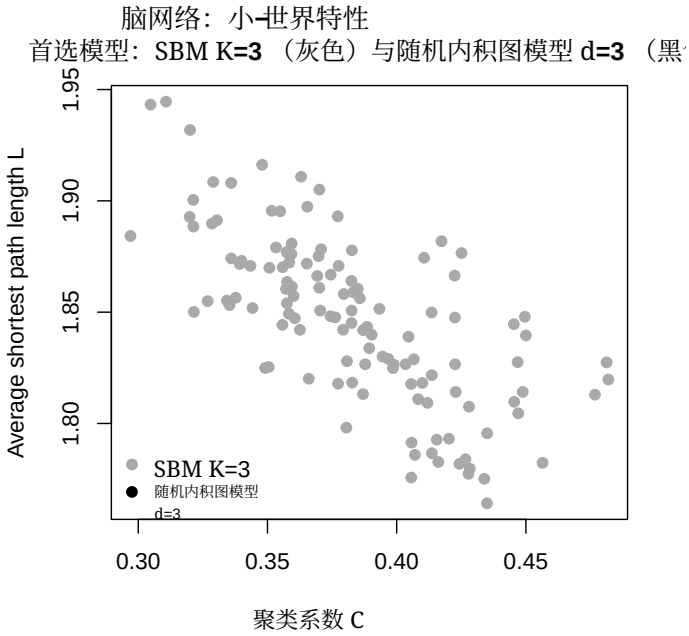

图 8：脑连接实验：所有扫描的全局聚类 C 与平均路径长度 L，按温度化后验下的首选模型着色（较浅的点偏向随机内积图模型(d =3)，较深的点偏向 SBM(3)）。几乎所有扫描都落在高聚类、短路径区域，并且绝大多数都支持三块 SBM。

7.3 实验 3：卡纳塔克邦村庄网络中的稳健结构与同配性

数据与工作模型。 我们使用来自印度卡纳塔克邦农村地区的第 1 波村庄社会网络数据。每个村庄 v 生成一个无向、无权重的家庭层面网络 G_v。节点代表家庭；如果家庭报告至少有一种社会互动（借贷、提供建议、社交拜访等），则相应两节点之间存在一条边。对于每个村庄，我们将所有互动层汇总为一个网络。在这 $n_v = 75$ 个村庄中，家庭数量约为 350 至 1,800。网络稀疏，但聚类程度很高（表4）：全局聚类系数中位数为 $C = 0.375\,[0.343, 0.429]$，平均最短路径长度的中位数为 $L = 4.10\,[3.91, 4.36]$，由此得到的小世界指数较大，为 $S = 30.3\,[25.5, 37.2]$。邻接矩阵主特征值的中位数为 $\lambda_1 = 15.9\,[14.4, 18.9]$。

对于每个村庄网络，我们考虑两种工作模型：

1. 边概率为 p_v的稀疏 Erd˝os–R´enyi 模型；以及

2. 一个具有固定块成员关系 $z^{(v)}$ 的三块随机块模型（SBM），该成员关系通过对 G_v 进行基于模块度的聚类得到，块级连接概率为 $B^{(v)}_{kl}$ 。

在这两种情况下，我们都对边概率（以及$B^{(v)}$中的各个条目）设置独立Beta先验，并逐个村庄进行后验计算。作为SBM类中的鲁棒性检验，我们还将谱随机块模型与 $K = 2$ 和 $K = 3$ 块进行比较；这得出了非常相似的Watson–Holmes结论（图10），这里只作简要报告。

网络泛函与决策。 我们从村庄 v的SBM中提取块层级连接矩阵 $B^{(v)}(\theta)$ 以及两个同配性度量：

- 块内与块间密度差异 $\Delta_{(v)}(\theta) = B_{(v)\text{ 块内}} - B_{(v)\text{ 块间}}$；以及 — —
- 相对于所选划分的模块度 $Q_{(v)}(\theta)$。

在各村庄中，后验点估计 $\hat{\Delta}^{(v)}$ 较小且为正，中位数为 $\hat{\Delta}^{(v)} \approx 0.011\,[0.009, 0.013]$（图 9a），表明块结构较弱。对于谱随机块模型分析，相应的差异更小（中位数为 $0.003\,[0.002, 0.004]$）。

我们将其表述为一个二元决策

$$a^{(v)}_{\text{struc}} = \begin{cases} \text{“strong assortativity”} & \text{if } \Delta^{(v)}(\theta) > \Delta_0, \\ \text{“weak/none”} & \text{otherwise,} \end{cases}$$

阈值为 $\Delta_0 = 0.10$，损失函数可以是对 $\Delta^{(v)}$ 的 0–1 损失或平方损失。为评估骨干结构，我们使用随机块模型计算每个家庭的期望度，并对每次后验抽样，衡量度数最高的前 $K = 10$ 个家庭所占的总期望度比例。如果该比例超过 50%，则将村庄归类为具有集中型 骨干结构；否则归类为分散型 。

稳健性分析与结果。 对于每个村庄，我们分别在 ER 和三块 SBM 下计算基线后验分布 $\Pi_0^{(v)}$ ，基于温度调整贝叶斯信息准则构建 ER、SBM}的模型后验分布，并针对三个决策问题计算贝叶斯行动和后验风险 $\rho_0^{(v)}$ ：(i) 模型选择（ER 与 SBM），(ii) 强同配性与弱同配性，以及 (iii) 集中型骨干与弥散型骨干。随后，我们构建 KL 球 $\mathcal{U}_C(\Pi_0^{(v)})$，并针对网格 $C \in [10^{-4}, 10^{-1}]$评估最不利倾斜后验分布 $\tilde{\Pi}_C^{(v)}$ 及相应的稳健风险 $\rho^{(v)}{}_{\text{rob}}(C)$。

温度调整后的模型后验分布在每个村庄中都以压倒性优势偏好 SBM，而非 ER。ER 上的后验质量在数值上与零无法区分；代表性村庄的 Watson–Holmes 敏感性曲线始终远低于单位斜率参考线（图 9c），在所考察的半径网格内没有发生模型切换。与此同时，SBM 后验分配给“强同配性”（$\Delta^{(v)} > \Delta_0$）或集中型骨干的质量几乎为零：所有村庄的贝叶斯决策都是“弱/无”和“弥散”，相应的后验错误概率实际上为零。因此，对于任何村庄，Watson–Holmes 稳健风险都不会在 $C \in [10^{-4}, 10^{-1}]$ 上引发决策变化，所以隐含的切换半径 $C_\star^{(v)}$均大于 0。1（在绝对连续性约束下形式上为无穷大）。

总之，卡纳塔克邦村庄网络呈现出显著的小世界结构，但块同配性仅十分微弱，也没有证据表明存在高度集中的骨干网络。在对工作模型进行局部 KL 扰动后，这些定性结论仍表现出惊人的稳定性；相比之下，在其他实验中，同样的 Watson–Holmes 分析揭示了近临界敏感性。

表 4：卡纳塔克邦村庄网络摘要。数值为各村庄的中位数 [四分位距] 跨越$n_v = 75$ 。

	C	L	S	λ_1
值	$0.375\,[0.343, 0.429]$	$4.10\,[3.91, 4.36]$	$30.3\,[25.5, 37.2]$	$15.9\,[14.4, 18.9]$

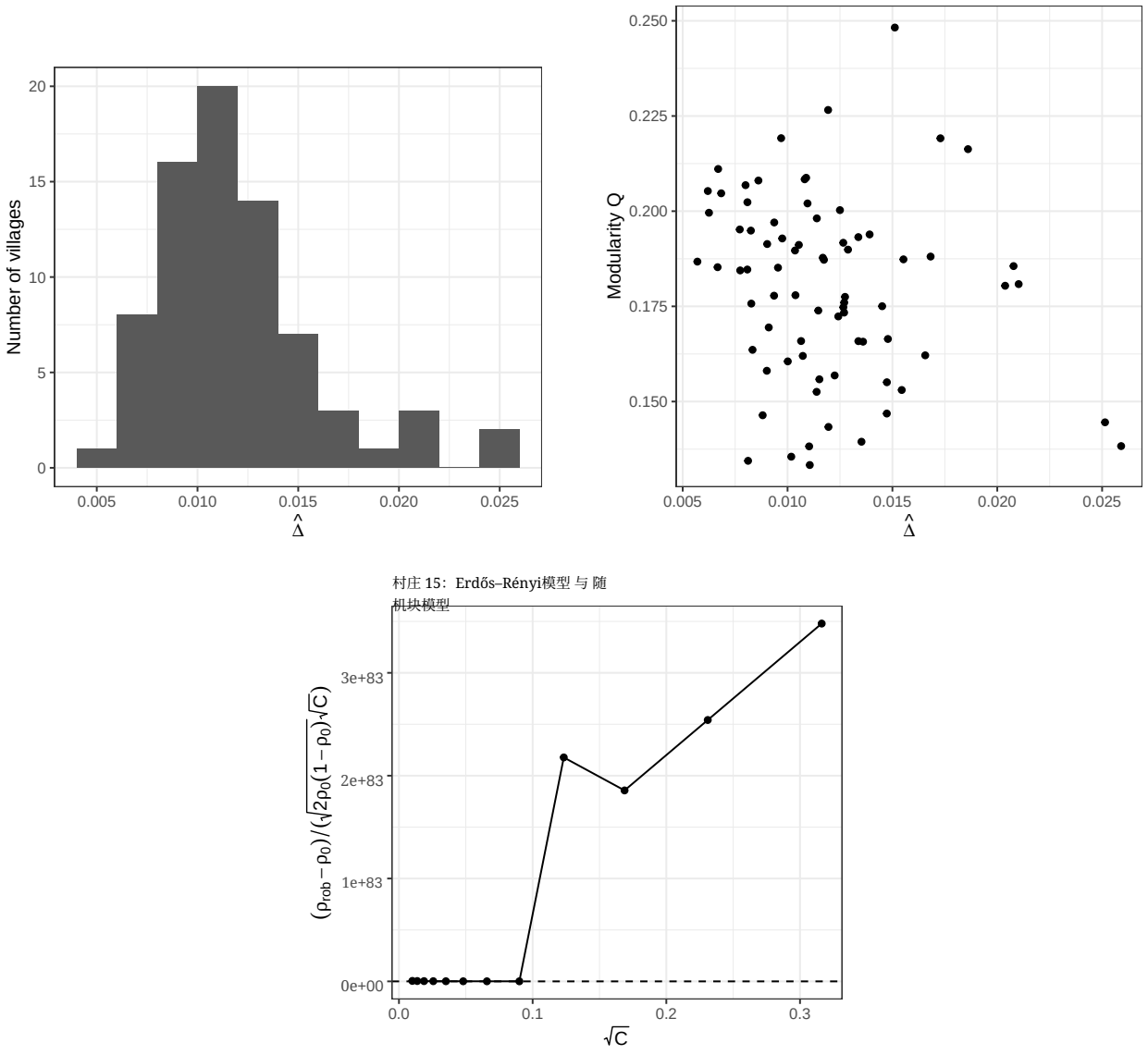

图9：卡纳塔克邦村庄网络，Erdős–Rényi模型与三块 SBM。(a) 各村庄的 SBM 同配性对比值 $\hat{\Delta}^{(v)}$ 分布。(b) 推断分区的 $\hat{\Delta}^{(v)}$ 与模块度 $Q^{(v)}$ 之间的关系。(c) 代表性村庄的沃森–霍姆斯归一化敏感性曲线，比较 Erdős–Rényi模型与 SBM；该曲线始终远低于单位斜率参考线，且在网格 $C \in [10^{-4}, 10^{-1}]$上没有发生模型切换。

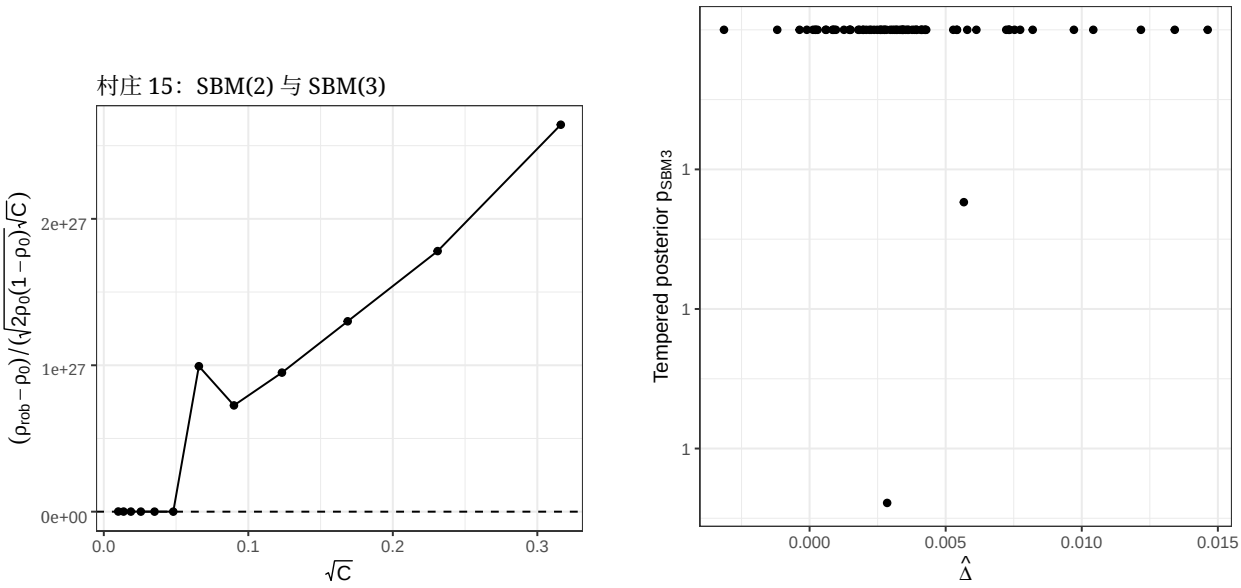

图 10：谱随机块模型鲁棒性检验。比较各村庄中的 $K = 2$ 和 $K = 3$ 谱随机块模型。温度调整贝叶斯信息准则始终偏好三块模型，而 Watson–Holmes 敏感性分析再次表明，在网格 $C \in [10^{-4}, 10^{-1}]$ 上没有决策切换。

基于观测协变量的同配性。 最后，我们用基于协变量定义的区块替代基于度的区块，分别针对性别、种姓和宗教构建随机块模型。对于每个村庄 v 和每种属性，我们根据家庭层面该属性的主导取值形成区块，并按照基线分析中的方法进行 Erdős–Rényi模型与随机块模型的比较。所得同配性对比值较小且略为负：各村庄的后验点估计中位数 $\hat{\ }\hat{\ }\hat{\ }$ 分别为 $\Delta_{\text{gender}} = -0.0054\,[-0.0068, -0.0043]$、$\Delta_{\text{caste}} = -0.0059\,[-0.0073, -0.0044]$ 和 $\Delta_{\text{religion}} = -0.0054\,[-0.0067, -0.0042]$，表明这些协变量所对应的是轻微的异配性，而非强烈的群体内聚类。

尽管如此，在所有村庄中，温度调整贝叶斯信息准则都明确地偏向基于协变量的随机块模型，而非齐性 ER 模型（温度化模型概率中位数 Pr(SBM | data) ≈ 1），因此，即使特定观测属性的同配性较弱，“需要某种偏离 ER 的结构化变化”这一结论仍然稳健。

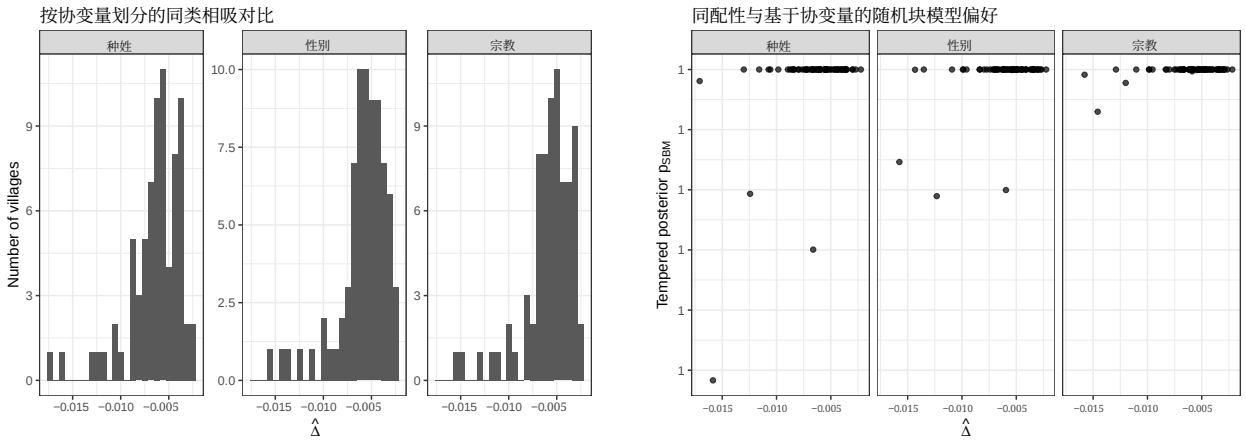

图 11：卡纳塔克邦村庄网络，基于协变量的随机块模型。左：基于性别、种姓和宗教的随机块模型的同配性对比度 $\hat{\Delta}^{(v)}$ 的分布。右：$\hat{\Delta}^{(v)}$ 与温度化后验模型概率 p_{SBM}的关系，表明即使估计的对比度接近于零或略为负值，随机块模型仍明显优于Erdős–Rényi模型。

潜在空间鲁棒性：随机块模型与随机内积图模型的比较。为了检验上述块模型结论是否只是随机块模型参数化造成的假象，我们还对每个村庄 v比较了三块随机块模型与 $d = 3$ 通过邻接谱嵌入拟合的随机点积图（RDPG）；后者是一个维度高得多的潜在空间模型。与脑部实验一样，我们通过贝叶斯信息准则近似边际似然，并在{随机块模型、随机内积图模型} 之间构造温度为 $\tau = 0.25$ 的温度化伪后验。在所有 $n_v = 75$ 村庄中，潜在空间模型的温度化后验概率质量几乎为零：RDPG 的温度化概率中位数为 $\tilde{p}_{\mathrm{RDPG}} = 0$ ，四分位距为 $[0, 0]$, ，且基线贝叶斯行动始终选择随机块模型。对于这一随机块模型与 RDPG 之间的决策，决策论稳健性切换半径均处于稳健性下限所决定的下界（$C^\star \approx 2.8$），远超本节其他部分所考察的半径，因此，要使 RDPG 具有竞争力，需要极大的 KL 扰动。图12 显示，小世界指数 S 与$\tilde{p}_{\mathrm{RDPG}}$不存在可辨别的关联，而且在整个（$C$， L）小世界范围内，每个村庄的首选模型都是随机块模型。因此，在这一高信号场景中，建模的主要问题是是否要摆脱齐性（ER）；一旦允许存在块结构，进一步提高潜在空间的灵活性对稳健结论几乎没有影响。

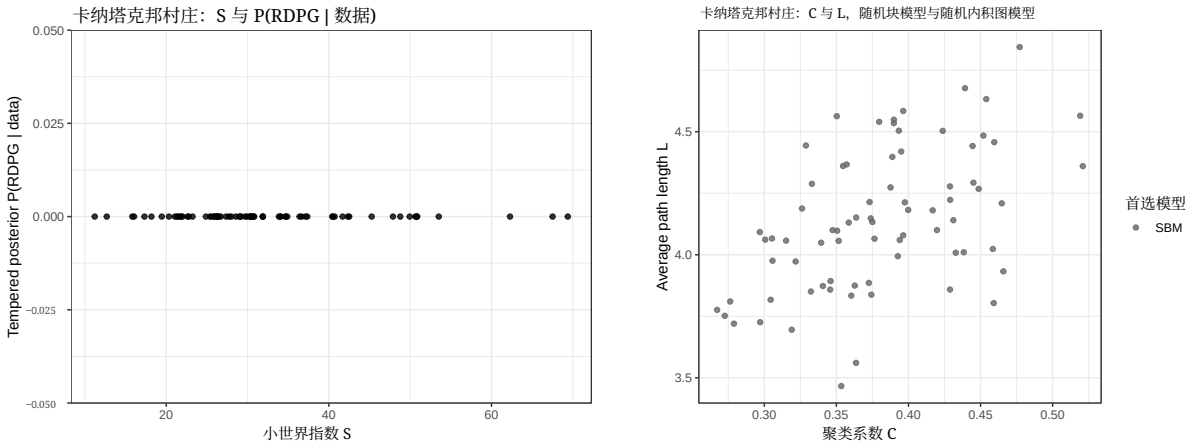

图 12：卡纳塔克邦村庄网络：随机块模型与随机内积图模型。左侧：小世界指数 S 与温度化后验概率 $\tilde{p}_{\mathrm{RDPG}} = \Pr(\mathrm{RDPG} \mid \text{数据})$；所有村庄对潜在空间模型的赋予概率质量基本为零。右侧：全局聚类 C 与平均路径长度 L，点的颜色表示首选模型；所有村庄均选择三块 SBM。

8 讨论

我们构建了一个决策理论框架，用于评估贝叶斯网络分析对工作模型局部模型设定错误的敏感程度。该框架以 Watson–Holmes 鲁棒性概念为出发点：在参考后验的一个较小 Kullback–Leibler 邻域内，使动作的最坏情形后验期望损失最小。我们将这一视角具体应用于可交换网络模型，以及由网络泛函驱动的决策。通过结合图子极限、经典渗流理论和随机图渐近理论，该框架既带来概念层面的洞见，也为鲁棒网络推断提供了具体的信息论极限。

在网络泛函层面，我们证明，当决策依赖于配置模型中的易感性、基于渗流的稳健性指标、图子上的 SIS 噪声指数或谱间隙等量时，决策论稳健化的稳健后验风险具有精确的小半径展开。在平方损失下，首要膨胀项由损失的后验方差控制，并与散度半径的平方根成正比。在接近碎裂阈值或流行病阈值时，稳健性指标本身大致按距临界点的距离的倒数发散，这些展开揭示了一种普适的临界行为：决策层面不确定性的膨胀速率对应于距临界点的距离的倒数四次方。因此，随着网络接近相变，基于稳健性泛函的决策会变得比泛函本身更加不稳定，而且这种不稳定性可以量化。

在信息论方面（第 4 节），我们分析了稀疏 Erd˝os–R´enyi 图与双区块随机区块模型之间的决策理论稳健模型选择问题，既研究了带标签形式，也通过稀疏图子进行了研究。我们推导出了显式的每顶点信息和鲁棒性噪声指标 $I(\lambda)$ 与 $J(\lambda)$，它们决定了局部扰动下贝叶斯因子误差的指数衰减。通过将这一两点实验嵌入广泛的稀疏图非参数类——包括配置模型和稀疏图子类——我们建立了相匹配的决策理论极小极大下界。一旦要求对局部 KL 扰动具有鲁棒性，任何贝叶斯或频率学派方法都无法在一致意义下改进鲁棒误差指数 $J(\lambda)$。一个

关于配置模型中近临界渗流泛函的类似极小极大现象表明，我们理论所识别的临界指数是该问题固有的，而非特定参数化设定的产物。

此外，我们证明了决策论稳健性能够高效地应用于现有网络推断流程之上。对于 KL 球，可通过对后验样本或变分样本进行熵倾斜来获得最不利后验分布，从而将稳健化归结为一个一维凸优化问题。对于更一般的 ϕ–散度球，我们提出了一种镜像下降对抗算法，并将其与约束哈密顿蒙特卡罗相结合，以探索倾斜后验。这些方法只需增加适度的计算开销，即可为随机块模型、图子、配置模型和潜在位置模型生成标准后验汇总及模型比较准则的稳健化版本。

我们对功能性脑连接和卡纳塔克邦村庄社会网络所做的实证研究，展示了决策论稳健性如何为实质性结论提供参考。在脑网络中，社团表示与潜在空间表示之间的贝叶斯因子比较，在流行病式阈值识别较弱的区域被发现对局部扰动高度敏感，而某些谱汇总则相对稳定。在卡纳塔克邦村庄中，决策论敏感性分析指出了这样一些村庄和干预策略：它们在单一工作模型下看似占优，但对局部模型设定错误十分脆弱。这提示我们，在解读看似明确的排名时应保持谨慎。

仍有若干局限和拓展方向。首先，我们的稳健性保证是局部的，能够抵御以 KL 散度或更一般的 ϕ–散度衡量的小幅扰动，但无法应对严重的模型设定错误或网络的对抗性重连。其次，非参数极小极大结果聚焦于相对简单的稀疏模型（Erd˝os–R´enyi、随机块模型、配置模型和图子）；将类似分析拓展到更丰富的潜在空间模型、时间网络或多重网络，以及包含额外节点属性的模型，仍是一项开放挑战。第三，我们的计算依赖近似后验（马尔可夫链蒙特卡罗、变分方法或谱伪后验），而系统研究近似误差如何与决策论稳健化相互作用，将很有价值。

尽管存在这些限制，我们的结果表明，决策论稳健性为网络分析提供了一种有用的组织原则。决策论稳健性提供了一种数学上易于处理的方法，用于量化贝叶斯决策的稳定性；这自然关联到图子极限和随机图渐近理论，并能导出具有明确极小极大含义、可解释的噪声指标和临界指数。这项工作是迈向网络模型中更广泛的决策论稳健性理论的一步。值得探索的方向包括：为动态网络和时间网络开发稳健程序，纳入缺失边或节点属性等额外不确定性来源，以及设计诊断工具和可视化方法，使决策论敏感性分析成为应用网络研究中的常规做法。

参考文献

Jayadev Acharya、Ayush Jain、Gautam Kamath、Ananda T. Suresh 和 Huanyu Zhang。《随机图中的稳健估计：极小极大视角》。《统计年刊》，2023年。预印本见 arXiv:2111.05320。

David J. Aldous。《随机变量部分可交换数组的表示》。多元分析杂志，11(4):581–598，1981年。Oriol Artime、Marco Grassia、Manlio De Domenico、James P Gleeson、Hern´an A Makse、Giuseppe Mangioni、Matja˘z Perc 和 Filippo Radicchi。《复杂网络的鲁棒性与韧性》。《自然综述：物理》，6(2):114–131，2024年。Marco Avella Medina、Jos´e Luis Montiel Olea、Cynthia Rush 和 Amilcar S. Velez。《关于 α-后验分布及其变分近似对模型设定错误的鲁棒性》。《机器学习研究杂志》，23(34):1–51，2022年。Abhijit Banerjee、Arun G Chandrasekhar、Esther Duflo 和 Matthew O Jackson。《小额信贷的扩散》。《科学》，341(6144):1236498，2013年。James O. Berger 和 L. Mark Berliner。《使用 ε-污染先验的稳健贝叶斯与经验贝叶斯分析》。《统计年刊》，14(2):461–486，1986年。Duncan S. Callaway、Mark E. J. Newman、Steven H. Strogatz 和 Duncan J. Watts。《网络的稳健性与脆弱性：随机图上的渗流》。《物理评论快报》，85(25):5468– 5471，2000年。Reuven Cohen、Keren Erez、Daniel ben Avraham 和 Shlomo Havlin。《互联网对随机故障的韧性》。《物理评论快报》，85(21):4626–4628，2000年。Persi Diaconis 和 Svante Janson。《图极限与可交换随机图》。《经济研究评论》，76(3):1162–1194，2009年。Lars Peter Hansen 和 Thomas J. Sargent。《鲁棒性》。普林斯顿大学出版社，2008年。Seyed Rouzbeh Hasheminezhad 和 Ulrik Brandes。《优先连接图的鲁棒性：改变基线》。《应用网络科学》，8(1):45，2023年。Emmanuel Jacob 和 Peter M¨orters。《无标度空间网络的鲁棒性》。《概率年刊，45(3):1680–1722，2017年。Aron J. E. M. Janssen、Remco van der Hofstad 和 Sergey Tikhonov。《配置模型的临界窗口》。《电子概率杂志》，19:1–45，2014年。Kei Kawasumi 和 Takehisa Hasegawa。《具有选择性加固的随机网络抵御攻击的鲁棒性》。《科学报告》，14:8733，2024年。L´aszl´o Lov´asz。《大型网络与图极限》。美国数学学会，2012年。Fabio Maccheroni、Massimo Marinacci 和 Aldo Rustichini。《模糊厌恶、鲁棒性与偏好的变分表示》。《计量经济学》，74(6):1447–1498，2006年。Jeffrey W. Miller 和 David B. Dunson。《通过粗化实现稳健贝叶斯推断》。《美国统计学会杂志》，114(527):1113–1125，2019年。doi: 10.1080/01621459.2018. 1469995。Sandrine P´ech´e 和 Vianney Perchet。《社区检测对随机几何扰动的鲁棒性》。载于《神经信息处理系统进展》第*33*卷，第21088–21099页，2020年。

Pierre Stephan 和 Laurent Massouli´e。《社区检测谱方法的鲁棒性》。《机器学习研究杂志》，20：1–51，2019年。Remco van der Hofstad。《随机图与复杂网络，第*1*卷》。剑桥大学出版社，2017年。Brani Vidakovic。 γ-极小极大：保守稳健贝叶斯学派的一种范式。载于 Fabrizio Ruggeri、David R. Kennett 和 Larry Wasserman 编，《稳健贝叶斯分析》，第241–259页。施普林格，2000年。

Renato Vizuete、Paolo Frasca 和 Federica Garin。基于图子的 SIS 流行病敏感性分析。*IEEE* 控制系统快报，4(3)：542–547，2020年。预印本见 arXiv:1912.10330。

Abraham Wald。 统计决策函数。威立，1950年。

James Watson 和 Chris Holmes。近似模型与稳健决策。统计科学，31(4)：465–489，2016年。

James Watson、Luis Nieto-Barajas 和 Chris Holmes。利用 Kullback–Leibler散度刻画非参数随机概率测度的变化。统计学，51(3):558–571，2017年。

张昊天、Elaheh Fata 和 Shreyas Sundaram。复杂网络中的鲁棒性概念及其在韧性共识中的应用。*IEEE*网络系统控制汇刊，4(3):393–405，2017年。

马尔可夫链蒙特卡罗和镜像下降的计算细节

本节汇总第6节中使用的算法步骤。算法1 介绍了应用于后验分布或伪后验抽样（通常通过马尔可夫链蒙特卡罗或变分推断获得）的 KL 球熵倾斜过程，而算法2给出了适用于一般 ϕ–散度球的离散镜像下降对抗算法。

算法 1 通过 KL 球上的熵倾斜实现稳健马尔可夫链蒙特卡罗

要求： 基线后验或伪后验抽样 $\{(\theta^s,\ w_s)\}_{s=1}^S$（通常来自马尔可夫链蒙特卡罗或变分推断）、一个动作 a、损失值 $L_s = L(a,\ \theta^s)$、KL半径 $C > 0$以及数值容差 $\varepsilon > 0$。**确保：** 倾斜权重 $\{q_s^\star\}$ 和稳健后验风险估计 $\sum_s q_s^\star L_s$。1: 定义对偶目标函数

$$\psi(\lambda) := \frac{C + \log\Big(\sum_{s=1}^S w_s \exp\{\lambda L_s\}\Big)}{\lambda}, \qquad \lambda > 0.$$

2: 初始化搜索区间 $[\lambda_{\min}, \lambda_{\max}]$, 例如 $\lambda_{\min} = 10^{-4}$, $\lambda_{\max} = 10^4$。
3: **当** $\lambda_{\max} - \lambda_{\min} > \varepsilon$ **时执行**
4: 设置 $\lambda \leftarrow (\lambda_{\min} + \lambda_{\max})/2$。
5: 计算

$$Z(\lambda) := \sum_{s=1}^S w_s e^{\lambda L_s}, \qquad q_s(\lambda) := \frac{w_s e^{\lambda L_s}}{Z(\lambda)}.$$

6: 评估KL约束

$$K(\lambda) := \sum_{s=1}^S q_s(\lambda) \log \frac{q_s(\lambda)}{w_s}.$$

7: **如果** $K(\lambda) > C$ **则**8: 设置 $\lambda_{\max} \leftarrow \lambda$。9: **否则**10: 设置 $\lambda_{\min} \leftarrow \lambda$。11: **结束 if**12: **结束 while**13: 对所有 s, 设置 $\lambda^\star \leftarrow \lambda_{\min}$和 $q_s^\star \leftarrow q_s(\lambda^\star)$。14: **返回** $\{q_s^\star\}$和 $\sum_{s=1}^S q_s^\star L_s$ 作为稳健后验风险。

算法 2 在 ϕ–散度球上的镜像下降对抗算法

要求： 基准权重 $\boldsymbol{w} = (w_1, \dots, w_S)$、损失 $L_s = L(a, \theta^s)$、半径 $C > 0$、步长 $\eta > 0$、迭代次数 T。

Ensu输出： 近似对抗权重 $\boldsymbol{q}^{(T)}$ 和鲁棒风险估计 $\sum_s q_s^{(T)} L_s$。

1: 初始化 $u_s^{(0)} \leftarrow 0$ 和 $q_s^{(0)}$ 对所有 s, $\leftarrow w_s$。

2: **对于** $t = 0, \dots, T-1$ **执行**

3: 形成当前对抗权重

$$q_s^{(t)} \propto w_s \exp\{u_s^{(t)}\}, \qquad s = 1, \dots, S,$$

并重新归一化，使得 $\sum_s q_s^{(t)} = 1$。

4: 计算当前稳健风险

$$\bar{L}^{(t)} := \sum_{r=1}^{S} q_r^{(t)} L_r.$$

5: 设置梯度

$$g_s^{(t)} := L_s - \bar{L}^{(t)}, \qquad s = 1, \dots, S.$$

6: 在对数倾斜空间中执行镜像步：

$$\tilde{u}_s^{(t+1)} \leftarrow u_s^{(t)} + \eta\, g_s^{(t)}.$$

7: 计算暂定权重

$$\tilde{q}_s^{(t+1)} \propto w_s \exp\{\tilde{u}_s^{(t+1)}\}, \qquad s = 1, \dots, S,$$

并重新归一化。

8: 投影回 ϕ球：

$$q^{(t+1)} \leftarrow \arg\min_{q} \Big\{ \mathrm{KL}\big(q \| \tilde{q}^{(t+1)}\big) : \sum_s q_s = 1,\ q_s \geq 0,\ D_\phi(q \| w) \leq C \Big\}.$$

以 $\tilde{\boldsymbol{q}}^{(t+1)}$ 作为热启动。（对于 KL 散度，此投影有闭式解；对于一般的 ϕ，这是一个小型凸规划。）

9: 对所有 s更新 $u_s^{(t+1)} \leftarrow \log(q_s^{(t+1)}/w_s)$。

10: **结束循环**11: **返回** $\boldsymbol{q}^{(T)}$ 和 $\sum_s q_s^{(T)} L_s$。

补充证明

命题 S.1（随机块模型的狄利克雷扰动的期望 KL 散度）。设 $W^\star$ 为一个阶梯函数图子，对应于具有区块边概率 $P^\star = (p^\star_{ab})_{1 \leq a,b \leq K} \in (0,1)^{K \times K}$的 K 区块随机块模型（SBM）。记 $\boldsymbol{p}^\star = (p_1^\star, \dots, p_{K^2}^\star)$ 为 $P^\star$ 的向量化，使其归一化后满足 $p_i^\star \in (0,1)$ 和 $\sum_{i=1}^{K^2} p_i^\star = 1$。

考虑一个“几何 对 $P^\star$ 进行“广义贝叶斯自助法”扰动：在给定 $\boldsymbol{p}^\star$ 抽样的条件下

随机单元权重

$$\boldsymbol{W} = (W_1, \dots, W_{K^2}) \sim \mathrm{Dirichlet}\big(\alpha_n \boldsymbol{p}^\star\big),$$

并定义 Kullback–Leibler散度

$$\mathrm{KL}(\boldsymbol{W} \| \boldsymbol{p}^\star) := \sum_{i=1}^{K^2} W_i \log \frac{W_i}{p_i^\star}.$$

Then

$$\mathbb{E}\big[\mathrm{KL}(\boldsymbol{W} \| \boldsymbol{p}^\star)\big] \;=\; \sum_{i=1}^{K^2} p_i^\star \Big\{ \psi_0(\alpha_n p_i^\star + 1) - \psi_0(\alpha_n + 1) - \log p_i^\star \Big\}, \tag{11}$$

其中 ψ_0 是双伽马函数。

此外，当 $\alpha_n \to \infty$ 时，

$$\mathbb{E}\big[\mathrm{KL}(\boldsymbol{W} \| \boldsymbol{p}^\star)\big] \;=\; \frac{K^2 - 1}{2\alpha_n} \;+\; \mathcal{O}\!\left(\frac{1}{\alpha_n^2}\right), \tag{12}$$

与具体的基准随机块模型 $P^\star$ 无关。

证明。 为简洁起见，记 $d := K^2$ 。设 $\boldsymbol{W} \sim \mathrm{Dir}(\alpha_n \boldsymbol{p}^\star)$。那么 $W_i > 0$ 几乎处处成立，$\sum_i W_i = 1$，且 $\boldsymbol{W}$ 相对于单纯形上的勒贝格测度的密度为

$$f(\boldsymbol{w}) \propto \prod_{i=1}^{d} w_i^{\alpha_n p_i^\star - 1}, \qquad \boldsymbol{w} \in \Delta^{d-1}.$$

KL 散度可分解为

$$\mathrm{KL}(\boldsymbol{W} \| \boldsymbol{p}^\star) = \sum_{i=1}^{d} W_i \log W_i - \sum_{i=1}^{d} W_i \log p_i^\star.$$

取期望并使用 $\mathbb{E}[W_i] = p_i^\star$ 可得

$$\mathbb{E}\big[\mathrm{KL}(\boldsymbol{W} \| \boldsymbol{p}^\star)\big] = \sum_{i=1}^{d} \mathbb{E}[W_i \log W_i] - \sum_{i=1}^{d} p_i^\star \log p_i^\star. \tag{13}$$

现在计算 $\mathbb{E}[W_i \log W_i]$。 W_i 的边缘分布为贝塔分布(a_i, b_i)，其中 $a_i = \alpha_n p_i^\star$且 $b_i = \alpha_n(1 - p_i^\star)$。令 $X \sim$服从贝塔分布(a, b)，其密度正比于 $x^{a-1}(1-x)^{b-1}$，定义在$(0,1)$上。对于$t > -a$ ，有

$$\mathbb{E}[X^t] = \frac{B(a + t, b)}{B(a, b)} = \frac{\Gamma(a + t)\Gamma(a + b)}{\Gamma(a + b + t)\Gamma(a)}.$$

对 t求导，

$$\frac{\mathrm{d}}{\mathrm{d}t}\mathbb{E}[X^t] = \mathbb{E}[X^t \log X] = \big\{\psi_0(a + t) - \psi_0(a + b + t)\big\}\,\mathbb{E}[X^t],$$

其中 ψ_0 是双伽马函数。在 $t = 1$ 处求值并使用 $\mathbb{E}[X] = a/(a + b)$，得到

$$\mathbb{E}[X \log X] = \frac{a}{a + b}\,\big\{\psi_0(a + 1) - \psi_0(a + b + 1)\big\}.$$

将其应用于 $W_i \sim$ 贝塔分布(a_i, b_i)，其中 $a_i = \alpha_n p_i^\star$ 且 $b_i = \alpha_n(1 - p_i^\star)$，得到

$$\mathbb{E}[W_i \log W_i] = p_i^\star \big\{ \psi_0(\alpha_n p_i^\star + 1) - \psi_0(\alpha_n + 1) \big\}.$$

代入式（13）可得

$$\mathbb{E}\big[\mathrm{KL}(\boldsymbol{W} \| \boldsymbol{p}^\star)\big] = \sum_{i=1}^{d} p_i^\star \big\{ \psi_0(\alpha_n p_i^\star + 1) - \psi_0(\alpha_n + 1) \big\} - \sum_{i=1}^{d} p_i^\star \log p_i^\star,$$

这恰好就是式（11）。

对于渐近分析，回顾以下展开式

$$\psi_0(x+1) = \log x + \frac{1}{2x} + \mathcal{O}\left(\frac{1}{x^2}\right) \qquad \text{as } x \to \infty.$$

因此，当 $\alpha_n \to \infty$ 时，

$$\psi_0(\alpha_n p_i^\star + 1) = \log(\alpha_n p_i^\star) + \frac{1}{2\alpha_n p_i^\star} + \mathcal{O}\left(\frac{1}{\alpha_n^2}\right),$$

and

$$\psi_0(\alpha_n + 1) = \log \alpha_n + \frac{1}{2\alpha_n} + \mathcal{O}\left(\frac{1}{\alpha_n^2}\right).$$

因此

$$\psi_0(\alpha_n p_i^\star + 1) - \psi_0(\alpha_n + 1) - \log p_i^\star = \frac{1}{2\alpha_n}\left(\frac{1}{p_i^\star} - 1\right) + \mathcal{O}\left(\frac{1}{\alpha_n^2}\right),$$

两边乘以 $p_i^\star$ yields

$$p_i^\star \left\{ \psi_0(\alpha_n p_i^\star + 1) - \psi_0(\alpha_n + 1) - \log p_i^\star \right\} = \frac{1}{2\alpha_n}(1 - p_i^\star) + \mathcal{O}\left(\frac{1}{\alpha_n^2}\right).$$

对 i 求和并利用 $\sum_i p_i^\star = 1$，我们得到

$$\mathbb{E}\big[\mathrm{KL}(\boldsymbol{W} \| \boldsymbol{p}^\star)\big] = \frac{1}{2\alpha_n} \sum_{i=1}^{d} (1 - p_i^\star) + \mathcal{O}\left(\frac{1}{\alpha_n^2}\right) = \frac{d-1}{2\alpha_n} + \mathcal{O}\left(\frac{1}{\alpha_n^2}\right),$$

这就是（12），其中 $d = K^2$。 □

定理 S.1（KL 球内可交换网络模型的可达性）。固定 n 和一个具有 K 个块的工作阶梯图元 $W^\star$，令 $G^\star = G(W^\star)$ 表示其在 n 个顶点图上的关联图分布。对于 $C > 0$，令 $\Gamma_C(G^\star)$ 表示如式（2）所定义的、以 $G^\star$ 为中心且半径为 C 的 KL 球。假设 $W^\star$ 的所有块概率均位于 $(\varepsilon, 1-\varepsilon)$ 内，其中某个 $\varepsilon > 0$ 满足此条件；并且假设 C 足够小，使得每个满足 $G(W) \in \Gamma_C(G^\star)$ 的 K 块阶梯图元 W 的块概率也都位于 $(\varepsilon/2, 1-\varepsilon/2)$ 内。

考虑以下定义在 K 块随机块模型参数空间上的马尔可夫链，其分布属于 $\Gamma_C(G^\star)$：

~1. 扰动移动。从当前块矩阵 $P = (p_{ab})$ 出发，抽取相互独立的 $Y_{ab} \sim \Gamma(\alpha_{ab}, 1)$，其中 $\alpha_{ab} > 0$，设

$$\widetilde{p}_{ab} = \frac{\widetilde{Y}_{ab}}{\sum_{c,d} \widetilde{Y}_{cd}},$$

~并构造提议 $P = (\widetilde{p}_{ab})$。如果对应的阶梯图元 $W_{\widetilde{P}}$ 满足 $G(W_{\widetilde{P}}) \in \Gamma_C(G^\star)$，则接受此次移动并设为 $P' \leftarrow P$；否则拒绝并设为 $P' \leftarrow P$。

2. 重缩放移动。（可选。）以一定概率（使用 $1/2$）m，将随机选取的 P条目的子集乘以区间（$1-\rho$, $1+\rho$）中的随机因子；如有需要，再进行归一化。仅当所得模型属于 $\Gamma_C(G^\star)$ 时才接受，否则保持为 P。

那么，该马尔可夫链在 $\Gamma_C(G^\star)$的内部上是 ψ不可约且非周期的。特别地，对于任意两个内部位于 $\Gamma_C(G^\star)$中的 K块随机块模型 P， $P^\dagger$，以及任意包含于$\Gamma_C(G^\star)$中的邻域 U $P^\dagger$，

$$\mathbb{P}_P\big(\exists t \geq 1 : P_t \in U\big) > 0.$$

对于其图子可由 K块分块阶梯图子在割范数下近似的随机点积图，通过将上述扰动移动应用于阶梯图子近似，也可得到相同结论，且近似误差可以任意小。

证明。我们首先证明，仅采用扰动移动时的不可约性和非周期性；加入重缩放移动只会增大马尔可夫链的支撑集。

步骤 1：参数空间与内部。 令 $\mathcal{S} \subset (0,1)^{K^2}$ 表示块概率向量 $p = (p_1, \ldots\ldots, p_{K^2})$的开概率单纯形，其中 $\sum_i p_i = 1$。关于 $W^\star$ 和 C的假设意味着集合

$$\mathcal{S}_C := \big\{p \in \mathcal{S} : G(p) \in \Gamma_C(G^\star)\big\}$$

是 $\mathcal{S}$ 的非空开子集：KL 球是开集，而约束 $p_i \in (\varepsilon/2, 1-\varepsilon/2)$ 排除了单纯形的边界。我们将 $\mathcal{S}_C$ 称为 KL 球的内部。

步骤 2：狄利克雷扰动具有满支撑集。给定当前状态 $p \in \mathcal{S}_C$，扰动~ ~ ~
移动会抽取相互独立的 $Y_{ab} \sim \Gamma(\alpha_{ab}, 1)$，并设定 $\widetilde{p}_{ab} = Y_{ab} / \sum_{c,d} Y_{cd}$。向量 $\widetilde{p}$服从参数严格为正的狄利克雷分布 (α_{ab})，因此相对于 $\mathcal{S}$ 上勒贝格测度的密度形式为

$$f_p(\widetilde{p}) \propto \prod_{a,b} \widetilde{p}_{ab}^{\alpha_{ab}-1}, \qquad \widetilde{p} \in \mathcal{S}.$$

该密度在整个 $\mathcal{S}$ 上连续且严格为正。特别地，对于任何勒贝格测度为正的博雷尔集 $B \subset \mathcal{S}$,

$$\mathbb{P}_p(\widetilde{p} \in B) > 0.$$

步骤 3：在 $\mathcal{S}_C$ 上的不可约性。设 P和 $P^\dagger$是 KL 球内部的两个阶梯图子，其对应的分块向量为 $p, p^\dagger \in \mathcal{S}_C$，并令 U为包含在 $\mathcal{S}_C$ 中的 $p^\dagger$ 的任意开邻域。由于 $\mathcal{S}_C$ 是开集，这样的邻域确实存在，且勒贝格测度为正。由于狄利克雷密度 f_p 在整个 $\mathcal{S}$上严格为正，因此我们有

$$\mathbb{P}_p\big(\widetilde{p} \in U\big) > 0.$$

每当 $\widetilde{p} \in U \subset$ $\mathcal{S}_C$，扰动移动都会被接受，因此一步转移核满足 s

$$K(p, U) := \mathbb{P}_p(P_1 \in U) \geq \mathbb{P}_p(\widetilde{p} \in U) > 0.$$

因此，从任意起点 $p \in \mathcal{S}_C$ 出发，都可以在一步内以正概率到达 $\mathcal{S}_C$ 中的任意开子集 U。这意味着，在 $\mathcal{S}_C$ 上的马尔可夫链相对于限制在 $\mathcal{S}_C$ 上的勒贝格测度是 ψ–不可约的。

步骤 4：非周期性。要证明非周期性，只需证明存在一个非零测度集合 $A \subset \mathcal{S}_C$，使得马尔可夫链有正概率在一步内停留在 A。固定 $p \in \mathcal{S}_C$，并令$B \subset \mathcal{S} \setminus \mathcal{S}_C$ 为包含在 KL球补集中的任意正勒贝格测度可测集

。由于 f_p 在 $\mathcal{S}$上严格为正，因此我们有 $\mathbb{P}_p(\widetilde{p} \in B) > 0$。每当 $\widetilde{p} \in B$ 时，移动都会被拒绝，马尔可夫链便停留在 p。因此

$$K(p, \{p\}) = \mathbb{P}_p(P_1 = p) \;\geq\; \mathbb{P}_p(\widetilde{p} \in B) \;>\; 0.$$

因此，每个内部点 $p \in \mathcal{S}_C$ 的自转移概率都严格大于零，这意味着该马尔可夫链在 $\mathcal{S}_C$上是非周期的。

步骤 5：重缩放移动与随机点积图。加入重缩放移动（定理陈述中的步骤 2）只会扩大可达点的集合，不会影响上述已确立的不可约性或非周期性。

对于图子 W 可在割范数下由 K–$\sim$ $\sim$分块阶梯图子 W_K逼近的随机点积图，我们可以对分块模型 W_K应用同一个马尔可夫链。给定任意两个随机点积图图子 W，$W^\dagger$，其对应的概率律 $G(W)$ 和 $G(W^\dagger)$ 均属于 $\Gamma_C(G^\star)$，选取足够大的K，使得 W 和 $W^\dagger$ 在割范数下都能由 $\mathcal{S}_C$ 中的阶梯图子逼近，且误差小于任意指定的容差。根据上述随机块模型的情形，从 W 的阶梯近似出发，该阶梯图子上的马尔可夫链以正概率可到达 $W^\dagger$ 的任意小邻域；相应的随机点积图图子因而也可在所选近似误差范围内到达。

证明完成。 □

定理 S.2（精确小 KL 展开）。设 $(\mathcal{X},\ \mathcal{A},\ P)$ 为一个概率空间，并设 $f\colon \mathcal{X} \to \mathbb{R}$ 是一个可测函数，满足

$$m := \mathbb{E}_P[f], \qquad \sigma^2 := \operatorname{Var}_P(f) \in [0, \infty),$$

中心矩母函数

$$M(\lambda) := \mathbb{E}_P\big[e^{\lambda(f-m)}\big]$$

对所有 λ 在 0 的某个邻域内均为有限值。对 $C > 0$ 定义

$$\mathcal{U}_C(P) := \big\{Q :\ Q \ll P,\ \mathrm{KL}(Q\|P) \leq C\big\}, \qquad S_f(C) := \sup_{Q \in \mathcal{U}_C(P)} \int f \,\mathrm{d}Q,$$

其中 $\mathrm{KL}(Q\|P) := \int \log\!\left(\frac{\mathrm{d}Q}{\mathrm{d}P}\right) \mathrm{d}Q$。于是，当 $C \downarrow 0$时，

$$S_f(C) = m + \sqrt{2\,\operatorname{Var}_P(f)}\,\sqrt{C} + o\big(\sqrt{C}\big). \tag{14}$$

此外，如果 $\operatorname{Var}_P(f) > 0$，则系数 $\sqrt{2\operatorname{Var}_P(f)}$ 是精确的，亦即

$$\lim_{C \downarrow 0} \frac{S_f(C) - m}{\sqrt{2\,\operatorname{Var}_P(f)}\,\sqrt{C}} = 1.$$

特别地，对于任意 $k < \sqrt{2\,\text{方差}_P(f)}$ 都存在一个序列 $C_j \downarrow 0$，使得

$$S_f(C_j) > m + k\,\sqrt{C_j}$$

对所有足够大的 j。

证明。 如果 f在 P下几乎处处为常数，记作 $f \equiv m$，那么 $S_f(C) = m$对所有 $C \geq 0$都成立，并且（14）显然成立，其中 $\sigma^2 = 0$。因此我们假设 $\sigma^2 > 0$。

记 $\tilde{f} := f - m$，使得 $\mathbb{E}_P[\tilde{f}] = 0$和 $_P$的方差$(\tilde{f}) = \sigma^2$。令

$$M(\lambda) := \mathbb{E}_P\big[e^{\lambda \tilde{f}}\big], \qquad \Lambda(\lambda) := \log M(\lambda),$$

˜是 f在 P下的矩母函数和累积量生成函数。根据假设，对于 0 的某个邻域内的 λ，$M(\lambda) < \infty$，且 Λ 在该处是解析的，其泰勒展开为

$$\Lambda(\lambda) = \tfrac{1}{2}\sigma^2\lambda^2 + \mathcal{O}(|\lambda|^3), \qquad \lambda \to 0.$$

对偶表示。对于每个 $\lambda > 0$ 以及任意 $Q \ll P$，Donsker–Varadhan变分不等式给出

$$\lambda \int f \,\mathrm{d}Q - \mathrm{KL}(Q\|P) \;\leq\; \log \mathbb{E}_P\big[e^{\lambda f}\big].$$

重新整理可得，

$$\int f \,\mathrm{d}Q \;\leq\; \frac{1}{\lambda}\Big\{\log \mathbb{E}_P\big[e^{\lambda f}\big] + \mathrm{KL}(Q\|P)\Big\}.$$

如果 $\mathrm{KL}(Q\|P) \leq C$，则有

$$\int f \,\mathrm{d}Q \;\leq\; m + \frac{1}{\lambda}\big\{\Lambda(\lambda) + C\big\},$$

因为 $\log\ \mathbb{E}_P[e^{\lambda f}] = \lambda m + \Lambda(\lambda)$。对 $Q \in \mathcal{U}_C(P)$ 取上确界，再对 $\lambda > 0$ 取下确界，可得

$$S_f(C) \;\leq\; m + \inf_{\lambda > 0} g(\lambda, C), \qquad g(\lambda, C) := \frac{\Lambda(\lambda) + C}{\lambda}. \tag{15}$$

指数倾斜与下界。 对于下界，我们考虑指数倾斜测度

$$\frac{\mathrm{d}Q_\lambda}{\mathrm{d}P} := \frac{e^{\lambda \tilde{f}}}{M(\lambda)}, \qquad \lambda > 0.$$

于是 $Q_\lambda \ll P$，根据指数倾斜的标准性质可得

$$\mathbb{E}_{Q_\lambda}[\tilde{f}] = \Lambda'(\lambda), \qquad \mathrm{KL}(Q_\lambda\|P) = \lambda\Lambda'(\lambda) - \Lambda(\lambda).$$

特别地，

$$\int f \,\mathrm{d}Q_\lambda = m + \Lambda'(\lambda). \tag{16}$$

倾斜的渐近分析。根据 Λ的泰勒展开，我们得到

$$\Lambda(\lambda) = \tfrac{1}{2}\sigma^2\lambda^2 + \mathcal{O}(\lambda^3), \qquad \Lambda'(\lambda) = \sigma^2\lambda + \mathcal{O}(\lambda^2), \qquad \lambda \to 0.$$

因此

$$C(\lambda) := \mathrm{KL}(Q_\lambda\|P) = \lambda\Lambda'(\lambda) - \Lambda(\lambda) = \tfrac{1}{2}\sigma^2\lambda^2 + \mathcal{O}(\lambda^3), \quad \lambda \to 0, \tag{17}$$

and

$$\int f \,\mathrm{d}Q_\lambda = m + \sigma^2\lambda + \mathcal{O}(\lambda^2), \qquad \lambda \to 0. \tag{18}$$

由于对于所有充分小的 $\lambda > 0$， $\sigma^2 > 0$ and $\Lambda''(\lambda) = $方差$_{Q_\lambda}(\tilde{f}) > 0$，函数 $\lambda \mapsto C(\lambda)$ 在某个 $\lambda_0 > 0$ 的区间 $(0, \lambda_0)$ 上严格递增，且当 $\lambda \downarrow 0$ 时， $C(\lambda) \downarrow 0$。因此，它在此区间上可逆，并且对于足够小的 $C > 0$，我们可以定义逆函数 $\lambda(C) \in (0, \lambda_0)$，使得 $C(\lambda(C)) = C$。

由（17）可得

$$C = \tfrac{1}{2}\sigma^2\lambda(C)^2 + \mathcal{O}(\lambda(C)^3) \quad \Rightarrow \quad \lambda(C) = \frac{\sqrt{2C}}{\sigma} + \mathcal{O}(C), \qquad C \downarrow 0,$$

使用 $\lambda（C） = \mathcal{O}(\sqrt{C})$。代入（18）得到

$$\int f \, \mathrm{d}Q_{\lambda(C)} = m + \sqrt{2\sigma^2 C} + \mathcal{O}(C), \qquad C \downarrow 0. \tag{19}$$

关于 $S_f(C)$ 的下界。对每个较小的 $C > 0$，根据构造有 $Q_{\lambda(C)} \in \mathcal{U}_C(P)$，因此

$$S_f(C) \ \geq \ \int f \, \mathrm{d}Q_{\lambda(C)} = m + \sqrt{2\sigma^2 C} + \mathcal{O}(C),$$

这意味着

$$\liminf_{C \downarrow 0} \frac{S_f(C) - m}{\sqrt{C}} \ \geq \ \sqrt{2\sigma^2}. \tag{20}$$

关于 $S_f（C）$ 的上界。利用（15），对于任意 $\lambda > 0$,

$$S_f(C) - m \ \leq \ g(\lambda, C) = \frac{\Lambda(\lambda) + C}{\lambda}.$$

取 $\lambda = t\sqrt{C}$，令 $t > 0$ 固定且 C 足够小。那么，当 $C \downarrow 0$ 时,

$$\Lambda(\lambda) = \tfrac{1}{2}\sigma^2 t^2 C + \mathcal{O}(C^{3/2}),$$

因此

$$g(t\sqrt{C}, C) = \frac{\frac{1}{2}\sigma^2 t^2 C + C + \mathcal{O}(C^{3/2})}{t\sqrt{C}} = \Big(\tfrac{1}{2}\sigma^2 t + \frac{1}{t}\Big)\sqrt{C} + \mathcal{O}(C).$$

Let

$$F(t) := \tfrac{1}{2}\sigma^2 t + \frac{1}{t}, \qquad t > 0.$$

A si简单的微积分检验表明， F 在 $t_\star = \sqrt{2}/\sigma$ 处取得唯一极小值，且 h

$$F(t_\star) = \sqrt{2\sigma^2}.$$

因此，对于任意 $\varepsilon > 0$，我们都可以选择足够接近 $t_\star$ 的 t_ε，使得 $F(t_\varepsilon) \leq \sqrt{2\sigma^2 + \varepsilon}$。对于这一选择,

$$g(t_\varepsilon\sqrt{C}, C) = F(t_\varepsilon)\sqrt{C} + \mathcal{O}(C) \leq \big(\sqrt{2\sigma^2} + \varepsilon\big)\sqrt{C} + \mathcal{O}(C).$$

对 $\lambda > 0$ 取下确界，然后令 $C \downarrow 0$，得到

$$\limsup_{C \downarrow 0} \frac{S_f(C) - m}{\sqrt{C}} \ \leq \ \sqrt{2\sigma^2} + \varepsilon. \tag{21}$$

由于 $\varepsilon > 0$ 是任意的，

$$\limsup_{C\downarrow 0} \frac{S_f(C) - m}{\sqrt{C}} \;\le\; \sqrt{2\sigma^2}. \tag{22}$$

结合（20）和（22）可得

$$\lim_{C\downarrow 0} \frac{S_f(C) - m}{\sqrt{C}} = \sqrt{2\sigma^2},$$

这正是（14）。锐度结论由该极限的存在性立即得到：若 $k < \sqrt{2\sigma^2}$，则对于所有充分小的 C，我们必有 $(S_f(C) - m)/\sqrt{C} > k$，因此 $S_f(C) > m + k\sqrt{C}$。

证明完毕。 □

定理3.3的证明

定理*3.3*的证明。记 $R_0 := R(\theta_0)$ 以及 $\Delta_0 := \Delta(\theta_0)$。根据假设 3.1 和链式法则，

$$\nabla_\theta R(\theta_0) = c_0\, \Delta_0^{-2}\, \nabla_\theta \rho(\theta_0) + \nabla_\theta H(\theta_0).$$

根据定理假设中的 **(i)** 项，我们有

$$G := \nabla_\theta R(\theta_0), \qquad \|G\| \asymp \Delta_0^{-2} \quad \text{as } \Delta_0 \downarrow 0.$$

根据假设 3.2，在 $\Pi_{0,\,n}$ 我们可以写成

$$\theta = \theta_0 + r_n Z_n, \qquad Z_n \Rightarrow Z \sim N(0, \Sigma)$$

以 $P_{\theta_0}^{(n)}$ –概率成立，并且条款 **(ii)** 确保 $\|Z_n\|$ 具有一致有界的二阶和四阶矩（同样以 $P_{\theta_0}^{(n)}$ –概率成立）。在 θ_0 附近、R 为 C^2 的邻域上对 R 作泰勒展开，可得

$$R(\theta) = R_0 + r_n G^\top Z_n + R_n^{\mathrm{rem}},$$

with

$$R_n^{\mathrm{rem}} = O\big(r_n^2 \|Z_n\|^2\big)$$

在该邻域上一致成立。

基准后验风险。贝叶斯估计量为

$$a_n^\star = \int R(\theta)\, \Pi_{0,n}(\mathrm{d}\theta) = R_0 + r_n G^\top \mathbb{E}_{\Pi_{0,n}}[Z_n] + \mathbb{E}_{\Pi_{0,n}}\big[R_n^{\mathrm{rem}}\big].$$

根据 R_n^{rem}的界以及 Z_n的一致矩界，

$$\mathbb{E}_{\Pi_{0,n}}\big[R_n^{\mathrm{rem}}\big] = O_{P_{\theta_0}^{(n)}}\big(r_n^2\big) = o_{P_{\theta_0}^{(n)}}(r_n),$$

so

$$a_n^\star = R_0 + r_n G^\top \mathbb{E}_{\Pi_{0,n}}[Z_n] + o_{P_{\theta_0}^{(n)}}(r_n).$$

因此，$R(\theta)$ 在$\Pi_{0,\,n}$ 下的中心化波动可写为

$$R(\theta) - a_n^\star = r_n G^\top \big(Z_n - \mathbb{E}_{\Pi_{0,n}}[Z_n]\big) + \big(R_n^{\mathrm{rem}} - \mathbb{E}_{\Pi_{0,n}}[R_n^{\mathrm{rem}}]\big) + o_{P_{\theta_0}^{(n)}}(r_n).$$

余项满足

$$R_n^{\mathrm{rem}} - \mathbb{E}_{\Pi_{0,n}}[R_n^{\mathrm{rem}}] = O_{P_{\theta_0}^{(n)}}\big(r_n^2\|Z_n\|^2\big),$$

因此

$$\mathrm{Var}_{\Pi_{0,n}}\big(R_n^{\mathrm{rem}}\big) = O_{P_{\theta_0}^{(n)}}\big(r_n^4\big) = o_{P_{\theta_0}^{(n)}}\big(r_n^2\|G\|^2\big),$$

因为 $\|G\| \asymp \Delta_0^{-2} \to \infty$ 和 $r_n \to 0, \Delta_0 \to 0$。记

$$Z_n^0 := Z_n - \mathbb{E}_{\Pi_{0,n}}[Z_n],$$

因此我们得到

$$R(\theta) - a_n^\star = r_n G^\top Z_n^0 + o_{P_{\theta_0}^{(n)}}\big(r_n\|G\|\big),$$

从而

$$\rho_{0,n} = \mathrm{Var}_{\Pi_{0,n}}(R(\theta)) = r_n^2 G^\top \Sigma_n G + o_{P_{\theta_0}^{(n)}}\big(r_n^2\|G\|^2\big),$$

其中 $\Sigma_n :=$ 方差$_{\Pi_{0,n}}(Z_n) \to \Sigma$ 在 $P_{\theta_0}^{(n)}$–概率意义下成立，这由局部贝叶斯–Bernstein–von Mises假设和矩界得出。

记

$$W_0 := G^\top \Sigma G.$$

根据 Σ 的非退化性，存在常数 $0 < c_1 \le c_2 < \infty$，使得

$$c_1\|G\|^2 \le W_0 \le c_2\|G\|^2.$$

结合 $\|G\| \asymp \Delta_0^{-2}$，可得 $W_0 \asymp \Delta_0^{-4}$，因此存在一个常数 $V_0 \in (0, \infty)$（取决于路径上的局部几何 θ_0），使得

$$W_0 = \frac{V_0}{\Delta_0^4}\big(1 + o(1)\big) \quad \text{as } \Delta_0 \downarrow 0.$$

将此结果与$\rho_{0,n}$ 的近似结合，可得

$$\rho_{0,n} = \frac{V_0\, r_n^2}{\Delta_0^4}\big(1 + o_{P_{\theta_0}^{(n)}}(1)\big),$$

即（4）。

平方损失的分布。定义

$$L_n(\theta) := \big(a_n^\star - R(\theta)\big)^2.$$

根据 $a_n^\star$的定义，

$$\rho_{0,n} = \mathrm{Var}_{\Pi_{0,n}}(R(\theta)) = \mathbb{E}_{\Pi_{0,n}}\big[L_n(\theta)\big].$$

由上述展开可得，在 $\Pi_{0,\ n}$ 下，

$$a_n^\star - R(\theta) = -r_n G^\top Z_n^0 + o_{P_{\theta_0}^{(n)}}\big(r_n\|G\|\big),$$

so

$$L_n(\theta) = \big(a_n^\star - R(\theta)\big)^2 = r_n^2\big(G^\top Z_n^0\big)^2 + o_{P_{\theta_0}^{(n)}}\big(r_n^2\|G\|^2\big).$$

令 $\tau_n^2 := \rho_{0,\,n}$ 并定义归一化损失

$$Y_n := -\tau_n^{-1}\big(R(\theta) - a_n^\star\big), \qquad L_n(\theta) = \tau_n^2 Y_n^2.$$

根据局部贝叶斯–Bernstein–von Mises假设和一致矩界，$G^\top Z_n^0$ 是渐近正态的，方差为 W_0，且余项在 $\tau_n \asymp r_n\|G\|$尺度下可以忽略。因此，利用德尔塔方法／连续映射论证可得

$$Y_n \Rightarrow Y \sim N(0,1)$$

在$\Pi_{0,\,n}$ 以 $P_{\theta_0}^{(n)}$ –概率收敛，并且矩界将这一弱收敛提升为阶数不超过4的矩收敛。特别地，

$$\mathbb{E}_{\Pi_{0,n}}[Y_n^2] = 1 \quad \text{and} \quad \mathrm{Var}_{\Pi_{0,n}}(Y_n^2) \to \mathrm{Var}(Y^2) = 2$$

以 $P_{(n)}\theta_0$–概率收敛。由于 $L_n = \tau_n^2 Y_n^2$且$\tau_n^2 = \rho_{0,\,n}$，我们得到

$$\mathbb{E}_{\Pi_{0,n}}[L_n] = \rho_{0,n} \quad \text{and} \quad \mathrm{Var}_{\Pi_{0,n}}(L_n) = 2\rho_{0,n}^2\big(1 + o_{P_{\theta_0}^{(n)}}(1)\big).$$

此外，对于每个固定的 n ，在$\Pi_{0,\,n}$ 下， L_n 的（中心化）矩母函数在原点的某个邻域内有限；例如，当 R 至多呈多项式增长，且$\Pi_{0,\,n}$ 在 θ_0附近局部具有次高斯尾部时，该条件成立。结合定理假设中的第(iii)项，这意味着定理S.2 的假设在$P = \Pi_{0,\,n}$ 和 $f = L_n$下均得到满足，并且该定理中的 $o(\sqrt{C})$余项可以在归一化损失$L_n/\rho_{0,\,n}$ 这一族上，对较小的 C一致取值。

应用精确小 *KL* 展开。根据定理 S.2，对于每个固定的 n 以及所有充分小的$C > 0$,

$$\sup_{\widetilde{\Pi}:\,\mathrm{KL}(\widetilde{\Pi}\|\Pi_{0,n})\le C} \int L_n(\theta)\,\widetilde{\Pi}(\mathrm{d}\theta) = \mathbb{E}_{\Pi_{0,n}}[L_n] + \sqrt{2\ \mathrm{Var}_{\Pi_{0,n}}(L_n)}\,\sqrt{C} + o(\sqrt{C}),$$

其中， $o(\sqrt{C})$ 项在 $C \downarrow 0$ 时趋于 0，并且根据第 (iii) 项中的一致指数矩界，当 C 属于充分小的区间 $(0, C_0]$时，可以将其在 n 上一致地选取。

根据定义，

$$\rho_{\mathrm{rob},n}(C) := \sup_{\widetilde{\Pi}:\,\mathrm{KL}(\widetilde{\Pi}\|\Pi_{0,n})\le C} \int L_n(\theta)\,\widetilde{\Pi}(\mathrm{d}\theta),$$

因此代入 $\mathbb{E}_{\Pi_{0,\,n}}[L_n] = \rho_{0,\,n}$ 和方差$\Pi_{0,\,n}(L_n) = 2\rho_{0,\,n}^2(1 + o_{P_{\theta_0}^{(n)}}(1))$，可得对于所有充分小的 C,

$$\rho_{\mathrm{rob},n}(C) = \rho_{0,n} + 2\,\rho_{0,n}\sqrt{C} + o_{P_{\theta_0}^{(n)}}\big(\rho_{0,n}\sqrt{C}\big),$$

其中 $o_{P_{\theta_0}^{(n)}}(\rho_{0,n}\sqrt{C})$ 项关于 n 在 $C \in (0, C_0]$ 上一致。取 $C = \mathcal{C}_n \downarrow 0$ 即可得到（5）以及该收敛性

$$\frac{\rho_{\mathrm{rob},n}(\mathcal{C}_n) - \rho_{0,n}}{\rho_{0,n}\sqrt{\mathcal{C}_n}} \xrightarrow[n\to\infty]{P_{\theta_0}^{(n)}} 2,$$

这就证明了精确膨胀结论（第 (2) 部分）。

锐度。 由定理 S.2 应用于 $f = L_n$ 可得，对每个固定的 n,

$$\rho_{\mathrm{rob},n}(C) = \rho_{0,n} + \sqrt{2\ \mathrm{Var}_{\Pi_{0,n}}(L_n)}\,\sqrt{C} + o\big(\sqrt{C}\big) \quad \text{as } C \downarrow 0.$$

两边除以 $\rho_{0,n}\sqrt{C}$ 并利用方差 $\Pi_{0,n}(L_n) = 2\rho_{0,n}^2(1 + o_{P_{\theta_0}^{(n)}}(1))$，得到

$$\frac{\rho_{\mathrm{rob},n}(C) - \rho_{0,n}}{\rho_{0,n}\sqrt{C}} = \frac{\sqrt{2\ \mathrm{Var}_{\Pi_{0,n}}(L_n)}}{\rho_{0,n}} + o_{P_{\theta_0}^{(n)}}(1) \xrightarrow[n\to\infty]{P_{\theta_0}^{(n)}} 2$$

对每个固定的、足够小的 $C > 0$。等价地，对于任意 $\varepsilon > 0$，存在 $C_0 > 0$ 和 n_0，使得对所有 $n \geq n_0$ 和所有 $C \in (0,\ C_0]$，

$$P_{\theta_0}^{(n)}\left(\frac{\rho_{\mathrm{rob},n}(C) - \rho_{0,n}}{\rho_{0,n}\sqrt{C}} \geq 2 - \varepsilon\right) \to 1.$$

现在固定 $k < 2$ 并选择 $\varepsilon \in (0,\ 2 - k)$。根据前面的公式，存在 $C_0 > 0$ 和 n_0，使得对所有 $n \geq n_0$ 和所有 $C \in (0,\ C_0]$，事件

$$\rho_{\mathrm{rob},n}(C) > \rho_{0,n} + k\,\rho_{0,n}\sqrt{C}$$

以趋于 1 的 $P_{\theta_0}^{(n)}$ 概率发生。特别地，我们可以任取一个确定性序列 $\mathcal{C}_n \downarrow 0$，使得对所有 n 都有 $\mathcal{C}_n \leq C_0$；对于该序列，我们得到

$$\rho_{\mathrm{rob},n}(\mathcal{C}_n) > \rho_{0,n} + k\,\rho_{0,n}\sqrt{\mathcal{C}_n}$$

对所有充分大的 n，以 $P_{\theta_0}^{(n)}$ 概率趋于 1。这证明了第（3）部分中的锐度结论，并表明（5）中的系数 2 渐近最优。

证明至此完成。 □

引理证明4.1

证明。 在 $P_{(n)\,0}$ 和 $P_1^{(n)}$ 两种情况下，边都是相互独立的；不同之处仅在于伯努利参数。因此

$$D_n = \mathrm{KL}\big(P_1^{(n)} \| P_0^{(n)}\big) = \sum_{1 \leq i < j \leq n} \mathrm{KL}\big(\mathrm{Bern}(p_{1,ij}) \| \mathrm{Bern}(p_n)\big),$$

其中 $p_{1,ij} = p_n^{\mathrm{in}}$ 当 $\sigma(i) = \sigma(j)$ 时，否则为 $p_{1,ij} = p_n^{\mathrm{out}}$，其中 σ 为社区分配。将块内和块间的配对分组，可得

$$D_n = N_n^{\mathrm{in}}\,\mathrm{KL}\big(\mathrm{Bern}(p_n^{\mathrm{in}}) \| \mathrm{Bern}(p_n)\big) + N_n^{\mathrm{out}}\,\mathrm{KL}\big(\mathrm{Bern}(p_n^{\mathrm{out}}) \| \mathrm{Bern}(p_n)\big).$$

对于渐近分析，记 $r_n := p_n = c/n$，并对一般的 $\delta \in \{\lambda, -\lambda\}$，

$$q_n := r_n + \frac{\delta}{n} = \frac{c + \delta}{n}.$$

对于一个参数为 q_n（对应于 $P_1^{(n)}$）且参数为 r_n（对应于 $P_0^{(n)}$）的单条边，其 KL 散度为

$$K_n(\delta) := \mathrm{KL}\big(\mathrm{Bern}(q_n) \| \mathrm{Bern}(r_n)\big) = q_n \log\frac{q_n}{r_n} + (1 - q_n)\log\frac{1 - q_n}{1 - r_n}.$$

第一项是

$$q_n \log\frac{q_n}{r_n} = \frac{c + \delta}{n}\log\frac{(c + \delta)/n}{c/n} = \frac{c + \delta}{n}\log\frac{c + \delta}{c}.$$

第二项使用 $\log(1-x) = -x - x^2/2 + O(x^3)$ 作为 $x \to 0$:

$$\log(1-q_n) = -\frac{c+\delta}{n} - \frac{(c+\delta)^2}{2n^2} + O\left(\frac{1}{n^3}\right), \qquad \log(1-r_n) = -\frac{c}{n} - \frac{c^2}{2n^2} + O\left(\frac{1}{n^3}\right),$$

so

$$\log\frac{1-q_n}{1-r_n} = -\frac{\delta}{n} - \frac{(c+\delta)^2 - c^2}{2n^2} + O\left(\frac{1}{n^3}\right) = -\frac{\delta}{n} + O\left(\frac{1}{n^2}\right).$$

两边乘以 $1 - q_n = 1 + O(1/n)$，得到

$$(1-q_n)\log\frac{1-q_n}{1-r_n} = -\frac{\delta}{n} + O\left(\frac{1}{n^2}\right).$$

因此

$$K_n(\delta) = \frac{c+\delta}{n}\log\frac{c+\delta}{c} - \frac{\delta}{n} + O\left(\frac{1}{n^2}\right),$$

从而

$$n\,K_n(\delta) = (c+\delta)\log\frac{c+\delta}{c} - \delta + O\left(\frac{1}{n}\right).$$

Now

$$D_n = N_n^{\text{in}} K_n(\lambda) + N_n^{\text{out}} K_n(-\lambda),$$

so

$$\frac{D_n}{n} = \frac{N_n^{\text{in}}}{n} K_n(\lambda) + \frac{N_n^{\text{out}}}{n} K_n(-\lambda).$$

在块大小相等的对称二块随机块模型中,

$$N_n^{\text{in}} = \frac{n^2}{4} + O(n), \qquad N_n^{\text{out}} = \frac{n^2}{4} + O(n),$$

so

$$\frac{N_n^{\text{in}}}{n} = \frac{n}{4} + O(1), \qquad \frac{N_n^{\text{out}}}{n} = \frac{n}{4} + O(1).$$

因此

$$\begin{aligned}\frac{D_n}{n} &= \left(\frac{n}{4} + O(1)\right) K_n(\lambda) + \left(\frac{n}{4} + O(1)\right) K_n(-\lambda) \\ &= \frac{1}{4}\Big\{nK_n(\lambda) + nK_n(-\lambda)\Big\} + O\big(K_n(\lambda) + K_n(-\lambda)\big).\end{aligned}$$

利用 $K_n(\delta) = O(1/n)$ 以及上文对 $nK_n(\delta)$ 的展开式，可得

$$\begin{aligned}\frac{D_n}{n} &= \frac{1}{4}\Big[(c+\lambda)\log\frac{c+\lambda}{c} - \lambda + (c-\lambda)\log\frac{c-\lambda}{c} + \lambda\Big] + O\left(\frac{1}{n}\right) \\ &= \frac{1}{4}\Big[(c+\lambda)\log\frac{c+\lambda}{c} + (c-\lambda)\log\frac{c-\lambda}{c}\Big] + O\left(\frac{1}{n}\right).\end{aligned}$$

这表明

$$\frac{D_n}{n} \xrightarrow[n\to\infty]{} I(\lambda) := \frac{1}{4}\Big[(c+\lambda)\log\frac{c+\lambda}{c} + (c-\lambda)\log\frac{c-\lambda}{c}\Big],$$

因此 $D_n = I(\lambda)\,n + o(n)$。

最后，对 $I(\lambda)$ 关于 λ 在 0 附近进行泰勒展开，得到

$$I(\lambda) = \frac{\lambda^2}{4c} + O\left(\frac{\lambda^4}{c^3}\right), \qquad \lambda \to 0,$$

正如所声称的。 □

引理的证明4.2

证明。 由于边在 $P_{(n)\,0}$和 $P_1^{(n)}$ 下相互独立，

$$\sum_A P_0^{(n)}(A)^{1-t} P_1^{(n)}(A)^t = \prod_e \sum_{a\in\{0,1\}} P_{0,e}(a)^{1-t} P_{1,e}(a)^t,$$

其中 $P_{0,\ e}$ = 服从 Bern(p_n) 分布，而 $P_{1,\ e}$ = 根据 e 是否为块内或块间边，服从 Bern(p_n^{in}) 或 Bern(p_n^{out}) 分布。因此

$$\mathcal{C}_n = \sup_{0\le t\le 1}\Big(N_n^{\text{in}}\phi_n^+(t) + N_n^{\text{out}}\phi_n^-(t)\Big),$$

其中，对于 $r,\ q\in\in(0,\ 1)$,

$$\phi(r,q;t) := -\log\big(r^{1-t}q^t + (1-r)^{1-t}(1-q)^t\big),$$

and

$$\phi_n^+(t) := \phi\big(p_n, p_n^{\text{in}}; t\big), \qquad \phi_n^-(t) := \phi\big(p_n, p_n^{\text{out}}; t\big).$$

令 $u := 1/n$，并注意 $p_n = cu$, $p_n^{\text{in}} = (c+\lambda)u$, $p_n^{\text{out}} = (c-\lambda)u$。对固定的 $c,\ \lambda,\ t$，将 $\phi_n^{\pm}(t)$ 展开为 $u\to 0$。记

$$r := cu, \qquad q_\pm := (c\pm\lambda)u,$$

so

$$\phi(r,q_\pm;t) = -\log\Big(r^{1-t}q_\pm^t + (1-r)^{1-t}(1-q_\pm)^t\Big).$$

Let

$$S_\pm := r^{1-t}q_\pm^t + (1-r)^{1-t}(1-q_\pm)^t.$$

将第二项因式分解:

$$S_\pm = (1-r)^{1-t}(1-q_\pm)^t\left[1 + \frac{r^{1-t}q_\pm^t}{(1-r)^{1-t}(1-q_\pm)^t}\right],$$

so

$$\phi(r,q_\pm;t) = -(1-t)\log(1-r) - t\log(1-q_\pm) - \log\Big(1 + \frac{r^{1-t}q_\pm^t}{(1-r)^{1-t}(1-q_\pm)^t}\Big).$$

利用 $\log(1-x) = -x - x^2/2 + O(x^3)$ 和 $r,\ q_\pm = O(u)$,

$$-(1-t)\log(1-r) - t\log(1-q_\pm) = (1-t)r + tq_\pm + O(u^2) = uc + ut(\pm\lambda) + O(u^2).$$

此外,

$$r^{1-t}q_\pm^t = c^{1-t}(c\pm\lambda)^t u + O(u^2),$$

且 $(1-r)^{1-t}(1-q_\pm)^t = 1 + O(u)$，因此

$$\frac{r^{1-t}q_\pm^t}{(1-r)^{1-t}(1-q_\pm)^t} = c^{1-t}(c\pm\lambda)^t u + O(u^2).$$

因此

$$-\log\Big(1 + \frac{r^{1-t}q_\pm^t}{(1-r)^{1-t}(1-q_\pm)^t}\Big) = -c^{1-t}(c\pm\lambda)^t u + O(u^2).$$

结合,

$$\phi_n^{\pm}(t) = u\Big[c \pm t\lambda - c^{1-t}(c\pm\lambda)^t\Big] + O(u^2),$$

因此

$$n\,\phi_n^{\pm}(t) = c \pm t\lambda - c^{1-t}(c \pm \lambda)^t + O\!\left(\frac{1}{n}\right).$$

利用上述区块计数,

$$\frac{N_n^{\text{in}}}{n} = \frac{n-2}{4} = \frac{n}{4} + O(1), \qquad \frac{N_n^{\text{out}}}{n} = \frac{n}{4},$$

so

$$\frac{\mathcal{C}_n}{n} = \sup_{0\le t\le 1}\left\{\frac{N_n^{\text{in}}}{n}\phi_n^{+}(t) + \frac{N_n^{\text{out}}}{n}\phi_n^{-}(t)\right\} = \sup_{0\le t\le 1}\left\{\frac{1}{4}\big[n\phi_n^{+}(t) + n\phi_n^{-}(t)\big] + O\!\left(\frac{1}{n}\right)\right\}.$$

利用 $n\phi_n^{\pm}(t)$ 的展开并令 $n\to\infty$,

$$\begin{aligned}\lim_{n\to\infty}\frac{\mathcal{C}_n}{n} &= \sup_{0\le t\le 1}\frac{1}{4}\Big[\big(c + t\lambda - c^{1-t}(c+\lambda)^t\big) + \big(c - t\lambda - c^{1-t}(c-\lambda)^t\big)\Big] \\ &= \sup_{0\le t\le 1}\frac{1}{4}\Big[2c - c^{1-t}\big((c+\lambda)^t + (c-\lambda)^t\big)\Big] = J(\lambda),\end{aligned}$$

由此证明了所声称的极限。

对于小信号展开，在 λ 中展开 $(c\pm\lambda)^t$:

$$(c\pm\lambda)^t = c^t\Big(1 \pm t\frac{\lambda}{c} + \frac{t(t-1)}{2}\frac{\lambda^2}{c^2} + O\!\left(\frac{\lambda^3}{c^3}\right)\Big), \qquad \lambda\to 0.$$

求和得,

$$(c+\lambda)^t + (c-\lambda)^t = 2c^t\Big(1 + \frac{t(t-1)}{2}\frac{\lambda^2}{c^2} + O\!\left(\frac{\lambda^4}{c^4}\right)\Big),$$

so

$$c^{1-t}\big[(c+\lambda)^t + (c-\lambda)^t\big] = 2c\Big(1 + \frac{t(t-1)}{2}\frac{\lambda^2}{c^2} + O\!\left(\frac{\lambda^4}{c^4}\right)\Big).$$

因此

$$J(\lambda;t) := \frac{1}{4}\Big\{2c - c^{1-t}\big[(c+\lambda)^t + (c-\lambda)^t\big]\Big\} = -\frac{t(t-1)}{4c}\,\lambda^2 + O\!\left(\frac{\lambda^4}{c^3}\right),$$

对 t 属于 $(0,\ 1)$ 的紧子集一致成立。由于 $-t(t-1)\ \ge 0$ 在 $[0,1]$ 上取值，并在 $t = 1/2$ 处达到其最大值$1/4$,

$$J(\lambda) = \sup_{0\le t\le 1} J(\lambda;t) = \frac{\lambda^2}{16c} + O\!\left(\frac{\lambda^4}{c^3}\right), \qquad \lambda\to 0.$$

这也得出了所述的渐近关系 $J(\lambda)\ = \frac{1}{4}I(\lambda)\ + O(\lambda^4/c^3)$。– □

引理的证明4.4

证明。在参数为 $(\pi,\ P_0)$ 或 $(\pi,\ P_\lambda)$ 的带标签随机块模型下，我们可以构造 G_n a s

$$Z_1,\dots,Z_n \overset{\text{i.i.d.}}{\sim} \pi, \qquad A_{ij}\mid Z_{1:n} \sim \text{Bern}\big(P_\lambda(Z_i,Z_j)\big), \quad 1\le i<j\le n,$$

在无序对 $(i,\ j)$ 之间相互独立。由此得到的图上的分布为 $\mathbb{P}_\lambda^{(n)}$ ，对于 $(\pi,\ P_0)$ 也类似，为 $\mathbb{P}_0^{(n)}$ 。

对于阶梯图子 W_0， W_λ，图函数抽样方案为

$$U_1,\dots,U_n \overset{\text{i.i.d.}}{\sim} \mathrm{Unif}[0,1], \qquad A_{ij} \mid U_{1:n} \sim \mathrm{Bern}\big(W_\lambda(U_i,U_j)\big), \quad 1 \le i < j \le n,$$

并且各边之间仍相互独立。将 $[0,1]$ 划分为 K 个长度为 π_k 的子区间，并定义 Z_i 为 U_i 的块索引，即满足 U_i 位于块 k 中的唯一 k。于是 $Z_1,\dots,Z_n$ 独立同分布$\sim$ π，并且

$$W_\lambda(U_i,U_j) = P_\lambda(Z_i,Z_j) \qquad \text{for all } 1 \le i < j \le n.$$

因此，给定 $(Z_i)_{i=1}^n$后，图子模型下的邻接矩阵与带标签随机块模型下的分布相同，因而 G_n 上的边缘分布一致：

$$\widetilde{\mathbb{P}}^{(n)}_{W_\lambda} = \mathbb{P}^{(n)}_\lambda, \qquad \widetilde{\mathbb{P}}^{(n)}_{W_0} = \mathbb{P}^{(n)}_0.$$

由于这两种分布在有限 n下完全一致，这一对分布的任何泛函在两种表示下都相同。特别是，

$$D\big(\mathbb{P}^{(n)}_\lambda \| \mathbb{P}^{(n)}_0\big) = D\big(\widetilde{\mathbb{P}}^{(n)}_{W_\lambda} \| \widetilde{\mathbb{P}}^{(n)}_{W_0}\big),$$

并且，对于每个半径 $\mathcal{C}_n$，

$$J_n\big(\mathbb{P}^{(n)}_\lambda, \mathbb{P}^{(n)}_0; \mathcal{C}_n\big) = J_n\big(\widetilde{\mathbb{P}}^{(n)}_{W_\lambda}, \widetilde{\mathbb{P}}^{(n)}_{W_0}; \mathcal{C}_n\big).$$

除以 n 并令 $n \to \infty$，即可得到 $I(\lambda)$ 和 $J(\lambda)$ 的所述恒等式。 □

定理证明4.5

证明。 令 $L_n(G_n)$表示对数似然比

$$L_n(G_n) := \log \frac{\mathrm{d}\widetilde{\mathbb{P}}^{(n)}_{W_\lambda}}{\mathrm{d}\widetilde{\mathbb{P}}^{(n)}_{W_0}}(G_n),$$

从而

$$\mathrm{BF}_n(G_n) = \frac{\pi_1}{\pi_0}\,\exp\{L_n(G_n)\},$$

且 φ_n^{BF}是两个简单图子假设 H_0和 H_1之间的似然比（贝叶斯因子）检验，其阈值固定并取决于先验分布。特别地，对于固定的 π_0， $\pi_1 \in (0,1)$，改变先验分布只会使似然比阈值平移一个常数，不会影响指数误差率。

根据引理 4.4，对于每个 n，图子分布 $\widetilde{\mathbb{P}}^{(n)}_{W_0}$ 和 $\widetilde{\mathbb{P}}^{(n)}_{W_\lambda}$ 在图上的分布与相应的带标签随机块模型分布 G_n 和 $\mathbb{P}^{(n)}_0$ 完全相同 $\mathbb{P}^{(n)}_\lambda$。特别地，

$$\widetilde{\mathbb{P}}^{(n)}_{W_0} = \mathbb{P}^{(n)}_0, \qquad \widetilde{\mathbb{P}}^{(n)}_{W_\lambda} = \mathbb{P}^{(n)}_\lambda,$$

作为公共图样本空间上的概率测度，因此，分布对的任何泛函（包括 KL 散度、切尔诺夫信息和决策论稳健性指标）在图子表示和带标签随机块模型表示中都相同。特别地，图子实验的逐顶点信息指标 $I(\lambda)$ 和决策论稳健性噪声指数 $J(\lambda)$ 与带标签随机块模型实验 $\big(\mathbb{P}^{(n)}_0,\ \mathbb{P}^{(n)}_\lambda\big)_{n\ge1}$中的相应指标一致。

针对两点实验的一般决策理论稳健检验结果（在其中所述的局部渐近正态性和二次稳健风险条件下）表明，对于任意半径

序列 $\mathcal{C}_n = o(n)$ 以及任意取值于 (0,1) 的固定先验分布，似然比检验的决策理论稳健贝叶斯风险满足

$$-\lim_{n\to\infty}\frac{1}{n}\log R_n^{\mathrm{WH}}(\varphi_n^{\mathrm{LR}};\mathcal{C}_n)=J(\lambda),$$

其中，φ_n^{LR}表示似然比检验，而 $J(\lambda)$ 是一个仅取决于该实验的极限单位顶点信息和噪声指标的泛函。

由于图子实验和带标签的随机块模型实验在 G_n 上诱导出相同的概率律，$I(\lambda)$，因此根据引理 4.4，它们具有相同的指标 $J(\lambda)$。因此，图子实验中的似然比检验/贝叶斯因子检验对于任意 $J(\lambda)$，都能达到相同的决策理论鲁棒性误差指数 $\mathcal{C}_n = o(n)$。这正是所要证明的等式

$$-\lim_{n\to\infty}\frac{1}{n}\log R_n^{\mathrm{WH}}(\varphi_n^{\mathrm{BF}};\mathcal{C}_n)=J(\lambda).$$

□

定理4.6的证明

证明。 根据假设，图子实验序列

$$\{\widetilde{\mathbb{P}}_W^{(n)} : W\in\mathcal{W}_n\}$$

满足与第 4.1 节中相同的局部渐近正态性和正则性条件。特别地，对于两点子实验

$$\big(\widetilde{\mathbb{P}}_{W_0}^{(n)},\widetilde{\mathbb{P}}_{W_\lambda}^{(n)}\big)_{n\ge1},$$

局部对数似然比具有带信息指标 $I(\lambda)$ 的二次展开，而决策理论鲁棒风险具有相应的、带噪声指标 $J(\lambda)$ 的二次近似。

因此，第 4.3 节的一般决策理论鲁棒极小极大下界适用于这个两点子实验，并对任意半径 $\mathcal{C}_n = o(n)$ 给出，

$$\liminf_{n\to\infty}\frac{1}{n}\log\inf_{\varphi_n}R_n^{\mathrm{WH}}\big(\varphi_n;W_0,W_\lambda,\mathcal{C}_n\big)\ \ge\ -J(\lambda).$$

根据 R_n^{WH}，$\mathcal{W}_n(\varphi_n;\mathcal{C}_n)$ 的定义，这等价于

$$\liminf_{n\to\infty}\frac{1}{n}\log\inf_{\varphi_n}R_{n,\mathcal{W}_n}^{\mathrm{WH}}(\varphi_n;\mathcal{C}_n)\ \ge\ -J(\lambda).$$

另一方面，定理 4.5 表明，贝叶斯因子检验 φ_n^{BF}在这个两点子实验中达到决策理论鲁棒误差指数 $J(\lambda)$：

$$-\lim_{n\to\infty}\frac{1}{n}\log R_n^{\mathrm{WH}}(\varphi_n^{\mathrm{BF}};\mathcal{C}_n)=J(\lambda).$$

由于 $\{W_0,W_\lambda\}\subset\mathcal{W}_n$ 对所有 n 均成立，我们有

$$R_{n,\mathcal{W}_n}^{\mathrm{WH}}\big(\varphi_n^{\mathrm{BF}};\mathcal{C}_n\big)=R_n^{\mathrm{WH}}(\varphi_n^{\mathrm{BF}};W_0,W_\lambda,\mathcal{C}_n),$$

因此

$$-\lim_{n\to\infty}\frac{1}{n}\log R_{n,\mathcal{W}_n}^{\mathrm{WH}}\big(\varphi_n^{\mathrm{BF}};\mathcal{C}_n\big)=J(\lambda).$$

结合极小极大下界与这一可达性结果可知，$J(\lambda)$ 确实是检验 W_0 与 W_λ 时，在图子类 $\mathcal{W}_n$ 中的非参数决策理论鲁棒性极小极大误差指数。

□

引理的证明4.7

回顾第 4.1.1 节， W_0 和 W_λ 表示分别对应稀疏 Erdős–Rényi 模型和双块随机块模型的阶梯函数图子，而 $P_{(n)0}$，无标号 和 $P_1^{(n)}$，无标号 表示图函数抽样方案下的诱导图分布。特别地，

$$P_{0,\mathrm{unlab}}^{(n)} = \widetilde{\mathbb{P}}_{W_0}^{(n)}, \qquad P_{1,\mathrm{unlab}}^{(n)} = \widetilde{\mathbb{P}}_{W_\lambda}^{(n)},$$

其中， $\widetilde{\mathbb{P}}_W^{(n)}$ 表示由图子 W生成的可交换随机图的分布。

另一方面，令 $\big(\mathbb{P}_0^{(n)},\ \mathbb{P}_\lambda^{(n)}\big)_{n\ge 1}$ 为潜在块标签为 Z_1、……、 Z_n 相互独立同分布$\sim\ \pi=(1/2,\ 1/2)$ 且边概率矩阵为 P_0， P_λ 的带标签随机块模型实验，具体如第 4.1节所述。也就是说，

$$A_{ij} \mid Z_{1:n} \sim \mathrm{Bernoulli}\big(P_m(Z_i,Z_j)\big), \quad 1\le i<j\le n, \quad m\in\{0,\lambda\},$$

i对无序对 $(i,\ j)$ 相互独立，且 $\mathbb{P}_m^{(n)}$ 是模型 m 下 G_n 的边缘分布。

对于阶梯图子 W_0， W_λ，图函数抽样方案为

$$U_1,\dots,U_n \overset{\text{i.i.d.}}{\sim} \mathrm{Unif}[0,1], \qquad A_{ij} \mid U_{1:n} \sim \mathrm{Bernoulli}\big(W_m(U_i,U_j)\big), \quad 1\le i<j\le n,$$

同样地，各边之间相互独立。将 $[0,1]$ 划分为两个长度分别为 $\pi_1=\pi_2=1/2$ 的子区间，并定义 Z_i 为 U_i 的块索引，即满足 U_i 位于块 k 中的唯一 $k\in\{1,2\}$。那么，Z_1、……、 Z_n 相互独立同分布$\sim\ \pi$，并且

$$W_\lambda(U_i,U_j)=P_\lambda(Z_i,Z_j), \qquad W_0(U_i,U_j)=P_0(Z_i,Z_j),$$

对所有 $1\le i<j\le n$ 均成立。因此，对 G_n 取边缘分布后，阶梯图子模型与潜在标签随机块模型在图上诱导出相同的分布：

$$\widetilde{\mathbb{P}}_{W_\lambda}^{(n)} = \mathbb{P}_\lambda^{(n)}, \qquad \widetilde{\mathbb{P}}_{W_0}^{(n)} = \mathbb{P}_0^{(n)},$$

这正是将引理 4.4应用于这些阶梯图子后的结果。

因此，

$$D_n^{\mathrm{unlab}} := \mathrm{KL}\big(P_{1,\mathrm{unlab}}^{(n)} \| P_{0,\mathrm{unlab}}^{(n)}\big) = \mathrm{KL}\big(\mathbb{P}_\lambda^{(n)} \| \mathbb{P}_0^{(n)}\big),$$

$P_0^{(n)}$，无标签与 $P_{(n)1}$，无标签之间的切尔诺夫信息，与 $\mathbb{P}_0^{(n)}$和$\mathbb{P}_\lambda^{(n)}$ 之间的切尔诺夫信息相同：

$$\mathcal{C}_n^{\mathrm{unlab}} := \sup_{0\le t\le 1} -\log \sum_A P_{0,\mathrm{unlab}}^{(n)}(A)^{1-t} P_{1,\mathrm{unlab}}^{(n)}(A)^t = \sup_{0\le t\le 1} -\log \sum_A \mathbb{P}_0^{(n)}(A)^{1-t} \mathbb{P}_\lambda^{(n)}(A)^t =: \mathcal{C}_n.$$

引理4.1和4.2 给出

$$\frac{1}{n}\,\mathrm{KL}\big(\mathbb{P}_\lambda^{(n)} \| \mathbb{P}_0^{(n)}\big) \longrightarrow I(\lambda), \qquad \frac{\mathcal{C}_n}{n} \longrightarrow J(\lambda),$$

从而

$$\frac{D_n^{\mathrm{unlab}}}{n} \to I(\lambda), \qquad \frac{\mathcal{C}_n^{\mathrm{unlab}}}{n} \to J(\lambda),$$

使得 $D_n^{\mathrm{unlab}} = I(\lambda)\ n + o(n)$ 且 $\mathcal{C}_n^{\mathrm{unlab}} = J(\lambda)\ n + o(n)$。

定理4.8 的证明

我们沿用定理中的记号： $M \in \{0,1\}$ 是模型索引，其先验分布为 $\Pi(M=0) = \Pi(M=1) = 1/2$，而 $P_{(n)\,0,\ \text{无标签}}$ ，$P_{1}^{(n)}$ ，无标签 是图上的无标签 Erdős–Rényi模型和随机块模型分布。

(i) 贝叶斯因子的 ***Chernoff*** 最优性。对于两个简单假设 $P_{0}^{(n)}$ ，unlab 和$P_{1}^{(n)}$ ，unlab ，在等先验分布和 0–1 损失下，似然比（贝叶斯因子）检验是贝叶斯最优的。令 $\mathcal{C}_n^{\text{unlab}}$表示 $P_{0}^{(n)}$ ，unlab 与 $P_{(n)\,1,\ \text{unlab}}$之间的切尔诺夫信息，即

$$\mathcal{C}_n^{\text{unlab}} := \sup_{0\le t\le 1} -\log \sum_{A} P_{0,\text{unlab}}^{(n)}(A)^{1-t} P_{1,\text{unlab}}^{(n)}(A)^{t}.$$

两个简单假设的经典切尔诺夫定理（例如，任何一本关于渐近假设检验的标准教材）意味着，最优贝叶斯风险（特别是误分类概率$R_{n,\ m}$）以指数 $\mathcal{C}_n^{\text{unlab}}$ 指数衰减，即

$$-\frac{1}{n}\log R_{n,m} \longrightarrow \lim_{n\to\infty} \frac{\mathcal{C}_n^{\text{unlab}}}{n}, \qquad m=0,1,$$

只要右侧的极限存在。

引理 4.7 表明，在稀疏区域 $p_n = c/n$,

$$\frac{\mathcal{C}_n^{\text{unlab}}}{n} \longrightarrow J(\lambda).$$

因此

$$-\frac{1}{n}\log R_{n,m} \longrightarrow J(\lambda), \qquad m=0,1,$$

这就证明了 (i) 部分。

(ii) 稳健贝叶斯风险。在给定 G_n 的条件下，令 $P_n(\cdot \mid G_n)$ 表示由先验分布 $1/2$ 和配对 $(P_{(n)\,0,\ \text{未标记}}$ $P_{1}^{(n)}$ ，未标记) 在 $M \in \{0,1\}$ 上诱导的后验分布，并定义（非稳健的）后验误分类概率

$$e_n(G_n) := \mathbb{E}_{P_n(\cdot\mid G_n)}\big[\mathbb{1}\{\delta_n(G_n) \neq M\}\big] = \min\big\{\Pi_n(M=0 \mid G_n), \Pi_n(M=1 \mid G_n)\big\}.$$

在真实模型 $m \in \{0,1\}$ 下，（非稳健的）误分类概率为

$$R_{n,m} = \mathbb{E}_{P_{m,\text{unlab}}^{(n)}}[e_n(G_n)].$$

固定 G_n ，并令 Q 为 $\{0,1\}$ 上任意满足 $\mathrm{KL}\big(Q\|P_n(\cdot \mid G_n)\big) \le \mathcal{C}_n$ 的替代后验分布。由于 M 仅取两个值，由 Pinsker不等式可得

$$\big\|Q - P_n(\cdot \mid G_n)\big\|_{\mathrm{TV}} \le \sqrt{\frac{1}{2}\,\mathrm{KL}\big(Q\|P_n(\cdot \mid G_n)\big)} \le \sqrt{\frac{\mathcal{C}_n}{2}}.$$

对于指示损失 $f(M) = \mathbb{1}\{\delta_n(G_n) \neq M\}$，对于 $\{0,1\}$ 上的任意两个概率测度 Q 和 P，有

$$\big|\mathbb{E}_Q[f(M)] - \mathbb{E}_P[f(M)]\big| \le \big\|Q-P\big\|_{\mathrm{TV}}.$$

将其应用于 $P = P_n(\cdot \mid G_n)$ 可得

$$\mathbb{E}_Q\big[\mathbb{1}\{\delta_n(G_n) \neq M\}\big] \leq e_n(G_n) + \sqrt{\frac{\mathcal{C}_n}{2}}.$$

对 Q 取上确界，满足 $\mathrm{KL}(Q\|P_n) \leq \mathcal{C}_n$ ，然后在 $P_{m,\mathrm{unlab}}^{(n)}$ 下取期望，unlab可得

$$\begin{aligned}\mathcal{R}_n^{\mathrm{WH}}(m;\mathcal{C}_n) &:= \mathbb{E}_{P_{m,\mathrm{unlab}}^{(n)}}\Big[\sup_{Q:\,\mathrm{KL}(Q\|P_n(\cdot|G_n))\leq\mathcal{C}_n} \mathbb{E}_Q\big[\mathbb{1}\{\delta_n(G_n) \neq M\}\big]\Big] \\ &\leq \mathbb{E}_{P_{m,\mathrm{unlab}}^{(n)}}[e_n(G_n)] + \sqrt{\frac{\mathcal{C}_n}{2}} \;=\; R_{n,m} + \sqrt{\frac{\mathcal{C}_n}{2}}.\end{aligned}$$

另一方面，将 $Q = P_n(\cdot \mid G_n)$ 移入上确界内可得

$$\mathcal{R}_n^{\mathrm{WH}}(m;\mathcal{C}_n) \geq \mathbb{E}_{P_{m,\mathrm{unlab}}^{(n)}}[e_n(G_n)] = R_{n,m}.$$

Thus

$$R_{n,m} \;\leq\; \mathcal{R}_n^{\mathrm{WH}}(m;\mathcal{C}_n) \;\leq\; R_{n,m} + \sqrt{\frac{\mathcal{C}_n}{2}}.$$

现在假设 $\mathcal{C}_n \downarrow 0$ 和

$$\mathcal{C}_n = o\big(R_{n,m}^2\big), \qquad \text{equivalently} \qquad \sqrt{\mathcal{C}_n} = o(R_{n,m}),$$

对于给定的 $m \in \{0,1\}$。则 $\sqrt{\mathcal{C}_n}/\mathcal{R}_{n,\ m} \to 0$ ，结合前面的式子可得

$$\mathcal{R}_n^{\mathrm{WH}}(m;\mathcal{C}_n) = R_{n,m}\,\big(1 + o(1)\big), \qquad m = 0, 1.$$

特别地，

$$-\frac{1}{n}\log \mathcal{R}_n^{\mathrm{WH}}(m;\mathcal{C}_n) = -\frac{1}{n}\log R_{n,m} + o(1) \longrightarrow J(\lambda),$$

由 (i) 得证。这就证明了 (ii)。

定理证明4.9

根据定义，

$$\begin{aligned}\mathfrak{R}_n^\star(\mathcal{C}_n) &= \inf_{\delta_n,\Pi_n}\sup_{P\in\mathcal{P}_n} \mathbb{E}_P\big[e_n^{\mathrm{rob}}(\mathcal{C}_n;G_n)\big] \\ &\geq \inf_{\delta_n,\Pi_n} \max\Big\{\mathbb{E}_{P_{0,\mathrm{unlab}}^{(n)}}\big[e_n^{\mathrm{rob}}(\mathcal{C}_n;G_n)\big], \mathbb{E}_{P_{1,\mathrm{unlab}}^{(n)}}\big[e_n^{\mathrm{rob}}(\mathcal{C}_n;G_n)\big]\Big\},\end{aligned}$$

因为 $P_{(n)\,0,\ \mathrm{unlab}}$ $P_1^{(n)}$ $_{,\ \mathrm{unlab}} \in \mathcal{P}_n$ 对于所有充分大的 n。

固定一个选择器 δ_n ，对于每个实现 G_n，令 $\Pi_n(\cdot \mid G_n)$ 表示由先验分布 $\Pi(M=0) = \Pi(M=1) = 1/2$ 和简单对 $\big(P_{(n)\,0,\ \mathrm{unlab}}$ $P_1^{(n)}$ $_{,\ \mathrm{unlab}}\big)$ 诱导的 $M \in \{0,1\}$ 上的后验分布。定义（非稳健的）后验误分类概率

$$e_n(G_n) := \mathbb{E}_{\Pi_n(\cdot|G_n)}\big[\mathbb{1}\{\delta_n(G_n) \neq M\}\big].$$

对于 $m \in \{0,1\}$，令

$$R_{n,m}(\delta_n) := \mathbb{E}_{P_{m,\mathrm{unlab}}^{(n)}}[e_n(G_n)].$$

对于每个 G_n，稳健化误差泛函满足

$$e_n^{\mathrm{rob}}(\mathcal{C}_n;G_n)=\sup_{Q:\,\mathrm{KL}(Q\|\Pi_n(\cdot|G_n))\le\mathcal{C}_n}\mathbb{E}_Q\big[\mathbb{1}\{\delta_n(G_n)\neq M\}\big]\ge\mathbb{E}_{\Pi_n(\cdot|G_n)}\big[\mathbb{1}\{\delta_n(G_n)\neq M\}\big]=e_n(G_n),$$

因为我们可以在上确界中取 $Q=\Pi_n(\cdot\mid G_n)$。因此，对每个 $m\in\{0,1\}$,

$$\mathbb{E}_{P^{(n)}_{m,\mathrm{unlab}}}\big[e_n^{\mathrm{rob}}(\mathcal{C}_n;G_n)\big]\ge\mathbb{E}_{P^{(n)}_{m,\mathrm{unlab}}}[e_n(G_n)]=R_{n,m}(\delta_n).$$

先对 m 取最大值，再对选择器 δ_n 取下确界（其中 Π_n 是相应的后验分布），得到

$$\mathfrak{R}_n^\star(\mathcal{C}_n)\ \ge\ \inf_{\delta_n}\max_{m\in\{0,1\}}R_{n,m}(\delta_n).$$

为了确定右侧的指数速率，考虑一个贝叶斯双点实验：$M\in\{0,1\}$ 以先验分布 $\Pi(M=0)=\Pi(M=1)=1/2$ 抽取，然后从 $P_M^{(n)}$，无标记 中抽取 G_n。对于任意选择器 δ_n，我们可以将贝叶斯（混合）误分类风险写为

$$r_n(\delta_n):=\mathbb{P}\big(\delta_n(G_n)\neq M\big)=\frac12\,\mathbb{P}_{P^{(n)}_{0,\mathrm{unlab}}}\big(\delta_n(G_n)\neq0\big)+\frac12\,\mathbb{P}_{P^{(n)}_{1,\mathrm{unlab}}}\big(\delta_n(G_n)\neq1\big).$$

另一方面，根据 $e_n(G_n)$ 的定义，以及联合先验—似然模型下的全期望公式,

$$r_n(\delta_n)=\mathbb{E}_{G_n}\big[e_n(G_n)\big]=\frac12\,R_{n,0}(\delta_n)+\frac12\,R_{n,1}(\delta_n).$$

因此，对每个 δ_n,

$$\max_{m\in\{0,1\}}R_{n,m}(\delta_n)\ \ge\ r_n(\delta_n),$$

因此

$$\inf_{\delta_n}\max_m R_{n,m}(\delta_n)\ \ge\ \inf_{\delta_n}r_n(\delta_n),$$

其中，右侧是以等先验检验两个简单假设$P_0^{(n)}$,unlab和 $P_{(n)\,1,\mathrm{unlab}}$时的经典最小贝叶斯风险。

众所周知（简单假设检验的 Chernoff 理论），似然比/贝叶斯因子检验 δ_n^{LR} 可在忽略次指数因子的意义下达到这一最小贝叶斯风险，且其错误概率满足

$$-\log r_n(\delta_n^{\mathrm{LR}})=\mathcal{C}_n^{\mathrm{unlab}}+O(1),$$

其中，$\mathcal{C}_n^{\mathrm{unlab}}$是 $P_0^{(n)}$,unlab与 $P_{(n)\,1,\mathrm{unlab}}$之间的切尔诺夫信息。由引理 4.7,

$$\mathcal{C}_n^{\mathrm{unlab}}=J(\lambda)\,n+o(n),$$

so

$$-\frac1n\log\big(\inf_{\delta_n}r_n(\delta_n)\big)\longrightarrow J(\lambda),\qquad n\to\infty.$$

特别地，$\inf_{\delta_n}r_n(\delta_n)$ 以速率 $\exp\{-J(\lambda)n+o(n)\}$ 衰减，并且根据不等式 $\inf_{\delta_n}\max_m R_{n,m}(\delta_n)\ \ge\inf_{\delta_n}r_n(\delta_n)$,相同的指数下界也适用于 $\inf_{\delta_n}\max_m R_{n,m}(\delta_n)$。

C将其与先前的界 $\mathfrak{R}_n^\star(\mathcal{C}_n)\ \ge\inf_{\delta_n}\max_m R_{n,m}(\delta_n)$ 结合，可得

$$\limsup_{n\to\infty}\frac1n\log\frac{1}{\mathfrak{R}_n^\star(\mathcal{C}_n)}\ \le\ \limsup_{n\to\infty}\frac1n\log\frac{1}{\inf_{\delta_n}\max_m R_{n,m}(\delta_n)}=J(\lambda),$$

即（6）。特别地，不存在任何程序（估计量、后验分布以及半径（$\mathcal{C}_n$）的选择）能够在 J（λ）上取得严格大于 $\mathcal{P}_n$ 的指数误差率。

定理证明4.10

对于下界，应用定理 4.9，其中 $\mathcal{P}_n = \{P_W^{(n)} : \ W \in \mathcal{W}_n\}$， P (n) W表示由 W诱导的图分布。根据假设，对于所有充分大的 n， W_0，$W_\lambda \in \mathcal{W}_n$因此 P (n) W_0和 $P_{W_\lambda}^{(n)}$都属于 $\mathcal{P}_n$，而在 $\mathcal{P}_n$ 上的非参数极小极大稳健风险不可能具有优于 $J(\lambda)$ 的指数速率。

对于上界，令 δ_n 为 $M \in \{0,1\}$ 上先验概率相等时区分 W_0 和 W_λ 的贝叶斯因子（似然比）检验，并令 $\Pi_n(\cdot \mid G_n)$ 表示相应的 M 后验分布。将所得的（非鲁棒）贝叶斯误分类概率记为

$$R_n := \max_{m\in\{0,1\}} \mathbb{P}_{P_{W_m}^{(n)}}\big(\delta_n(G_n) \neq m\big).$$

根据定理 4.8(i)，

$$-\frac{1}{n}\log R_n \ \longrightarrow \ J(\lambda).$$

现在令 $(\mathcal{C}_n)$ 为任意满足 $\mathcal{C}_n \downarrow 0$ 的序列，使得

$$\mathcal{C}_n = o(R_n^2), \qquad \text{i.e.} \qquad \sqrt{\mathcal{C}_n} = o(R_n).$$

特别地，由于 $R_n = \exp\{-J(\lambda)n + o(n)\}$，只需（且便于）要求

$$\mathcal{C}_n = o\big(\exp\{-2J(\lambda)n\}\big), \qquad \text{equivalently} \qquad \sqrt{\mathcal{C}_n} = o\big(\exp\{-J(\lambda)n\}\big).$$

根据定理 4.8(ii)，我们便有

$$\mathcal{R}_n^{\mathrm{WH}}(m;\mathcal{C}_n) = R_n(1+o(1)), \qquad m = 0,1.$$

对于任何其他 $P \in \mathcal{P}_n$， δ_n 的误分类概率至多为 1，且稳健化不会使其超过 1。因此

$$\begin{aligned}\mathfrak{R}_n^{\mathrm{WH}}(\mathcal{C}_n) &:= \inf_{\tilde\delta_n,\tilde\Pi_n}\sup_{P\in\mathcal{P}_n}\mathbb{E}_P\big[e_n^{\mathrm{rob}}(\mathcal{C}_n;G_n)\big] \\ &\le \sup_{P\in\mathcal{P}_n}\mathbb{E}_P\big[e_n^{\mathrm{rob}}(\mathcal{C}_n;G_n)\big] \le \max_{m\in\{0,1\}}\mathcal{R}_n^{\mathrm{WH}}(m;\mathcal{C}_n) = R_n(1+o(1)).\end{aligned}$$

因此

$$\liminf_{n\to\infty}\frac{1}{n}\log\frac{1}{\mathfrak{R}_n^{\mathrm{WH}}(\mathcal{C}_n)} \ \ge \ \liminf_{n\to\infty}\frac{1}{n}\log\frac{1}{R_n} = J(\lambda).$$

结合下界可得

$$\lim_{n\to\infty}\frac{1}{n}\log\frac{1}{\mathfrak{R}_n^{\mathrm{WH}}(\mathcal{C}_n)} = J(\lambda),$$

并表明，在图子类 $\mathcal{W}_n$ 上， W_0 与 W_λ 之间的贝叶斯因子检验在指数 $J(\lambda)$ 下是决策论稳健极小极大最优的。

命题5.1 的证明

根据定义，

$$\theta(\mu) := \frac{\mathbb{E}_\mu[D(D-1)]}{\mathbb{E}_\mu[D]}, \qquad \Delta(\mu) := 1-\theta(\mu),$$

因此，在次临界区间 $\theta(\mu) < 1$ 中，

$$R(\mu) := \frac{1}{1-\theta(\mu)} = \frac{1}{\Delta(\mu)}.$$

Thus

$$R(\mu) = \frac{c_0}{\Delta(\mu)} + H(\mu)$$

对所有满足 $\theta(\mu) < 1$ 的 μ，均有 $c_0 = 1$ and $H(\mu) \equiv 0$。

现在我们验证临界曲面附近的光滑性和梯度行为。固定度分布族的一个有限维参数化，例如一个光滑映射 $\vartheta \mapsto \mu_\vartheta$，其取值位于截断度分布单纯形的内部。对于此类参数化，映射 $\vartheta \mapsto \theta(\mu_\vartheta)$ 在 $\{\vartheta$ 上是 C^1 的：$\theta(\mu_\vartheta) < 1\}$，因此

$$\vartheta \mapsto R(\mu_\vartheta) = \big[1 - \theta(\mu_\vartheta)\big]^{-1}$$

在同一集合上。特别地，R 在 $\{\mu$ 的任意紧子集上都是光滑的：$\theta(\mu) < 1\}$。

W用参数 ϑ表示偏导数，由链式法则可得

$$\nabla_\vartheta R(\mu_\vartheta) = \frac{\nabla_\vartheta \theta(\mu_\vartheta)}{\big(1-\theta(\mu_\vartheta)\big)^2} = \Delta(\mu_\vartheta)^{-2}\, \nabla_\vartheta \theta(\mu_\vartheta).$$

设 $\vartheta_\star$ 是任意一点，满足 $\theta(\mu_{\vartheta_\star}) = 1$ 且 $\nabla_\vartheta \theta(\mu_{\vartheta_\star}) \neq 0$（以非退化方式趋近临界性）。由 $\nabla_\vartheta \theta$ 的连续性，存在 $\vartheta_\star$ 的一个邻域 N 以及常数 $0 < c_1 \leq c_2 < \infty$，使得

$$c_1 \;\leq\; \big\|\nabla_\vartheta \theta(\mu_\vartheta)\big\| \;\leq\; c_2 \qquad \text{for all } \vartheta \in N \cap \{\theta(\mu_\vartheta) < 1\}.$$

因此，在这个邻域内，对所有此类 ϑ，

$$c_1\, \Delta(\mu_\vartheta)^{-2} \;\leq\; \big\|\nabla_\vartheta R(\mu_\vartheta)\big\| = \Delta(\mu_\vartheta)^{-2} \big\|\nabla_\vartheta \theta(\mu_\vartheta)\big\| \;\leq\; c_2\, \Delta(\mu_\vartheta)^{-2}.$$

等价地，

$$\big\|\nabla_\vartheta R(\mu_\vartheta)\big\| \asymp \Delta(\mu_\vartheta)^{-2} \qquad \text{as } \Delta(\mu_\vartheta) \downarrow 0,\ \vartheta \to \vartheta_\star.$$

因此，$R(\mu) = 1/\Delta(\mu)$，其中 $\Delta(\mu) = 1 - \theta(\mu)$，且 $\|\nabla_\vartheta R(\mu_\vartheta)\| \asymp \Delta(\mu_\vartheta)^{-2}$ 在沿任意非退化路径趋近碎裂阈值时成立。这正是所选有限维参数化中的假设 3.1，其中 $\rho(\mu) = \theta(\mu)$，且 $\Delta(\mu) = 1 - \theta(\mu)$。

□

定理证明5.2

我们在配置模型子族中采用标准的两点论证。

步骤 1：选择一个近临界基点。固定一个满足 $\Delta_n \gg n^{-1/2}$ 的序列 $\Delta_n \downarrow 0$。对于每个 n，选择一个度分布$\mu_{0,\ n}$ 使得

$$\Delta(\mu_{0,n}) = 1 - \theta(\mu_{0,n}) \in [\Delta_n, 2\Delta_n],$$

根据 $\Delta(\mu)$ 的连续性，以及切片 $\{\mu :\ \Delta(\mu) \in [\Delta_n, 2\Delta_n]\}$ 对所有充分大的 n 均非空这一假设，这是可能的。

根据命题 5.1 和非退化条件 $\nabla_\mu \theta(\mu_\star) \neq 0$ 在临界曲面上，梯度 $\nabla_\mu \Delta(\mu) = -\nabla_\mu \theta(\mu)$ 连续，并且在该曲面的一个小

邻域内保持有界且与 0 保持正距离。因此，对于所有足够大的 n，我们可以选择一个单位方向向量 v_n 和一个常数 $c_\Delta > 0$，它们与 n 相互独立，使得

$$\left|\nabla_\mu \Delta(\mu_{0,n}) \cdot v_n\right| \;\geq\; c_\Delta > 0.$$

Let

$$h_n := \kappa n^{-1/2} v_n,$$

因此，对 某个稍小的常数 $\kappa > 0$，稍后再选取，并定义扰动后的参数 r

$$\mu_{1,n} := \mu_{0,n} + h_n.$$

Ta若 $\kappa > 0$ 足够小，我们可以确保对于所有充分大的 n，$\mu_{0,n}, \underline{\mu_{1,n}} \in (\mu, \mu)$.

步骤 2：两个构型的 KL 控制。考虑观测配置模型 $G_n \sim \mathrm{CM}_n(\mu)$ 的实验。我们可以按如下方式实现：首先抽取独立同分布度数$D_1, \ldots, D_n \sim \mu$（对 $\sum_i D_i$ 为偶数这一条件进行可忽略的条件化），然后对半边进行均匀随机配对。第二步是一个不依赖于 μ 的马尔可夫核，因此，根据数据处理不等式，

$$\mathrm{KL}\big(P^{(n)}_{\mu_{1,n}} \| P^{(n)}_{\mu_{0,n}}\big) \;\leq\; \mathrm{KL}\big(\mu_{1,n}^{\otimes n} \| \mu_{0,n}^{\otimes n}\big) = n\ \mathrm{KL}(\mu_{1,n} \| \mu_{0,n}).$$

我们采用一个固定的有限维参数化 $\vartheta \mapsto \mu_\vartheta$，其取值属于 (μ, μ)，并且关于 ϑ 光滑；同时假设度数的三阶矩一致有界。在此情形下，单次观测的 KL 散度具有局部二次展开：

$$\mathrm{KL}(\mu_{1,n} \| \mu_{0,n}) = \frac{1}{2}\, h_n^\top I(\mu_{0,n}) h_n + O(\|h_n\|^3),$$

其中，$I(\mu_{0,\ n})$ 是$\mu_{0,\ n}$处度分布的费舍尔信息矩阵。由于参数集 $(\mu,\ \mu)$ 是紧的，且 $I(\mu)$ 关于 μ 连续，因此有 $\sup_\mu \|I(\mu)\| < \infty$，从而

$$n\ \mathrm{KL}(\mu_{1,n} \| \mu_{0,n}) = \frac{1}{2}\, \kappa^2\, v_n^\top I(\mu_{0,n}) v_n + O(n^{-1/2}) \longrightarrow K_0 \in [0, \infty),$$

对于某个有限常数 K_0 proportional to κ^2。

通过选择足够小的 $\kappa > 0$，我们可以假设 $K_0 < 1$，并且对于所有足够大的 n,

$$\mathrm{KL}\big(P^{(n)}_{\mu_{1,n}} \| P^{(n)}_{\mu_{0,n}}\big) \leq K_0 + 1 < 2.$$

根据 Pinsker不等式,

$$\big\|P^{(n)}_{\mu_{1,n}} - P^{(n)}_{\mu_{0,n}}\big\|_{\mathrm{TV}} \leq \sqrt{\frac{1}{2}\ \mathrm{KL}\big(P^{(n)}_{\mu_{1,n}} \| P^{(n)}_{\mu_{0,n}}\big)} \leq \sqrt{\frac{K_0 + 1}{2}} =: 1 - \eta,$$

对于某个与 n 相互独立的 $\eta \in (0,\ 1)$。特别是，$P^{(n)}_{\mu_0,\ n}$与$P^{(n)}_{\mu_1,\ n}$ 之间的全变差距离一致地与 1 保持正距离。

步骤 3：在近临界切片上 $R(\mu)$ 中的分离。根据命题5.1，

$$R(\mu) = \frac{1}{\Delta(\mu)}, \qquad \Delta(\mu) = 1 - \theta(\mu),$$

并且 $\Delta(\mu)$ 是 C^1，其中 $\|\nabla_\mu \Delta(\mu)\|$ 在临界曲面 $\{\mu\colon \Delta(\mu) = 0\}$ 的某个邻域内有界且远离 0。

根据中值定理，对于每个 n，在线段$\mu_{0,n}$ 与$\mu_{1,n}$ 之间都存在 $\tilde{\mu}_n$，使得

$$\Delta(\mu_{1,n}) - \Delta(\mu_{0,n}) = \nabla_\mu \Delta(\tilde{\mu}_n) \cdot h_n.$$

当 $n \to \infty$ 时，我们有 $\Delta(\mu_{0,n}) \to 0$，因此 $\mu_{0,n}$（从而 $\tilde{\mu}_n$）趋近于临界曲面。由 $\nabla_\mu \Delta$ 的连续性以及在 $\mu_\star$ 处的非退化性，存在常数 $0 < c_1' \le c_2' < \infty$ 和 N，使得对所有 $n \ge N$，

$$c_1' \|h_n\| \;\le\; \big|\Delta(\mu_{1,n}) - \Delta(\mu_{0,n})\big| \;\le\; c_2' \|h_n\| = O\big(n^{-1/2}\big).$$

此外，$\|h_n\| = \kappa n^{-1/2}$ 且 $\Delta_n \gg n^{-1/2}$，因此对所有充分大的 n，

$$\big|\Delta(\mu_{1,n}) - \Delta(\mu_{0,n})\big| \le \tfrac{1}{4}\Delta_n.$$

由于 $\Delta(\mu_{0,n}) \in [\Delta_n, 2\Delta_n]$，这意味着对所有充分大的 n，

$$\Delta(\mu_{m,n}) \in [\Delta_n, 2\Delta_n], \qquad m = 0, 1,$$

因此，$\mu_{0,n}$ 和 $\mu_{1,n}$ 都位于近临界切片 $\{\mu$ 中：$\Delta(\mu) \in [\Delta_n, 2\Delta_n]\}$。

利用 $R(\mu) = 1/\Delta(\mu)$，

$$R(\mu_{1,n}) - R(\mu_{0,n}) = \frac{1}{\Delta(\mu_{1,n})} - \frac{1}{\Delta(\mu_{0,n})} = \frac{\Delta(\mu_{0,n}) - \Delta(\mu_{1,n})}{\Delta(\mu_{0,n})\,\Delta(\mu_{1,n})}.$$

在该切片上，对于 $m = 0,1$，有 $\Delta(\mu_{m,n}) \asymp \Delta_n$，且 $|\Delta(\mu_{1,n}) - \Delta(\mu_{0,n})| \asymp \|h_n\| = \kappa n^{-1/2}$。因此

$$\big|R(\mu_{1,n}) - R(\mu_{0,n})\big| \asymp \frac{\|h_n\|}{\Delta_n^2} = \frac{\kappa}{\sqrt{n}\,\Delta_n^2},$$

因此

$$\big(R(\mu_{1,n}) - R(\mu_{0,n})\big)^2 \asymp \frac{1}{n\,\Delta_n^4}, \tag{23}$$

其中常数与 n无关。

步骤 4：经典的两点极小极大下界。设 $a_n(G_n)$是 $R(\mu)$的任意估计量。对于平方损失，Le Cam 两点法表明，只要 $P_{\mu_0,n}^{(n)}$与 $P_{(n)\mu_{1,n}}$之间的全变差距离不超过某个 $1-\eta$，其中 $\eta > 0$，就有

$$\max_{m\in\{0,1\}} \mathbb{E}_{P_{\mu m,n}^{(n)}}\big[\big(a_n(G_n) - R(\mu_{m,n})\big)^2\big] \;\ge\; c_\eta \big(R(\mu_{1,n}) - R(\mu_{0,n})\big)^2,$$

其中 $c_\eta > 0$ 仅取决于 η。根据步骤 2，我们可以令 $\eta > 0$ 与 n相互独立，因此c_η 是一个固定的正常数。结合式（23）可得

$$\max_{m\in\{0,1\}} \mathbb{E}_{P_{\mu m,n}^{(n)}}\big[\big(a_n(G_n) - R(\mu_{m,n})\big)^2\big] \;\gtrsim\; \frac{1}{n\,\Delta_n^4},$$

其中的常数与 n相互独立。

对所有估计量 a_n 取下确界，表明近临界切片上的经典极小极大风险满足

$$\mathfrak{R}_n^{\mathrm{class}}(\Delta_n) \;\gtrsim\; \frac{1}{n\,\Delta_n^4},$$

这恰好是（7），其中 $c>0$。等价的 lim inf 表述可立即得到。正如定理陈述中所指出的，任何逐点支配经典平方误差风险的稳健化极小极大风险，也继承相同的下界。

□

定理 S.3（镜像下降对抗算法的复杂度）。设 Π 是参数空间 $\Theta\subset\mathbb{R}^d$ 上的参考后验，并固定半径 $C>0$。对于固定动作 a 和损失 $\ell(\theta):=\ell(a,\ \theta)$，定义稳健风险

$$R^{\mathrm{WH}}(\Pi, C) := \sup_{Q\ll\Pi:\, D_\phi(Q\|\Pi)\le C} \int_\Theta \ell(\theta)\, Q(\mathrm{d}\theta),$$

其中 D_ϕ 是一种 ϕ–散度。

假设：

1. 损失 ℓ: $\Theta\to\mathbb{R}$ 是 L–Lipschitz 连续的（相对于 Θ 上的欧几里得度量），且有界：对于所有 $\theta\in\Theta$, $|\ell(\theta)|\le M$。

2. 令 $\mathcal{Q}_C := \{Q \ll \Pi :\ D_\phi(Q\|\Pi) \le C\}$ 为散度球。泛函 $h(Q):=D_\phi(Q\|\Pi)$ 是 Fr´echet 可微的，并且在 $\|\cdot\|_{\mathrm{TV}}$ 的 $\mathcal{Q}_C$邻域上相对于全变差范数是 1–强凸的。我们使用相应的布雷格曼散度

$$D_h(Q\|Q') := h(Q) - h(Q') - \big\langle \nabla h(Q'), Q-Q' \big\rangle,$$

并交替记作 $D_h(Q\|Q')$ 和 $D_\phi(Q\|Q')$。

3. 对于每个 $Q\in\mathcal{Q}_C$，以 Q 为目标分布的约束哈密顿蒙特卡罗核满足以下关于 1–Wasserstein 距离 W_1 的混合界：存在常数 $A,B>0$（与 Q,d,δ相互独立），使得对于每个 $0<\delta<1/e$，存在一个整数 $K(Q,\delta)\le A\,d^{1/4}\log(B/\delta)$，满足

$$\mathbb{E}\big[W_1(\widetilde{Q}, Q)\big] \le \delta,$$

其中，$\widetilde{Q}$ 是经过 $K(Q,\delta)$ 步后 HMC 输出的概率分布。

考虑以下凸优化问题

$$\sup_{Q\in\mathcal{Q}_C} F(Q), \qquad F(Q) := \int_\Theta \ell(\theta)\, Q(\mathrm{d}\theta),$$

并令 $Q^\star\in\mathcal{Q}_C$为任意一个最大化点，使得 $R^{\mathrm{WH}}(\Pi,C) = F(Q^\star)$。

令 $(Q_t)_{t\ge1}$ 为镜像映射为 $h(Q)=D_\phi(Q\|\Pi)$、步长为 $\eta>0$、初始点为 $Q_1=\Pi$ 的（概念上的）镜像下降迭代序列，其定义如下：

$$Q_{t+1} := \arg\min_{Q\in\mathcal{Q}_C} \Big\{ \eta\,\langle g, Q\rangle + D_\phi(Q\|Q_t) \Big\}, \qquad g(\theta) := -\ell(\theta), \tag{24}$$

并定义平均迭代点

$$\widehat{Q}_T := \frac{1}{T}\sum_{t=1}^{T} Q_t.$$

在每次迭代 t中，我们使用精度为$\widetilde{\quad\quad}$ $\widetilde{\quad\quad}$、参数为 δ的约束哈密顿蒙特卡罗，从 Q_t 中近似采样，生成随机样本 $\theta_t \sim Q_t$，其中 Q_t 是HMC 输出的概率分布。定义稳健风险的蒙特卡罗估计

$$\widehat{R}_T := \frac{1}{T}\sum_{t=1}^{T} \ell(\theta_t).$$

那么，对于任意目标精度 $\varepsilon \in (0,\ 1)$，如果我们选择

$$T \ \geq \ \frac{8M^2C}{\varepsilon^2}, \qquad \eta \ = \ \sqrt{\frac{2C}{M^2T}}, \qquad \delta \ = \ \frac{\varepsilon}{2L},$$

则有

$$\left|R^{\mathrm{WH}}(\Pi, C) - \mathbb{E}[\widehat{R}_T]\right| \ \leq \ \varepsilon.$$

此外，在采用这些选择时，算法2 使用

$$T \ = \ O\!\left(\frac{M^2C}{\varepsilon^2}\right)$$

次镜像下降迭代（梯度计算），总共使用

$$O\!\left(d^{1/4}\,\frac{M^2C}{\varepsilon^2}\,\log\frac{L}{\varepsilon}\right)$$

步约束哈密顿蒙特卡罗。特别地，外层对抗优化对目标精度的依赖为多项式 $1/\varepsilon^2$，而内层采样复杂度关于维度的伸缩为 $d^{1/4}$ ，忽略对数因子。

证明。记

$$\mathcal{Q}_C := \{Q \ll \Pi : D_\phi(Q\|\Pi) \leq C\},$$

并定义凸泛函

$$f(Q) := -F(Q) = -\int_\Theta \ell(\theta)\, Q(\mathrm{d}\theta), \qquad Q \in \mathcal{Q}_C.$$

在 $\mathcal{Q}_C$ 上最大化 F 等价于在 $\mathcal{Q}_C$ 上最小化 f； f 的任何极小化点都是 F 的最大化点。

我们使用镜像下降，其镜像映射为 $h(Q) := D_\phi(Q\|\Pi)$，布雷格曼散度为 $D_\phi(Q\|Q')$。根据假设 (2)， h 关于邻域 $\mathcal{Q}_C$ 上的全变差范数 $\|\cdot\|_{\mathrm{TV}}$ Fr´echet 可微且为 1-强凸，因此

$$D_\phi(Q\|Q') \ \geq \ \frac{1}{2}\,\|Q - Q'\|_{\mathrm{TV}}^2 \qquad \text{for all } Q, Q' \text{ in this neighborhood.} \tag{25}$$

f 的梯度是如下（常数）符号函数

$$g(\theta) := -\ell(\theta),$$

其含义是，对于任意符号扰动 H，

$$\mathrm{D}f(Q)[H] = -\int_\Theta \ell(\theta)\, H(\mathrm{d}\theta) = \big\langle g, H \big\rangle.$$

我们将 g 视为对偶空间中的一个元素，其对偶范数为

$$\|g\|_* := \sup_{\|H\|_{\mathrm{TV}}\le 1} \big|\langle g, H\rangle\big| .$$

由 ℓ 的有界性以及全变差范数的定义，

$$\|g\|_* = \sup_{\|H\|_{\mathrm{TV}}\le 1} \left|\int_\Theta -\ell(\theta)\, H(\mathrm{d}\theta)\right| \le \sup_\theta |\ell(\theta)| \sup_{\|H\|_{\mathrm{TV}}\le 1} \|H\|_{\mathrm{TV}} \le M.$$

步骤 1：精确迭代的镜像下降不等式。镜像下降更新（24）可写为

$$Q_{t+1} = \arg\min_{Q\in\mathcal{Q}_C} \Big\{\eta\,\langle g, Q\rangle + h(Q) - h(Q_t) - \big\langle \nabla h(Q_t), Q - Q_t\big\rangle\Big\}.$$

由一阶最优性，对每个 $Q \in \mathcal{Q}_C$，我们有

$$\Big\langle \eta g + \nabla h(Q_{t+1}) - \nabla h(Q_t), Q - Q_{t+1}\Big\rangle \;\ge\; 0. \tag{26}$$

布雷格曼散度的三点恒等式表明，对任意 Q，Q'，Q''，

$$\big\langle \nabla h(Q') - \nabla h(Q''), Q - Q'\big\rangle = D_\phi(Q\|Q'') - D_\phi(Q\|Q') - D_\phi(Q'\|Q'').$$

将此应用于 $Q' = Q_{t+1}$、$Q'' = Q_t$ 和 $Q = Q^\star$，得到

$$\big\langle \nabla h(Q_{t+1}) - \nabla h(Q_t), Q^\star - Q_{t+1}\big\rangle = D_\phi(Q^\star\|Q_t) - D_\phi(Q^\star\|Q_{t+1}) - D_\phi(Q_{t+1}\|Q_t).$$

现在在（$Q = Q^\star$）中令26，得到

$$\eta\,\big\langle g, Q^\star - Q_{t+1}\big\rangle \;\ge\; D_\phi(Q^\star\|Q_t) - D_\phi(Q^\star\|Q_{t+1}) - D_\phi(Q_{t+1}\|Q_t).$$

重新排列后，

$$\big\langle g, Q_{t+1} - Q^\star\big\rangle \;\le\; \frac{1}{\eta}\Big(D_\phi(Q^\star\|Q_t) - D_\phi(Q^\star\|Q_{t+1}) - D_\phi(Q_{t+1}\|Q_t)\Big). \tag{27}$$

现在我们将 $Q_{t+1} - Q^\star$ 与 $Q_t - Q^\star$ 联系起来：

$$\big\langle g, Q_t - Q^\star\big\rangle = \big\langle g, Q_t - Q_{t+1}\big\rangle + \big\langle g, Q_{t+1} - Q^\star\big\rangle.$$

利用（27），然后应用柯西–施瓦茨不等式和强凸性（25），我们得到

$$\begin{aligned}\big\langle g, Q_t - Q^\star\big\rangle &\le \big\langle g, Q_t - Q_{t+1}\big\rangle \\ &\quad + \frac{1}{\eta}\Big(D_\phi(Q^\star\|Q_t) - D_\phi(Q^\star\|Q_{t+1}) - D_\phi(Q_{t+1}\|Q_t)\Big) \\ &\le \|g\|_*\,\|Q_t - Q_{t+1}\|_{\mathrm{TV}} \\ &\quad + \frac{1}{\eta}\Big(D_\phi(Q^\star\|Q_t) - D_\phi(Q^\star\|Q_{t+1}) - \tfrac{1}{2}\|Q_{t+1} - Q_t\|_{\mathrm{TV}}^2\Big).\end{aligned}$$

根据基本不等式 $ab \le \frac{\eta}{2}a^2 + \frac{1}{2\eta}b^2$，其中 $a = \|g\|_*$、$b = \|Q_t - Q_{t+1}\|_{\mathrm{TV}}$，可得

$$\|g\|_*\,\|Q_t - Q_{t+1}\|_{\mathrm{TV}} \le \frac{\eta}{2}\|g\|_*^2 + \frac{1}{2\eta}\|Q_t - Q_{t+1}\|_{\mathrm{TV}}^2.$$

将上述结果代入后，$\|Q_t - Q_{t+1}\|_{\mathrm{TV}}^2$ 项相互抵消，从而得到单步镜像下降不等式

$$\big\langle g, Q_t - Q^\star\big\rangle \;\le\; \frac{1}{\eta}\Big(D_\phi(Q^\star\|Q_t) - D_\phi(Q^\star\|Q_{t+1})\Big) + \frac{\eta}{2}\,\|g\|_*^2. \tag{28}$$

步骤 2：优化误差（精确迭代）。对（28）从 $t=1,\ \ldots\ldots,\ T$求和，得到

$$\sum_{t=1}^{T}\langle g, Q_t - Q^\star\rangle \ \le\ \frac{1}{\eta}\Big(D_\phi(Q^\star\|Q_1) - D_\phi(Q^\star\|Q_{T+1})\Big) + \frac{\eta T}{2}\,\|g\|_*^2.$$

由于 $D_\phi(\cdot\|\cdot) \ge 0$ 且 $Q_1 = \Pi$，我们得到

$$\sum_{t=1}^{T}\langle g, Q_t - Q^\star\rangle \ \le\ \frac{1}{\eta}D_\phi(Q^\star\|\Pi) + \frac{\eta T}{2}\,\|g\|_*^2 \ \le\ \frac{C}{\eta} + \frac{\eta T}{2}\,\|g\|_*^2,$$

因为 $Q^\star \in \mathcal{Q}_C$ 蕴含 $D_\phi(Q^\star\|\Pi) \le C$。

利用 $f(Q) = -F(Q)$，以及 f是梯度为 g的线性函数这一事实，我们有

$$f(Q_t) - f(Q^\star) = \langle g, Q_t - Q^\star\rangle \quad\Longrightarrow\quad F(Q^\star) - F(Q_t) = \langle g, Q_t - Q^\star\rangle.$$

Thus

$$\sum_{t=1}^{T}\big(F(Q^\star) - F(Q_t)\big) \ \le\ \frac{C}{\eta} + \frac{\eta T}{2}\,\|g\|_*^2.$$

两边除以 T，

$$\frac{1}{T}\sum_{t=1}^{T}\big(F(Q^\star) - F(Q_t)\big) \ \le\ \frac{C}{\eta T} + \frac{\eta}{2}\,\|g\|_*^2.$$

由于 F 是线性函数（因此既是凸函数也是凹函数），

$$F(Q^\star) - F(\widehat{Q}_T) = F(Q^\star) - \frac{1}{T}\sum_{t=1}^{T}F(Q_t) = \frac{1}{T}\sum_{t=1}^{T}\big(F(Q^\star) - F(Q_t)\big),$$

由此我们得出

$$F(Q^\star) - F(\widehat{Q}_T) \ \le\ \frac{C}{\eta T} + \frac{\eta}{2}\,\|g\|_*^2. \tag{29}$$

使用 $\|g\|_* \le M$后，29式变为

$$F(Q^\star) - F(\widehat{Q}_T) \ \le\ \frac{C}{\eta T} + \frac{\eta M^2}{2}.$$

右侧在 $\eta > 0$ 处取最小值

$$\eta^\star = \sqrt{\frac{2C}{M^2 T}},$$

对于该值

$$\frac{C}{\eta^\star T} + \frac{\eta^\star M^2}{2} = \sqrt{2}\,M\sqrt{\frac{C}{T}}.$$

因此

$$F(Q^\star) - F(\widehat{Q}_T) \ \le\ \sqrt{2}\,M\sqrt{\frac{C}{T}}. \tag{30}$$

特别是，如果

$$T \ \ge\ \frac{8M^2C}{\varepsilon^2}, \qquad \eta = \eta^\star,$$

then

$$F(Q^\star) - F(\widehat{Q}_T) \ \le\ \frac{\varepsilon}{2}.$$

~**步骤 3：HMC 近似带来的误差**。在第 t 次迭代时，令 Q_t 为 HMC~ 输出经过 $K(Q_t,\ \delta)$ 步、以 Q_t 为目标后的分布，并令 $\theta_t \sim Q_t$。根据假设 (3)，

$$\mathbb{E}\big[W_1(\widetilde{Q}_t, Q_t)\big] \le \delta.$$

由于 ℓ 在 $(\Theta,\ \|\cdot\|_2)$ 上是 L–Lipschitz 的，利用 W_1 的 Kantorovich–Rubinstein对偶性可得

$$\big|\mathbb{E}_{\widetilde{Q}_t}[\ell] - \mathbb{E}_{Q_t}[\ell]\big| \le L\, W_1(\widetilde{Q}_t, Q_t).$$

对 HMC随机性取期望，

$$\big|\mathbb{E}[\ell(\theta_t)] - F(Q_t)\big| \le L\,\mathbb{E}[W_1(\widetilde{Q}_t, Q_t)] \le L\delta.$$

定义

$$\widehat{R}_T = \frac{1}{T}\sum_{t=1}^{T} \ell(\theta_t), \qquad F(\widehat{Q}_T) = \frac{1}{T}\sum_{t=1}^{T} F(Q_t).$$

将上述界对 $t = 1,\ \ldots\ldots,\ T$ 取平均，得到

$$\big|\mathbb{E}[\widehat{R}_T] - F(\widehat{Q}_T)\big| \le L\delta. \tag{31}$$

因此，选择

$$\delta = \frac{\varepsilon}{2L}$$

可确保 HMC 导致的偏差至多为 $\varepsilon/2$。

步骤 4：合　并优化误差与采样误差。现在我们来界定总误 or

$$R^{\mathrm{WH}}(\Pi, C) - \mathbb{E}[\widehat{R}_T] = F(Q^\star) - \mathbb{E}[\widehat{R}_T].$$

根据三角不等式以及式（30）、式（31），

$$\begin{aligned}\big|F(Q^\star) - \mathbb{E}[\widehat{R}_T]\big| &\le \big|F(Q^\star) - F(\widehat{Q}_T)\big| + \big|F(\widehat{Q}_T) - \mathbb{E}[\widehat{R}_T]\big| \\ &\le \sqrt{2}\, M\sqrt{\frac{C}{T}} + L\delta.\end{aligned}$$

按照步骤 2 选择 T 和 η，并按照步骤 3 选择 $\delta = \varepsilon/(2L)$，则有

$$\sqrt{2}\, M\sqrt{\frac{C}{T}} \ \le\ \frac{\varepsilon}{2}, \qquad L\delta = \frac{\varepsilon}{2},$$

因此

$$\big|R^{\mathrm{WH}}(\Pi, C) - \mathbb{E}[\widehat{R}_T]\big| \le \varepsilon.$$

步骤 5：HMC采样复杂度。根据假设 (3)，对每个 Q_t 达到 Wasserstein精度δ，至多需要

$$K(Q_t, \delta) \le A\, d^{1/4} \log \frac{B}{\delta}$$

约束哈密顿蒙特卡罗步数。对于 $\delta = \varepsilon/(2L)$，这是

$$K(Q_t, \delta) = O\!\left(d^{1/4} \log \frac{L}{\varepsilon}\right),$$

关于 t 一致。由于我们在每次镜像下降迭代中运行一次 HMC，因此 HMC 步数总数为

$$T\,K(Q_t,\delta) = O\!\left(d^{1/4}\,\frac{M^2C}{\varepsilon^2}\,\log\frac{L}{\varepsilon}\right),$$

正如所述。镜像下降迭代（因此也包括损失评估）的次数为 $T = O(M^2C/\varepsilon^2)$。

□