arXiv:2602.00944v1 [math.NT] 1 Feb 2026

有理数域上多项式的蒙特卡洛不可约性与非本原性检测

IGOR RIVIN

Abstract. 我们研究用于测试 $\mathbb{Q}$上多项式不可约性并检测其算术非本原性的快速蒙特卡洛方法。

基于 Pemantle–Peres–Rivin 的子集和判据，我们开发了一种概率型不可约性测试。对于一般输入，该测试的预期运行时间（以检查的素数个数衡量）关于次数呈对数级增长。与标准的模不可约性测试不同，该方法会汇总模分解所得的信息，而不是丢弃未成功的尝试。

我们证明，若该测试未能通过，同时结合标准的模不可约性证书，则这是代数结构非一般性的强烈信号。特别是，这往往意味着伽罗瓦作用具有算术非本原性。我们提出一种显式且高效的蒙特卡洛算法，通过子域提取检测此类非本原性，并在非本原情形下构造代数证书。据我们所知，这是首个能够在高次数情形下检测 $\mathbb{Q}$ 上多项式算术非本原性的实用算法。

我们进一步证明，Pemantle–Peres–Rivin 检验产生的子集和数据可为多项式因式分解提供良好的初始条件：它能大幅缩小有理因子的可能次数范围，从而显著加快后续的提升过程。

所提出的方法在实践中的速度比已知的确定性算法快几个数量级，而且适用于次数远超当前确定性技术能力范围的多项式。

1. Introduction

1.1. 因式分解、不可约性与伽罗瓦群。 在 $\mathbb{Q}$上对多项式进行因式分解、检验不可约性以及确定伽罗瓦群，是计算代数和数论中的核心问题。确定性算法在理论上具有多项式时间复杂度，但在次数不高时也可能不实用；模方法则具有极强的可扩展性。

1.2. Pemantle–Peres–Rivin 子集和判据。 给定 f 模 p的因子次数（d_i），构造由所有和 $\sum_{i\in I} d_i$组成的子集和集合 S_p。如果 f 有一个次数为 d的有理因子，那么对所有好素数都有 $d \in S_p$。如果对抽样素数取交集后不包含任何非平凡次数，那么 f 不可约。

1.3. 失效模式与算术非本原性。 持续存在的子集和交集往往与算术非本原性相关，我们利用这一点作为快速结构标志。

日期：2026年2月3日。2020 数学主题分类。 11Y16, 12Y05, 12F10, 68W40.关键词和短语。 因式分解，蒙特卡罗，伽罗瓦群，非本原性。作者感谢Ramin Takloo-Bighash将这一系列问题重新带回作者的关注之中，感谢RichZippel在过去半个多世纪里产生了如此美妙的影响，并感谢Yuval Peres和Robin Pemantle为PPR方法奠定了基础方法论。

1.4. 贡献与概要。 我们提出了一种混合蒙特卡洛不可约性检验、一种能够生成显式证书的蒙特卡洛非本原性检测器，以及一种用于因式分解的热启动方法。

2. Algorithms and Complexity

2.1. 标准蒙特卡洛不可约性检验。 模素数 f 取模，并在f 模 p 不可约时停止，从而证明其在 $\mathbb{Q}$ 上不可约。

2.2. 基于 PPR 的不可约性检验。 对各素数 S_p 对应的子集和集合取交集；在一般性假设下，预期所需的素数数量为 $O(\log n)$ [3]。

2.3. 混合算法。 对 $O(\log n)$ 个素数运行 PPR；若仍无法得出结论，则改用标准检验。

2.4. 位复杂度与素数选择。 模因式分解需要 $\tilde{O}(n^2)$ 次域运-算 [1, 2, 4]；PPR 允许使用小得多的素数，从而减少 $\log p$ 因子。

3. Arithmetic Imprimitivity Detection

$\mathrm{Gal}(f/\mathbb{Q})$ 在根上的传递作用，如果保留一个非平凡块系，则称为非本原。等价地，若 $K = \mathbb{Q}(\alpha)$ 是根域，则非本原性等价于存在一个真中间域 $\mathbb{Q} \subsetneq M \subsetneq K$。

3.1. 蒙特卡洛检测器。当子集和检验失败（但仍能认证多项式不可约）时，我们将此作为结构标志，然后搜索 K 的非平凡子域。每当找到一个子域时，就会得到一份构造性证书。

3.2. **算例。**令 $P(u) = u^8 - u - 1$ 且

$$Q(u, x) = x^3 + \left(-\tfrac{1}{2}u - \tfrac{3}{2}\right) x^2 + \left(\tfrac{1}{2}u - \tfrac{3}{2}\right) x + 1.$$

构造 $F(x) = \mathrm{Res}_u(P(u)\ Q(u,\ x))$，其次数为 24。在 $K = \mathbb{Q}(\alpha)$ 中进行子域提取，使用 $F(\alpha) = 0$ 检测到一个由下式某个根生成的次数为 8 的子域：

$$y^8 + 24y^7 + 252y^6 + 1512y^5 + 5670y^4 + 13608y^3 + 20412y^2 - 256296y + 846369,$$

以及该域上关于 α 的相对三次方程：

$$x^3 + \left(-\tfrac{1}{2}y - \tfrac{3}{2}\right) x^2 + \left(\tfrac{1}{2}y - \tfrac{3}{2}\right) x + 1 = 0.$$

4. Warm-start factorization

当子集和交集没有坍缩时，保留下来的次数会给出一个较小的候选集 D，用于确定有理因子次数。将因子搜索限制在 $d \in D$，可以为 Hensel提升和重组方法提供良好的初始条件 [5, 4]。

这会将次数歧义从 $\{1, \ldots, n-1\}$ 缩减到一个小得多的集合，并能显著加快实际因式分解。

5. Examples and adversarial constructions

我们通过结式构造非本原族 $F(x) = \mathrm{Res}_u(P(u)\ Q(u,\ x))$。我们还通过将系数扰动为 $M = \prod_{p<B} p$ 的倍数来构造具有对抗性的“恶孪生”，从而保留模 $p < B$ 下的所有约化，同时通常恢复一般的全局伽罗瓦行为。

6. 结论

我们介绍了一系列用于测试多项式不可约性并分析其结构的蒙特卡洛算法，这些算法针对 $\mathbb{Q}$ 上的多项式，既有理论依据，又能在高次数情形下有效应用。

我们的首项贡献是提出了一种改进的概率不可约性测试，它建立在 Pemantle–Peres–Rivin 的子集和判据之上。对于一般输入，该方法只需考察 $O(\log n)$ 个素数，即可证实多项式不可约；同时，它会综合利用所有模因式分解的信息，而非丢弃未成功的试验。将其与标准的模不可约性测试结合后，可得到一种帕累托最优算法：其渐近性能绝不会逊于现有的蒙特卡洛方法，而且在实践中往往快得多。

我们的第二项贡献是发现：当子集和检验未能通过，但仍能证实多项式不可约时，这强烈表明其代数结构并非一般情形。利用这一现象，我们首次提出了一种实用的蒙特卡洛算法，用于检测有理数域上多项式的伽罗瓦作用的算术非本原性。与基于模统计量的纯启发式方法不同，我们的方法在非本原情形下能够给出明确的代数证书，具体形式为根域的非平凡子域及相应的相对方程。

第三，我们证明，不可约性测试所产生的子集和数据可以重复用于加速多项式因式分解。通过大幅限制可能的因子次数，这些信息为经典的提升和重组方法提供了一个良好的起点，在不引入新的模运算的情况下，降低了组合复杂度的重要来源。

在全文中，我们强调这些算法并非仅有理论意义。它们具有实用性，已得到实现，并且已成功应用于次数远超确定性因式分解和伽罗瓦群算法所能处理的范围。对模运算、小素数和信息聚合的依赖，使这些方法尤其适合大规模并行计算。

更广泛地说，我们的结果阐明了一条普遍原则：局部模数据经过适当聚合后可能包含丰富信息，但仅凭这些数据不足以认证全局代数结构。特别是，固定多项式模有限多个素数的因式分解模式，甚至固定其约化，并不能阻止算术伽罗瓦群一般而言尽可能大。因此，高效的认证需要将概率启发式方法与明确的域论构造相结合。我们希望，本文提出的技术既能作为实用工具，也能为进一步探索多项式算术算法提供一个框架。

Appendix A. Engineering considerations

标准蒙特卡洛测试和子集和方法都可以沿素数并行化。子集和方法会累积信息：每次模因式分解都会为证书作出贡献。PPR 还允许使用较小的素数，从而降低位复杂度中的 $\log p$ 因子。

References

[1] Elwyn R. Berlekamp. 大有限域上的多项式因式分解。*Mathematics of Computation*，24:713– 735，1970。

[2] David G. Cantor 和 Hans Zassenhaus。《有限域上多项式因式分解的新算法》。*Mathematics of Computation*，36:587–592，1981年。[3] Robin Pemantle、Yuval Peres 和 Igor Rivin。四个随机置换经对手共轭后以高概率生成 S_n 。《随机结构与算法》，49(3):409–428，2016年。[4] Joachim von zur Gathen 和 J¨urgen Gerhard。《现代计算机代数》。剑桥大学出版社，第三版，2013年。[5] Richard Zippel。稀疏多项式的概率算法。符号与代数计算，1:216–226，1979年。

Mathematics Department, Temple University电
子邮件地址：rivin@temple.edu