南开大学

Nankai University

南　　开　　大　　学

计　算　机　学　院

并行程序设计实验报告

期末研究开题报告

张明昆 2211585

年级：2022 级

专业：计算机科学与技术

指导教师：王刚

2024 年 4 月 7 日

摘要

本开题报告旨在探索 Gröbner 基高斯消元法的并行优化，以解决多元多项式理想成员判定问题中的高计算复杂度。Gröbner 基作为数学和计算代数领域的一个重要工具，虽然在多个领域有广泛应用，但其处理大规模问题时的效率低下是一个显著的短板。本研究提出的预计探索方向和实验设计，旨在通过并行计算和算法优化，显著提升 Gröbner 基高斯消元法在处理复杂问题时的性能。

关键字：Parallel Gröbner 基高斯消元法

目录

一、 背景介绍

(一) Gröbner 基简史

Gröbner 基,这个数学界的“瑞士军刀”,是经过数十年演变而来的。早在 1927 年,F.S.Macauly 就引入了全序的概念，对多项式的单项式进行排序，这为 Gröbner 基的诞生奠定了基础。而后，在 1964 年，H.Hironaka 在研究奇点分解时，引入了多项式除法算法，进一步拓宽了这一领域的研究。紧接着，在 1965 年，奥地利数学家 B.Buchberger 不仅引入了项序，确保了多项式除法的结果唯一性，还提出了 S-多项式的概念，并设计了计算 Gröbner 基的算法，即著名的 Buchberger 算法，从而开辟了解决多元多项式理想问题的新途径。

(二) Gröbner 基的应用

在密码学中，Gröbner 基扮演了解密的钥匙角色，特别是在处理多变量多项式方程系统的问题上，这些方程系统是多变量公钥密码体系的核心。通过解这些方程组，可以揭露加密信息，仿冒数字签名。然而，尽管 Gröbner 基提供了一种有效的求解工具，它的计算复杂度极高，早期的 Buchberger 算法效率低下，因此研究者们开发了更高效的算法，如 F4 和 F5。

Gröbner 基的计算虽然面临 NP 难题的挑战，但通过探索和利用系统内部的结构特征，可以显著提高算法的效率。例如，在某些布尔 Gröbner 基计算中，通过特殊的高斯消元方法来加速，展示了并行化算法潜力的一面。这正是我们研究的焦点，旨在通过并行计算，解锁 Gröbner 基算法的新可能。

二、 前人研究

在数学和计算代数领域，Gröbner 基的研究和开发已经走过了一段漫长而富有成果的道路。自 Buchberger 首次提出 Gröbner 基求解算法以来，众多科学家通过引入新的概念、方法和优化技术，极大地推动了这一领域的发展。以下是对这一进程的总结，重点介绍了几个关键的里程碑和最新进展。

- Buchberger 首次提出了 Gröbner 基求解算法，为后续研究奠定了基础。这一算法虽然开创性，但在处理复杂问题时效率不高。
- 继 Buchberger 之后，Lazard 引入了线性代数方法到 Gröbner 基的求解中，这一方法为后续的算法优化提供了新的思路。
- Faugère 提出了基于线性代数的 F4 算法和基于标签的 F5 算法，这两个算法被认为是目前求解 Gröbner 基最高效的方法。尤其是 F5 算法，它通过避免冗余计算和引入额外的检测标准来减少无效计算，虽然在执行效率上仍有提升空间。
- 在 F4 和 F5 算法的基础上，诸如 Arri-Perry(AP) [1]、Gao-Guan-Volny(G2V) [3] 和 Gao-Volny-Wang(GVW) [4] 等并行算法应运而生，进一步提高了 Gröbner 基计算的效率。除此之外，研究者还探索了对 Macaulay 矩阵的并行化改造、高效的约化准则以及利用 MPI 技术处理算法中间项的约化部分等优化方法 [5]
- Rodrigo Alexander Castro Campos 等人提出了针对布尔 Gröbner 基的有效实现策略，包括对 F4 算法的变体、新的并行实现 Buchberger 准则以及待定多项式的改进处理方法。[2]

通过这些年的不懈努力和创新，Gröbner 基的求解算法已经从早期的 Buchberger 算法发展到今天的高效并行算法。

三、 问题简介

(一) Gröbner 基的挑战

Gröbner 基为非线性多项式理想的成员判定提供了一种强大的计算代数方法，但其计算复杂度高，尤其在涉及大型问题时，传统算法往往难以承受计算负担。

(二) 特殊高斯消元算法

为了优化 Gröbner 基的计算过程，引入了一种特殊的高斯消元方法。这种方法针对的是有限域 GF(2) 上的运算，其特点包括：

- 运算数与规则：仅涉及 0 和 1 的运算，其中加法和乘法遵循特定的简化规则。
- 消元子模式：矩阵分为“消元子”和“被消元行”，其中消元子负责减去操作，被消元行则在消去过程中可能转换为消元子。

(三) 高效实现的追求

我们的研究旨在探索如何通过并行计算和算法优化，提高这一特殊高斯消元算法的效率，进而为 Gröbner 基的计算提供高效支持。这包括但不限于：

- 数据批处理：考虑矩阵规模可能达到百万级，如何有效地分批处理数据以适应内存限制。
- 并行化策略：如何利用并行计算优化消元子与被消元行的处理，加速整个消去过程。
- 优化消元过程：探索算法内部如何减少冗余计算，提高消元效率，包括消元行的升格机制和空行处理。

四、 拟采取的研究方案

在本研究中，我们将探索高斯消元法的并行化处理方法，特别关注于 Gröbner 基的计算过程，旨在提高高斯消元在多元多项式理想成员判定问题中的计算效率。高斯消元过程的并行化，特别是在处理大规模数据集时，具有显著的性能提升潜力。本研究将通过一系列实验，系统地探索和评估不同并行化策略在高斯消元法中的应用效果。

实验将在包括 Intel Devcloud、鲲鹏、金山云等多个平台上进行，利用 MPI、OpenMP、SIMD 等技术进行并行化优化，同时使用 CUDA 和 OneAPI 探索 GPU 优化的可能性。实验结果将基于性能提升比（Speedup）和执行时间等关键指标进行评估和比较。

(一) 实验一：MPI 多线程优化

- 目标：采用消息传递接口 (MPI) 实现高斯消元算法的多线程并行优化，并分析在不同任务规模下的性能表现。
- 方法：实验将以不同大小的数据集为基准，评估 MPI 并行化对算法性能的影响。

（二） 实验二：任务划分策略

- 目标：比较循环划分和块划分两种不同的任务划分策略，在高斯消元并行处理中的性能表现。
- 方法：通过实验评估在相同条件下，不同任务划分方式对性能的具体影响。

（三） 实验三：消息发送方式比较

- 目标：对比广播和流水线两种 MPI 消息发送方式，在并行高斯消元过程中的性能差异。
- 方法：实施两种通信机制，分析其在不同并行规模下的性能和效率。

（四） 实验四：结合 MPI 与 SIMD 向量化

- 目标：使用 MPI 配合 SIMD 向量化处理，探究并行化和向量化结合对性能的影响。
- 方法：在 MPI 并行框架下，引入 SIMD 向量化指令，评估其对算法加速的贡献。

（五） 实验五：多线程优化（MPI + OMP）

- 目标：结合 MPI 和 OpenMP（OMP）进行多线程优化，分析其性能提升。
- 方法：在 MPI 并行化基础上，进一步通过 OMP 实现线程级并行，对比单纯 MPI 并行的性能提升。

（六） 实验六：综合优化（MPI + SIMD + OMP）

- 目标：探索 MPI、SIMD 和 OMP 的综合并行优化效果。
- 方法：将 MPI 多进程并行、OMP 多线程优化和 SIMD 向量化处理结合起来，评估综合优化策略的性能。

（七） 实验七：平台迁移性能分析

- 目标：将 openmp 优化方法从 x86 平台迁移到 arm 平台上，分析性能表现。
- 方法：在两种硬件平台上实施相同的优化策略，比较并分析性能差异。

（八） 实验八：进程数量对性能的影响

- 目标：研究不同进程数量对 MPI 并行性能的影响。
- 方法：在固定的线程数下，调整进程数量，记录并分析性能变化。

本研究预期通过上述实验设计，深入理解并行化策略在高斯消元法中的应用效果，特别是在处理 Gröbner 基计算问题时的性能提升潜力。我们希望找到一种或多种有效的并行化方法，能够显著提高算法的执行效率，特别是在处理大规模数据集时。

参考文献

[1] A Arri and J Perry. The f5 criterion revised. *Journal of Symbolic Computation*, 46(9):1017–1029, 2001.

[2] Rodrigo Alexander Castro Campos, Feliú Davino Sagols Troncoso, and Francisco Javier Zaragoza Martínez. An efficient implementation of boolean gröbner basis computation. In *Latin American High Performance Computing Conference*, pages 116–130. Springer, 2016.

[3] Shu-hong Gao, Yin-hua Guan, and F Volny IV. A new incremental algorithm for computing gröbner bases. In *Proceedings of the 35th International Symposium on Symbolic and Algebraic Computation*, pages 13–19, New York, USA, 2010.

[4] Shu-hong Gao, F Volny, and Ming-sheng Wang. A new algorithm for computing gröbner bases, 2010. Online; accessed yyyy-mm-dd.

[5] 狄鹏. *Gröbner* **基生成算法的并行**. PhD thesis, 西安电子科技大学, 2015.