系统科学研究所

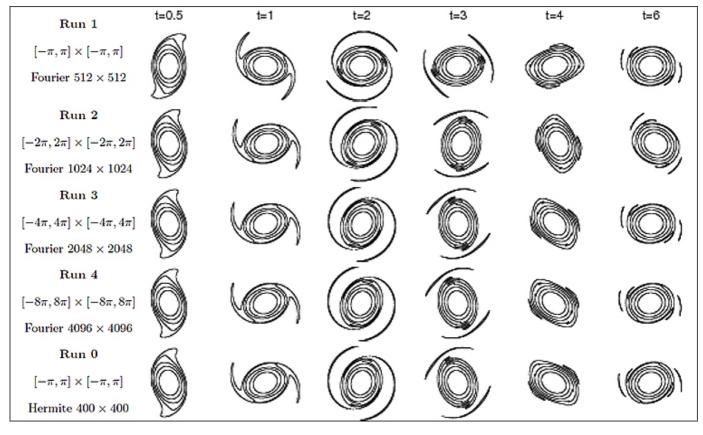
Institute of Systems Science, Academy of Mathematics and Systems Science , Chinese Academy of Sciences

首页 | 中国科学院

2019改版 > 科研进展、科技动态

求解HERMITE标准型的新算法研究进展

发布时间: 2018-12-03 | 来源: 数学机械化重点实验室



任意一个整数矩阵都可以通过初等变换约化为Hermite标准型。Hermite标准型在计算数论、公钥密码学等领域有十分广泛的应用。已有的计算Hermite标准型算法大致可分为两类,一类算法通过在某剩余类环中做三角化,然后再提升到整数环中得到Hermite标准型;另一类则是通过求解初等变换矩阵,然后通过矩阵乘积来得到Hermite标准型。

在2019年的符号与代数计算国际研讨会(ISSAC)上,信息技术部潘彦斌等[1]提出了一种求解整数矩阵 Hermite标准型的新算法。与之前进行初等变换或通过求解初等变换矩阵来计算Hermite标准型的方法不同,新算法通过求解带模线性方程组来计算Hermite标准型了其基本观察在于,整数矩阵前k列按行生成的格与其 Hermite标准型前k列按行生成的格完全相同,因此,整数矩阵前k列的任一行均可以写成其Hermite标准型的k 阶主子矩阵行的整系数线性组合,从而Hermite标准型的非对角线元素满足一个模其对角元的线性方程组,因此如果对角元已知,则可以通过求解该方程组得到增加的非型和发元素,从而可以更有效地控制中间变量的膨胀;另外,注意到对"随机"整矩阵而言,其Hermite标准型的对角线上最后一个元素,相对于其它对角线元素往往非常大,因此利用已有算法计算Hermite标准型前面的列,然后再利用新算法计算Hermite标准型的最后一列,往往更快,在合理假设下面,新算法的期望时间复杂度是同规模矩阵乘法复杂度的常数倍。

这项研究有助于在实践中加速已有的Hermite标准型求解算法,另外,对假设的研究,也为从理论上加速 Hermite标准型求解算法的时间复杂性提供了可行的途径。

[1] Renzhang Liu, Yanbin Pan.Computing Hermite Normal Form Faster via Solving System of Linear Equations. In Proc. Of ISSAC 2019.



版权所有 © 中国科学院系统科学研究所 京ICP备05002810号-1

地址:北京市海淀区中关村东路55号 邮编:100190

电话: 86-10-82541881

网址: http://iss.amss.cas.cn 技术支持: 青云软件

