西安电子科技大学学报 2007 34 (3): 360-362+397 ISSN: 1001-2400 CN: 61-1076/TN

有限域上乘法噪音多项式插值算法的改进

黄华伟, 李胜强, 陈汝伟, 肖国镇

(西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071)

收稿日期 修回日期 网络版发布日期 2007-5-31 接受日期

摘要 对J. von zur Gathen和I.E.Shparlinski提出的有限域上乘法噪音多项式插值算法进行了分析，提出了改进算法. 利用L.Babai最近向量格归约算法得到更精确的估计向量，再计算出插值多项式的倍数多项式的系数，从而计算出原插值多项式的系数. 改进算法降低了原算法中有限域阶的下界，对较小阶有限域上的多项式也可以进行乘法噪音插值.

关键词 多项式插值 模乘近似黑盒 格归约

分类号 TN918

Improved multiplicative noisy polynomial interpolation algorithm in the finite field

HUANG Hua-wei,LI Sheng-qiang,CHEN Ru-wei,XIAO Guo-zhen

(State Key Lab. of Integrated Service Networks, Xidian Univ., Xi′an 710071， China)

Abstract

This paper analyses a multiplicative noisy polynomial interpolation algorithm in the finite field presented by J. von zur Gathen and I. E. Shparlinski and presents an amended algorithm. By the lattice reduction algorithm on the nearest vector presented by L.Babai, a more accurate estimate vector can be obtained and the coefficients of the multiple polynomial of the interpolation polynomial can be computed. Then the coefficients of the original interpolation polynomial can be computed. The amended algorithm reduces the lower bound of the order of the finite field and can apply to the polynomials in the finite field whose order is lower.

Key words polynomial interpolation modular multiplicatively approximate black box(MMABB) lattice reduction

DOI:

通讯作者