第37卷 第16期 计 算 机 工 程 2011年8月
Vol.37 No.16 Computer Engineering August 2011

·软件技术与数据库· 文章编号：1000—3428(2011)16—0060—02 文献标识码：A 中图分类号：TP309

XL算法的冗余分析与改进

张 帆，李 蕾，熊 炎

(信阳师范学院计算机与信息技术学院，河南 信阳 464000)

摘 要：针对多变量二次方程组的求解问题，对XL算法的冗余性进行分析与改进。用XL算法扩展方程组存在冗余现象，采用该算法扩展由m个方程构成的n元二次方程组，所得到的新方程组中线性独立方程个数的上界为$[mn(n+3)-m(m-3)]/2$。基于此，对XL算法进行改进。分析表明，改进后的XL算法能降低求解多变量二次方程组的计算复杂性。

关键词：重复线性化；XL算法；代数攻击；高斯消元；计算复杂性

Redundancy Analysis and Improvement of XL Algorithm

ZHANG Fan, LI Lei, XIONG Yan

(College of Computer and Information Technology, Xinyang Normal University, Xinyang 464000, China)

【Abstract】 Aiming at problems of solving multiple quadratic equation systems, the redundancy of extending equations by Extended Linearization (XL) algorithm is analyzed. It is proved that there is redundancy in equations extended by XL algorithm. The upper bound, $[mn(n+3)-m(m-3)]/2$, of the number of linearly independent equations in the new system of equations, which extends from n-variable quadratic equations consisting of m equations, is given. The algorithm is obtained to overcome the redundancy problem and XL algorithm is improved, which effectively reduces the computational complexity of solving multi-variable quadratic equation system.

【Key words】 relinearization; Extended Linearization(XL) algorithm; algebraic attack; Gaussian elimination; computational complexity

DOI: 10.3969/j.issn.1000-3428.2011.16.020

1 概述

求解多变量二次方程系统问题(以下称之为 MQ-问题)是NP难的。对于较小的域，已知的最好方法是穷举法，而对于较大的域，也可采用Gröbner基算法[1]。但Gröbner基算法具有指数阶的计算复杂性，在实际中只能求解未知量个数较少的系统。文献[2]提出了一种新的求解MQ-问题的方法——重复线性化法。但是该算法计算复杂性难以估计，不过对于充分超定的MQ-问题，用重复线性化法可在多项式时间内求解。后来，文献[3]通过大量的实验证明，用重复线性化法得到的新方程中，有很多方程都不是线性独立的，因而重复线性化法并不像当初所期待的那样有效。于是文献[3]对重复线性化法进行了改进，提出了一种比重复线性化法更简单、更有效的新方法——XL(Extended Linearization)算法[3]。对于随机产生的由m个($m=\varepsilon n^2$，$0<\varepsilon\leqslant 1/2$)方程构成的$n$元二次方程组，用XL算法求解的计算复杂度约为$O(n^{\omega/\sqrt{\varepsilon}})$。其中，$\omega$是高斯消元法求解线性方程组的计算复杂性指数。通常$\omega=3$，在改进算法[4]中，$\omega=2.376$。文献[5]利用各单项式之间的约束关系对方程组进行约简，从而对XL算法进行了改进。文献[6]通过对方程组进行约简消去次数较高的单项式，从而达到降低计算复杂性的目的。

本文在用XL算法进行分析时，发现用XL算法产生的方程组中有许多方程不独立(线性)。可将这些不独立的方程区分出来，这样在用XL算法扩展方程时，如果将这些不独立的方程直接丢弃或者不产生这些方程，可使得到的方程组中线性独立的方程比例大大提高，从而减少了对不独立方程的处理。

2 XL算法简介

设K为一数域，$l_i=f_i(x_1,x_2,\mathrm{L},x_n)-b_i\in K[x_1,x_2,\mathrm{L},x_n](1\leqslant i\leqslant m)$均为二次多项式。$\Sigma$表示下列方程组：$l_i\equiv f_i(x_1,x_2,\mathrm{L},x_n)-b_i=0$，$(1\leqslant i\leqslant m)$。在以下的讨论中，总假设$\Sigma$中的方程相互独立。MQ-问题是：对于给定的$b=(x_1,x_2,\mathrm{L},b_m)\in K^m$，至少找到系统$\Sigma$的一个解$x=(x_1,x_2,\mathrm{L},x_n)\in K^n$。

XL算法[3]过程如下：

(1)乘积(multiply)：选择适当的D，对于所有的$k:0\leqslant k\leqslant D-2$，产生所有形如$\prod_{j=1}^{k}x_{i_j}\cdot l_i=0\ (0\leqslant k\leqslant D-2)$的方程。

(2)线性化(linearize)：将每个次数$\leqslant D$的单项式看作一个新变量，然后对(1)中产生的方程组进行高斯消元。

(3)求解(solve)：假设经过(2)后可以得到一个关于x_n的高次方程，利用Berlekamp算法在有限域K上求解该方程，得到x_n。

(4)循环(repeat)：将x_n代入原方程，简化后重复这一过程，从而求得其他变量的值。

3 XL算法产生方程的独立性分析

定义 设P_1、P_2均为多项式的集合，若P_1中的每个多项式都能被P_2中的多项式线性表示，P_2中的每个多项式也都能被P_1中的多项式线性表示，则称多项式集合P_1与P_2等价。

为了讨论方便，以下对方程$f_i(x_1,x_2,\mathrm{L},x_n)=0$和多项式$f_i(x_1,x_2,\mathrm{L},x_n)$不加区分。

引理 1 设$m\leqslant n$，$P=\left\{y_i+\sum_{j=i+1}^{n}a_{ij}y_j+b_i\middle|1\leqslant i\leqslant m\right\}$是以

基金项目：河南省自然科学基金资助项目(102102210242)

作者简介：张 帆(1982－)，女，讲师、硕士，主研方向：信息安全；李 蕾、熊 炎，讲师、硕士

收稿日期：2011-01-12 **E-mail**：15803760377@139.com

$y_1, y_2, \cdots, y_n$ 为变量的一次多项式的集合。Q 是用每个变量 $y_1, y_2, \cdots, y_n$ 分别乘 P 中所有多项式所得多项式的集合。即：

$$Q=\left\{y_i y_{i'}+\sum_{j=i+1}^{n} a_{ij} y_j y_{i'}+b_i y_{i'} \middle| 1 \leqslant i \quad m, 1 \quad i' \quad n\right\}$$

则 $P \cup Q$ 中有且仅有 $mn-m(m-3)/2$ 个多项式是线性独立的。

证明：记：

$$Q_1=\left\{y_i y_{i'}+\sum_{j=i+1}^{n} a_{ij} y_j y_{i'}+b_i y_{i'} \middle| 1 \leqslant i \quad m, i \quad i' \quad n\right\}$$

$$Q_2=\left\{y_i y_{i'}+\sum_{j=i+1}^{n} a_{ij} y_j y_{i'}+b_i y_{i'} \middle| 1 \leqslant i' < i \quad m\right\}$$

则 $Q=Q_1 \cup Q_2$，且 $|Q| = |Q_1| + |Q_2|$。因为：

$$|Q| = mn$$

$$|Q_2| = \#\{(i,i') \mid 1 \leqslant i' < i \quad m\} = C_m^2 = m(m-1)/2$$

所以：

$$|Q_1| = mn - m(m-1)/2$$

若 $P \cup Q_1$ 中多项式都线性独立，且 Q_2 中的多项式都能被 $P \cup Q_1$ 线性表示，则：

$$|P \cup Q_1| = |P| + |Q_1| = |P| + |Q| - |Q_1| =$$
$$m + mn - m(m-1)/2 = mn - m(m-3)/2$$

即可得引理成立。以下证明 $P \cup Q_1$ 中多项式都线性独立，且 Q_2 中的多项式都能被 $P \cup Q_1$ 线性表示：

(1)证明 $P \cup Q_1$ 中多项式都线性独立。记 $P \cup Q$ 的多项式中出现的所有单项式的集合为 H，即：

$$H=\{y_i, y_i y_j \mid 1 \leqslant i \quad j \quad n\}$$

将 H 中所有单项式看作新变量，然后进行如下排序：

$$y_i y_j = w_{(i-1)n-i(i-1)/2+j}, \quad 1 \leqslant i \quad j \quad n$$

$$y_i = w_{n(n+1)/2+i}$$

则：

$$Q_1=\{w_{(i-1)n-i(i-1)/2+i'}+\sum_{j=i+1}^{n} a_{ij} w_{(p_j-1)n-p_j(p_j-1)/2+q_j}+b_i w_{n(n+1)/2+i'} \mid$$
$$1 \leqslant i \quad m, i \quad i' \quad n\}$$

$$P=\{w_{n(n+1)/2+i}+\sum_{j=i+1}^{n} a_{ij} w_{n(n+1)/2+j}+b_i \mid 1 \leqslant i \quad m\}$$

其中，$p_j = \min\{i', j\}$；$q_j = \max\{i', j\}$。容易看出 $P \cup Q_1$ 中多项式具有如下特点：

1)每个多项式的第1项的下标最小；

2)所有单项式第1项的下标互不相同。

这说明当将 $P \cup Q_1$ 中的所有单项式写成系数矩阵与变量构成的列项链乘积时，其系数矩阵每行的第1个非零元不同列，从而该矩阵是满秩的，所以 $P \cup Q_1$ 中多项式是线性独立的。

(2)用数学归纳法易证 Q_2 中的多项式都能被 $P \cup Q_1$ 中的多项式线性表示。

由(1)和(2)知，引理成立。

引理 2 设 $\boldsymbol{A}$ 为矩阵，将 $\boldsymbol{A}$ 的第 i 列元素分别加到第 j 列的对应元素上，然后将第 i 列元素删除得到矩阵 $\boldsymbol{B}$，则 秩($\boldsymbol{A}$) ≥ 秩($\boldsymbol{B}$)。

证明：因为将 $\boldsymbol{A}$ 的第 i 列元素分别加到第 j 列的对应元素上所得矩阵秩不变，所以删除矩阵的一行或一列，所得矩阵的秩小于或等于原来矩阵的秩，即 秩($\boldsymbol{A}$) ≥ 秩($\boldsymbol{B}$)。

记 $L=\{l_h \mid 1 \leqslant h \quad m\}$，$x^k L=\{\prod_{j=1}^{k} x_{i_j} \cdot l_h \mid 1 \leqslant i_j \quad n, 1 \quad h \quad m\}$，$I_d=\bigcup_{k=0}^{d-2}\{\prod_{j=1}^{k} x_{i_j} \cdot l_h \mid 1 \leqslant i_j \quad n, 1 \quad h \quad m\}$，下面分析 XL 算法中冗余方程的个数。

定理 设 A_0 是由 n 个变量 m 个方程构成的多变量二次方程系统，使用 XL 算法得到的 $I_4 = L \cup xL \cup x^2 L$ 中最多有 $[mn(n+3)-m(m-3)]/2$ 个多项式线性独立。

证明：将 A_0 中方程的每个单项式都看作一个新变量 y_i(适当排序)，则这样的新变量共有：

$$\#\{x_i, x_i x_j \mid 1 \leqslant i, j \quad n\} = C_n^2 + 2n = \frac{n(n+3)}{2}$$

个，然后采用高斯消元法将 A_0 变为：

$$P_0=\{y_i+\sum_{j=i+1}^{n(n+3)/2} a_{ij} y_j + b_i \mid 1 \leqslant i \quad m\}$$

则 A_0 与 P_0 等价。记：

$$Q=\{y_i y_{i'}+\sum_{j=i+1}^{n(n+3)/2} a_{ij} y_j y_{i'}+b_i y_{i'} \mid 1 \leqslant i \quad m, 1 \quad i' \quad \frac{n(n+3)}{2}\}$$

则 $P_0 \cup Q$ 与 I_4 等价。由引理 1 知：当把每个 $y_i (1 \leqslant i \quad n(n+3)/2)$ 都看作独立变量时，$P_0 \cup Q$ 中有且仅有：

$$m\frac{n(n+3)}{2}-\frac{m(m-3)}{2}=\frac{mn(n+3)-m(m-3)}{2}$$

个多项式线性独立。但由于 y_i 相互不独立(比如 $(x_a x_b)x_c = x_a(x_b x_c)$)，因此 $P_0 \cup Q$ 中多项式的有些项是同类项，可以合并。当把 $P_0 \cup Q$ 中所有多项式写成系数矩阵与单项式构成的列向量乘积时，合并同类项的过程等价于：将其系数矩阵某一列元素分别加到另一列对应元素上，然后将前者删除，同时删除该列对应的单项式。由引理 2 知，$P_0 \cup Q$ 中多项式都看作是 x_i 的多项式时，其线性独立的多项式个数小于或等于 $[mn(n+3)-m(m-3)]/2$。由于 $P_0 \cup Q$ 与 I_4 等价，因此 I_4 中最多有 $[mn(n+3)-m(m-3)]/2$ 个多项式线性独立。

推论 当 $D=4$ 时，使用 XL 算法对 n 个变量 m 个方程构成的多变量二次方程系统 Σ 进行扩展得到的方程组中，最多有 $[mn(n+3)-m(m-3)]/2$ 个方程独立。

4 XL 算法的改进

由定理知，用 XL 算法扩展得到的方程中有很多方程不独立，若将这些不独立的方程去除，则可大大降低方程求解的计算复杂性和存储复杂性。为此，对 XL 算法进行了改进，改进后的 XL 算法过程如下：

(1)初始化：将由 $x_1, x_2, \cdots, x_n$ 构成的二次和一次单项式按式(2)方法进行排序，然后用高斯消元法将多项式集合 L 化为首多项式互异且序号连续的多项式集合 L'(当 L' 中首多项式不连续时，可对变量 $x_1, x_2, \cdots, x_n$ 重新排序使其连续)。

(2)乘积：选择适当的 D，产生所有的次数不超过 $D-2$ 的单项式 $T_{D-2}=\bigcup_{k=1}^{D-2}\{\prod_{j=1}^{k} x_{i_j} \mid 1 \leqslant i_j \quad n\}$，对 L' 中每个多项式 l_h，用 T_{D-2} 中所有不能被 l_h 首单项式整除的单项式分别乘多项式 l_h，产生多项式的集合 Q。

(3)线性化：将 Q 中多项式的每个单项式看作一个新变量，用高斯消元法进行消元，但把只含有一个变量 x_n 的项 $x_n^k (1 \leqslant k \quad D)$ 留在最后。

(4)求解：在 K 上求解上一步得到的只含一个变量 x_n 的方程(次数小于或等于 D)。

(5)循环：将 x_n 的值代入步骤(2)中，逐个求出其他变量的值。

改进前的 XL 算法产生的方程总数为：

$$m|T_{D-2}| \approx m|T_2 \setminus T_1| \cdot |T_{D-4}| \approx mC_n^2 |T_{D-4}|$$

(下转第64页)