有限体上の多変数連立代数方程式系に対する総当り探索の打破

～アルゴリズムの基礎研究と暗号解析への応用～

情報科学研究科/社会情報科学部

○准教授　玉置（たまき） 卓（すぐる）

キーワード　**指数時間アルゴリズム，多項式，低次数，算術回路**

研究概要

有限体上の多変数連立代数方程式系を解くことは，数学，科学，および工学における基本的は問題である．　有限体の位数を q，変数の個数を n とする．　このとき，q^n 通りの解候補を総当たり探索することにより問題を解くことができる．

本研究では，最悪時に　q^n　より速い計算時間でこの問題を解く初めてのアルゴリズムを示す．　我々のアルゴリズムは解の個数を数えることもできる．　このアルゴリズムの計算時間は，方程式の最大次数が d の場合，およそ　q^{n(1-1/0(d))}　である．

本研究では，　方程式が多項式ではなくある種の算術回路で定義されるような一般化された問題も扱い，それに対するアルゴリズムも与える．

有限体F_q上のn変数連立d次方程式系

入力　d次多項式 $P_1, P_2, \dots, P_m \in \mathrm{F}_q[x_1, x_2, \dots, x_n]$

出力　$a \in \mathrm{F}_q^n$　s.t.　$P_1(a) = P_2(a) = \cdots = P_m(a) = 0$

例 $[q = 3, n = 4, d = 5, m = 2]$

$$P_1 = 2x_1^2\, x_2^2\, x_3 + x_3^2\, x_4,\ P_2 = x_1 x_2 + x_2^2 + 1$$

$$a = (2,2,1,1)$$

アピールポイント

多変数連立代数方程式系を解くための商用/無料ソフトウェアが多数開発されている．それらの多くはグレブナ基底に基づいている．　計算時間は実用的な入力に対しては高速とされるが，　最悪時に総当り探索より遅くないことは保証されていない．　本研究の提案アルゴリズムは最悪時の計算時間保証を初めて与えたことが特徴である．　本研究のアルゴリズムおよび後続研究によって改良されたアルゴリズムは，　耐量子暗号　（量子計算機による攻撃に耐えられる暗号）の解析に用いられ始めている．