Beating Brute Force for Systems of Polynomial Equations over Finite Fields

Daniel Lokshtanov, Ramamohan Paturi, Suguru Tamaki, Ryan Williams, Huacheng Yu

(U. California, Santa Barbara) (U. California, San Diego) (U. Hyogo) (MIT) (Princeton U.)

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 $[q = 3, n = 4, d = 5, m = 2]$

$P_1 = 2x_1^2\, x_2^2\, x_3 + x_3^2\, x_4,\ P_2 = x_1x_2 + x_2^2 + 1$

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

背景

$d = 1$ のとき多項式時間で解ける (Gaußの消去法)

$d \geq 2$ のときNP困難, $\exists \varepsilon > 0, q^{(1-\varepsilon)n}$ 時間で解けるか未解決

他の問題の計算困難性を証明するための出発点

- 暗号の安全性 (Multivariate Cryptography ∈ 耐量子暗号)
- 計算時間の最適性 (Fine-Grained Complexity)

本研究の結果 [乱択アルゴリズム]

条件	計算時間
$q = d = 2$	$2^{0.8765n}$
$q = 2, d > 2$	$2^{\left(1-\frac{1}{5d}\right)n}$
$q = p^k, \log p < 4edk$	$q^{\left(1-\frac{1}{200d}\right)n}$
$q = p^k, \log p \geq 4edk$	$q^n \left(\frac{\log q}{edk}\right)^{-kn}$

($e = 2.718\dots$ はネイピア数)

本研究の結果 [決定性計数アルゴリズム]

任意の $q = p^k, d$ について $q^{\left(1-\frac{1}{300dq^{\frac{6}{7k}}}\right)n}$ 時間で
解の個数を数えられる

本研究の結果 [多項式の一般化 ($q = 2$)]

入力 ΣΠΣ算術回路 $P_1, P_2, \dots, P_m$
(P_i は変数と定数の和の積の和, 次数制限なし)

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

例 $P_1 = (x_1 + x_2 + 1)(x_2 + x_3) + (x_1 + x_4)x_2 + 1$
$P_2 = x_1x_2 \cdots x_n + x_2 + x_4$

全体の項の数が s のとき

アルゴリズム	計算時間
乱択	$2^{\left(1-\frac{1}{10\log\left(\frac{s}{n}\right)}\right)n}$
決定性計数	$2^{\left(1-\frac{1}{1100\log\left(\frac{s}{n}\right)}\right)n}$

F_2上のn変数連立d次方程式系はd-SATの一般化

例

$C_1 = (\neg x_1 \vee x_2 \vee x_3) \Rightarrow P_1 = x_1(1 + x_2)(1 + x_3)$
$C_2 = (x_1 \vee \neg x_3 \vee \neg x_4) \Rightarrow P_2 = (1 + x_1)x_2x_2$
$C_3 = (x_2 \vee x_3 \vee x_4) \Rightarrow P_3 = (1 + x_1)(1 + x_2)(1 + x_3)$

$C_1 \wedge C_2 \wedge C_3 = 1 \Leftrightarrow P_1 = P_2 = P_3 = 0$

cf. d-SATの計算時間

条件	計算時間
節の幅 d	$2^{\left(1-\frac{1}{d}\right)n}$
節の数 s	$2^{\left(1-\frac{1}{\log\left(\frac{s}{n}\right)}\right)n}$

乱択アルゴリズムの概要 [$q = 2$]

Step 1 $P \coloneqq (P_1 + 1)(P_2 + 1)\cdots(P_m + 1)$ so that $\exists x \in \{0,1\}^n, P(x) = 1 \Leftrightarrow \exists x \in \{0,1\}^n, P_1(x) = P_2(x) = P_3(x) = 0$

Step 2 $Q(y) \coloneqq \prod_{y' \in \{0,1\}^{n'}} (P(y, y') + 1)$ so that $\exists y \in \{0,1\}^{n-n'}, Q(y) = 0 \Leftrightarrow \exists x \in \{0,1\}^n, P(x) = 1$

Step 3

やりたいこと $Q(y)$ を展開して1つの多項式 $\sum_{S \subseteq [n-n']} a_S \prod_{i \in S} y_i$ と表現 (自明な方法だと2^n時間を超える)

実際にすること $Q(y)$ を近似する多項式 $Q'(y)$ を確率的に構成: $\forall y \in \{0,1\}^{n-n'}, \Pr_{Q'}[Q'(y) \neq Q(y)] \leq 1/3$

Step 4 $Q'(y)$ の真理値表を作成 ($\mathrm{poly}(n)2^{n-n'}$時間でできる)

Step 3〜4 を繰り返して多数決を取れば, 高い確率で $Q(y)$ の真理値表が得られる

Step 2 のn'の値, **Step 3** の計算時間は d に依存

まとめと課題

- 指数領域アルゴリズムのため実用的ではない ⇒ 多項式領域で $\exists \varepsilon > 0, q^{(1-\varepsilon)n}$ 時間で解けるか
- 自明な計算時間の上界しかない問題を, 有限体上の連立方程式系に効率よく帰着できるか