ON THE NUMBER OF SOLUTIONS OF A DIOPHANTINE EQUATION OVER A FINITE FIELD

Norichika Matsuki
3-9-34, Fujisaki, Narashino-shi, Chiba, Japan
n-matsuki@lime.plala.or.jp

Received: 4/1/15, Revised: 6/4/16, Accepted: 11/20/16, Published: 11/23/16

Abstract

We show that the number of distinct solutions of a Diophantine equation over a finite field is represented by the order and rank of a certain matrix derived from the coefficients.

1. Introduction

Let p be a prime, r be a positive integer, and $\mathbb{F}_q$ be a finite field with $q = p^r$ elements. For $f(x) = a_0x^{p-2} + a_1x^{p-3} + \cdots + a_{p-2} \in \mathbb{F}_p[x]$, define

$$A = \begin{pmatrix} a_0 & a_1 & \dots & a_{p-2} \\ a_1 & a_2 & \dots & a_0 \\ \dots & \dots & \dots & \dots \\ a_{p-2} & a_0 & \dots & a_{p-3} \end{pmatrix}.$$

Kronecker (cf. [3, Chapter VIII, page 226]) showed that the number of nonzero solutions to $f(x) = 0$ equals $p - 1 - \text{rank } A$. In this paper we extend Kronecker's result to Diophantine equations in several variables over $\mathbb{F}_q$.

First we give some notation and definitions. We denote by I_n the ideal $({x_1}^q - x_1, \dots, {x_n}^q - x_n)$ of $\mathbb{F}_q[x_1, \dots, x_n]$. For $f \in \mathbb{F}_q[x_1, \dots, x_n]$, we define $\overline{f}$ as the right-hand side of the congruence

$$f \equiv \sum_{0 \le r_1, \dots, r_n \le q-1} a_{r_1 \cdots r_n} {x_1}^{r_1} \cdots {x_n}^{r_n} \pmod{I_n}.$$

Then it holds that $f(b_1, \dots, b_n) = \overline{f}(b_1, \dots, b_n)$ for any $b_1, \dots, b_n \in \mathbb{F}_q$. Here we denote by $m_i = m_i(x_1, \dots, x_n)$ the i-th monomial in the following chain of monomials, ordered in the graded lexicographic order

$$1 \prec x_1 \prec \cdots \prec x_n \prec x_1x_2 \prec x_1x_3 \prec \cdots \prec x_{n-1}x_n \prec \cdots \prec {x_1}^{q-1} \cdots {x_n}^{q-1}$$

and $c_i(\overline{f})$ by the coefficient of the monomial m_i in $\overline{f}$. Note that $c_i(\overline{f}) = 0$ if $\overline{f}$ does not contain the monomial m_i. Then we define $K(\overline{f}) = \big(K(\overline{f})_{ij}\big)$ as the $q^n \times q^n$ matrix whose (i,j) entry is $c_j(\overline{m_i f})$, namely,

$$K(\overline{f})_{ij} = c_j(\overline{m_i f}) = \sum_{\substack{t \in \{1,\ldots,q^n\} \\ \text{s.t. } m_i m_t \equiv m_j \pmod{I_n}}} c_t(\overline{f}).$$

2. The Result

We shall introduce the basis to diagonalize $K(\overline{f})$ and show the spectrum of $K(\overline{f})$ coincides with the value set of f in the similar way as [4]. For our purpose, we need the following three lemmas. Although the first lemma is well-known, we give a proof for the sake of completeness.

Lemma 1. *The following statements are equivalent:*

(i) $f(b_1, \ldots, b_n) = 0$ *for all* $(b_1, \ldots, b_n) \in {\mathbb{F}_q}^n$.

(ii) $\overline{f} = 0$.

Proof. (ii) $\Rightarrow$ (i) is obvious. For (i) $\Rightarrow$ (ii), the proof given here is an adaptation of the proof of Lemma 2.1 in [1]. We use induction on n. It is obvious for $n = 1$.

Suppose that it is true for $n = k$ and that $f(b_1, \ldots, b_{k+1}) = 0$ for all $(b_1, \ldots, b_{k+1}) \in {\mathbb{F}_q}^{k+1}$. Write

$$\overline{f}(x_{k+1}) = \overline{a_{q-1}}{x_{k+1}}^{q-1} + \cdots + \overline{a_1}x_{k+1} + \overline{a_0},$$

where $a_0, \ldots, a_{q-1} \in \mathbb{F}_q[x_1, \ldots, x_k]$. For each fixed $(b_1, \ldots, b_k) \in {\mathbb{F}_q}^k$, it holds that $\overline{f}(b_{k+1}) = 0$ for all $b_{k+1} \in \mathbb{F}_q$. Hence $\overline{a_0}(b_1, \ldots, b_k) = \cdots = \overline{a_{q-1}}(b_1, \ldots, b_k) = 0$ for all $(b_1, \ldots, b_k) \in {\mathbb{F}_q}^k$. By the assumption, we have $\overline{a_0} = \cdots = \overline{a_{q-1}} = 0$. Thus it is also true for $n = k + 1$. $\square$

Lemma 2. *Let β be a generator of ${\mathbb{F}_q}^* = \mathbb{F}_q \setminus \{0\}$ and let*

$$\begin{aligned} w_i &= (d_{i1}, \ldots, d_{iq^n}) \\ &= \begin{cases} (1, \ldots, 1) & \text{if } i = 1, \\ (\underbrace{0, \ldots, 0}_{q^{i-2}}, \underbrace{\beta, \ldots, \beta}_{q^{i-2}}, \ldots, \underbrace{\beta^{q-1}, \ldots, \beta^{q-1}}_{q^{i-2}}, \underbrace{0, \ldots, 0}_{q^{i-2}}, \underbrace{\beta, \ldots, \beta}_{q^{i-2}}, \ldots) & \\ & \text{if } 2 \le i \le n, \\ (\underbrace{0, \ldots, 0}_{q^{n-1}}, \underbrace{\beta, \ldots, \beta}_{q^{n-1}}, \ldots, \underbrace{\beta^{q-1}, \ldots, \beta^{q-1}}_{q^{n-1}}) & \text{if } i = n+1, \\ (m_i(d_{2\,1}, \ldots, d_{n+1\,1}), \ldots, m_i(d_{2\,q^n}, \ldots, d_{n+1\,q^n})) & \text{if } n+2 \le i \le q^n. \end{cases} \end{aligned}$$

Denote by v_j the j-th column vector of the matrix whose rows are $w_1, \ldots, w_{q^n}$. Then $v_1, \ldots, v_{q^n}$ are linearly independent over $\mathbb{F}_q$.

Proof. Suppose that in ${\mathbb{F}_q}^n$, we have $a_1 w_1 + \cdots + a_{q^n} w_{q^n} = 0$, where $a_1, \ldots, a_{q^n} \in \mathbb{F}_q$. In other words,

$$a_1 + a_2 d_{2j} + \cdots + a_{q^n} d_{q^n j} = 0, \quad \text{for all } 1 \leq j \leq q^n.$$

By definition,

$$d_{ij} = m_i(d_{2\,j}, \ldots, d_{n+1\,j}), \quad \text{for all } 1 \leq i, j \leq q^n,$$

so that the polynomial function defined by

$$g(x_1, \ldots, x_n) = \sum_{i=1}^{q^n} a_i m_i(x_1, \ldots, x_n)$$

satisfies

$$g(d_{2\,j}, \ldots, d_{n+1\,j}) = 0, \quad \text{for all } 1 \leq j \leq q^n.$$

Since, by construction, we have $\{(d_{2\,j}, \ldots, d_{n+1\,j}) : 1 \leq j \leq q^n\} = {\mathbb{F}_q}^n$, it follows from Lemma 1 that $a_1 = \cdots = a_{q^n} = 0$. Hence $w_1, \ldots, w_{q^n}$ are linearly independent over $\mathbb{F}_q$ and so are $v_1, \ldots, v_{q^n}$. $\square$

Lemma 3. $K(\overline{f})v_j = f(d_{2\,j}, \ldots, d_{n+1\,j})v_j$.

Proof. Since

$$\begin{aligned} f(d_{2\,j}, \ldots, d_{n+1\,j})d_{ij} &= f(d_{2\,j}, \ldots, d_{n+1\,j}) m_i(d_{2\,j}, \ldots, d_{n+1\,j}) \\ &= \overline{m_i f}(d_{2\,j}, \ldots, d_{n+1\,j}) = \sum_{k=1}^{q^n} c_k(\overline{m_i f}) d_{kj}, \end{aligned}$$

we have

$$\begin{aligned} (K(\overline{f})_{i1}, \ldots, K(\overline{f})_{iq^n})v_j &= (c_1(\overline{m_i f}), \ldots, c_{q^n}(\overline{m_i f}))v_j \\ &= \sum_{k=1}^{q^n} c_k(\overline{m_i f}) d_{kj} = f(d_{2\,j}, \ldots, d_{n+1\,j}) d_{ij}. \end{aligned}$$

Hence the lemma follows. $\square$

The formula for the number of solutions is derived immediately from these lemmas.

Theorem 4. *Let $n(f)$ be the number of distinct solutions of $f \in \mathbb{F}_q[x_1, \ldots, x_n]$. Then $n(f) = q^n - \operatorname{rank} K(\overline{f})$.*

Proof. Let $F : {\mathbb{F}_q}^{q^n} \to {\mathbb{F}_q}^{q^n}$ be the linear map defined by $K(\overline{f})$. From Lemmas 2 and 3, we see that $\dim(\ker F) = n(f)$. By the rank-nullity theorem (e.g., [2, Chapter II, page 298]), it follows that $q^n = \operatorname{rank} K(\overline{f}) + n(f)$. $\square$

Acknowledgement. The author is grateful to an anonymous referee whose suggestions improved the paper significantly.

References

[1] N. Alon, Combinatorial Nullstellensatz, *Combin. Probab. Comput.* **8** (1999), 7–29.

[2] N. Bourbaki, *Algebra I*, Springer-Verlag, Berlin, 1989.

[3] L. E. Dickson, *History of the Theory of Numbers*, Dover Publications, New York, 2005.

[4] N. Matsuki, Counting problems and ranks of matrices, *Linear Algebra Appl.* **465** (2015), 104–106.