Available online at www.sciencedirect.com

ScienceDirect

Discrete Mathematics 306 (2006) 2257 – 2262

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Note

Graph colourings and solutions of systems of equations over finite fields[☆]

Jianguo Qian*, Hong Lin

School of Mathematical Sciences, Xiamen University, Xiamen, Fujian 361005, P.R. China

Received 2 January 2004; received in revised form 9 November 2005; accepted 22 March 2006
Available online 17 July 2006

Abstract

A congruence $f(x_1, x_2, \dots, x_t) \equiv 0 \bmod p^n$ (p is a prime) is said to be strong homogeneous if it has the form

$$x_i^{d-1} + x_i^{d-2}x_j + x_i^{d-3}x_j^2 + \cdots + x_j^{d-1} \equiv 0 \bmod p^n,$$

where $p \nmid d, d > n$ and $i, j \in \{1, 2, \dots, t\}, i \neq j$. A strong homogeneous equation over a finite field $\mathbb{F}_{p^n}$, $p^n > 2$, is defined analogously. For a system S of strong homogeneous congruences (or equations), the associated graph $G(S)$ of S is defined to be the graph whose vertex set is $\{x_1, x_2, \dots, x_t\}$ and two vertices x_i and x_j are adjacent whenever they belong to a congruence (or equation) in S. We show that the solutions of S have a close relation with the vertex colourings of $G(S)$. The number of solutions of S can be represented by the chromatic polynomials of the components of $G(S)$. This implies that the problem of finding the solutions to a system of equations over a finite field or congruences is NP-hard, even for a very special class. An asymptotic estimation to the number of the solutions of the system of SH-congruence is also established.

MSC: 11D79; 05C15

Keywords: Graph colouring; Congruence; Equation; Finite field

1. Introduction

In algebraic number theory, estimating the number of solutions of equations over a finite field is a charming and important problem with a long history. As mentioned in [13], Gauss first studied the solutions of the equation $ay^l + bz^m + c = 0$ over a finite field, and calculated the number of solutions for $(l, m) = (2, 2), (3, 3), (4, 4), (2, 4)$. Weil [14] made a further study on solutions of the equation $a_0x_0^{n_0} + a_1x_1^{n_1} + \cdots + a_rx_r^{n_r} = 0$, and posed a famous conjecture which has been very influential in the recent development of both number theory and algebraic geometry. Deligine finally solved Weil's conjecture and was awarded the Fields Medal in 1978 [9]. For general equation(s), Warning and Katz made some estimations on the number of solutions of a system of equations over a finite field [9]. For some more recent results on this topic, we refer to [1,4,7,8,10–12,15].

[☆] This work is supported in part by NSFC(10371102) and the Program of 985 Innovation Engineering on Information in Xiamen University (2004–2007).

* Corresponding author. +1 86 59 22580669; fax: +1 86 59 22183209.
E-mail address: jgqian@xmu.edu.cn (J. Qian).

0012-365X/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2006.03.071

In elementary number theory, Gauss introduced the notion of congruence in Disquisitions Arithmetica [6]. Results related to the solutions of some special congruences can be found in [4–6,8,11].

For non-negative integers a, b and $q \neq 0$, we say that a is congruent to b modulo q if q divides $b-a$ and as usual, this relation is written by $a \equiv b \bmod q$. Let n be a positive integer, p be a prime with $p^n > 2$ and let d, $d > n$, be a positive integer not divisible by p. A congruence $f(x_i, x_j) \equiv 0 \bmod p^n$ is said to be a strong homogeneous (p, n, d)-congruence (or more briefly, an SH-congruence) if it has the form

$$x_i^{d-1} + x_i^{d-2}x_j + x_i^{d-3}x_j^2 + \cdots + x_j^{d-1} \equiv 0 \bmod p^n. \tag{1}$$

Let S be a system of SH-congruences in the variables $x_1, x_2, \ldots, x_t$, $t \geq 2$ (here, for convenience, we assume that each of $x_1, x_2, \ldots, x_t$ appears in at least one congruence of S). The associated graph $G(S)$ of S is defined to be a simple undirected graph whose vertex set is $\{x_1, x_2, \ldots, x_t\}$ and two vertices x_i and x_j are adjacent whenever S contains the congruence (1).

For an example, let S be

$$\begin{cases} x_1^{d-1} + x_1^{d-2}x_2 + \cdots + x_2^{d-1} \equiv 0 \\ x_2^{d-1} + x_2^{d-2}x_3 + \cdots + x_3^{d-1} \equiv 0 \\ x_3^{d-1} + x_3^{d-2}x_4 + \cdots + x_4^{d-1} \equiv 0 \\ x_4^{d-1} + x_4^{d-2}x_1 + \cdots + x_1^{d-1} \equiv 0 \end{cases}$$

mod p^n. Then S is a system of SH-congruences in the variables x_1, x_2, x_3, x_4 and $G(S)$ is a cycle of length 4.

From the definition of $G(S)$, it can be seen that each vertex of $G(S)$ has degree at least 1. In other words, each component of $G(S)$ contains at least two vertices, or equivalently, $G(S)$ contains no isolated vertices. Again from the definition of $G(S)$, it can be seen that for fixed p, n, and d, the function $S \to G(S)$ is a bijection between systems of SH-congruences and simple undirected graphs without isolated vertices.

Let p, n, d be defined as above. Similar to the definition of strong homogeneous congruence, an equation $f(x_i, x_j)=0$ over a finite field $\mathbb{F}_{p^n}$ is said to be a strong homogeneous (p, n, d)-equation (briefly, an SH-equation) if it has the form

$$x_i^{d-1} + x_i^{d-2}x_j + x_i^{d-3}x_j^2 + \cdots + x_j^{d-1} = 0. \tag{2}$$

The associated graph $G(S)$ of a system S of strong homogeneous equations is defined analogously. A system of strong homogeneous congruences or equations over a finite field are generally called an SH-system, with no confusion.

For a graph G of t vertices $x_1, x_2, \ldots, x_t$, a vector $(\xi_1, \xi_2, \ldots, \xi_t) \bmod p^n$ (or over a finite field $\mathbb{F}_{p^n}$) is said to be a vertex colouring of G if $\xi_i \not\equiv \xi_j \bmod p^n$ (or $\xi_i \neq \xi_j$) for any two adjacent vertices x_i and x_j. $\xi_1, \xi_2, \ldots, \xi_t$ are also called the colours. For a natural number λ, we denote by $\pi_\lambda(G)$ the number of vertex colourings of G using at most λ different colours. It is well known that $\pi_\lambda(G)$ is a polynomial in λ (see [2,3] for details):

$$\pi_\lambda(G) = \sum_{i=0}^{t-k} (-1)^i a_i \lambda^{t-i},$$

where $a_0 = 1$, a_1 and k are the numbers of edges and components in G, respectively, and a_i is a positive integer for every i, $1 \leqslant i \leqslant t-k$. $\pi_\lambda(G)$ is also called the chromatic polynomial of G.

In this paper, we show that the solutions of an SH-system S has a close relation with the vertex colourings of $G(S)$. More precisely, the solutions of S and the vertex colourings of $G(S)$ are determined uniquely from each other. It follows that, for a system S of SH-congruences modulo p^n, the number of solutions of S is

$$n(S) = \prod_{j=1}^{k} \left(p^{(n-1)t_j} + \frac{p^{n-1}(p-1)}{l} \pi_l(G_j)\right),$$

where $l = \gcd(d, p-1)$, $G_1, G_2, \ldots, G_k$, are the components of $G(S)$ and t_j, $j \in \{1, 2, \ldots, k\}$, is the number of vertices in G_j. This implies that $n(S)/p^{(n-1)t} \to 1$ as $n \to +\infty$.