ARTICLE IN PRESS YJNTH:5929

Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the DLW conjectures

Xiang-Dong Hou

Department of Mathematics and Statistics, University of South Florida, Tampa, FL 33620, United States

ARTICLE INFO

Article history:
Received 6 February 2017
Accepted 6 November 2017
Available online xxxx
Communicated by D. Wan

MSC:
05C35
11T06
11B65

Keywords:
Finite field
Monomial graph
Permutation polynomial

ABSTRACT

In 2007, Dmytrenko, Lazebnik and Williford posed two related conjectures about polynomials over finite fields. Conjecture 1 is a claim about the uniqueness of certain monomial graphs. Conjecture 2, which implies Conjecture 1, deals with certain permutation polynomials of finite fields. Two natural strengthenings of Conjecture 2, referred to as Conjectures A and B in the present paper, were also insinuated. In a recent development, Conjecture 2 and hence Conjecture 1 have been confirmed. The present paper gives a proof of Conjecture A.

1. Introduction

Let $\mathbb{F}_q$ denote the finite fields with q elements. For $f, g \in \mathbb{F}_q[X, Y]$, $G_q(f, g)$ is a bipartite graph with vertex partitions $P = \mathbb{F}_q^3$ and $L = \mathbb{F}_q^3$, and edges defined as follows: a vertex $(p_1, p_2, p_3) \in P$ is adjacent to a vertex $[l_1, l_2, l_3] \in L$ if and only if

$$p_2 + l_2 = f(p_1, l_1) \quad \text{and} \quad p_3 + l_3 = g(p_1, l_1). \tag{1.1}$$

E-mail address: xhou@usf.edu.

https://doi.org/10.1016/j.jnt.2017.11.001

The graph $G_q(f,g)$ is called a *polynomial graph*, and when f and g are both monomials, it is called a *monomial graph*. Polynomial graphs were introduced by Lazebnik and Ustimenko in [7] to provide examples of dense graphs of high girth. In particular, the monomial graph $G_q(XY, XY^2)$ has girth 8, and its number of edges achieves the maximum asymptotic magnitude of the function $g_3(n)$ as $n \to \infty$, where $g_k(n)$ is the maximum number of edges in a graph of order n and girth $\geq 2k+1$. (For surveys on the function $g_k(n)$, see [1,3].)

Let $q = p^e$, where p is an odd prime and $e \geq 1$. It was proved in [2] that every monomial graph of girth ≥ 8 is isomorphic to $G_q(XY, X^kY^{2k})$ for some $1 \leq k \leq q-1$, and the following conjecture was posed in [2]:

Conjecture 1. *([2, Conjecture 4]) Every monomial graph of girth 8 is isomorphic to $G_q(XY, XY^2)$.*

To prove Conjecture 1, it suffices to show that if $1 \leq k \leq q-1$ is such that $G_q(XY, X^kY^{2k})$ has girth ≥ 8, then k is a power of p.

A polynomial $h \in \mathbb{F}_q[X]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if the mapping $x \mapsto h(x)$ is a permutation of $\mathbb{F}_q$. For $1 \leq k \leq q-1$, let

$$A_k = X^k\big[(X+1)^k - X^k\big] \in \mathbb{F}_q[X] \tag{1.2}$$

and

$$B_k = \big[(X+1)^{2k} - 1\big]X^{q-1-k} - 2X^{q-1} \in \mathbb{F}_q[X]. \tag{1.3}$$

It was proved in [2] that if $1 \leq k \leq q-1$ is such that $G_q(XY, X^kY^{2k})$ has girth ≥ 8, then both A_k and B_k are PPs of $\mathbb{F}_q$. Consequently, a second conjecture was proposed:

Conjecture 2. *([2, Conjecture 16]) If $1 \leq k \leq q-1$ is such that both A_k and B_k are PPs of $\mathbb{F}_q$, then k is a power of p.*

Note that if k is a power of p, then A_k and B_k are clearly PPs of $\mathbb{F}_q$. Obviously, Conjecture 2 implies Conjecture 1. Although the polynomials A_k and B_k are both related to the graph $G_q(XY, X^kY^{2k})$, it is not clear how they are related to each other. Therefore, it is natural to consider the polynomials A_k and B_k separately, giving rise to the following two stronger versions of Conjecture 2; see [4–6].

Conjecture A. *Assume that $1 \leq k \leq q-1$. Then A_k is a PP of $\mathbb{F}_q$ if and only if k is a power of p.*

Conjecture B. *Assume that $1 \leq k \leq q-1$. Then B_k is a PP of $\mathbb{F}_q$ if and only if k is a power of p.*

Please cite this article in press as: X.-D. Hou, On the DLW conjectures, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2017.11.001