Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Finite Fields and Their Applications ••• (••••) •••–•••
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

On monomial graphs of girth eight

Vasyl Dmytrenko [a], Felix Lazebnik [b,*], Jason Williford [c]

[a] *Department of Mathematics, Temple University, Philadelphia, PA 19122, USA*
[b] *Department of Mathematical Science, Ewing Hall, University of Delaware, Newark, DE 19716, USA*
[c] *Department of Mathematical Sciences, Worcester Polytechnic Institute, 100, Institute road, Worcester, MA 01609-2280, USA*

Received 28 September 2005; revised 9 March 2006

Communicated by Gary L. Mullen

Abstract

Let e be a positive integer, p be an odd prime, $q = p^e$, and $\mathbb{F}_q$ be the finite field of q elements. Let $f_2, f_3 \in \mathbb{F}_q[x, y]$. The graph $G = G_q(f_2, f_3)$ 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 $(p) = (p_1, p_2, p_3) \in P$ is adjacent to a vertex $[l] = [l_1, l_2, l_3]$ if and only if

$$p_2 + l_2 = f_2(p_1, l_1) \quad \text{and} \quad p_3 + l_3 = f_3(p_1, l_1).$$

Motivated by some questions in finite geometry and extremal graph theory, we ask when G has no cycle of length less than eight, i.e., has girth at least eight. When f_2 and f_3 are monomials, we call G a monomial graph. We show that for $p \geqslant 5$, and $e = 2^a 3^b$, a monomial graph of girth at least eight has to be isomorphic to the graph $G_q(xy, xy^2)$, which is an induced subgraph of the classical generalized quadrangle $W(q)$. For all other e, we show that a monomial graph is isomorphic to a graph $G_q(xy, x^k y^{2k})$, with $1 \leqslant k \leqslant (q-1)/2$ and satisfying several other strong conditions. These conditions imply that $k = 1$ for all $q \leqslant 10^{10}$. In particular, for a given positive integer k, the graph $G_q(xy, x^k y^{2k})$ can be of girth eight only for finitely many odd characteristics p.

Keywords: Monomial graph; Cycle; Girth eight; Generalized quadrangle; Permutation polynomial

* Corresponding author.
E-mail addresses: vdmytr@math.temple.edu (V. Dmytrenko), lazebnik@math.udel.edu (F. Lazebnik), jsw@wpi.edu (J. Williford).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2006.03.001

Please cite this article in press as: V. Dmytrenko et al., On monomial graphs of girth eight, Finite Fields Appl. (2006), doi:10.1016/j.ffa.2006.03.001

1. Introduction

All graphs considered in this paper are finite, undirected, with no loops or multiple edges. For all graph-theoretic terms that we do not define, the reader is referred to Bollobás [3]. By $v(G)$ we denote the number of vertices of G (the *order* of G), and by $e(G)$, the number of edges of G (the *size* of G). The *degree* of a vertex of a graph is the number of vertices adjacent to it. A graph is called *r-regular* if the degrees of all its vertices are equal to r. By C_n, $n \geqslant 3$, we will denote the cycle on n vertices, or an *n-cycle*. If a graph does not contain a subgraph isomorphic to a graph H, we say that it is *H-free*. The *girth* of a graph containing cycles is the length of a shortest cycle. A graph is called *connected* if every pair of distinct vertices is connected by a path. The *distance* between two distinct vertices in a connected graph is the length of the shortest path connecting them. The *diameter* of a connected graph is the greatest of all distances between its vertices.

Let q be a prime power, and let $\mathbb{F}_q$ be the field of q elements. For arbitrary functions $f_i : \mathbb{F}_q^2 \to \mathbb{F}_q$, $i = 2, \ldots, n$, let a bipartite graph $G = G_q(f_2, \ldots, f_n)$ of *dimension n* be defined as follows. The vertex set of G is a union of two copies P and L of n-dimensional vector spaces over $\mathbb{F}_q$. Their elements are called *points* and *lines*, respectively, and a point $(p) = (p_1, \ldots, p_n)$ and a line $[l] = [l_1, \ldots, l_n]$ are adjacent, denoted $(p) \sim [l]$, if and only if

$$p_i + l_i = f_i(p_1, l_1), \quad i = 2, \ldots, n. \tag{1}$$

The graphs $G_q(f_2, \ldots, f_n)$ were introduced in Viglione [37] and Lazebnik and Viglione [19] where their connectivity was studied. They form a part of more general families of graphs defined by systems of equations. For the definition of the latter, their origins, properties and numerous applications, see Lazebnik and Woldar [22] and references therein. For more recent related results, see Lazebnik and Mubayi [17], Lazebnik and Viglione [20], Dmytrenko [8], and Dmytrenko, Lazebnik and Viglione [9].

Since every function $f : \mathbb{F}_q^2 \to \mathbb{F}_q$ can be interpolated by a polynomial of two variables, we can assume that all f_i are in the polynomial ring $\mathbb{F}_q[x, y]$, and that their degree with respect to each of the variables is at most $q - 1$. If all f_i in (1) are monomials, we refer to these graphs as *monomial graphs*.

It turns out that some known remarkable graphs or their large induced subgraphs, which have been of interest to researchers in finite geometry and in extremal graph theory for the several last decades, can be presented as monomial graphs. We wish to mention the following three examples.

(1) The graph $\Gamma_2 = G_q(xy)$ defined by one equation

$$p_2 + l_2 = p_1 l_1$$

is isomorphic to an induced subgraph of the point–line incidence graph of $PG(2, q)$, the classical projective plane of order q. The graph Γ_2 can be obtained from the point–line incidence graph of $PG(2, q)$ by deleting a pair of adjacent vertices and all vertices which are neighbors of one of them. It is easy to see that the graph Γ_2 is of order $2q^2$, q-regular and of girth six. See, e.g., [22] or Lazebnik and Thomason [18] for details.

(2) One can show that the graph $\Gamma_3 = G_q(xy, xy^2)$, q is odd, defined by the system

Please cite this article in press as: V. Dmytrenko et al., On monomial graphs of girth eight, Finite Fields Appl. (2006), doi:10.1016/j.ffa.2006.03.001

$$p_2 + l_2 = p_1 l_1,$$
$$p_3 + l_3 = p_1 l_1^2$$

is isomorphic to an induced subgraph of the point–line incidence graph of $W(q)$, a classical generalized quadrangle of order q. On generalized quadrangles, see Payne and Thas [28], Payne [27] and van Maldeghem [36]. The graph Γ_3 can be obtained from the point–line incidence graph of $W(q)$ by deleting a pair of adjacent vertices, and all vertices which are at distance one or two from one of them (see [8] for details). Thge graph Γ_3 is of order $2q^3$, q-regular and of girth eight.

(3) It is possible to show that the graph $\Gamma_5 = G_q(xy, xy^2, xy^3, xy^4)$ defined by the system

$$p_2 + l_2 = p_1 l_1,$$
$$p_3 + l_3 = p_1 l_1^2,$$
$$p_4 + l_4 = p_1 l_1^2,$$
$$p_5 + l_5 = p_1 l_1^4$$

is of order $2q^5$, q-regular and contains no cycles of length 4, 6 and 10 (but contains cycles of length 8).

The graphs Γ_2 and Γ_3, though presented somewhat differently, were discovered and rediscovered several times. See, e.g., Payne [26], Ustimenko [34,35], Wenger [38], Ustimenko and Lazebnik [21]. The graph Γ_5, also presented differently, appears in [38] for q prime, and (independently of [38]) for all prime powers q in [21]. For a presentation of these graphs as monomial graphs, see [19,21,37].

In both [38] and [21], the graphs $\Gamma_2, \Gamma_3, \Gamma_5$ appeared in the context of extremal Turán-type problems. Let $\mathrm{ex}(v, C_{2k})$ denote the greatest number of edges in a C_{2k}-free graph of order v. By Erdős' Even Circuit theorem, $\mathrm{ex}(v, C_{2k}) = O(v^{1+1/k})$, $v \to \infty$ (see Bondy and Simonovits [5]). This upper bound is known to be sharp in magnitude only for $k = 2, 3, 5$, and graphs Γ_k, $k = 2, 3, 5$, provide examples of magnitude $v^{1+1/k}$, $v \to \infty$. For more on this subject, see Benson [1], Singleton [30], Bondy [4], Simonovits [29,31], [22], and Füredi, Naor and Verstraëte [11].

As we pointed out, the graph Γ_2 is a subgraph in the point–line incidence graph of a projective plane. Having an s-regular 4-cycle-free bipartite graph with $2s^2$ vertices, one may try to extend it to an $(s+1)$-regular point–line incidence graph of a projective plane on $2(s^2+s+1)$ vertices. For 4-cycle-free graphs $G_q(f_2)$ such extension is always possible and unique. One may try to use this fact to construct new projective planes, and many nonisomorphic finite projective planes can be obtained this way (see, e.g., [18,25]). If f_2 is a monomial, it is easy to argue (or see [9]) that every 4-cycle-free graph $G_q(f_2)$ is isomorphic to $G_q(xy)$, and the extended graph is the point–line incidence graph of the projective plane $PG(2, q)$.

The analogous relation in dimension three is much less understood. As we mentioned above, for odd prime powers q, the graph Γ_3 is isomorphic to an induced subgraph of the point–line incidence graph of a classical generalized quadrangle $W(q)$. For each odd prime power q only two nonisomorphic generalized quadrangles of order q are known. They are usually denoted by $W(q)$ and $Q(4, q)$, and it is known that one is the dual of another, see Benson [2]. This means that their point–line incidence graphs are isomorphic. Therefore, for odd q, only one example of an infinite series of $(q+1)$-regular bipartite graphs of girth eight and diameter four is known. Just as a 4-cycle-free graph $G_q(f_2)$ gives rise to a projective plane, a three-dimensional graph $G_q(f_2, f_3)$ of girth eight may give rise to a generalized quadrangle.

Please cite this article in press as: V. Dmytrenko et al., On monomial graphs of girth eight, Finite Fields Appl. (2006), doi:10.1016/j.ffa.2006.03.001

This brings us to the main goal of this paper, which is the study of the existence of such graphs. We concentrate on the case where the functions f_2 and f_3 are monomials. For q even, contrary to the two-dimensional case, there are examples of monomial graphs of girth eight which do lead to nonisomorphic quadrangles. These graphs are all derived from the known hyperovals in $PG(2, q)$; see [27,36] for a description of the connection between hyperovals and generalized quadrangles, see [8] for the connection between some monomial graphs of girth eight and hyperovals, and see Glynn [13,14], Cherowitzo [7] for a list of known hyperovals in $PG(2, q)$, q even. It is conjectured [13] that known examples of monomial hyperovals represent all possible ones. The conjecture was checked by computer for all $e \leqslant 28$ in [14], and for all $e \leqslant 40$, recently, by Chandler [6].

For odd q, the situation is closer to the two-dimensional case in the sense that we could not find an example of a girth eight monomial graph nonisomorphic to Γ_3. What is different from that case is that we could prove the uniqueness of Γ_3 only for some sets of values of q.

We need one more definition in order to state our results. A *permutation polynomial on* $\mathbb{F}_q$ is a polynomial $f \in \mathbb{F}_q[x]$ such that the function defined by $a \mapsto f(a)$ is a bijection on $\mathbb{F}_q$.

Theorem 1. *Let $q = p^e$ be an odd prime power. Then every monomial graph of girth at least eight is isomorphic to the graph $G = G_q(xy, x^k y^{2k})$, where k is not divisible by p. If $q = 3$, then G is isomorphic to $G_3(xy, xy^2)$, and has girth eight. If $q \geqslant 5$, the following statements also hold*:

(a) $1 \leqslant k < \frac{q-1}{2}$, *and* $\gcd(k, q-1) = 1$.
(b) $k \equiv 1 \bmod (p-1)$.
(c) *If $k > 1$, then $2k-1$ does not divide $q-1$.*
(d) $\binom{2k}{k} \equiv 2 \bmod p$, *and* $\binom{4k}{2k} \equiv 6 \bmod p$.
(e) *If $q - 1 = nk + r$, $1 \leqslant r < k$, and p does not divide n, then* $\binom{2r}{r} \equiv \binom{nk}{2nk-q+1} \equiv 0 \bmod p$.
(f) $F(x) = ((x+1)^{2k} - 1)x^{q-1-k} - 2x^{q-1}$ *is a permutation polynomial on* $\mathbb{F}_q$.
(g) $G(x) = ((x+1)^k - x^k)x^k$ *is a permutation polynomial on* $\mathbb{F}_q$.

Note that part (d) of the theorem implies that for a given $k \geqslant 2$, there exist only finitely many odd characteristics p for which a monomial graph can be of girth at least eight.

The following theorem imposes additional necessary conditions on k for the graph $G_q(xy, x^k y^{2k})$ to be of girth at least eight.

Theorem 2. *Let $q = p^e$ be an odd prime power, $p \geqslant 5$, and $1 \leqslant k < \frac{q-1}{2}$. Then if the graph $G = G_q(xy, x^k y^{2k})$ has girth at least eight, then all of the digits of k in the representation of k base p must be at most $\frac{p-1}{4}$.*

Theorems 1 and 2 imply the following result, which gives an explicit set of values of q for which the monomial graphs of girth at least eight are completely understood.

Theorem 3. *Let $q = p^e$ be an odd prime power, with $p \geqslant 5$ and $e = 2^a 3^b$ for integers $a, b \geqslant 0$. Then every monomial graph of girth at least eight is isomorphic to Γ_3 and has girth eight. For all odd q, $3 \leqslant q \leqslant 10^{10}$, every monomial graph nonisomorphic to Γ_3 has girth at most six.*

Note that Theorem 3, in particular, covers all fields $\mathbb{F}_{p^e}$ with $1 \leqslant e \leqslant 4$ and $p \geqslant 5$.

Please cite this article in press as: V. Dmytrenko et al., On monomial graphs of girth eight, Finite Fields Appl. (2006), doi:10.1016/j.ffa.2006.03.001

The paper is organized as follows. The next section contains all necessary definitions and results needed for our proofs of Theorems 1–3, which are presented in Section 3. Section 4 contains comments and some open problems.

We would like to end this introduction with the following conjecture.

Conjecture 4. *Let q be an odd prime power. Then every monomial graph of girth eight is isomorphic to Γ_3.*

2. Preliminary results

In this section we present all definitions, notations and results which are needed for our proofs of Theorems 1–3 in the next section. Though many of these definitions and results can be stated for much more general algebraically defined graphs, we restrict ourselves mainly to monomial three-dimensional graphs with $q = p^e$, where p is an odd prime. By $\mathbb{F}_q^*$ we will denote both the set $\mathbb{F}_q \setminus \{0\}$, and the multiplicative group of the finite field $\mathbb{F}_q$. As it was mentioned in the introduction, we may and will always assume that exponents u, v, k, m in $G_q(x^u y^v, x^k y^m)$ are nonnegative integers and do not exceed $q-1$.

2.1. Δ_k-map and cycles

Here we would like to describe the existence of 4- and 6-cycles in graphs $G_q(f_2, f_3)$ in algebraic terms.

For $k = 2, 3$, we define a map $\Delta_k : \mathbb{F}_q[x, y] \to \mathbb{F}_q[z_1, \ldots, z_k, t_1, \ldots, t_k]$ as follows:

$$\Delta_2(f)(z_1, z_2, t_1, t_2) = f(z_1, t_1) - f(z_2, t_1) + f(z_2, t_2) - f(z_1, t_2) \quad \text{and}$$

$$\Delta_3(f)(z_1, z_2, z_3, t_1, t_2, t_3) = f(z_1, t_1) - f(z_2, t_1) + f(z_2, t_2) - f(z_3, t_2) + f(z_3, t_3) - f(z_1, t_3).$$

Hence $\Delta_k(f)$ is a polynomial over $\mathbb{F}_q$ in $2k$ variables. A solution $(a_1, \ldots, a_k; b_1, \ldots, b_k)$ of the equation $\Delta_k(f) = 0$ or a system of equations $\Delta_k(f) = \Delta_k(g) = 0$ over $\mathbb{F}_q^{2k}$ is called *trivial* if one of the following occurs: $a_k = a_1$, $b_k = b_1$, $a_i = a_{i+1}$ or $b_i = b_{i+1}$ for some $i = 1, \ldots, k-1$. Otherwise, a solution is called *nontrivial*.

Proposition 5. *Let $G = G_q(f_2, f_3)$. Then G contains a cycle of length $2k$, $k = 2, 3$, if and only if the system of equations*

$$\Delta_k(f_2) = \Delta_k(f_3) = 0 \tag{2}$$

has a nontrivial solution.

Proof. Let $(p^1) \sim [l^1] \sim \cdots \sim (p^k) \sim [l^k] \sim (p^1)$ be a $2k$-cycle in G, $(p^i) = (p_1^i, p_2^i, p_3^i)$, $[l^i] = [l_1^i, l_2^i, l_3^i]$, $i = 1, \ldots, k$, $k = 2, 3$. For $j = 2$ and $j = 3$, using repeatedly the adjacency condition (1), we obtain

$$l_j^1 = f_j(p_1^1, l_1^1) - p_j^1,$$
$$p_j^2 = f_j(p_1^2, l_1^1) - f_j(p_1^1, l_1^1) + p_j^1,$$

Please cite this article in press as: V. Dmytrenko et al., On monomial graphs of girth eight, Finite Fields Appl. (2006), doi:10.1016/j.ffa.2006.03.001

$$l_j^2 = f_j\left(p_1^2, l_1^2\right) - f_j\left(p_1^2, l_1^1\right) + f_j\left(p_1^1, l_1^1\right) - p_j^1,$$

$$\vdots$$

$$l_j^k = \sum_{i=1}^{k} f_j\left(p_1^i, l_1^i\right) - \sum_{i=1}^{k-1} f\left(p_1^{i+1}, l_1^{i+1}\right) - p_j^1,$$

$$p_j^1 = f\left(p_1^1, l_1^k\right) + \sum_{i=1}^{k-1} f\left(p_1^{i+1}, l_1^i\right) - \sum_{i=1}^{k} f_j\left(p_1^i, l_1^i\right) + p_j^1.$$

The last equation yields $\Delta_k(f_j)(S) = 0$, where $S = (p_1^1, \ldots, p_1^k; l_1^1, \ldots, l_1^k)$. Since a neighbor of any vertex is uniquely determined by the neighbor's first coordinate, and all vertices of the $2k$-cycle $(p^1), [l^1], \ldots, (p^k), [l^k]$ are distinct, the solution S is nontrivial.

Let S be a nontrivial solution of (2). Then we define a closed walk corresponding to S in the following way. Assign arbitrary values to $p_2^1, \ldots, p_m^1$. This, together with p_1^1 of S, determines (p^1). Having (p^1) and $p_1^2, \ldots, p_1^k, l_1^1, \ldots, l_1^k$ of S, we uniquely determine the remaining vertices of the walk by using (1). Since S is nontrivial, all vertices of the obtained closed walk are distinct. Hence, it is a $2k$-cycle. □

Thus the presence of a 4- or a 6-cycle in $G = G_q(f_2, f_3)$ can be seen by looking to just the first coordinates of its subsequent vertices. We say that G contains a $2k$-cycle *corresponding to* or *defined by* $S = (a_1^1, \ldots, a_1^k; b_1^1, \ldots, b_1^k)$ if there exists a $2k$-cycle $(p^1) \sim [l^1] \sim (p^2) \sim [l^2] \sim \cdots \sim (p^k) \sim [l^k] \sim (p^1)$ in G with $a_i = p_1^i$ and $b_i = l_1^i$, for each $i = 1, \ldots, k$. Such a cycle exists if and only if S is a nontrivial solution (2).

2.2. Isomorphisms and automorphisms

In the following proposition we collect all facts on isomorphisms and automorphism of graphs $G_q(f_2, f_3)$ that will be used later in this paper. All proofs are immediate and we omit them.

Proposition 6. *Let $q = p^e$ be a prime power, and let $f_2, f_3 \in \mathbb{F}_q[x, y]$.*

(a) (*Point–line isomorphism*) *If $g_i(x, y) = f_i(y, x)$ for $i = 2, 3$, then graphs $G_q(f_2, f_3)$ and $G_q(g_2, g_3)$ are isomorphic, an explicit isomorphism is given by $(x) = (x_1, x_2, x_3) \mapsto [x] = [x_1, x_2, x_3]$ and $[x] = [x_1, x_2, x_3] \mapsto (x) = (x_1, x_2, x_3)$.*

(b) (*Induced Frobenius isomorphism*) *For each integer $a \geqslant 0$, graphs $G_q(f_2, f_3)$ and $G_q(f_2^{p^a}, f_3^{p^a})$ are isomorphic due to the explicit isomorphism defined via $(p_1, p_2, p_3) \mapsto (p_1^{p^a}, p_2^{p^a}, p_3^{p^a})$ and $[l_1, l_2, l_3] \mapsto [l_1^{p^a}, l_2^{p^a}, l_3^{p^a}]$.*

2.3. Permutation polynomials

We remind the reader that a polynomial $f \in \mathbb{F}_q[x]$ is called a *permutation polynomial*, if it permutes the elements of $\mathbb{F}_q$, i.e., if the corresponding function $f : \mathbb{F}_q \to \mathbb{F}_q$, $a \mapsto f(a)$, is a bijection.

As $a^q = a$ for every $a \in \mathbb{F}_q$, we may always assume that degrees of polynomials (considered as functions over $\mathbb{F}_q$) with respect to any variable are at most $q - 1$.

Please cite this article in press as: V. Dmytrenko et al., On monomial graphs of girth eight, Finite Fields Appl. (2006), doi:10.1016/j.ffa.2006.03.001

It is clear that every linear polynomial over $\mathbb{F}_q$ is a permutation polynomial. We will often use the following simple statements.

Proposition 7. [23]

(a) *The degree of a nonlinear permutation polynomial does not divide to* $q-1$. *The monomial* x^n *is a permutation polynomial if and only if* $\gcd(n, q-1) = 1$.
(b) *If* $f \in \mathbb{F}_q[x]$ *is a permutation polynomial, and* $f(0) = 0$, *then* $\prod_{x\in\mathbb{F}_q^*} f(x) = -1$.

The conditions for a polynomial to be a permutation polynomial are rather complicated. The following criterion remains to be one of the most popular and powerful tools in the theory of permutation polynomials for more than 100 years. It is called the *Hermite–Dickson criterion* (see, for example, [32]), since it was shown by Hermite in [12] for prime fields and the general case was established by Dickson in [10].

Theorem 8 *(Hermite–Dickson criterion). Let* $\mathbb{F}_q$ *be a field of characteristic* p. *Then* $f \in \mathbb{F}_q[x]$ *is a permutation polynomial if and only if the following two conditions hold*:

(a) f *has exactly one root in* $\mathbb{F}_q$;
(b) *for each integer* t *with* $1 \leqslant t \leqslant q-2$ *and* $t \not\equiv 0 \bmod p$, *the reduction of* $f(x)^t \bmod (x^q - x)$ *has degree* $\leqslant q-2$.

Now we give some results on permutation polynomials, which are closely connected with our investigations of polynomial graphs. The following theorem was proven by Matthews in [24].

Theorem 9. *Let* $q = p^e$ *be an odd prime power. Then* $\psi_k(x) = 1 + x + \cdots + x^k \in \mathbb{F}_q[x]$ *is a permutation polynomial if and only if* $k \equiv 1 \bmod p(q-1)$.

The following lemma is a little weaker than Theorem 9, but we will need it in Section 3.

Lemma 10. [8] *Let* q *be an odd prime power,* a *be a positive integer, and let* $\phi_a : \mathbb{F}_q \setminus \{1\} \to \mathbb{F}_q$ *be defined by* $\phi_a(x) = (x^{a+1} - 1)/(x-1)$. *Then* ϕ_a *is injective if and only if* $a \equiv 1 \bmod (q-1)$.

Proof. If $a \equiv 1 \bmod (q-1)$, then $a = s(q-1) + 1$, and for all $\alpha \in \mathbb{F}_q \setminus \{1\}$,

$$\phi_a(\alpha) = \frac{\alpha^{s(q-1)+2} - 1}{\alpha - 1} = \frac{\alpha^2 - 1}{\alpha - 1} = \alpha + 1.$$

Hence, ϕ_a is injective.

Suppose ϕ_a is injective, and let β be the only element of $\mathbb{F}_q$ which is not a value of ϕ_a. Let $a = s(q-1) + t$, $0 \leqslant t < q-1$. Then the polynomial $f(x) = 1 + x + \cdots + x^t + (\beta - t - 1) \times (1 - (x-1)^{q-1})$ is a permutation polynomial since $f(x) = \phi_a(x)$ for all $x \neq 1$ and $f(1) = \beta$. By Theorem 8(b), $\deg f < q-1$, therefore, $\beta = t+1$, and $f(x) = 1 + x + \cdots + x^t$. Then, by Theorem 9, $t \equiv 1 \bmod p(q-1)$. Hence, $a \equiv t \equiv 1 \bmod (q-1)$. □

Lemma 11. *Let* $q = p^e \geqslant 5$ *be an odd prime power. Let* k *be an integer such that* $1 \leqslant k < q-1$ *and* $\gcd(k, q-1) = 1$. *Suppose there exists* $A \in \mathbb{F}_q$ *such that the function* f *on* $\mathbb{F}_q$ *given by*

Please cite this article in press as: V. Dmytrenko et al., On monomial graphs of girth eight, Finite Fields Appl. (2006), doi:10.1016/j.ffa.2006.03.001

$f(x) = \frac{x^{2k}-1}{(x-1)^k}$ for $x \neq 1$, and $f(1) = A$ is a bijection. Then $1 \leqslant k < \frac{q-1}{2}$. If, in addition, $k \equiv 1 \bmod (p-1)$, then $\binom{2k}{k} \equiv 2 \bmod p$ and $A = 2$.

Proof. Let $h_f(x) = (x^{2k}-1)(x-1)^{q-1-k} + A(1-(x-1)^{q-1})$. Then $h_f(a) = f(a)$ for every $a \in \mathbb{F}_q$, and $A \neq f(-1) = 0$. Hence, h_f is a permutation polynomial. Computing the coefficient at x^{q-1} in $h_f \bmod (x^q - x)$, we obtain that it is equal to $-\binom{q-1-k}{k} - A$ for all k, $1 \leqslant k < q-1$. By Theorem 8, it must be zero, hence

$$0 \neq A = -\binom{q-1-k}{k}.$$

Since $\binom{q-1-k}{k} = 0$ for $(q-1)/2 < k < q-1$, and $q \geqslant 5$, we conclude that $1 \leqslant k < (q-1)/2$ ($k \neq (q-1)/2$ since $\gcd(k, q-1) = 1$ and $q \geqslant 5$).

Using the identity

$$\binom{q-m}{r} \equiv (-1)^r \binom{m+r-1}{r} \mod p \tag{3}$$

from Turnwald [33] for $m = k+1$ and $r = k$, k odd, we obtain $-\binom{q-1-k}{k} \equiv \binom{2k}{k} \bmod p$.

On the other hand, as f is a bijection, and each of $(x-1)^k$, $x^k - 1$, $x^k + 1$ is a permutation polynomial on $\mathbb{F}_q$, applying Proposition 7(b), we obtain:

$$-1 = \prod_{x \neq -1} f(x) = A \cdot \prod_{x \neq -1,1} \frac{x^{2k}-1}{(x-1)^k} = A \prod_{x \neq -1,1} \frac{1}{(x-1)^k} \prod_{x \neq -1,1} \left(x^k - 1\right) \prod_{x \neq -1,1} \left(x^k + 1\right)$$
$$= A\left(2^k\right)\left(\frac{1}{2}\right)\left(-\frac{1}{2}\right) = -A2^{k-2}.$$

Hence $A = 2^{2-k}$. If $k \equiv 1 \bmod (p-1)$, then, as $2^{p-1} \equiv 1 \bmod p$, we obtain $2^{2-k} \equiv 2 \bmod p$, and $A = 2$. □

3. Proofs of Theorems 1–3

3.1. 4- and 6-cycle-free conditions

We begin with the question of when a monomial graph $G = G_q(x^u y^v, x^k y^m)$ is 4-cycle-free. The existence of a 4-cycle in a graph $G_q(f_2, f_3)$ of dimension three implies the existence of a 4-cycle in each of the two-dimensional graphs $G_q(f_i)$, $i = 2, 3$. Indeed, deleting the third (respectively, the second) coordinate in every vertex of the 4-cycle in $G_q(f_2, f_3)$ gives a 4-cycle in $G_q(f_2)$ (respectively, $G_q(f_3)$).

By $\bar{a}$ we denote the greatest common divisor of integers a and $q-1$.

Lemma 12. *The graph $G = G_q(x^u y^v, x^k y^m)$ has no 4-cycles if and only if the exponents u, v, k, m satisfy one of the following conditions*:

(i) $\bar{u} = \bar{v} = 1$;
(ii) $\bar{k} = \bar{m} = 1$;

(iii) $\bar{u} = \bar{k} = 1$ *and* $\gcd(\bar{v}, \bar{m}) = 1$;
(iv) $\bar{v} = \bar{m} = 1$ *and* $\gcd(\bar{u}, \bar{k}) = 1$.

Proof. Let $f_2 = x^u y^v$ and $f_3 = x^k y^m$. By Proposition 5, $C = (a)[b](c)[d]$ is a 4-cycle in G if the corresponding first components a_1, b_1, c_1, d_1 form a nontrivial solution of the system $\Delta_2(f_2) = \Delta_2(f_3) = 0$. The latter can be rewritten in the following form:

$$\left(a_1^u - c_1^u\right)\left(b_1^v - d_1^v\right) = \left(a_1^k - c_1^k\right)\left(b_1^m - d_1^m\right) = 0.$$

If $\bar{u} > 1$, then we have a solution of $\Delta_2(f_2) = 0$ for any pair $b_1 \neq d_1$. If also $\bar{m} > 1$, we may choose a solution of $\Delta_2(f_3) = 0$ independently of a_1, c_1 to obtain a 4-cycle in G. Hence, $\max(\bar{u}, \bar{m}) = 1$, and similarly $\max(\bar{v}, \bar{k}) = 1$.

Now if $\bar{u} = \bar{v} = 1$, we have (i); obviously, in this case we do not have 4-cycles since we do not have nontrivial solutions of (2). Similarly, with $\bar{k} = \bar{m} = 1$ we have (ii).

Suppose that $\bar{v} = \bar{m} = 1$. Then a 4-cycle is possible only if we have a common solution of $(a_1/c_1)^u = 1$ and $(a_1/c_1)^k = 1$. This happens if and only if $\gcd(\bar{u}, \bar{k}) > 1$, otherwise, we have (iv). Finally, $\bar{u} = \bar{k} = 1$ and the 4-cycle-free condition lead to (iii). □

The next two lemmas reduce the study of 4- and 6-cycle-free monomial graphs to graphs $G_q(xy, x^k y^{2k})$.

Lemma 13. *Let q be an odd prime power. Then a monomial graph G of girth at least eight is isomorphic to a monomial graph $G_q(xy, x^{k'} y^{m'})$ for some nonnegative integers k' and m'.*

Proof. Let $G = G_q(x^u y^v, x^k y^m)$. Since G contains no 4-cycles, the parameters u, v, k, m satisfy at least one of conditions (i)–(iv) in the statement of Lemma 12.

Let positive integers u', v' satisfy $uu' \equiv vv' \equiv 1 \bmod (q-1)$. Then in case (i) the mapping $(p_1, p_2, p_3) \mapsto (p_1^{u'}, p_2, p_3)$, $[l_1, l_2, l_3] \mapsto [l_1^{v'}, l_2, l_3]$ is an isomorphism of G to $G_q(xy, x^{k'} y^{m'})$, where $k' \equiv u'k \bmod (q-1)$ and $m' \equiv v'm \bmod (q-1)$. A similar argument applies in case (ii). To finish the proof, we show that in cases (iii) and (iv) G contains a 6-cycle.

Due to the point–line isomorphism (Proposition 6(a)), it is sufficient to consider only case (iii). Let $S = (1, 0, -1; 1, -1, 0)$. Then $\Delta_3(x^u y^v)(S) = 1 - (-1)^{u+v}$, and $\Delta_3(x^k y^m)(S) = 1 - (-1)^{k+m}$. As we are in case (iii), both u and k are odd, therefore, S is a nontrivial solution of the system $\Delta_3(x^u y^v) = \Delta_3(x^k y^m) = 0$ and G contains a 6-cycle. Hence, as $\gcd(\bar{v}, \bar{m}) = 1$, exactly one of v and m is even. Due to the point–line isomorphism, we may assume that m is even, hence, $\bar{m} \geqslant 2$, and v is odd.

Arguing as in case (i), we may assume $k = 1$. Hence, $G = G_q(x^u y^v, xy^m)$, where v is odd, m is even, and $\bar{u} = \gcd(\bar{v}, \bar{m}) = 1$.

If $\bar{v} = 1$, then, since $\bar{u} = 1$, we are in case (i), which has been already considered. Therefore $\bar{v} \geqslant 3$, and there exist distinct α, β and γ such that $\alpha^v = \beta^v = \gamma^v$. Then α^m, β^m and γ^m are all distinct. Indeed, if, say $\alpha^m = \beta^m$, then the order d of α/β in $\mathbb{F}_q^*$ is greater than 1 and would divide both v and m. This contradicts the fact that $\gcd(\bar{v}, \bar{m}) = 1$. Consider $S_1 = (\frac{\beta^m - \gamma^m}{\alpha^m - \gamma^m}, 0, 1; \alpha, \beta, \gamma)$. We have $\Delta_3(x^u y^v)(S_1) = 0$, and $\Delta_3(xy^m)(S_1) = 0$. Hence S_1 is a nontrivial solution of the system $\Delta_3(x^u y^v) = \Delta_3(xy^v) = 0$. By Proposition 5, S_1 defines a 6-cycle in G. Thus case (iii) is not possible, and the proof is finished. □

Please cite this article in press as: V. Dmytrenko et al., On monomial graphs of girth eight, Finite Fields Appl. (2006), doi:10.1016/j.ffa.2006.03.001

The following lemma imposes additional restrictions on k and m for graphs $G_q(xy, x^k y^m)$ of girth at least eight. Though part (b) of the lemma implies part (a), the latter is used in the proof of part (b), and we include it for convenience.

Lemma 14. *Let $G = G_q(xy, x^k y^m)$ be a monomial graph of girth at least eight. Then*

(a) *$k + m$ is odd, $\bar{k} \leqslant 2$, and $\bar{m} \leqslant 2$;*
(b) *$m \equiv 2k \bmod (q-1)$ and $\bar{k} = 1$, or $k \equiv 2m \bmod (q-1)$ and $\bar{m} = 1$;*
(c) *G is isomorphic to $G_q(xy, x^k y^{2k})$ for odd k not divisible by p and $1 \leqslant k < q-1$, or to $G_q(xy, x^m y^{2m})$ for odd m not divisible by p and $1 \leqslant m < q-1$.*

Proof. (a) Suppose that $k + m$ is even. Let $S = (1, 0, -1; 1, -1, 0)$. Then $\Delta_3(xy)(S) = \Delta_3(x^k y^m)(S) = 0$. As q is odd, S is a nontrivial solution of the system. By Proposition 5, G contains a 6-cycle defined by S, a contradiction. Therefore $k + m$ is odd.

For $a, b \in \mathbb{F}_q$, $a \neq b$, let $S_1 = (1, 0, \frac{b-1}{b-a}; 1, a, b)$. Then $\Delta_3(xy)(S_1) = 0$ for all such a and b, and $\Delta_3(x^k y^m)(S_1) = 1 - b^m + (\frac{b-1}{b-a})^k (b^m - a^m)$.

If $\bar{m} \geqslant 3$, there exist at least three distinct solutions of the equation $x^m = 1$. Let a and b be two of them which are both not equal to 1. Then $\Delta_3(x^k y^m)(S_1) = 0$. Note that $a \neq 1$ implies $\frac{b-1}{b-a} \neq 1$, and $b \neq 1$ implies $\frac{b-1}{b-a} \neq 0$. Hence S_1 is a nontrivial solution, and it defines a 6-cycle in G, a contradiction. Therefore $\bar{m} \leqslant 2$. The condition $\bar{k} \leqslant 2$ follows from the point–line isomorphism.

(b) Suppose that k is odd. Then m is even, $\bar{k} = 1$, and $\bar{m} = 2$ by part (a). Let $S_2 = (c, 1, d; d, c, 1)$. We wish to show that if $m \not\equiv 2k \bmod (q-1)$, there exist c, d such that S_2 is a nontrivial solution of $\Delta_3(xy) = \Delta_3(x^k y^m) = 0$. Then G contains a 6-cycle defined by S_2, a contradiction.

Indeed, $\Delta_3(xy)(S_2) = 0$ for all c and d. Hence it is sufficient to consider the second equation only.

Since $\Delta_3(x^k y^m)(S_2) = c^k d^m - d^m + c^m - d^k c^m + d^k - c^k$, S_2 is a solution of $\Delta_3(x^k y^m) = 0$ if and only if $(c^k - 1)(d^m - 1) = (d^k - 1)(c^m - 1)$, and S_2 is nontrivial if and only if $1, c, d$ are all distinct.

Let l be the multiplicative inverse of $k \bmod (q-1)$, i.e., $kl \equiv 1 \bmod (q-1)$. Set $f = c^k$ and $g = d^k$. Then $c^m = f^{lm}$, $d^m = g^{lm}$ and the last equation can be rewritten as

$$\frac{f^{lm} - 1}{f - 1} = \frac{g^{lm} - 1}{g - 1}. \tag{4}$$

If $m \not\equiv 2k \bmod (q-1)$, then $lm \not\equiv 2 \bmod (q-1)$, and, by Lemma 10, the function $\phi_{lm-1} = (x^{lm} - 1)/(x - 1)$ on $\mathbb{F}_q \setminus \{1\}$ is not a bijection. Hence there exists a solution (c, d) of (4) with $c \neq d$. As $c \neq 1$ and $d \neq 1$, S_2 is a nontrivial solution of $\Delta_3(xy) = \Delta_3(x^k y^m) = 0$. This proves that $m \equiv 2k \bmod (q-1)$.

If p divides k, then $k = p^a k'$, where k' is not divisible by p, and the graph $G_q(xy, x^k y^{2k})$ is isomorphic to the graph $G_q(xy, x^{k'} y^{2k'})$ by Proposition 6(b). Finally, the inequality $1 \leqslant k < q - 1$ follows from the reduction by modulo $x^q - x$ and the condition $\gcd(k, q-1) = 1$.

Similarly, if we assume that k is even, then m is odd, $\bar{m} = 1$, and $k \equiv 2m \bmod (q-1)$. This ends the proof of (b), and part (c) immediately follows. □

Please cite this article in press as: V. Dmytrenko et al., On monomial graphs of girth eight, Finite Fields Appl. (2006), doi:10.1016/j.ffa.2006.03.001

The previous lemma narrows our focus to graphs of the form $G(xy, x^k y^{2k})$, where $\gcd(k, q-1) = 1$. In the next lemma we construct two functions which must be bijections if a graph $G(xy, x^k y^{2k})$ has girth at least eight.

Lemma 15. *Let q be an odd prime power, and let $\gcd(k, q-1) = 1$, $1 \leqslant k < q-1$. If $G = G_q(xy, x^k y^{2k})$ has girth at least eight, the following must hold*:

(a) *the function $f : \mathbb{F}_q \setminus \{1\} \to \mathbb{F}_q$ given by $f(x) = \frac{x^{2k}-1}{(x-1)^k}$ for $x \neq 1$ is an injection*;

(b) *the function on $\mathbb{F}_q$ given by $g(x) = \frac{x^k-1}{(x-1)^{2k}}$ for $x \neq 1$ and $g(1) = 0$ is a bijection.*

Proof. (a) Let $f(x) = (x^{2k}-1)/(x-1)^k$ be *not* one-to-one on $\mathbb{F}_q \setminus \{1\}$. Then there exist distinct $c, d \in \mathbb{F}_q \setminus \{1\}$ such that $f(c) = f(d)$. If one of c, d is equal -1, then another is equal to -1, which contradicts $c \neq d$. As none of c and d is 1 or -1, none of $c^{2k} - 1$ or $d^{2k} - 1$ is zero. Let $a = \frac{d-1}{c-1}$. Then

$$a^k = \frac{(d-1)^k}{(c-1)^k} = \frac{d^{2k}-1}{c^{2k}-1}.$$

We claim that $S = (a, 0, 1; c, d, 1)$ is a nontrivial solution of the system $\Delta_3(xy) = \Delta_3(x^k y^{2k}) = 0$. Indeed, $\Delta_3(xy)(S) = ac - a - d + 1 = a(c-1) - (d-1) = 0$, and $\Delta_3(x^k y^{2k})(S) = a^k c^{2k} - a^k - d^{2k} + 1 = a^k(c^{2k}-1) - (d^{2k}-1) = 0$. As $a \neq 0, 1$, and all $c, d, 1$ are distinct, S is a nontrivial solution, and, by Proposition 5, G contains a 6-cycle.

Hence $f(x) = (x^{2k}-1)/(x-1)^k$ must be one-to-one on $\mathbb{F}_q \setminus \{1\}$.

(b) As graphs $G(xy, x^k y^{2k})$ and $G_q(xy, x^{2k} y^k)$ are isomorphic, a similar calculation to the one in part (a) (with the same $S = (a, 1, 0; c, d, 1)$) shows that $g(x)$ is injective on $\mathbb{F}_q \setminus \{1\}$. Since $\gcd(k, q-1) = 1$, $(x^k - 1)/(x-1)^{2k}$ is never zero for $x \neq 1$, implying that $g(x)$ is a bijection. □

3.2. Proof of Theorem 1

By Lemmas 13 and 14, we may assume that G is isomorphic to $G_q(xy, x^k y^{2k})$, where k is not divisible by p. In particular, this implies the statement for $q = 3$.

(a) The condition $\gcd(k, q-1) = 1$ was also obtained in Lemma 14. Now Lemma 15(a) implies that the function f can be extended to a bijection on $\mathbb{F}_q$. Then the inequality $1 \leqslant k < \frac{q-1}{2}$ follows from Lemma 11.

(e) We consider a polynomial $h(x) = ((x+1)^k - 1)x^{q-2k-1}$. The exponent $q - 2k - 1 > 0$ since $1 \leqslant k < \frac{q-1}{2}$ by part (a). Note that for the function g from Lemma 15(b), $h(a) = g(1+a)$ for all $a \in \mathbb{F}_q^*$ and $h(0) = 0 = g(1)$. As g is a bijection on $\mathbb{F}_q$, h is a permutation polynomial.

Since $k > 1$ and $\gcd(k, q-1) = 1$, $nk < q - 1 < (n+1)k$. Hence, as $k < \frac{q-1}{2}$, we have $0 < 2(q-1) - 2nk < q - 1$, and

$$h(x)^n = \big((x+1)^k - 1\big)^n x^{(q-1-2k)n} \equiv \big((x+1)^k - 1\big)^n x^{2(q-1)-2nk} \mod \big(x^q - x\big).$$

Please cite this article in press as: V. Dmytrenko et al., On monomial graphs of girth eight, Finite Fields Appl. (2006), doi:10.1016/j.ffa.2006.03.001

Let j be an exponent of x in a term of the expansion of $((x+1)^k-1)^n$ such that $x^{j+2(q-1)-2nk} \equiv x^{q-1} \bmod (x^q-x)$. As

$$\left((x+1)^k-1\right)^n = \sum_{m=0}^{n} \binom{n}{m} (x+1)^{km} (-1)^{n-m} = \sum_{m=0}^{n} (-1)^{n-m} \binom{n}{m} \sum_{j=0}^{km} \binom{km}{j} x^j,$$

it is easy to verify that such a term appears only when $m=n$ and $j=2nk-(q-1)$. The coefficient of this term is $\binom{nk}{2nk-q+1}$. Then by identity (3), $\binom{nk}{2nk-q+1} \equiv \binom{2r}{r} \bmod p$. As h is a permutation polynomial, the conclusion follows from the Hermite–Dickson criterion.

(b) If q is prime, $q=p$, then $2 \leqslant n < p$, hence p does not divide n. If $1 \leqslant r < k < (p-1)/2$, the binomial coefficient $\binom{2r}{r}$ is not divisible by p. This contradicts (e), and therefore $k=1$. For q not prime, as $\mathbb{F}_p$ is a subfield of $\mathbb{F}_q$, the graph $G_p(xy, x^{k \bmod (p-1)} y^{2k \bmod (p-1)})$ is a subgraph of G. As its girth is at least eight, we obtain $k \equiv 1 \bmod (p-1)$.

(f) We extend the function f of Lemma 15(a) to a permutation polynomial $h_f(x) = (x^{2k}-1)(x-1)^{q-1-k} + 2(1-(x-1)^{q-1})$, as it was done in the proof of Lemma 11. Let $t=x-1$ and $F(t) = h_f(t+1) - 2 = ((t+1)^{2k}-1)t^{q-1-k} - 2t^{q-1}$. Then $F(t)$ is a permutation polynomial.

(d) The first congruence now follows from Lemma 15(a) and Lemma 11. In order to obtain the second congruence, we consider the coefficient at t^{q-1} in $F^2(t) \bmod (t^q-t)$. Omitting tedious but straightforward transformations, we obtain that for every k, $1 \leqslant k < q-1$,

$$\binom{4k}{q-1+2k} + \binom{4k}{2k} - \binom{2k}{k}^2 - 2 \equiv \binom{4k}{q-1+2k} + \binom{4k}{2k} - 6 \mod p.$$

As $1 \leqslant k < (q-1)/2$, we have $4k < q-1+2k$, hence $\binom{4k}{q-1+2k} = 0$. This yields $\binom{4k}{2k} \equiv 6 \bmod p$.

(g) Let g be the function defined in Lemma 15(b). Then it is a bijection, since the conditions of Lemma 15 are satisfied. Then the function $h_g(x) = g(x+1)$, $h_g(0)=0$, has the same range on $\mathbb{F}^*$ as the function $G(x) = h_g(\frac{1}{x}) = ((x+1)^k - x^k)x^k$, namely $\mathbb{F}^*$. The expression $((x+1)^k-x^k)x^k$ is 0 for $x=0$. Hence $G(x)$ is a permutation polynomial.

(c) The degree of $G(x)$ is $2k-1>1$. As the degree of a nonlinear permutation polynomial over F_q does not divide $q-1$, see Proposition 7(a), we obtain that $2k-1$ does not divide $q-1$.

3.3. Proof of Theorem 2

Let $k = \sum_{i=0}^{N} k_i p^i$ where all $0 \leqslant k_i \leqslant p-1$. Since neither 2 nor 6 is divisible by p for $p \geqslant 5$, we know, by Theorem 1, that neither $\binom{2k}{k}$ nor $\binom{4k}{2k}$ is divisible by p. By a theorem of Kummer [16] (see also Knuth [15]), the greatest exponent e such that prime power p^e divides the binomial coefficient $\binom{a}{b}$ is the number of 'carries' when we add b and $a-b$ in base p. For $a=2k$ and $b=a-b=k$, since no 'carries' occur, we obtain that $0 \leqslant k_i \leqslant \frac{p-1}{2}$ for all i. Hence the base p digits of $2k$ are $2k_i$. Setting $a=4k$ and $b=a-b=2k$, since no 'carries' occur, we obtain that $0 \leqslant 2k_i \leqslant \frac{p-1}{2}$ for all $i=1,\ldots,N$. This is equivalent to the statement of the theorem.

3.4. Proof of Theorem 3

By Lemma 14(c), G is isomorphic to a graph $G_q(xy, x^k y^{2k})$, where k satisfies the necessary conditions stated in Theorems 1 and 2. If $a=b=0$, then $q=p$, and the graph $G_q(xy, x^k y^{2k})$

Please cite this article in press as: V. Dmytrenko et al., On monomial graphs of girth eight, Finite Fields Appl. (2006), doi:10.1016/j.ffa.2006.03.001

is isomorphic to Γ_3 as we showed in the proof of the congruence $k \equiv 1 \bmod (p-1)$ in Theorem 1(b). For $e \geqslant 2$, we use induction on e. To establish the base cases, we prove the theorem for $2 \leqslant e \leqslant 4$. Let $k = \sum_{i=0}^{N} k_i p^i$ be the representation of k in base p. By Theorem 2, all $0 \leqslant k_i \leqslant \frac{p-1}{4}$. Then $1 \leqslant N \leqslant 3$, and we have

$$k \equiv k_0 + \cdots + k_N \mod (p-1) \quad \text{and} \quad 1 \leqslant k_0 + \cdots + k_N \leqslant \frac{p-1}{4} N \leqslant p-1.$$

Having $1 \leqslant k \leqslant p-1$ and $k \equiv 1 \bmod (p-1)$, we conclude that $k = 1$. This proves the theorem, in particular, for $q = p^2$ and $q = p^3$.

Let $e \geqslant 6$, and the theorem holds for all exponents of the form $e' = 2^{a'}3^{b'}$, where $2 \leqslant e' < e$. We write e in the form $e = rt$ where $r \in \{2, 3\}$. Then $t = e/r$ is of the form $2^{a''}3^{b''}$, and $2 \leqslant t < e$. Then $\mathbb{F}_{p^t}$ is a proper subfield of $\mathbb{F}_{p^e}$, and G must have girth at least eight when considered as a graph over this subfield. Using the induction hypothesis, we must have $k \equiv 1 \bmod (p^t - 1)$. This implies that

$$k \equiv \sum_{i=0}^{rt-1} k_i p^{i \bmod t} \equiv 1 \mod \bigl(p^t - 1\bigr).$$

However, as all $0 \leqslant k_i \leqslant \frac{p-1}{4}$ by Theorem 2, we have

$$\sum_{i=0}^{rt-1} k_i p^{i \bmod t} \leqslant r \sum_{i=0}^{t-1} \frac{(p-1)}{4} p^i \leqslant 3\frac{(p-1)}{4} \sum_{i=0}^{t-1} p^i \leqslant \frac{3}{4}\bigl(p^t - 1\bigr).$$

Therefore $\sum_{i=0}^{rt-1} k_i p^{i \bmod t} = 1$, forcing $k = 1$.

The statement concerning all odd prime powers q such that $3 \leqslant q \leqslant 10^{10}$ was verified by using computer. The program utilized the necessary conditions on k from Theorem 1.

4. Concluding remarks

The nonexistence of girth eight graphs $G_q(xy, f_3)$ for several classes of polynomials f_3 which are not monomials, was proved in [8]. In particular, it was done in the case when f_3 is a binomial for all sufficiently large odd q. There it was also shown that in order for an s-regular bipartite graph, $s \geqslant 3$, on $2s^3$ vertices of girth eight to be extended to a generalized quadrangle of order s, it must have diameter six.

The second conjecture we would like to state concerns permutation polynomials.

Conjecture 16. *Let q be an odd prime power, $1 \leqslant k \leqslant q-1$, and p does not divide k. Then the polynomials $F(x) = ((x+1)^{2k} - 1)x^{q-1-k} - 2x^{q-1}$ and $H(x) = ((x+1)^k - x^k)x^k = (x^2 + x)^k - x^{2k}$ are permutation polynomials on $\mathbb{F}_q$ if and only if $k = 1$.*

It should be noted that this implies but is not equivalent to Conjecture 4 since the polynomials above are derived from a special class of potential 6-cycles.

Please cite this article in press as: V. Dmytrenko et al., On monomial graphs of girth eight, Finite Fields Appl. (2006), doi:10.1016/j.ffa.2006.03.001

Acknowledgments

The authors thank Qing Xiang for bringing Ref. [24] to our attention, to Misha Muzychuk for mentioning the fact given in Proposition 7(b), and to Stan Payne and Jef Thas for helpful discussions on generalized quadrangles. We thank Michael Zieve for pointing to an error in our original version of Proposition 7(a). We also thank anonymous referees whose thoughtful suggestions helped to improve our original presentation.

References

[1] C.T. Benson, Minimal regular graphs of girths eight and twelve, Canad. J. Math. 18 (1966) 1091–1094.
[2] C.T. Benson, Generalized quadrangles and (B, N) pairs, PhD thesis, Cornel University, 1965.
[3] B. Bollobás, Modern Graph Theory, Springer, New York, 1998.
[4] J.A. Bondy, Extremal problems of Paul Erdős on circuits in graphs, in: Paul Erdős and His Mathematics. II, in: Bolyai Soc. Math. Stud., vol. 11, Janos Bolyai Math. Soc., Budapest, 2002, pp. 135–156.
[5] J.A. Bondy, M. Simonovits, Cycles of even length in graphs, J. Combin. Theory Ser. B 16 (1974) 97–105.
[6] D.B. Chandler, Personal communication, August 2005.
[7] W.E. Cherowitzo, Hyperovals in Desarguesian planes: An electronic update, Informal notes, http://www-math.cudenver.edu/~wcherowi/res.html, February 2000.
[8] V. Dmytrenko, Classes of polynomial graphs, PhD thesis, University of Delaware, 2004.
[9] V. Dmytrenko, F. Lazebnik, R. Viglione, An isomorphism criterion for monomial graphs, J. Graph Theory 48 (2005) 322–328.
[10] L.E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, Ann. of Math. 11 (1–6) (1896/1897) 161–183.
[11] Z. Füredi, A. Naor, J. Verstraëte, On the Turán number for the hexagon, Adv. Math., in press.
[12] C. Hermite, Sur les fonctions de sept lettres, C. R. Math. Acad. Sci. Paris 57 (1863) 750–757.
[13] D.G. Glynn, Two new sequences of ovals in finite Desarguesian planes of even order, in: Combinatorial Mathematics, X, Adelaide, 1982, in: Lecture Notes in Math., vol. 1036, Springer, Berlin, 1983, pp. 217–229.
[14] D.G. Glynn, A condition for the existence of ovals in PG$(2, q)$, q even, Geom. Dedicata 32 (2) (1989) 247–252.
[15] D.E. Knuth, Art of Computer Programming, vol. 1, second ed., Addison–Wesley, 1973.
[16] E.E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, J. für Math. 44 (1852) 115–116.
[17] F. Lazebnik, D. Mubayi, New lower bounds for Ramsey numbers of graphs and hypergraphs, Adv. in Appl. Math. 28 (3/4) (2002) 544–559.
[18] F. Lazebnik, A. Thomason, Orthomorphisms and the construction of projective planes, Math. Comp. 73 (247) (2004) 1547–1557.
[19] F. Lazebnik, R. Viglione, An infinite series of regular edge- but not vertex-transitive graphs, J. Graph Theory 41 (2002) 249–258.
[20] F. Lazebnik, R. Viglione, On the connectivity of certain graphs of high girth, Discrete Math. 277 (2004) 309–319.
[21] F. Lazebnik, V.A. Ustimenko, New examples of graphs without small cycles and of large size, European J. Combin. 14 (5) (1993) 445–460.
[22] F. Lazebnik, A.J. Woldar, General properties of some families of graphs defined by systems of equations, J. Graph Theory 38 (2001) 65–86.
[23] R. Lidl, H. Niederreiter, Finite Fields. With a foreword by P.M. Cohn, second ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997.
[24] R. Matthews, Permutation properties of the polynomial $1 + x + \cdots + x^k$ over a finite field, Proc. Amer. Math. Soc. 120 (1) (1994) 47–51.
[25] S.E. Payne, M.F. Tinsley, On $v_1 \times v_2$ (n, s, t)-configurations, J. Combin. Theory 7 (1969) 1–14.
[26] S.E. Payne, Affine representation of generalized quadrangles, J. Algebra 51 (1970) 473–485.
[27] S.E. Payne, A census of finite generalized quadrangles, in: W.M. Kantor, R.A. Liebler, S.E. Payne, E.E. Shult (Eds.), Finite Geometries, Buildings, and Related Topics, Clarendon, Oxford, 1990, pp. 29–36.
[28] S.E. Payne, J.A. Thas, Finite Generalized Quadrangles, Res. Notes Math., vol. 110, Pitman, Boston, MA, 1984, vi+312 pp.
[29] M. Simonovits, Extremal graph theory, in: Selected Topics in Graph Theory, vol. 2, Academic Press, London, 1983, pp. 161–200.

Please cite this article in press as: V. Dmytrenko et al., On monomial graphs of girth eight, Finite Fields Appl. (2006), doi:10.1016/j.ffa.2006.03.001

[30] R. Singleton, On minimal graphs of maximum even girth, J. Combin. Theory 1 (1966) 306–332.
[31] M. Simonovits, Paul Erdős' influence on extremal graph theory, in: R.L. Graham, J. Nešetřil (Eds.), The Mathematics of Paul Erdős, vol. II, in: Algorithms Combin., vol. 14, Springer, Berlin, 1997, pp. 148–192.
[32] C. Small, Arithmetic of Finite Fields, Monogr. Textbooks Pure Appl. Math., vol. 148, Marcel Dekker, New York, 1991, xiv+216 pp.
[33] G. Turnwald, A new criterion for permutation polynomials, Finite Fields Appl. 1 (1) (1995) 64–82.
[34] V.A. Ustimenko, A linear interpretation of the flag geometries of Chevalley groups, Ukr. Mat. Zh., Kiev University 42 (3) (1990) 383–387.
[35] V.A. Ustimenko, On the embeddings of some geometries and flag systems in Lie algebras and superalgebras, in: Root Systems, Representation and Geometries, IM AN UkrSSR, Kiev, 1990, pp. 3–16.
[36] H. van Maldeghem, Generalized Polygons, Birkhäuser, Basel, 1998.
[37] R. Viglione, Properties of some algebraically defined graphs, PhD thesis, University of Delaware, 2002.
[38] R. Wenger, Extremal graphs with no C^4's, C^6's, or C^{10}'s, J. Combin. Theory Ser. B 52 (1) (1991) 113–116.

Please cite this article in press as: V. Dmytrenko et al., On monomial graphs of girth eight, Finite Fields Appl. (2006), doi:10.1016/j.ffa.2006.03.001