Monomial Graphs and Generalized Quadrangles

Brian G. Kronenthal

Department of Mathematical Sciences, Ewing Hall, University of Delaware, Newark, DE 19716, USA

Abstract

Let $\mathbb{F}_q$ be a finite field, where $q = p^e$ for some odd prime p and integer $e \geq 1$. Let $f, g \in \mathbb{F}_q[x, y]$ be monomials. The monomial graph $G_q(f, g)$ is a bipartite graph with vertex partition $P \cup L$, $P = \mathbb{F}_q^3 = L$, and $(x_1, x_2, x_3) \in P$ is adjacent to $[y_1, y_2, y_3] \in L$ if and only if $x_2 + y_2 = f(x_1, y_1)$ and $x_3 + y_3 = g(x_1, y_1)$. Dmytrenko, Lazebnik, and Williford proved in [6] that if $p \geq 5$ and $e = 2^a 3^b$ for integers $a, b \geq 0$, then all monomial graphs $G_q(f, g)$ of girth at least eight are isomorphic to $G_q(xy, xy^2)$, an induced subgraph of the point-line incidence graph of a classical generalized quadrangle of order q. In this paper, we will prove that for any integer $e \geq 1$, there exists a lower bound $p_0 = p_0(e)$ depending only on the largest prime divisor of e such that the result holds for all $p \geq p_0$. In particular, we will show that for any integers $a, b, c, d, y \geq 0$, the result holds for $p \geq 7$ with $e = 2^a 3^b 5^c$; $p \geq 11$ with $e = 2^a 3^b 5^c 7^d$; and $p \geq 13$ with $e = 2^a 3^b 5^c 7^d 11^y$.

Keywords:
Monomial Graph, Cycle, Girth eight, Generalized Quadrangle, Permutation polynomial
2010 MSC: 12E99, 51E12, 05C38

1. Introduction

We begin with some definitions. In this paper, a *graph* $\mathcal{G} = (V, E)$ consists of a finite set V of vertices and a set E of edges, where edges are two-element subsets of V. If $\{u, v\} \in E$ for some $u, v \in V$, then u and v are said to be *adjacent*. The *degree of a vertex* v is the number of vertices adjacent to v. If every $v \in V$ has degree t, then $\mathcal{G}$ is called a *t-regular graph*. A *uv-walk of length* $k \geq 1$ in $\mathcal{G}$ is a sequence $(u = v_0, e_1, v_1, e_2, v_2, ..., e_k, v_k = v)$ of alternating vertices and edges, where $e_i = \{v_{i-1}, v_i\}$ for $i = 1, ..., k$. For every vertex u, we define (u) to be a *uu-walk of length 0*. $\mathcal{G}$ is *connected* if for every pair of vertices u and v, there exists a uv-walk in $\mathcal{G}$. In a connected graph, the *distance*

Email address: kronenth@math.udel.edu (Brian G. Kronenthal)
URL: https://sites.google.com/site/bkronenthal/ (Brian G. Kronenthal)

from vertex u to vertex v is the length of a shortest uv-walk. The *diameter* of a connected graph $\mathcal{G}$ is the largest distance between any two of its vertices. A *k-cycle* is a uv-walk of length $k \geq 3$ where $u = v$, but no other vertices repeat. If $\mathcal{G}$ contains any cycles, the *girth* of $\mathcal{G}$ is the length of a shortest cycle in $\mathcal{G}$. $\mathcal{G}$ is called *bipartite* if V may be partitioned into two sets, say P and L, such that every edge $\{x, y\}$ has the property that $x \in P$ and $y \in L$ (or vice versa). Other standard graph theory definitions may be found, for example, in Bollobás [1].

Let $\mathbb{F}_q$ be a finite field of order q. A *permuation polynomial of* $\mathbb{F}_q$ is a polynomial $f \in \mathbb{F}_q[x]$ whose associated function on $\mathbb{F}_q$ that maps $a \mapsto f(a)$ is a bijection.

Now, let $f_2, ..., f_n \in \mathbb{F}_q[x, y]$ be monomials. A *monomial graph $G_q(f_2, ..., f_n)$ of dimension n* is a bipartite graph where $P = \mathbb{F}_q^n = L$, and $(x_1, x_2, ..., x_n) \in P$ is adjacent to $[y_1, y_2, ..., y_n] \in L$ if $x_i + y_i = f_i(x_1, y_1)$ for all $i = 2, 3, ..., n$. In this paper, we will focus only on the $n = 3$ case.

A central reason behind studying monomial graphs is to construct new generalized quadrangles of odd prime power order; we start with a definition.

Definition 1. *Let $s \geq 1$ and $t \geq 1$ be integers. A (finite) generalized quadrangle of order (s, t) is an incidence structure $(\mathcal{P}, \mathcal{L}, I)$ in which $\mathcal{P}$ and $\mathcal{L}$ are disjoint (nonempty) sets of objects called points and lines (respectively), and for which I is a symmetric incidence relation on $\mathcal{P} \cup \mathcal{L}$ satisfying the following axioms:*

1. *Each point is incident with t+1 lines and two distinct points are incident with at most one line.*
2. *Each line is incident with s+1 lines and two distinct lines are incident with at most one point.*
3. *If P is a point and l is a line not incident with P, then there is a unique pair $(Q, m) \in \mathcal{P} \times \mathcal{L}$ for which $PImIQIl$.*

For information on generalized quadrangles, see Payne and Thas [15] or Van Maldeghem [13], for example. In this paper, we will be interested in the case $s = t \geq 2$; we will therefore use the notation $GQ(t)$ in place of $GQ(t, t)$, and say "order t" instead of "order (t, t)".

No $GQ(t)$ of non-prime power order are known. When t is a power of 2, many examples of nonisomorphic generalized quadrangles are known. However, for a given odd prime power t, only two nonisomorphic generalized quadrangles are known. These classical examples are usually denoted by $Q_4(t)$ and $W(t)$, and are dual to each other.

From now on, instead of using the geometric perspective from Definition 1, we will consider the corresponding point-line incidence graphs, often called Levi graphs, of these geometries. As a graph, $GQ(t)$ is a bipartite $(t + 1)$-regular graph with diameter 4 and girth 8; the two sets of the vertex partition of $GQ(t)$ each contain $t^3 + t^2 + t + 1$ vertices. Since $Q_4(t)$ and $W(t)$ are dual, their incidence graphs are isomorphic; thus, from a graph theoretical perspective, only one $GQ(t)$ of odd prime power order is known (up to graph isomorphism).

The primary motivation for this paper, as well as for Dmytrenko, Lazebnik, and Williford in [6], was to construct a new $GQ(t)$ of odd prime power order.

Let q be an odd prime power. Consider an edge $\{u, v\}$ of $GQ(q)$, and let $\mathcal{T}$ be the subgraph of $GQ(q)$ induced by the set of all vertices at a distance at most two from u or v. As the girth of $GQ(q)$ is eight, $\mathcal{T}$ is a tree (a connected graph with no cycles) on $2(q^2 + q + 1)$ vertices. It turns out that the graph obtained from the classical $GQ(q)$ by removing $\mathcal{T}$ is isomorphic to the monomial graph $\Gamma_3(q) := G_q(xy, xy^2)$; for a proof, see Dmytrenko [5]. This suggests a reasonable strategy for constructing a new generalized quadrangle of odd order. First, construct a q-regular girth eight graph that is not isomorphic to $\Gamma_3(q)$, and has vertex partition $P \cup L$ such that $|P| = q^3 = |L|$. Second, "attach" (an isomorphic copy of) $\mathcal{T}$ to it. The viability of the first step was investigated in [6], where it was conjectured that the strategy fails because a suitable monomial graph does not exist:

Conjecture 2. *[6] Let $q = p^e$ be an odd prime power. Then every monomial graph over $\mathbb{F}_q$ of girth at least eight is isomorphic to $\Gamma_3(q)$.*

This conjecture is of particular interest because it stands in stark contrast to the case when q is a power of 2. As explained in [6], "there are examples of monomial graphs of girth eight which do lead to nonisomorphic quadrangles," and so the described strategy of constructing new generalized quadrangles succeeds in this case. See Payne [14], [13], and Cherowitzo [3] for additional information.

To address Conjecture 2, the following result was proven in [6]:

Theorem 3. *[6] Let $q = p^e$ be an odd prime power, with $p \geq 5$ and $e = 2^a 3^b$ for integers $a, b \geq 0$. Then every monomial graph over $\mathbb{F}_q$ of girth at least eight is isomorphic to $\Gamma_3(q)$ and has girth eight. Furthermore, for $3 \leq q \leq 10^{10}$, every monomial graph over $\mathbb{F}_q$ nonisomorphic to $\Gamma_3(q)$ has girth at most six.*

The purpose of this paper is to extend the results of Theorem 3 towards Conjecture 2. Our main result is the following theorem:

Theorem 4. *Let $q = p^e$ be an odd prime power, with:*

1. *$p \geq p_0$, a lower bound that depends only on the largest prime divisor of e.*

In particular, suppose:

2. *$e = 2^a 3^b 5^c$ for integers $a, b, c \geq 0$ and $p \geq 7$,*
3. *$e = 2^a 3^b 5^c 7^d$ for integers $a, b, c, d \geq 0$ and $p \geq 11$, or*
4. *$e = 2^a 3^b 5^c 7^d 11^y$ for integers $a, b, c, d, y \geq 0$ and $p \geq 13$.*

Then every monomial graph over $\mathbb{F}_q$ of girth at least eight is isomorphic to $\Gamma_3(q)$, and hence has girth exactly eight.

Theorem 4 implies that if $q = p^e$ for any noted combination of p and e, it is impossible to construct a new $GQ(q)$ using the strategy explained above. This result severely limits the cases in which the described construction could potentially succeed.

To prove Theorem 4, we will make use of several results. Before presenting them, a bit of notation is necessary. Let $(k_0, k_1, ..., k_n)_p$ denote the *base p representation of k*; in other words, $k = (k_0, k_1, ..., k_n)_p$ if $k = \sum_{i=0}^{n} k_i p^i$ with integers k_i such that $0 \leq k_i \leq p - 1$ for all $i = 0, 1, ..., n$.

Theorem 5 (Kummer's Theorem [10]; see also Knuth [9]). *A prime p divides $\binom{r}{s}$ exactly n times if and only if adding s and $r-s$ in base p produces exactly n carries.*

Theorem 6 (Lucas' Theorem [12]; see also Granville [7]). *Let p be prime, $r = (r_0, r_1, ..., r_n)_p$ and $s = (s_0, s_1, ..., s_n)_p$. Then $\binom{r}{s} \equiv \binom{r_0}{s_0}\binom{r_1}{s_1}\cdots\binom{r_n}{s_n} \pmod{p}$.*

Theorem 7 (Hermite-Dickson criterion; proven by Hermite [8] and Dickson [4]; see also Lidl/Niederreiter [11]). *Let $\mathbb{F}_q$ be of characteristic p. Then $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following two conditions hold:*

1. *f has exactly one root in $\mathbb{F}_q$;*
2. *for each integer t with $1 \leq t \leq q-2$ and $p \nmid t$, the reduction of $f^t \pmod{x^q - x}$ has degree at most $q-2$.*

The Hermite-Dickson criteria is commonly stated in this form because in order to prove that $f \in \mathbb{F}_q[x]$ is a permutation polynomial, it is convenient to check only those t such that $p \nmid t$. However, it is noted in [11] that given a permutation polynomial $f \in \mathbb{F}_q[x]$, the reduction of $f^t \pmod{x^q - x}$ has degree at most $q-2$ for all integers t with $1 \leq t \leq q-2$; the condition $p \nmid t$ is not required. It is for this reason that we will not be concerned with the condition $p \nmid t$ in this paper.

Finally, we will need the following results from [6]:

Theorem 8. *Let $q = p^e$ be an odd prime power. Then every monomial graph of girth at least eight is isomorphic to the graph $G_q(xy, x^k y^{2k})$, where k is not divisible by p. If $q \geq 5$, the following statements also hold:*

1. *$1 \leq k < \frac{q-1}{2}$, $\gcd(k, q-1) = 1$, and $k \equiv 1 \pmod{p-1}$.*
2. *$((x+1)^{2k} - 1)x^{q-1-k} - 2x^{q-1} \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$.*

We will now discuss how the remainder of this paper is structured. In section 2, we will use the Hermite-Dickson criterion to derive a system of congruences. We will use these congruences in section 3 to prove upper bounds on the base p digits of k. Finally, these bounds will be used in section 4 to prove Theorem 4.

2. The Congruences

Let $e \geq 1$ be an integer, p an odd prime, and $q = p^e$. Let G be a monomial graph of girth at least eight. Then by Theorem 8, G is isomorphic to $G_q(xy, x^k y^{2k})$ where

$$F = ((x+1)^{2k} - 1)x^{q-1-k} - 2x^{q-1} \ \in \ \mathbb{F}_q[x]$$

is a permutation polynomial of $\mathbb{F}_q$. The Hermite-Dickson criterion implies that the coefficient of x^{q-1} in $F^t \pmod{x^q - x}$ must be zero. We will therefore examine F^t:

$$
\begin{aligned}
F^t &= \left[\left((x+1)^{2k}-1\right)x^{q-1-k} - 2x^{q-1}\right]^t \\
&= \sum_{j=0}^{t}\binom{t}{j}\left((x+1)^{2k}-1\right)^{t-j}x^{(t-j)(q-1-k)}(-1)^j 2^j x^{j(q-1)} \\
&= \sum_{j=0}^{t}(-1)^j 2^j\binom{t}{j}\left((x+1)^{2k}-1\right)^{t-j}x^{-(t-j)k+t(q-1)} \\
&= \sum_{j=0}^{t}(-1)^j 2^j\binom{t}{j}\left(\sum_{h=0}^{t-j}\binom{t-j}{h}(x+1)^{2k(t-j-h)}(-1)^h\right)x^{-(t-j)k+t(q-1)} \\
&= \sum_{j=0}^{t}\sum_{h=0}^{t-j}(-1)^{j+h}2^j\binom{t-j}{h}\binom{t}{j}\sum_{i=0}^{2k(t-j-h)}\binom{2k(t-j-h)}{i}x^{i-(t-j)k+t(q-1)} \qquad (1)
\end{aligned}
$$

To determine the coefficient of x^{q-1}, we note that $x^{i-(t-j)k+t(q-1)} \equiv x^{q-1} \pmod{x^q-x}$ if and only if $i-(t-j)k+t(q-1) \in \{q-1, 2(q-1), 3(q-1), ...\}$, which occurs if and only if $i-(t-j)k \in \{(1-t)(q-1), (2-t)(q-1), (3-t)(q-1), ...\}$. As $0 \le i \le 2k(t-j-h)$ and $1 \le k < \frac{q-1}{2}$, we have the following bounds on $i-(t-j)k$:

$$-(t-j)k \le i-(t-j)k \le k(t-j)-2kh = k(t-j-2h) < \frac{t-j-2h}{2}(q-1)$$

Now, $i-(t-j)k$ satisfies one of the following conditions:

1. $i-(t-j)k = (a-t)(q-1)$ for some positive integer $a < t$ with $t \neq j$. Since $0 \le i = (t-j)k + (a-t)(q-1)$, we have $k \ge \frac{(t-a)(q-1)}{t-j} \ge \frac{q-1}{t}$ (as $t-a > 0$ and $0 \le j < t$).
2. $i-(t-j)k = (a-t)(q-1)$ for some positive integer $a > t$ with $t \neq j$. Since $2k(t-j)-2kh = 2k(t-j-h) \ge i = (t-j)k + (a-t)(q-1)$, we have $(t-j)k \ge 2kh + (a-t)(q-1)$, and so $k \ge \frac{(a-t)(q-1)}{t-j-2h} \ge \frac{q-1}{t}$ (this uses $a-t > 0$; in addition, $0 < (a-t)(q-1) = i-(t-j)k < \frac{t-j-2h}{2}(q-1)$ implies that $t-j-2h > 0$).
3. $i-(t-j)k = 0$ (i.e. $a = t$) Since $i-(t-j)k \le k(t-j-2h)$, this case requires $t-j-2h \ge 0$ $\left(\text{so } h \le \frac{t-j}{2}\right)$, but there are no additional restrictions on k.
4. If $j = t$, then $-(t-j)k \le i-(t-j)k \le k(t-j)-2kh$ implies $i = 0$. Therefore, $i = 0 = (t-j)k$, which was accounted for in case 3.

This proves that if we assume $k < \frac{q-1}{t}$, we need only consider case 3 terms. Therefore, we will proceed under this assumption (in fact, we will show in the proof of Proposition 10 that all k relevant to Theorem 4 satisfy this bound). Substituting $i = (t-j)k$ into (1) yields the coefficient of x^{q-1} in $F^t \pmod{x^q-x}$; as this coefficient must be zero by Hermite-Dickson, we have:

$$\sum_{j=0}^{t}(-1)^j 2^j \binom{t}{j} \sum_{h=0}^{\lfloor \frac{t-j}{2} \rfloor}(-1)^h \binom{t-j}{h}\binom{2k(t-j-h)}{k(t-j)} \equiv 0 \pmod{p}. \quad (2)$$

We will now evaluate (2) for some small values of t; the result will be a sequence of congruences. We will use (κ_i) to denote the congruence resulting from the substitution $t = i$; congruence (κ_i) must be satisfied whenever $G_q(xy, x^k y^{2k})$ has girth at least eight and $k < \frac{q-1}{i}$. The system of congruences will later be used to determine which k meet these criteria. When $t = 1$, (2) yields $-2 + \binom{2k}{k} \equiv 0 \pmod{p}$, and so

$$\binom{2k}{k} \equiv 2 \pmod{p}. \quad (\kappa_1)$$

When $t = 2$, we have $2 - 4\binom{2k}{k} + \binom{4k}{2k} \equiv 0 \pmod{p}$; substituting (κ_1) implies $2 - 4 \cdot 2 + \binom{4k}{2k} \equiv 0 \pmod{p}$, and therefore

$$\binom{4k}{2k} \equiv 6 \pmod{p}. \quad (\kappa_2)$$

Continuing this process of evaluating (2) for subsequent values of t, and substituting previous congruences where possible, yields the following:

$$\binom{8k}{4k} - 4\binom{6k}{4k} \equiv 10 \pmod{p} \quad (\kappa_4)$$

$$\binom{12k}{6k} - 6\binom{10k}{6k} + 15\binom{8k}{6k} \equiv 84 \pmod{p} \quad (\kappa_6)$$

$$\binom{16k}{8k} - 8\binom{14k}{8k} + 28\binom{12k}{8k} - 56\binom{10k}{8k} \equiv 186 \pmod{p} \quad (\kappa_8)$$

$$\binom{20k}{10k} - 10\binom{18k}{10k} + 45\binom{16k}{10k} - 120\binom{14k}{10k} + 210\binom{12k}{10k} \equiv 1276 \pmod{p} \quad (\kappa_{10})$$

In general, it is clear from (2) that

$$\sum_{h=0}^{\lfloor \frac{2s-1}{2} \rfloor}(-1)^h \binom{2s}{h}\binom{2k(2s-h)}{2ks} \equiv b_{2s} \pmod{p} \quad (\kappa_{2s})$$

for some integer b_{2s}.

The reader should note that (κ_3), (κ_5), (κ_7), and (κ_9) were omitted from the above list because they will not be needed in this paper. However, they were used to derive the above list of congruences. Furthermore, it can be proven that $b_{2s} = 2^{2s} - (-1)^s\binom{2s}{s}$ (and that $b_{2s+1} = 2^{2s+1}$); the proof is straightforward

(although technical), and is available on the author's webpage. Note that this implies $b_{2s} > 0$ for all integers $s > 0$. Finally, we remind the reader that (κ_t) has only been proven to hold when $k < \frac{q-1}{t}$.

3. The Base p Digits of k

The proof of Theorem 4 will rely heavily on the base p representation of k. Therefore, we will start by limiting the base p digits that can appear in that representation. Let $e \geq 1$ be an integer, p be an odd prime, and $q = p^e$. Assume that $G_q(xy, x^k y^{2k})$ has girth at least eight. Recall that we may use (κ_t) if and only if $k < \frac{q-1}{t}$. Before proving our main result, we will need a lemma:

Lemma 9. *Let $q = p^e$ be an odd prime power. Assume the graph $G_q(xy, x^k y^{2k})$ has girth at least eight, where $1 \leq k < \frac{q-1}{2}$.*

1. *If $p = 3$, then all base p digits of k are at most 1.*
2. *If $p \geq 5$, then all base p digits of k are at most $\frac{p-1}{4}$.*

Proof. Recall the base p notation $k = (k_0, ..., k_n)_p$ if $k = \sum_{i=0}^{n} k_i p^i$ with integers k_i such that $0 \leq k_i \leq p-1$ for all $i = 0, 1, ..., n$.

1. Let $p = 3$. Consider (κ_1); as $3 \nmid 2$, we know $3 \nmid \binom{2k}{k}$. By Kummer's Theorem, there are no carries when k and $2k - k = k$ are added in base p. Therefore, $0 \leq 2k_i \leq p - 1 = 2$, and so $0 \leq k_i \leq 1$.
2. This is Theorem 2 of [6]. □

Proposition 10. *Let $e, z \geq 1$ be integers. Then there exists prime p_z such that for all primes $p \geq p_z$, the following statement holds:*

> *If $q = p^e$, $1 \leq k < \frac{q-1}{2}$, and $G_q(xy, x^k y^{2k})$ has girth at least eight, then all base p digits of k are at most $\frac{p-1}{2z}$.*

Proof. We proceed by induction on z. When $z = 1$, the result follows from Lemma 9 with $p_1 = 3$. When $z = 2$, the result follows from part 2 of Lemma 9 with $p_2 = 5$. Now, assume that for some fixed integer $z \geq 1$, the result holds for all v with $2 \leq v < z$.

First, we will show that $1 \leq k \leq \frac{q-1}{2(z-1)}$. If not, $k > \frac{q-1}{2(z-1)}$. Then $k < q - 1 < 2(z-1)k$. Let $k = (k_0, k_1, ..., k_n)_p$. By the induction hypothesis, each $k_i \leq \frac{p-1}{2(z-1)}$; so $2(z-1)k = (2(z-1)k_0, 2(z-1)k_1, \ldots, 2(z-1)k_n)_p$. Furthermore, $k < q - 1 < 2(z-1)k$ implies that $q-1$ has at least as many base p digits as k, but no more than $2(z-1)k$ does. As k and $2(z-1)k$ each have $n+1$ base p digits, $q-1 = p^e - 1$ must also have $n+1$ digits. So $n+1 = e$. Since $q-1$ is the largest number with e base p digits, this contradicts $q-1 < 2(z-1)k$. Hence, $k \leq \frac{q-1}{2(z-1)}$. Furthermore, equality would imply $2(z-1)k = q-1$, and so $k|(q-1)$. This means $k = \gcd(k, q-1)$, which contradicts part 1 of Theorem

8 unless $k = 1$ and $q = 2z - 1$. Thus, we conclude that equality cannot occur for $p > 2z - 1$; so $1 \leq k < \frac{q-1}{2(z-1)}$ for all $p > 2z - 1$.

Let $p > 2z - 1$. Since $1 \leq k < \frac{q-1}{2(z-1)}$, the congruence $(\kappa_{2(z-1)})$ applies:

$$\binom{(4z-4)k}{2(z-1)k} + a_1\binom{(4z-6)k}{2(z-1)k} + a_2\binom{(4z-8)k}{2(z-1)k} + \ldots$$
$$+ a_{z-3}\binom{(2z+2)k}{2(z-1)k} + a_{z-2}\binom{(2z)k}{2(z-1)k} \equiv b_{2(z-1)} \pmod{p},$$

where $a_i = (-1)^i\binom{2(z-1)}{i}$ and $b_{2(z-1)} > 0$ is a positive integer. Define p'_z to be the largest prime that divides b_2, b_4, $b_6, \ldots,$ or $b_{2(z-1)}$, and suppose

$$p \geq p_z := \min\{p | p \text{ is prime, } p > p'_z, \text{ and } p > 2z - 1\}.$$

Note that p'_z is well-defined because every $b_{2s} \neq 0$. Since $p \nmid b_{2(z-1)}$, p cannot divide every binomial coefficient on the left-hand side of $(\kappa_{2(z-1)})$.

As we will show below, the cases $p \nmid \binom{(4z-4)k}{2(z-1)k}$, $p \nmid \binom{(4z-6)k}{2(z-1)k}$, $\ldots$, $p \nmid \binom{(2z+2)k}{2(z-1)k}$, and $p \nmid \binom{2zk}{2(z-1)k}$ imply the upper bounds $0 \leq k_i \leq \frac{p-1}{4z-4}$, $0 \leq k_i \leq \frac{p-1}{4z-6}$, $\ldots$, $0 \leq k_i \leq \frac{p-1}{2z+2}$, and $0 \leq k_i \leq \frac{p-1}{2z}$, respectively. At least one of these cases must hold, and so $0 \leq k_i \leq \frac{p-1}{2z}$, as claimed.

We will now illustrate how to derive the bound implied by the case $p \nmid \binom{2zk}{2(z-1)k}$; the others may be proven similarly. By Kummer's Theorem, $p \nmid \binom{2zk}{2(z-1)k}$ implies that there are no carries when $2(z-1)k$ and $2zk-2(z-1)k = 2k$ are added in base p. Since the induction hypothesis implies that the base p digits of k are at most $\frac{p-1}{2(z-1)}$, $2(z-1)k = (2(z-1)k_0, 2(z-1)k_1, \ldots, 2(z-1)k_n)_p$ and $2k = (2k_0, 2k_1, \ldots, 2k_n)_p$. Thus, $0 \leq 2(z-1)k_i + 2k_i \leq p - 1$ for all i, and so $0 \leq k_i \leq \frac{p-1}{2z}$. □

Note that in the above proof, we excluded more primes than was necessary. Specifically, the argument holds for all primes $p > 2z - 1$ that do not divide b_2, b_4, $b_6, \ldots,$ or $b_{2(z-1)}$. We will now apply the Proposition 10 (and this fact) to some small values of z to obtain the following corollary:

Corollary 11. *Let $q = p^e$ be an odd prime power. Assume the graph $G_q(xy, x^k y^{2k})$ has girth at least eight, where $1 \leq k < \frac{q-1}{2}$.*

1. *If $p \geq 7$, then all base p digits of k are at most $\frac{p-1}{6}$.*
2. *If $p \geq 11$, then all base p digits of k are at most $\frac{p-1}{10}$.*
3. *If $p \geq 13$, then all base p digits of k are at most* $\begin{cases} 3 & \text{if } p = 31 \\ \frac{p-1}{12} & \text{else.} \end{cases}$

Proof.

1. When $z = 3$, $p'_3 = 5 = 2z - 1$ is the largest prime factor of b_2 or b_4; so $k_i \leq \frac{p-1}{6}$ for all $p \geq p_3 = 7$.

2. When $z = 4$, $7|84$ implies that $p'_4 = 7 = 2z-1$, and so $p_4 = 11$. Therefore, $k_i \leq \frac{p-1}{8}$ for all $p \geq p_4 = 11$. When $z = 5$, $p'_5 = 31 > 9 = 2z-1$, and so $p_5 = 37$; however, the only prime $p \geq 11$ dividing b_2, b_4, b_6, or b_8 is $p = 31$. Therefore, $k_i \leq \frac{p-1}{10}$ for all $p \geq p_5 = 11$ except for $p = 31$, in which case $k_i \leq \left\lfloor \frac{31-1}{8} \right\rfloor = 3$. The result holds because $\left\lfloor \frac{31-1}{10} \right\rfloor = 3$ as well.
3. Let $z = 6$. As $1276 = 2^2 \cdot 11 \cdot 29$, $k_i \leq \frac{p-1}{12}$ for all $p \geq 13$ except for $p = 29$ and $p = 31$. When $p = 29$, $k_i \leq \left\lfloor \frac{29-1}{10} \right\rfloor = 2 = \left\lfloor \frac{29-1}{12} \right\rfloor$. As in case 2 above, $p = 31$ implies that $k_i \leq \left\lfloor \frac{31-1}{8} \right\rfloor = 3$. □

4. Proof of Theorem 4

In the remainder of this paper, we prove Theorem 4 by adapting the proof (from [6]) of Theorem 3. First, we must prove Proposition 12, which will use the notation p_z that was introduced in Proposition 10.

Proposition 12. *Let $e > 1$ be an integer; denote the largest prime divisor of e by ϕ. Assume $p \geq p_{\frac{\phi+1}{2}}$, let $q = p^e$, and let $1 \leq k < \frac{q-1}{2}$. If $G = G_q(xy, x^k y^{2k})$ has girth at least eight and $p \nmid k$, then $k \equiv 1 \pmod{q-1}$, and so $k = 1$.*

As can be seen in the following proof, the condition "$p \geq p_{\frac{\phi+1}{2}}$" may be replaced by the more general condition that "all base p digits of k are at most $\frac{p-1}{\phi+1}$." However, we use "$p \geq p_{\frac{\phi+1}{2}}$" to emphasize that for a given e, the proposition holds for all but finitely many p.

Proof. Let $q = p^e$ be an odd prime power with $p \geq p_{\frac{\phi+1}{2}}$. Suppose $1 \leq k < \frac{q-1}{2}$, and let $k = \sum_{i=0}^{N} k_i p^i$. We proceed by induction on e. If e is prime, then $N < \phi$. Furthermore, the assumption that $p \geq p_{\frac{\phi+1}{2}}$ implies that all base p digits of k are at most $\frac{p-1}{\phi+1}$. Therefore,

$$1 \leq k_0 + ... + k_N \leq \frac{p-1}{\phi+1}(N+1) \leq p-1.$$

Since it is also true that $1 \equiv k \equiv k_0 + ... + k_N \pmod{p-1}$, this forces $k_0 + ... + k_N = 1$. Thus, $p \nmid k$ implies $k = 1$.

Now, assume that for some integer $e \geq 1$, the result holds for all integers e' with $2 \leq e' < e$. Define $e = rt$ for some prime divisor r of e; note that $r \leq \phi$. Since $t|e$, $\mathbb{F}_{p^t}$ is a proper subfield of $\mathbb{F}_{p^e}$. Therefore, since G has girth at least eight over $\mathbb{F}_{p^e}$, G must also have girth at least 8 over the subfield $\mathbb{F}_{p^t}$. Thus, our induction hypothesis states that $k \equiv 1 \pmod{p^t - 1}$. This implies that

$$1 \equiv k \equiv \sum_{i=0}^{rt-1} k_i p^{i \bmod t} \pmod{p^t - 1}. \tag{3}$$

Furthermore,

$$\sum_{i=0}^{rt-1} k_i p^{i \bmod t} \leq \sum_{i=0}^{rt-1} \left(\frac{p-1}{\phi+1}\right) p^{i \bmod t} \leq r \sum_{i=0}^{t-1} \left(\frac{p-1}{\phi+1}\right) p^i$$
$$\leq \frac{\phi}{\phi+1}(p-1) \sum_{i=0}^{t-1} p^i = \frac{\phi}{\phi+1}(p-1)\left(\frac{p^t-1}{p-1}\right)$$
$$= \frac{\phi}{\phi+1}(p^t-1) < p^t - 1.$$

Along with equation (3), this inequality implies that $\sum_{i=0}^{rt-1} k_i p^{i \bmod t} = 1$. Since $p \nmid k$, we conclude $k = 1$, as desired. □

Proposition 12 implies the following result:

Corollary 13. *Let $q = p^e$ be an odd prime power with:*

1. *$p \geq 7$ and $1 < e = 2^a 3^b 5^c$ for integers $a, b, c \geq 0$, or*
2. *$p \geq 11$ and $1 < e = 2^a 3^b 5^c 7^d$ for integers $a, b, c, d \geq 0$, or*
3. *$p \geq 13$ and $1 < e = 2^a 3^b 5^c 7^d 11^y$ for integers $a, b, c, d, y \geq 0$.*

Furthermore, suppose $1 \leq k < \frac{q-1}{2}$. If $G = G_q(xy, x^k y^{2k})$ has girth at least eight and $p \nmid k$, then $k \equiv 1 \pmod{q-1}$, and so $k = 1$.

Proof. We showed in the proof of Corollary 11 that when $\phi = 5$, $p_3 = 7$, and that when $\phi = 7$, $p_4 = 11$. Therefore, Proposition 12 implies parts 1 and 2 of this corollary.

We now prove part 3. When $\phi = 11$, Corollary 11 implies that the base p digits of k are at most $\frac{p-1}{12}$ for all $p \geq 13$, $p \neq 31$. Therefore, Proposition 12 implies this result for those primes. We must account for the $p = 31$ case separately.

Let $q = 31^e$ with $1 < e = 2^a 3^b 5^c 7^d 11^y$ for integers $a, b, c, d, y \geq 0$. Suppose $1 \leq k < \frac{q-1}{2}$ and let $k = \sum_{i=0}^{N} k_i 31^i$. We proceed by induction on e. If $e \in \{2, 3, 5, 7, 11\}$, then $N < 11$. Furthermore, all base 31 digits of k are at most 3. Therefore,

$$1 \leq k_0 + ... + k_N \leq 3(N+1) \leq 33.$$

Since it is also true that $1 \equiv k \equiv k_0 + ... + k_N \pmod{30}$, this forces $k_0 + ... + k_N = 1$ or 31. If $k_0 + ... + k_N = 1$, then $31 \nmid k$ implies $k = 1$, as desired. If instead $k_0 + ... + k_N = 31$, $N < 11$ allows only two possibilities:

1. $N = 10$, there exist distinct i, j such that $k_i = k_j = 2$, and $k_h = 3$ for all $h \neq i$, $h \neq j$. This case is impossible because by Lucas' Theorem,

$$\binom{2k}{k} \equiv \binom{6}{3}^9 \binom{4}{2}^2 \equiv 9 \not\equiv 2 \pmod{31},$$

which violates (κ_1).

2. $N = 10$, there exists i such that $k_i = 1$, and $k_h = 3$ for all $h \neq i$. This case is impossible because by Lucas' Theorem,

$$\binom{2k}{k} \equiv \binom{6}{3}^{10}\binom{2}{1} \equiv 10 \not\equiv 2 \pmod{31},$$

which again violates (κ_1).

Therefore, $k_0 + ... + k_N = 1$, and so $k = 1$.

Now, assume that the result holds for all $e' = 2^{a'}3^{b'}5^{c'}7^{d'}11^{y'}$ with a', b', c', d', y' non-negative integers and $2 \leq e' < e$. Define $e = rt$ where $r \in \{2, 3, 5, 7, 11\}$. Then $t = \frac{e}{r} = 2^{a''}3^{b''}5^{c''}7^{d''}11^{y''}$ for some non-negative integers a'', b'', c'', d'', y''. Since $t|e$, $\mathbb{F}_{31^t}$ is a proper subfield of $\mathbb{F}_{31^e}$. Therefore, since G has girth at least 8 over $\mathbb{F}_{31^e}$, G must also have girth at least 8 over the subfield $\mathbb{F}_{31^t}$. Thus, our induction hypothesis states that $k \equiv 1 \pmod{31^t - 1}$. This implies that

$$1 \equiv k \equiv \sum_{i=0}^{rt-1} k_i 31^{i \bmod t} \pmod{31^t - 1}. \tag{4}$$

Furthermore,

$$\sum_{i=0}^{rt-1} k_i 31^{i \bmod t} \leq \sum_{i=0}^{rt-1} 3 \cdot 31^{i \bmod t} \leq 3r \sum_{i=0}^{t-1} 31^i \leq 33\left(\frac{31^t - 1}{31 - 1}\right) = \frac{33}{30}(31^t - 1).$$

Along with equation (4), this inequality implies that $\sum_{i=0}^{rt-1} k_i 31^{i \bmod t} = 1$ or 31^t. Assume to the contrary that $\sum_{i=0}^{rt-1} k_i 31^{i \bmod t} = 31^t$. Note that there exists a smallest integer $j \geq 0$ such that $k_j = 3$. Indeed, if $k_i \leq 2$ for all $i = 0, 1, ..., rt - 1$, then

$$31^t = \sum_{i=0}^{rt-1} k_i 31^{i \bmod t} \leq 2r \sum_{i=0}^{t-1} 31^i \leq 22\left(\frac{31^t - 1}{30}\right) = \frac{22}{30}(31^t - 1) < 31^t - 1,$$

a contradiction. Now, (κ_8) must be satisfied when $p = 31$ because Proposition 10 implies that $k < \frac{q-1}{8}$ for all $p \geq 11$. To see this, we follow results of Proposition 10 as z increases:

- $0 \leq k_i \leq \frac{p-1}{4}(z = 2)$ and $1 \leq k < \frac{q-1}{4}(z = 3)$ for $p \geq 5$
- $0 \leq k_i \leq \frac{p-1}{6}(z = 3)$ and $1 \leq k < \frac{q-1}{6}(z = 4)$ for $p \geq 7$
- $0 \leq k_i \leq \frac{p-1}{8}(z = 4)$ and $1 \leq k < \frac{q-1}{8}(z = 5)$ for $p \geq 11$

Thus,
$16k = (16k_0, ..., 16k_{j-1}, 17, ...)_{31}$,
$14k = (14k_0, ..., 14k_{j-1}, 11, ...)_{31}$,
$12k = (12k_0, ..., 12k_{j-1}, 5, ...)_{31}$,

$10k = (10k_0, ..., 10k_{j-1}, 30, 10k_{j+1}, ..., 10k_{rt-1})_{31}$,
$8k = (8k_0, ..., 8k_{j-1}, 24, 8k_{j+1}, ..., 8k_{rt-1})_{31}$, and so by Lucas' Theorem,

$$\begin{aligned}
0 &\equiv 186 \\
&\equiv \binom{16k}{8k} - 8\binom{14k}{8k} + 28\binom{12k}{8k} - 56\binom{10k}{8k} \\
&\equiv \binom{16k_0}{8k_0} \cdots \binom{16k_{j-1}}{8k_{j-1}} \binom{17}{24} \cdots - 8\binom{14k_0}{8k_0} \cdots \binom{14k_{j-1}}{8k_{j-1}} \binom{11}{24} \cdots \\
&\quad + \ 28\binom{12k_0}{8k_0} \cdots \binom{12k_{j-1}}{8k_{j-1}} \binom{5}{24} \cdots - 56\binom{10k}{8k} \\
&\equiv -56\binom{10k}{8k} \pmod{31}
\end{aligned}$$

Therefore, $\binom{10k}{8k} \equiv 0 \pmod{31}$, which is impossible by Lucas' Theorem since all base 31 digits of k are at most 3. Thus, we must have $\sum_{i=0}^{rt-1} k_i 31^{i \bmod t} = 1$, and therefore the desired result of $k = 1$. □

Proof (of Theorem 4). The $e = 1$ case was addressed in the proof of Theorem 1b in [6]. Therefore, we need only consider $e > 1$. It was shown in [6] that every monomial graph of girth at least eight is isomorphic to a graph $G = G_q(xy, x^k y^{2k})$. Proposition 12 shows that in fact $G = \Gamma_3(q)$, which proves part 1 of Theorem 4. Parts 2, 3, and 4 follow by using similar reasoning, except that $G = \Gamma_3(q)$ is proven by parts 1, 2, and 3 of Corollary 13, respectively. □

5. Concluding Remarks

It is of interest that some results in the previous section hold for additional k under certain conditions. Specifically:

1. Part 1 of Corollary 13 and part 2 of Theorem 4 hold for $p = 5$ with $k < \frac{q-1}{8}$.
2. Part 2 of Corollary 13 and part 3 of Theorem 4 hold for $p = 5$ with $k < \frac{q-1}{8}$, and for $p = 7$ with $k < \frac{q-1}{12}$.
3. Part 3 of Corollary 13 and part 4 of Theorem 4 hold for $p = 7$ with $k < \frac{q-1}{12}$, and for $p = 11$ with $k < \frac{q-1}{20}$.

The possibility of removing the bound on k for each of these three cases is the subject of ongoing research. Another avenue for improving Theorem 4 would be to find a more explicit form for p_z. However, the techniques in this paper require certain primes to either be handled separately (as was done for $p = 31$ in Corollary 13), or excluded. We are uncertain whether a more effective technique exists.

We would also like to note that an alternate strategy for proving Conjecture 2 is to instead prove the following conjecture:

Conjecture 14. *[6] Let q be an odd prime power, $1 \leq k \leq q-1$, and $p \nmid k$. Then $F = ((x+1)^{2k} - 1)x^{q-1-k} - 2x^{q-1} \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $k = 1$.*

Indeed, suppose Conjecture 14 is true. Then either $k = p^a$ and F is a permutation polynomial, or $k \neq p^a$ and F is not a permutation polynomial. In the first case, $k = p^a$ implies that Conjecture 2 follows from the isomorphism

$$\Gamma_3(q) \to G_q(xy, x^{p^a} y^{2p^a})$$

with $(p_1, p_2, p_3) \mapsto \left(p_1, p_2, p_3^{p^a}\right)$ and $[l_1, l_2, l_3] \mapsto \left[l_1, l_2, l_3^{p^a}\right]$. In the second case, the fact that F is not a permutation polynomial means that $G_q(xy, x^k y^{2k})$ contains a 6-cycle; so Conjecture 2 holds vacuously.

Furthermore, it was shown in [6] that if $G_q(xy, x^k y^{2k})$ has girth at most 8, then $G = ((x+1)^k - x^k)x^k = (x^2+x)^k - x^{2k} \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$. Therefore, the above argument also holds when F is replaced by G in Conjecture 14.

Acknowledgements

The author thanks Felix Lazebnik for his invaluable assistance, both with the preparation of this paper and with the research of the results presented. In addition, thanks to Gary Ebert and Eric Moorehouse for their suggestions regarding the program Magma; Bryan Petrak for a variety of useful discussions; and the referees for comments that helped to improve the original version of this paper.

References

[1] B. Bollobás, Modern Graph Theory, Springer, New York, 1998.

[2] P.J. Cameron, Combinatorics: Topics, Techniques, Algorithms, Cambridge University Press, New York, 1994.

[3] W.E. Cherowitzo, Hyperovals in Desarguesian Planes: An Electronic Update, Informal notes, http://math.ucdenver.edu/∼wcherowi/research/hyperoval/hypero.html

[4] 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.

[5] V. Dmytrenko, Classes of polynomial graphs, PhD thesis, University of Delaware, 2004.

[6] V. Dmytrenko, F. Lazebnik, and J. Williford, On monomial graphs of girth eight, Finite Fields and Their Applications 13 (2007) 828-842.

[7] A. Granville, Arithmetic Properties of Binomial Coefficients I: Binomial coefficients modulo prime powers, Canadian Mathematical Society Conference Proceedings 20 (1997) 253-275.

[8] C. Hermite, Sur les fonctions de sept lettres, C.R. Math. Acad. Sci. Paris 57 (1863) 750-757.

[9] D.E. Knuth, Art of Computer Programming, Vol. 1, second ed., Addison-Wesley, 1973.

[10] E.E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, J. fur Math. 44 (1852) 115-116.

[11] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, New York, 2008.

[12] E. Lucas, Théorie des Fonctions Numériques Simplement Périodiques, American Journal of Mathematics 2 (1878): 184-196, 197-240, 289-321.

[13] H. van Maldeghem, Generalized Quadrangles, Birkhäuser, Boston, 1998.

[14] S.E. Payne, A census of finite generalized quadrangles, W.M. Kantor, R.A. Liebler, S.E. Payne, E.E. Shult (Editors), Finite Geometries, Buildings, and Related Topics, Clarendon, Oxford, 1990, pp. 29-36.

[15] S.E. Payne and J.A. Thas, Finite Generalized Quadrangles, Research Notes in Mathematics, vol. 110, Pitman, Boston 1984.