Journal of Integer Sequences, Vol. 18 (2015),
Article 15.7.8

An Integer Sequence Motivated by Generalized Quadrangles

Brian G. Kronenthal
Department of Mathematics
Kutztown University of Pennsylvania
15200 Kutztown Road
Kutztown, PA 19530-9335
USA
kronenthal@kutztown.edu

Abstract

In this paper, we prove a closed form for a sequence motivated by the search for new generalized quadrangles of odd order. We present two proofs: a direct proof to explain the closed form's derivation and a shorter inductive argument. The sequence in question is derived from congruences that arise from applying the Hermite-Dickson criterion to a permutation polynomial that is related to the girth of monomial graphs.

1 Introduction

In this section, we first present some definitions and notation that we will need (Section 1.1). Then we provide some background and motivation for the results presented in this paper (Section 1.2).

1.1 Fundamental definitions and notation

We begin with some definitions. A *graph* $\mathcal{G} = (V, E)$ consists of a set V of vertices and a set E of edges. The *order* of a graph is the number of vertices it contains (namely $|V|$). 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 the same finite degree t, then $\mathcal{G}$ is called a *t-regular graph*. A *uv-walk of length $k \geq 1$* is a sequence $(u = v_0, e_1, v_1, e_2, v_2, \ldots, e_k, v_k = v)$ of alternating vertices and edges, where $e_i = \{v_{i-1}, v_i\}$ for $i = 1, \ldots, k$. For every vertex u, we define (u) to be a *uu-walk of length 0*. A graph $\mathcal{G}$ 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* 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 C_k* 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 $\mathcal{G}$. A connected graph that does not contain any cycles is called a *tree*. A graph $\mathcal{G}$ is *bipartite* if its vertex set 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). Two graphs $\mathcal{G}_1 = (V_1, E_1)$ and $\mathcal{G}_2 = (V_2, E_2)$ are *isomorphic* if there exists a bijection $\varphi : V_1 \to V_2$ such that $x, y \in V_1$ are adjacent if and only if $\varphi(x), \varphi(y) \in V_2$ are adjacent. Other standard graph theory definitions may be found, for example, in Bollobás [2].

Let $\mathbb{F}_q$ denote the finite field of order q. A *permutation polynomial of* $\mathbb{F}_q$ is a polynomial $f \in \mathbb{F}_q[x]$ whose induced function on $\mathbb{F}_q$, defined by $a \mapsto f(a)$, is a bijection. Let $f_2, f_3 : \mathbb{F}_q^2 \to \mathbb{F}_q$ be functions. An *algebraically defined graph $G_q(f_2, f_3)$ of dimension three* is a bipartite graph with partite sets $P = \mathbb{F}_q^3 = L$, and $(x_1, x_2, x_3) \in P$ is adjacent to $[y_1, y_2, y_3] \in L$ if $x_i + y_i = f_i(x_1, y_1)$ for $i = 2, 3$. If both f_2 and f_3 are monomials, we call $G_q(f_2, f_3)$ a *monomial graph*.

1.2 Motivation

One reason for studying monomial graphs is the desire to construct new generalized quadrangles of odd prime power order. While typically viewed as incidence geometries (see Payne and Thas [13], Van Maldeghem [15], and Benson [1] for additional information), we will view generalized quadrangles from the perspective of their point-line incidence graphs, also known as Levi graphs. In other words, for the remainder of this paper, we will adopt a purely graph-theoretical viewpoint. Hence, we define a finite *generalized quadrangle of order* q, denoted $GQ(q)$, to be a bipartite $(q+1)$-regular graph of girth eight and diameter four. No $GQ(q)$ of non-prime power order is currently known. Many examples of nonisomorphic $GQ(q)$ are known when q is a power of 2. However, for a given odd prime power q, only one $GQ(q)$ is known (up to graph isomorphism).

The *affine part* of a generalized quadrangle is the subgraph induced by all vertices at distance three from a fixed edge. In all known $GQ(q)$ for odd prime powers q, the affine part is simply an isomorphic copy of $G_q(xy, xy^2)$, which we denote by $\Gamma_3(q)$.

Now, a primary motivation for Dmytrenko, Lazebnik, and Williford [5] and Kronenthal [10] was to construct a new $GQ(q)$ of odd prime power order as follows. 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 $|P| = q^3 = |L|$. Next, "attach" a tree to it in such a way that the result is a new generalized quadrangle.

To address the first step, we note that our goal is to find an algebraically defined graph with many of the same properties as $\Gamma_3(q)$, a monomial graph. Therefore, it is logical to first search for a replacement among monomial graphs. This strategy was investigated by Dmytrenko, Lazebnik and Williford [5], who conjectured that a suitable monomial graph does not exist.

Conjecture 1. [5] 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, where the described strategy of constructing nonisomorphic generalized quadrangles succeeds. See Payne [12], Van Maldeghem [15], and Cherowitzo [3] for additional information.

Working towards a proof of Conjecture 1, Dmytrenko, Lazebnik and Williford [5] proved the following result:

Theorem 2. *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* $\mathbb{F}_q$.

The permutation polynomial from part 2 of Theorem 2 was then used in conjunction with the Hermite-Dickson criterion:

Theorem 3 (Hermite-Dickson criterion)**.** (See Hermite [8] and Dickson [4]; see also Lidl and 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 $\mathbb{F}_q$; and*
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 $q-2$.*

Indeed, let $e \geq 1$ be an integer, p an odd prime, and $q = p^e \geq 5$. Let G be a monomial graph of girth at least eight. Then by Theorem 2, G is isomorphic to $G_q(xy, x^k y^{2k})$ and

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

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 for all $1 \leq t \leq q-2$. This yields

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

for details of this derivation, see Kronenthal [10].

We now consider instances of (1) for some small values of t; the result is a sequence of congruences. We use (κ_i) to denote the congruence resulting from the substitution $t = i$. When $t = 1$, (1) yields $-2 + \binom{2k}{k} \equiv 0 \pmod{p}$, and so

$$\binom{2k}{k} \equiv 2 \pmod{p}. \tag{κ_1}$$

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

$$\binom{4k}{2k} \equiv 6 \pmod{p}. \tag{κ_2}$$

Continuing this process of evaluating (1) for subsequent values of t, and back-substituting previous congruences at each step, yields the following:

$$\binom{6k}{3k} - 3\binom{4k}{3k} \equiv 8 \pmod{p} \tag{κ_3}$$

$$\binom{8k}{4k} - 4\binom{6k}{4k} \equiv 10 \pmod{p} \tag{κ_4}$$

$$\binom{10k}{5k} - 5\binom{8k}{5k} + 10\binom{6k}{5k} \equiv 32 \pmod{p} \tag{κ_5}$$

$$\binom{12k}{6k} - 6\binom{10k}{6k} + 15\binom{8k}{6k} \equiv 84 \pmod{p} \tag{κ_6}$$

$$\binom{14k}{7k} - 7\binom{12k}{7k} + 21\binom{10k}{7k} - 35\binom{8k}{7k} \equiv 128 \pmod{p} \tag{κ_7}$$

$$\binom{16k}{8k} - 8\binom{14k}{8k} + 28\binom{12k}{8k} - 56\binom{10k}{8k} \equiv 186 \pmod{p} \tag{κ_8}$$

$$\vdots$$

In general, we obtain that for every integer $t \geq 1$,

$$\sum_{h=0}^{\left\lfloor \frac{t-1}{2} \right\rfloor} (-1)^h \binom{t}{h} \binom{2k(t-h)}{kt} \equiv b_t \pmod{p}, \tag{κ_t}$$

where the integer b_t represents the terms in (1) not involving k (after back-substituting $(\kappa_1), \ldots, (\kappa_{t-1})$). The sequence $(b_t)_{t \geq 1}$ appears in Sloane's Online Encyclopedia of Integer Sequences as sequence number A247984 [14]:

> 2, 6, 8, 10, 32, 84, 128, 186, 512, 1276, 2048, 3172, 8192, 19816, 32768, 52666, 131072, 310764, 524288, 863820, 2097152, 4899736, 8388608, 14073060, 33554432, 77509464, 134217728, 228318856, 536870912, 1228859344, ...

The following theorem, our main result, states a closed form for b_t.

Theorem 4. *For all positive integers t, let b_t be as defined in (κ_t). Then*

$$b_t = \begin{cases} 2^t, & \text{if } t \text{ is odd;} \\ 2^t - (-1)^{t/2}\binom{t}{t/2}, & \text{if } t \text{ is even.} \end{cases}$$

Theorem 4 first appeared as a comment, without proof, in Kronenthal [10]. The purpose of this paper is to prove Theorem 4 in two ways. In Section 2, we prove the theorem directly (much like how we originally derived it). In Section 3, we present a shorter inductive argument.

However, before ending this section, we note that after the change of variables $g = t - j$, (1) may be rewritten as

$$\sum_{g=0}^{t}(-2)^{t-g}\binom{t}{g}\sum_{h=0}^{\lfloor g/2\rfloor}(-1)^h\binom{g}{h}\binom{2k(g-h)}{kg} \equiv 0 \pmod{p}. \tag{2}$$

This will be used both in Section 2 and in Section 3.

2 A direct proof

In this section, we prove Theorem 4 directly. We begin with a number of preliminary results.

Lemma 5. (Graham, Knuth, and Patashnik [7, Equation 5.10]) *Let n and k be non-negative integers. Then*

$$\sum_{j=0}^{n}\binom{j}{k} = \binom{n+1}{k+1}.$$

Lemma 6. (Graham, Knuth, and Patashnik [7, Equation 5.5]) *Let $k \neq 0$ be an integer. Then*

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}.$$

Lemma 7. (Gould [6, Equation 1.47 with $x = 1$]) *For all $j \leq n$,*

$$\sum_{k=1}^{n}(-1)^k\binom{n}{k}\frac{k^j}{k+1} = (-1)^j\frac{1}{n+1}.$$

In the following, let $\mathbb{N} = \{1, 2, 3, \ldots\}$ denote the set of natural numbers.

Lemma 8. *Let $j, n \in \mathbb{N}$. Then*

$$\sum_{\substack{y_1+\cdots+y_j=n \\ y_1,\ldots,y_j\in\mathbb{N}}} \binom{n}{y_1, y_2, \ldots, y_{j-1}, y_j} = \sum_{k=1}^{j} (-1)^{j-k} k^n \binom{j}{j-k}.$$

Lemma 8 follows directly from Kao and Zetterberg [9, Theorem 2.2].

Lemma 9. *Let $i, t \in \mathbb{N}$ such that $i < t$. Then*

$$\sum_{j=1}^{t-i} \sum_{t>x_1>\cdots>x_j=i} (-1)^{j+1} \binom{t}{x_1}\binom{x_1}{x_2}\cdots\binom{x_{j-1}}{i} = (-1)^{t+i-1}\binom{t}{i},$$

where $x_i \in \mathbb{N}$ for all $i = 1, 2, \ldots, j$.

Proof. We have

$$\begin{aligned}
&\sum_{j=1}^{t-i} \sum_{t>x_1>\cdots>x_j=i} (-1)^{j+1} \binom{t}{x_1}\binom{x_1}{x_2}\cdots\binom{x_{j-1}}{i} \\
&= \binom{t}{i} \sum_{j=1}^{t-i} (-1)^{j+1} \sum_{t>x_1>\cdots>x_j=i} \binom{t-i}{t-x_1, x_1-x_2, \ldots, x_{j-2}-x_{j-1}, x_{j-1}-i} \\
&= \binom{t}{i} \sum_{j=1}^{t-i} (-1)^{j+1} \sum_{\substack{y_1+\cdots+y_j=t-i \\ y_1,\ldots,y_j\in\mathbb{N}}} \binom{t-i}{y_1, y_2, \ldots, y_{j-1}, y_j} \\
&= \binom{t}{i} \sum_{j=1}^{t-i} (-1)^{j+1} \sum_{k=1}^{j} (-1)^{j-k} k^{t-i} \binom{j}{j-k} \quad \text{(by Lemma 8 with } n = t-i) \\
&= \binom{t}{i} \sum_{k=1}^{t-i} (-1)^{k-1} k^{t-i} \sum_{j=0}^{t-i} \binom{j}{k} \\
&= \binom{t}{i} \sum_{k=1}^{t-i} (-1)^{k-1} k^{t-i} \binom{t-i+1}{k+1} \quad \text{(by Lemma 5)} \\
&= -\binom{t}{i} (t-i+1) \sum_{k=1}^{t-i} (-1)^{k} \binom{t-i}{k} \frac{k^{t-i}}{1+k} \quad \text{(by Lemma 6)} \\
&= -\binom{t}{i} (t-i+1) \left((-1)^{t-i} \frac{1}{t-i+1} \right) \quad \text{(by Lemma 7 with } n = t-i \text{ and } j = t-i) \\
&= \binom{t}{i} (-1)^{t+i-1}.
\end{aligned}$$

□

Lemma 10. (Graham, Knuth, and Patashnik [7, Equation 5.24]) *Let $l \geq 0$, m, and n be integers. Then*

$$\sum_k \binom{l}{m+k}\binom{s+k}{n}(-1)^k = (-1)^{l+m}\binom{s-m}{n-l}.$$

We now use (2) and the above lemmas to prove Theorem 4. Define

$$C_t = \sum_{g=0}^{\lfloor t/2 \rfloor} (-1)^{t-g} 2^{t-2g} \binom{t}{2g}\binom{2g}{g},$$

$$L_t = \sum_{h=0}^{\left\lfloor \frac{t-1}{2} \right\rfloor} (-1)^h \binom{t}{h}\binom{2k(t-h)}{kt},$$

and

$$a_{t,u} = (-2)^{t-u}\binom{t}{u}.$$

Note that on the left-hand side of (2), C_t is the constant term (i.e., the term not involving k, which comes from the terms with $h = g/2$ followed by the change of variables $g \mapsto 2g$), L_t consists of all non-constant terms containing binomial coefficients of the form $\binom{x}{kt}$ for some x (L_t is the left-hand side of (κ_t)), and $a_{t,u}$ is the coefficient of L_u when it appears in the calculation of (κ_t). Then (2) is equivalent to

$$C_t + \sum_{g=1}^{t-1} a_{t,g} L_g + \sum_{h=0}^{\left\lfloor \frac{t-1}{2} \right\rfloor} (-1)^h \binom{t}{h}\binom{2k(t-h)}{kt} \equiv 0 \pmod{p},$$

and therefore congruence (κ_t) may be rewritten as

$$\sum_{h=0}^{\left\lfloor \frac{t-1}{2} \right\rfloor} (-1)^h \binom{t}{h}\binom{2k(t-h)}{kt} \equiv -C_t - \sum_{g=1}^{t-1} a_{t,g} L_g \pmod{p}.$$

In other words,

$$L_t \equiv -C_t - \sum_{g=1}^{t-1} a_{t,g} L_g \pmod{p}.$$

Expanding and back-substituting for some small values of t, we have:

$$\begin{aligned}
L_1 &\equiv -C_1 \pmod p\\
L_2 &\equiv -a_{2,1}\cdot L_1 - C_2 \equiv a_{2,1}C_1 - C_2 \pmod p\\
L_3 &\equiv -a_{3,2}\cdot L_2 - a_{3,1}\cdot L_1 - C_3\\
&\equiv -a_{3,2}(a_{2,1}C_1 - C_2) + a_{3,1}C_1 - C_3\\
&\equiv (a_{3,1} - a_{3,2}a_{2,1})C_1 + a_{3,2}C_2 - C_3 \pmod p\\
L_4 &\equiv -a_{4,3}\cdot L_3 - a_{4,2}\cdot L_2 - a_{4,1}\cdot L_1 - C_4\\
&\equiv -a_{4,3}\big((a_{3,1} - a_{3,2}a_{2,1})C_1 + a_{3,2}C_2 - C_3\big) - a_{4,2}(a_{2,1}C_1 - C_2) + a_{4,1}C_1 - C_4\\
&\equiv (a_{4,1} - a_{4,3}a_{3,1} - a_{4,2}a_{2,1} + a_{4,3}a_{3,2}a_{2,1})C_1 + (a_{4,2} - a_{4,3}a_{3,2})C_2 + a_{4,3}C_3 - C_4 \pmod p
\end{aligned}$$

In general, congruence (κ_t) may be written as

$$\begin{aligned}
L_t = \sum_{h=0}^{\lfloor\frac{t-1}{2}\rfloor} (-1)^h \binom{t}{h}\binom{2k(t-h)}{kt}\\
\equiv -C_t + \sum_{i=1}^{t-1} C_i \sum_{j=1}^{t-i} \sum_{t>x_1>\cdots>x_j=i} (-1)^{j+1} a_{t,x_1}a_{x_1,x_2}\cdots a_{x_{j-1},i} \pmod p.
\end{aligned} \tag{3}$$

We are now ready to prove our main result.

Proof of Theorem 4. From (3), the right-hand side of congruence (κ_t) is

$$\begin{aligned}
b_t &= -C_t + \sum_{i=1}^{t} C_i \sum_{j=1}^{t-i} \sum_{t>x_1>\cdots>x_j=i} (-1)^{j+1} a_{t,x_1}a_{x_1,x_2}\cdots a_{x_{j-1},i}\\
&= -\sum_{g=0}^{\lfloor t/2\rfloor} (-1)^{t-g}2^{t-2g}\binom{t}{2g}\binom{2g}{g} + \sum_{i=1}^{t-1}\left(\sum_{g=0}^{\lfloor i/2\rfloor}(-1)^{i-g}2^{i-2g}\binom{i}{2g}\binom{2g}{g}\right)\\
&\quad \sum_{j=1}^{t-i}\sum_{t>x_1>\cdots>x_j=i}(-1)^{j+1}\left((-2)^{t-x_1}\binom{t}{x_1}\right)\left((-2)^{x_1-x_2}\binom{x_1}{x_2}\right)\cdots\left((-2)^{x_{j-1}-i}\binom{x_{j-1}}{i}\right)\\
&= -\sum_{g=0}^{\lfloor t/2\rfloor} (-1)^{t-g}2^{t-2g}\binom{t}{2g}\binom{2g}{g}\\
&\qquad + (-2)^t \sum_{i=1}^{t-1}\left(\sum_{j=1}^{t-i}\sum_{t>x_1>\cdots>x_j=i}(-1)^{j+1}\binom{t}{x_1}\cdots\binom{x_{j-1}}{i}\right)\sum_{g=0}^{\lfloor i/2\rfloor}(-4)^{-g}\binom{i}{2g}\binom{2g}{g}
\end{aligned}$$

$$
\begin{aligned}
&= -\sum_{g=0}^{\lfloor t/2 \rfloor} (-1)^{t-g} 2^{t-2g} \binom{t}{2g} \binom{2g}{g} \\
&\qquad + (-2)^t \sum_{i=1}^{t-1} \left(\binom{t}{i} (-1)^{t+i-1} \right) \sum_{g=0}^{\lfloor i/2 \rfloor} (-4)^{-g} \binom{i}{2g} \binom{2g}{g} \quad \text{(by Lemma 9)} \\
&= (-2)^t \sum_{i=1}^{t} \left(\binom{t}{i} (-1)^{t+i-1} \right) \sum_{g=0}^{\lfloor i/2 \rfloor} (-4)^{-g} \binom{i}{2g} \binom{2g}{g} \\
&= (-1)^{t-1} (-2)^t \sum_{g=0}^{\lfloor t/2 \rfloor} (-4)^{-g} \binom{2g}{g} \sum_{i=1}^{t} (-1)^i \binom{t}{i} \binom{i}{2g} \\
&= -2^t \left(\sum_{i=1}^{t} (-1)^i \binom{t}{i} + \sum_{g=1}^{\lfloor t/2 \rfloor} (-4)^{-g} \binom{2g}{g} \sum_{i=1}^{t} (-1)^i \binom{t}{i} \binom{i}{2g} \right) \\
&= -2^t \left(-1 + \sum_{g=1}^{\lfloor t/2 \rfloor} (-4)^{-g} \binom{2g}{g} \sum_{i=1}^{t} (-1)^i \binom{t}{i} \binom{i}{2g} \right) \\
&= -2^t \left(-1 + \sum_{g=1}^{\lfloor t/2 \rfloor} (-4)^{-g} \binom{2g}{g} (-1)^t \binom{0}{2g-t} \right) \quad \text{(by Lemma 10)} \\
&= \begin{cases} 2^t, & \text{if } t \text{ is odd;} \\ -2^t \left(-1 + (-4)^{-t/2} \binom{t}{t/2} (-1)^t \right), & \text{if } t \text{ is even;} \end{cases} \\
&= \begin{cases} 2^t, & \text{if } t \text{ is odd;} \\ 2^t - (-1)^{t-t/2} 2^t (2^2)^{-t/2} \binom{t}{t/2}, & \text{if } t \text{ is even;} \end{cases} \\
&= \begin{cases} 2^t, & \text{if } t \text{ is odd;} \\ 2^t - (-1)^{t/2} \binom{t}{t/2}, & \text{if } t \text{ is even.} \end{cases}
\end{aligned}
$$

□

3 An inductive proof

In this section, we prove Theorem 4 inductively. We begin by reorganizing the terms of (2). The left-hand side of congruence (κ_t) will be those terms with $g = t$ and $h \neq g/2$, namely

$$\sum_{h=0}^{\left\lfloor \frac{t-1}{2} \right\rfloor} (-1)^h \binom{t}{h} \binom{2k(t-h)}{kt}.$$

We partition the remaining terms into two sums:

$$\sum_{g=0}^{t}(-1)^{g/2}2^{t-g}\binom{t}{g}\binom{g}{g/2}=\sum_{g=0}^{\lfloor t/2\rfloor}(-1)^{t-g}2^{t-2g}\binom{t}{2g}\binom{2g}{g}$$

contains all terms such that $h=g/2$, and

$$\sum_{g=1}^{t-1}(-2)^{t-g}\binom{t}{g}\sum_{h=0}^{\left\lfloor\frac{g-1}{2}\right\rfloor}(-1)^{h}\binom{g}{h}\binom{2k(g-h)}{kg}$$

contains all remaining terms (i.e., all terms such that $g\neq t$ and $h\neq g/2$). Note that the inner sum is the left-hand side of congruence (κ_g). Hence, we rewrite (2) as

$$\sum_{h=0}^{\left\lfloor\frac{t-1}{2}\right\rfloor}(-1)^{h}\binom{t}{h}\binom{2k(t-h)}{kt}\equiv-\sum_{g=0}^{\lfloor t/2\rfloor}(-1)^{t-g}2^{t-2g}\binom{t}{2g}\binom{2g}{g}-\sum_{g=1}^{t-1}(-2)^{t-g}\binom{t}{g}b_g \pmod{p},$$

which proves

$$b_t=-\sum_{g=0}^{\lfloor t/2\rfloor}(-1)^{t-g}2^{t-2g}\binom{t}{2g}\binom{2g}{g}-\sum_{g=1}^{t-1}(-2)^{t-g}\binom{t}{g}b_g. \tag{4}$$

Now, before proving our main result, we state a well-known lemma.

Lemma 11. *Let t be a positive integer. Then* $\sum_{g=0}^{\lfloor t/2\rfloor}\binom{t}{2g}=2^{t-1}$ *and*

$$\sum_{g=1}^{\lfloor t/2\rfloor}\binom{t}{2g-1}=\begin{cases}2^{t-1}, & \textit{if } t \textit{ is even;}\\ 2^{t-1}-1, & \textit{if } t \textit{ is odd.}\end{cases}$$

Proof of Theorem 4. We proceed by induction. When $t=1$, (4) implies that

$$b_1=-(-1)(2)\binom{1}{0}\binom{0}{0}=2.$$

Now, suppose the result holds for all positive integers less than t. Then from (4),

$$\begin{aligned}
b_t &= -\sum_{g=0}^{\lfloor t/2\rfloor}(-1)^{t-g}2^{t-2g}\binom{t}{2g}\binom{2g}{g} - \sum_{g=1}^{t-1}(-2)^{t-g}\binom{t}{g}b_g \\
&= -\sum_{g=0}^{\lfloor t/2\rfloor}(-1)^{t-g}2^{t-2g}\binom{t}{2g}\binom{2g}{g} - \sum_{g=0}^{\left\lfloor \frac{t-1}{2}\right\rfloor}(-2)^{t-2g}\binom{t}{2g}\left(2^{2g}-(-1)^g\binom{2g}{g}\right) \\
&\quad - \sum_{g=1}^{\lfloor t/2\rfloor}(-1)^{t+1}2^t\binom{t}{2g-1} \\
&= -\sum_{g=0}^{\lfloor t/2\rfloor}\left[(-1)^{t-g}2^{t-2g}\binom{t}{2g}\binom{2g}{g} + (-2)^{t-2g}\binom{t}{2g}\left(2^{2g}-(-1)^g\binom{2g}{g}\right)\right] \\
&\quad + \left(\frac{1+(-1)^t}{2}\right)\left(2^t-(-1)^{t/2}\binom{t}{t/2}\right) - \sum_{g=1}^{\lfloor t/2\rfloor}(-1)^{t+1}2^t\binom{t}{2g-1} \\
&= -\sum_{g=0}^{\lfloor t/2\rfloor}(-2)^t\binom{t}{2g} + \left(\frac{1+(-1)^t}{2}\right)\left(2^t-(-1)^{t/2}\binom{t}{t/2}\right) - \sum_{g=1}^{\lfloor t/2\rfloor}(-1)^{t+1}2^t\binom{t}{2g-1} \\
&= (-1)^{t+1}2^t\sum_{g=0}^{\lfloor t/2\rfloor}\binom{t}{2g} + \left(\frac{1+(-1)^t}{2}\right)\left(2^t-(-1)^{t/2}\binom{t}{t/2}\right) + (-2)^t\sum_{g=1}^{\lfloor t/2\rfloor}\binom{t}{2g-1} \\
&= (-1)^{t+1}2^{2t-1} + \left(\frac{1+(-1)^t}{2}\right)\left(2^t-(-1)^{t/2}\binom{t}{t/2}\right) + (-2)^t\left(2^{t-1}-\frac{1-(-1)^t}{2}\right) \\
&\qquad\qquad \text{(by Lemma 11)} \\
&= \begin{cases} 2^t, & \text{if } t \text{ is odd;} \\ 2^t-(-1)^{t/2}\binom{t}{t/2}, & \text{if } t \text{ is even.} \end{cases}
\end{aligned}$$

□

4 Concluding remarks

In this paper, we have provided direct and inductive proofs of Theorem 4. One interesting future direction is as follows:

Open Problem 12. Prove Theorem 4 using a combinatorial argument.

We conclude by stating two results that were proven using Theorem 4. Theorem 13 used b_1 and b_2, while Theorem 14 relied on Theorem 4 in its entirety.

Theorem 13. (Dmytrenko, Lazebnik, and Williford [5]) *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.*

Theorem 14. (Kronenthal [10]) *Let $q = p^e$ be an odd prime power and $e \geq 2$. Then there exists p_0 such that for all $p \geq p_0$, every monomial graph over $\mathbb{F}_q$ of girth at least eight is isomorphic to $\Gamma_3(q)$, and hence has girth exactly eight. Furthermore, p_0 depends only on the largest prime divisor of e. In particular:*

1. *if $e = 2^a 3^b 5^c$ with $a, b, c \geq 0$, then $p_0 = 7$.*
2. *if $e = 2^a 3^b 5^c 7^d$ with $a, b, c, d \geq 0$, then $p_0 = 11$.*
3. *if $e = 2^a 3^b 5^c 7^d 11^y$ with integers $a, b, c, d, y \geq 0$, then $p_0 = 13$.*

5 Acknowledgments

The author is grateful to Felix Lazebnik for his support while conducting this research, as well as for suggesting Open Problem 12.

References

[1] C. T. Benson, On the structure of generalized quadrangles, *J. Algebra* **15** (1970) 443–454.

[2] B. Bollobás, *Modern Graph Theory*, Springer, 1998.

[3] W. E. Cherowitzo, *Hyperovals in Desarguesian planes: an electronic update*, informal notes, available at `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** (1896–1897) 161–183.

[5] V. Dmytrenko, F. Lazebnik, and J. Williford, On monomial graphs of girth eight, *Finite Fields Appl.* **13** (2007) 828–842.

[6] H. W. Gould, *Combinatorial Identities*, Morgantown, WV, 1972.

[7] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*, 2nd edition, Addison-Wesley Publishing Company, 1994.

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

[9] R. C. Kao and L. H. Zetterberg, An identity for the sum of multinomial coefficients, *Amer. Math. Monthly* **64** (1957) 96–100.

[10] B. G. Kronenthal, Monomial graphs and generalized guadrangles, *Finite Fields Appl.* **18** (2012) 674–684.

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

[12] S. E. Payne, A census of finite generalized quadrangles, in *Finite Geometries, Buildings, and Related Topics*, Oxford Univ. Press, 1990, pp. 29–36.

[13] S. E. Payne and J. A. Thas, *Finite Generalized Quadrangles*, Research Notes in Mathematics, Vol. 110, Pitman, 1984.

[14] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, published electronically at http://oeis.org.

[15] H. Van Maldeghem, *Generalized Polygons*, Birkhäuser, 1998.

2010 *Mathematics Subject Classification*: Primary 12E99; Secondary 51E12.
Keywords: permutation polynomial, monomial graph, generalized quadrangle, girth, cycle.

(Concerned with sequences A246800 and A247984.)

Received February 10 2015; revised versions received July 10 2015. Published in *Journal of Integer Sequences*, July 16 2015.