ON THE CONNECTIVITY OF CERTAIN GRAPHS OF HIGH GIRTH

FELIX LAZEBNIK AND RAYMOND VIGLIONE

Abstract. Let q be a prime power and $k \geq 2$ be an integer. In [2] and [3] it was determined that the number of components of certain graphs $D(k,q)$ introduced in [1] is at least q^{t-1} where $t = \lfloor \frac{k+2}{4} \rfloor$. This implied that these components (most often) provide the best-known asymptotic lower bound for the greatest number of edges in graphs of their order and girth. In [4], it was shown that the number of components is (exactly) q^{t-1} for q odd, but the method used there failed for q even. In this paper we prove that the number of components of $D(k,q)$ for even $q > 4$ is again q^{t-1} where $t = \lfloor \frac{k+2}{4} \rfloor$. Our proof is independent of the parity of q as long as $q > 4$. Furthermore, we show that for $q = 4$ and $k \geq 4$, the number of components is q^t.

1. Introduction and Main Results

In this paper, all graphs are assumed to be simple, i.e. undirected with no loops or multiple edges. By $V(G)$ we denote the set of vertices of G. The *order* of G is the number of its vertices, and the *size* of G is the number of its edges. The *girth* of a graph G containing a cycle is the length of its shortest cycle, and we denote it by $g(G)$. The number of components of G will be denoted by $c(G)$.

Let q be a prime power, and let $\mathbb{F}_q$ denote the finite field of q elements. For an integer $k \geq 2$, let P_k and L_k be two copies of $\mathbb{F}_q^k$, the k-dimensional vector space over $\mathbb{F}_q$. Elements of P_k will be called *points*, and elements of L_k will be called *lines*. It will be convenient to denote points $a \in P_k$ by (a), and lines $a \in L_k$ by $[a]$. Let $f_i : \mathbb{F}_q^{2i-2} \to \mathbb{F}_q$ be arbitrary functions for $i \geq 2$. The bipartite graph $D(k,q)$ is defined as follows: the vertex set of $D(k,q)$ is the disjoint union of P_k and L_k, and a point $(p) = (p_1, p_2, \ldots, p_k)$ is adjacent to a line $[l] = [l_1, l_2, \ldots, l_k]$ if and only if the following relations on their coordinates hold:

$$\begin{aligned} l_2 + p_2 &= p_1 l_1, \\ l_3 + p_3 &= p_1 l_2, \\ \text{and for } 4 \leq i \leq k, \quad l_i + p_i &= \begin{cases} -p_{i-2} l_1, & i \equiv 0 \text{ or } 1 \mod 4 \\ \ \ p_1 l_{i-2}, & i \equiv 2 \text{ or } 3 \mod 4. \end{cases} \end{aligned} \tag{1.1}$$

This family was introduced by Lazebnik and Ustimenko in [1], where it was proved that graphs $D(k,q)$ are edge transitive and of girth $g(D(k,q)) \geq k+5$ for odd k. In [3], Lazebnik, Ustimenko and Woldar showed that for odd $k \geq 6$, graphs $D(k,q)$ are disconnected. Let $CD(k,q)$ denote a component of $D(k,q)$ (due to edge transitivity all components are isomorphic). It was shown in [3] that $c(D(k,q)) \geq q^{t-1}$, where $t = \lfloor \frac{k+2}{4} \rfloor$, and therefore the order of $CD(k,q)$ is at most $2q^{k-t+1}$. This implied that graphs $CD(k,q)$ provide the best-known lower bounds for the maximum number of edges in graphs of their order and girth, with the only exceptions being for girth 11 and 12. The result represented a slight improvement of the previous best known lower bound given by the graphs constructed by Margulis [7], and independently by Lubotzky, Phillips and Sarnak [6] (often referred to as Ramanujan graphs).

At that point, determining the exact value of $c(D(k,q))$ became important, since if it were greater than q^{t-1}, it would imply that graphs $CD(k,q)$ have even smaller order (for the same girth and degree), hence greater edge density. In [4], Lazebnik, Ustimenko and Woldar proved that this is not the case for odd q, i.e., that for odd q, $c(D(k,q)) = q^{t-1}$ (the statement and proof of this were actually embedded in Corollaries 5.1 and 5.2). The method of [4] could not be used for even q; moreover, for $q = 4$, at least for small k, the number of components is actually q^t (as shown by computer). This gave the hope that for even q the number of components can grow faster than for odd q.

In this paper, we show that (unfortunately!) this is not the case. For $q = 4$, the number of components is actually 4^t, but the rate of growth with respect to k is the same. Our main results are the following:

Theorem 1. *Let q be an even prime power, $k \geq 4$ be an integer, and $t = \lfloor \frac{k+2}{4} \rfloor$.*
(i) If $q > 4$, then $c(D(k,q)) = q^{t-1}$.
(ii) $c(D(k,4)) = 4^t$.

Combined with all earlier results on the connectivity of $D(k,q)$, it immediately gives a complete description of $c(D(k,q))$:

Theorem 2. *Let q be a prime power, $k \geq 2$ be an integer, and $t = \lfloor \frac{k+2}{4} \rfloor$.*
(i) If $q \neq 4$, then $c(D(k,q)) = q^{t-1}$.
(ii) $c(D(2,4)) = c(D(3,4)) = 1$, and for $k \geq 4$, $c(D(k,4)) = 4^t$.

Our proof of Theorem 1 is based on the ideas of [2] – [4], where q was assumed odd, but several important modifications had to be introduced to deal with q even. After this was done we realized that it was possible to combine the two proofs into one which is independent of the parity of q for $q > 4$. The case $q = 4$ required additional modifications.

In Section 2 we introduce all notions and facts needed for the proof of Theorem 1 which is presented in Section 3.

For more information about graphs $D(k,q)$, $CD(k,q)$, and their applications, see [5] and references therein.

2. More definitions and Preliminary Results

The original construction of graphs $D(k,q)$ in [1] employed the notion of an affine Lie algebra, and the notations which were subsequently used in [2] – [4] reflected the corresponding root systems. Since these algebraic notions are not important for this paper, we use simpler notations from Lazebnik and Woldar [5], and Viglione [9]. We begin with the notion of an "invariant" (see [2], [3]) which is central in our studies of components of $D(k,q)$.

2.1. **Invariants.** Let $k \geq 6$ and $t = \lfloor \frac{k+2}{4} \rfloor$. For every point $(p) = (p_1, ..., p_k)$ and every line $[l] = [l_1, ..., l_k]$ in $D(k, q)$, let $a_r = a_r((p))$ or $a_r = a_r([l])$, $2 \leq r \leq t$, be given by:

$$a_r((p)) = \begin{cases} p_1p_4 + p_2^2 - p_5 + p_6, & \text{if } r = 2; \\ p_1p_{4r-4} + p_2p_{4r-6} + p_2p_{4r-7} - p_3p_{4r-8} - p_{4r-3} + p_{4r-2} + \\ \sum_{i=2}^{r-2}(p_{4i-3}p_{4(r-i)-2} - p_{4i-1}p_{4(r-i)-4}), & \text{if } r \geq 3; \end{cases}$$

and

$$a_r([l]) = \begin{cases} -l_1l_3 + l_2^2 + l_5 - l_6, & \text{if } r = 2; \\ -l_1l_{4r-5} + l_2l_{4r-6} + l_2l_{4r-7} - l_3l_{4r-8} + l_{4r-3} - l_{4r-2} + \\ \sum_{i=2}^{r-2}(l_{4i-3}l_{4(r-i)-2} - l_{4i-1}l_{4(r-i)-4}), & \text{if } r \geq 3. \end{cases}$$

Then the *invariant vector* (or simply *invariant*) $\vec{a}(u)$ of a vertex u is

$$\vec{a} = \vec{a}(u) = \langle a_2(u), a_3(u), ..., a_t(u) \rangle.$$

The relation between invariants and components of $D(k, q)$ is the following.

Proposition 1 ([2], [3]). *Let u and v be vertices from the same component of $D(k, q)$. Then $\vec{a}(u) = \vec{a}(v)$. Moreover, for any $t-1$ field elements $x_i \in \mathbb{F}_q$, $2 \leq i \leq t = \lfloor \frac{k+2}{4} \rfloor$, there exists a vertex v of $D(k, q)$ for which $\vec{a}(v) = \langle x_2, x_3, ..., x_t \rangle$.*

In [4] the converse of this proposition was established for q odd, which gave the result $c(D(k, q)) = q^{t-1}$ for odd q. In this paper we aim to establish its converse for $q > 4$ even. Thus the invariant characterizes the components of $D(k, q)$ for all $q > 4$. For $q = 4$, another invariant will need to be defined. Although it will not be strong enough to yield an analog of Proposition 1, it will help us to find $c(D(k, 4))$ (see Section 3).

2.2. **Automorphisms.** In this section we rewrite some automorphisms of $D(k, q)$ given in [1] – [4] in a more user-friendly way by using our notations. The automorphisms we will use in this paper are listed below. In each case the fact that the mappings are automorphisms of $D(k, q)$ is easily verified. For an automorphism σ, the image of point (p) and of line $[l]$ is denoted by $(p)^\sigma$ and $[l]^\sigma$, respectively. For $(p) = (p_1 ..., p_i, ...)$, we write p_i^σ to represent the ith coordinate of $(p)^\sigma$, and similarly we do for lines.

In our description of the automorphisms, we indicate the action of the map on each coordinate separately. If a particular coordinate v_i of a vector v is fixed by an automorphism σ, i.e., $v_i^\sigma = v_i$, then it is not explicitly indicated in the definition. For example, below we see that the cases $i = 1$ or $i \equiv 3 \mod 4$ are not listed after the brace in the definition of the automorphism $t_0(x)$. Hence for all these i, $p_i^{t_0(x)} = p_i$. They can also be referred to as "additive", since the action amounts to adding certain quantities to coordinates. We begin with the family $t_0(x)$:

$$p_i^{t_0(x)} = p_i + \begin{cases} p_1x, & i = 2 \\ -2p_2x - p_1x^2, & i = 4 \\ -(p_{i-2} + p_{i-3})x + p_{i-5}x^2, & i \equiv 0 \mod 4,\ i \geq 8 \\ -p_{i-2}x, & i \equiv 1 \mod 4,\ i \geq 5 \\ -p_{i-3}x, & i \equiv 2 \mod 4,\ i \geq 6 \end{cases}$$

$$l_i^{t_0(x)} = l_i + \begin{cases} x, & i = 1 \\ -l_2x, & i = 4 \\ -l_{i-3}x, & i \equiv 0,2 \mod 4,\ i \geq 6 \end{cases}$$

Next is $t_1(x)$:

$$p_i^{t_1(x)} = p_i + \begin{cases} x, & i = 1 \\ p_{i-1}x, & i \equiv 1,3 \mod 4,\ i \geq 3 \end{cases}$$

$$l_i^{t_1(x)} = l_i + \begin{cases} l_1x, & i = 2 \\ 2l_2x + l_1x^2, & i = 3 \\ l_{i-1}x, & i \equiv 1 \mod 4,\ i \geq 5 \\ l_{i-2}x, & i \equiv 2 \mod 4,\ i \geq 6 \\ (l_{i-1} + l_{i-2})x + l_{i-3}x^2, & i \equiv 3 \mod 4,\ i \geq 7 \end{cases}$$

Next is $t_{4m-3}(x)$ for $m \geq 2$:

$$p_i^{t_{4m-3}(x)} = p_i + \begin{cases} x, & i = 4m-3 \\ -p_1x, & i = 4m-1 \\ p_2x, & i = 4m+1 \\ p_{i-4m}x, & i \equiv 1,3 \mod 4,\ i \geq 4m+3 \end{cases}$$

$$l_i^{t_{4m-3}(x)} = l_i + \begin{cases} -x, & i = 4m-3 \\ l_2x, & i = 4m+1 \\ l_{i-4m}x, & i \equiv 1,3 \mod 4,\ i \geq 4m+3 \end{cases}$$

Next is $t_{4m-2}(x)$ for $m \geq 2$:

$$p_i^{t_{4m-2}(x)} = p_i + \begin{cases} x, & i = 4m-2 \\ -p_{i-4m}x, & i \equiv 0,2 \mod 4,\ i \geq 4m+2 \end{cases}$$

$$l_i^{t_{4m-2}(x)} = l_i + \begin{cases} -x, & i = 4m-2 \\ -l_1x, & i = 4m \\ -l_{i-4m}x, & i \equiv 0,2 \mod 4,\ i \geq 4m+2 \end{cases}$$

The last family of automorphisms we will need can be referred to as "multiplicative". For nonzero field elements a and b, the automorphism $m(a,b)$ multiplies the coordinates of points and lines by monomials of a and b:

$$(p) \mapsto (ap_1, abp_2, a^2bp_3, ab^2p_4, ..., a^ib^ip_{4i-3}, a^ib^ip_{4i-2}, a^{i+1}b^ip_{4i-1}, a^ib^{i+1}p_{4i}, ...),$$
$$[l] \mapsto [bl_1, abl_2, a^2bl_3, ab^2l_4, ..., a^ib^il_{4i-3}, a^ib^il_{4i-2}, a^{i+1}b^il_{4i-1}, a^ib^{i+1}l_{4i}, ...].$$

2.3. **Projections and lifts.** The following notions and statements will be used in proofs in Section 3.

For $k \geq 3$, the *projection* $\pi : V(D(k,q)) \to V(D(k-1,q))$ is defined via

$$(p_1, ..., p_k) \mapsto (p_1, ..., p_{k-1}), \quad [l_1, ..., l_k] \mapsto [l_1, ..., l_{k-1}],$$

and is easily seen to be a graph homomorphism of $D(k,q)$ to $D(k-1,q)$ (the adjacent vertices of $D(k,q)$ are mapped to the adjacent vertices of $D(k-1,q)$). The vertex $w = v^\pi \in V(D(k-1,q))$ will often be denoted by v'; we say that v is a *lift* of w and w is a *projection* of v. If B is a component of $D(k,q)$, we will often denote B^π by B', and π_B will denote the restriction of π to B. We say that an automorphism τ *stabilizes* B if $B^\tau = B$; the set of all such automorphisms is denoted by $\mathrm{Stab}(B)$. A component of $D(k,q)$ containing a vertex v will be denoted by $C(v)$. The point and line corresponding to zero vector $\vec{0}$ will be denoted by (0) and $[0]$, respectively. We will always denote the component $C((0))$ of $D(k,q)$ by just C. Then C' will be the corresponding component in $D(k-1,q)$.

Proofs of the following three propositions can be found in [4].

Proposition 2 ([4]). *Let τ be an automorphism of $D(k,q)$, and B be a component of $D(k,q)$ with $v \in V(B)$. Then τ stabilizes B if and only if $v^\tau \in B$. In particular, $t_0(x)$, $t_1(x)$ and $m(a,b)$ are in $\mathrm{Stab}(C)$ for all $x, a, b \in \mathbb{F}_q$, $a, b \neq 0$.*

Proposition 3 ([4]). *Let B be a component of $D(k,q)$. Then π_B is a t-to-1 graph homomorphism for some t, $1 \leq t \leq q^{k-1}$. In particular, let $k \equiv 0, 3 \mod 4$, and suppose π_C is a t-to-1 mapping for some $t > 1$. Then $t = q$.*

Proposition 4 ([4]). *The map $\pi_C : V(C) \to V(C')$ is surjective.*

3. Proofs

As we mentioned in Section 1, Theorem 1 (i) with q odd was essentially stated and proved in [4, Corollary 5.1, 5.2]. The proof in [4] was based on induction on k, and it was broken into four cases, depending on the value of k mod 4. Two of those cases can be repeated verbatim in the proof of our theorem for q even, and we present them for completeness below as Cases 3 and 4. Two other cases, Cases 1 and 2, were heavily dependent on the fact that q was odd and here we present new proofs of these cases which are independent of the parity of q for $q > 4$.

Lemma 1. *Let q be a prime power, $q > 4$, and $k \geq 6$. If $v \in V(D(k,q))$ satisfies $\vec{a}(v) = 0$, then $v \in V(C)$.*

Proof. The proof proceeds by induction on k. It is known (see [8],[4]) that for $q > 4$, graphs $D(k,q)$ are connected for $k = 2, 3, 4, 5$ (in [4, Theorem 4], the case $q = 4$ was included by mistake).

We begin with the base case $k = 6$. Let $v \in V(D(6,q))$ with $\vec{a}(v) = \vec{0}$, and let $v' = v^\pi \in V(D(5,q))$. Since $D(5,q)$ is connected, then $v' \in C' = D(5,q)$. Since π_C is surjective by Proposition 4, there is $w \in V(C)$ such that $w^\pi = v' = v^\pi$. Since the sixth coordinate of any vertex u is uniquely determined by its initial five coordinates and $\vec{a}(u)$, we have $v = w \in V(C)$.

The inductive step is treated in four separate cases. For $k \equiv 0, 1, 3 \mod 4$ (i.e., Cases 1, 2, and 3 below), our goal is to show that π_C is a q-to-1 map. These are exactly the values of k for which the invariants of C and C' are the same. To see that this settles these cases, choose $v \in V(D(k,q))$ such that $\vec{a}(v) = \vec{0}$. Let $v' = v^\pi \in V(D(k-1,q))$. Since $\vec{a}(v) = \vec{a}(v') = \vec{0}$, $v' \in C'$ by the induction hypothesis. But then since π_C is a q-to-1 map, all of the lifts of v', including v itself, lie in C, and we are done. So we proceed with the cases.

Case 1: $k \equiv 3 \mod 4$, $k \geq 7$. Write $k = 4j-1$, $j \geq 2$. Let $(p') \in V(D(k-1,q))$ with $p_{4j-5} = p_{4j-3} = p_{4j-2} = 1$, $p_{4j-4} = -1$ and zeroes elsewhere, i.e.,

$$(p') = (0, ..., 0, 1, -1, 1, 1).$$

One easily checks that $\vec{a}(p') = \vec{0}$, so $(p') \in V(C')$ by the induction hypothesis. Since π_C is surjective there is $(p) \in V(C)$ with $(p)^\pi = (p')$, i.e., for some $y \in \mathbb{F}_q$,

$$(p) = (0, ..., 0, 1, -1, 1, 1, y).$$

Now note that $(0, ..., 0, 1, -1, 1, 1, y) \sim [0, ..., 0, 1, -1, 1, 1, y]$, so that this line is also in $V(C)$. One easily checks that $[0, ..., 0, 1, -1, 1, 1, y]^{t_1(1)} = [0, ...0, 1, -1, 0, 0, y+1]$. By Proposition 2 this new line is in $V(C)$. Also $[0, ..., 0, 1, -1, 0, 0, y+1]^{t_0(-1)} = [-1, 0, ..., 0, 1, -1, 0, 1, y+1] \in V(C)$, again by Proposition 2. Furthermore $[-1, 0, ...0, 0, 1, -1, 0, 1, y+1] \sim (0, ..., 0, 1, -1, 1, 1, y+1)$, so that this last point is in $V(C)$. Thus $(0, ..., 0, 1, -1, 1, 1, y)$ and $(0, ..., 0, 1, -1, 1, 1, y+1)$ are in $V(C)$. All we have just discussed is represented below, where all vertices are in $V(C)$:

$$(0, ..., 0, 1, -1, 1, 1, y) \sim [0, ..., 0, 1, -1, 1, 1, y] \xrightarrow{t_1(1)} [0, ..., 0, 1, -1, 0, 0, y+1] \xrightarrow{t_0(-1)}$$
$$[-1, 0, ..., 0, 1, -1, 0, 1, y+1] \sim (0, ..., 0, 1, -1, 1, 1, y+1).$$

In other words, (p') has two lifts to $D(k,q)$. Therefore by Proposition 3, π_C is a q-to-1 map.

Case 2: $k \equiv 0 \mod 4$, $k \geq 8$. Write $k = 4j$, $j \geq 2$. Let $(p') \in V(D(k-1,q))$ with $p_{4j-2} = p_{4j-3} = 1$ and zeroes elsewhere, i.e.,

$$(p') = (0, ..., 0, 1, 1, 0).$$

Clearly $\vec{a}(p') = \vec{0}$, so $(p') \in V(C')$ by the induction hypothesis. Since π_C is surjective there is $(p) \in V(C)$ with $(p)^\pi = (p')$, i.e., for some $y \in \mathbb{F}_q$,

$$(p) = (0, ..., 0, 1, 1, 0, y).$$

First suppose $y \neq 0$. Then

$$(p)^{m(a,b)} = (0, ..., 0, a^j b^j, a^j b^j, 0, a^j b^{j+1} y).$$

Clearly one can always choose $a, b \in \mathbb{F}_q \setminus \{0\}$ such that $ab = 1$ but $b \neq 1$. Then with this choice of a and b,

$$(p)^{m(a,b)} = (0, ..., 0, 1, 1, 0, by) \in V(C)$$

by Proposition 2. But $(0, ..., 0, 1, 1, 0, by) \neq (0, ..., 0, 1, 1, 0, y)$ since $y \neq 0$ and $b \neq 1$. Therefore (p') has two lifts to $D(k,q)$, and as before we are done.

So suppose $y = 0$, i.e.,

$$(p) = (0, ..., 0, 1, 1, 0, 0) \in V(C).$$

Then

$$(0)^{t_{4j-3}(1) t_{4j-2}(1)} = (0, ..., 0, 1, 0, 0, 0)^{t_{4j-2}(1)} = (p)$$

and $t_{4j-3}(1)t_{4j-2}(1) \in \mathrm{Stab}(C)$ by Proposition 2. Now let $(p') \in V(D(k-1,q))$ with $p_{4j-5} = p_{4j-4} = 1$ and zeroes elsewhere, i.e.,

$$(p') = (0, ..., 0, 1, 1, 0, 0, 0).$$

Clearly $\vec{a}(p') = \vec{0}$, so $(p') \in V(C')$ by the induction hypothesis. Since π_C is surjective there is $(p) \in V(C)$ with $(p)^\pi = (p')$, i.e., for some $y \in \mathbb{F}_q$,

$$(p) = (0, ..., 0, 1, 1, 0, 0, 0, y).$$

Since $t_0(1)$, $t_{4j-3}(1)t_{4j-2}(1) \in \mathrm{Stab}(C)$, we have

$$(p)^{t_0(1)t_{4j-3}(1)t_{4j-2}(1)} = (0, ..., 0, 1, 1, -1, -1, 0, y+1)^{t_{4j-3}(1)t_{4j-2}(1)} =$$

$$(0, ..., 0, 1, 1, 0, 0, 0, y+1) \in V(C).$$

So (p') has two lifts to $V(C)$, and π_C is a q-to-1 map by Proposition 3.

Case 3: $k \equiv 1 \mod 4$, $k \geq 9$. Write $k = 4j-3$, $j \geq 3$. Let $(p') \in V(D(k-1,q))$ with $p_{4j-5} = 1$ and zeroes elsewhere, i.e.,

$$(p') = (0, ..., 0, x, 0).$$

Clearly $\vec{a}(p') = \vec{0}$, so $(p') \in V(C')$ by the induction hypothesis. Since π_C is surjective there is $(p) \in V(C)$ with $(p)^\pi = (p')$, i.e., for some $y \in \mathbb{F}_q$,

$$(p) = (0, ..., 0, x, 0, y).$$

The reader may verify that (p) is stabilized by $t_0(x)t_{4j-3}(-x)$, so by Proposition 2, $t_0(x)t_{4j-3}(-x) \in \mathrm{Stab}(C)$. Again by Proposition 2, $t_0(x) \in \mathrm{Stab}(C)$, so that $t_{4j-3}(-x) \in \mathrm{Stab}(C)$ for any $x \in \mathbb{F}_q$. Thus $(0, ..., 0, -x) = (0)^{t_{4j-3}(-x)} \in V(C)$ and (0) has q distinct lifts to C. Thus π_C is q-to-1.

Case 4: $k \equiv 2 \mod 4$, $k \geq 10$. Choose $v \in V(D(k,q))$ with $\vec{a}(v) = \vec{0}$ and let $v' = v^\pi \in V(D(k-1,q))$. Then $\vec{a}(v') = \vec{0}$ (since the length of the invariant vector is now one less than before). Let w be any lift of v' to C. Then $\vec{a}(w) = \vec{0} = \vec{a}(v)$ and $w^\pi = v' = v^\pi$. This implies that $v = w$, as in the base case $k = 6$. Thus $v \in V(C)$.

□

In order to deal with the case $q = 4$, we will need an analog of Lemma 1. We begin by defining an invariant vector for $D(k,4)$. Its definition is very close to the one given in Section 2.1, the only difference being the presence of an extra coordinate. For $u \in V(k,4)$ and $t = \lfloor \frac{k+2}{4} \rfloor$, the invariant is given by

$$\vec{b} = \vec{b}(u) = \langle b_1(u), b_2(u), ..., b_t(u) \rangle,$$

where $b_i = a_i$ for all $i \geq 2$ (see Section 2.1) and

$$\begin{aligned} b_1((p)) &= p_1 p_2 + p_3 + p_4^2, \\ b_1([l]) &= l_1 l_2 + l_3^2 + l_4. \end{aligned}$$

The following statement is a version of Proposition 1 for $q = 4$. Though it is weaker than this proposition (see Remark at the end of this section), it is sufficient for our purposes.

Lemma 2. *Let u be in the component of $D(k,4)$ containing (0). Then $\vec{b}(u) = \vec{0}$.*

Proof. Suppose $(p) \in V(C)$ with $\vec{b}((p)) = \vec{0}$. Then

$$(p) = (p_1, p_2, p_3, p_4, ...) \sim [l_1, p_2 + p_1 l_1, p_3 + p_1 p_2 + p_1^2 l_1, p_4 + p_2 l_1, ...] = [l].$$

Proposition 1 gives that $b_i([l]) = b_i((p)) = 0$ for all $i \geq 2$. By assumption $b_1((p)) = p_1 p_2 + p_3 + p_4^2 = 0$. Since we are in characteristic 2 and $a^4 = a$ for any $a \in \mathbb{F}_4$,

$$b_1([l]) = l_1(p_2 + p_1 l_1) + (p_3 + p_1 p_2 + p_1^2 l_1)^2 + (p_4 + p_2 l_1) =$$

$$p_1^2 p_2^2 + p_3^2 + p_4 = (p_1 p_2 + p_3 + p_4^2)^2 = 0.$$

Thus $\vec{b}([l]) = \vec{0}$. Similarly, one shows that if $[l] \in V(C)$ with $\vec{b}([l]) = \vec{0}$ and $(p) \sim [l]$, then $\vec{b}((p)) = 0$. Therefore if a vertex in C has invariant $\vec{0}$, so do all of its neighbors. Since C is connected and $\vec{a}(0) = \vec{0}$, all vertices in C must have invariant $\vec{0}$. □

We are ready to state and prove the analog of Lemma 1 for $q = 4$.

Lemma 3. *Let $k \geq 4$. If $v \in V(D(k,4))$ satisfies $\vec{b}(v) = 0$ then $v \in V(C)$.*

Proof. Our proof imitates the one of Lemma 1, and we just sketch its main steps. We know (see, e.g., [9]) that $D(2,4)$ and $D(3,4)$ are both connected.

We use induction on k. The base case is $k = 4$. Let $v \in V(D(4,4))$ with $\vec{b}(v) = \vec{0}$, and let $v' = v^\pi \in V(3,4)$. Since $D(3,4)$ is connected, so $v' \in C' = D(3,4)$. Since π_C is surjective, there is $w \in V(C)$ such that $w^\pi = v' = v^\pi$. Since the fourth coordinate of any vertex u is uniquely determined by its initial three coordinates and $\vec{a}(u)$ (note $x \mapsto x^2$ is an automorphism of $\mathbb{F}_4$), we have $v = w \in V(C)$.

We proceed through the cases as in the proof of Lemma 1. Anytime a point (p') is defined, we have $\vec{b}(p') = \vec{0}$. By the induction hypothesis, this gives $(p') \in V(C')$. We already know that $\vec{a}(p') = \vec{0}$, so we need only check that $b_1(p') = 0$. In all cases, it is easy to see that it implies either $p_1 = p_2 = p_3 = p_4 = 0$ or $p_3 = p_4 = 1$, yielding $b_1(p') = 0$ and hence $\vec{b}(p') = \vec{0}$. □

Now we are ready to prove Theorem 1.

Proof of Theorem 1: (i) We have already mentioned (see the beginning of the proof of Lemma 1) that for $2 \leq k \leq 5$ and $q > 4$ graphs $D(k,q)$ are connected. Hence the statement is correct in these cases. We also remind the reader that for all $k \geq 2$ and prime powers q, $D(k,q)$ is edge-transitive ([1]), hence all its components are isomorphic.

Let $k \geq 6$. Combining Lemma 1 and Proposition 1 we have that $v \in V(C)$ if and only if $\vec{a}(v) = \vec{0}$. To determine the number of points in C, we need only determine how many solutions there are to the equation $\vec{a}((p)) = \vec{0}$, or equivalently to the system of equations $a_r = 0$ for every $r \geq 2$. To satisfy $a_2 = 0$, we arbitrarily choose $p_1, ..., p_5$ and solve for p_6. For each subsequent equation $a_r = 0$, we arbitrarily choose p_{4r-3}, p_{4r-4} and p_{4r-5}, and then solve it for p_{4r-2}. Thus we need to choose 5 point coordinates in the first equation, and another 3 in each of the $t-2$ others. At this point there are $k-(4t-2)$ coordinates of (p) left "free", namely $p_{4t-1}, ..., p_k$; each may be assigned a value arbitrarily. Thus the number of points in C is

$$q^{5+3(t-2)+k-(4t-2)} = q^{k-t+1}.$$

Since the total number of points in $D(k,q)$ is q^k, and all its components are isomorphic, we have $c(D(k,q)) = \frac{q^k}{q^{k-t+1}} = q^{t-1}$.

(ii) The proof of this part follows the one for part (i). The only change is that Lemmas 2 and 3 must be used instead of Lemma 1. □

We now proceed by showing that the invariant vector of a vertex characterizes the component containing the vertex, as was shown for q odd in [4]. The proof is short, and we include it here for completeness.

Corollary 1. *Let $k \geq 6$ and $q > 4$. Then $\vec{a}(u) = \vec{a}(v)$ if and only if $C(u) = C(v)$.*

Proof. Let $t = \lfloor \frac{k+2}{4} \rfloor$, and let $C(v)$ be the component of $D(k, q)$ containing the vertex v. Let X be the set of components of $D(k, q)$ and define the mapping $f : X \mapsto \mathbb{F}_q^{t-1}$ via $f(C(v)) = \vec{a}(v)$. From Proposition 1 we know that f is well defined, i.e., $C(u) = C(v)$ implies $\vec{a}(u) = \vec{a}(v)$. By Theorem 1, $|X| = q^{t-1}$ $(= |\mathbb{F}_q^{t-1}|)$, so that f is bijective. Thus $C(u) = C(v)$ whenever $\vec{a}(u) = \vec{a}(v)$. □

Remark 1. The analog of Corollary 1 does not hold for $q = 4$. The reason for this is the presence of the special first coordinate in the invariant.

Indeed, let ω be a primitive element for $\mathbb{F}_4$. Then $(p) = (0, 0, \omega, 0, ..., 0) \sim [0, 0, \omega, 0, ..., 0] = [l]$ in $D(k, 4)$, but

$$\vec{b}((p)) = \langle \omega, 0, ..., 0 \rangle \neq \langle \omega^2, 0, ..., 0 \rangle = \vec{b}([l]).$$

Acknowledgement. We are grateful to Andrew Woldar for his useful comments on the original version of this paper.

References

[1] F. Lazebnik, V. A. Ustimenko, Explicit construction of graphs with an arbitrary large girth and of large size, *Discrete Appl. Math.* 60 (1995), 275–284.

[2] F. Lazebnik, V. A. Ustimenko, A. J. Woldar, A new series of dense graphs of large girth, *Rutcor Research Report RRR* 99-93, December 1993.

[3] F. Lazebnik, V. A. Ustimenko, A. J. Woldar, A new series of dense graphs of high girth, *Bulletin of the AMS* 32 (1) (1995), 73–79.

[4] F. Lazebnik, V.A. Ustimenko, A.J. Woldar, A characterization of the components of the graphs $D(k, q)$, *Discrete Math.* 157 (1996), 271–283.

[5] F. Lazebnik, A.J. Woldar, General properties of families of graphs defined by some systems of equations, *J. Graph Theory*, 38 (2) (2001), 65-86.

[6] A. Lubotzky, R. Phillips, and P. Sarnak, Ramanujan graphs, *Combinatorica* 8 (3) (1988), 261–277.

[7] G.A. Margulis, Explicit group-theoretical construction of combinatorial schemes and their application to design of expanders and concentrators, *J. Probl. Inform. Transmission* 24 (1988), 39–46.

[8] A. Schliep, The software GADAR and its application to extremal graph theory, Congr. Numer. 104 (1994), 193–203.

[9] R. Viglione, Properties of some algebraically defined graphs, Ph.D. Thesis, University of Delaware, 2002.

Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA
E-mail address: `lazebnik@math.udel.edu`

Department of Mathematics and Computer Science, Kean University, Union, NJ 07083, USA
E-mail address: `rviglion@kean.edu`