SOME FAMILIES OF GRAPHS, HYPERGRAPHS AND DIGRAPHS DEFINED BY SYSTEMS OF EQUATIONS: A SURVEY

FELIX LAZEBNIK AND SHUYING SUN

Abstract. The families of graphs defined by a certain type of system of equations over commutative rings have been studied and used since 1990s, and the only survey of these studies appeared in 2001. In this paper we mostly concentrate on the related results obtained in the last fifteen years, including generalizations of these constructions to digraphs and hypergraphs.

We also offer a unified elementary (i.e., Lie algebra free) exposition of the properties of a family of graphs known as $D(k, q)$. The original results on these graphs appeared in several papers, with the notations reflecting their origins in Lie algebras. The components of graphs $D(k, q)$ provide the best known general lower bounds for the number of edges in graphs of given order and given girth (the length of a shortest cycle).

The paper also contains several open problems and conjectures.

1. Introduction

One goal of this survey is to summarize results concerning certain families of graphs, hypergraphs and digraphs defined by certain systems of equations, concentrating on the results which appeared during the last fifteen years. Another goal is to provide a comprehensive treatment of, probably, the best known family of such graphs, denoted by $D(k, q)$, including most of related (and revised) proofs. The original results on these graphs were scattered among many papers, with the notations not necessarily consistent and reflecting the origins of these graphs in Lie algebras. It is our hope that this new exposition will make it easier for those who wish to understand the methods, continue research in the area or find new applications.

For a summary of related results which appeared before 2001, see Lazebnik and Woldar [71]. One important feature of that article was an attempt of setting simpler notation and presenting results in greater generality. The current presentation is based on that paper. Let us begin with a quote from [71] (with updated reference labels):

> In the last several years some algebraic constructions of graphs have appeared in the literature. Many of these constructions were motivated by problems from extremal graph theory, and, as a consequence, the graphs obtained were primarily of interest in the context of a particular extremal problem. In the case of the graphs

Date: September 14, 2016.

Key words and phrases. Girth, embedded spectra, lift of a graph, cover of a graph, edge-decomposition, isomorphism, generalized polygons, digraph, hypergraph, degenerate Turán-type problems.

> appearing in [103], [58]–[65], [34], the authors recently discovered that they exhibit many interesting properties *beyond* those which motivated their construction. Moreover, these properties tend to remain present even when the constructions are made far more general. This latter observation forms the motivation for our paper.

The research conducted since the appearance of [71] was done in two directions: attempting to apply specializations of general constructions to new problems, and trying to strengthen some old results.

Before proceeding, we establish some notation; more will be introduced later. The missing graph-theoretic definitions can be found in Bollobás [8]. Most graphs we consider in this paper are undirected, and without loops or multiple edges. Sometimes loops will be allowed, in which case we will state it. Given a graph Γ, we denote the vertex set of Γ by $V(\Gamma)$ and the edge set by $E(\Gamma)$. Elements of $E(\Gamma)$ will be written as xy, where $x, y \in V(\Gamma)$ are the corresponding adjacent vertices. For a vertex v of Γ, let $N(v) = N_\Gamma(v)$ denote its neighborhood in Γ.

Though most of the graphs we plan to discuss are defined over finite fields, many of their properties hold over commutative rings, and this is how we proceed. Let R be an arbitrary commutative ring, different from the zero ring, and with multiplicative identity. We write R^n to denote the Cartesian product of n copies of R, and we refer to its elements as *vectors*. For $q = p^e$, with $p \geq 2$ and prime, let $\mathbb{F}_q$ denote the field of q elements.

The paper is organized as follows. In Section 2 we go over the main constructions for graphs, and their general properties are discussed in Section 3. In Section 4 we discuss various applications of the specialization of constructions from Section 2, including recent results on similarly constructed digraphs. Section 5 deals with constructions for hypergraphs. In Section 6 we present a comprehensive treatment of graphs $D(k, q)$, including revised proofs of the main old results, and survey new results. In Section 7 we mention some applications of graphs $D(k, q)$, and we conclude by a brief discussion on the related work in coding theory and cryptography in Section 8.

2. Main Constructions

2.1. **Bipartite version.** Let $f_i : R^{2i-2} \to R$, $2 \leq i \leq n$, be arbitrary functions on R of two, four, ..., $2n-2$ variables. We define the bipartite graph $B\Gamma_n = B\Gamma(R; f_2, \ldots, f_n)$, $n \geq 2$, as follows. The set of vertices $V(B\Gamma_n)$ is the disjoint union of two copies of R^n, one denoted by P_n and the other by L_n. Elements of P_n will be called *points* and those of L_n *lines*. In order to distinguish points from lines we introduce the use of parentheses and brackets: if $a \in R^n$, then $(a) \in P_n$ and $[a] \in L_n$. We define edges of $B\Gamma_n$ by declaring point $(p) = (p_1, p_2, \ldots, p_n)$ and line $[l] = [l_1, l_2, \ldots, l_n]$ adjacent if and only if the following $n-1$ relations on their coordinates hold:

$$\begin{aligned} p_2 + l_2 &= f_2(p_1, l_1) \\ p_3 + l_3 &= f_3(p_1, l_1, p_2, l_2) \\ &\ldots \quad \ldots \\ p_n + l_n &= f_n(p_1, l_1, p_2, l_2, \ldots, p_{n-1}, l_{n-1}) \end{aligned} \tag{2.1}$$

For a function $f_i : R^{2i-2} \to R$, we define $\overline{f_i} : R^{2i-2} \to R$ by the rule

$$\overline{f_i}(x_1, y_1, \ldots, x_{i-1}, y_{i-1}) = f_i(y_1, x_1, \ldots, y_{i-1}, x_{i-1})$$

We call f_i *symmetric* if the functions f_i and $\overline{f_i}$ coincide. The following is trivial to prove.

Proposition 1. *Graphs $B\Gamma(R; f_2, \ldots, f_n)$ and $B\Gamma(R; \overline{f_2}, \ldots, \overline{f_n})$ are isomorphic, an explicit isomorphism being given by $\varphi : (a) \leftrightarrow [a]$.*

We now define our second fundamental family of graphs for which we require that all functions be symmetric.

2.2. **Ordinary version.** Let $f_i : R^{2i-2} \to R$ be symmetric for all $2 \le i \le n$. We define $\Gamma_n = \Gamma(R; f_2, \ldots, f_n)$ to be the graph with vertex set $V(\Gamma_n) = R^n$, where distinct vertices (vectors) $a = \langle a_1, a_2, \ldots, a_n \rangle$ and $b = \langle b_1, b_2, \ldots, b_n \rangle$ are adjacent if and only if the following $n-1$ relations on their coordinates hold:

$$\begin{aligned} a_2 + b_2 &= f_2(a_1, b_1) \\ a_3 + b_3 &= f_3(a_1, b_1, a_2, b_2) \\ &\ldots \quad \ldots \\ a_n + b_n &= f_n(a_1, b_1, a_2, b_2, \ldots, a_{n-1}, b_{n-1}) \end{aligned} \tag{2.2}$$

For the graphs Γ_n our requirement that all functions f_i be symmetric is necessary to ensure that adjacency be symmetric. Without this condition one obtains not graphs, but digraphs. It is sometimes beneficial to allow loops in Γ_n, i.e., considering $a_i = b_i$ for all i and satisfying (2.2).

2.3. **Special induced subgraphs.** Let $B\Gamma_n$ be the bipartite graph defined in Section 2.1, and let A and B be arbitrary subsets of R. We set

$$\begin{aligned} P_{n,A} &= \{(p) = (p_1, p_2, \ldots, p_n) \in P_n \mid p_1 \in A\} \\ L_{n,B} &= \{[l] = [l_1, l_2, \ldots, l_n] \in L_n \mid l_1 \in B\} \end{aligned}$$

and define $B\Gamma_n[A, B]$ to be the subgraph of $B\Gamma_n$ induced on the set of vertices $P_{n,A} \cup L_{n,B}$. Since we restrict the range of only the first coordinates of vertices of $B\Gamma_n$, graph $B\Gamma_n[A, B]$ can alternately be described as the bipartite graph with bipartition $P_{n,A} \cup L_{n,B}$ and adjacency relations as given in (2.1). This is a valuable observation as it enables one to "grow" the graph $B\Gamma_n[A, B]$ directly, without ever having to construct $B\Gamma_n$. In the case where $A = B$, we shall abbreviate $B\Gamma_n[A, A]$ by $B\Gamma_n[A]$.

Similarly, for arbitrary $A \subseteq R$ we define $\Gamma_n[A]$ to be the subgraph of Γ_n induced on the set $V_{n,A}$ of all vertices having respective first coordinate from A. Again, explicit construction of Γ_n is not essential in constructing $\Gamma_n[A]$; the latter graph is obtained by applying the adjacency relations in (2.2) directly to $V_{n,A}$. (Note that when $A = R$ one has $B\Gamma_n[R] = B\Gamma_n$ and $\Gamma_n[R] = \Gamma_n$.)

3. General properties of graphs $B\Gamma_n$ and Γ_n

The goal of this section is to state the properties of $B\Gamma_n = B\Gamma(R; f_2, \ldots, f_n)$ and $\Gamma_n = \Gamma(R; f_2, \ldots, f_n)$, which are *independent* of the choice of n, R, and the functions $f_2, \ldots, f_n$. Specializing these parameters, one can obtain some additional properties of the graphs. All proofs can be found in [71] or references therein, and

we omit them, with the exception of Theorem 1 below. Though trivial, it is of utmost importance for understanding the graphs.

3.1. **Degrees and neighbor-complete colorings.** One of the most important properties of graphs $B\Gamma_n$ and Γ_n defined in the previous section is the following. In the case of Γ_n we do allow loops, and assume that a loop on a vertex adds 1 to the degree of the vertex.

Theorem 1. *For every vertex v of $B\Gamma_n$ or of Γ_n, and every $\alpha \in R$, there exists a unique neighbor of v whose first coordinate is α.*

If $|R| = r$, all graphs $B\Gamma_n$ or Γ_n are r-regular. If 2 is a unit in R, then Γ_n contains exactly r loops.

Proof. Fix a vertex $v \in V(B\Gamma_n)$, which we may assume is a point $v = (a) \in P_n$ (if $v \in L_n$, the argument is similar). Then for any $\alpha \in R$, there is a unique line $[b] \in L_n$ which is adjacent to (a) and for which $b_1 = \alpha$. Indeed, with respect to the unknowns b_i the system (2.1) is triangular, and each b_i is uniquely determined from the values of $a_1, \dots, a_i, b_1, \dots b_{i-1}$, $2 \le i \le n$.

This implies that if $|R| = r$, then both $B\Gamma_n$ and Γ_n are r-regular. A vertex $a \in V(\Gamma_n)$ has a loop on it if and only if it is of the form $\langle a_1, a_2, \dots, a_n\rangle$, where

$$a_i = \frac{1}{2} f_i(a_1, a_1, \dots, a_{i-1}, a_{i-1}), \;\; 2 \le i \le n$$

Hence, there are exactly r loops. Erasing them we obtain a simple graph with r vertices of degree $r-1$ and $r^n - r$ vertices of degree r. □

Based on this theorem, it is clear that each of the graphs $B\Gamma_n$ and Γ_n allows a vertex coloring by all elements of R such that the neighbors of every vertex are colored in all possible colors: just color every vertex by its first coordinate. These colorings are never proper, as the color of a vertex is the same as the color of exactly one of its neighbors. Such colorings were introduced by Ustimenko in [94] under the name of "parallelotopic" and further explored by Woldar [105] under the name of "rainbow", and in [71] under the name of "neighbor-complete colorings", which we adopt here. In [94] some group theoretic constructions of graphs possessing neighbor-complete colorings are given; in [105] purely combinatorial aspects of such colorings are considered. Non-trivial examples of graphs possessing neighbor-complete colorings are not easy to construct. Remarkably, graphs $B\Gamma_n$ and Γ_n always admit them.

Similar statements, with obvious modifications, hold for graphs $B\Gamma_n[A, B]$ and $\Gamma_n[A]$, and we leave such verification to the reader.

3.2. **Covers and lifts.** The notion of a covering for graphs is analogous to the one in topology. We call $\overline{\Gamma}$ a *cover* of graph Γ (and we write $\overline{\Gamma} \to \Gamma$) if there exists a surjective mapping $\theta : V(\overline{\Gamma}) \to V(\Gamma)$, $\overline{v} \mapsto v$, which satisfies the two conditions:

(i) θ preserves adjacencies, i.e., $uv \in E(\Gamma)$ whenever $\overline{u}\,\overline{v} \in E(\overline{\Gamma})$;
(ii) For any vertex $\overline{v} \in V(\overline{\Gamma})$, the restriction of θ to $\overline{N}(\overline{v})$ is a bijection between $\overline{N}(\overline{v})$ and $N(v)$.

Note that our condition (ii) ensures that θ is degree-preserving; in particular, any cover of an r-regular graph is again r-regular. If $\overline{\Gamma}$ is a cover of Γ, we also say that $\overline{\Gamma}$ is a *lift* of Γ.

For $k < n$, denote by $\eta = \eta(n,k)$ the mapping $R^n \to R^k$ which projects $v \in R^n$ onto its k initial coordinates, viz.

$$v = \langle v_1, v_2, \ldots, v_k, \ldots v_n \rangle \mapsto v = \langle v_1, v_2, \ldots, v_k \rangle$$

Clearly, η provides a mapping $V(\Gamma_n) \to V(\Gamma_k)$, and its restriction to $V_{n,A} = A \times R^{n-1}$ gives mappings $V(\Gamma_n[A]) \to V(\Gamma_k[A])$. In the bipartite case, we further impose that η preserves vertex type, i.e. that

$$(p) = (p_1, p_2, \ldots, p_k, \ldots p_n) \mapsto (p) = (p_1, p_2, \ldots, p_k)$$
$$[l] = [l_1, l_2, \ldots, l_k, \ldots l_n] \mapsto [l] = [l_1, l_2, \ldots, l_k]$$

Here, η induces, in obvious fashion, the mappings $V(B\Gamma_n[A]) \to V(B\Gamma_k[A])$.

In what follows, the functions f_i $(2 \le i \le n)$ for the graphs $B\Gamma_n[A]$ are assumed to be arbitrary, while those for $\Gamma_n[A]$, continue, out of necessity, to be assumed symmetric. The proof of the following theorem is easy and can be found in [71].

Theorem 2. *For every $A \subseteq R$, and every k, n, $2 \le k < n$, $B\Gamma_n[A] \to B\Gamma_k[A]$. $\Gamma_n[A] \to \Gamma_k[A]$ if and only if no edge of $\Gamma_n[A]$ projects to a loop of $\Gamma_k[A]$.*

Remark 1. If a graph Γ contains cycles, its girth, denoted by $girth(\Gamma)$, is the length of its shortest cycle. One important consequence of Theorem 2, particularly amenable to girth related Turán type problems in extremal graph theory, is that the girth of a graph is not greater than the girth of its cover. In particular, the girth of $B\Gamma_n$ or Γ_n is a non-decreasing function of n. More precisely,

$$girth(B\Gamma(R; f_2, \ldots, f_k)) \le girth(B\Gamma(R; f_2, \ldots, f_k \ldots, f_n)),$$

and similarly for graphs $B\Gamma_n[A]$ or $\Gamma_n[A]$.

3.3. **Embedded spectra.** The spectrum $spec(\Gamma)$ of a graph Γ is defined to be the multiset of eigenvalues of its adjacency matrix. One important property of covers discussed in Section 3.2 is that the spectrum of any graph embeds (as a multiset, i.e., taking into account also the multiplicities of the eigenvalues) in the spectrum of its cover. This result can be proven in many ways, for example as a consequence of either Theorem 0.12 or Theorem 4.7, both of Cvetković [21]. As an immediate consequence of this fact and Theorem 2, we obtain

Theorem 3. *Assume R is finite and let $A \subseteq R$. Then for each k, n, $2 \le k < n$,*

$$spec(B\Gamma_k[A]) \subseteq spec(B\Gamma_n[A])$$

For graphs $\Gamma_n[A]$, one has $spec(\Gamma_k[A]) \subseteq spec(\Gamma_n[A])$ provided no edge of $\Gamma_n[A]$ projects to a loop of $\Gamma_k[A]$.

3.4. **Edge-decomposition of K_n and $K_{m,m}$.** Let Γ and Γ' be graphs. An *edge-decomposition of Γ by Γ'* is a collection $\mathcal{C}$ of subgraphs of Γ, each isomorphic to Γ', such that $\{E(\Lambda) \mid \Lambda \in \mathcal{C}\}$ is a partition of $E(\Gamma)$.

We also say in this case that Γ' *decomposes* Γ. It is customary to refer to the subgraphs Λ in $\mathcal{C}$ as *copies* of Γ', in which case one may envision an edge-decomposition of Γ by Γ' as a decomposition of Γ into edge-disjoint copies of Γ'.

As usual, let K_n denote the complete graph on n vertices, and $K_{m,n}$ the complete bipartite graph with partitions of sizes m and n. The questions of decomposition of K_n or $K_{m,n}$ into copies of a graph Γ' are classical in graph theory and have been of interest for many years. In many studied cases Γ' is a matching, or a cycle, or a complete graph, or a complete bipartite graph, i.e., a graph with a rather simple

structure. In contrast, the structure of $B\Gamma_n$ or Γ_n, is usually far from simple. In this light the following theorem from [71] is a bit surprising.

Theorem 4. *Let $|R| = r$. Then $B\Gamma_n$ decomposes K_{r^n,r^n}.*
If 2 is a unit in R, then Γ_n (with no loops) decomposes K_{r^n}.

This result was motivated by a question of Thomason [90], who asked whether graph $D(n, q)$ (which will be defined later in this paper) edge-decomposes K_{q^n,q^n}.

3.5. **Automorphisms.** What are the automorphism groups of graphs $B\Gamma_n$? Though we cannot name any particular non-trivial automorphism of these graphs for arbitrary functions $f_2, \dots, f_n$, the automorphism group can be quite rich for some special choices of functions $f_2, \dots, f_n$.

In the case when every function f_i depends on p_1 and l_1 only, graphs $B\Gamma_n$ always contain special automorphisms. Let G denote the additive group of R, and G^{n-1} denote the direct product of $n-1$ copies of G. It is easy to see that for any $v = \langle v_2, \dots, v_n\rangle \in R^{n-1}$, the map $g_v : V(B\Gamma_n) \to V(B\Gamma_n)$ given by

$$(p) = (p_1, p_2, \dots, p_n) \mapsto (p_1, p_2 + v_2, \dots, p_n + v_n)$$
$$[l] = [l_1, l_2, \dots, l_n] \mapsto [l_1, l_2 - v_2, \dots, l_n - v_n]$$

is an automorphism of $B\Gamma_n$, and that the following theorem holds.

Theorem 5. *If each function f_i, $i = 2, \dots, n$, in the definition of $B\Gamma_n$ depends on p_1 and l_1 only, the automorphism group $Aut(B\Gamma_n)$ contains a subgroup isomorphic to G^{n-1}.*

We would like to end this section with a problem.

Problem 1. *Generalize the constructions of this section to the case where R is an abelian group, and investigate the properties of the obtained graphs.*

4. Applications

In this section we survey some applications of graphs $B\Gamma_n$ and Γ_n, and of similarly constructed hypergraphs and digraphs. In most instances, the graphs considered are specializations of $B\Gamma_n$ and Γ_n, with R taken to be the finite field $\mathbb{F}_q$ and the functions f_i chosen in such a way as to ensure the resulting graphs having other properties. We also mention some open problems and conjectures.

4.1. **Wenger graphs.** Specializing R to $\mathbb{F}_q$, in $B\Gamma_n$, and taking $f_k = p_1^{k-1}l_1$, $2 \le k \le m+1$, one obtains graphs $W_m(q)$, which are called *Wenger graphs*. Graphs isomorphic to $W_m(q)$ were introduced in [103] by Wenger in the context of extremal graph theory. Their generalization was rediscovered by Lazebnik and Ustimenko in [58], and Wenger graphs have received a considerable attention since then. The presentation of $W_m(q)$ as above is due to Lazebnik and Viglione [67]. For the related results, see Viglione [100, 101], [67], Futorny and Ustimenko [37], Shao, He and Shan [84], Li, Lu and Wang [72]. For a minisurvey of Wenger graphs (up to 2013), see Cioăba, Lazebnik and Li [15]. In the same paper, the spectra of Wenger graphs was determined, extending the cases of $m = 2, 3$ from [72], and the result implies that the graphs are expanders for every fixed m and large q. The results of [84] concerning cycle lengths in $W_m(q)$ were extended by Wang, Lazebnik and Thomason in [102]. Alexander, Lazebnik and Thomason, see [2], showed that

for fixed m and large q, Wenger graphs are hamiltonian. The automorphism group of Wenger graphs was determined by Cara, Rottey and Van de Voorde in [14].

Conjecture 1. ([102]) *For every $m \geq 2$, and every prime power q, $q \geq 3$, $W_m(q)$ contains cycles of length $2k$, where $4 \leq k \leq q^{m+1}$ and $k \neq 5$.*

In [13], Cao, Lu, Wan, L.-P. Wang and Q. Wang, considered the generalized Wenger graphs $B\Gamma_m(\mathbb{F}_q; f_2, \ldots, f_{m+1})$, with $f_k = g_k(p_1)l_1$, $2 \leq k \leq m+1$, where $g_k \in \mathbb{F}_q[X]$ and the map $\mathbb{F}_q \to \mathbb{F}_q^{m+1}$, $u \mapsto (1, g_2(u), \ldots, g_{m+1}(u))$ is injective. An important particular case of these graphs is obtained when $g_k(X) = X^{p^{k-2}}$, $2 \leq k \leq m+1$. The authors call these graphs the *linearized Wenger graphs* $L_m(q)$, and they determine their girth, diameter and the spectrum. For $q = p^e$, the results imply that the graphs $L_e(q)$ are expanders. It follows from [2] that for a fixed e and large p, graphs $L_e(p^e)$ are hamiltonian.

Problem 2. *Determine the lengths of cycles in the linearized Wenger graph $L_m(q)$.*

4.2. **Generalized polygons.** A *generalized k-gon* of order (q, q), for $k \geq 3$ and $q \geq 2$, denoted Π_q^k, is a $(q+1)$-regular bipartite graph of girth $2k$ and diameter k. It is easy to argue that in such a graph each partition contains $n_q^k = q^{k-1} + q^{k-2} + \ldots + q + 1$ vertices (for information on generalized polygons, see, e.g., Van Maldeghem [98], Thas [87] or Brouwer, Cohen and Neumaier [10]). It follows from a theorem by Feit and Higman [31] that if Π_q^k exists, then $k \in \{3, 4, 6\}$. For each of these k, Π_q^k are known to exist only for arbitrary prime power q. In the case $k = 3$, the graph is better known as the point-line incidence graph of a projective plane of order q; for $k = 4$ – as the generalized quadrangle of order q, and for $k = 6$, as the generalized hexagon of order q. Fixing an edge in graph Π_q^k, one can consider a subgraph in Π_q^k induced by all vertices at the distance at least $k-1$ from the edge. It is easy to argue that the obtained graph is q-regular, has girth $2k$ (for $q \geq 4$) and diameter $2(k-1)$ (for $q \geq 4$). We refer to this graph as a *biaffine part of* Π_q^k (also known as an affine part). Hence, a biaffine part is a q-regular induced subgraph of Π_q^k having q^{k-1} vertices in each partition, and deleting all edges of a biaffine part results in a spanning tree of Π_q^k with each inner vertex of degree $q+1$.

If Π_q^k is edge transitive, then all its biaffine parts are isomorphic and we can speak about *the* biaffine part, and denote it by Λ_q^k. Some classical generalized polygons are known to be edge-transitive. It turns out that their biaffine parts can be represented as graphs $B\Gamma_n$:

$$\Lambda_q^3 \quad \text{as} \quad B\Gamma_2(\mathbb{F}_q; p_1 l_1) \tag{4.1}$$

$$\Lambda_q^4 \quad \text{as} \quad B\Gamma_3(\mathbb{F}_q; p_1 l_1, p_1 l_2) \cong B\Gamma_3(\mathbb{F}_q; p_1 l_1, p_1 l_1^2) \tag{4.2}$$

$$\Lambda_q^6 \quad \text{as} \quad B\Gamma_5(\mathbb{F}_q; p_1 l_1, p_2 l_1, p_3 l_1, p_2 l_3 - p_3 l_2) \tag{4.3}$$

We wish to mention that many other representations of these graphs are possible, and some are more convenient than others when we study particular properties of the graphs. The description of Λ_q^6 above is due to Williford [104].

Presentations of Λ_q^k in terms of systems of equations appeared in the literature in different ways. Firstly as an attempt to coordinatize incidence geometries Π_q^k, see Payne [77], [98] and references therein.

Another approach, independent of the previous, is based on the work of Ustimenko [91, 92, 93], where incidence structures in group geometries, used historicaly first to present generalized polygons, were described as relations in the corresponding affine Lie algebras. Some details and examples of related computations can be found in [58], in Ustimenko and Woldar [97], in Woldar [106], and in more recent work by Terlep and Williford [88].

The descriptions of biaffine parts Λ_q^k of the classical k-gons Π_q^k via graphs $B\Gamma_{k-1}$ above, suggested to generalize the latter to the values of k for which no generalized k-gons exist. The property of growing girth of graphs $B\Gamma_n$ that we mentioned in Remark 1 of Section 3.2 turned out to be fundamental for constructing families of dense graphs without cycles of certain lengths, and in particular, of large girth. We describe these application in Section 5.4.

Graphs $B\Gamma_n$ can also be used in the attempts of constructing new generalized k-gons ($k \in \{3, 4, 6\}$) via the following logic: first construct a $B\Gamma_{k-1}$ graph of girth $2k$ and diameter $2(k-1)$, and then try to "attach a tree" to it. In other words, construct a Λ_{k-1} like graph not isomorphic to one coming from Π_q^k, and then extend it to a generalized k-gon. For $k = 3$, the extension will always work. Of course, this approach has an inherited drawback, as graphs $B\Gamma_{k-1}$ always have a restriction on their automorphism group (see Section 3.5).

Lazebnik and Thomason used this approach in [57] to construct planes of order 9 and, possibly new planes of order 16. The planes they constructed all possessed a special group of automorphisms isomorphic to the additive group of the field, but they were not always translation planes. Of the four planes of order 9, three admit the additive group of the field $\mathbb{F}_9$ as a group of translations, and the construction yielded all three. The known planes of order 16 comprise four self- dual planes and eighteen other planes (nine dual pairs); of these, the method gave three of the four self-dual planes and six of the nine dual pairs, including the sporadic (not translation) plane of Mathon. An attempt to construct new generalized quadrangles is discussed in the next section.

4.3. **Monomial graphs and generalized quadrangles.** When all functions f_i are monomials of two variables, we call the graph $B\Gamma_n(\mathbb{F}_q; f_2, \dots, f_n)$, a *monomial graph*. These graphs were first studied in Viglione [100] and in Dmytrenko [22]. Let $B(q; m, n) = B\Gamma_2(\mathbb{F}_q; X^m Y^n)$. For m, n fixed and q sufficiently large, the isomorphism problem for graphs $B(q; m, n)$ was solved in [100], and for all m, n, q, in Dmytrenko, Lazebnik and Viglione [23].

Theorem 6. ([23]) *Let m, n, m', n' be positive integers and let q, q' be prime powers. The graphs $B(q; m, n)$ and $B(q'; m', n')$ are isomorphic if and only if $q = q'$ and $\{\gcd(m, q-1), \gcd(n, q-1)\} = \{\gcd(m', q-1), \gcd(n', q-1)\}$ as multisets.*

It is easy to argue, see [23], that every 4-cycle-free graph of the form $B(q; m, n)$, is isomorphic to $B(q; 1, 1)$ $(= B\Gamma(\mathbb{F}_q; XY))$, and so is isomorphic to the biaffine part of the point-line incidence graph of $PG(2, q)$.

An analogous statement in dimension three is less clear. For each odd prime power q only two non-isomorphic generalized quadrangles of order q, viewed as finite geometries, are known. They are usually denoted by $W(q)$ and $Q(4, q)$, and it is known that one is the dual of the other, see Benson [4]. This means that viewed as bipartite graphs they are isomorphic. For odd prime powers q, the graph

$B\Gamma_3(\mathbb{F}_q; XY, XY^2)$, which has girth 8, is the biaffine part of $W(q)$. Just as a 4-cycle-free graph $B\Gamma_2(\mathbb{F}_q; f_2)$ gives rise to a projective plane, a three-dimensional 4- and 6-cycle-free graph $B\Gamma(\mathbb{F}_q; f_2, f_3)$ may give rise to a generalized quadrangle. This suggests to study the existence of such graphs, and it is reasonable to begin to search for them in the 'vicinity' of graph $B\Gamma_3(\mathbb{F}_q; XY, XY^2)$, by which we mean among the monomial graphs. Another motivation to study monomial graphs in this context is the following. For q even, contrary to the two-dimensional case, the monomial graphs can lead to a variety of non-isomorphic generalized quadrangles, see Payne [78], [98], Glynn [39, 40], Cherowitzo [17]. It is conjectured in [39] that known examples of such quadrangles represent all possible ones. The conjecture was checked by computer for all $e \leq 28$ in [40], and for all $e \leq 40$, by Chandler [16] (remember that $q = 2^e$ in this case).

The study of monomial graphs of girth eight for odd q began in Dmytrenko [22], and continued in Dmytrenko, Lazebnik and Williford [24], and in Kronenthal [51]. All results in these papers suggested that that for q odd, every monomial graph $B\Gamma_3(\mathbb{F}_q; f_2, f_3)$ of girth at least eight is isomorphic to graph $B\Gamma_3(\mathbb{F}_q; XY, XY^2)$ (as it was conjectured in [24]). Finally, Hou, Lappano and Lazebnik in [43] showed that this is the case.

Theorem 7. ([43]) *Let q be an odd prime power. Then every monomial graph $B\Gamma_3(\mathbb{F}_q; f_2, f_3)$ of girth at least eight is isomorphic to graph $B\Gamma_3(\mathbb{F}_q; XY, XY^2)$.*

We wish to note that investigation of cycles in monomial graphs lead to several interesting questions about bijective functions on $\mathbb{F}_q$, also known as permutation polynomials (every function on $\mathbb{F}_q$ can be represented as a polynomial). Some of them are still unresolved.

Conjecture 2. ([24]) *Let $q = p^e$ be an odd prime power. For an integer k, $1 \leq k \leq q-1$, let $A_k = X^k[(X+1)^k - X^k]$ and $B_k = [(X+1)^{2k} - 1]X^{q-1-k} - 2X^{q-1}$ be polynomials in $\mathbb{F}_q[X]$. Then each of them is a permutation polynomial of $\mathbb{F}_q$ if and only if k is a power of p.*

It was shown in [22] and [24] that the validity of this conjecture for either A_k or B_k, would imply Theorem 7. Though the conjecture is still open for each of the polynomials, new results on these polynomials obtained in [43] were sufficient to prove Theorem 7.

Hence, no new generalized 4-gon can be constructed this way. What if not both polynomials f_2, f_3 are monomials? In [52], Kronenthal and Lazebnik showed that over every algebraically closed field $\mathbb{F}$ of characteristic zero, every graph $B\Gamma_3(\mathbb{F}; XY, f_3)$ of girth at least eight, where f_3 is any polynomial in $\mathbb{F}[X, Y]$, is isomorphic to graph $B\Gamma_3(\mathbb{F}; XY, XY^2)$. Their methods imply that the same result holds over infinitely many finite fields. In particular, the following theorem holds.

Theorem 8. ([52]) *Let q be a power of a prime p, $p \geq 5$, and let $M = M(p)$ be the least common multiple of integers $2, 3, \ldots, p-2$. Suppose $f_3 \in \mathbb{F}_q[X, Y]$ has degree at most $p-2$ with respect to each of X and Y. Then over every finite field extension $\mathbb{F}$ of $\mathbb{F}_{q^M}$, every graph $B\Gamma_3(\mathbb{F}; XY, f_3)$ of girth at least eight is isomorphic to graph $B\Gamma_3(\mathbb{F}; XY, XY^2)$.*

Recently, Kronenthal, Lazebnik and Williford [53] extended these "uniqueness" results to the family of graphs $B\Gamma_3(\mathbb{F}; X^mY^n, f_3)$ (with XY replaced by an arbitrary monomial X^mY^n).

Problem 3. *(i) Let q be an odd prime power, and let $f_2, f_3 \in \mathbb{F}_q[X,Y]$. Is it true that every graph $B\Gamma_3(\mathbb{F}_q; f_2, f_3)$ with girth at least eight is isomorphic to graph $B\Gamma_3(\mathbb{F}_q; XY, XY^2)$?*
(ii) Let q be an odd prime power, and let $f_2 \in \mathbb{F}_q[X,Y]$ and $f_3 \in \mathbb{F}_q[W,X,Y,Z]$. Is it true that every graph $B\Gamma_2(\mathbb{F}_q; f_2, f_3)$ with girth at least eight is isomorphic to graph $B\Gamma_2(\mathbb{F}_q; XY, XY^2)$?

It is clear that a negative answer to each of two parts of Problem 3 may lead to a new generalized quadrangle. It will lead to one, if such graph exists and it is possible to "attach" to it a $(q+1)$-regular tree on $2(q^2+q+1)$ vertices. Though we still cannot conjecture the uniqueness result for odd q, we believe that it holds over algebraically closed fields.

Conjecture 3. ([52]) *Let $\mathbb{F}$ be an algebraically closed field of characteristic zero, and let $f_2, f_3 \in \mathbb{F}[X,Y]$. Then every graph $B\Gamma_3(\mathbb{F}; f_2, f_3)$ with girth at least eight is isomorphic to graph $B\Gamma_3(\mathbb{F}; XY, XY^2)$.*

4.4. **Dense (m,n)-bipartite graphs of girth 8.** Let $f(n,m)$ denote the greatest number of edges in a bipartite graph whose bipartition sets have cardinalities n, m $(n \geq m)$ and whose girth is at least 8. In [27] Erdős conjectured that $f(n,m) = O(n)$ for $m = O(n^{2/3})$. For a motivation of this question see de Caen and Székely [12]. Using some results from combinatorial number theory and set systems, this conjecture was refuted in [12], by showing the existence of an infinite family of (m,n)-bipartite graphs with $m \sim n^{2/3}$, girth at least 8, and having $n^{1+1/57+o(1)}$ edges. As the authors pointed out, this disproved Erdős' conjecture, but fell well short of their upper bound $O(n^{1+1/9})$.

Using certain induced subgraphs of algebraically defined graphs, Lazebnik, Ustimenko and Woldar [60] constructed explicitly an infinite family of $(n^{2/3}, n)$-bipartite graphs of girth 8 with $n^{1+1/15}$ edges. Here is the construction.

Let q be an odd prime power, and set $P = \mathbb{F}_q \times \mathbb{F}_{q^2} \times \mathbb{F}_q$, $L = \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \times \mathbb{F}_q$. We define the bipartite graph $\Gamma(q)$ with bipartition $P \cup L$ in which (p) is adjacent to $[l]$ provided

$$l_2 + p_2 = p_1 l_1$$
$$l_3 + p_3 = -(p_2 \overline{l_1} + \overline{p_2} l_1)$$

(here, $\overline{x}$ denotes the image of x under the involutory automorphism of $\mathbb{F}_{q^2}$ with fixed field $\mathbb{F}_q$).

In the context of the current survey, $\Gamma(q)$ is closely related to the induced subgraph $B\Gamma_3[\mathbb{F}_q, \mathbb{F}_{q^2}]$ of $B\Gamma_3 = B\Gamma_3(\mathbb{F}_{q^2}; p_1 l_1, -(p_2\overline{l_1} + \overline{p_2} l_1))$ (see Section 2.3). Indeed, the only difference is that the third coordinates of vertices of $\Gamma(q)$ are required to come from $\mathbb{F}_q$.

Assuming now that $q^{1/3}$ is an integer, we may further choose $A \subset \mathbb{F}_q$ with $|A| = q^{1/3}$. Set $P_A = A \times \mathbb{F}_{q^2} \times \mathbb{F}_q$, and denote by $\Gamma'(q)$ the subgraph of $\Gamma(q)$ induced on the set $P_A \cup L$. Then the family $\{\Gamma'(q)\}$ gives the desired $(n^{2/3}, n)$-bipartite graphs of girth 8 and $n^{1+1/15}$ edges, where $n = q^2$. (See [60] for details.)

Problem 4. *Improve the magnitude (exponent of n) in either the lower or the upper bound in the inequality*

$$c_1 n^{1+1/15} \leq f(n^{2/3}, n) \leq c_2 n^{1+1/9}.$$

where c_1, c_2 are positive constants.

4.5. **Digraphs.** Consider a digraph with loops $D_n = \Gamma_n(\mathbb{F}_q; f_2, \dots, f_n)$, defined as in Subsection 2.2 by system (2.2). The study of these digraphs was initiated in Kodess [48]. Some general properties of these digraphs are similar to the ones of graphs Γ_n. A digraph is called *strongly connected* if there exists a directed path between any of its two vertices, and every digraph is a union of its strongly connected (or just strong) components.

Suppose each function f_i is a function of only two variables, and there is an arc from a vertex $\langle a_1, \dots, a_n\rangle$ to a vertex $\langle b_1, \dots, b_n\rangle$ if

$$a_i + b_i = f_i(a_1, b_1) \text{ for all } i,\ 2 \le i \le n$$

The strong connectivity of these digraphs was studied by Kodess and Lazebnik [49]. Utilizing some ideas from [100], they obtained necessary and sufficient conditions for strong connectivity of D_n and completely described its strong components. The results are expressed in terms of the properties of the span over $\mathbb{F}_p$ of the image of an explicitly constructed vector function from $\mathbb{F}_q^2$ to $\mathbb{F}_q^{n-1}$, whose definition depends on the functions f_i. The details are a bit lengthy, and can be found in [49].

Finding the diameter of strong digraphs D_n seems to be a very hard problem, even for $n = 2$. Specializing f_2 to a monomial of two variables, i.e., $f_2 = X^m Y^n$, makes it a bit easier, though exact results are still hard to obtain. In [50], Kodess, Lazebnik, Smith and Sporre studied the diameter of digraphs $D(q; m, n) = D_2(\mathbb{F}_q; X^m Y^n)$. They obtained precise values and good bounds on the diameter of these graphs for many instances of the parameters. For some of the results the connection to Waring numbers over finite fields was utilized. The necessary and sufficient conditions for strong connectivity of $D(q; m, n)$ in terms of the arithmetic properties of q, m, n appeared in [49].

Another interesting question about monomial digraphs is the isomorphism problem: when is $D(q; m_1, n_1)$ isomorphic to $D(q; m_2, n_2)$? A similar question for bipartite monomial graphs $B(q; m, n)$ was answered in Theorem 6. For those graphs $(B(q; m, n))$ just the count of 4-cycles resolves the isomorphism question for fixed m, n and large q ([100]), and the count of complete bipartite subgraphs gives the answer for all q, m, n ([24]). In contrast, for digraphs $D(q; m, n)$, counting cycles of length from one (loops) to seven is not sufficient: there exist digraphs for which these counts coincide, and which are not isomorphic (see [48]). In this regard, we would like to state the following problem and a conjecture. For any digraphs E and H, let $|E(H)|$ denote the number of subdigraphs of E isomorophic to H.

Problem 5. *Are there digraphs $D_1, \dots, D_k$ such that any two monomial digraphs $D = D(q; m, n)$ and $D' = D(q'; m', n')$ are isomorphic if and only if $|D(D_i)| = |D'(D_i)|$ for each $i = 1, \dots, k$?*

Though the sufficiency of the condition in the following conjecture is easy to check, its necessity is still to be established.

Conjecture 4. ([48]) *Let q be a prime power. The digraphs $D(q; m_1, n_1)$ and $D(q; m_2, n_2)$ are isomorphic if and only if there exists k, coprime with $q - 1$, such that*

$$m_2 \equiv k m_1 \mod (q-1)$$
$$n_2 \equiv k n_1 \mod (q-1)$$

5. Constructions for hypergraphs

In this paper, a *hypergraph* $\mathcal{H}$ is a family of distinct subsets of a finite set. The members of $\mathcal{H}$ are called *edges*, and the elements of $V(\mathcal{H}) = \bigcup_{E\in\mathcal{H}} E$ are called *vertices*. If all edges in $\mathcal{H}$ have size r, then $\mathcal{H}$ is called an *r-uniform* hypergraph or, simply, *r-graph*. For example, a 2-graph is a graph in the usual sense. A vertex v and an edge E are called *incident* if $v \in E$. The *degree* of a vertex v of $\mathcal{H}$ is the number of edges of $\mathcal{H}$ incident with v. An r-graph $\mathcal{H}$ is *r-partite* if its vertex set $V(\mathcal{H})$ can be colored in r colors in such a way that no edge of $\mathcal{H}$ contains two vertices of the same color. In such a coloring, the color classes of $V(\mathcal{H})$ – the sets of all vertices of the same color – are called *parts* of $\mathcal{H}$. We refer the reader to Berge [5, 6] for additional background on hypergraphs.

5.1. **Multicolor Ramsey Numbers.** Let $k \geq 2$. The *multicolor Ramsey number* $r_k(C_4)$ is defined to be the smallest integer $n = n(k)$ with the property that any k-coloring of the edges of the complete graph K_n must result in a monochromatic subgraph isomorphic to C_4. Using a 4-cycle free graph $\Gamma_2 = \Gamma_2(\mathbb{F}_q; XY)$ with q being an odd prime power, Lazebnik and Woldar [70] showed that $r_q(C_4) \geq q^2 + 2$. This compared well with an upper bound by Chung and Graham [20], which implied that $r_q(C_4) \leq q^2 + q + 1$. For details, and more on the multicolor Ramsey numbers, see [20], [70], and a survey by S. P. Radziszowski [80].

5.2. **Edge-decomposition of complete k-partite r-graphs and complete r-graphs.** In [55], Lazebnik and Mubayi generalized Theorem 4 to edge-decompositions of complete uniform r-partite hypergraphs and complete uniform hypergraphs, respectively. The following comment is from [55].

> Looking back, it is fair to say that most of these generalizations turned out to be rather straightforward and natural. Nevertheless it took us much longer to see this than we originally expected: some "clear" paths led eventually to nowhere, and several technical steps presented considerable challenge even after the "right" definitions had been found.

As before, let $\mathbb{F}_q$ be the field of q elements. For integers $d, i, r \geq 2$, let $f_i : \mathbb{F}_q^{(i-1)r} \to \mathbb{F}_q$ be a function. For $x^i = (x_1^i, \ldots, x_d^i) \in \mathbb{F}_q^d$, let $(x^1, \ldots, x^i)$ stand for $(x_1^1, \ldots, x_d^1, x_1^2, \ldots, x_d^2, \ldots, x_1^i, \ldots, x_d^i)$.

Suppose d, k, r are integers and $2 \leq r \leq k$, $d \geq 2$. First we define a k-partite r-graph $\mathcal{T} = \mathcal{T}(q, d, k, r, f_2, f_3, \ldots, f_d)$. Let the vertex set $V(\mathcal{T})$ be a disjoint union of sets, or color classes, $V^1, \ldots, V^k$, where each V^j is a copy of $\mathbb{F}_q^d$. By $a^j = (a_1^j, a_2^j, \ldots, a_d^j)$ we denote an arbitrary vertex from V^j. The edge set $E(\mathcal{T})$ is defined as follows: for every r-subset $\{i_1, \ldots, i_r\}$ of $\{1, \ldots, k\}$ (the set of colors), we consider the family of all r-sets of vertices $\{a^{i_1}, \ldots, a^{i_r}\}$, where each $a^j \in V^j$, and such that the following system of $r - 1$ equalities hold:

$$
\begin{aligned}
&\sum_{j=1}^{r} a_2^{i_j} = f_2(a_1^{i_1}, \ldots, a_1^{i_r}) \\
&\sum_{j=1}^{r} a_3^{i_j} = f_3(a_1^{i_1}, \ldots, a_1^{i_r}, a_2^{i_1}, \ldots, a_2^{i_r}) \\
&\quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\
&\sum_{j=1}^{r} a_d^{i_j} = f_d(a_1^{i_1}, \ldots, a_1^{i_r}, a_2^{i_1}, \ldots, a_2^{i_r}, \ldots, a_{d-1}^{i_1}, \ldots, a_{d-1}^{i_r})
\end{aligned} \tag{5.1}
$$

The system (5.1) can also be used to define another class of r-graphs, $\mathcal{K} = \mathcal{K}(q, d, r, f_2, f_3, \ldots, f_d)$, but in order to do this, we have to restrict the definition to only those functions f_i which satisfy the following symmetry property: for every permutation π of $\{1, 2, \ldots, i-1\}$,

$$f_i(x^{\pi(1)}, \ldots, x^{\pi(i-1)}) = f_i(x^1, \ldots, x^{i-1}).$$

Then let the vertex set $V(\mathcal{K}) = \mathbb{F}_q^d$, and let the edge set $E(\mathcal{K})$ be the family of all r-subsets $\{a^{i_1}, \ldots, a^{i_r}\}$ of vertices which satisfy system (5.1). We impose the symmetry condition on the f_i to make the definition of an edge independent of the order in which its vertices are listed.

$\mathcal{K}$ can be also viewed as a q^d-partite r-graph, each partition having one vertex only. If $d = r$, then $\{i_1, \ldots, i_r\} = \{1, \ldots, d\}$.

Theorem 9. ([55]) *Let q, d, r, k be integers, $2 \le r \le k$, $d \ge 2$, and q be a prime power. Then*

1. *$\mathcal{T}$ is a regular r-graph of order kq^d and size $\binom{k}{r} q^{dr-d+1}$. The degree of each vertex is $\binom{k-1}{r-1} q^{dr-2d+1}$.*
2. *For odd q, $\mathcal{K}$ is an r-graph of order q^d and size $\frac{1}{q^{d-1}} \binom{q^d}{r}$.*

For $r = 2$ and q odd, the number of loops in graph Γ_n could be easily counted. Removing them leads to a bi-regular graph, with some vertices having degree q and other having degree $q-1$. In general this is not true for $r \ge 3$. Nevertheless, it is true when $q = p$ is an odd prime, and the precise statement follows. In this case, the condition $(r, p) = 1$ implies $(r-1, p) = 1$, which allows one to prove the following theorem by induction on r.

Theorem 10. ([55]) *Let p, d, r be integers, $2 \le r < p$, $d \ge 2$, and p be a prime. Then $\mathcal{K}$ is a bi-regular r-graph of order p^d and size $\frac{1}{p^{d-1}} \binom{p^d}{r}$. It contains $p^d - p$ vertices of degree Δ and p vertices of degree $\Delta + (-1)^{r+1}$, where $\Delta = \frac{1}{p^{d-1}} \left(\binom{p^d - 1}{r-1} + (-1)^r \right)$.*

We now turn to edge-decompositions of hypergraphs. Let $\mathcal{H}$ and $\mathcal{H}'$ be hypergraphs. An *edge-decomposition of $\mathcal{H}$ by $\mathcal{H}'$* is a collection $\mathcal{P}$ of subhypergraphs of $\mathcal{H}$, each isomorphic to $\mathcal{H}'$, such that $\{E(\mathcal{X}) \mid \mathcal{X} \in \mathcal{P}\}$ is a partition of $E(\mathcal{H})$. We also say in this case that $\mathcal{H}'$ *decomposes* $\mathcal{H}$, and refer to the hypergraphs from $\mathcal{P}$ as *copies* of $\mathcal{H}'$.

Let $T^{(r)}_{kq^d}$, $2 \le r \le k$, $d \ge 1$, denote the complete k-partite r-graph with each partition class containing q^d vertices. This is a regular r-graph of order kq^d and size $\binom{k}{r}q^{dr}$, and the degree of each vertex is $\binom{k-1}{d-1}q^{dr-d}$.

As before, let $K^{(r)}_{q^d}$ denote the complete r-graph on q^d vertices. The following theorem holds for *arbitrary* functions $f_2, \dots, f_r$. The proof below is similar to the one for 2-graphs from [71].

Theorem 11. ([55]) *Let q, d, r, k be integers, $2 \le r \le k$, $d \ge 2$, and q be a prime power. Then*

(1) *$\mathcal{T} = \mathcal{T}(q, d, r, k, f_2, f_3, \dots, f_d)$ decomposes $T^{(r)}_{kq^d}$.*
(2) *$\mathcal{K} = \mathcal{K}(q, d, r, f_2, f_3, \dots, f_d)$ decomposes $K^{(r)}_{q^d}$ provided that q is odd and $(r, q) = 1$.*

As an immediate corollary of this theorem one obtains constructive lower bounds for the Ramsey numbers.

Corollary 1. ([55]) *Let $\mathcal{H}$ be any r-uniform hypergraph which is not a subhypergraph in $\mathcal{K} = \mathcal{K}(q, d, r, f_2, f_3, \dots, f_d)$. Let $k = q^{d-1}$, q be odd and $(r, q) = 1$. Then*

$$r_k(\mathcal{H}) \ge q^d + 1 = k^{d/(d-1)} + 1.$$

5.3. **Girth five uniform hypergraphs.** For $k \ge 2$, a *cycle* in a hypergraph $\mathcal{H}$ is an alternating sequence of vertices and edges of the form $v_1, E_1, v_2, E_2, \dots, v_k, E_k, v_1$, such that

(i) $v_1, v_2, \dots, v_k$ are distinct vertices of $\mathcal{H}$,
(ii) $E_1, E_2, \dots, E_k$ are distinct edges of $\mathcal{H}$,
(iii) $v_i, v_{i+1} \in E_i$ for each $i \in \{1, 2, \dots, k-1\}$, and $v_k, v_1 \in E_k$.

We refer to a cycle with k edges as a *k-cycle*, and denote the family of all k-cycles by $\mathcal{C}_k$. For example, a 2-cycle consists of a pair of vertices and a pair of edges such that the pair of vertices is a subset of each edge. The above definition of a hypergraph cycle is the "classical" definition (see, for example, Duchet [25]). For $r = 2$ and $k \ge 3$, it coincides with the definition of a cycle C_k in graphs and, in this case, $\mathcal{C}_k$ is a family consisting of precisely one member. The *girth* of a hypergraph $\mathcal{H}$, containing a cycle, is the minimum length of a cycle in $\mathcal{H}$.

In [66], Lazebnik and Verstraëte considered a Turán-type extremal question of determining the maximum number of edges in an r-graph on n vertices of girth five. For graphs ($r = 2$), this is an old problem of Erdős [26]. The best known lower and upper bounds are $(1/2\sqrt{2})n^{3/2} + O(n)$ and $(1/2)(n-1)^{1/2}n$, respectively. For bipartite graphs, on the other hand, this maximum is $(1/2\sqrt{2})n^{3/2} + O(n)$ as $n \to \infty$. Many attempts at reducing the gap between the constants $1/2\sqrt{2}$ and $1/2$ in the lower and upper bounds have not succeeded thus far. Turán-type questions for hypergraphs are generally harder than for graphs, and the following result was surprising, as in this case the constants in the lower and the upper bounds for the maximum turned out to be equal, and the difference between the bounds was $O(n^{1/2})$.

Theorem 12. [66] *Let $\mathcal{H}$ be a 3-graph on n vertices and of girth at least five. Then*

$$|\mathcal{H}| \le \tfrac{1}{6} n \sqrt{n - \tfrac{3}{4}} + \tfrac{1}{12} n.$$

For any odd prime power $q \ge 27$, there exist 3-graphs $\mathcal{H}$ on $n = q^2$ vertices, of girth five, with

$$|\mathcal{H}| = \tbinom{q+1}{3} = \tfrac{1}{6} n^{3/2} - \tfrac{1}{6} n^{1/2}.$$

In the context of this survey, we wish to mention that the original construction for the lower bound came from considering the following algebraically defined 3-graph $\mathcal{G}_q$ of order $n = q(q-1)$, of girth five (for sufficiently large n) and the number of edges $\sim \frac{1}{6} n^{3/2} - \frac{1}{4} n + o(n^{1/2})$, $n \to \infty$. Let $\mathbb{F}_q$ denote the finite field of odd characteristic, and let C_q denote the set of points on the curve $2x_2 = x_1^2$, where $(x_1, x_2) \in \mathbb{F}_q \times \mathbb{F}_q$. Define a hypergraph $\mathcal{G}_q$ as follows. The vertex set of $\mathcal{G}_q$ is $\mathbb{F}_q \times \mathbb{F}_q \setminus C_q$. Three distinct vertices $a = (a_1, a_2)$, $b = (b_1, b_2)$ and $c = (c_1, c_2)$ form an edge $\{a, b, c\}$ of $\mathcal{G}_q$ if and only if the following three equations are satisfied:

$$\begin{aligned} a_2 + b_2 &= a_1 b_1 \\ b_2 + c_2 &= b_1 c_1 \\ c_2 + a_2 &= c_1 a_1 \end{aligned}$$

It is not difficult to check that $\mathcal{G}_q$ has girth at least five for all odd q and girth five for all sufficiently large q. The number of edges in $\mathcal{G}_q$ is precisely $\binom{q}{3}$, since there are $\binom{q}{3}$ choices for distinct a_1, b_1 and c_1, which uniquely specify a_2, b_2 and c_2 such that a, b, c are not on the curve $2y = x^2$ and $\{a, b, c\}$ is an edge.

The idea to consider the hypergraph $\mathcal{H}_q$, whose edges are 3-sets of vertices of triangles in the polarity graph of $PG(2, q)$ with absolute points deleted, is due to Lovász, see [66] for details. It raised the asymptotic lower bound to $\sim \frac{1}{6} n^{3/2} - \frac{1}{6} n + o(n^{1/2})$, $n \to \infty$, as stated in Theorem 12.

More on Turán-type problems for graphs and hypergaph, see Bollobás [7], Füredi [32], and Füredi and Simonovits [36].

5.4. **Dense graphs without cycles of certain length.** For more on this subject, see [7], and the most recent survey [36]. Our goal here is to mention some results, not mentioned in [36], and related constructions obtained by the algebraically defined graphs.

Let $\mathcal{F}$ be a family of graphs. By $ex(\nu, \mathcal{F})$ we denote the greatest number of edges in a graph on ν vertices which contains no subgraph isomorphic to a graph from $\mathcal{F}$. Let C_n denote the cycle of length $n \ge 3$. The best bounds on $ex(\nu, \{C_3, C_4, \cdots, C_{2k}\})$ for fixed k, $2 \le k \ne 5$, are presented below.

Let $\epsilon = 0$ if k is odd, and $\epsilon = 1$ if k is even. When the girth is odd, the bounds are

$$\frac{1}{2^{1+1/k}} \nu^{1+\frac{2}{3k-3+\epsilon}} \le ex(\nu, \{C_3, C_4, \cdots, C_{2k}\}) \le \frac{1}{2} \nu^{1+\frac{1}{k}} + \frac{1}{2} \nu. \tag{5.2}$$

When the girth is even, they are

$$\frac{1}{2^{1+1/k}} \nu^{1+\frac{2}{3k-3+\epsilon}} \le ex(\nu, \{C_3, C_4, \cdots, C_{2k}, C_{2k+1}\}) \le \frac{1}{2^{1+1/k}} \nu^{1+\frac{1}{k}} + \frac{1}{2} \nu. \tag{5.3}$$

The upper bounds in both (5.2) and (5.3) are immediate corollaries of the result by Alon, Hoory and Linial [3]. The lower bound holds for an infinite sequence of values of ν. It was established by Lazebnik, Ustimenko and Woldar in [62] using some graphs $B\Gamma_n$, and those will be discussed in detail in Section 6.

For $k = 2, 3, 5$ there exist more precise results by Neuwirth [76], Hoory [41], Abajo and Diánez [1].

Theorem 13. *For $k = 2, 3, 5$ and $\nu = 2(q^k + q^{k-1} + \cdots + q + 1)$, q is a prime power,*

$$ex(\nu, \{C_3, C_4, \cdots, C_{2k}, C_{2k+1}\}) = (q+1)(q^k + q^{k-1} + \cdots + q + 1),$$

and every extremal graph is a generalized $(k+1)$-gon Π_q^{k+1}.

Suppose $\mathcal{F} = \{C_{2k}\}$. It was shown by Erdős, but never published, that

$$ex(\nu, \{C_{2k}\}) = O(\nu^{1+1/k}).$$

The first proof followed from a stronger result by Bondy and Simonovits [9], who showed that $ex(\nu, \{C_{2k}\}) \le 100kv^{1+1/k}$. The upper bound was improved by Verstraëte [99] to $8(k-1)\nu^{1+1/k}$, by Pikhurko [79] to $(k-1)\nu^{1+1/k} + O(\nu)$ and by Bukh and Jiang [11] to $80\sqrt{k \log k}\nu^{1+1/k} + O(\nu)$. The only values of k for which $ex(\nu, \{C_{2k}\}) = \Theta(v^{1+1/k})$ are $k = 2, 3$, and 5, with the strongest results appearing in Füredi [32, 33] (for $k = 2$), Füredi, Naor and Verstraëte [35] (for $k = 3$), and by Lazebnik, Ustimenko and Woldar [65] (for $k = 5$).

In [97], the authors provide several best lower bounds for some bipartite graphs with given bi-degree and girth.

In [88], Terlep and Williford considered the graphs $TW(q) = B\Gamma_8(\mathbb{F}_q; f_2, \ldots, f_8)$, where

$$f_2 = p_1 l_1,\ f_3 = p_1 l_2,\ f_4 = p_1 l_3,\ f_5 = p_1 l_4,\ f_6 = p_2 l_3 - 2p_3 l_2 + p_4 l_1,$$

$$f_7 = p_1 l_6 + p_2 l_4 - 3p_4 l_2 + 2p_5 l_1, \text{ and } f_8 = 2p_2 l_6 - 3p_6 l_2 + p_7 l_1.$$

These graphs provide the best asymptotic lower bound on $ex(\nu, \{C_{14}\})$. The approach to their construction is similar to the one in [59], and it is obtained from Lie algebras related to generalized Kac-Moody algebras of rank 2.

Theorem 14. ([88]) *For infinitely many values of q, $ex(\nu, \{C_{14}\}) \ge \frac{1}{2^{9/8}}\nu^{9/8}$.*

We wish to note that $TW(q)$ graphs also have no cycles of length less than 12. For $q = 5, 7$, they do contain 12-cycles, and likely have girth 12 in general. The proof performs a Gröbner basis computation using the computer algebra system Magma, which established the absence of 14-cycles over the field of algebraic numbers. The transition to finite fields was made using the Lefschetz principle.

We wish to end this section with two problems.

Problem 6. *Provide a computer-free proof of the fact that $TW(q)$ graphs contain no 14-cycles for infinitely many q.*

It is a long standing question to determine the magnitude of $ex(\nu, \{C_8\})$. The best lower bound is $\Omega(\nu^{6/5})$ and it comes from the generalized hexagon, which has girth 12. The best upper bound is $O(\nu^{5/4})$ and it comes from the general bound $O(\nu^{1+1/k})$ on $2k$-cycle-free graphs.

Problem 7. *Is there a graph $B\Gamma_3(\mathbb{F}_q; f_2, f_3, f_4)$ that contains no 8-cycles for infinitely many q?*

Positive answer to this question will imply that $ex(\nu, \{C_8\}) = \Theta(\nu^{5/4})$.

6. Graphs $D(k,q)$ and $CD(k,q)$

For any $k \geq 2$, and any prime power q, the bipartite graph $D(k,q)$ is defined as $B\Gamma_k(\mathbb{F}_q; f_2, \ldots, f_k)$, where $f_2 = p_1 l_1$, $f_3 = p_1 l_2$, and for $4 \leq i \leq k$,

$$f_i = \begin{cases} -p_{i-2} l_1 & \text{for } i \equiv 0 \text{ or } 1 \mod 4 \\ p_1 l_{i-2} & \text{for } i \equiv 2 \text{ or } 3 \mod 4 \end{cases}$$

It was shown that these graphs are edge-transitive and, most importantly, the girth of $D(k,q)$ is at least $k+5$ for odd k. It was shown in [62] that for $k \geq 6$ and q odd, graphs $D(k,q)$ are disconnected, and the order of each component (any two being isomorphic) is at least $2q^{k-\lfloor \frac{k+2}{4} \rfloor + 1}$. Let $CD(k,q)$ denote one of these components. It is the family of graphs $CD(k,q)$ which provides the best lower bound mentioned before, being a slight improvement over the previous best lower bound $\Omega(\nu^{1+\frac{2}{3k+3}})$ given by the family of Ramanujan graphs constructed by Margulis [74], and independently by Lubotzky, Phillips and Sarnak [73].

The construction of the graphs $D(k,q)$ was motivated by attempts to generalize the notion of the biaffine part of a generalized polygon, and it was facilitated by results of Ustimenko [93] on the embedding of Chevalley group geometries into their corresponding Lie algebras. For more recent exposition of these ideas, see [97], [106], and [88].

In fact, $D(2,q)$ and $D(3,q)$ (q odd) are exactly the biaffine parts of a regular generalized 3-gon and 4-gon, respectively (see [58] for more details). We wish to point out that $D(5,q)$ is not the biaffine part of the generalized hexagon.

As we mentioned before, the generalized k-gons exist only for $k = 3, 4, 6$ ([31]), therefore, $D(k,q)$ are not subgraphs of generalized k-gons for $k \geq 4$.

In this section, we will discuss the important properties of these graphs in detail.

6.1. Equivalent Definition of $D(k,q)$.

Proposition 2. *Let q be any prime power, $k \geq 2$, and $a_1, \ldots, a_{k-1} \in \mathbb{F}_q^*$, then $H(k,q) = B\Gamma_k(\mathbb{F}_q; f_2, \ldots, f_k)$ is isomorphic to $D(k,q)$, where $f_2 = a_1 p_1 l_1$, $f_3 = a_2 p_1 l_2$, and for $4 \leq i \leq k$,*

$$f_i = \begin{cases} -a_{i-1} p_{i-2} l_1 & \text{for i} \equiv 0 \text{ or } 1 \mod 4 \\ a_{i-1} p_1 l_{i-2} & \text{for i} \equiv 2 \text{ or } 3 \mod 4 \end{cases}$$

Proof. Let $\varphi : V(D(k,q)) \mapsto V(H(k,q))$ be defined via $(p) \to (x)$, and $[l] \to [y]$ where

$$\begin{aligned} x_1 &= p_1, & y_1 &= l_1 \\ x_2 &= a_1 p_2, & y_2 &= a_1 l_2 \\ x_{2i+1} &= a_{2i} a_{2i-2} \ldots a_2 a_1 p_{2i+1}, & y_{2i+1} &= a_{2i} a_{2i-2} \ldots a_2 a_1 l_{2i+1} \\ x_{2i} &= a_{2i-1} a_{2i-3} \ldots a_1 p_{2i}, & y_{2i} &= a_{2i-1} a_{2i-3} \ldots a_1 l_{2i} \end{aligned}$$

Clearly, φ is a bijection. Now we prove that φ preserves the adjacency. Indeed,

$$(p)^\varphi \sim [l]^\varphi$$

if and only if $x_2 + y_2 = a_1 x_1 y_1$, $x_3 + y_3 = a_2 x_1 y_2$, and

$$\begin{cases} x_{4t} + y_{4t} & = -a_{4t-1} x_{4t-2} y_1 \\ x_{4t+1} + y_{4t+1} & = -a_{4t} x_{4t-1} y_1 \\ x_{4t+2} + y_{4t+2} & = a_{4t+1} x_1 y_{4t} \\ x_{4t+3} + y_{4t+3} & = a_{4t+2} x_1 y_{4t+1} \end{cases}$$

if and only if $a_1 p_2 + a_1 l_2 = a_1 p_1 l_1$, $a_2 a_1 p_3 + a_2 a_1 l_3 = a_2 p_1 a_1 l_2$, and

$$\begin{cases} a_{4t-1} a_{4t-3} \dots a_1 (p_{4t} + l_{4t}) & = -a_{4t-1} a_{4t-3} \dots a_1 p_{4t-3} l_1 \\ a_{4t} a_{4t-2} \dots a_2 a_1 (p_{4t+1} + l_{4t+1}) & = -a_{4t} a_{4t-2} \dots a_2 a_1 p_{4t-1} l_1 \\ a_{4t+1} a_{4t-1} \dots a_1 (p_{4t+2} + l_{4t+2}) & = a_{4t+1} p_1 a_{4t-1} \dots a_1 l_{4t} \\ a_{4t+2} a_{4t} \dots a_2 a_1 (p_{4t+3} + l_{4t+3}) & = a_{4t+2} p_1 a_{4t} \dots a_2 a_1 l_{4t+1} \end{cases}$$

if and only if

$$(p) \sim [l]$$

□

By Proposition 2, for any prime power q and $k \geq 2$, $D(k,q)$ is isomorphic to $B\Gamma_k(\mathbb{F}_q; f_2, \dots, f_k)$ where $f_2 = p_1 l_1$, $f_2 = p_1 l_2$, and for $4 \leq i \leq k$,

$$f_i = \begin{cases} p_{i-2} l_1 & \text{for i} \equiv 0 \text{ or } 1 \mod 4 \\ p_1 l_{i-2} & \text{for i} \equiv 2 \text{ or } 3 \mod 4 \end{cases}$$

From now on, we will use these equation for $D(k,q)$.

Moreover, in the case of $q = 2$,

$$D(2,2) \cong C_8, D(3,2) \cong 2C_8, D(4,2) \cong 4C_8,$$

and

$$D(k,2) \cong 4^{k-4} C_{16}.$$

for $k \geq 5$. So from now on, we assume that $q \geq 3$.

6.2. **Automorphisms of $D(k,q)$.** There are many automorphisms of $D(k,q)$, below we will list all the automorphisms we will use. It is a straightforward verification that the mappings we describe are indeed automorphisms, and it is left to the reader. For more details, see [58], [59], [34] or [63].

6.2.1. *Multiplicative Automorphisms.* For any $a, b \in \mathbb{F}_q^*$, consider the map $m_{a,b} : \mathcal{P}_k \mapsto \mathcal{P}_k, \mathcal{L}_k \mapsto \mathcal{L}_k$ such that $(p) \xrightarrow{m_{a,b}} (p')$, and $[l] \xrightarrow{m_{a,b}} [l']$ where $p'_1 = a p_1$, $l'_1 = b l_1$, and for any $2 \leq i \leq k$,

$$p'_i = \begin{cases} a^{\lfloor \frac{i-1}{4} \rfloor + 1} b^{\lfloor \frac{i}{4} \rfloor + 1} p_i & \text{for i} \equiv 0,\ 1 \text{ or } 2 \mod 4 \\ a^{\lfloor \frac{i}{4} \rfloor + 2} b^{\lfloor \frac{i}{4} \rfloor + 1} p_i & \text{for i} \equiv 3 \mod 4 \end{cases}$$

$$l'_i = \begin{cases} a^{\lfloor \frac{i-1}{4} \rfloor + 1} b^{\lfloor \frac{i}{4} \rfloor + 1} l_i & \text{for i} \equiv 0,\ 1 \text{ or } 2 \mod 4 \\ a^{\lfloor \frac{i}{4} \rfloor + 2} b^{\lfloor \frac{i}{4} \rfloor + 1} l_i & \text{for i} \equiv 3 \mod 4 \end{cases}$$

In Table 1, each entry illustrates how each coordinate is changed under the map $m_{a,b}$, i.e., the factor that the corresponding coordinate of a point or a line is multiplied by. For example, $m_{a,b}$ changes p_1 to ap_1, l_1 to bl_1, both p_{4t+3} and l_{4t+3} to their product with $a^{t+2} b^{t+1}$.

TABLE 1. Multiplicative Automorphism

	$m_{a,b}$		$m_{a,b}$
p_1	$*a$	l_1	$*b$
p_{4t}	$*a^t b^{t+1}$	l_{4t}	$*a^t b^{t+1}$
p_{4t+1}	$*a^{t+1} b^{t+1}$	l_{4t+1}	$*a^{t+1} b^{t+1}$
p_{4t+2}	$*a^{t+1} b^{t+1}$	l_{4t+2}	$*a^{t+1} b^{t+1}$
p_{4t+3}	$*a^{t+2} b^{t+1}$	l_{4t+3}	$*a^{t+2} b^{t+1}$

Proposition 3. *For any $a, b \in \mathbb{F}_q^*$, $m_{a,b}$ is an automorphism of $D(k, q)$.*

6.2.2. *Additive Automorphisms.* For any $x \in \mathbb{F}_q$, and any $0 \leq j \leq k$, we define the map $t_{j,x} : \mathcal{P}_k \to \mathcal{P}_k, \mathcal{L}_k \to \mathcal{L}_k$ as follows:

(1) The map $t_{0,x}$ fixes the first coordinate of a line, whereas $t_{1,x}$ fixes the first coordinate of a point. In Table 2, each entry illustrates how each coordinate is changed under the map. If the entry is empty, it means that this coordinate is fixed by the map. For example, the map $t_{1,x}$ changes the following coordinates of a line according to the rule: $l_1 \to l_1 + x$, $l_4 \to l_4 + l_2 x$, $l_{2t} \to l_{2t-3} x$ for $t \geq 3$.

TABLE 2. Additive Automorphism

	$t_{0,x}$	$t_{1,x}$	$t_{2,x}$
p_1	$+x$		
p_2		$+p_1 x$	$+x$
p_3	$+p_2 x$		$-p_1 x$
p_4		$+2p_2 x + p_1 x^2$	
p_5	$+p_4 x$	$+p_3 x$	$-p_2 x$
p_{4t+1}	$+p_{4t} x$	$+p_{4t-1} x$	$-p_{4t-3} x$
p_{4t+2}		$+p_{4t-1} x$	$+p_{4t-2} x$
p_{4t+3}	$+p_{4t+2} x$	$-p_{4t} x$	$-p_{4t-1} x$
p_{4t}		$+p_{4t-2} x + p_{4t-3} x + p_{4t-5} x^2$	$+p_{4t-4} x$
l_1		$+x$	
l_2	$+l_1 x$		$-x$
l_3	$+2l_2 x + l_1 x^2$		
l_4		$+l_2 x$	$+l_1 x$
l_5	$+l_4 x$		$-l_2 x$
l_{4t+1}	$+l_{4t} x$		$-l_{4t-3} x$
l_{4t+2}	$+l_{4t} x$	$+l_{4t-1} x$	$+l_{4t-2} x$
l_{4t+3}	$+l_{4t+2} x + l_{4t+1} x + l_{4t} x^2$		$-l_{4t-1} x$
l_{4t}		$+l_{4t-3} x$	$+l_{4t-4} x$

(2) For $2 \leq j \leq k$, $t_{j,x}$ is a map which keeps the first $j-1$ coordinates of a point and a line the same. In Table 3, each entry illustrates how each coordinate is changed under the corresponding map.

TABLE 3. Additive Automorphism (Continued)

$j \equiv 2\ ,\ 3 \mod 4$				$j \equiv 0\ ,\ 1 \mod 4$			
	$t_{j,x}$		$t_{j,x}$		$t_{j,x}$		$t_{j,x}$
p_i $i \le j-1$		l_i $i \le j-1$		p_i $i \le j-1$		l_i $i \le j-1$	
p_j	$+x$	l_j	$-x$	p_j	$+x$	l_j	$-x$
p_{j+1+2t}		l_{j+1+2t}		p_{j+1+2t}		l_{j+1+2t}	
p_{j+2}		l_{j+2}	$+l_1x$	p_{j+2}	$-p_1x$	l_{j+2}	
p_{j+4+2t}	$+p_{2t+2}x$	l_{j+4+2t}	$+l_{2t+2}x$	p_{j+4+2t}	$-p_{2t+2}x$	l_{j+4+2t}	$-l_{2t+2}x$

Proposition 4. *For any $x \in \mathbb{F}_q$, and any $0 \le j \le k$, $t_{j,x}$ is an automorphism of $D(k,q)$.*

6.2.3. *Polarity Automorphism.* Consider the map $\phi : \mathcal{P}_k \to \mathcal{L}_k, \mathcal{L}_k \to \mathcal{P}_k$ such that

$$(p_1,p_2,p_3,p_4,\dots,p_{k-1},p_k) \xrightarrow{\phi} \begin{cases} [p_1,p_2,p_4,p_3,\dots,p_k,p_{k-1}] & \text{if } k \text{ is even} \\ [p_1,p_2,p_4,p_3,\dots,p_{k-1},p_{k-2},p_k] & \text{if } k \text{ is odd} \end{cases}$$

and

$$[l_1,l_2,l_3,l_4,\dots,l_{k-1},l_k] \xrightarrow{\phi} \begin{cases} (l_1,l_2,l_4,l_3,\dots,l_k,l_{k-1}) & \text{if } k \text{ is even} \\ (l_1,l_2,l_4,l_3,\dots,l_{k-1},l_{k-2},l_k) & \text{if } k \text{ is odd} \end{cases}$$

Proposition 5. *If k is even, or q is even, then ϕ is an automorphism of $D(k,q)$.*

Theorem 15. ([59]) *For any integer $k \ge 2$, and any prime power q, the automorphism group of $D(k,q)$ is transitive on $\mathcal{P}_k$, is transitive on $\mathcal{L}_k$, and the graph is edge-transitive. If any one of k and q is even, then $D(k,q)$ is vertex-transitive.*

6.3. **Girth of $D(k,q)$.** Lazebnik and Ustimenko in [59] showed that $girth(D(k,q)) \ge k+5$ for odd k. Here we present a proof of this result by using the new notation for graphs $D(k,q)$ and correct a minor drawback in their original proof.

Theorem 16. ([59]) *Let $k \ge 3$ be an odd integer, and q be a prime power, then $girth(D(k,q)) \ge k+5$.*

Proof. The idea of the proof is the following:
For any two distinct vertices $x, y \in V(D(k,q))$ and any integer $2 \le m \le (k+3)/2$, we show that there is at most one path in $D(k,q)$ of length m with the endpoints x and y.
We consider the following two cases.

Case 1: $k = 4r-3$ with $r \ge 2$.

Lemma 1. *If $[l^1] = [0] \sim (p^1) = (0) \sim [l^2] \sim (p^2) \sim \cdots \sim [l^r] \sim (p^r) \sim [l^{r+1}]$ is a path of length $2r$, where for any $1 \le i \le r+1$,$[l^i] = [l^i_1, \cdots, l^i_k]$, and for any $1 \le i \le r$, $(p^i) = (p^i_1, \cdots, p^i_k)$, then we have the following:*

(1) For any $2 \le i \le r$, $l^i_{4i-5} = l^i_{4i-4} = l^i_{4i-3} = p^i_{4i-3} = p^i_{4i-5} = p^i_{4i-2} = 0$.
(2) For any $3 \le i \le r$, $l^i_{4i-7} = 0$ *and* $l^2_2 = 0$.
(3) For all $2 \le i \le r$, $l^{i+1}_{4i-4} \neq 0$.

Proof. If $[l^1] \sim (p^1) \sim [l^2] \sim (p^2) \sim \cdots \sim [l^r] \sim (p^r) \sim [l^{r+1}]$ is a path, then $l^i_1 \neq l^{i+1}_1$ for $i = 1, \cdots, r$, and $p^i_1 \neq p^{i+1}_1$ for $i = 1, \cdots, r-1$. In particular, $l^2_1 \neq 0$ and $p^2_1 \neq 0$.
Since $(p^1) = (0)$, we have $[l^2] = [l^2_1, 0, 0, \cdots, 0]$. Also, it is easy to check that $(p^2) = (p^2_1, p^2_2, 0, p^2_4, 0, 0, \cdots, 0)$.
We next show that for $3 \le i \le r$,

$$l^i_{4i-7} = l^i_{4i-5} = l^i_{4i-4} = \cdots = l^i_{4r-3} = 0,$$

and for $2 \le i \le r$

$$p^i_{4(i-1)-1} = p^i_{4(i-1)+1} = p^i_{4(i-1)+2} = \cdots = p^i_{4r-3} = 0.$$

To prove this, we begin with the following claim.

Claim 1. *Let* $2 \le i \le r-1$. *If* $p^i_{4(i-1)-1} = p^i_{4(i-1)+1} = p^i_{4(i-1)+2} = \cdots = p^i_{4r-3} = 0$, *then* $l^{i+1}_{4i-3} = l^{i+1}_{4i-1} = l^{i+1}_{4i} = \cdots = l^{i+1}_{4r-3} = 0$.

Indeed, since $[l^{i+1}] \sim (p^i)$, for any $j \ge i$, we have the following,

$$l^{i+1}_{4j-3} + p^i_{4j-3} = p^i_{4j-5} l^{i+1}_1, \quad l^{i+1}_{4j-1} + p^i_{4j-1} = p^i_1 l^{i+1}_{4j-3}$$
$$l^{i+1}_{4j} + p^i_{4j} = p^i_{4j-2} l^{i+1}_1, \quad l^{i+1}_{4j+2} + p^i_{4j+2} = p^i_1 l^{i+1}_{4j}$$

Since $p^i_{4j-5} = p^i_{4j-3} = p^i_{4j-2} = p^i_{4j} = 0$ for $j \ge i$, we have $l^{i+1}_{4j-3} = l^{i+1}_{4j-1} = l^{i+1}_{4j} = l^{i+1}_{4j+2} = 0$ for $j \ge i$. Therefore, Claim 1 holds.

Now we prove part (2) of Lemma 1 by induction on i. In the case of $i = 2$, it is trivial since $p^2_3 = p^2_5 = p^2_6 = \cdots = p^2_{4r-3} = 0$. Let (2) hold for $i \ge 2$, which means that $p^i_{4(i-1)-1} = p^i_{4(i-1)+1} = p^i_{4(i-1)+2} = \cdots = p^i_{4r-3} = 0$. By Claim 1,

$$l^{i+1}_{4i-3} = l^{i+1}_{4i-1} = l^{i+1}_{4i} = \cdots = l^{i+1}_{4r-3} = 0.$$

Since $(p^{i+1}) \sim [l^{i+1}]$, for any $j \ge i$, we have the following,

$$p^{i+1}_{4j-1} + l^{i+1}_{4j-1} = p^{i+1}_1 l^{i+1}_{4j-3}, \quad p^{i+1}_{4j+1} + l^{i+1}_{4j+1} = p^{i+1}_{4j-1} l^{i+1}_1$$
$$p^{i+1}_{4j+2} + l^{i+1}_{4j+2} = p^{i+1}_1 l^{i+1}_{4j}, \quad p^{i+1}_{4j+4} + l^{i+1}_{4j+4} = p^{i+1}_{4j+2} l^{i+1}_1$$

Since $l^{i+1}_{4j-3} = l^{i+1}_{4j-1} = l^{i+1}_{4j} = l^{i+1}_{4j+2}$ for $j \ge i$, we have $p^{i+1}_{4j-1} = p^{i+1}_{4j+1} = p^{i+1}_{4j+2} = p^{i+1}_{4j+4} = 0$ for $j \ge i$. Therefore, part (2) holds, then by Claim 1, part (1) also holds.

Finally, we show part (3) also holds. In the case of $i = 2$, we have

$$l^3_4 + p^2_4 = p^2_2 l^3_1,$$

and hence,

$$l^3_4 = p^2_2 l^3_1 - p^2_4 = p^2_2 l^3_1 - (p^2_2 l^2_1 - l^2_4) = p^2_2 (l^3_1 - l^2_1) = (p^2_1 l^2_1 - l^2_2)(l^3_1 - l^2_1)$$
$$= p^2_1 l^2_1 (l^3_1 - l^2_1) \neq 0.$$

For $3 \leq i \leq r$, since $[l^{i+1}] \sim (p^i)$, we have

$$l^{i+1}_{4i-4} + p^i_{4i-4} = p^i_{4i-6} l^{i+1}_1,$$

and hence,

$$\begin{aligned} l^{i+1}_{4i-4} &= p^i_{4i-6} l^{i+1}_1 - p^i_{4i-4} \\ &= p^i_{4i-6} l^{i+1}_1 + l^i_{4i-4} - p^i_{4i-6} l^i_1 \\ &= p^i_{4i-6}(l^{i+1}_1 - l^i_1) \\ &= (p^i_1 l^i_{4i-8} - l^i_{4i-6})(l^{i+1}_1 - l^i_1) \\ &= (p^i_1 l^i_{4i-8} - p^{i-1}_1 l^i_{4i-8})(l^{i+1}_1 - l^i_1) \\ &= (p^i_1 - p^{i-1}_1)(l^{i+1}_1 - l^i_1) l^i_{4i-8}. \end{aligned}$$

The third equality holds since $l^i_{4i-4} = 0$ for $2 \leq i \leq r$, and the fifth equality holds since $p^{i-1}_{4i-6} = 0$. As $p^i_1 \neq p^{i-1}_1$ and $l^{i+1}_1 \neq l^i_1$, we have $l^{i+1}_{4i-4} \neq 0$ for any $2 \leq i \leq r$. □

Claim 2. *Let $[l]$ and $[m]$ be two lines in $D(k,q)$, then for every i, $1 \leq i \leq r$, all the paths connecting $[l]$ and $[m]$ of length $2i$ pass through a common point.*

Proof. Suppose that there is a path P of length $2i$ connecting $[l]$ and $[m]$. Let P be $[l] = [\tilde{l}^1] \sim (\tilde{p}^1) \sim \cdots \sim [\tilde{l}^i] \sim (\tilde{p}^i) \sim [\tilde{l}^{i+1}] = [m]$. We want to show that $(\tilde{p}^1)$ is uniquely determined by $[l]$ and $[m]$.
Since $D(k,q)$ is transitive on $\mathcal{L}_k$ by Theorem 15, there is $\alpha \in Aut(D(k,q))$ such that $[\tilde{l}^1]^\alpha = [0]$. Let the first coordinate of $(\tilde{p}^1)^\alpha$ be z, i.e., $(\tilde{p}^1)^\alpha = (z, 0, \ldots, 0)$. Then $\beta = t_{2,-z}$ is an automorphism such that $(\tilde{p}^1)^{\alpha\beta} = (0, \ldots)$. Now let $(p^j) = (\tilde{p}^j)^{\alpha\beta}$ and $[l^j] = [\tilde{l}^j]^{\alpha\beta}$ for any $j \geq 1$. Hence $[l^1] = [0]^\beta = [0]$, and $(p^1) = (0)$. Suppose that $[\tilde{l}^{i+1}]^\alpha = [a_1, a_2, \cdots, a_{4r-3}]$, then

$$[l^{i+1}] = [a_1, a_2, \cdots, a_{4r-3}]^\beta = [a_1, a_2 - a_1 z, \cdots, a_{4r-4}, a_{4r-3} - a_{4r-4} z].$$

Therefore,

$$\begin{aligned} l^{i+1}_{4i-4} &= a_{4i-4}, \\ l^{i+1}_{4i-3} &= a_{4i-3} + a_{4i-4} z. \end{aligned}$$

As $l^{i+1}_{4i-3} + p^i_{4i-3} = p^i_{4i-5} l^{i+1}_1$, and $p^i_{4i-3} = p^i_{4i-5} = 0$, by Lemma 1 part (1), we have $l^{i+1}_{4i-3} = 0$. Therefore,

$$a_{4i-3} + a_{4i-4} z = 0.$$

Since $l^{i+1}_{4i-4} \neq 0$ by Lemma 1 part (3), we have $a_{4i-4} \neq 0$, and hence

$$z = \frac{-a_{4i-3}}{a_{4i-4}}.$$

So z is uniquely determined by $[\tilde{l}^{i+1}]^\alpha = [m]^\alpha$. Since z is the first coordinate of $(\tilde{p}^1)^\alpha$ with $(\tilde{p}^1)^\alpha = (z, 0, \ldots, 0)$, and α is determined by $[l]$, then $(\tilde{p}^1)$ is uniquely determined by $[l]$ and z, and hence uniquely determined by $[l]$ and $[m]$. □

Since $r = \frac{k+3}{4}$, we have $girth(D(k,q)) \geq k + 5$ by Claim 2. This finishes the proof of the Theorem 16.

Case 2: $k = 4r - 1$ with $r \geq 1$.
For $k = 3$, it is easy to show that the girth is 8 (see [58]). Now assume that $k \geq 7$. Since the projection of a path in $D(k, q)$ on the first $k - 2$ coordinates gives a path in $D(k - 2, q)$, then $girth(D(k, q)) \geq girth(D(k - 2, q)) \geq k + 3$. We wish to show that there is no cycle of length $k + 3 = 4r + 2$ in $D(k, q)$. Consider a path $[\tilde{l}^1] \sim (\tilde{p}^1) \sim [\tilde{l}^2] \sim \cdots \sim [\tilde{l}^{r+1}] \sim (\tilde{p}^{r+1})$ of length $2r + 1$ connecting a line $[\tilde{l}^1] = [l]$ and a point $(\tilde{p}^{r+1}) = (p)$. Let $\alpha \in Aut(D(k, q))$ be an automorphism such that $[\tilde{l}^1]^\alpha = [0]$. Then $(\tilde{p}^1)^\alpha = (z, 0, \ldots, 0)$. Assume that $(\tilde{p}^{r+1})^\alpha = (b_1, b_2, \ldots, b_k)$, and $\beta = t_{2,-z}$. Let $[l^i] = [\tilde{l}^i]^{\alpha\beta}$ and $(p^i) = (\tilde{p}^i)^{\alpha\beta}$, for $1 \leq i \leq r + 1$. Then $[l^1] = [0]$, $(p^1) = (0)$, and $l_1^i \neq l_1^{i+1}, p_1^i \neq p_1^{i+1}$ for $1 \leq i \leq r$.

Lemma 2. *For $r \geq 1$, $l_{4r-3}^{r+1} = l_{4r-1}^{r+1} = 0$, and $p_{4r-2}^{r+1} \neq 0$.*

Proof. Since $l_{4r-3}^{r+1} + p_{4r-3}^r = l_1^{r+1} p_{4r-5}^r$, and $p_{4r-5}^r = p_{4r-3}^r = 0$ by Lemma 1 part (1), we have $l_{4r-3}^{r+1} = 0$. Therefore, combined with Lemma 1 part (1), we obtain $l_{4r-1}^{i+1} - l_{4r-1}^i = (p_1^{i+1} - p_1^i) l_{4r-3}^{i+1} = 0$ for any $1 \leq i \leq r$. As $l_{4r-1}^1 = 0$, we have $l_{4r-1}^{r+1} = 0$. Therefore, we have

$$\begin{aligned} p_{4r-2}^{r+1} &= p_1^{r+1} l_{4r-4}^{r+1} - l_{4r-2}^{r+1} \\ &= p_1^{r+1} l_{4r-4}^{r+1} - (p_1^r l_{4r-4}^{r+1} - p_{4r-2}^r) \\ &= (p_1^{r+1} - p_1^r) l_{4r-4}^{r+1}, \end{aligned}$$

the last equality holds by Lemma 1 part (1) again. Since $l_{4r-4}^{r+1} \neq 0$ by Lemma 1 part (3), and $p_1^{r+1} \neq p_1^r$, we have $p_{4r-2}^{r+1} \neq 0$. □

Since $(p^{r+1}) = (b_1, b_2, \ldots, b_k)^{t_{2,-z}}$, then $(p^{r+1}) = (b_1 - z, b_2 - z, \ldots, b_{4r-2}, b_{4r-1} - b_{4r-2} z)$. As $[l^{r+1}] \sim (p^{r+1})$, we have

$$l_{4r-1}^{r+1} + (b_{4r-1} - b_{4r-2} z) = p_1^{r+1} l_{4r-3}^{r+1},$$

where $l_{4r-3}^{r+1} = 0$ by Lemma 2. Therefore,

$$l_{4r-1}^{r+1} + b_{4r-1} - b_{4r-2} z = 0.$$

where $l_{4r-1}^{r+1} = 0$, $b_{4r-2} = p_{4r-2}^{r+1} \neq 0$ by Lemma 2. Therefore, the last equality considered as an equation with respect to z, has a unique solution. Similarly as in Case 1, this implies that $D(k, q)$ has no cycles of length $4r + 2 = k + 3$. This finishes the proof of Theorem 16. □

Corollary 2. *Let $k \geq 2$ be an even integer, and q be a prime power, then*

$$girth(D(k, q)) \geq k + 4.$$

The following conjecture was stated in [34] for all $q \geq 5$, and here we extend it to the case where $q = 4$.

Conjecture 5. *$D(k, q)$ has girth $k + 5$ for k odd and $k + 4$ for k even, and all prime powers $q \geq 4$.*

For the following values of k, and q, Conjecture 5 was confirmed ([83], [89], [90]) by using computers.

$$q = 4, 5, \quad 2 \le k \le 14.$$
$$q = 7, \quad 2 \le k \le 8.$$
$$q = 8, 9, \quad 2 \le k \le 7.$$
$$q = 11, 13, \quad 2 \le k \le 6.$$
$$q = 16, 17, 19, 23, \quad 2 \le k \le 4.$$
$$q = 25, 27, 29, 31, 37, 41, 43, 47, 49, \quad k = 2, 3.$$

For $q = 3$, the girth of $D(k, 3)$ exhibits different behavior, and we do not understand it completely. The following table provides the values of the girth for $2 \le k \le 26$.

TABLE 4. Girth of $D(k, 3)$ for small k

k	2	3	4	5	6	7	8	9	10	11	12	13	14
girth	6	8	12	12	12	12	12	18	18	18	18	18	18
k	15	16	17	18	19	20	21	22	23	24	25	26	
girth	20	20	24	24	24	28	28	28	28	28	34	34	

Problem 8. *Determine the girth of $D(k, 3)$ for all $k \ge 2$.*

Conjecture 5 was proved only for infinitely many pairs of (k, q).

Theorem 17. ([34]) *For any $k \ge 3$ odd, and q being a member of the arithmetic progression $\{1 + n(\frac{k+5}{2})\}_{n\ge1}$,*

$$girth(D(k, q)) = k + 5.$$

By modifying an idea from [34], Lazebnik and Sun [56] could strengthen this result.

Theorem 18. ([56]) *Let $k \equiv 3 \mod 4$, and for $q \ge 4$ with $\frac{k+5}{4}|(q-1)$, $girth(D(k, q)) = k + 5$.*

In [18], Cheng, Chen and Tang found another sequence of pairs (k, q) for which the girth of $D(k, q)$ could be determined precisely.

Theorem 19. ([18]) *For any $q \ge 4$, and any odd k such that $(k + 5)/2$ is a power of the characteristic of $\mathbb{F}_q$,*

$$girth(D(k, q)) = k + 5.$$

Recently, the same authors generalized this result.

Theorem 20. ([19]) *For any prime p, and any positive integers h, m, s with $h|(p^m - 1)$ and $hp^s > 3$,*

$$girth(D(2hp^s - 4, p^m)) = girth(D(2hp^s - 5, p^m)) = 2hp^s.$$

Suppose the girth of $D(k,q)$ satisfies Conjecture 5. Then the following theorem allows us to determine the exact value of the girth of $D(k',q)$ for infinitely many values of k', namely, $k' = p^m girth(D(k,q)) - 4$ and $k' = p^m girth(D(k,q)) - 5$ for an arbitrary positive integer m.

Theorem 21. ([56]) *Let $k \geq 3$, and p be the characteristic of $\mathbb{F}_q$. Let $g_k = girth(D(k,q))$. If g_k satisfies Conjecture 5, then*

$$girth(D(pg_k - 4, q)) = pg_k,$$

and

$$girth(D(pg_k - 5, q)) = pg_k.$$

By Theorems 17, 18, 21, Conjecture 5 is true for $(k+5)/2$ being the product of a factor of $q-1$ which is at least 4 and a power of the characteristic of $\mathbb{F}_q$, and for $(k+5)/4$ being the product of a factor of $q-1$ which is at least 2 and a power of the characteristic of $\mathbb{F}_q$.

6.4. **Connectedness of $D(k,q)$.** Let $c(G)$ be the number of components of a graph G. In [62], Lazebnik, Ustimenko and Woldar proved that for $k \geq 6$ and q odd, graphs $D(k,q)$ are disconnected. As graphs $D(k,q)$ are edge-transitive, all components are isomorphic. Let $CD(k,q)$ denote one of them. It was shown in [62] 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 $2q^{k-t+1}$. Moreover, in [63], the same authors proved that for all odd q, $c(D(k,q)) = q^{t-1}$. Lazebnik and Viglione [68] showed that $c(D(k,q)) = q^{t-1}$ for even $q > 4$, $c(D(k,4)) = q^t$ for $k \geq 4$, and $c(D(2,4)) = c(D(3,4)) = 1$.

In order to characterize the components, we begin with the notion of an invariant vector of the component (see [62]).

6.4.1. *Invariant vector.* Let $k \geq 6$ and $t = \lfloor \frac{k+2}{4} \rfloor$. For every point $(p) = (p_1, \ldots, p_k)$ and every line $[l] = [l_1, \ldots, l_k]$ in $D(k,q)$, and for any $2 \leq r \leq t$, let $a_r : \mathcal{P}_k \cup \mathcal{L}_k \to \mathbb{F}_q$ be given by:

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

and

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

For example,

$$a_3((p)) = p_1p_8 - p_2p_6 - p_2p_5 + p_3p_4 - p_9 + p_{10},$$

and

$$a_3([l]) = l_1l_7 - l_2l_6 - l_2l_5 + l_3l_4 + l_9 - l_{10}.$$

The *invariant vector* $\vec{a}(u)$ of a vertex u is defined as:

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

The following proposition justifies the term.

Theorem 22. ([62]) *If $(p) \sim [l]$, then $\vec{a}((p)) = \vec{a}([l])$.*

Proof. Since $(p) \sim [l]$, then each component of $[l]$ can be written in terms of (p) and l_1 in the following way:

$$\begin{aligned}
&l_2 = p_1 l_1 - p_2 \\
&l_3 = p_1^2 l_1 - p_1 p_2 - p_3 \\
&l_i = p_{i-2} l_1 - p_i && \text{for i} \equiv 0\ ,\ 1 \mod 4 \\
&l_i = p_1 p_{i-4} l_1 - p_1 p_{i-2} - p_i && \text{for i} \equiv 2\ ,\ 3 \mod 4
\end{aligned}$$

If $r = 2$,

$$\begin{aligned}
&a_2([l]) \\
&= -l_1(p_1^2 l_1 - p_1 p_2 - p_3) + p_1^2 l_1^2 + p_2^2 - 2p_1 l_1 p_2 - p_3 l_1 + p_5 + p_1 p_2 l_1 - p_1 p_4 - p_6 \\
&= -l_1^2 p_1^2 + p_1 p_2 l_1 + p_3 l_1 + p_1^2 l_1^2 + p_2^2 - 2p_1 p_2 l_1 - p_3 l_1 + p_5 + p_1 p_2 l_1 - p_1 p_4 - p_6 \\
&= p_2^2 - p_1 p_4 + p_5 - p_6 \\
&= a_2((p)).
\end{aligned}$$

Now, for $r \geq 3$, we have the following:

$$\begin{aligned}
a_r([l]) = (-1)^{r-1}[&p_1 p_{4r-9} l_1^2 - p_1 p_{4r-7} l_1 - p_{4r-5} l_1 - (p_1 l_1 - p_2)(p_1 p_{4r-10} l_1 - \\
&p_1 p_{4r-8} - p_{4-6}) - (p_1 l_1 - p_2)(p_{4r-9} l_1 - p_{4r-7}) + (p_1^2 l_1 - p_1 p_2 - p_3) \\
&(p_{4r-10} l_1 - p_{4r-8}) + p_{4r-5} l_1 - p_{4r-3} - p_1 p_{4r-6} l_1 + p_1 p_{4r-4} + p_{4r-2} - \\
&\sum_{i=2}^{r-2} (p_{4i-5} l_1 - p_{4i-3})(p_1 p_{4(r-i-1)-2} l_1 - p_1 p_{4(r-i-1)} - p_{4(r-i)-2}) + \\
&\sum_{i=2}^{r-2} (p_{4(r-i-1)-2} l_1 - p_{4(r-i-1)})(p_1 p_{4i-5} l_1 - p_1 p_{4i-3} - p_{4i-1}) \\
= (-1)^{r-1}[&p_1 p_{4r-4} - p_2 p_{4r-6} - p_2 p_{4r-7} + p_3 p_{4r-8} - p_{4r-3} + p_{4r-2} + \\
&\sum_{i=2}^{r-2} (-p_{4i-3} p_{4(r-i)-2} + p_{4i-1} p_{4(r-i)-4})] \\
= a_r((p)).
\end{aligned}$$

□

Corollary 3. *All the vertices in the same component of $D(k, q)$ have the same invariant vector.*

A natural question at this point is whether the equality of invariant vectors of two vertices of $D(k, q)$ implies that the vertices are in the same component. The answer is affirmative for $k \geq 6$ and $q \neq 4$, and we will discuss it later in this paper.

Let (0) denote the point corresponding to zero vector. By Corollary 3, and the fact that $\vec{a}((0)) = \vec{0}$, we have the following:

Theorem 23. *Let u be in the component of $D(k, q)$ containing (0). Then*

$$\vec{a}(u) = \vec{0}.$$

6.4.2. *Lower Bound on $c(D(k,q))$.*

Theorem 24. ([62]) *For any $k \geq 2$, and q be a prime power, let $t = \lfloor \frac{k+2}{4} \rfloor$. Then*

$$c(D(k,q)) \geq q^{t-1}.$$

Proof. Let $x = (x_2, \ldots, x_t)$ and $y = (y_2, \ldots, y_t)$ be distinct vectors in $\mathbb{F}_q^{t-1}$. Consider points $(p) = (p_1, \ldots, p_k)$, and $(p') = (p'_1, \ldots, p'_k)$ be defined by:

$$p_j = \begin{cases} x_{\frac{j-2}{4}} & \text{if } j \equiv 2 \mod 4, \\ 0 & \text{otherwise.} \end{cases}$$

and

$$p'_j = \begin{cases} y_{\frac{j-2}{4}} & \text{if } j \equiv 2 \mod 4, \\ 0 & \text{otherwise.} \end{cases}$$

It is easy to see that $\vec{a}((p)) = x \neq y = \vec{a}((p'))$, and by Corollary 3, (p) and (p') are in different components. Therefore, there are at least q^{t-1} components. □

6.4.3. *Projections and Lifts.* For $k \geq 3$, the *projection*

$$\pi : V(D(k,q)) \to V(D(k-1,q))$$

is defined via

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

As we mentioned in Section 3.2, π is a graph homomorphism of $D(k,q)$ to $D(k-1,q)$. 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 group of all such automorphisms is denoted by $Stab(B)$. A component of $D(k,q)$ containing a vertex v will be denoted by $C(v)$. The point and line corresponding to the 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 $D(k-1,q)$.

Theorem 25. ([63]) *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 $Stab(C)$ for all $x, a, b \in \mathbb{F}_q$, $a, b \neq 0$.*

Theorem 26. ([63]) *Let B be a component of $D(k,q)$. Then π_B is a t-to-1 graph homomorphism for some t, $1 \leq t \leq q$. In particular, let $k \equiv 0,\ 3 \mod 4$, and suppose π_C is a t-to-1 mapping for some $t > 1$. Then $t = q$.*

Theorem 27. ([63]) *The map $\pi_C : V(C) \to V(C')$ is surjective.*

6.4.4. *Exact Number of Components for $q \neq 4$.*

Theorem 28. ([68]) *Let q be a prime power, $q \neq 4$, and $k \geq 6$. If $v \in V(D(k,q))$ satisfies $\vec{a}(v) = \vec{0}$, then $v \in V(C)$.*

Proof. The proof proceeds by induction on k. It is known([63]) that for $q \neq 4$, graphs $D(k,q)$ are connected for $k = 2, 3, 4, 5$.
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 Theorem 27, 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 $v = w \in V(C)$.
Suppose that the theorem is true for $k' < k$, with $k \geq 7$.
If $k \equiv 2 \mod 4$, 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 $\vec{a}(v') = \vec{0}$. 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 $v \in V(C)$.
If $k \equiv 0,\ 1,\ 3 \mod 4$, we want to show that π_C is a q-to-1 map. (In the case of $k \equiv 0,\ 3 \mod 4$, it suffices to show that there is a point $(p') \in V(C')$ which has two lifts to $D(k,q)$ in $V(C)$ by Theorem 26.) These are exactly the values of k for which the invariant vectors of C and C' are the same. 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 $\vec{a}(v) = \vec{a}(v') = \vec{0}$, then $v' \in C'$ 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 these cases.

Case 1: $k \equiv 3 \mod 4$. Let $(p') \in V(D(k-1,q))$ be

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

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

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

Note that:

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

Since $t_{0,1}$, $t_{1,1} \in Stab(C)$ by Theorem 25, all the vertices above are in $V(C)$. Hence (p') has two lifts to $D(k,q)$ in C.

Case 2: $k \equiv 0 \mod 4$. Write $k = 4j$, $j \geq 2$. Let $(p') \in V(D(k-1,q))$ be

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

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 $y \in \mathbb{F}_q$,

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

First suppose $y \neq 0$. Then

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

One can always choose $a, b \in \mathbb{F}_q^*$ such that $ab = 1$ but $b \neq 1$. With this choice of a and b, we have

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

by Theorem 25. Since $y \neq 0$, and $b \neq 1$, (p') has two lifts to $D(k,q)$ in C.
Now suppose $y = 0$, then

$$(0) \xrightarrow{t_{4j-3,1}} (0, \ldots, 0, 1, 0, 0, 0) \xrightarrow{t_{4j-2,1}} (p).$$

Therefore, $t_{4j-3,1} t_{4j-2,1} \in Stab(C)$ by Theorem 25. Now let (p') be

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

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 $y \in \mathbb{F}_q$,

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

Note that:

$$(p) \xrightarrow{t_{1,-1}} (0, \ldots, 0, 1, 1, -1, -1, 0, y+1) \xrightarrow{t_{4j-3,1}t_{4j-2,1}} (0, \ldots, 0, 1, 1, 0, 0, 0, y+1).$$

Since $t_{1,-1}$, $t_{4j-3,1}t_{4j-2,1} \in Stab(C)$ by Theorem 25, all the vertices above are in $V(C)$. Hence (p') has two lifts to $D(k,q)$ in C.

Case 3: $k \equiv 1 \mod 4$. Write $k = 4j-3$, $j \geq 3$. For any $x \in \mathbb{F}_q$, let $(p') \in V(D(k-1,q))$ be

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

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 $y \in \mathbb{F}_q$,

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

It can be verified that (p) is stabilized by $t_{1,x}t_{4j-3,-x}$, hence $t_{1,x}t_{4j-3,-x} \in Stab(C)$ by Theorem 25. Since $t_{1,x} \in Stab(C)$, we have $t_{4j-3,-x} \in Stab(C)$ for any $x \in \mathbb{F}_q$. Thus $(0, \ldots, 0, -x) = (0)^{t_{4j-3,-x}} \in V(C)$, and (0) has q distinct lifts to C. Thus π_C is q-to-1. □

Theorem 29. ([68]) *Let q be a prime power $q \neq 4$, $k \geq 2$ be an integer, and $t = \lfloor \frac{k+2}{4} \rfloor$. Then $c(D(k,q)) = q^{t-1}$.*

Proof. We have already mentioned (see the beginning of the proof of Theorem 28) that for $2 \leq k \leq 5$, and $q \neq 4$, $D(k,q)$ is 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, hence all its components are isomorphic.
Let $k \geq 6$. Combining Theorem 23 and Theorem 28, 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 $r \geq 2$. For $3 \leq r \leq t$, and arbitrary $p_1, \ldots, p_5$, $p_{4r-3}, p_{4r-4}, p_{4r-5}$ and $p_{4t-1}, \ldots, p_k$, we can uniquely solve for p_{4r-2} for $2 \leq r \leq t$. Therefore, there are $q^{5+3(t-2)+k-(4t-2)} = q^{k-t+1}$ points in C.
Since the total number of points in $D(k,q)$ is q^k, and all its components are isomorphic, we have

$$c(D(k,q)) = \frac{q^k}{q^{k-t+1}} = q^{t-1}.$$

□

We will show that the invariant vector of a vertex characterizes the component containing the vertex.

Corollary 4. ([68]) *Let $k \geq 6$, and $q \neq 4$. 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 Theorem 22, we know that f is well

defined, i.e., $C(u) = C(v)$ implies $\vec{a}(u) = \vec{a}(v)$. By Theorem 29, $|X| = q^{t-1}$, so that f is bijective. Thus $C(u) = C(v)$ whenever $\vec{a}(u) = \vec{a}(v)$. □

6.4.5. *Exact Number of Components for $D(k, 4)$.* In order to deal with the case $q = 4$, we will need an analog of Theorem 28. We begin by defining an invariant vector for $D(k, 4)$. Its definition is very close to $\vec{a}$ defined before, 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

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

where $b_i = a_i$ for all $i \geq 2$ and

$$b_1((p)) = p_1p_2 + p_3 + p_4^2,$$
$$b_1([l]) = l_1l_2 + l_3^2 + l_4.$$

The following statement is analogous to Theorem 23.

Theorem 30. ([68]) *Let u be in the component of $D(k, 4)$ containing (0). Then*

$$\vec{b}(u) = \vec{0}.$$

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

$$(p) = (p_1, p_2, p_3, p_4, \ldots) \sim [l_1, p_2 + p_1l_1, p_3 + p_1p_2 + p_1^2l_1, p_4 + p_2l_1, \ldots] = [l].$$

Theorem 23 gives us that $b_i([l]) = b_i((p)) = 0$ for all $i \geq 2$. By assumption $b_1((p)) = p_1p_2 + p_3 + p_4^2 = 0$. Since we are in characteristic 2 field and $a^4 = a$ for any $a \in \mathbb{F}_4$,

$$b_1([l]) = l_1(p_2 + p_1l_1) + (p_3 + p_1p_2 + p_1^2l_1)^2 + (p_4 + p_2l_1) =$$
$$p_1^2p_2^2 + p_3^2 + p_4 = (p_1p_2 + p_3 + p_4^2)^2 = 0.$$

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 $\vec{b}((p)) = \vec{0}$. Therefore, if a vertex in C has invariant $\vec{0}$, so do all of its neighbors. Since C is connected and $\vec{b}(0) = \vec{0}$, all vertices in C must have invariant $\vec{0}$. □

The following Theorem is the analog of Theorem 28 for $q = 4$, and its proof is similar to the one of Theorem 28.

Theorem 31. ([68]) *Let $k \geq 4$. If $v \in V(D(k, 4))$ satisfies $\vec{b}(v) = \vec{0}$ then $v \in V(C)$.*

Similarly to the proof of Theorem 29, one can show that:

Theorem 32. ([68]) *$c(D(2, 4)) = c(D(3, 4)) = 1$, and $c(D(k, 4)) = 4^t$ with $k \geq 4$ and $t = \lfloor \frac{k+2}{4} \rfloor$.*

Remark 2. The analog of Corollary 4 does not hold for $q = 4$. The reason for this is the special first coordinate of the invariant vector. Indeed, let ω be a primitive element of $\mathbb{F}_4$. Then

$$(p) = (0, 0, \omega, 0, \ldots, 0) \sim [0, 0, \omega, 0, \ldots, 0] = [l],$$

in $D(k, 4)$, but

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

6.5. **Diameter of $CD(k,q)$.** Let $d(CD(k,q))$ denote the diameter of the graph $CD(k,q)$. For small values of k and q, we have the following computational results ([83],[89],[90]).

For $k=2$, the diameter of $CD(2,q)$ is 4 for $3 \le q \le 49$.
For $k=3$, the diameter of $CD(3,q)$ is 6 for $3 \le q \le 47$.
For $k \ge 4$, the diameter of $CD(k,q)$ is $k+4$ for k even, and $k+5$ for k odd, for the following pairs (k,q):

k	4	5	6	7	8	9 -12
q	3,5-23	5-13	5-13	5,7,8,9	5,7	5

For $q=3$ and $q=4$, the diameter exhibits different behavior.

TABLE 5. Diameter of $CD(k,3)$ for small k

k	2	3	4	5	6	7	8	9	10	11	12	13	14	15
diameter	4	6	8	12	12	12	14	17	17	22	22	24	24	26

TABLE 6. Diameter of $CD(k,4)$ for small k

k	2	3	4	5	6	7	8	9	10	11	12
diameter	4	6	6	8	8	10	12	16	16	16	18

Conjecture 6. ([64]) *There exists a positive constant C such that for all $k \ge 2$, and all prime powers q,*

$$d(CD(k,q)) \le (\log_{q-1} q)k + C.$$

The following conjecture was stated by Schliep [83].

Conjecture 7. ([83]) *The diameter of $CD(3,q)$ is 6 for all prime powers q. The diameter of $CD(k,q)$ is $k+5$, if $k>3$ is odd, and $k+4$, if k is even, provided that q is a large enough prime power.*

Some parts of Conjecture 7 were proved in [83], namely for $k=3$ and all odd prime powers q, and for $k=4$ and prime power q satisfying the following three conditions: q is odd, $(q-1,3)=1$, and either 5 is a square in $\mathbb{F}_q$ or $z^4-4z^2-z+1=0$ has a solution in $\mathbb{F}_q$. For the lower bound of the diameter, Schliep in [83] proved that for all odd $k>5$ and all prime powers q, $d(CD(k,q)) \ge k+3$. Recently, this bound was improved by Sun [86]: for all prime powers $q \ne 4$, $d(CD(k,q)) \ge k+5$ for odd $k \ge 5$, and $d(CD(k,q)) \ge k+4$ for even $k \ge 4$.

6.6. **Spectrum of $D(k,q)$.** We would like to end this section with a problem about the spectra of the graphs $D(k,q)$, which have the same eigenvalues as the graphs $CD(k,q)$, but with higher multiplicities. In particular, we wish to find the second largest eigenvalue λ_2 for these graphs, defined as the largest eigenvalue smaller than q. Though it is known to have a relation to the diameter of $CD(k,q)$, λ_2 is also related to other properties of these graphs, including the expansion properties (see Hoory, Linial and Wigderson [42] on such relations). It is known that for some q the graphs $D(k,q)$ are not Ramanujan, i.e., they have $\lambda_2 > 2\sqrt{q-1}$. This follows from computations performed first by Reichard [81], and soon after, and independently, by Thomason [90]. Later these computations were extended and confirmed by other researchers. At the same time we are not aware of any example of $D(k,q)$ with $\lambda_2 > 2\sqrt{q-1}+1$. For $k=2,3$, the corresponding λ_2 was determined in [72]. In [15], they were determined by another method, as for these values of k, graphs $D(k,q)$ are isomorphic to the first two members of the family of Wenger graphs. Very recently, Moorhouse, Sun and Williford [75] showed that for $CD(4,q)$, $\lambda_2 \le 2\sqrt{q}$, and determined the spectrum of $CD(4,q)$ for prime q.

Problem 9. *(i) Determine a good upper bound on $\lambda_2(D(k,q))$ for $k \ge 5$.*

(ii) Determine the spectrum of $D(k,q)$ for $k \ge 4$.

7. Applications of graphs $D(k,q)$ and $CD(k,q)$

7.1. **Bipartite graphs of given bi-degree and girth.** A bipartite graph Γ with bipartition $V_1 \cup V_2$ is said to be *biregular* if there exist integers r, s such that $\deg(x)=r$ for all $x \in V_1$ and $\deg(y)=s$ for all $y \in V_2$. In this case, the pair r,s is called the *bi-degree* of Γ. By an (r,s,t)*-graph* we shall mean any biregular graph with bi-degree r,s and girth exactly $2t$.

For which $r,s,t \ge 2$ do (r,s,t)-graphs exist? Trivially, $(r,s,2)$-graphs exist for all $r,s \ge 2$; indeed, these are the complete bipartite graphs. For all $r,t \ge 2$, Sachs [82], and Erdős and Sachs [28], constructed r-regular graphs with girth $2t$. From such graphs, $(r,2,t)$-graphs can be trivially obtained by subdividing (i.e. inserting a new vertex on) each edge of the original graph.

In [34] Füredi, Lazebnik, Seress, Ustimenko and Woldar showed, by explicit construction, that (r,s,t)-graphs exist for all $r,s,t \ge 2$. Their results can be viewed as biregular versions of the results from [82] and [28]. The paper [34] contains two constructions: a *recursive* one and an *algebraic* one. The recursive construction establishes existence for all $r,s,t \ge 2$, but the algebraic method works only for $r,s \ge t$. However, the graphs obtained by the algebraic method are much denser and exhibit the following nice property: one can construct an (r,s,t)-graph Γ such that for all $r \ge r' \ge t \ge 3$ and $s \ge s' \ge t \ge 3$, Γ contains an (r',s',t)-graph Γ' as an induced subgraph.

7.2. **Cages.** Let $k \ge 2$ and $g \ge 3$ be integers. A (k,g)-graph is a k-regular graph with girth g. A (k,g)*-cage* is a (k,g)-graph of minimum order. The problem of determining the order $\nu(k,g)$ of a (k,g)-cage is unsolved for most pairs (k,g) and is extremely hard in the general case. For the state of the art survey on cages, we refer the reader to Exoo and Jajcay [30].

In [64], Lazebnik, Ustimenko and Woldar established general upper bounds on $\nu(k,g)$ which are roughly the 3/2 power of the lower bounds (the previous results had upper bounds equal roughly the squares of lower bounds), and provided explicit

constructions for such (k, g)-graphs. The main ingredients of their construction were graphs $CD(n, q)$ and certain induced subgraphs of these, manufactured by the method described in Section 2.3. The precise result follows.

Theorem 33. [64] *Let $k \geq 2$ and $g \geq 5$ be integers, and let q denote the smallest odd prime power for which $k \leq q$. Then*

$$\nu(k, g) \leq 2kq^{\frac{3}{4}g-a},$$

where $a = 4,\ 11/4,\ 7/2,\ 13/4$ for $g \equiv 0, 1, 2, 3 \pmod 4$, respectively.

7.3. **Structure of extremal graphs of large girth.** Let $n \geq 3$, and let Γ be a graph of order ν and girth at least $n + 1$ which has the greatest number of edges possible subject to these requirements (i.e. an extremal graph). Must Γ contain an $(n+1)$-cycle? In [69] Lazebnik and Wang present several results where this question is answered affirmatively, see also [38]. In particular, this is always the case when ν is large compared to n: $\nu \geq 2^{a^2+a+1}n^a$, where $a = n - 3 - \lfloor \frac{n-2}{4} \rfloor$, $n \geq 12$. To obtain this result they used certain generic properties of extremal graphs, as well as of the graphs $CD(n, q)$.

8. Applications to coding theory and cryptography.

Dense graphs without short cycles have been used in coding theory in construction and analysis of Low-Density Parity-Check (LDPS) codes. See, e.g., Kim, Peled, Pless and Perepelitsa [45], Kim, Peled, Pless, Perepelitsa and Friedland [46], Kim, Mellinger and Storme [44], Sin and Xiang [85], Kumar, Pradhan, Thangaraj and Subramanian [54]. For the last sixteen years, V.A. Ustimenko and his numerous collaborators and students have been applying algebraically defined graphs and digraphs to coding theory and cryptography. We mention just a few recent papers, and many additional references can be found therein: Klisowski and Ustimenko [47], Wróblewska and Ustimenko [107] and Ustimenko [95].

Acknowledgments

The authors are grateful to Dr. Ye Wang for making her notes on graphs $D(k, q)$ available to the authors, to Mr. Ben Nassau for pointing to some typos, to Dr. Brian Kronenthal for several useful comments on the original version of the manuscript, and, especially, to an anonymous referee for several corrections and many useful suggestions. This work was partially supported by a grant from the Simons Foundation (#426092, Felix Lazebnik).

References

[1] E. Abajo and A. Diánez, *Graphs with maximum size and lower bounded girth*, Applied Math. Letters **25** (2012), 575–579.
[2] J. Alexander, Ph. D. Thesis, University of Delaware, 2016.
[3] N. Alon, S. Hoory and N. Linial, *Moore bound for irregular graphs*, Graphs Combin. **18**, no.1, (2002), 53–57.
[4] C. T. Benson, *Generalized Quadrangles and (B, N) Pairs*, Ph. D. Thesis, Cornel University, 1965.
[5] Berge, C., *Hypergraphs*, Combinatorics of Finite Sets, North–Holland, Amsterdam, 1989.
[6] Berge, C., *Hypergraphs*, in Selected Topics in Graph Theory 3, edited by Lowell W. Beineke and Robin J. Wilson, Academic Press Limited, (1998), 189-207.
[7] B. Bollobás, *Extremal Graph Theory*, Academic Press, London, 1978.

[8] B. Bollobás, *Modern Graph Theory*, Springer-Verlag New York Inc., 1998.
[9] J. A. Bondy and M. Simonovits, *Cycles of even length in graphs*, J. Combin. Theory, Ser. B **16**, (1974), 97–105.
[10] A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-Regular Graphs*, Springer-Verlag, Berlin, 1989.
[11] B. Bukh and Z. Jiang, *A bound on the number of edges in graphs without an even cycle*, arXiv preprint arXiv:1403.1601.
[12] D. de Caen and L. A. Székely, *The maximum size of 4– and 6–cycle free bipartite graphs on m, n vertices*, in Graphs, Sets and Numbers, Proc. of the Conference Dedicated to the 60th Birthdays of A. Hajnal and Vera T. Sós, Budapest, 1991, Coll. Math. Soc. J. Bolyai.
[13] X. Cao, M. Lu, D. Wan, L. -P. Wang and Q. Wang, *Linearized Wenger graphs*, Discrete Mathematics **338**, (2015), 1595-1602.
[14] P. Cara, S. Rottey and G. Van de Voorde, *A construction for infinite families of semisymmetric graphs revealing their full automorphism group*, J. Algebr. Comb. **39**, (2014), 967–988.
[15] S. M. Cioăba, F. Lazebnik and W. Li, *On the Spectrum of Wenger Graphs*, J. of Combin. Theory Ser. B **107**, (2014), 132–139.
[16] D. B. Chandler, Personal communication, August 2005.
[17] W. E. Cherowitzo, *Hyperovals in Desarguesian planes: an electronic update*, Informal notes, `http://www-math.cudenver.edu/~wcherowi/res.html`, February 2000.
[18] X. Cheng, W. Chen and Y. Tang, *On the girth of the bipartite graph $D(k, q)$*, Discrete Mathematics **335**, (2014), 25–34.
[19] X. Cheng, W. Chen and Y. Tang, *On the conjecture for the girth of the bipartite graph $D(k, q)$*, Discrete Mathematics **339**, (2016), 2384–2392.
[20] F. R. K. Chung and R. L. Graham, *On multicolor Ramsey numbers for complete bipartite graphs*, J. Combin. Theory Ser. B **18**, (1975), 164-169.
[21] D. M. Cvetković, M. Doob and H. Sachs, *Spectra of Graphs – Theory and Application*, Deutscher Verlag der Wissenschaften, Berlin, Academic Press, New York, 1980.
[22] V. Dmytrenko, *Classes of polynomial graphs*, Ph.D. thesis, University of Delaware, 2004.
[23] V. Dmytrenko, F. Lazebnik and R. Viglione, *An Isomorphism Criterion for Monomial Graphs*, J. Graph Theory **48**, (2005), 322–328.
[24] V. Dmytrenko, F. Lazebnik and J. Williford, *On monomial graphs of girth eight*, Finite Fields and Their Applications **13**, (2007), 828–842.
[25] P. Duchet, *Hypergraphs*, Handbook of Combinatorics, Volume 1, North–Holland, Amsterdam, 1985.
[26] P. Erdős, *Some recent progress on extremal problems in graph theory*, Congr. Numer. **14**, (1975), 3–14.
[27] P. Erdős, *Some old and new problems in various branches of combinatorics*, Proc. of the Tenth Southeastern Conference on Combinatorics, Graph Theory and Computing, Boca Raton, 1979, Vol. 1, Congressus Numerantium **23**, (1979), 19–38.
[28] P. Erdős and H. Sachs, *Reguläre Graphen gegebener Taillenweite mit minimaler Knotenzahl*, Wiss. Z. Univ. Halle Martin Luther Univ. Halle– Wittenberg Math.–Natur.Reine **12**, (1963), 251–257.
[29] P. Erdős and M. Simonovits, *Compactness results in extremal graph theory*, Combinatorica **2** (3), (1982), 275–288.
[30] J. Exoo and R. Jajcay, *Dynamic Cage Survey*, Electronic J. Combin., Dynamic Survey #DS16, (2013), 1–55.
[31] W. Feit and G. Higman, *The nonexistence of certain generalized polygons*, J. Algebra **1**, (1964), 114–131.
[32] Z. Füredi, *Turán Type Problems*, Survey's in Combinatorics, Cambridge University Press, Cambridge, 1991.
[33] Z. Füredi, *On the number of edges of quadrilateral-free graphs*, J. Combin. Theory Ser. B **68** (1), (1996), 1–6.
[34] Z. Füredi, F. Lazebnik, Á. Seress, V. A. Ustimenko and A. J. Woldar, *Graphs of prescribed girth and bi-degree*, J. Combin.Theory Ser. B **64** (2), (1995), 228-239.
[35] Z. Füredi, A. Naor, and J. Verstraëte, *On the Turan number for the hexagon*, Adv. Math. **203**, (2006), 476-496.

[36] Z. Füredi and M. Simonovits, *The history of degenerate (bipartite extremal graph problems)*, Erdős centennial, 169-264, Bolyai Soc. Math. Stud., 25, Janos Bolyai Math. Soc., Budapest, 2013.

[37] V. Futorny and V. Ustimenko, *On small world semiplanes with generalized Schubert cells*, Acta Appl. Math. **98**, (2007), 47–61.

[38] D. K. Garnick and N. A. Nieuwejaar, *Non-isomorphic extremal graphs without three-cycles and four-cycles*, J. Combin. Math. Combin. Comput. **12**, (1992), 33–56.

[39] D. G. Glynn, *Two new sequences of ovals in finite Desarguesian planes of even order*, Combinatorial mathematics, X (Adelaide, 1982), 217–229, Lecture Notes in Math. 1036, Springer, Berlin, 1983.

[40] D. G. Glynn, *A condition for the existence of ovals in* $\mathrm{PG}(2,q), q$ *even*, Geom. Dedicata **32** (2), (1989), 247–252.

[41] S.Hoory, *The Size of Bipartite Graphs with a Given Girth*, J. Comb. Theory Ser. B **86** (2), (2002), 215–220.

[42] S. Hoory, N. Linial and A. Wigderson, *Expander graphs and their application*, Bull. Amer. Math. Soc. **43**, (2006), 439-561.

[43] X. -D. Hou, S.D. Lappano and F. Lazebnik, *Proof of a Conjecture on Monomial Graphs*, (2016), to appear in Finite Fields and Their Applications.

[44] J. -L. Kim, K.E. Mellinger and L. Storme, *Small weight codewords in LDPC codes defined by (dual) classical generalized quadrangles*, Des. Codes Cryptogr. **42** (1), (2007), 73–92.

[45] J. -L. Kim, U. N. Peled, V. Pless and I. Perepelitsa, *Explicit Construction of LPDC codes with girth at least six*, Proceedings of the 40th Allerton Conference on Communication, Control and Computing, UIUC, October 2002.

[46] J. -L. Kim, U. N. Peled, V. Pless, I. Perepelitsa and S. Friedland, *Explicit Construction of LPDC codes with no 4-cycle*, Information Theory, IEEE Transactions, **50** (10), (2004), 2378 – 2388.

[47] M. Klisowski and V. Ustimenko, *On the comparison of cryptographical properties of two different families of graphs with large cycle indicator*, Math. Comput. Sci. **6**, (2012), 181–198.

[48] A. Kodess, *Properties of some algebraically defined digraphs*, Ph. D. Thesis, University of Delaware, 2014.

[49] A. Kodess and F. Lazebnik, *Connectivity of Some Algebraically Defined Digraphs*, The Electronic J. Combin. **22** (3), (2015), #P3.27, 1–11.

[50] A. Kodess, F. Lazebnik, S. Smith and J. Sporre, *Diameter of some monomial digraphs.* Contemporary Developments in Finite Fields and Applications, A. Canteaut, G. Effinger, S. Huczynska, D. Panario, L. Storme Eds., World Scientific, Singapur, 2016, 160–177.

[51] B.G. Kronenthal, *Monomial Graphs and Generalized Quadrangles*, Finite Fields and Their Applications **18**, (2012), 674–684.

[52] B.G. Kronenthal and F. Lazebnik, *On the uniqueness of some girth eight algebraically defined graphs*, Applied Discrete Mathematics **206**, (2016), 188-194.

[53] B.G. Kronenthal, F. Lazebnik and J. Williford *On the uniqueness of some girth eight algebraically defined graphs, II*, Unpublished manuscript, 2016.

[54] A. Kumar, A. Pradhan, A. Thangaraj and A. Subramanian, *Code Sequences with Block-Error Thresholds*, arXiv:1510.06828v1 [cs.IT] 23 Oct 2015.

[55] F. Lazebnik and D. Mubayi, *New lower bounds for Ramsey numbers of graphs and hypergraphs*, Advances in Applied Mathematics **28** (3/4), (2002), 544–559.

[56] F. Lazebnik and S. Sun, http://udel.edu/ shuying/girthDkq.pdf.

[57] F. Lazebnik and A. Thomason, *Orthomorphisms and the Construction of Projective Planes*, Mathematics of Computation **73** (247), (2004), 1547–1557.

[58] F. Lazebnik and V. A. Ustimenko, *New examples of graphs without small cycles and of large size*, Europ. J. Combin. **14**, (1993), 445–460.

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

[60] F. Lazebnik, V. A. Ustimenko, A. J. Woldar, *New constructions of bipartite graphs on* m, n *vertices with many edges and without small cycles*, J. Combin. Theory Ser. B **61** (1), (1994), 111–117.

[61] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *Properties of certain families of* $2k$*-cycle free graphs*, J. Combin. Theory Ser. B **60** (2), (1994), 293–298.

[62] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *A new series of dense graphs of high girth*, Bulletin of the AMS **32** (1), (1995), 73–79.
[63] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *A characterization of the components of the graphs $D(k, q)$*, Discrete Mathematics **157**, (1996), 271–283.
[64] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *New upper bounds on the order of cages*, Electronic J. Combin. **14** (13), (1997), 1–11.
[65] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *Polarities and 2k-cycle-free graphs*, Discrete Mathematics **197/198**, (1999), 503–513.
[66] F. Lazebnik and J. Verstraëte, *On hypergraphs of girth five*, Electronic J. Combin. **10** (25), (2003), 1–15.
[67] F. Lazebnik and R. Viglione, *An infinite series of regular edge- but not vertex-transitive graphs*, J. Graph Theory **41**, (2002), 249–258.
[68] F. Lazebnik and R. Viglione, *On the connectivity of certain graphs of high girth*, Discrete Mathematics **277**, (2004), 309–319.
[69] F. Lazebnik and P. Wang, *On the extremal graphs of high girth*, J. Graph Theory **26**, (1997), 147–153.
[70] F. Lazebnik and A. J. Woldar, *New lower bound on the multicolor Ramsey numbers $r_k(C_4)$*, J. Combin. Theory Ser. B **79**, (2000), 172–176.
[71] F. Lazebnik and A. J. Woldar, *General properties of some families of graphs defined by systems of equations*, J. Graph Theory **38**, (2001), 65–86.
[72] W. -C. W. Li, M. Lu and C. Wang, *Recent developments in low-density parity-check codes*, Coding and cryptology, 107-123, Lecture Notes in Comput. Sci., 5557, Springer, Berlin, 2009.
[73] A. Lubotzky, R. Phillips, and P. Sarnak, *Ramanujan graphs*, Combinatorica **8** (3), (1988), 261–277.
[74] G. A. Margulis, *Explicit group-theoretical construction of combinatorial schemes and their application to design of expandors and concentrators*, Journal of Problems of Information Transmission **24**, (1988), 39–46 (translation from Problemy Peredachi Informatsii **24** (1), January-March 1988, 51–60.)
[75] G. E. Moorhouse, S. Sun, J. Williford, *The Eigenvalues of the Graphs $D(4, q)$*, (2016), submitted for publication.
[76] I. Neuwirth, *The size of bipartite graphs with girth eight*, arXiv:math.CO/0102210, 2001.
[77] S.E. Payne, *Affine representations of generalized quadrangles*, J. Algebra **16**, (1970), 473–485.
[78] S. E. Payne, *A census of finite generalized quadrangles, in Finite geometries, buildings, and related topics*, Editors: W.M. Kantor, R.A. Liebler, S.E. Payne and E.E. Shult , Clarendon Press, Oxford, (1990), 29–36.
[79] O. Pikhurko, *A note on the Tur an function of even cycles*, Proc. Amer. Math. Soc. **140** (11), (2012), 3687-3692.
[80] S. P. Radziszowski, *Small Ramsey numbers*, Electronic J. Combin. **1** DS1, (2014), 1–94.
[81] S. Reichard, Private communication, 2001.
[82] H. Sachs, *Regular graphs with given girth and restricted circuits*, J. London Math. Society **38**, (1963), 423-429.
[83] A. Schliep, *GADAR and its application to extremal graph theory*, Master Thesis, University of Delaware,1994.
[84] J. -Y. Shao, C. -X. He and H. -Y. Shan, *The existence of even cycles with specific lengths in Wenger's graph*, Acta Math. Appl. Sin. Engl. **24**, (2008), 281–288.
[85] P. Sin and Q. Xiang, *On the dimension of certain LDPC codes based on q-regular bipartite graphs*, IEEE Trans. Inform. Theory **52**, (2006), 3735–3737.
[86] S. Sun, http://udel.edu/ shuying/diameterLB.pdf.
[87] J.A. Thas, *Generalized Polygons*, Handbook of Incidence Geometry, Edited by F. Buekenhout, Elsevier Science, 1995.
[88] T.A. Terlep and J. Williford, *Graphs from Generalized Kac-Moody Algebras*, Siam Journal on Discrete Math. **26** (3), (2012), 1112–1120.
[89] A. Thomason, Private communication, 1997.
[90] A. Thomason, Private communication, 2002.
[91] V.A. Ustimenko, *A linear interpretation of the flag geometries of Chevalley groups*, Kiev University, Ukrainskii Matematicheskii Zhurnal **42** (3), March (1990), 383–387; English translation.

[92] V.A. Ustimenko, *On the embeddings of some geometries and flag systems in Lie algebras and superalgebras*, in Root systems, representation and geometries, Kiev, IM AN UkrSSR, (1990), 3–16.
[93] V.A. Ustimenko, *On some properties of geometries of the Chevalley groups and their generalizations*, in Investigation in Algebraic Theory of Combinatorial Objects, (Ed. I. A. Faradzev, A. A. Ivanov, M. H. Klin, A. J. Woldar) Kluwer Acad. Publ., Dordresht, (1991), 112–121.
[94] V. A. Ustimenko, *Coordinatization of a regular tree and its quotients*, in: Voronoi's Impact to Modern Science, Book 2 (Ed. P. Engel and H. Syta (Nat. Acad. of Sci., Ukraine), Kiev Institute of Mathematics, Kiev, (1998), 228pp.
[95] V. A. Ustimenko, *On the flag geometry of simple group of Lie type and multivariate cryptography*, Algebra and Discrete Mathematics **19** (1), (2015), 130–144.
[96] V. A. Ustimenko and A. J. Woldar, *An improvement on the Erdős bound for graphs of girth 16*, Contemporary Math. Series of the Amer. Math. Soc. **184**, (1995), 419–425.
[97] V. A. Ustimenko and A. J. Woldar, *Extremal properties of regular and affine generalized polygons as tactical configurations*, Europ. J. Combin. **23**, (2003), 99-111.
[98] H. Van Maldeghem, Generalized polygons. Monographs in Mathematics **93**, Birkh user Verlag, Basel, 1998.
[99] J. Verstraëte, *On arithmetic progressions of cycle lengths in graphs*, Combin. Probab. Computing **9**, (2000), 369-373.
[100] R. Viglione, *Properties of some algebraically defined graphs*, Ph. D. Thesis, University of Delaware, 2002.
[101] R. Viglione, *On the diameter of Wenger graphs*, Acta Appl. Math. **104**, (2008), 173–176.
[102] Y. Wang, F. Lazebnik and A. Thomason, *On Some Cycles in Wenger Graphs*, To appear in Acta Math. Appl. Sin. Engl..
[103] R. Wenger, *Extremal graphs with no* $C^4, C^6,$ or C^{10}*'s*, J. Combin. Theory Ser. B **52**, (1991), 113-116
[104] J. Williford, Private communication, 2012.
[105] A. J. Woldar, *Rainbow graphs*, Procedings of OSU-Denison Conference: In honor of the 65th birthday of Dijen K. Ray-Chaudhuri, Codes and Designs, (K.T. Arasu and A. Seress, editors), deGruyter, Berlin, 2002.
[106] A.J. Woldar, *On generalizing generalized polygons*, Innovations Incidence Geom **10**, (2010), 147–170.
[107] A. Wróblewska and V. Ustimenko, *On new examples of families of multivariate stable maps and their cryptographical applications*, Annales UMCS Informatica AI XIV **1**, (2014), 19–36.

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

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