Some families of graphs, hypergraphs and digraphs defined by triangular systems of polynomial equations

Felix Lazebnik[a] Ye Wang[b]

Submitted: Apr 8, 2025; Accepted: Dec 14, 2025; Published: Feb 13, 2026

Dedicated to the memory of Pamela G. Irwin (1962 - 2023)

Abstract

The families of graphs defined by a certain type of system of equations over commutative rings have been studied and used since the 1990s. This survey presents these families and their applications related to graphs, digraphs, and hypergraphs. Some open problems and conjectures are mentioned.

Mathematics Subject Classifications: 05C35, 05C38, 05C75, 11T06, 11T55, 51E12, 51E15

[a]Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA (fellaz@udel.edu).
[b]Corresponding author. College of Mathematical Sciences, Harbin Engineering University, Harbin 150001, China (ywang@hrbeu.edu.cn).

Contents

1 Introduction

One goal of this survey is to summarize results concerning families of graphs, hypergraphs and digraphs defined by certain systems of equations. Another goal is to provide a comprehensive treatment of, probably, the best known family of such graphs, denoted by $D(k, q)$. The original results on these graphs were scattered among many papers, with the notation 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 to continue research in the area or find new applications.

For a summary of related results which appeared before 2001, see Lazebnik and Woldar [109]. One important feature of that article was an attempt of setting simpler notation and presenting results in greater generality. Let us begin with a quote from [109] (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 appearing in [173, 96, 98, 99, 60, 97, 100, 101, 102, 103], the authors 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 [109] was done in two directions: attempting to apply specializations of general constructions to new problems, and trying to strengthen some old results. This work was presented in a 2017 survey by Lazebnik, Sun and Wang [93]. Here we make use of both [109] and [93], often following them closely, and include results that were not covered in these papers. We also thought that it is better to make the survey dynamic, and update it regularly.

Before proceeding, we establish some notation; more will be introduced later. The missing graph-theoretic definitions can be found in Bollobás [15]. Most graphs we consider in this survey 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 prime $p \geqslant 2$ and integer $e \geqslant 1$, let $\mathbb{F}_q$ denote the field of q elements.

The survey is organized as follows. In Section 2, we go over the main constructions, 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 the graphs $D(k,q)$ and $CD(k,q)$, and survey new results. In Section 7, we mention some applications of the graphs $D(k,q)$ and $CD(k,q)$, and we conclude with a brief discussion on the related work in coding theory and cryptography in Section 8.

2 Main constructions

2.1 Bipartite version

Let $f_i : R^{2i-2} \to R$, $2 \leqslant i \leqslant n$, be arbitrary functions on R of 2, 4, …, $2n-2$ variables, respectively. We define the bipartite graph $B\Gamma_n = B\Gamma(R; f_2, \ldots, f_n)$, $n \geqslant 2$, 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 a point $(p) = (p_1, p_2, \ldots, p_n)$ and a line $[l] = [l_1, l_2, \ldots, l_n]$ adjacent if and only if the following $n-1$ relations on their coordinates hold:

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

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. *The 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 $\varphi : (a) \leftrightarrow [a]$.*

2.2 Ordinary version

We now define our second fundamental family of graphs for which we require that all functions are symmetric. Let $f_i : R^{2i-2} \to R$ be symmetric for all $2 \leqslant i \leqslant n$. 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:

$$\begin{aligned} a_2 + b_2 &= f_2(a_1, b_1), \\ a_3 + b_3 &= f_3(a_1, b_1, a_2, b_2), \\ \dots &\quad \dots \\ a_n + b_n &= f_n(a_1, b_1, a_2, b_2, \dots, a_{n-1}, b_{n-1}). \end{aligned} \tag{2}$$

For the graphs Γ_n, our requirement that all functions f_i are symmetric is necessary to ensure that adjacency is symmetric. Without this condition one obtains not graphs, but digraphs. It is sometimes beneficial to allow loops in Γ_n, which appear when $a_i = b_i$ for all i and satisfying (2).

2.3 Uniform k-partite hypergraphs

In this survey, 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 k-*partite* if its vertex set $V(\mathcal{H})$ can be colored in k 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 [10, 11] for additional background on hypergraphs.

In [92], Lazebnik and Mubayi generalized constructions of graphs $B\Gamma_n$ and Γ_n to hypergraphs. The following comment is from [92].

> 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.

Though the following definitions can be made over an arbitrary commutative ring R, different from the zero, and with multiplicative identity, we will restrict ourselves to the case where R is a finite field.

As before, let $\mathbb{F}_q$ be the field of q elements. For integers $d, i, r \geqslant 2$, let $f_i : \mathbb{F}_q^{(i-1)r} \to \mathbb{F}_q$ be a function. For $x^i = (x^i_1, \dots, x^i_d) \in \mathbb{F}_q^d$, let $(x^1, \dots, x^i)$ stand for $(x^1_1, \dots, x^1_d, x^2_1, \dots, x^2_d, \dots, x^i_1, \dots, x^i_d)$.

Suppose d, k, r are integers and $2 \leqslant r \leqslant k$, $d \geqslant 2$. First we define a k-partite r-graph $\mathcal{T} = \mathcal{T}(q, d, k, r, f_2, f_3, \dots, f_d)$. Let the vertex set $V(\mathcal{T})$ be a disjoint union of sets, or color classes, $V^1, \dots, V^k$, where each V^j is a copy of $\mathbb{F}_q^d$. By $a^j = (a^j_1, a^j_2, \dots, a^j_d)$ we denote an arbitrary vertex from V^j. The edge set $E(\mathcal{T})$ is defined as follows: for every r-subset $\{i_1, \dots, i_r\}$ of $\{1, \dots, k\}$ (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 $d-1$ equalities hold:

$$\begin{aligned}
\sum_{j=1}^{r} a_2^{i_j} &= f_2(a_1^{i_1}, \ldots, a_1^{i_r}), \\
\sum_{j=1}^{r} a_3^{i_j} &= f_3(a_1^{i_1}, \ldots, a_1^{i_r}, a_2^{i_1}, \ldots, a_2^{i_r}), \\
\ldots \quad \ldots & \quad \ldots \quad \ldots \quad \ldots \\
\sum_{j=1}^{r} a_d^{i_j} &= f_d(a_1^{i_1}, \ldots, a_1^{i_r}, a_2^{i_1}, \ldots, a_2^{i_r}, \ldots, a_{d-1}^{i_1}, \ldots, a_{d-1}^{i_r}).
\end{aligned} \tag{3}$$

The system (3) 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 (3). 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. Note that $\mathcal{K}$ can be also viewed as a q^d-partite r-graph, each partition having one vertex only. If $d = r$, then $\{i_1, \ldots, i_r\} = \{1, \ldots, d\}$.

3 General properties of graphs $B\Gamma_n$, Γ_n and hypergraphs $\mathcal{T}$, $\mathcal{K}$

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 [109] or references therein, and we omit them, with the exception of Theorem 2 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 the graphs $B\Gamma_n$ and Γ_n defined in Section 2 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 2. *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 (1) is triangular, and each b_i is uniquely determined from the values of $a_1, \ldots, a_i, b_1, \ldots b_{i-1}$, $2 \leqslant i \leqslant n$.

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 $\langle a_1, a_2, \ldots, a_n\rangle$, where

$$a_i = \frac{1}{2} f_i(a_1, a_1, \ldots, a_{i-1}, a_{i-1}), \quad 2 \leqslant i \leqslant n.$$

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. □

The proof above justifies the term "triangular" in the title of this survey as, for a fixed (a), system (1) is a triangular system of linear equations with respect to b_i.

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 [157] under the name of "parallelotopic" and further explored by Woldar [175] under the name of "rainbow", and in [109] under the name of "neighbor-complete colorings", which we adopt here. In [157], some group theoretic constructions of graphs possessing neighbor-complete colorings are given; in [175], purely combinatorial aspects of such colorings are considered. Non-trivial examples of graphs possessing neighbor-complete colorings are not easy to construct. Remarkably, $B\Gamma_n$ and Γ_n always admit them.

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

3.2 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

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

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 $B\Gamma_n$, $B\Gamma_n[A, B]$ can alternately be described as the bipartite graph with bipartition $P_{n,A} \cup L_{n,B}$ and adjacency relation as given in (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 the 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) directly to $V_{n,A}$. (Note that when $A = R$ one has $B\Gamma_n[R] = B\Gamma_n$ and $\Gamma_n[R] = \Gamma_n$.)

3.3 Covers and lifts

The notion of a covering for graphs is analogous to the one in topology. We call $\overline{\Gamma}$ a *cover* of 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, i.e.,

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

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.,

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

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

In what follows, the functions f_i $(2 \leqslant i \leqslant n)$ 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 [109].

Theorem 3. *For every $A \subseteq R$ and every k, n, $2 \leqslant k < n$,*

$$B\Gamma_n[A] \to B\Gamma_k[A].$$

No edge of $\Gamma_n[A]$ projects to a loop of $\Gamma_k[A]$ if and only if

$$\Gamma_n[A] \to \Gamma_k[A].$$

Remark 4. If a graph Γ contains cycles, its girth, denoted by $girth(\Gamma)$, is the length of its shortest cycle. An important consequence of Theorem 3, 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, for $2 \leqslant k \leqslant n$,

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

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

A relation of $B\Gamma_n$ to voltage lifts will be discussed in Section 6.7.

3.4 Embedded spectra

The spectrum $spec(\Gamma)$ of a graph Γ is defined to be the multiset of eigenvalues of its adjacency matrix. An important property of covers discussed in Section 3.3 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, Doob and Sachs [38]. As an immediate consequence of this fact and Theorem 3, we obtain the following result.

Theorem 5. *Assume R is finite and let $A \subseteq R$. Then for each k, n, $2 \leqslant k < n$,*

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

For the 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 $\Gamma_k[A]$.

3.5 Edge-decomposition of K_n and $K_{m,n}$

The results of this subsection were motivated by a question from Thomason [153], who asked whether $D(k, q)$ (which will be defined later in this survey) edge-decomposes K_{q^k,q^k}.

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 $E(\Gamma)$.

In this case, we also say 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 [109] is a bit surprising.

Theorem 6. ([109]) *Let $|R| = r$. Then*

1. *$B\Gamma_n$ decomposes K_{r^n,r^n}.*
2. *Γ_n (without loops) decomposes K_{r^n} if 2 is a unit in R.*

3.6 Edge-decomposition of complete k-partite r-graphs and complete r-graphs

We begin by presenting several parameters of hypergraphs

$$\mathcal{T} = \mathcal{T}(q, d, k, r, f_2, \ldots, f_d) \text{ and } \mathcal{K} = \mathcal{K}(q, d, r, f_2, \ldots, f_d).$$

The proof of the following theorem is similar to that for $B\Gamma_n$ and Γ_n.

Theorem 7. ([92]) *Let q, d, r, k be integers, $2 \leqslant r \leqslant k$, $d \geqslant 2$, 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 Γ_n could be easily counted. Removing them leads to a bi-regular graph, with some vertices having degree q and others having degree $q - 1$. In general, this is not true for $r \geqslant 3$. 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 8. ([92]) *Let p, d, r be integers, $2 \leqslant r < p$, $d \geqslant 2$, 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 $E(\mathcal{H})$. In this case, we also say that $\mathcal{H}'$ *decomposes* $\mathcal{H}$, and we refer to the hypergraphs from $\mathcal{P}$ as *copies* of $\mathcal{H}'$.

Let $T^{(r)}_{kq^d}$, $2 \leqslant r \leqslant k$, $d \geqslant 1$, 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 $f_2, \ldots, f_r$. The proof of the following theorem is similar to that for 2-graphs from [109].

Theorem 9. ([92]) *Let q, d, r, k be integers, $2 \leqslant r \leqslant k$, $d \geqslant 2$, and q be a prime power. Then*

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

4 Specializations of general constructions and their 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 that the resulting graphs have additional desired properties. In particular, many applications deal with the existence of graphs (hypergraphs) of a fixed order, having many edges and not containing certain subgraphs (subhypergraphs). Our next section provides related terminology and basic references.

4.1 Generalized polygons

A *generalized k-gon* of order (q, q), for $k \geqslant 3$ and $q \geqslant 2$, 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 [164], Thas [151] or Brouwer, Cohen and Neumaier [17]). It follows from a theorem by Feit and Higman [56] that if Π_q^k exists, then $k \in \{3, 4, 6\}$. For each of these k, Π_q^k is known to exist only for arbitrary prime powers q. For $k = 3$, 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 the graph Π_q^k, one can consider a subgraph in Π_q^k induced by all vertices at distance at least $k-1$ from the edge. It is easy to argue that the resulting graph is q-regular, has girth $2k$ (for $q \geqslant 4$) and diameter $2(k-1)$ (for $q \geqslant 4$). 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. Deleting all vertices 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 $B\Gamma_n$:

$$\begin{aligned}
&\Lambda_q^3 \text{ as } B\Gamma_2(\mathbb{F}_q; p_1 l_1),\\
&\Lambda_q^4 \text{ as } B\Gamma_3(\mathbb{F}_q; p_1 l_1, p_1 l_2) \cong B\Gamma_3(\mathbb{F}_q; p_1 l_1, p_1 l_1^2),\\
&\Lambda_q^6 \text{ as } B\Gamma_5(\mathbb{F}_q; p_1 l_1, p_2 l_1, p_3 l_1, p_2 l_3 - p_3 l_2).
\end{aligned}$$

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 [174].

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 [129], [164] and references therein.

Another approach, independent of the previous, is based on the work of Ustimenko, see [154, 155, 156], where incidence structures in group geometries, which were initially used 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 Lazebnik and Ustimenko [96], in Ustimenko and Woldar [163], in Woldar [176], in Terlep and Williford [150] and in more recent work by Yang, Sun and Zhang [183].

The descriptions of the biaffine parts Λ_q^k of the classical k-gons Π_q^k via the 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 nondecreasing girth of the graphs $B\Gamma_n$ that we mentioned in Remark 4 of Section 3.3 turned out to be fundamental for constructing families of graphs with many edges and without cycles of certain lengths, and in particular, of large girth. We describe these applications in Section 4.3.

The graphs $B\Gamma_n$ can also be used to attempt to construct new generalized k-gons ($k \in \{3,4,6\}$) via the following logic: first construct a graph $B\Gamma_{k-1}$ 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, preferably not isomorphic to one coming from Π_q^k, and then, if possible, extend it to a generalized k-gon. For $k=3$, the extension will always work. Of course, this approach has an inherited restriction on the obtained k-gon, as the automorphism group of any graph $B\Gamma_{k-1}$ contains a subgroup isomorphic to the additive group of the field $\mathbb{F}_q$ (or a ring R). This subgroup is formed by the following q maps ϕ_a, $a \in \mathbb{F}_q$:

$$\phi_a : (p_1, p_2, \ldots, p_{k-1}) \mapsto (p_1, p_2, \ldots, p_{k-1} + a), \tag{4}$$

$$[l_1, l_2, \ldots, l_{k-1}] \mapsto [l_1, l_2, \ldots, l_{k-1} - a]. \tag{5}$$

Lazebnik and Thomason used this approach in [95] 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. Some attempts to construct new generalized quadrangles are discussed in Section 4.9.

4.2 Turán-type extremal problems

For more on this subject, see the book by Bollobás [14] and the survey by Füredi and Simonovits [62].

Let $\mathcal{F}$ be a family of graphs. By $ex(\nu, \mathcal{F})$ we denote the largest number of edges in a graph on ν vertices which contains no subgraph isomorphic to a graph from $\mathcal{F}$, and $ex(\nu, \mathcal{F})$ is referred to as the *Turán number* of $\mathcal{F}$. Determining the Turán number $ex(\nu, \mathcal{F})$ for a fixed $\mathcal{F}$, is called a *Turán-type extremal graph problem.* Graphs from $\mathcal{F}$ are called *forbidden* graphs, and if a graph G does not contain any graph from $\mathcal{F}$ as a subgraph, we say that G is *$\mathcal{F}$-free.*

If $\mathcal{F}$ contains no bipartite graphs, the leading term in the asymptotic of $ex(\nu, \mathcal{F})$ is given by the celebrated Erdős–Stone–Simonovits Theorem, see [14]. When $\mathcal{F}$ contains a bipartite graph, then determining $ex(\nu, \mathcal{F})$ is called the *degenerate Turán-type extremal graph problem*, and often only the bounds of $ex(\nu, \mathcal{F})$ are known in this case.

Replacing "graph" by "hypergraph" in the above definitions, we obtain the corresponding ones for hypergraphs.

Let C_n denote the cycle of length n, where $n \geqslant 3$. If n is even, we refer to C_n as an *even* cycle. Note that C_{2k} is bipartite, and many of the applications mentioned later in this survey will be related to forbidden even cycles.

We will also use the following standard notation for the comparison of functions. Let f and g be two real positive functions defined on positive integers. We write

$f = o(g)$ if $f(n)/g(n) \to 0$ as $n \to \infty$;

$f = O(g)$ if there exists a positive constant c such that $f(n) \leqslant cg(n)$ for all sufficiently large n;

$f = \Theta(g)$ if $f = O(g)$ and $g = O(f)$;

$f = \Omega(g)$ if $g = O(f)$;

$f \sim g$ if $f(n)/g(n) \to 1$ as $n \to \infty$.

4.3 Graphs without cycles of certain length and with many edges

For more on this subject, see [14, 62]. Our goal here is to mention some results, not mentioned in [62], and related constructions obtained by the algebraically defined graphs.

The best bounds on $ex(\nu, \{C_3, C_4, \cdots, C_{2k}\})$ for fixed k, $2 \leqslant k \neq 5$, are presented as follows. Let $\epsilon = 0$ if k is odd, and $\epsilon = 1$ if k is even. Then

$$\frac{1}{2^{1+1/k}}\nu^{1+\frac{2}{3k-3+\epsilon}} \leqslant ex(\nu, \{C_3, C_4, \cdots, C_{2k}\}) \leqslant \frac{1}{2}\,\nu^{1+\frac{1}{k}} + \frac{1}{2}\,\nu, \tag{6}$$

and

$$\frac{1}{2^{1+1/k}}\nu^{1+\frac{2}{3k-3+\epsilon}} \leqslant ex(\nu, \{C_3, C_4, \cdots, C_{2k}, C_{2k+1}\}) \leqslant \frac{1}{2^{1+1/k}}\,\nu^{1+\frac{1}{k}} + \frac{1}{2}\,\nu. \tag{7}$$

The upper bounds in both (6) and (7) are immediate corollaries of the result by Alon, Hoory and Linial [4]. The lower bound holds for an infinite sequence of values of ν. It was established by Lazebnik, Ustimenko and Woldar in [100] 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 [127], Hoory [71] and Abajo and Diánez [1].

Theorem 10. *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 $\mathcal{F} = \{C_{2k}\}$. Erdős Even Circuit Theorem (see Erdős [49]) asserts that

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

and the upper bound is probably sharp, but, as far as we know, Erdős never published a proof of it. The first proof followed from a stronger result by Bondy and Simonovits [16], which implied that

$$ex(\nu, \{C_{2k}\}) \leqslant 100kv^{1+1/k}.$$

The upper bound was improved by Verstraëte [165] to $8(k-1)\nu^{1+1/k}$, by Pikhurko [132] to $(k-1)\nu^{1+1/k} + O(\nu)$ and by Bukh and Jiang [18] 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 [57, 58] by Füredi (for $k = 2$), in [61] by Füredi, Naor and Verstraëte (for $k = 3$), and in [103] by Lazebnik, Ustimenko and Woldar (for $k = 5$).

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 the $2k$-cycle-free graphs.

Problem 11. 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?

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

4.4 Wenger graphs

A large part of this subsection is based on Cioabă, Lazebnik and Li [34].

4.4.1 Defining equations for Wenger graphs

Let $q = p^e$, where p is a prime and $e \geqslant 1$ is an integer. For $m \geqslant 1$, $1 \leqslant k \leqslant m$, let $f_{k+1} = l_k p_1$. Consider the graph $W_m(q) = B\Gamma_{m+1}(\mathbb{F}_q; f_2, f_3, \ldots, f_{m+1})$:

$$\begin{aligned} l_2 + p_2 &= l_1 p_1, \\ l_3 + p_3 &= l_2 p_1, \\ &\vdots \\ l_{m+1} + p_{m+1} &= l_m p_1. \end{aligned}$$

The graph $W_m(q)$ has $2q^{m+1}$ vertices, is q-regular and has q^{m+2} edges.

In [173], Wenger introduced a family of p-regular bipartite graphs $H_k(p)$ as follows. For every $k \geqslant 2$ and every prime p, the partite sets of $H_k(p)$ are two copies of integer sequences $\{0, 1, \ldots, p-1\}^k$, with vertices $a = (a_0, a_1, \ldots, a_{k-1})$ and $b = (b_0, b_1, \ldots, b_{k-1})$ forming an edge if

$$b_j \equiv a_j + a_{j+1} b_{k-1} \pmod{p} \text{ for all } j = 0, \ldots, k-2.$$

The introduction and study of these graphs were motivated by the degenerate Turán-type extremal graph theory problem of determining $\mathrm{ex}(\nu, \{C_{2k}\})$. It is shown in [16] that $\mathrm{ex}(\nu, \{C_{2k}\}) = O(\nu^{1+1/k})$, $\nu \to \infty$. Lower bounds of magnitude $\nu^{1+1/k}$ were known (and still are) for $k = 2, 3, 5$ only, and the graphs $H_k(p)$, $k = 2, 3, 5$, provided new and simpler examples of such magnitude extremal graphs.

In [96], using a construction based on a certain Lie algebra, the authors arrived at a family of bipartite graphs $H'_n(q)$ for $n \geqslant 3$ and prime power q, whose partite sets were two copies of $\mathbb{F}_q^{n-1}$, with vertices $(p) = (p_2, p_3, \ldots, p_n)$ and $[l] = [l_1, l_3, \ldots, l_n]$ forming an edge if

$$l_k - p_k = l_1 p_{k-1} \ \text{ for all } \ k = 3, \ldots, n.$$

It is easy to see that for all $k \geqslant 2$ and prime p, the graphs $H_k(p)$ and $H'_{k+1}(p)$ are isomorphic, and the map

$$\begin{aligned} \phi : (a_0, a_1, \ldots, a_{k-1}) &\mapsto (a_{k-1}, a_{k-2}, \ldots, a_0), \\ (b_0, b_1, \ldots, b_{k-1}) &\mapsto [b_{k-1}, b_{k-2}, \ldots, b_0], \end{aligned}$$

provides an isomorphism from $H_k(p)$ to $H'_{k+1}(p)$. Hence, $H'_n(q)$ can be viewed as generalizations of $H_k(p)$. It is also easy to show that the graphs $H'_{m+2}(q)$ and $W_m(q)$ are isomorphic: the function

$$\begin{aligned} \psi : (p_2, p_3, \ldots, p_{m+2}) &\mapsto [p_2, p_3, \ldots, p_{m+2}], \\ [l_1, l_3, \ldots, l_{m+2}] &\mapsto (-l_1, -l_3, \ldots, -l_{m+1}), \end{aligned}$$

mapping points to lines and lines to points, is an isomorphism from $H'_{m+2}(q)$ to $W_m(q)$.

We call the graphs $W_m(q)$ *Wenger graphs*. Another useful presentation of Wenger graphs appeared in Lazebnik and Viglione [105]. In this presentation, the functions on the right-hand sides of the equations are represented as monomials of p_1 and l_1 only, see Viglione [167]. For this, define a bipartite graph $W'_m(q)$ with the same partite sets as $W_m(q)$, where $(p) = (p_1, p_2, \ldots, p_{m+1})$ and $[l] = [l_1, l_2, \ldots, l_{m+1}]$ are adjacent if

$$l_k + p_k = l_1 p_1^{k-1} \ \text{ for all } \ k = 2, \ldots, m+1. \tag{8}$$

The map

$$\begin{aligned} \omega : (p) &\mapsto (p_1, p_2, p'_3, \ldots, p'_{m+1}), \ \text{where } p'_k = p_k + \sum_{i=2}^{k-1} p_i p_1^{k-i}, \ k = 3, \ldots, m+1, \\ [l] &\mapsto [l_1, l_2, \ldots, l_{m+1}], \end{aligned}$$

defines an isomorphism from $W_m(q)$ to $W'_m(q)$.

4.4.2 Automorphisms of Wenger graphs

It was shown in [96] that the automorphism group of $W_m(q)$ acts transitively on each of the partitions, and on the set of edges of $W_m(q)$. In other words, the graphs $W_m(q)$

are point-, line-, and edge-transitive. A more detailed study, see Lazebnik and Viglione [106], also showed that $W_1(q)$ is vertex-transitive for all q, and $W_2(q)$ is vertex-transitive for even q. For all $m \geqslant 3$ and $q \geqslant 3$, and for $m = 2$ and all odd q, the graphs $W_m(q)$ are not vertex-transitive.

The full automorphism group of $W_1(q)$ and $W_2(q)$ were completely described in [167]. Some sets of automorphisms of $W_m(q)$ can be found in [96]. A more general result, for all graphs $W_m(q)$, is contained in a paper [24] by Cara, Rottey and Van de Voorde. They showed that the full automorphism group of $W_m(q)$ is isomorphic to a subgroup of the group $P\Gamma L(m+2, q)$ that stabilizes a q-arc contained in a normal rational curve of $PG(m+1, q)$, provided $q \geqslant m+3$ or prime $q = m+2$, $m \geqslant 2$.

4.4.3 Connectivity of Wenger graphs

Another result of [106] is that $W_m(q)$ is connected when $1 \leqslant m \leqslant q-1$, and disconnected when $m \geqslant q$, in which case it has q^{m-q+1} components, each isomorphic to $W_{q-1}(q)$. The statement about the number of components of $W_m(q)$ becomes apparent from the representation (8). Indeed, as $l_1 p_1^i = l_1 p_1^{i+q-1}$, all points and lines in a component have the property that their coordinates i and j, where $i \equiv j \mod (q-1)$, are equal. Hence, points (p), having $p_1 = \ldots = p_q = 0$, and at least one distinct coordinate p_i, $q+1 \leqslant i \leqslant m+1$, belong to different components. This shows that the number of components is at least q^{m-q+1}. As $W_{q-1}(q)$ is connected and $W_m(q)$ is edge-transitive, all components are isomorphic to $W_{q-1}(q)$. Hence, there are exactly q^{m-q+1} of them.

It was pointed out in [34] that a result of Watkins [172] and the edge-transitivity of $W_m(q)$ imply that the vertex connectivity (and consequently the edge connectivity) of $W_m(q)$ equals the degree of regularity q, for any $1 \leqslant m \leqslant q-1$. In [168], Viglione proved that when $1 \leqslant m \leqslant q-1$, the diameter of $W_m(q)$ is $2m+2$. It will follow from Theorem 13 (see ahead) that for every fixed m and sufficiently large q, $W_m(q)$ are expanders, which are defined below.

Let $G = (V, E)$ be a finite graph. For a subset of vertices $S \subseteq V$, let ∂S denote the set of edges with one endpoint in S and the other endpoint in $V \setminus S$, i.e.,

$$\partial S := \{xy \in E : x \in S, y \in V \setminus S\}.$$

The Cheeger constant (also known as the isoperimetric number or expansion ratio) of G is defined by

$$\min\left\{\frac{|\partial S|}{|S|} : S \subseteq V, 0 < |S| \leqslant \frac{1}{2}|V|\right\}.$$

An infinite family of *expanders* is a family of regular graphs whose Cheeger constants are uniformly bounded away from 0.

Let G be a connected d-regular graph with n vertices, and let $\lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_n$ be the eigenvalues of the adjacency matrix of G. Suppose λ_2 is the second largest eigenvalue in absolute value. Then we call G a *Ramanujan* graph if $\lambda_2 \leqslant 2\sqrt{d-1}$.

4.4.4 Cycles in Wenger graphs

Let $q = p^e$ for prime p and integer $e \geqslant 1$, and $m \geqslant 2$. It is easy to check that all graphs $W_m(q)$ contain an 8-cycle. Shao, He and Shan [143] proved that in $W_m(q)$, for any integer $l \neq 5, 4 \leqslant l \leqslant 2p$ and any vertex v, there is a cycle of length $2l$ passing through the vertex v. We wish to remark that the edge-transitivity of $W_m(q)$ implies the existence of a $2l$-cycle through any edge, a stronger statement. The results of [143] concerning cycle lengths in $W_m(q)$ were extended by Wang, Lazebnik and Thomason in [171] as follows.

1. For $m \geqslant 2$ and $p \geqslant 3$, $W_m(q)$ contains cycles of length $2l$, where $4 \leqslant l \leqslant 4p+1$ and $l \neq 5$.

2. For $q \geqslant 5$, $0 < c < 1$ and every integer l with $3 \leqslant l \leqslant q^c$, if $1 \leqslant m \leqslant (1 - c - \frac{7}{3}\log_q 2)l - 1$, $W_m(q)$ contains a $2l$-cycle. In particular, $W_m(q)$ contains cycles of length $2l$, where $m + 2 \leqslant l \leqslant q^c$, provided q is sufficiently large.

Alexander, Lazebnik and Thomason, see [2], showed that for fixed m and large q, Wenger graphs are hamiltonian.

Conjecture 12. ([171]) For every $m \geqslant 2$ and every prime power q with $q \geqslant 3$, $W_m(q)$ contains cycles of length $2k$, where $4 \leqslant k \leqslant q^{m+1}$ and $k \neq 5$.

Representation (8) points to a relation of Wenger graphs with the moment curve $t \mapsto (1, t, t^2, t^3, \ldots, t^m)$, and hence with the Vandermonde's determinant, which was explicitly used in [173]. This is also in the background of some geometric constructions by Mellinger and Mubayi [121] of magnitude extremal graphs without short even cycles, and in the previously mentioned article [24].

4.4.5 Spectrum of Wenger graphs

Futorny and Ustimenko [63] considered applications of Wenger graphs in cryptography and coding theory, as well as some generalizations. They also conjectured that the second largest eigenvalue λ_2 of the adjacency matrix of Wenger graphs $W_m(q)$ is bounded from above by $2\sqrt{q}$. The results of this paper confirm the conjecture for $m = 1$ and 2, or $m = 3$ and $q \geqslant 4$, and refute it in other cases. We wish to point out that for $m = 1$ and 2, or $m = 3$ and $q \geqslant 4$, the upper bound $2\sqrt{q}$ also follows from the known values of λ_2 for the point-line $(q+1)$-regular incidence graphs of the generalized polygons $PG(2, q)$, $Q(4, q)$ and $H(q)$ and eigenvalue interlacing, see [17]. In [111], Li, Lu and Wang showed that the graphs $W_m(q)$, $m = 1, 2$, are Ramanujan, by computing the eigenvalues of another family of graphs described by systems of equations in [97], namely $D(k, q)$, for $k = 2, 3$. Their result follows from the fact that $W_1(q) \cong D(2, q)$, and $W_2(q) \cong D(3, q)$.

Extending the cases of $m = 2, 3$ from [111], the spectra of Wenger graphs were completely determined in [34].

Theorem 13. ([34]) *For all prime powers q and $1 \leqslant m \leqslant q-1$, the distinct eigenvalues of $W_m(q)$ are*

$$\pm q,\ \pm\sqrt{mq},\ \pm\sqrt{(m-1)q},\ \cdots,\ \pm\sqrt{2q},\ \pm\sqrt{q},\ 0.$$

The multiplicity of the eigenvalue $\pm\sqrt{iq}$ of $W_m(q)$, $0 \leqslant i \leqslant m$, is

$$(q-1)\binom{q}{i}\sum_{d=i}^{m}\sum_{k=0}^{d-i}(-1)^k\binom{q-i}{k}q^{d-i-k}.$$

The idea of the proof of this theorem in [34] is the following. Let L and P denote the set of lines and points of the bipartite graph $W_m(q)$, respectively. Let H denote the distance-two graph of $W_m(q)$ on L. This means that the vertex set of H is L, and two distinct lines $[l]$ and $[l']$ of $W_m(q)$ are adjacent in H if there exists a point $(p) \in P$, such that $[l] \sim (p) \sim [l']$ in $W_m(q)$. It is easy to see that the eigenvalues of $W_m(q)$ can be expressed through those of H as $\pm\sqrt{\lambda+q}$, $\lambda \in spec(H)$. It turns out that H is actually the Cayley graph of the additive group of the vector space $\mathbb{F}^{m+1}$ with a generating set $S = \{(t, tu, \ldots, tu^m) | t \in \mathbb{F}_q^*, u \in \mathbb{F}_q\}$. It allowed computation of the eigenvalues of H using the techniques of Lovász [114] and Babai [5], and, hence, of $W_m(q)$.

As we already mentioned, this theorem implies that the graphs $W_m(q)$ are expanders for every fixed m and large q.

4.5 Some Wenger-like graphs

Extended from Wenger graphs, there are some Wenger-like graphs. In [133], Porter introduced some Wenger-like graphs and studied their properties.

4.5.1 Generalized Wenger graphs

Cao, Lu, Wan, L.-P. Wang and Q. Wang [23] considered the *generalized Wenger graphs* $G_m(q) = B\Gamma(\mathbb{F}_q; f_2, \ldots, f_{m+1})$, with $f_k = g_k(p_1)l_1$, $2 \leqslant k \leqslant m+1$, where $g_k \in \mathbb{F}_q[X]$ and the mapping $\mathbb{F}_q \to \mathbb{F}_q^{m+1}$, $u \mapsto (1, g_2(u), \ldots, g_{m+1}(u))$ is injective. A more general result in [109] implies that the generalized Wenger graph $G_m(q)$ is q-regular. The authors of [23] determined the spectrum of the generalized Wenger graphs.

Theorem 14. ([23]) *For all prime powers q and positive integer m, the eigenvalues of the generalized Wenger graph $G_m(q)$ counted with multiplicities, are*

$$\pm\sqrt{qN_{F_\omega}},\ \omega = (\omega_1, \omega_2, \ldots, \omega_{m+1}) \in \mathbb{F}_q^{m+1},$$

where $F_\omega(u) = \omega_1 + \omega_2 g_2(u) + \ldots + \omega_{m+1} g_{m+1}(u)$ and $N_{F_\omega} = |\{u \in \mathbb{F}_q : F_\omega(u) = 0\}|$. For $0 \leqslant i \leqslant q$, the multiplicity of $\pm\sqrt{qi}$ is

$$n_i = |\{\omega \in \mathbb{F}_q^{m+1} : N_{F_\omega} = i\}|.$$

Moreover, the number of components of $G_m(q)$ is

$$q^{m+1-rank_{\mathbb{F}_q}(1, g_2, \ldots, g_{m+1})}.$$

Therefore $G_m(q)$ is connected if and only if $1, g_2, \ldots, g_{m+1}$ are $\mathbb{F}_q$-linearly independent.

The idea of the proof is similar to the one in [34] with the distance-two graph H of $G_m(q)$ on L being the Cayley graph of the additive group of the vector space $\mathbb{F}^{m+1}$ with a generating set $S = \{(t, tg_2(u), \ldots, tg_{m+1}(u)) | t \in \mathbb{F}_q^*, u \in \mathbb{F}_q\}$.

4.5.2 Linearized Wenger graphs

An important particular case of the generalized Wenger graphs is obtained when $g_k(X) = X^{p^{k-2}}$, $2 \leqslant k \leqslant m+1$. The authors of [23] called these graphs the *linearized Wenger graphs* $L_m(q)$, and they determined the girth, diameter and spectrum. If $m > e$, the linearized Wenger graph is not connected. It has q^{m-e} connected components, each of which is isomorphic to the graph with $m = e$.

Theorem 15. ([23]) *If $m \leqslant e$, the diameter of the linearized Wenger graph $L_m(q)$ is $2(m+1)$.*

The outline of the proof is as follows. Consider the distance between any two lines L and L' in $L_m(q)$. If there is a path of length $2(m+1)$ with endpoints L and L', then the coordinates of vertices on the path must satisfy a system of linear equations. By the fact that if the coefficient matrix of the linear equations is nonsingular, then the system of linear equations has a unique solution, there are solutions for the coordinates of vertices on the path. Thus the diameter of any two vertices in the same partite set is at most $2(m+1)$. Modifying the construction so that the path goes through the point P, similarly, the distance between P and L is no more than $2(m+1)$, so that the diameter of $L_m(q)$ is at most $2(m+1)$. On the other hand, the distance $2(m+1)$ can be attained. Choose two lines L and L' such that $L' - L = [0, \ldots, 0, 1]$, if the distance between them is $2s$ with $s \leqslant m$. Then the system of linear equations has no solution. So the distance between them is at least $2(m+1)$.

Theorem 16. ([23]) *Let $q = p^e$. If $m \geqslant 1, e \geqslant 1$ and p is an odd prime, or $m = 1, e \geqslant 2$ and $p = 2$, then the girth of the linearized Wenger graph $L_m(q)$ is 6; if $p = 2$ and either $e = m = 1$ or $e \geqslant 1, m \geqslant 2$, then the girth of the linearized Wenger graph $L_m(q)$ is 8.*

For all $q \geqslant 2$, $L_1(q)$ is isomorphic to $W_1(q)$, which is 4-cycle-free. Hence, $L_m(q)$ has girth at least 6 for $m \geqslant 1$. The authors also determined the coordinates of points and lines of a shortest cycle in $L_m(q)$ in the proof of Theorem 16.

The spectrum of the linearized Wenger graphs is computed in [23] for $m \geqslant e$, and by Yan and Liu [182] for $m < e$. The proofs of the following two theorems rely on the spectrum of the generalized Wenger graphs as shown in Theorem 14.

Theorem 17. ([23]) *Let $m \geqslant e$. The linearized Wenger graph $L_m(q)$ has q^{m-e} components. The distinct eigenvalues are*

$$0, \ \pm\sqrt{qp^i}, \ 0 \leqslant i \leqslant e.$$

The multiplicities of the eigenvalues $\pm\sqrt{qp^i}$ are $q^{m-e}p^{e-i}\frac{\prod_{j=0}^{e-i-1}(p^e-p^j)^2}{\prod_{j=0}^{e-i-1}(p^{e-i}-p^j)}$. The multiplicity of the eigenvalue 0 is $q^{m-e}\sum_{i=1}^{e}(p^e-p^{e-i})\frac{\prod_{j=0}^{e-i-1}(p^e-p^j)^2}{\prod_{j=0}^{e-i-1}(p^{e-i}-p^j)}$.

For the following theorem, the Gaussian binomial coefficients are required:

$$\binom{n}{k}_p = \begin{cases} \prod_{t=0}^{k-1} \frac{p^n - p^t}{p^k - p^t}, & \text{if } 1 \leqslant k \leqslant n, \\ 1, & \text{if } k = 0, \\ 0, & \text{if } k > n, \end{cases}$$

where n and k are nonnegative integers.

Theorem 18. ([182]) *Let $m < e$. The eigenvalues of the linearized Wenger graph $L_m(q)$ are*

$$0, \ \pm q, \ \pm\sqrt{qp^i}, \ 0 \leqslant i \leqslant m-1.$$

The multiplicities of the eigenvalues $\pm q$ are 1, the multiplicities of the eigenvalues $\pm\sqrt{qp^i}$ are $p^{e-i}n_i$, and the multiplicity of the eigenvalue 0 *is* $2(q^{m+1} - 1 - \sum_{i=0}^{m-1} p^{e-i} n_i)$*, where*

$$n_i = \binom{e}{i}_p \sum_{j=0}^{m-i-1} (-1)^j p^{\frac{j(j-1)}{2}} \binom{e-i}{j}_p (q^{m-i-j} - 1),$$

where $\binom{e}{i}_p$ and $\binom{e-i}{j}_p$ are the Gaussian binomial coefficients.

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, $L_e(p^e)$ are hamiltonian. The lengths of some cycles in $L_m(q)$ were found in [170] by Wang using a similar method as in [171] and the adjacency of some points and lines in cycles.

Theorem 19. ([170]) *Let q be a power of the prime p with $p \geqslant 3$. For any integer k with $3 \leqslant k \leqslant p^2$, the linearized Wenger graph $L_m(q)$ contains cycles of length $2k$.*

Problem 20. Determine the lengths of all cycles in the linearized Wenger graph $L_m(q)$.

4.5.3 Jumped Wenger graphs

Another particular case of the generalized Wenger graphs is obtained when $(g_2(X), \ldots, g_{m+1}(X)) = (X, X^2, \ldots, X^{i-1}, X^{i+1}, \ldots, X^{j-1}, X^{j+1}, \ldots, X^{m+2})$. L.-P. Wang, Wan, W. Wang and Zhou of [169] called these graphs the *jumped Wenger graphs* $J_m(q, i, j)$, where $1 \leqslant i < j \leqslant m+1$. It is easy to obtain that $J_m(q, i, j)$ is q-regular, and if $m+2 < q$, $J_m(q, i, j)$ is connected. The authors also determined their girth and diameter.

Theorem 21. ([169]) *If $1 \leqslant m < q - 2$, the diameter of the jumped Wenger graph $J_m(q, i, j)$ is at most $2(m+1)$. In particular, the diameters of $J_m(q, m, m+2)$, $J_m(q, m+1, m+2)$ and $J_m(q, m, m+1)$ are all $2(m+1)$.*

The proof of this theorem used an idea similar to that in the proof of Theorem 15.

Theorem 22. ([169]) *The girth of the jumped Wenger graph $J_m(q, i, j)$ is at most* 8.

In the proof, the coordinates of each point and line in the cycle of length 8 are shown. The exact girth of $J_m(q, i, j)$ is determined via case by case analysis, see [169].

4.6 Sun graphs

Here we discuss a large family of regular Cayley graphs that, in general, are not bipartite and are defined by a system of equations described in Section 2.2. In particular, the generalized distance-two graphs of Wenger graphs and of the linearized Wenger graphs belong to this family.

Let $k \geqslant 3$ and $\mathbb{F}_q$ denote the field of q elements. Let $f_i, g_i \in \mathbb{F}_q[X]$ with $g_i(-X) = -g_i(X)$, for $3 \leqslant i \leqslant k$. Consider a graph $S(k,q) = S(k,q; f_3, g_3, \cdots, f_k, g_k)$ with the vertex set $\mathbb{F}_q^k$ and edges defined as follows: vertices $a = \langle a_1, a_2, \ldots, a_k \rangle$ and $b = \langle b_1, b_2, \ldots, b_k \rangle$ are adjacent if $a_1 = b_1$ and the following $k-2$ relations on their components hold:

$$b_i - a_i = g_i(b_1 - a_1) f_i\Big(\frac{b_2 - a_2}{b_1 - a_1}\Big), \quad 3 \leqslant i \leqslant k.$$

We call $S(k,q)$ *Sun graphs*. The requirement $g_i(-X) = -g_i(X)$ ensures that the adjacency in $S(k,q)$ is symmetric. It was introduced and studied by Sun [146] and Cioabă, Lazebnik and Sun [35].

Note that $S(k,q)$ are not bipartite. It is easy to see that they are Cayley graphs with underlying group being the additive group of the vector space $\mathbb{F}_q^k$ with generating set

$$\Big\{\Big(a, au, g_3(a)f_3(u), \cdots, g_k(a)f_k(u)\Big) \mid a \in \mathbb{F}_q^*, u \in \mathbb{F}_q\Big\}.$$

This implies that $S(k,q)$ is a vertex-transitive $q(q-1)$-regular graph, and their spectra can be studied using [5, 114]. Note that for $f_i = X^{i-1}$ and $g_i = X$, $3 \leqslant i \leqslant k+1$, $S(k+1,q)$ coincides with the distance-two graph of the Wenger graphs $W_k(q)$ on lines, and for $f_i = X^{p^{i-2}}$ and $g_i = X$ with $3 \leqslant i \leqslant k+1$, $S(k+1,q)$ coincides with the distance-two graph of the linearized Wenger graphs $L_k(q)$ on lines.

The connectivity and expansion properties of the graphs $S(k,q)$ were studied in [146, 35]. The spectral properties of $S(3,q;x^2,x^3)$ for prime q between 5 and 19, and of $S(4,q;x^2,x^3,x^3,x^3)$ for prime q between 5 and 13, show that these graphs are *not* distance-two graphs of any q-regular bipartite graphs.

4.7 Terlep–Williford graphs

In [150], Terlep and Williford considered the graphs $TW(q) = B\Gamma(\mathbb{F}_q; f_2, \ldots, f_8)$, where

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

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

These graphs provide the best asymptotic lower bound on the Turán number of the 14-cycle $ex(\nu, \{C_{14}\})$. The approach to their construction is similar to the one in [97], and it is obtained from a Lie algebra related to a generalized Kac–Moody algebra of rank 2.

Theorem 23. ([150]) *For infinitely many values of* ν,

$$ex(\nu, \{C_{14}\}) \geqslant (1/2^{9/8})\nu^{9/8}.$$

The best known upper bound is still of magnitude $\nu^{8/7}$, as follows from the Erdős Even Circuit Theorem and [16]. We wish to note that $TW(q)$ 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 in [150] 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, see, e.g., Marker [120]. We end this section with a problem.

Problem 24. Provide a computer-free proof of the fact that the graphs $TW(q)$ contain no 14-cycles for infinitely many q.

4.8 Verstraëte–Williford graphs

Let q be an odd prime power. In [166], Verstraëte and Williford considered the graphs G_q with vertex set $V = \mathbb{F}_q^4$, where distinct vertices $a = \langle a_1, a_2, a_3, a_4\rangle$ and $b = \langle b_1, b_2, b_3, b_4\rangle$ are adjacent if

$$a_2 + b_2 = a_1b_1, \quad a_3 + b_4 = a_1^2b_1, \quad a_4 + b_3 = a_1b_1^2.$$

One can easily check that every G_q has q^2 vertices of degree $q-1$ and all other vertices are of degree q. Hence, G_q has $\frac{1}{2}(q^5 - q^2)$ edges. It is also easy to check that G_q contains neither 4-cycles nor 6-cycles. The last statement also follows from the fact that G_q is a polarity graph of $D(4, q)$ and Theorem 1 in [103]. For details, see Section 6.2.3.

A *theta-graph*, denoted $\theta_{k,l}$, consists of $k \geqslant 2$ internally disjoint paths of length l with the same endpoints. It is demonstrated in [166] that for any odd prime power q, G_q contains no subgraph isomorphic to $\theta_{k,l}$. Together with the upper bound of Faudree and Simonovits from [55], it implies the asymptotic order of magnitude of the Turán number for $\theta_{3,4}$, namely that

$$ex(\nu, \theta_{3,4}) = \Theta(\nu^{5/4}).$$

More on the existence of $\theta_{k,l}$ in other graphs can be found in [166].

4.9 Monomial graphs and generalized quadrangles

When all f_i are monomials of two variables, we call the graphs $B\Gamma(\mathbb{F}_q; f_2, \ldots, f_n)$ *monomial graphs*. These graphs were first studied in [167] and in Dmytrenko [43]. Let $B(q; m, n) = B\Gamma(\mathbb{F}_q; p_1^m l_1^n)$. For fixed m, n and sufficiently large q, the isomorphism problem for $B(q; m, n)$ was solved in [167], and for all m, n, q, in Dmytrenko, Lazebnik and Viglione [44].

Theorem 25. ([44]) *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 [44], that every 4-cycle-free graph of the form $B(q; m, n)$, is isomorphic to $B(q; 1, 1)$, and so is isomorphic to the biaffine part of the point-line incidence graph of $PG(2, q)$. This result extends simply to the graphs $B\Gamma(\mathbb{F}; p_1^m l_1^n)$, where $\mathbb{F}$ is an algebraically closed field. On the other hand, it does not hold when $\mathbb{F} = \mathbb{R}$ – the field of real numbers. Kronenthal, Miller, Nash, Roeder, Samamah and Wong [89] showed that there exists $f \in \mathbb{R}[p_1, l_1]$ such that $\Gamma(\mathbb{R}; f)$ has girth 6 and is nonisomorphic to $\Gamma(\mathbb{R}; p_1 l_1)$ by providing $f = f(p_1, l_1) = \sum_{i,j \in \mathbb{N}} \alpha_{i,j} p_1^i l_1^j \in \mathbb{Q}[p_1, l_1] \setminus \{0\}$, where both i and j are odd for all nonzero $\alpha_{i,j}$ and either all $\alpha_{i,j} \geqslant 0$ or all $\alpha_{i,j} \leqslant 0$.

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 [8]. This means that viewed as bipartite graphs, they are isomorphic. For any odd prime power q, the graph $B\Gamma(\mathbb{F}_q; p_1 l_1, p_1 l_1^2)$, which has girth 8, is the biaffine part of $W(q)$. Just as a 4-cycle-free graph $B\Gamma(\mathbb{F}_q; f_2)$ 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 the graphs $B\Gamma(\mathbb{F}_q; p_1 l_1, p_1 l_1^2)$, by which we mean among monomial graphs.

The study of monomial graphs of girth eight for odd q began in [43], and continued in Dmytrenko, Lazebnik and Williford [45], and in Kronenthal [86]. All results in these papers suggested that for q odd, every monomial graph $B\Gamma(\mathbb{F}_q; f_2, f_3)$ of girth at least eight is isomorphic to the graph $B\Gamma(\mathbb{F}_q; p_1 l_1, p_1 l_1^2)$, as was conjectured in [45].

We wish to note that the investigation of cycles in monomial graphs leads 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). It was shown in [43] that if q is odd and the girth of $B\Gamma(\mathbb{F}_q; p_1 l_1, p_1^m l_1^n)$ is eight, then $m = k$ and $n = 2k$ for an integer k satisfying certain conditions. This led to the following conjecture.

Conjecture 26. ([45]) Let $q = p^e$ be an odd prime power. For an integer k with $1 \leqslant k \leqslant q - 1$, 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 [43, 45] that the validity of the conjecture for either A_k or B_k, would imply the following theorem.

Theorem 27. ([74]) *Let q be an odd prime power. Then every monomial graph $B\Gamma(\mathbb{F}_q; f_2, f_3)$ of girth at least eight is isomorphic to the graph $B\Gamma(\mathbb{F}_q; p_1 l_1, p_1 l_1^2)$.*

Hou, Lappano and Lazebnik in [74] proved Theorem 27 by making sufficient progress on Conjecture 26, though falling short of proving it either for A_k or for B_k. Finally, Conjecture 26 for A_k was confirmed by Hou [73], and for B_k, by Bartoli and Bonini [6].

Hence, no new generalized 4-gon can be constructed in this way. What if not both polynomials f_2 and f_3 are monomials? In [87], Kronenthal and Lazebnik showed that over every algebraically closed field $\mathbb{F}$ of characteristic zero, every graph $B\Gamma(\mathbb{F}; p_1 l_1, f_3(p_1, l_1))$

of girth at least eight is isomorphic to the graph $B\Gamma(\mathbb{F}; p_1l_1, p_1l_1^2)$. Their methods imply that the same result holds over infinitely many finite fields. In particular, the following theorem holds.

Theorem 28. ([87]) *Let q be a power of a prime p, $p \geqslant 5$, and let $M = M(p)$ be the least common multiple of integers $2, 3, \ldots, p-2$. Suppose $f_3 \in \mathbb{F}_q[p_1, l_1]$ has degree at most $p-2$ with respect to each of p_1 and l_1. Then over every finite field extension $\mathbb{F}$ of $\mathbb{F}_{q^M}$, every graph $B\Gamma(\mathbb{F}; p_1l_1, f_3(p_1, l_1))$ of girth at least eight is isomorphic to the graph $B\Gamma(\mathbb{F}; p_1l_1, p_1l_1^2)$.*

Kronenthal, Lazebnik and Williford [88] extended these "uniqueness" results to the family of graphs $B\Gamma(\mathbb{F}; p_1^ml_1^n, f_3(p_1, l_1))$ (with p_1l_1 replaced by an arbitrary monomial $p_1^ml_1^n$). Then Xu, Cheng and Tang [179] extended these results to the family of graphs $\Gamma(\mathbb{F}; f_2, f_3)$, where $f_2 = g(p_1)h(l_1)$, which is the product of two univariate polynomials, and $f_3 = f_3(p_1, l_1)$.

Problem 29. (i) Let q be an odd prime power, and let $f_2, f_3 \in \mathbb{F}_q[p_1, l_1]$. Is it true that every graph $B\Gamma(\mathbb{F}_q; f_2, f_3)$ with girth at least eight is isomorphic to the graph $B\Gamma(\mathbb{F}_q; p_1l_1, p_1l_1^2)$?
(ii) Let q be an odd prime power, and let $f_2 \in \mathbb{F}_q[p_1, l_1]$ and $f_3 \in \mathbb{F}_q[p_1, l_1, p_2, l_2]$. Is it true that every graph $B\Gamma(\mathbb{F}_q; f_2, f_3)$ with girth at least eight is isomorphic to the graph $B\Gamma(\mathbb{F}_q; p_1l_1, p_1l_1^2)$?

It is clear that a negative answer to each of the two parts of Problem 29 may lead to a new generalized quadrangle. It will lead to one, if such a graph exists and it is possible to "attach" it to 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 30. ([87]) Let $\mathbb{F}$ be an algebraically closed field of characteristic zero, and let $f_2, f_3 \in \mathbb{F}[p_1, l_1]$. Then every graph $B\Gamma(\mathbb{F}; f_2, f_3)$ with girth at least eight is isomorphic to the graph $B\Gamma(\mathbb{F}; p_1l_1, p_1l_1^2)$.

The investigations in [87] were continued in Nassau [126]. Let $\mathbb{F}$ be an algebraically closed field of characteristic zero. Consider the graph $B\Gamma(\mathbb{F}; f_2, f_3)$. In their definition (1), the first defining polynomial functions are $f_2 = f_2(p_1, l_1)$ and $f_3 = f(p_1, l_1, p_2, l_2)$. Note that f_3 can always be thought of as a function of three variables rather than four, namely $f_3 = f_3(p_1, l_1, p_2) = f(p_1, l_1, p_2, f_2(p_1, l_1) - p_2)$ or $f_3 = f_3(p_1, l_1, l_2) = f(p_1, l_1, f_2(p_1, l_1) - l_2, l_2)$. Therefore, we may assume that $f_3 = f_3(p_1, l_1, p_2)$. In particular, if f_3 is actually a function of two variables, say l_1 and p_2, we write it as $f_3(l_1, p_2)$. Among several results in [126], we mention just a few.

Theorem 31. ([126]) *Let $\mathbb{F}$ be an algebraically closed field, and let m, n be positive integers.*

1. *If $B\Gamma(\mathbb{F}; p_1l_1, f_3(l_1, p_2))$ has girth at least 8, then its girth is 8 and it is isomorphic to the graph $B\Gamma(\mathbb{F}; p_1l_1, p_1l_1^2)$.*

2. *If* $B\Gamma(\mathbb{F}; p_1 l_1, p_1^m g(l_1, p_2))$*, where* g *is a polynomial over* $\mathbb{F}$*, has girth at least 8, then its girth is 8 and it is isomorphic to the graph* $B\Gamma(\mathbb{F}; p_1 l_1, p_1 l_1^2)$*.*

3. *If* $B\Gamma(\mathbb{F}; p_1^m l_1^n, f_3(p_1, l_1, p_2))$ *has girth at least 8, then* $m = 1$ *or* $m = 2$*.*

Another question raised in [126] was the following: Suppose that q is an odd prime power. Given $B\Gamma(\mathbb{F}_q; f_2(p_1, l_1), f_3(p_1, l_1, p_2))$, is it always possible to find a polynomial $h = h(p_1, l_1)$ such that the graphs $B\Gamma(\mathbb{F}_q; f_2(p_1, l_1), h(p_1, l_1))$ and $B\Gamma(\mathbb{F}_q; f_2(p_1, l_1), f_3(p_1, l_1, p_2))$ are isomorphic? There are many examples in which the answer to this question is affirmative. Moreover, given f_3, the polynomial h can be found in many ways. For example, it is easy to verify that the following graphs are isomorphic:

$$B\Gamma(\mathbb{F}_q; p_1 l_1, p_1^2 l_1 - p_1 p_2) \cong B\Gamma(\mathbb{F}_q; p_1 l_1, p_2 l_1)$$

$$\cong B\Gamma(\mathbb{F}_q; p_1 l_1, p_1 l_1^2) \cong B\Gamma(\mathbb{F}_q; p_1 l_1, p_1^2 l_1).$$

Does one really need three variables in f_3 to create a graph not isomorphic to those with two variables p_1 and l_1 for infinitely many q? The answer to this question is positive. The following graph appeared in [126]:

$$B\Gamma(\mathbb{F}_p; p_1 l_1, p_1 l_1 p_2 (p_1 + p_2 + p_1 p_2)),$$

where p is an odd prime, and it was conjectured to have the property, i.e., it is not isomorphic to any graph $B\Gamma(\mathbb{F}_p; f_2(p_1, l_1), h(p_1, l_1))$. The result was proven for primes $p \equiv 1 \pmod 3$ in Lazebnik and Taranchuk [94]. The authors showed that the automorphism group of the graph $B\Gamma(\mathbb{F}_p; p_1 l_1, p_1 l_1 p_2 (p_1 + p_2 + p_1 p_2))$ is trivial. At the same time, the automorphism group of any graph $B\Gamma(\mathbb{F}_p; f_2(p_1, l_1), h(p_1, l_1))$ contains a subgroup isomorphic to the additive group of the field $\mathbb{F}_p$, formed by the automorphisms ϕ_a presented in (4), (5). Hence, for every prime $p \equiv 1 \pmod 3$, the graphs $B\Gamma(\mathbb{F}_p; p_1 l_1, p_1 l_1 p_2 (p_1 + p_2 + p_1 p_2))$ and $B\Gamma(\mathbb{F}_p; f_2(p_1, l_1), h(p_1, l_1))$ are not isomorphic.

Kodess, Kronenthal and Wong [81] studied $B\Gamma(\mathbb{F}; f(p_1) h(l_1), g(p_1) j(l_1))$, and classified all graphs $B\Gamma(\mathbb{F}; f(p_1) h(l_1), g(p_1) h(l_1))$ by girth, where $\mathbb{F}$ is an algebraically closed field. Ganger, Golden, Kronenthal and Lyons [64] proved that every graph $B\Gamma(\mathbb{R}; f_2(p_1, l_1))$ has girth 4 or 6 and classified infinite families of such graphs by girth, where $\mathbb{R}$ is the field of real numbers. Then Kodess, Kronenthal, Manzano-Ruiz and Noe [80] gave a complete classification of monomial graphs $B\Gamma(\mathbb{R}; p_1^m l_1^n, p_1^s l_1^t)$.

The case of graphs $B\Gamma(\mathbb{F}_q; p_1 l_1, f_3(p_1, l_1))$ of girth at least eight for q even is rather different: many non-isomorphic ones exist even in the case when $f_3(p_1, l_1) = p_1 f(l_1)$, with f being a special permutation polynomial of $\mathbb{F}_{2^e}$.

To the end of this section, we assume that $q = 2^e$. A permutation polynomial f of $\mathbb{F}_q$, $q > 2$, is called an *oval polynomial* or just *o-polynomial*, if its degree is at most $q - 2$, $f(0) = 0$, $f(1) = 1$ and for any distinct a, b, c in $\mathbb{F}_q$,

$$\det \begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ f(a) & f(b) & f(c) \end{pmatrix} \neq 0.$$

It is easy to argue, see, for example Hirschfeld [70], that the maximum number of points in a projective plane of order q with no three of them being collinear is $q+2$. If such a set exists, it is called a *hyperoval* in the plane. In $PG(2,q)$, $q>2$, hyperovals exist, and each is projectively equivalent to the set

$$D(f) := \{(1,t,f(t)), t \in \mathbb{F}_q\} \cup \{(0,0,1),(0,1,0)\}$$

for some o-polynomial f. It is easy to argue that graph $B\Gamma(\mathbb{F}_q; p_1l_1, p_1f(l_1))$, where f is an o-polynomial, is of girth eight, and is in fact the biaffine part of a generalized quadrangle. Therefore, new o-polynomials can lead to new generalized quadrangles. This is a reason why the classification of hyperovals in finite projective planes remains an active field of research, see Segre [140, 141, 142], Glynn [66, 67], Payne [130, 131], Cherowitzo, Penttila, Pinneri and Royle [31], Cherowitzo [29], Cherowitzo, O'Keefe and Penttila [30]. All known infinite families of projectively non-equivalent hyperovals in $PG(2,q)$, $q>2$, are listed below, see Mesnager [122]. They are presented by their o-polynomials.

1. The translation hyperovals: $f(x) = x^{2^m}$, where $gcd(m,e) = 1$.
2. The Segre hyperovals: $f(x) = x^6$, where e is odd.
3. The Glynn hyperovals: $f(x) = x^{3\times 2^{(e+1)/2}+4}$, where e is odd.
4. The Glynn hyperovals: $f(x) = x^{2^{(e+1)/2}+2^{(e+1)/4}}$, where $e \equiv 3 \pmod 4$.
5. The Glynn hyperovals: $f(x) = x^{2^{(e+1)/2}+2^{(3e+1)/4}}$, where $e \equiv 1 \pmod 4$.
6. The Cherowitzo hyperovals: $f(x) = x^{2^m} + x^{2^m+2} + x^{3\times 2^m+4}$, where $m = (e+1)/2$ and e is odd.
7. The Payne hyperovals: $f(x) = x^{\frac{1}{6}} + x^{\frac{1}{2}} + x^{\frac{5}{6}}$, where e is odd.
8. The Subiaco hyperovals:
$$f_a(x) = ((a^2(x^4+x) + a^2(1+a+a^2)(x^3+x^2))(x^4+a^2x^2+1)^{2^e-2} + x^{2^{e-1}},$$
where $\Sigma_{i=0}^{e-1}(1/a)^{2^i} = 1$ and $a \notin \mathbb{F}_4$ if $e \equiv 2 \pmod 4$.
9. The Adelaide hyperovals:
$$f(x) = \frac{T(\beta^e)(x+1)}{T(\beta)} + \frac{T((\beta x + \beta^q)^e)}{T(\beta)(x+T(\beta)x^{2^{e-1}}+1)^{e-1}} + x^{2^{e-1}},$$
where $e \geqslant 4$ is even, $\beta \in \mathbb{F}_{q^2} \setminus \{1\}$ with $\beta^{q+1} = 1$, $e \equiv \pm(q-1)/3 \pmod{q+1}$, and $T(x) = x + x^q$.

As far as we know, many sporadic hyperovals found originally by computer searches, led to discoveries of some families listed above. The first five examples in the list above are hyperovals with o-polynomials being of the form x^n. They are often called *monomial* hyperovals. It is conjectured in [66] that all monomial hyperovals are in the list. The conjecture was checked by computer for all $e \leqslant 28$ in [67], and for all $e \leqslant 40$, by Chandler [26].

4.10 $(n^{2/3}, n)$-bipartite graphs of girth 8 with many edges

Let $f(m, n)$ denote the largest number of edges in a bipartite graph whose bipartition sets have cardinalities m, n ($n \geqslant m$) and whose girth is at least 8. In [51], Erdős conjectured that $f(m, n) = O(n)$ for $m = O(n^{2/3})$. For a motivation of this question, see De Caen and Székely [22]. Using some results from combinatorial number theory and set systems, this conjecture was refuted in [22], 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 [98] explicitly constructed 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

$$\begin{aligned} l_2 + p_2 &= p_1 l_1, \\ l_3 + p_3 &= -(p_2 \overline{l_1} + \overline{p_2} l_1), \end{aligned}$$

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

Remark 32. A bipartite graph of girth eight and diameter four with every vertex in one partition having degree $s + 1$ and every vertex in another partition having degree $t + 1$ is called a generalized quadrangle of order (s, t). Such exists for $s = q$ and $t = q^2$. It can be obtained from the Hermitian variety $H(3, q^2)$ or, alternatively, from the geometry of the rank two twisted Chevalley group ${}^2A_3(q)$. Graph $\Gamma(q)$ is the biaffine part of it. We omit the details.

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 $B\Gamma(\mathbb{F}_{q^2}; p_1 l_1, -(p_2 \overline{l_1} + \overline{p_2} l_1))$ (see Section 3.2). Indeed, the only difference is that the third coordinates of the vertices of $\Gamma(q)$ are required to come from $\mathbb{F}_q$. It was mentioned by Taranchuk [149], that the expression $-(p_2 \overline{l_1} + \overline{p_2} l_1)$ in the definition of $\Gamma(q)$ can be replaced by a monomial $p_1 {l_1}^{q+1}$, producing an isomorphic graph on both $P \cup L$ and its induced subgraph on $P_A \cup L$.

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 by the set $P_A \cup L$. Then the family $\{\Gamma'(q)\}$ gives the desired $(n^{2/3}, n)$-bipartite graphs of girth 8 and with $n^{1+1/15}$ edges, where $n = q^2$, see [98] for details. It was noted by Füredi [59], that in order to obtain asymptotically the same number of edges, one could begin with the whole generalized quadrangle of type (q, q^2) and consider an induced subgraph on the same subset of its points and the whole set of its lines.

Problem 33. Improve the magnitude (exponent of n) in either the upper or the lower bound in the inequality

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

where c_1, c_2 are positive constants.

Modifying the construction of $\Gamma(q)$ in [98], Düzgün, Riet, and Taranchuk [47] defined a bipartite graph with $P = \mathbb{F}_q \times \mathbb{F}_{q^t} \times \mathbb{F}_q$, $L = \mathbb{F}_{q^t} \times \mathbb{F}_{q^t} \times \mathbb{F}_q$ in which (p) is adjacent to $[l]$ provided

$$\begin{aligned} l_2 + p_2 &= p_1 l_1, \\ l_3 + p_3 &= p_1 N(l_1), \end{aligned}$$

where $N : \mathbb{F}_{q^t} \to \mathbb{F}_q$ is the norm function. The resultant graph is $\{C_4, \theta_{t,3}\}$-free and namely, when $t = 4$, the graph is $\{C_4, \theta_{4,3}\}$-free with the vertex part sizes of order $n^{2/3}$ and n, and the graph has $\Theta(n^{1+1/9})$ edges, which is the best-known upper bound for $f(n^{2/3}, n)$.

4.11 Distance-regular graphs and crooked functions

Distance-regular graphs exhibit a high degree of combinatorial symmetry, and can be defined as follows. A *distance-regular* graph is a regular graph such that for any two vertices v and w, the number of vertices at distance j from v and at distance k from w depends only upon j, k, and the distance between v and w. Often an equivalent definition is given by using the intersection arrays of distance-regular graphs, but we omit this notion. These graphs were introduced by Biggs [13] and were discussed at length in [17], Van Dam, Koolen and Tanaka [41]. In [41], many references appearing after the publication of [17] were added, and many connections of distance-regular graphs to other areas of combinatorics and graph theory were discussed. Some distance-regular graphs can be defined by using systems of equations considered in the current survey.

An infinite family of distance-regular graphs was constructed by De Caen, Mathon, Moorhouse [21] as follows. Let $q = 2^{2t-1}$ and $s = 2^e$ where $\gcd(e, 2t-1) = 1$. Consider a graph $G(q, s)$ with vertex set $\mathbb{F}_q \times \mathbb{F}_2 \times \mathbb{F}_q$, with two (possibly equal) vertices (a, i, α) and (b, j, β) being adjacent when

$$\alpha + \beta = a^s b + a b^s + (i + j)(a^{s+1} + b^{s+1}).$$

Bending and Fon-Der-Flaass [7] generalized this construction by introducing the notion of crooked function. Let V be a vector space of odd dimension m over $\mathbb{F}_2$. A function $f : V \to V$ is called a *crooked function* (CF) if the following three conditions hold:

(i) $f(0) = 0$;

(ii) $f(x) + f(y) + f(z) = f(x + y + z)$ for any three distinct x, y, and z;

(iii) $f(x) + f(y) + f(z) = f(x + a) + f(y + a) + f(z + a)$ for all x, y, z and all $a \neq 0$.

The definition implies that a CF f is a bijection, and for any nonsingular linear transformations A and B of V, the function $g = BfA = B(f(A(x)))$ is also crooked. In this case, f and g are called *equivalent.* Let $a \neq 0$ and

$$H_a(f) = \{f(x) + f(x + a), \;\; x \in V\},$$

i.e., $H_a(f)$ is the image of the derivative of f. Condition 3 states that for every $a \neq 0$, no three points of $H_a(f)$ are collinear. It follows that f is a CF if and only if $f(0) = 0$ and $H_a(f)$ is the complement of a hyperplane for every $a \neq 0$. It is also shown that for a fixed CF f, all sets $H_a(f)$ are distinct. See [7] for details.

In [7], the *crooked graph* G_f (corresponding to a CF function f) is defined as follows. Its vertex set is $V \times \mathbb{F}_2 \times V$ with distinct vertices (a, i, α) and (b, j, β) being adjacent if and only if

$$\alpha + \beta = f(a + b) + (i + j + 1)(f(a) + f(b)).$$

Though this equation is not precisely a triangular system for graph $\Gamma_3 = \Gamma(\mathbb{F}_{2^e}; f_2, f_3)$ (f_2 is missing), some properties of graph G_f are close to the ones of Γ_3. It is not difficult to show that any two vertices in the subset

$$F_{a,i} := \{(a, i, \alpha) \mid \alpha \in V\}.$$

are at distance at least three, and that any two distinct subsets $F_{a,i}$ and $F_{b,j}$ are joined by a perfect matching. It follows that G_f is a $2e$-cover of the complete graph K_{2e+1}, and each $F_{a,i}$ is a fibre. It is clear that if two CF functions are equivalent, then the corresponding crooked graphs are isomorphic. It was shown in [7] that G_f is a distance-regular graph without triangles in which every pair of vertices at distance 2 lies in a unique 4-cycle.

As an attempt of providing examples of possibly new crooked functions and crooked graphs, the following proposition appeared in [7].

Let $* : V \times V$ be a bilinear multiplication satisfying

(i) $x * x \neq y * y$ for any $x \neq y$,

(ii) $x * y \neq y * x$ for any linearly independent x and y.

Then $f(x) = x * x$ is crooked. The converse also holds: if $*$ is a bilinear multiplication such that $f(x) = x * x$ is crooked, then this multiplication satisfies (i) and (ii).

Examples of such a multiplication $*$ can be constructed as follows: take $V = \mathbb{F}_{2^e}$, e odd, take k coprime to n, and let $x * y = xy^{2^k}$. These give the examples of graphs from [21] with loops deleted. As the authors of [7] stated, they had not been able to find new examples of crooked functions which did not come from a bilinear multiplication, nor any other crooked functions.

A set of all CF functions forms a proper subsets in a set of *almost bent* (AB) functions, which, in turn, forms a proper subset of the set of *almost perfect nonlinear* functions (APN). See Van Dam and Fon-Der-Flaass [40] for various equivalent definitions of CF, AB and APN functions, and proofs of the statement above concerning the corresponding sets containments. Here we just want to mention that APN functions can be defined by using only (ii) in the definition of CF. AB and APN functions were studied extensively and independently of CF because of their applications to cryptography, coding theory and combinatorics. Identifying an e-dimensional vector space over $\mathbb{F}_2$ with the finite field $\mathbb{F}_{2^e}$, any function can be represented by a polynomial. It was shown by Nyberg and Knudsen [128] that every bijective quadratic APN is crooked, by Kyureghyan [90] and [91] that all monomial crooked functions are of the form $x^{2^k+2^l}$, and by Bierbrauer and Kyureghyan [12] that binomial crooked functions are quadratic. It is not known if crooked functions of higher degree exist. For known examples, discussions and many references on APN functions, see Carlet [25], and Li and Kaleyski [110].

We wish to mention three combinatorial applications.

1. Let f be an AB function with $f(0) = 0$. Then the graph with vertex set $V \times V$, where two distinct vertices (x, a) and (x, b) are adjacent if

$$a + b = f(x + y),$$

   is a distance-regular graph, and it is isomorphic to a well-known distance-regular Kasami graph of diameter 3. This description was suggested by De Caen and Van Dam in [20]. Clearly, what we have is the graph $\Gamma(\mathbb{F}_{2^e}; f_2)$ with $f_2 = f$ and all loops deleted. A direct proof that this is indeed a distance-regular Kasami graph is given by Van Dam and Fon-Der-Flaass [39] for CR functions, and it was adjusted for AB functions.

2. Let f be an APN function. Consider a bipartite graph $B\Gamma(\mathbb{F}_{2^e}; f_2)$ with $f_2 = f$, i.e., a point (x, a) is adjacent to a line $[y, b]$ if $a + b = f(x + y)$. This graph is isomorphic (if it is connected) to a semi-biplane constructed by Coulter and Henderson [36]. In it, every two vertices from the same partition are adjacent to zero or two vertices from another partition.

3. For each $t \geqslant 1$, let W_t denote the class of graphs other than stars of diameter 2 and contain neither a triangle nor a $K_{2,t}$. It was conjectured by Wood [42] that W_t is finite for $t \geqslant 2$. Recently, Eberhard, Taranchuk and Timmons [48] disproved this conjecture for all $t \geqslant 3$. For $t = 3, 5$, they modified crooked graphs from [21] and [7]. For $t = 3$, the obtained graphs were $\{C_3, K_{2,3}\}$-free. Furthermore, their edge count, together with the upper bound $ex(\nu, K_{2,3}) \leqslant \frac{1}{\sqrt{2}}\nu^{\frac{3}{2}} + O(\nu)$ from Kővári, Sós and Turán [85], implies that if k is an integer and $\nu = 2^{4k+3}$, then

$$ex(\nu, \{C_3, K_{2,3}\}) = \frac{1}{\sqrt{2}}\nu^{3/2} + o(\nu^{3/2}).$$

   For these values of ν, it improves the general lower bound for $ex(\nu, \{C_3, K_{2,3}\})$, which is $\left(\frac{1}{\sqrt{3}} + o(1)\right)\nu^{3/2}$ for all sufficiently large ν. See also Allen, Keevash, Sudakov, and Verstraëte [3] for best-known general bounds for $ex(\nu, \{C_3, K_{2,3}\})$.

4.12 Digraphs

Consider a digraph with loops $D_n = \Gamma(\mathbb{F}_q; f_2, \ldots, f_n)$, defined as in Section 2.2 by system (2), with f_i's not necessarily symmetric. The study of these digraphs was initiated by Kodess [79]. Some general properties of these digraphs are similar to those of the graphs Γ_n. A digraph is called *strongly connected* if there exists a directed path between any two of its vertices, and every digraph is a union of its strongly connected (or just strong) components.

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

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

The strong connectivity of these digraphs was studied by Kodess and Lazebnik [82]. Utilizing some ideas from [167], 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 [82].

Finding the diameter of strongly connected 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., $f_2 = X^mY^n$, makes it a bit easier, though exact results are still hard to obtain. In [84], Kodess, Lazebnik, Smith and Sporre studied the diameter of digraphs $D(q; m, n) = \Gamma(\mathbb{F}_q; X^mY^n)$. They obtained precise values and good bounds on the diameter of these digraphs for many instances of the parameters. For some of the results, the connection to Waring's number 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 [82].

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 the bipartite monomial graphs $B(q; m, n)$ was answered in Theorem 25. For those graphs $B(q; m, n)$, just the count of 4-cycles resolves the isomorphism question for fixed m, n and large q (see [167]), and the count of complete bipartite subgraphs gives the answer for all q, m, n (see [45]). In contrast, for the 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 [79]). In this regard, we would like to state the following problem and a conjecture. For any digraphs A and B, let $|A(B)|$ denote the number of subdigraphs of A isomorphic to B.

Problem 34. Are there digraphs $D_1, \ldots, D_k$ 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 $i = 1, \ldots, k$?

Kodess and Lazebnik [83] discussed several necessary conditions and several sufficient conditions for the isomorphism. Though the sufficiency of the condition in the following conjecture is easy to verify, see [83], its necessity is still to be established.

Conjecture 35. ([79]) 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

$$\begin{aligned} m_2 &\equiv k m_1 \mod (q-1), \\ n_2 &\equiv k n_1 \mod (q-1). \end{aligned}$$

The conjecture is still not resolved even when q is a prime. As a bi-product of the work on isomorphism of monomial digraphs, Coulter, De Winter, Kodess and Lazebnik [37] established a peculiar result on the number of roots of certain polynomials over finite fields. It can be considered as an application of the digraphs $D(q; m, n)$ to algebra.

4.13 Multicolor Ramsey numbers

Let $k \geqslant 2$. The *multicolor Ramsey number* $r_k(G)$ is the minimum integer N such that in any edge-coloring of the complete graph K_N with k colors, there is a monochromatic G. Using a 4-cycle free graph $\Gamma_2 = \Gamma(\mathbb{F}_q; XY)$ with q being an odd prime power, Lazebnik and Woldar [108] showed that $r_q(C_4) \geqslant q^2 + 2$. It compared well with an upper bound by Chung and Graham [33], which implied that $r_q(C_4) \leqslant q^2 + q + 1$. The following result was generalized in [92].

Theorem 36. ([92]) *Let p be a prime. Then*

$$tk^2 + 1 \leqslant r_k(K_{2,t+1}) \leqslant tk^2 + k + 2, \tag{9}$$

where the lower bound holds whenever t and k are both prime powers of p. If k is a prime power, then

$$r_k(C_4) \geqslant k^2 + 2.$$

The upper bound in (9) follows from [85]. For the lower bound, the construction was algebraic. Recently, Taranchuk [148] suggested that the construction of $K_{2,t+1}$-free graphs that are used to construct the lower bound in (9) can be obtained as a particular case of a Γ_n-like graph. Let $q = p^e$, where p is a prime and $e \geqslant 1$, and let $\mathbb{F}_q$ be a field of order q. The field $\mathbb{F}_q$ can be viewed as an e-dimensional vector space $\mathbb{F}_p^e$ over $\mathbb{F}_p$. Given a positive integer d, $1 \leqslant d < e$, consider a linear map f of $\mathbb{F}_p^e$ onto any of its $(e-d)$-dimensional subspaces W. As the kernel of f has dimension d, it contains p^d vectors. It is known that any function on $\mathbb{F}_q$ can be interpolated by a polynomial with one indeterminate of degree at most $q-1$. Without changing notation, we denote the polynomial that interpolates the linear map f by f again. Consider the graph G with the vertex set $V(G) = \mathbb{F}_q \times W$ and two distinct vertices $\langle x_1, x_2 \rangle$ and $\langle y_1, y_2 \rangle$ being adjacent if

$$x_2 + y_2 = f(x_1 y_1).$$

It is clear that if $t = p^d$, then $n = |V(G)| = q\,|W| = q^2/t$. It is easy to verify that G is $K_{2,t+1}$-free, and, after the loops are deleted, it is left with

$$\frac{\sqrt{t}}{2} n^{3/2} - \frac{\sqrt{tn}}{2}$$

edges. Partitioning the edge set of the complete graph K_n into copies of G (Theorem 6), leads to the lower bound in (9).

Li and Lih [112] used Wenger graphs to determine the asymptotic behavior of the Ramsey number $r_n(C_{2k}) = \Theta(n^{k/(k-1)})$ when $k \in \{2, 3, 5\}$. For details, and more on the multicolor Ramsey numbers, see [33, 108, 113], and a survey by Radziszowski [135].

4.14 Miscellaneous constructions and applications

Two graphs on the same vertex set are *G-creating* if their union contains G as a subgraph. Let $H(n, k)$ be the maximum number of pairwise C_k-creating hamiltonian paths of K_n. By the constructions of bipartite graphs with many edges and without even cycles in Reiman [137], Benson [9] and Lazebnik, Ustimenko and Woldar [100], Soltész [145] showed that

$$n^{n/k-o(n)} \leqslant H(n, 2k) \leqslant n^{(1-2/(3k^2-2k))n-o(n)}.$$

Then Harcos and Soltész [69] used Ramanujan graphs to improve the upper bound to $n^{(1-\frac{1}{3k})n+o(n)}$, and Byrne and Tait [19] improved this upper bound to $n^{\frac{2}{3}n+o(n)}$ for $k = 3$, to $n^{\frac{4}{5}n+o(n)}$ for $k = 4, 5$, and to $n^{(1-\frac{2}{3k})n+o(n)}$ for $k \geqslant 6$. Mirzaei, Suk and Verstraëte [123] studied the effect of forbidding short even cycles in incidence graphs of point-line arrangements in the plane. By modifying the construction in [97], the authors constructed an arrangement of n points and n lines in the plane, such that their incidence graph has girth at least $k + 5$, and determines at least $\Omega(n^{1+4/(k^2+6k-3)})$ incidences.

5 Some Turán-type extremal problems for hypergraphs

Let $ex_r(\nu, H)$ be the largest number of edges in an H-free r-uniform hypergraph on ν vertices. For $r = 2$, we use the notation for usual graphs: $ex(\nu, H) = ex_2(\nu, H)$.

For $k \geqslant 2$, a *cycle* (Berge cycle) in a hypergraph $\mathcal{H}$ is an alternating sequence of vertices and edges of the form $v_1, E_1, v_2, E_2, \ldots, v_k, E_k, v_1$, such that

(i) $v_1, v_2, \ldots, v_k$ are distinct vertices of $\mathcal{H}$,

(ii) $E_1, E_2, \ldots, E_k$ are distinct edges of $\mathcal{H}$,

(iii) $v_i, v_{i+1} \in E_i$ for each $i \in \{1, 2, \ldots, k-1\}$, 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 [46]). For $r = 2$ and $k \geqslant 3$, 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 [104], Lazebnik and Verstraëte considered the Turán-type extremal problem of determining the maximum number of edges in an r-graph on ν vertices of girth five. For graphs ($r = 2$), this is an old problem of Erdős [50]. The following inequalities are the best known:

$$\frac{1}{2\sqrt{2}}\nu^{3/2} + \Omega(\nu^{5/4}) \leqslant ex(\nu, \{C_3, C_4\}) \leqslant \frac{1}{2}\nu\sqrt{\nu - 1},$$

where the upper bound holds for all ν and can be derived easily, and the lower bound is a recent result by Ma and Yang [118] for $\nu = 2(q^2 + q + 1)$ and q a prime power.

For bipartite graphs, on the other hand, this maximum is $(1/2\sqrt{2})\nu^{3/2} + O(\nu)$ as $\nu \to \infty$. Many attempts at reducing the gap between the constants $1/2\sqrt{2}$ and $1/2$ in the main terms of the upper and lower bounds have not succeeded so 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 upper and lower bounds for the maximum turned out to be equal, and the difference between the bounds was $O(\nu^{1/2})$.

Theorem 37. ([104]) *Let $\mathcal{H}$ be a 3-graph on ν vertices and of girth at least five. Then*

$$|\mathcal{H}| \leqslant \frac{1}{6}\nu\sqrt{\nu - \frac{3}{4}} + \frac{1}{12}\nu.$$

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

$$|\mathcal{H}| = \binom{q+1}{3} = \frac{1}{6}\nu^{3/2} - \frac{1}{6}\nu^{1/2}.$$

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 $\mathcal{G}_q$ (Lazebnik–Verstraëte 3-graph), of order $\nu = q(q-1)$, of girth five (for sufficiently large ν) and number of edges $\sim \frac{1}{6}\nu^{3/2} - \frac{1}{4}\nu + o(\nu^{1/2})$, $\nu \to \infty$. Let $\mathbb{F}_q$ denote the finite field of odd characteristic, and let S_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 $\mathbb{F}_q \times \mathbb{F}_q \setminus S_q$. 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 [104] for details. It raised the asymptotic lower bound to $\frac{1}{6}\nu^{3/2} - \frac{1}{6}\nu + o(\nu^{1/2})$, $\nu \to \infty$, as stated in Theorem 37. So, treating $\leqslant$ in an asymptotic sense, we have

$$\frac{1}{6}\nu^{3/2} - \frac{1}{6}\nu + o(\nu^{1/2}) \;\leqslant\; ex_3(\nu, \{\mathcal{C}_3, \mathcal{C}_4\}) \;\leqslant\; \frac{1}{6}\nu\sqrt{\nu - \frac{3}{4}} + \frac{1}{12}\nu.$$

Mukherjee [125] used the construction of bipartite graphs without even cycles and with many edges in [100] to prove that $ex_3(\nu, \widetilde{C}_6) = \Theta(\nu^{7/3})$, where $\widetilde{C}_6$ is the 3-uniform hypergraph obtained by adding a new vertex x to $V(C_6)$ and $\widetilde{C}_6 = \{e \cup x : e \in E(C_6)\}$.

A k-partite graph is said to be *balanced* k-partite if each partite set has the same number of vertices. Let $ex(\nu, \nu, \nu, \mathcal{F})$ be the maximum number of edges in balanced 3-partite graphs on partition classes of size ν, which are $\mathcal{F}$-free. Lv, Lu and Fang constructed balanced 3-partite graphs with many edges, which are $\mathcal{C}_4$-free in [116] and $\{\mathcal{C}_3, \mathcal{C}_4\}$-free in [117], and showed that

$$ex(\nu, \nu, \nu, \mathcal{C}_4) = \Big(\frac{3}{\sqrt{2}} + o(1)\Big)\,\nu^{3/2}$$

and

$$ex(\nu, \nu, \nu, \{\mathcal{C}_3, \mathcal{C}_4\}) \geqslant \Big(\frac{6\sqrt{2} - 8}{(\sqrt{2} - 1)^{3/2}} + o(1)\Big)\,\nu^{3/2}.$$

For more on Turán-type problems for graphs and hypergraphs, see [14, 57, 62].

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

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

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

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 [100] that for $k \geqslant 6$ and odd q, the 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 [119], and independently by Lubotzky, Phillips and Sarnak [115].

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 in Ustimenko [156] on the embedding of Chevalley group geometries into their corresponding Lie algebras. For a more recent exposition of these ideas, see [163, 176, 150].

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 [96] 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 $k = 3, 4, 6$, see [56]. Therefore, $D(k, q)$ are not subgraphs of generalized k-gons for $k \geqslant 4$.

In this section we will discuss some basic properties of these graphs.

6.1 Equivalent representation of $D(k, q)$

The defining equations for $D(k, q)$ have changed with time, and the changes reflected better understanding of their automorphisms. The following statement describes some transformations of the defining equations that lead to isomorphic graphs.

Proposition 38. ([146, 93]) *Let $a_1, \ldots, a_{k-1} \in \mathbb{F}_q^*$ with $k \geqslant 2$. Let the graph $H(k, q) = B\Gamma(\mathbb{F}_q; f_2, \ldots, f_k)$ where $f_2 = a_1 p_1 l_1$, $f_3 = a_2 p_1 l_2$, and for $4 \leqslant i \leqslant k$,*

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

Then $H(k, q)$ is isomorphic to $D(k, q)$.

Proof. Let $\varphi : V(D(k, q)) \to V(H(k, q))$ be defined via $(p) \mapsto (x)$, and $[l] \mapsto [y]$, 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. The verification that φ preserves the adjacency is straightforward, and can be found in [146, 93]. □

Taking

$$a_i = \begin{cases} -1, & \text{for } i \equiv 0 \text{ or } 3 \pmod 4, \\ 1, & \text{for } i \equiv 1 \text{ or } 2 \pmod 4, \end{cases}$$

and using Proposition 38, we see that $D(k, q)$ is isomorphic to $B\Gamma(\mathbb{F}_q; f_2, \ldots, f_k)$ where $f_2 = p_1 l_1$, $f_2 = p_1 l_2$, and for $4 \leqslant i \leqslant k$,

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

From now on, we will use this representation of $D(k, q)$.

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

$$D(k, 2) \cong 2^{k-3} C_{16},$$

for $k \geqslant 5$. Here nH denotes the union of n disjoint copies of a graph H. Therefore we assume that $q \geqslant 3$ for the rest of this section.

6.2 Automorphisms of $D(k,q)$

There are many automorphisms of $D(k,q)$, and below we list the ones that are used to establish some properties of the graph. It is a straightforward verification that the mappings we describe are indeed automorphisms. For more details, see [96, 97], Füredi, Lazebnik, Seress, Ustimenko and Woldar [60], Lazebnik, Ustimenko and Woldar [101] and Erskine [53]. The automorphisms in these references may look different to the ones we list here since we use another representation of the graph.

6.2.1 Multiplicative automorphisms

For any $a,b \in \mathbb{F}_q^*$, consider the map $m_{a,b} : P_k \to P_k, L_k \to L_k$ such that $(p) \overset{m_{a,b}}{\mapsto} (p')$, and $[l] \overset{m_{a,b}}{\mapsto} [l']$ where $p'_1 = ap_1$, $l'_1 = bl_1$, and for any $2 \leqslant i \leqslant k$,

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

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

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 $a^{t+2}b^{t+1}$.

	$m_{a,b}$		$m_{a,b}$
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}	$*a^{t+2} b^{t+1}$

Table 1: Multiplicative automorphism

Proposition 39. *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 $0 \leqslant j \leqslant k$, we define the map $t_{j,x} : P_k \to P_k, L_k \to L_k$ 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, we illustrate how each coordinate is changed under the maps. 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: $l_1 \mapsto l_1 + x$, $l_4 \mapsto l_4 + l_2 x$, $l_{2t} \mapsto l_{2t} + l_{2t-3}x$ for $t \geqslant 3$, and the following coordinates of a point according to the rule: $p_2 \mapsto p_2 + p_1 x$, $p_4 \mapsto p_4 + 2p_2 x + p_1 x^2, \cdots$.

	$t_{0,x}$	$t_{1,x}$	$t_{2,x}$
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}	$+p_{4t+2} x$		$-p_{4t-1} x$
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}		$+l_{4t-3} x$	$+l_{4t-4} x$

Table 2: Additive automorphism

2. For $2 \leqslant j \leqslant k$, $t_{j,x}$ is a map which fixes the first $j-1$ coordinates of a point and a line. In Table 3, we illustrate how each coordinate is changed under the corresponding map.

Proposition 40. *For any $x \in \mathbb{F}_q$ and $0 \leqslant j \leqslant k$, $t_{j,x}$ is an automorphism of $D(k,q)$.*

6.2.3 Polarity automorphism

Consider the map $\phi : P_k \to L_k, L_k \to P_k$ such that

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

$j \equiv 0\ ,\ 1 \pmod 4$			
	$t_{j,x}$		$t_{j,x}$
p_i $i \leqslant j-1$		l_i $i \leqslant j-1$	
p_j	$+x$	l_j	$-x$
p_{j+1+2t}		l_{j+1+2t}	
p_{j+2}	$-p_1 x$	l_{j+2}	
p_{j+4}	$-p_2 x$	l_{j+4}	$-l_2 x$
p_{j+4+2t}	$-p_{2t+1} x$	l_{j+4+2t}	$-l_{2t+1} x$

$j \equiv 2\ ,\ 3 \pmod 4$			
	$t_{j,x}$		$t_{j,x}$
p_i $i \leqslant j-1$		l_i $i \leqslant j-1$	
p_j	$+x$	l_j	$-x$
p_{j+1+2t}		l_{j+1+2t}	
p_{j+2}		l_{j+2}	$+l_1 x$
p_{j+4}	$+p_2 x$	l_{j+4}	$+l_2 x$
p_{j+4+2t}	$+p_{2t+2} x$	l_{j+4+2t}	$+l_{2t+2} x$

Table 3: Additive automorphism (continued)

and

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

The proof of the following proposition is straightforward.

Proposition 41. *If k is even, or q is even, then ϕ is an automorphism of $D(k, q)$.*

Theorem 42. ([97]) *For any integer $k \geqslant 2$, and any prime power q, the automorphism group of $D(k, q)$ is transitive on P_k, transitive on L_k, and the graph is edge-transitive. If any one of k and q is even, then $D(k, q)$ is vertex-transitive.*

Moreover, the automorphism group of $D(k, q)$ acts transitively on the set of paths of length 3 (3-paths). This useful fact appeared implicitly in several papers, and it was rediscovered independently and stated explicitly in [150, 146, 53]. For $k \geqslant 4$ with $k \not\equiv 3 \pmod 4$ and any prime power q, the automorphism group of $D(k, q)$ acts transitively on the set of all ordered 3-paths (see [53]). It will be discussed in Section 6.4 that, except for finitely many k, the graph $D(k, q)$ is disconnected and all its components are isomorphic. The components are denoted by $CD(k, q)$. The order of the automorphism group of $CD(k, q)$, for some small k and q, was computed in [53], and the following conjecture appeared there.

Conjecture 43. ([53]) Let $k \geqslant 3$, $m = k - \lfloor \frac{k-2}{4} \rfloor$ and let $q = p^e$ be an odd prime power larger than 3. Then the automorphism group of the graph $CD(k,q)$ has order exactly

$$\begin{cases} eq^{m+1}(q-1)^2, & \text{if } q \equiv 3 \pmod 4, \\ 2eq^{m+1}(q-1)^2, & \text{if } q \equiv 0,1,2 \pmod 4. \end{cases}$$

This count suggests that the stabilizer of the 3-path

$$[1,0,\ldots,0] \sim (0,0,\ldots,0) \sim [0,0,\ldots,0] \sim (1,0,\ldots,0)$$

in the action of the automorphism group of $CD(k,q)$ on its 3-paths is generated by the multiplicative automorphisms and the Frobenius automorphisms of the field. The results in [167] on the structure of the automorphism group of $D(2,q)$ and $D(3,q)$ support this. For $q = 3$, the number of components of $D(k,3)$ is not well-understood.

Problem 44. Determine the automorphism group of the graph $CD(k,q)$.

6.3 Girth of $D(k,q)$

Lazebnik and Ustimenko in [97] showed that $girth(D(k,q)) \geqslant k+5$ for odd k, and $girth(D(k,q)) \geqslant k+4$ for even k.

Theorem 45. ([97]) *Let $k \geqslant 2$ be an integer, and let q be a prime power. Then $girth(D(k,q)) \geqslant k+5$ if k is odd, and $girth(D(k,q)) \geqslant k+4$ if k is even.*

Recently, Taranchuk [147] presented a simpler proof of this theorem. Here are the main ideas of his proof. The algebraically defined graph $A(n,q) = B\Gamma(\mathbb{F}_q; f_2, \ldots, f_n)$ was introduced by Ustimenko in [159, 160, 161], where

$$f_i = \begin{cases} p_{i-1}\ell_1, & \text{if } i \text{ is even}, \\ p_1\ell_{i-1}, & \text{if } i \text{ is odd}, \end{cases}$$

for $2 \leqslant i \leqslant n$. Let (0) denote the point corresponding to the zero vector. The point (0) in $A(n,q)$ is not contained in any cycle of length less than $2n+2$. Then there is a covering map from $D(2k+1,q)$ to $A(k+2,q)$ which maps the point (0) in $D(2k+1,q)$ to the point (0) in $A(k+2,q)$. By transitivity of $D(2k+1,q)$ on the set of points and the properties of covering maps, no cycle of length less than $2k+6$ can appear in $D(2k+1,q)$.

The following conjecture was stated in [60] for all $q \geqslant 5$, and here we extend it to the case $q \geqslant 4$.

Conjecture 46. The graph $D(k,q)$ has girth $k+5$ for odd k and girth $k+4$ for even k, and all prime powers $q \geqslant 4$.

The conjecture is wide open, and it was confirmed only for a few infinite families of k and q, see Schliep [139], Thomason [152, 153], Xu, Cheng and Tang [180] and Xu [178].

For $q = 2$, the girth of $D(k, 2)$ is 8 if $k = 2, 3, 4$, and 16 if $k \geqslant 5$. For $q = 3$, the girth of $D(k, 3)$ exhibits different behavior, and we do not understand it completely. The known results on the girth for $2 \leqslant k \leqslant 320$ are summarized by Xu, Cheng and Tang in [181]. They are shown in the following table with either the exact values of the girth or upper bounds for the girth, where $[m, n]$ denotes the set of all integers k such that $m \leqslant k \leqslant n$. Note that the lower bound of the girth is $k + 5$ for odd k, and $k + 4$ for even k.

k	2	3	$[4, 8]$	$[9, 14]$	$[15, 16]$	$[17, 19]$	$[20, 24]$
girth	6	8	12	18	20	24	28
k	$[25, 26]$	$[31, 32]$	35	39	$[49, 50]$	51	55
girth	34	36	40	$\leqslant 48$	54	56	$\leqslant 68$
k	67	71	79	[103,104]	111	135	143
girth	72	$\leqslant 80$	$\leqslant 96$	108	$\leqslant 136$	$\leqslant 144$	$\leqslant 160$
k	[157,158]	159	211	223	271	287	[319,320]
girth	162	$\leqslant 192$	216	$\leqslant 272$	$\leqslant 288$	$\leqslant 320$	324

Table 4: Known girth of $D(k, 3)$ for $2 \leqslant k \leqslant 320$

Problem 47. Determine the girth of $D(k, 3)$ for all $k \geqslant 2$.

Conjecture 46 was proved only for infinitely many pairs of (k, q). The following results describe all of them.

Theorem 48. ([60]) *For odd $k \geqslant 3$, and q being a member of the arithmetic progression $\{1 + n(\frac{k+5}{2})\}_{n \geqslant 1}$,*

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

Remark 49. The theorem could be extended for even $k \geqslant 2$ and q being a member of the arithmetic progression $\{1 + n(\frac{k+4}{2})\}_{n \geqslant 1}$, and in this case $girth(D(k, q)) = k + 4$. The proof is essentially the same as the proof in [60], and we omit it.

By modifying an idea from [60], this result was strengthened in [146].

Theorem 50. ([146]) *For any $k \geqslant 3$ with $k \equiv 3 \pmod 4$, and q being a member of the arithmetic progression $\{1 + n(\frac{k+5}{4})\}_{n \geqslant 1}$,*

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

Cheng, Chen and Tang found other sets of pairs (k, q) for which the girth of $D(k, q)$ could be determined precisely, see [27, 28]. See also the aforementioned papers [180, 181]. Their results are as follows.

Theorem 51. ([27]) *For any $q \geqslant 4$, and any odd k such that $(k+5)/2$ is a power of the characteristic of $\mathbb{F}_q$,*

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

Theorem 52. ([28]) *For any prime p, and any positive integers h, m, s with $h|(p^m - 1)$ and $hp^s > 3$,*

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

Theorem 53. ([180]) *For any $q > 3$,*

$$girth(D(3,q)) = girth(D(4,q)) = 8 \text{ and } girth(D(5,q)) = 10.$$

Theorem 54. ([181]) (i) $girth(D(4t+2,q)) = girth(D(4t+1,q))$.
(ii) $girth(D(4t+3,q)) = 4t+8$ if $girth(D(2t,q)) = 2t+4$.
(iii) $girth(D(8t,q)) = 8t+4$ if $girth(D(4t-2,q)) = 4t+2$.
(iv) $girth(D(2^{s+2}t-5,q)) = 2^{s+2}t$ if $p \geqslant 3, 2^s \mid (q-1), 2^{s+1} \nmid (q-1), 2 \nmid t$ and $t \mid_p (q-1)$, where $t \mid_p (q-1)$ denotes $t \mid (q-1)p^r$ for some $r \geqslant 0$.

We wish to note that part (iv) of Theorem 54 can be easily obtained from part (ii) and Theorem 52.

Suppose that the girth of $D(k,q)$ satisfies Conjecture 46. Then the following theorem allows us to determine the exact values of the girth of $D(k',q)$ for infinitely many values of k'.

Theorem 55. ([146]) *Let p be the characteristic of $\mathbb{F}_q$ and $g_k = girth(D(k,q))$, where $k \geqslant 3$. Suppose that g_k satisfies Conjecture 46. Then*

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

In addition, if $k \not\equiv 3 \pmod 4$, then the following also holds:

$$girth\big(D(pg_k - 4, q)\big) = pg_k.$$

By Theorems 48, 50, and 55, Conjecture 46 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 $\mathbb{F}_q$.

The known values of girth of $D(k,q)$ for $2 \leqslant k \leqslant 100$ and $4 \leqslant q \leqslant 97$ are shown in Tables 7-13 (see Appendix), which are proven either by computer or Theorems 48-55, and empty cells correspond to the cases where the girth is unknown.

6.4 Connectivity of $D(k, q)$

Let $c(G)$ be the number of components of a graph G. In [100], Lazebnik, Ustimenko and Woldar proved that for $k \geqslant 6$ and odd q, the graph $D(k, q)$ is disconnected. As the graph $D(k, q)$ is edge-transitive, all components are isomorphic. Let $CD(k, q)$ denote one of them. It was shown in [100] that $c(D(k, q)) \geqslant q^{t-1}$, 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 [101], the same authors proved that for all odd q, $c(D(k, q)) = q^{t-1}$. It is shown in [106] that $c(D(k, q)) = q^{t-1}$ for even $q > 4$, $c(D(k, 4)) = q^t$ for $k \geqslant 4$, 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 [100]).

6.4.1 Invariant vector

Let $k \geqslant 6$ and $t = \lfloor \frac{k+2}{4} \rfloor$. For every point $(p) = (p_1, \dots, p_k)$ and every line $[l] = [l_1, \dots, l_k]$ in $D(k, q)$, and for any $2 \leqslant r \leqslant t$, let $a_r : P_k \cup L_k \to \mathbb{F}_q$ be given by:

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

and

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

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 to be

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

The following proposition justifies the term. The proof is straightforward, and the details can be found in the original paper [100], and with the representation of $D(k, q)$ adopted in this survey, in [93].

Theorem 56. ([100]) *If $(p) \sim [l]$, then $\vec{a}((p)) = \vec{a}([l])$.*

Corollary 57. *All the vertices in the same component of $D(k, q)$ have the same invariant vector.*

Let (0) denote the point corresponding to the zero vector. By Corollary 57, and the fact that $\vec{a}((0)) = \vec{0}$, we obtain the following theorem.

Theorem 58. ([100]) *Let u be a vertex in the component of $D(k,q)$ containing* (0). *Then*

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

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 $k \geqslant 6$ and $q \neq 4$, and we will discuss it in the following four subsections. This discussion will also lead to determining the number of components $c(D(k,q))$.

6.4.2 Lower bound for $c(D(k,q))$

Theorem 59. ([100]) *For any $k \geqslant 2$, let $t = \lfloor \frac{k+2}{4} \rfloor$ and let q be a prime power. Then*

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

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 $(p') = (p'_1, \ldots, p'_k)$ defined by:

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

and

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

It is easy to see that $\vec{a}((p)) = x \neq y = \vec{a}((p'))$, and by Corollary 57, (p) and (p') are in different components. So there are at least q^{t-1} components. □

6.4.3 Projections and lifts

The results presented in this subsection are rather technical. They will allow us to show in the following two subsections that equality of invariant vectors of two points of $D(k,q)$ implies that the points belong to the same component of $D(k,q)$. The proofs can be found in the original papers [101] for odd q, in [106] for even q, and, using the representation of $D(k,q)$ adopted in this survey, in [93].

For $k \geqslant 3$, 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 3.3, 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 60. ([101, 106]) *Let τ be an automorphism of $D(k,q)$, and let 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 61. ([101, 106]) *Let B be a component of $D(k,q)$. Then π_B is a t-to-1 graph homomorphism for some t, $1 \leqslant t \leqslant q$. In particular, let $k \equiv 0,\ 3 \pmod 4$, and suppose π_C is a t-to-1 mapping for some $t > 1$. Then $t = q$.*

Theorem 62. ([101, 106]) *The map $\pi_C : V(C) \to V(C')$ is surjective.*

6.4.4 Exact number of components of $D(k,q)$, $q \neq 4$

The proofs of the results of this subsection can be found in the original paper [101] for odd q, in [106] for even q, and using the representation of $D(k,q)$ adopted in this survey, in [93].

Theorem 63. ([101, 106]) *Let q be a prime power, $q \neq 4$, and $k \geqslant 6$. 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 from [101] that for $q \neq 4$, the 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 62, there is a $w \in V(C)$ 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 $k \geqslant 7$.

If $k \equiv 2 \pmod 4$, 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 $k \equiv 0, 1, 3 \pmod 4$, we show that π_C is a q-to-1 map. (In the case of $k \equiv 0, 3 \pmod 4$, 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 61). 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 one can proceed with these cases. Since the proof in the case $k \equiv 0 \pmod 4$ is more involved, we illustrate our approach with this case only.

Case $k \equiv 0 \pmod 4$. Write $k = 4j$ for $j \geqslant 2$. Let

$$(p') = (0, \ldots, 0, 1, 1, 0) \in V(D(k-1, q)).$$

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 that $y \neq 0$. 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 60. Since $y \neq 0$, and $b \neq 1$, (p') has two lifts to $D(k, q)$ in C.
Now suppose that $y = 0$, 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 60. Now let

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

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 60, all the vertices above are in $V(C)$. Hence (p') has two lifts to $D(k, q)$ in C.

Cases $k \equiv 1, 3 \pmod 4$ can be dealt with similarly, and the details can be found in the references. □

Theorem 64. ([106]) *Let q be a prime power with $q \neq 4$, and let $k \geqslant 2$ 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 63) that for $2 \leqslant k \leqslant 5$ 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 $k \geqslant 2$ and prime powers q, $D(k,q)$ is edge-transitive, hence all its components are isomorphic.

Let $k \geqslant 6$. Combining Theorems 58 and 63, 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 $r \geqslant 2$. For $3 \leqslant r \leqslant t$, 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 $2 \leqslant r \leqslant t$. 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

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

We will show that the invariant vector of a vertex characterizes the component containing the vertex. Let $C(x)$ be the component of $D(k,q)$ containing the vertex x.

Corollary 65. ([106]) *Let $k \geqslant 6$ and $q \neq 4$. Then $\vec{a}(u) = \vec{a}(v)$ if and only if $C(u) = C(v)$.*

Proof. Let $t = \lfloor \frac{k+2}{4} \rfloor$. Let X be the set of all components of $D(k,q)$ and we define the mapping $f : X \to \mathbb{F}_q^{t-1}$ via $f(C(v)) = \vec{a}(v)$. From Theorem 56, we know that f is well defined, i.e., $C(u) = C(v)$ implies $\vec{a}(u) = \vec{a}(v)$. By Theorem 64, $|X| = q^{t-1}$, so that f is bijective. Thus $C(u) = C(v)$ whenever $\vec{a}(u) = \vec{a}(v)$. $\square$

6.4.5 Exact number of components of $D(k,4)$

In order to deal with the case $q = 4$, we will need an analog of Theorem 63. 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 $u \in V(D(k,4))$, 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 $i \geqslant 2$ and

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

The following three theorems are analogs to Theorems 58, 63 and 64 for $q = 4$. Their proofs are similar to those, and can be found in [106], or, using the presentation of $D(k,q)$ adopted in this survey, in [93].

Theorem 66. ([106]) *Let u be in the component of $D(k,4)$ containing (0). Then*

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

Theorem 67. ([106]) *Let $k \geqslant 4$. If $v \in V(D(k,4))$ satisfies $\vec{b}(v) = \vec{0}$, then $v \in V(C)$.*

Similarly to the proof of Theorem 64, one can show the following result.

Theorem 68. ([106]) *Let $k \geqslant 4$ and $t = \lfloor \frac{k+2}{4} \rfloor$. Then $c(D(k,4)) = 4^t$ and $c(D(2,4)) = c(D(3,4)) = 1$.*

Remark 69. The analog of Corollary 65 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 $diam(CD(k,q))$ denote the diameter of the graph $CD(k,q)$. For small values of k and q, we have the following computational results, see [139, 152, 153].

(i) For $k = 2$, the diameter of $CD(2,q)$ is 4 for $3 \leqslant q \leqslant 49$.

(ii) For $k = 3$, the diameter of $CD(3,q)$ is 6 for $3 \leqslant q \leqslant 47$.

(iii) For $k \geqslant 4$, the diameter of $CD(k,q)$ is as follows, in which $[m,n]$ denotes the set of all integers i such that $m \leqslant i \leqslant n$.

k	4	5,6	5, 6	7	8	9,10	11,12
q	3,[5,23]	5	[7,13]	5,[7,9]	5,7	5	5
diameter	8	12	10	12	12	14	16

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

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 5: Diameter of $CD(k,3)$ 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

Table 6: Diameter of $CD(k,4)$ for small k

Conjecture 70. ([102]) There exists a positive constant c such that for all $k \geqslant 2$ and all prime powers q,

$$diam(CD(k,q)) \leqslant (\log_{q-1} q)k + c.$$

The following conjecture was stated in [139].

Conjecture 71. ([139]) 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 71 were proved in [139], 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, it is shown in [139] that for all odd $k \geqslant 5$ and all prime powers q, $diam(CD(k,q)) \geqslant k+3$. Then this bound was improved by [146]: for all prime powers $q \neq 4$, $diam(CD(k,q)) \geqslant k+5$ for odd $k \geqslant 5$, and $diam(CD(k,q)) \geqslant k+4$ for even $k \geqslant 4$.

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 [72] on such relations). It is known that for some (k,q), the graphs $D(k,q)$ are Ramanujan, i.e., they have $\lambda_2 \leqslant 2\sqrt{q-1}$. In particular, it is the case for $k=2,3$, see [111] or [34], where the whole spectrum was determined. However, Reichard [136] and Thomason [153] independently showed by computer that the graphs $D(4,q)$ are not Ramanujan for certain q. This implies that for the same q, the graphs $D(k,q)$ are not Ramanujan for $k \geqslant 4$, since the spectrum of $D(4,q)$ is embedded in that of $D(k,q)$, for $k \geqslant 4$. 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 $\lambda_2 > 2\sqrt{q-1}+1$. The following bound appears in Ustimenko [158] (see Moorhouse, Sun and Williford [124] for discussion and details).

Conjecture 72. (Ustimenko) For all (k,q), $CD(k,q)$ has second largest eigenvalue less than or equal to $2\sqrt{q}$.

For $k=4$, this conjecture was proven in [124], where the whole spectrum of the graph $D(4,q)$ was determined. For $k=5$ and odd q, the conjecture was proven by Gupta and Taranchuk [68]. Both papers [124] and [68] utilized group representations.

Problem 73. Determine a good upper bound of $\lambda_2(D(k,q))$ for $k \geqslant 7$, or find the spectrum of $D(k,q)$ for $k \geqslant 5$.

6.7 Graphs $B\Gamma_n$ and $CD(k,q)$ as iterated voltage lifts

Here we describe how one can view the graphs $B\Gamma_n = B\Gamma(R; f_2, \ldots, f_n)$ and $CD(k,q)$ as the result of iterated voltage lifts. The connection for $CD(k,q)$ was described in [53], and our presentation here is close to that in [53].

Let Γ be an undirected graph, with loops and multiple edges allowed. We replace each edge of Γ by a pair of oppositely directed arcs, and denote the resulting digraph by $\overrightarrow{\Gamma}$. If e is an arc, then e^{-1} will denote its reverse. If $D(\overrightarrow{\Gamma})$ is the set of all arcs of $\overrightarrow{\Gamma}$, then $|D(\overrightarrow{\Gamma})| = 2|E(\Gamma)|$.

For a finite group G, a mapping $\alpha : D(\overrightarrow{\Gamma}) \to G$ is called a *voltage assignment* on $\overrightarrow{\Gamma}$ if $\alpha(e^{-1}) = (\alpha(e))^{-1}$ for all $e \in D(\overrightarrow{\Gamma})$. Given a voltage assignment α, we denote the *voltage lift of* $\overrightarrow{\Gamma}$ *corresponding to* α as a digraph $\overrightarrow{\Gamma}^{\alpha}$ defined as follows.

The vertex set V of $\overrightarrow{\Gamma}^{\alpha}$ is the Cartesian product $V(\Gamma) \times G$, and the arc set is $D(\overrightarrow{\Gamma}) \times G$. Let e be an arc in $\overrightarrow{\Gamma}$ from vertex u to vertex v. We define the arc (e,g) in $\overrightarrow{\Gamma}^{\alpha}$ to have initial vertex (u,g) and terminal vertex $(v, g\alpha(e))$. By the definition of voltage assignments, arc (e^{-1}, g^{-1}) in $\overrightarrow{\Gamma}^{\alpha}$ has initial vertex $(v, g\alpha(e))$ and terminal vertex (u,g). Replacing each of these pairs of arcs with an undirected edge joining u and v, we obtain an undirected graph that we denote by Γ^{α} and call the *voltage lift of* Γ *corresponding to* α.

Now we explain how the graph $B\Gamma_n = B\Gamma(R; f_2, \ldots, f_n)$ can be viewed as a voltage lift of $B\Gamma_{n-1} = B\Gamma(R; f_2, \ldots, f_{n-1})$. For this, we define a voltage assignment α so that $B\Gamma_n = B\Gamma_{n-1}^{\alpha}$. Let $G = (R, +)$ be the additive group of the ring R with $|R| = r$, and let us define $B\Gamma_1$ to be the complete bipartite graph $K_{r,r}$. Vertices in one partition can be denoted by (p_1) (points) and in the other one by $[l_1]$ (lines), where all distinct p_1 and all distinct l_1 range over G. We can view vectors $(a_1, a_2, \ldots, a_{k-1}, a_k) \in R^k$ as ordered pairs $((a_1, a_2, \ldots, a_{n-1}), a_n) \in R^{n-1} \times G$. If $(p_1, p_2, \ldots, p_{n-1})$ and $[l_1, l_2, \ldots, l_{n-1}]$ form an edge e in $B\Gamma_{n-1}$, and $\alpha(e)$ is defined as $f_k(p_1, \ldots, p_{n-1}, l_1, \ldots l_{n-1})$, then $(p_1, p_2, \ldots, p_{n-1}, p_n)$ and $[l_1, l_2, \ldots, l_{n-1}, l_n]$ form an edge in $B\Gamma_n$.

Now we explain how the graph $CD(k,q)$ can be viewed as a voltage lift of $CD(k-1,q)$. Let $G = (\mathbb{F}_q, +)$ be the additive group of the field $\mathbb{F}_q$, and let us define $CD(1,q)$ to be the complete bipartite graph $K_{q,q}$. By the argument above, we conclude that if $2 \leqslant k \neq 4n+2$, $n \geqslant 1$, then $CD(k,q)$ is a voltage lift of $CD(k-1,q)$. If $k = 4n+2 \geqslant 6$, then we know that $D(k,q)$ has q times more components than $D(k-1,q)$. Each is denoted by $CD(k,q)$ and is isomorphic to $CD(k-1,q)$.

Theorem 74. ([53]) Let $2 \leqslant k \neq 4n+2, n \geqslant 2$, and let q be a prime power. For $\Gamma = CD(k-1,q)$, there exists a voltage assignment $\alpha : D(\overrightarrow{\Gamma}) \to (\mathbb{F}_q, +)$ such that the lifted graph Γ^{α} is isomorphic to $CD(k,q)$.

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 $r, s, t \geqslant 2$, do (r, s, t)-graphs exist? Trivially, $(r, s, 2)$-graphs exist for all $r, s \geqslant 2$; indeed, these are the complete bipartite graphs. For all $r, t \geqslant 2$, Sachs [138] and Erdős and Sachs [52] 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.

By explicit construction, (r, s, t)-graphs exist for all $r, s, t \geqslant 2$, see [60]. The results can be viewed as biregular versions of the results from [138] and [52]. The paper [60] contains two constructions: a *recursive* one and an *algebraic* one. The recursive construction establishes existence for all $r, s, t \geqslant 2$, but the algebraic method works only for $r, s \geqslant t$. 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 $r \geqslant r' \geqslant t \geqslant 3$ and $s \geqslant s' \geqslant t \geqslant 3$, Γ contains an (r', s', t)-graph Γ' as an induced subgraph.

7.2 Cages

Let $k \geqslant 2$ and $g \geqslant 3$ 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 survey on cages, we refer the reader to Exoo and Jajcay [54].

In [102], Lazebnik, Ustimenko and Woldar established general upper bounds for $\nu(k, g)$ which are roughly the $3/2$ power of the lower bounds (the previous results had upper bounds roughly equal to the squares of the lower bounds), and provided explicit constructions for such (k, g)-graphs. The main ingredients of their construction were the graphs $CD(n, q)$ and certain induced subgraphs of these, manufactured by the method described in Section 3.2. The precise result follows.

Theorem 75. ([102]) Let $k \geqslant 2$ and $g \geqslant 5$ be integers, and let q denote the smallest odd prime power for which $k \leqslant q$. Then

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

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

7.3 Structure of extremal graphs of large girth

Let $n \geqslant 3$, 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 [107], Lazebnik and Wang present several results where this question is answered affirmatively, see also Garnick and Nieuwejaar [65]. In particular, this is always the case when ν is large compared to n: $\nu \geqslant 2^{a^2+a+1}n^a$, where $a = n - 3 - \lfloor \frac{n-2}{4} \rfloor$, $n \geqslant 12$. To obtain this result they used certain generic properties of extremal graphs, as well as of the graphs $CD(k, q)$.

8 Applications to coding theory and cryptography

Graphs with many edges and without short cycles have been used in coding theory in the construction and analysis of Low-Density Parity-Check (LDPC) codes, see, e.g., Kim, Peled, Pless and Perepelitsa [76], Kim, Peled, Pless, Perepelitsa and Friedland [77], Kim, Mellinger and Storme [75], Sin and Xiang [144], Pradhan, Thangaraj and Subramanian [134]. For the last sixteen years, 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 [78], Wróblewska and Ustimenko [177] and Ustimenko [162].

Chojecki, Erskine, Tuite and Ustimenko [32] gave graph constructions similar to $D(k, q)$, presented many computational results concerning their parameters, stated several conjectures, and mentioned possible applications of these graphs and related groups to LDPC codes, noncommutative cryptography and stream ciphers design.

Acknowledgements

The authors are grateful to Shuying Sun for helpful discussions, and to Grahame Erskine, Alex Kodess, Brian Kronenthal, Meng Liu, Ben Nassau, Vladislav Taranchuk, James Tuite and Jason Williford for valuable suggestions. We also are indebted to the editors and to the referees whose comments greatly improved this survey. This work was partially supported by NSFC (#12471323, Ye Wang).

References

[1] E. Abajo and A. Diánez, Graphs with maximum size and lower bounded girth, *Appl. Math. Lett.*, **25** (2012) 575–579.

[2] J. Alexander, Selected results in combinatorics and graph theory, Ph. D. thesis, University of Delaware, 2016.

[3] P. Allen, P. Keevash, B. Sudakov, and J. Verstraëte, Turán numbers of bipartite graphs plus an odd cycle, *J. Combin. Theory Ser. B*, **106** (2014) 134–162.

[4] N. Alon, S. Hoory, and N. Linial, Moore bound for irregular graphs, *Graphs Combin.*, **18**(1) (2002) 53–57.

[5] L. Babai, Spectra of Cayley graphs, *J. Combin. Theory Ser. B*, **18** (1979) 180–189.

[6] D. Bartoli and M. Bonini, More on the DLW conjectures, *Finite Fields Appl.*, **93** (2024) 102332.

[7] T. Bending and D. Fon-Der-Flaass, Crooked functions, bent functions, and distance regular graphs, *Electron. J. Combin.*, **5** (1998) #R34.

[8] C. T. Benson, Generalized quadrangles and (B, N) pairs, Ph. D. thesis, Cornel University, 1965.

[9] C. T. Benson, Minimal regular graphs of girths eight and twelve, *Canad. J. Math.*, **18** (1966) 1091–1094.

[10] C. Berge, *Hypergraphs, Combinatorics of Finite Sets*, North–Holland, Amsterdam, 1989.

[11] C. Berge, Hypergraphs, in *Selected Topics in Graph Theory 3*, edited by Lowell W. Beineke and Robin J. Wilson, Academic Press Limited, (1998) 189–207.

[12] J. Bierbrauer and G. Kyureghyan, Crooked binomials, *Des. Codes Cryptogr.*, **46** (2008) 269–301.

[13] N. Biggs, *Algebraic Graph Theory*, Cambridge University Press, Cambridge, 1974.

[14] B. Bollobás, *Extremal Graph Theory*, Academic Press, London, 1978.

[15] B. Bollobás, *Modern Graph Theory*, Springer-Verlag New York Inc., 1998.

[16] J. A. Bondy and M. Simonovits, Cycles of even length in graphs, *J. Combin. Theory Ser. B*, **16** (1974) 97–105.

[17] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-Regular Graphs*, Springer-Verlag, Berlin, 1989.

[18] B. Bukh and Z. Jiang, A bound on the number of edges in graphs without an even cycle, *Combin. Probab. Comput.*, **26** (2017) 1–15.

[19] J. Byrne and M. Tait, Improved upper bounds on even-cycle creating Hamilton paths, *Discrete Math.*, **347** (2024) 114107.

[20] D. de Caen and E. R. van Dam, Association schemes related to Kasami codes and Kerdock sets, *Des. Codes Cryptogr.*, **18** (1999) 89–102.

[21] D. de Caen, R. Mathon, and G. E. Moorhouse, A family of antipodal distance-regular graphs related to the classical Preparata codes, *J. Algebraic Combin.*, **4** (1995) 317–327.

[22] 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.

[23] X. Cao, M. Lu, D. Wan, L. -P. Wang, and Q. Wang, Linearized Wenger graphs, *Discrete Math.*, **338** (2015) 1595–1602.

[24] P. Cara, S. Rottey, and G. Van de Voorde, A construction for infinite families of semisymmetric graphs revealing their full automorphism group, *J. Algebraic Combin.* **39** (2014) 967–988.

[25] C. Carlet, *B*oolean Functions for Cryptography and Coding Theory, Cambridge University Press, Cambridge, 2020.

[26] D. B. Chandler, Private communication, 2005.

[27] X. Cheng, W. Chen, and Y. Tang, On the girth of the bipartite graph $D(k, q)$, *Discrete Math.*, **335** (2014) 25–34.

[28] X. Cheng, W. Chen, and Y. Tang, On the conjecture for the girth of the bipartite graph $D(k, q)$, *Discrete Math.*, **339** (2016) 2384–2392.

[29] W. Cherowitzo, α-Flocks and hyperovals, *Geom. Dedicata*, **72** (1998) 221–246.

[30] W. Cherowitzo, C. M. O'Keefe, and T. Penttila, A unified construction of finite geometries associated with q-clans in characteristic two, *Adv. Geom.*, **3** (2003) 1–21.

[31] W. Cherowitzo, T. Penttila, I. Pinneri, and G. F. Royle, Flocks and ovals, *Geom. Dedicata*, **60** (1996) 17–37.

[32] T. Chojecki, G. Erskine, J. Tuite, V. Ustimenko, On affine forestry over integral domains and families of deep Jordan-Gauss graphs, *European J. Combin.*, **11** (2025) 10.

[33] 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.

[34] S. M. Cioabă, F. Lazebnik, and W. Li, On the spectrum of Wenger graphs, *J. Combin. Theory Ser. B*, **107** (2014) 132–139.

[35] S. M. Cioabă, F. Lazebnik, and S. Sun, Spectral and combinatorial properties of some algebraically defined graphs, *Electron. J. Combin.*, **25**(4) (2018) #P4.60, 1–16.

[36] R. S. Coulter and M. Henderson, A class of functions and their application in constructing semi-biplanes and association schemes, *Discrete Math.*, **202** (1999) 21–31.

[37] R. S. Coulter, S. De Winter, A. Kodess, and F. Lazebnik, A result on polynomials derived via graph theory, *Math. Mag.*, **92** (2019) 288–295.

[38] D. M. Cvetković, M. Doob, and H. Sachs, *Spectra of Graphs – Theory and Application*, Deutscher Verlag der Wissenschaften, Berlin, Academic Press, New York, 1980.

[39] E. R. van Dam and D. Fon-Der-Flaass, Uniformly packed codes and more distance regular graphs from CR functions, *J. Algebr. Comb.*, **12** (2000) 115–121.

[40] E. R. van Dam and D. Fon-Der-Flaass, Codes, graphs, and schemes from nonlinear functions, *European J. Combin.*, **24** (2003) 85–98.

[41] E. R. van Dam, J. H. Koolen, and H. Tanaka, Distance-regular graphs, *Electron. J. Combin.*, (2016) #DS22.

[42] A. Devillers, N. Kamčev, B. D. McKay, P. Ó. Catháin, G. Royle, G. Van de Voorde, I. M. Wanless, and D. R. Wood, Triangle-free graphs with diameter 2, Matrix Annals, pp. 693–709. Springer, 2025.

[43] V. Dmytrenko, Classes of polynomial graphs, Ph. D. thesis, University of Delaware, 2004.

[44] V. Dmytrenko, F. Lazebnik, and R. Viglione, Isomorphism criterion for monomial graphs, *J. Graph Theory*, **48** (2005) 322–328.

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

[46] P. Duchet, *Hypergraphs*, Handbook of Combinatorics, Volume 1, North–Holland, Amsterdam, 1985.

[47] B. Düzgün, A. Riet, and V. Taranchuk, New constructions of unbalanced $\{C_4, \theta_{3,t}\}$-free bipartite graphs, Proceedings of the 13th European Conference on Combinatorics, Graph Theory and Applications EUROCOMB'25, Budapest, 2025, 383–388.

[48] S. Eberhard, V. Taranchuk, C. Timmons, Examples of diameter-2 graphs with no triangles or $K_{2,t}$, Australas. J. Combin., to appear.

[49] P. Erdős, Extremal problems in graph theory, Theory of Graphs and its Applications, (M. Fiedler ed.) (*Proc. Symp. Smolenice, 1963*), Academic Press, New York (1965) 29–36.

[50] P. Erdős, Some recent progress on extremal problems in graph theory, *Congr. Numer.*, **14** (1975) 3–14.

[51] 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.

[52] 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.

[53] G. Erskine, Diameter, girth, and other properties of highly symmetric graphs, Ph. D. thesis, The Open University, 2017.

[54] J. Exoo and R. Jajcay, Dynamic Cage Survey, *Electron. J. Combin.*, Dynamic Survey #DS16 (2013) 1–55.

[55] R. J. Faudree and M. Simonovits, On a class of degenerate extremal graph problems, *Combinatorica*, **3**(1) (1983) 83–93.

[56] W. Feit and G. Higman, The nonexistence of certain generalized polygons, *J. Algebra*, **1** (1964) 114–131.

[57] Z. Füredi, Turán Type Problems, Surveys in Combinatorics, Cambridge University Press, Cambridge, 1991.

[58] Z. Füredi, On the number of edges of quadrilateral-free graphs, *J. Combin. Theory Ser. B*, **68**(1) (1996) 1–6.

[59] Z. Füredi, Private communication, 1996.

[60] 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.

[61] Z. Füredi, A. Naor, and J. Verstraëte, On the Turán number for the hexagon, *Adv. Math.*, **203** (2006) 476–496.

[62] 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.

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

[64] A. J. Ganger, S. N. Golden, B. G. Kronenthal, and C. A. Lyons, On the girth of two-dimensional real algebraically defined graphs, *Discrete Math.*, **342** (2019) 2834–2842.

[65] 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.

[66] 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.

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

[68] H. Gupta and V. Taranchuk, On the eigenvalues of graphs $D(5,q)$, *Finite Fields Appl.*, **94** (2024) 102358.

[69] G. Harcos and D. Soltész, New bounds on even cycle creating hamiltonian paths using expander graphs, *Combinatorica*, **40**(3) (2020) 435–454.

[70] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford University Press, Oxford, 1998.

[71] S. Hoory, The size of bipartite graphs with a given girth, *J. Comb. Theory Ser. B*, **86**(2) (2002) 215–220.

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

[73] X. -D. Hou, On the DLW conjectures, *J. Number Theory*, **187** (2018) 288–295.

[74] X. -D. Hou, S. D. Lappano, and F. Lazebnik, Proof of a conjecture on monomial graphs, *Finite Fields Appl.*, **43** (2017) 42–68.

[75] 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.

[76] 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.

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

[78] 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.

[79] A. Kodess, Properties of some algebraically defined digraphs, Ph. D. thesis, University of Delaware, 2014.

[80] A. Kodess, B. G. Kronenthal, D. Manzano-Ruiz, and E. Noe, Classification by girth of three-dimensional algebraically defined monomial graphs over the real numbers, *Discrete Math.*, **344** (2021) 112286.

[81] A. Kodess, B. G. Kronenthal, and T. W. H. Wong, On the girth of three-dimensional algebraically defined graphs with multiplicatively separable functions, *Electron. J. Combin.*, **29**(4) (2022) #P4.21, 1–16.

[82] A. Kodess and F. Lazebnik, Connectivity of some algebraically defined digraphs, *Electron. J. Combin.*, **22**(3) (2015) #P3.27, 1–11.

[83] A. Kodess and F. Lazebnik, A note on the isomorphism problem for monomial digraphs, *J. Interconnect. Netw.*, **17** (2017) 1741006.

[84] 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.

[85] T. Kővári, V. T. Sós, and P. Turán, On a problem of K. Zarankiewicz, *Colloq. Math.*, **3** (1954) 50–57.

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

[87] B. G. Kronenthal and F. Lazebnik, On the uniqueness of some girth eight algebraically defined graphs, *Discrete Appl. Math.*, **206** (2016) 188–194.

[88] B. G. Kronenthal, F. Lazebnik, and J. Williford, On the uniqueness of some girth eight algebraically defined graphs, Part II, *Discrete Appl. Math.*, **254** (2019) 161–170.

[89] B. G. Kronenthal, J. Miller, A. Nash, J. Roeder, H. Samamah, and T. W. H. Wong, Nonisomorphic two-dimensional algebraically defined graphs over $\mathbb{R}$, *J. Graph Theory*, **108** (2025) 50–64.

[90] G. Kyureghyan, The only crooked power functions are $x^{2^k+2^l}$, *European J. Combin.*, **28** (2007) 1345–1350.

[91] G. Kyureghyan, Crooked maps in $\mathbb{F}_{2^n}$, *Finite Fields Appl.*, **13** (2007) 713–726.

[92] F. Lazebnik and D. Mubayi, New lower bounds for Ramsey numbers of graphs and hypergraphs, *Adv. Appl. Math.*, **28**(3/4) (2002) 544–559.

[93] F. Lazebnik, S. Sun, and Y. Wang, Some families of graphs, hypergraphs and digraphs defined by systems of equations: a survey, *Lect. Notes Semin. Interdiscip. Mat.*, **14** (2017) 105–142.

[94] F. Lazebnik and V. Taranchuk, A new family of algebraically defined graphs with small automorphism group, *Electron. J. Combin.*, **29**(1) (2022) #P1.43, 1–20.

[95] F. Lazebnik and A. Thomason, Orthomorphisms and the construction of projective planes, *Math. Comp.*, **73**(247) (2004) 1547–1557.

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

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

[98] F. Lazebnik, V. A. Ustimenko, and 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.

[99] 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.

[100] F. Lazebnik, V. A. Ustimenko, and A. J. Woldar, A new series of dense graphs of high girth, *Bull. Amer. Math. Soc.*, **32**(1) (1995) 73–79.

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

[102] F. Lazebnik, V. A. Ustimenko, and A. J. Woldar, New upper bounds on the order of cages, *Electron. J. Combin.*, **14**:#R13, (1997).

[103] F. Lazebnik, V. A. Ustimenko, and A. J. Woldar, Polarities and $2k$-cycle-free graphs, *Discrete Math.*, **197/198** (1999) 503–513.

[104] F. Lazebnik and J. Verstraëte, On hypergraphs of girth five, *Electron. J. Combin.*, **10**:#P25 (2003) 1–15.

[105] F. Lazebnik and R. Viglione, An infinite series of regular edge- but not vertex-transitive graphs, *J. Graph Theory*, **41** (2002) 249–258.

[106] F. Lazebnik and R. Viglione, On the connectivity of certain graphs of high girth, *Discrete Math.*, **277** (2004) 309–319.

[107] F. Lazebnik and P. Wang, On the extremal graphs of high girth, *J. Graph Theory*, **26** (1997) 147–153.

[108] 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.

[109] 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.

[110] K. Li and N. Kaleyski, Two new infinite families of APN functions in trivariate form, *IEEE Trans. Inform. Theory*, **70**(2) (2024) 1436–1452.

[111] 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.

[112] Y. Li and K. -W. Lih, Multi-color Ramsey numbers of even cycles, *European Journal of Combinatorics*, **30** (2009) 114–118.

[113] M. Liu and Y. Wang, Polynomial resultants and Ramsey numbers of a theta graph, *Adv. Appl. Math.*, **167** (2025) 102881.

[114] L. Lovász, Spectra of graphs with transitive groups, *Period. Math. Hungar.*, **6** (1975) 191–195.

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

[116] Z. Lv, M. Lu, and C. Fang, A note on 3-partite graphs without 4-cycles, *Des. Codes Cryptogr.*, **28** (2020) 753–757.

[117] Z. Lv, M. Lu, and C. Fang, Density of balanced 3-partite graphs without 3-cycles or 4-cycles, *Electron. J. Combin.*, **29**(4) (2022) #P4.44.

[118] J. Ma and T. Yang, On extremal numbers of the triangle plus the four-cycle, *Forum Math. Sigma*, **13** (2025) e154.

[119] G. A. Margulis, Explicit group-theoretical construction of combinatorial schemes and their application to design of expandors and concentrators, *Probl. Inf. Transm.*, **24** (1988) 39–46 (translation from Problemy Peredachi Informatsii **24**(1) January-March 1988, 51–60.)

[120] D. Marker, *Model Theory: An Introduction (Graduate Texts in Mathematics, vol. 217)*, Springer-Verlag, New York, 2002.

[121] M. E. Mellinger and D. Mubayi, Constructions of bipartite graphs from finite geometries, *J. Graph Theory*, **49** (2005) 1–10.

[122] S. Mesnager, Bent vectorial functions and linear codes from o-polynomials, *Des Codes Cryptogr.*, **77** (2015) 99–116.

[123] M. Mirzaei, A. Suk, and J. Verstraëte, Constructions of point-line arrangements in the plane with large girth, arXiv:1911.11713, 2019.

[124] G. E. Moorhouse, S. Sun, and J. Williford, The eigenvalues of the graphs $D(4, q)$, *J. Combin. Theory Ser. B*, **125** (2017) 1–20.

[125] S. Mukherjee, Extremal numbers of hypergraph suspensions of even cycles, *European J. Combin.*, **118** (2024) 103935.

[126] B. Nassau, Studies of some classes of algebraically defined graphs, Ph. D. thesis, University of Delaware, 2020.

[127] I. Neuwirth, The size of bipartite graphs with girth eight, arXiv:math/0102210, 2001.

[128] K. Nyberg and L. R. Knudsen, Provable security against a differential attack, *J. Cryptol.*, **8**(1) (1995) 27–37.

[129] S. E. Payne, Affine representations of generalized quadrangles, *J. Algebra*, **16** (1970) 473–485.

[130] S. E. Payne, A new infinite family of generalized quadrangles, *Congr. Numer.*, **49** (1985) 115–128.

[131] 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.

[132] O. Pikhurko, A note on the Turán function of even cycles, *Proc. Amer. Math. Soc.*, **140**(11) (2012) 3687–3692.

[133] M. B. Porter, Extended Wenger graphs, Ph. D. thesis, University of California, Irvine, 2018.

[134] A. K. Pradhan, A. Thangaraj, and A. Subramanian, Construction of near-capacity protograph LDPC code sequences with block-error thresholds, *IEEE Trans. Commun.*, **64** (2016) 27–37.

[135] S. P. Radziszowski, Small Ramsey numbers, *Electron. J. Combin.*, **1** #DS1 (2024) 1–133.

[136] S. Reichard, Private communication, 2001.

[137] I. Reiman, Uber ein Problem von K. Zarankiewicz, *Acta Math. Acad. Sci. Hungar.*, **9** (1958) 269–273.

[138] H. Sachs, Regular graphs with given girth and restricted circuits, *J. Lond. Math. Soc.*, **38** (1963) 423–429.

[139] A. Schliep, GADAR and its application to extremal graph theory, Master's thesis, University of Delaware, 1994.

[140] B. Segre, Sui k-archi nei piani finiti di caratteristica 2, *Rev. Math. Pures Appl.*, **2** (1957) 289–300.

[141] B. Segre, Ovali e curve σ nei piani di Galois di caratteristica due, *Atti Accad. Naz. Lincei Rend.*, **8** (1962) 785–790.

[142] B. Segre and U. Bartocci, Ovali ed altre curve nei piani di Galois di caratteristica due, *Acta Arith.*, **18** (1971) 423–449.

[143] 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. Ser.*, **24** (2008) 281–288.

[144] 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.

[145] D. Soltész, Even cycle creating paths, *J. Graph Theory*, **93** (2020) 350–362.

[146] S. Sun, On some families of algebraically defined graphs, Ph.D. thesis, University of Delaware, 2017.

[147] V. Taranchuk, A simple proof for the lower bound of the girth of graphs $D(n, q)$, *Discrete Math.*, **347** (2024) 113705.

[148] V. Taranchuk, Private communication, 2024.

[149] V. Taranchuk, Private communication, 2026.

[150] T. A. Terlep and J. Williford, Graphs from generalized Kac-Moody algebras, *SIAM J. Discrete Math.*, **26**(3) (2012) 1112–1120.

[151] J. A. Thas, *Generalized Polygons*, Handbook of Incidence Geometry, Edited by F. Buekenhout, Elsevier Science, 1995.

[152] A. Thomason, Private communication, 1997.

[153] A. Thomason, Private communication, 2002.

[154] 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.

[155] 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.

[156] 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.

[157] V. A. Ustimenko, Coordinatisation of 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.

[158] V. A. Ustimenko, On group theoretical construction of expanding graphs, *Algebra Discrete Math.*, **3** (2003) 102–109.

[159] V. A. Ustimenko, Maximality of affine group and hidden graph cryptosystems, *Algebra Discrete Math.*, **10** (2004) 51–65.

[160] V. A. Ustimenko, On linguistic dynamical systems, families of graphs of large girth, and cryptography, *J. Math. Sci.*, **140** (2007) 461–471.

[161] V. A. Ustimenko, On the extremal graph theory and symbolic computations, *Rep. Natl. Acad. Sci. Ukr.*, **2** (2013) 42–49 (in Russian).

[162] V. A. Ustimenko, On the flag geometry of simple group of Lie type and multivariate cryptography, *Algebra Discrete Math.*, **19**(1) (2015) 130–144.

[163] V. A. Ustimenko and A. J. Woldar, Extremal properties of regular and affine generalized polygons as tactical configurations, *European J. Combin.*, **23** (2003) 99–111.

[164] H. Van Maldeghem, *Generalized Polygons*, Monographs in Mathematics **93**, Birkh user Verlag, Basel, 1998.

[165] J. Verstraëte, On arithmetic progressions of cycle lengths in graphs, *Combin. Probab. Comput.*, **9** (2000) 369–373.

[166] J. Verstraëte and J. Williford, Graphs without theta subgraphs, *J. Combin. Theory Ser. B*, **134** (2019) 76–87.

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

[168] R. Viglione, On the diameter of Wenger graphs, *Acta Appl. Math.*, **104** (2008) 173–176.

[169] L. -P. Wang, D. Wan, W. Wang, and H. Zhou, On jumped Wenger graphs, *Commun. Math. Res.*, **38**(2) (2022) 319–332.

[170] Y. Wang, On some cycles in linearized Wenger graphs, *Discrete Math.*, **340**(12) (2017) 2782–2788.

[171] Y. Wang, F. Lazebnik, and A. Thomason, On some cycles in Wenger graphs, *Acta Math. Appl. Sin. Engl. Ser.*, **36** (2020) 492–502.

[172] M. E. Watkins, Connectivity of transitive graphs, *J. Combin. Theory*, **8** (1970) 23–29.

[173] R. Wenger, Extremal graphs with no C^4, C^6, or C^{10}'s, *J. Combin. Theory Ser. B*, **52** (1991) 113–116.

[174] J. Williford, Private communication, 2012.

[175] A. J. Woldar, Rainbow graphs, Proceedings 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.

[176] A. J. Woldar, On generalizing generalized polygons, *Innov. Incidence Geom.*, **10** (2010) 147–170.

[177] A. Wróblewska and V. Ustimenko, On new examples of families of multivariate stable maps and their cryptographical applications, *Ann. Univ. Mariae Curie-Skłodowska Sect. AI Informatica* **14**(1) (2014) 19–36.

[178] M. Xu, On the study of two classes of algebraic bipartite graphs defined by systems of equations, Ph. D. thesis, Yangzhou University, 2023.

[179] M. Xu, X. Cheng, and Y. Tang, On the characterization of some algebraically defined bipartite graphs of girth eight, *Discrete Appl. Math.*, **305** (2021) 221–232.

[180] M. Xu, X. Cheng, and Y. Tang, On the girth cycles of the bipartite graph $D(k, q)$, *Discrete Math.*, **346** (2023) 113500.

[181] M. Xu, X. Cheng, and Y. Tang, Girth of the algebraic bipartite graph $D(k, q)$, *Finite Fields Appl.*, **92** (2023) 102296.

[182] H. Yan and C. Liu, A note on the spectrum of linearized Wenger graphs, *Discrete Math.*, **340** (2017) 1050-1053.

[183] F. Yang, Q. Sun, and C. Zhang, Semisymmetric graphs defined by finite-dimensional generalized Kac-Moody algebras, *Bull. Malays. Math. Sci. Soc.*, **45** (2022) 3293–3305.

Appendix: Girth of $D(k, q)$

The known values of girth of $D(k, q)$ for $2 \leqslant k \leqslant 100$ and $4 \leqslant q \leqslant 97$ are shown in Tables 7-13. They are proven either by computer or Theorems 48-55, and empty cells correspond to the cases where the girth is unknown.

q \ k	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
4	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
5	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
7	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
8	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
9	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
11	6	8	8	10	10	12	12			16	16	18	18	20	20
13	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
16	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
17	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
19	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
23	6	8	8	10	10	12	12			16	16	18	18	20	20
25	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
27	6	8	8	10	10	12	12			16	16	18	18	20	20
29	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
31	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
32	6	8	8	10	10	12	12			16	16	18	18	20	20
37	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
41	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
43	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
47	6	8	8	10	10	12	12			16	16	18	18	20	20
49	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
53	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
59	6	8	8	10	10	12	12			16	16	18	18	20	20
61	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
64	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
67	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
71	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
73	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
79	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
81	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
83	6	8	8	10	10	12	12			16	16	18	18	20	20
89	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20
97	6	8	8	10	10	12	12	14	14	16	16	18	18	20	20

Table 7: Girth of $D(k, q)$ for $2 \leqslant k \leqslant 16$ and $4 \leqslant q \leqslant 97$

q \ k	17	18	19	20	21	22	23	24	25	26	27	28	29	30
4	22	22	24	24	26	26	28	28			32	32		
5	22	22	24	24	26	26	28	28			32	32		
7	22	22	24	24	26	26	28	28			32	32		
8	22	22	24	24	26	26	28	28			32	32		
9	22	22	24	24	26	26	28	28	30	30	32	32		
11	22	22	24	24	26	26	28	28			32	32		
13	22	22	24	24	26	26	28	28			32	32		
16	22	22	24	24	26	26	28	28	30	30	32	32		
17	22	22	24	24			28	28			32	32	34	34
19	22	22	24	24			28	28			32	32		
23	22	22	24	24			28	28			32	32		
25	22	22	24	24	26	26	28	28	30	30	32	32		
27	22	22	24	24	26	26	28	28	30	30	32	32		
29	22	22	24	24			28	28			32	32		
31			24	24			28	28	30	30	32	32		
32	22	22	24	24			28	28			32	32		
37			24	24			28	28			32	32		
41			24	24			28	28			32	32		
43			24	24			28	28			32	32		
47			24	24			28	28			32	32		
49	22	22	24	24	26	26	28	28			32	32		
53			24	24	26	26	28	28			32	32		
59			24	24			28	28			32	32		
61			24	24			28	28	30	30	32	32		
64	22	22	24	24	26	26	28	28			32	32		
67	22	22	24	24			28	28			32	32		
71			24	24			28	28			32	32		
73			24	24			28	28			32	32		
79			24	24	26	26	28	28			32	32		
81	22	22	24	24	26	26	28	28	30	30	32	32		
83			24	24			28	28			32	32		
89	22	22	24	24			28	28			32	32		
97			24	24			28	28			32	32		

Table 8: Girth of $D(k,q)$ for $17 \leqslant k \leqslant 30$ and $4 \leqslant q \leqslant 97$

q \ k	31	32	33	34	35	36	37	38	39	40	41	42	43	44
4	36	36			40	40			44	44			48	48
5	36	36			40	40			44	44			48	48
7	36	36			40	40	42	42	44	44			48	48
8	36	36			40	40			44	44			48	48
9	36	36			40	40	42	42	44	44			48	48
11	36	36			40	40			44	44			48	48
13	36	36			40	40			44	44			48	48
16	36	36			40	40			44	44			48	48
17	36	36			40	40			44	44			48	48
19	36	36	38	38	40	40			44	44			48	48
23	36	36			40	40			44	44	46	46	48	48
25	36	36			40	40			44	44			48	48
27	36	36			40	40			44	44			48	48
29	36	36			40	40			44	44			48	48
31	36	36			40	40							48	48
32	36	36			40	40			44	44			48	48
37	36	36			40	40							48	48
41	36	36			40	40							48	48
43	36	36			40	40	42	42					48	48
47	36	36			40	40					46	46	48	48
49	36	36			40	40	42	42	44	44			48	48
53	36	36			40	40							48	48
59	36	36			40	40							48	48
61	36	36			40	40							48	48
64	36	36			40	40	42	42	44	44			48	48
67	36	36			40	40			44	44			48	48
71	36	36			40	40							48	48
73	36	36			40	40							48	48
79	36	36			40	40							48	48
81	36	36			40	40	42	42	44	44			48	48
83	36	36			40	40							48	48
89	36	36			40	40			44	44			48	48
97	36	36			40	40							48	48

Table 9: Girth of $D(k,q)$ for $31 \leqslant k \leqslant 44$ and $4 \leqslant q \leqslant 97$

q \ k	45	46	47	48	49	50	51	52	53	54	55	56	57	58
4			52	52			56	56						
5	50	50	52	52			56				60	60		
7			52	52			56	56						
8			52	52			56	56						
9			52	52	54	54	56				60	60		
11			52	52			56							
13			52	52			56							
16			52	52			56				60	60		
17							56							
19							56							
23							56							
25	50	50	52	52			56				60	60		
27			52	52	54	54	56				60	60		
29							56	56	58	58				
31							56				60	60	62	62
32							56						62	62
37							56							
41							56							
43							56	56						
47							56							
49			52	52			56	56						
53			52	52			56							
59							56		58	58				
61							56				60	60		
64			52	52			56	56						
67							56							
71							56	56						
73							56							
79			52	52			56							
81			52	52	54	54	56				60	60		
83							56							
89							56							
97							56							

Table 10: Girth of $D(k,q)$ for $45 \leqslant k \leqslant 58$ and $4 \leqslant q \leqslant 97$

q \ k	59	60	61	62	63	64	65	66	67	68	69	70	71	72
4	64	64							72	72				
5	64	64					70	70	72					
7	64	64					70	70	72					
8	64	64							72					
9	64	64							72	72				
11	64	64							72					
13	64	64							72					
16	64	64							72					
17	64	64			68	68			72					
19	64	64							72				76	76
23	64	64							72					
25	64	64					70	70	72					
27	64	64							72	72				
29	64	64							72					
31	64	64							72					
32	64	64							72					
37	64	64							72	72	74	74		
41	64	64							72					
43	64	64							72					
47	64	64							72					
49	64	64					70	70	72					
53	64	64							72					
59	64	64							72					
61	64	64							72					
64	64	64							72	72				
67	64	64	66	66					72					
71	64	64					70	70	72					
73	64	64							72	72				
79	64	64							72					
81	64	64							72	72				
83	64	64							72					
89	64	64							72					
97	64	64							72					

Table 11: Girth of $D(k,q)$ for $59 \leqslant k \leqslant 72$ and $4 \leqslant q \leqslant 97$

q \ k	73	74	75	76	77	78	79	80	81	82	83	84	85	86
4			80	80							88		90	90
5			80	80							88		90	90
7			80				84	84			88		90	90
8			80	80							88		90	90
9			80				84	84			88		90	90
11			80								88	88	90	90
13	78	78	80								88		90	90
16			80	80							88		90	90
17			80								88		90	90
19			80								88		90	90
23			80								88		90	90
25			80	80							88		90	90
27	78	78	80								88		90	90
29			80								88		90	90
31			80										90	90
32			80	80							88		90	90
37			80										90	90
41			80	80	82	82							90	90
43			80				84	84	86	86			90	90
47			80										90	90
49			80				84	84			88		90	90
53			80										90	90
59			80										90	90
61			80										90	90
64			80	80			84	84			88		90	90
67			80								88		90	90
71			80										90	90
73			80										90	90
79	78	78	80										90	90
81			80	80			84	84			88		90	90
83			80		82	82							90	90
89			80								88	88	90	90
97			80										90	90

Table 12: Girth of $D(k, q)$ for $73 \leqslant k \leqslant 86$ and $4 \leqslant q \leqslant 97$

q \ k	87	88	89	90	91	92	93	94	95	96	97	98	99	100
4					96	96							104	
5					96	96			100	100			104	
7					96	96	98	98					104	
8					96	96							104	
9					96	96							104	
11					96	96							104	
13					96	96							104	104
16					96	96							104	
17					96	96								
19					96	96								
23	92	92			96	96								
25					96	96			100	100			104	
27					96	96							104	
29					96	96								
31					96	96								
32					96	96								
37					96	96								
41					96	96								
43					96	96								
47	92	92	94	94	96	96								
49					96	96	98	98					104	
53					96	96							104	104
59					96	96								
61					96	96								
64					96	96							104	
67					96	96								
71					96	96								
73					96	96								
79					96	96							104	
81					96	96							104	
83					96	96								
89					96	96								
97					96	96								

Table 13: Girth of $D(k, q)$ for $87 \leqslant k \leqslant 100$ and $4 \leqslant q \leqslant 97$