

On affine forestry over integral domains and families of deep Jordan-Gauss graphs

Tymoteusz Chojecki*

chojecki.tymoteusz@gmail.com

Grahame Erskine†

grahame.erskine@open.ac.uk

James Tuite‡

james.t.tuite@open.ac.uk

Vasyl Ustimenko‡§¶

Vasyl.Ustymenko@rhul.ac.uk

Abstract

Let K be a commutative ring. We refer to a connected bipartite graph $G = G_n(K)$ with partition sets $P = K^n$ (points) and $L = K^n$ (lines) as an *affine graph* over K of dimension $\dim(G) = n$ if the neighbourhood of each vertex is isomorphic to K . We refer to G as an *algebraic affine graph* over K if the incidence between a point (x_1, x_2, \dots, x_n) and line $[y_1, y_2, \dots, y_n]$ is defined via a system of polynomial equations of the kind $f_i = 0$ where $f_i \in K[x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n]$. We say that an affine algebraic graph is a *Jordan-Gauss graph* over K if the incidences between points and lines are given by a quadratic system of polynomial equations, and the neighbourhood of each vertex is given as a solution set of the system of linear equations in row-echelon form.

For each integral domain K we consider the known explicit construction of the family of Jordan-Gauss graphs $A(n, K)$, $n = 2, 3, \dots$ with cycle indicator $\geq 2n + 2$. Additionally several constructions of families of edge intransitive Jordan-Gauss graphs over K of increasing girth with well defined projective limit will be presented. This projective limit is a forest defined by the system of algebraic equations. In the case $K = \mathbb{F}_q$, $q \geq 3$ we present results of computer experiments for the evaluation of girth, cycle indicator, diameter and the second largest eigenvalue of the constructed graphs, and we formulate several conjectures on their properties. One of the conjectures is that the girth of $A(n, \mathbb{F}_q)$ is $2\lceil(n+5)/2\rceil$. We discuss briefly some applications of Jordan-Gauss graphs of large girth to Graph Theory, Algebraic Geometry and the theory of LDPC codes; and we consider ideas to use groups related to these graphs in Noncommutative Cryptography and Stream Ciphers Design.

MSC2020 classification: 05D99, 11T71, 05C38, 05C25, 05C50, 05C82.

Keywords: bipartite algebraic graphs of increasing girth; small world graphs; constructions of expanders; graph based multivariate transformations; cryptographic applications.

*Maria Curie-Skłodowska University, Lublin, Poland

†Open University, Milton Keynes, UK

‡Royal Holloway, University of London, UK

§Institute of telecommunications and global information space, Kyiv, Ukraine

¶Corresponding author

1 Introduction

Background

In this paper we investigate interpretations of a q -regular forest (a q -regular simple graph without cycles) in terms of algebraic geometry over the finite field \mathbb{F}_q . More precisely, we are interested in sequences of (finite) bipartite regular algebraic graphs G_i , defined by nonlinear equations over \mathbb{F}_q , such that their projective limit T is well defined and does not contain cycles.

Since the projective limit T is acyclic, it follows that the girth of G_i grows with the parameter i . We also consider the projective limits of homogeneous algebraic graphs of increasing girth defined over an arbitrary field F . Important examples of bipartite algebraic graphs over an arbitrary field F with known girth and diameter are the generalised polygons $GP_m(F)$, $m = 3, 4, 6$ which are geometries of the Chevalley groups $A_2(F)$, $B_2(F)$ and $G_2(F)$ (see [6, 7]).

It is noteworthy that the restriction of the incidence relation I on the largest orbits of unipotent subgroups of these groups is an affine algebraic graph $AG_s(F)$ with partition sets isomorphic to F^s where $s = 2, 3, 5$. We can view points and lines as vectors indexed by the positive roots of A_2 , B_2 and G_2 which are vectors of R^2 . So the pointset and the lineset can be thought of as totalities P and L of tuples:

$$(x_{(1,0)}, x_{(1,1)}) = (x) \text{ and } [y_{(0,1)}, y_{(1,1)}] = [y] \text{ (case of } A_2),$$

$$(x_{(1,0)}, x_{(1,1)}, x_{(1,2)}) \text{ and } [y_{(1,0)}, y_{(1,1)}, y_{(1,2)}] \text{ (case of } B_2), \text{ and}$$

$$(x_{(1,0)}, x_{(1,1)}, x_{(1,2)}, x_{(1,3)}, x_{(2,3)}) \text{ and } [y_{(1,0)}, y_{(1,1)}, y_{(1,2)}, y_{(1,3)}, y_{(2,3)}] \text{ (case of } G_2).$$

Parentheses $()$ and brackets $[]$ allow us to distinguish points from lines. If $F = \mathbb{F}_q$ then the graphs $GP_m(F)$, $m = 3, 4, 6$ are $q + 1$ -regular graphs of girth $2m$, and their induced subgraphs $AG_s(F)$, $s = 2, 3, 5$ are q -regular graphs of even girth $\geq 2m$.

In the case of A_2 and B_2 , the incidence condition between points and lines of the Jordan-Gauss graphs $AG_2(F)$ and $AG_3(F)$ are given by quadratic equations with the single monomial term and nonzero coefficients 1 and -1 . So the point $(x_{(1,0)}, x_{(1,1)})$ and line $[y_{01}, y_{11}]$ are incident in $AG_2(F)$ if and only if

$$(x_{(1,1)} - y_{(1,1)} = x_{(1,0)}y_{(0,1)}).$$

Incidence of $(x_{(1,0)}, x_{(1,1)}, x_{(1,2)})$ and $[y_{(1,0)}, y_{(1,1)}, y_{(1,2)}]$ of $AG_3(F)$ means that

$$(x_{(1,1)} - y_{(1,1)} = x_{(1,0)}y_{(0,1)}) \text{ and } (x_{(1,2)} - y_{(1,2)} = y_{(0,1)}x_{(1,1)}).$$

In the case of a field F of characteristic zero we can consider induced subgraphs $AG_s(\mathbb{Z})$ of $AG_s(F)$, in which points and lines are the tuples with integer coordinates. Obviously we can define affine graphs $AG_s(K)$, $s = 2, 3$ for an arbitrary commutative ring K with partition sets K^s and incidence relations given by the above equations. One can prove that in the case of an integral domain K , i.e. a commutative ring without zero divisors, the girth of $GA_s(K)$, $s = 2, 3$ is at least $2s + 2$.

An infinite forest can be interpreted as the geometry of a Kac-Moody group over the field F with the diagram \tilde{A}_1 . There are two different root systems with Cartan matrices ${}^jA = ({}^j a_{i,j})$, $j = 1, 2$ of rank 2 for which ${}^j a_{1,1} = {}^j a_{2,2} = 2$, ${}^1 a_{2,1} = {}^1 a_{1,2} = -2$, ${}^2 a_{2,1} = -1$, ${}^2 a_{1,2} = -4$. This motivates the idea to construct the infinite family $\Gamma_n(F) = D(n, F)$ with vertex set $F^n \cup F^n$ of Jordan-Gauss graphs of increasing girth g_n . In [15, 16, 17, 18] the root system \tilde{A}_1 corresponding to the Cartan matrix 1A was used for this purpose. This infinite set of roots contains *real* roots $(i + 1, i)$, $(i, i + 1)$, $i \geq 0$ together with *imaginary* roots (i, i) , $i \geq 1$. To make studies of the girth easier, the authors of [16] use *twins* $(i, i)'$, $i \geq 2$ of imaginary roots.

The inequality $\text{girth}(D(n, \mathbb{F}_q) \geq 2[(n+5)/2]$ was proven in [17]. The fact that for natural analogs $D(n, K)$, defined over an arbitrary integral domain K , the relation $\text{girth}(D(n, K) \geq 2[(n+5)/2]$ holds was proven essentially later [37]. The importance of this result is connected with the cases of graphs $D(n, K[x_1, x_2, \dots, x_m])$ over multivariate rings which are important for the theory of symbolic computation.

Definitions and notation

In this paper we study the properties of a number of families of bipartite graphs. We adopt the following definitions and notation.

All graphs (which may be finite or infinite) are assumed to be simple (no loops or multiple edges) and undirected unless otherwise stated. The *girth* $\text{girth}(G)$ of a graph G is the length of a shortest cycle in G , or ∞ if no cycle exists. We define the *local girth* $\text{lgirth}(v)$ of a vertex v to be the minimal length of a cycle through v , and the *cycle indicator* $\text{cind}(G)$ of G to be the maximum of the local girth across all vertices of G . The diameter $\text{diam}(G)$ is the maximum distance between any two vertices of the graph.

The idea of presentation of a branching process via the generation of walks on regular graphs motivates the following definitions. Let G be a k -regular graph, where k may be finite or infinite. We say that the *depth* $\text{depth}(v)$ of the vertex v of a graph G is d if all vertices at distance at most d from v form a tree, but the graph of vertices at distance $d + 1$ contains a cycle. We define the depth $\text{depth}(G)$ of a k -regular graph G as the maximal depth of its vertices. Note that in the case of vertex transitive graph G its girth $\text{girth}(G)$ is at least $2 \text{depth}(G) + 2$.

For a commutative ring K , we refer to a connected bipartite graph $G = G_n(K)$ with partition sets $P = K^n$ (points) and $L = K^n$ (lines) as an *affine graph* over K of dimension $\text{dim}(G) = n$ if the neighbourhood of each vertex is isomorphic to K . We refer to G as an *algebraic affine graph* over K if the incidence between a point (x_1, x_2, \dots, x_n) and line $[y_1, y_2, \dots, y_n]$ is defined via a system of polynomial equations of the kind $f_i = 0$ where $f_i \in K[x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n]$. We say that an affine algebraic graph is a *Jordan-Gauss graph* over K if the incidences between points and lines are given by a quadratic system of polynomial equations, and the neighbourhood of each vertex is given as a solution set of the system of linear equations in row-echelon form. A *homogeneous algebraic graph* over an arbitrary field F is a graph for which the vertex set and edge set are algebraic varieties over F , and the dimension of the neighbourhood of each vertex is the same.

For other basic definitions of graph theory, the reader may consult [2], [3] or [5]. For basic algebraic definitions we refer to [46]. The concept of *algebraic graph* can be found in [1].

Structure of paper

The current paper is dedicated to further studies of the properties of infinite families of Jordan-Gauss graphs. Some of them $(A(n, K), B(n, m, K))$ [45] have already been already introduced as homomorphic images of $D(n, K)$ induced by the deletion of some coordinates and corresponding variables; other families are new, being obtained via deletion of coordinates and modification of some incidence equations. Most graphs under investigation are not edge transitive, i.e. their groups of automorphisms do not act transitively on the sets of points and lines; so the cycle indicator of such a graph may differ from the girth.

For the Jordan-Gauss graphs $\Gamma_n(\mathbb{F}_q)$ under investigation, we compute their depth, girth, cycle indicator and the second largest eigenvalue via computer calculation. It turns out that in all

investigated cases, the second largest eigenvalue is bounded from above by $2\sqrt{q}$. So we can conjecture that families of ‘almost Ramanujan’ graphs $\Gamma_n(\mathbb{F}_q)$ exist.

In particular, in Sections 3 and 4 we investigate two graph families $A(n, q) = A(n, \mathbb{F}_q)$ and $D(n, q) = D(n, \mathbb{F}, q)$. In the case of the general family $A(n, K)$ where K is an integral domain with at least 4 elements, we know or conjecture the following.

- (1) $\text{cind}(A(n, K)) \geq 2n + 2$ (already proven, see [35] or [36]).
- (2) $\text{girth}(A(n, K)) = 2\lfloor(n + 5)/2\rfloor$ (not proven, but supported by our computer calculations).
- (3) $\text{diam}(A(n, K)) \leq 2n + 2$ (not proven, but supported by our computer calculations).
- (4) $\text{depth}(A(n, K)) = n$ (not proven, but supported by our computer calculations).
- (5) If K is a commutative ring with unity of odd characteristic with at least 5 elements then $A(n, K)$ is a connected graph (already proven [36]).
- (6) The second largest eigenvalue of $A(n, \mathbb{F}_q)$ is at most $2\sqrt{q}$ (not proven, but supported by large scale computer calculations).

In the case of the family $D(n, K)$, where K is an integral domain with at least 5 elements, we know or conjecture the following.

- (1) $\text{cind}(D(n, K)) = \text{girth}(D(n, K)) \geq 2\lfloor(n + 5)/2\rfloor$ (already proven in [37]). Computer experiments support the conjecture that $\text{girth}(D(n, K)) = 2\lfloor(n + 5)/2\rfloor$. Equality is already proven in the case of fields of characteristic zero [31] and finite fields of special orders [10].
- (2) If K has unity and is of odd characteristic, then each connected component $CD(n, K)$ of $D(n, K)$ is a Jordan-Gauss graph of dimension $n - \lfloor(n + 2)/4\rfloor + 1$ [38]. In fact the case of $K = \mathbb{F}_q$ for odd q was investigated earlier in [19]. In [20] it was shown that a connected component of $D(n, q)$ with even $q \geq 6$ also has dimension $n - \lfloor(n + 2)/4\rfloor + 1$, and that a connected component of $D(n, \mathbb{F}_4)$ has dimension $n - \lfloor(n + 2)/4\rfloor$ [20].

Computer experiments support the following conjectures about connected components of affine graphs $D(n, K)$, where K is an integral domain with at least 4 elements.

- (3) The family of affine edge-transitive graphs $CD(n, K)$ is a family of affine small world graphs.
- (4) The second largest eigenvalue of $CD(n, \mathbb{F}_q)$ is at most $2\sqrt{q}$ (not proven, but supported by large scale computer calculations).

Remark. Computer calculations will allow us to formulate mathematical statements about an infinite totality of combinatorial objects, as the following example shows.

Example. Computer experiments showed that $\text{girth}(D(n, \mathbb{F}_5)) = \text{girth}(D(n, \mathbb{F}_7)) = 2\lfloor(n + 5)/2\rfloor$ for $n = 2, 3, \dots, 14$. We deduce from this the following statement.

Proposition 1.1. *Let K be an integral domain of characteristic 5 or 7. Then the incidence structure $D(n, K)$ has girth $2\lfloor(n + 5)/2\rfloor$ for $n = 2, 3, \dots, 14$.*

Section 2 contains definitions of families of large girth, families with large cycle indicator and families of deep graphs in the cases of finite and affine graphs. Section 3 contains the definitions of graphs $A(n, K)$, $D(n, K)$ and $B(n, m, K)$. Their application to extremal and spectral graph theory are discussed here. Section 4 is dedicated to descriptions of connected components of graphs $D(n, K)$ and $B(n, m, K)$ and results on depth, girth and cycle indicators of graphs

$B(n, m, K)$ and new Jordan-Gauss graphs ${}^sD_T(n, K)$. Section 5 is dedicated to the application of forest approximations $D(n, K)$ and $A(n, K)$ to algebraic graph theory. In Section 6 we consider applications of explicit constructions of deep Jordan-Gauss graphs to constructions for noncommutative cryptography and design of stream ciphers.

2 On families of affine algebraic graphs with specific properties

Let K be a commutative ring with unity. The variety K^n is known as an *affine space over K* or a *free module*. We define an *affine forest* over K as a family of bipartite graphs $G(n_i, K)$, where n_i is increasing sequence of positive integers, with partition sets isomorphic to K^{n_i} such that the neighbourhood of each vertex is isomorphic to the variety K , and the well-defined projective limit $G(K) = \lim_{i \rightarrow \infty} (G(n_i, K))$ has no cycles. The projective limit is defined by the family of graph homomorphisms $\eta_i : G(n_{i+1}, K) \rightarrow G(n_i, K)$, $i = 1, 2, \dots$

Each bipartite graph $G(n_j, K)$ can be identified with an incidence structure with point set $P_j = K^{n_j}$, line set $L_j = K^{n_j}$ and incidence relations I_j . We study the case of *algebraic* bipartite graphs where the incidence between points and lines is defined via a system of polynomial equations.

We review some known affine forests formed by algebraic bipartite graphs, together with a variety of new examples with similarities to known affine forests $D(n, K)$ where K is an integral domain. For each presented graph $G(n_i, K)$ we consider the following tasks.

- (1) Investigation of the trees of $G(K)$ via studies of the connected components $CG(n_i, K)$ of graphs $G(n_i, K)$.
- (2) For each connected component $CG(K)$ we will investigate the girth ($CG(n_i, K)$) (the length of its smallest cycle).
- (3) For each $CG(n_i, K)$ we evaluate its diameter $\text{diam}(CG(n_i, K))$.
- (4) For each $CG(n_i, K)$ we evaluate its cycle indicator $\text{cind}(C(n_i, K))$ which is the maximum of the minimal length of a cycle through any vertex v of $CG(n_i, K)$.

In the case $K = \mathbb{F}_q$ we use computer simulations to investigate tasks (2), (3) and (4), and in addition we evaluate the second largest eigenvalue of $CG(n_i, \mathbb{F}_q)$. We also formulate some theoretical results on graphs of the kind $CG(n_i, K)$. We observe some applications of graphs $CG(n_i, \mathbb{F}_q)$ to extremal and spectral graph theory, applications of $CG(n_i, \mathbb{F}_q)$ to the theory of homogeneous algebraic graphs, and practical application of the properties of $CG(n_i, K)$ to the theory of LDPC codes and cryptography.

In the case of cryptographical applications, more general graphs $CG(n_i, K)$ where K is an arbitrary commutative ring can be used. The cases of finite arithmetical rings \mathbb{Z}_n , Boolean rings B_n of order 2^n or infinite rings $K[x_1, x_2, \dots, x_m]$, $K \in \{\mathbb{Z}_n, B_n, \mathbb{F}_q\}$ are already used in cryptographical algorithms.

Walks from a given vertex v of the forest $G(K)$ define an infinite branching process $B(K)$. So the equations of $G(K)$ give a description of the deterministic part of this process. Members $G(n_i, K)$ of an algebraic forest with “sufficiently large” i can be used for the practical approximation of this branching process in computer memory.

The idea of presentation of a branching process via the generation of walks on regular graphs motivates the following definitions. Let G be a k -regular graph, where k may be finite or infinite. We say that the *depth* $\text{depth}(v)$ of the vertex v of G is d if all vertices at distance at

most d from v form a tree, but the graph of vertices at distance $d + 1$ contains a cycle.

We say that a family $G_i, i = 2, 3, \dots$ of regular graphs of order v_i and bounded degree k_i , where $k_i > 2$, is a *family of deep graphs* if for each i there exists a vertex $x_i \in V(G_i)$ of depth $\text{depth}(x_i) \geq c \log_{k_i}$ for some constant c . In fact it can be shown that we may assume that $c \leq 1$.

We define the *depth* of a k -regular graph as the maximal depth of any of its vertices. Families of k -regular deep graphs are families with the fastest possible growth of depth.

Let K be a commutative ring. We refer to a connected bipartite graph G with partition sets $P = K^n$ and $L = K^n$ as an *affine algebraic graph* over K of dimension $\dim(G) = n$ if the neighbourhood of each vertex is isomorphic to K .

We say that an affine algebraic graph is a *Jordan-Gauss graph* over K if incidences between points and lines are given by a quadratic system of polynomial equations, and the neighbourhood of each vertex is given as a solution set of the system of linear equations in row-echelon form. We say that the family of affine graphs G_i over K is a *family of deep affine graphs* if for each i there exists some vertex $x \in V(G_i)$ with depth $\text{depth}(x) \geq c \dim(G_i)$ for some positive constant c .

The existence of the family of deep Jordan-Gauss graphs $CD(n, K)$ over an arbitrary integral domain K was proven in [37]. Our paper is dedicated to other examples of families of deep Jordan-Gauss graphs, and studies of their topological properties. In the case of finite fields we evaluate expansion properties of Jordan-Gauss graphs via evaluation of their second largest eigenvalues.

We say that a family of affine graphs G_i of increasing dimension over K is a *family of affine graphs with large girth* if for each i the girth $\text{girth}(G_i)$ of G_i is at least $c \dim(G_i)$ for some positive constant c . It is easy to see that every family of affine graphs of large girth is a family of deep affine graphs.

We say that a family of affine graphs G_i of increasing dimension over K is a *family of affine small world graphs* if for each i the diameter $\text{diam}(G_i)$ of G_i is at most $c \dim(G_i)$ for some positive constant c .

We say that a family of affine graphs G_i of increasing dimension over a commutative ring K is a *family with large cycle indicator* if $\text{cind}(G_i) \geq c \dim(G_i)$ for some positive constant c . It follows from the definitions that every affine family of large girth will be a family with large cycle indicator.

It is easy to see that if a vertex v of a bipartite graph G has local girth d then the cycle indicator of G is at least $2d + 2$. So every family of affine deep graphs will be a family of affine graphs with large cycle indicator.

3 Algebraic forests over finite fields and extremal and spectral graph theories and LDPC codes

Studies of the maximal size $\text{ex}(C_3, C_4, \dots, C_{2m}, v)$ of a finite simple graph on v vertices without cycles of length $3, 4, \dots, 2m$, i.e. graphs of girth greater than $2m$, form an important direction of extremal graph theory. It follows from the famous Even Circuit Theorem by P. Erdős that we have the inequality $\text{ex}(C_3, C_4, \dots, C_{2m}, v) \leq cv^{1+1/m}$, where c is a certain constant. The bound is known to be sharp only for $m = 2, 3, 5$. The first general lower bounds of the kind $\text{ex}(v, C_3, C_4, \dots, C_n) = \Omega(v^{1+c/n})$, where c is some constant with $c < \frac{1}{2}$, were obtained in the 50s by Erdős via studies of families of graphs of large girth, i.e. infinite families of simple regular

graphs G_i of degree k_i and order v_i such that $\text{girth}(G_i) \geq c \log_{k_i}(v_i)$, where c is a constant independent of i . Erdős proved the existence of such a family with arbitrary large but bounded degree $k_i = k$ with $c = \frac{1}{4}$ by his famous probabilistic method.

Just two explicit families of regular simple graphs of large girth with unbounded girth and arbitrarily large k are known: the family $X(p, q)$ of Cayley graphs for $\text{PSL}_2(p)$, where p and q are primes, had been defined by G. Margulis [23] and investigated by A. Lubotzky, Phillips and Sarnak [22]; and the family of algebraic graphs $CD(n, q)$ [18]. The best known lower bound for $d \neq 2, 3, 5$ had been deduced from the existence of the above mentioned families of graphs $\text{ex}(v, C_3, C_4, \dots, C_{2d}) \geq c(v^{1+2/(3d-3+e)})$, where $e = 0$ if d is odd, and $e = 1$ if d is even. By the theorem of Alon and Boppana, large enough members of an infinite family of q -regular graphs satisfy the inequality $\lambda \geq 2\sqrt{q-1} - o(1)$, where λ is the second largest eigenvalue in absolute value (see [21]).

Recall that *Ramanujan graphs* are q -regular graphs for which the inequality $\lambda \leq 2\sqrt{q-1}$ holds. We say that regular graphs of bounded degree q form a *family of Ramanujan graphs* if the second largest eigenvalue of each graph is bounded from above by $2\sqrt{q-1}$. It is clear that a family of Ramanujan graphs of bounded degree q has the best possible spectral gap $q - \lambda$. We say that a family of q -regular graphs G_i is a *family of almost Ramanujan graphs* if its second largest eigenvalues are bounded above by $2\sqrt{q}$. The family $X(p, q)$ noted above is a family of Ramanujan graphs; for this reason we refer to them as Cayley-Ramanujan graphs.

The following conjecture was formulated in [34], where the author tried to prove it.

Conjecture 3.1. *The family $CD(n, q)$ is a family of almost Ramanujan graphs.*

This proof contains a gap, but computer experiments support the conjecture. It is known that if $q \geq 5$, these graphs are not Ramanujan despite the fact that the projective limit $CD(q)$ of $CD(n, q)$ is a q -regular tree. The reason is that the eigenspace of $CD(q)$ is not a Hilbert space (the topology is p -adic).

The expanding properties of $X(p, q)$ and $D(n, q)$, and the high girth property of both families, can be used for the construction of cryptographic algorithms (hash functions [8, 9], fast stream ciphers with good mixing properties [39], other application [40] and further references). Notice that both properties had been used for construction of a good class of LDPC error correcting codes, which is an important practical tool for security in satellite communications [24, 21, 13]. The usage of $CD(n, q)$ as Tanner graphs [32, 11, 12] producing LDPC codes leads to better properties of corresponding codes in comparison with the use of Cayley-Ramanujan graphs (see [25]). Both families $X(p, q)$ and $CD(n, q)$ consist of edge transitive graphs; they have similar expansion properties and the property of being graphs of large girth.

Graphs $D(n, \mathbb{F}_q)$ are defined by a system of quadratic equations with nonzero coefficients 1 and -1 . A simple change of \mathbb{F}_q for an arbitrary commutative ring K with unity leads to graphs $D(n, K)$, see [41], where it was stated that the projective limit $D(K)$ of these graphs when n tends to infinity is a forest if K is an integral domain. In fact for the integral domain K , the girth of $D(n, K)$ is at least $n + 5$ provided n is odd (see [37]). In the case of arbitrary K , the graph $D(K)$ can be introduced (see [44]) as an infinite bipartite graph $D(K)$ defined on sets of points of the kind

$$(x) = (x_1, x_2, x_3, x'_3, x_4, x'_4, \dots, x'_n, x_n, \dots), \quad x_i \in K, \quad x'_i \in K$$

and lines of the kind

$$[y] = [y_1, y_2, y_3, y'_3, \dots, y_n, y'_n, \dots], \quad y_i \in K, \quad y'_i \in K$$

via incidence relation $I : (x)I[y]$ if and only if the following relations hold:

$$x_2 - y_2 = y_1 x_1,$$

$$x_3 - y_3 = x_1 y_2,$$

$$x_4 - y_4 = y_1 x_3,$$

$$x_5 - y_5 = x_1 y_4,$$

...

together with equalities

$$x'_3 - y'_3 = y_1 x_2,$$

$$x'_4 - y'_4 = x_1 y'_3,$$

$$x'_5 - y'_5 = y_1 x'_4,$$

...

If n is odd then $x_n - y_n = x_1 y_{n-1}$ and $x'_n - y'_n = y_1 x'_{n-1}$.

If n is even then $x_n - y_n = y_1 x_{n-1}$ and $x'_n - y'_n = x_1 y'_{n-1}$.

We also consider the family of graphs $B(n, m, K)$ for the case $m \leq n$, whose vertices are points of the kind

$$(x) = (x_1, x_2, x_3, x'_3, \dots, x_{m+2}, x'_{m+2}, x'_{m+3}, x'_{m+4}, \dots, x'_{n+2})$$

from set $P_{m,n} = K^{m+n+2}$, and lines of the kind

$$[y] = [y_1, y_2, y_3, y'_3, \dots, y_{m+2}, y'_{m+2}, y'_{m+3}, y'_{m+4}, \dots, y'_{n+2}]$$

from $L_{m,n} = K^{m+n+2}$, such that (x) and $[y]$ are incident if and only if the relations from the above list hold for variables

$$\{x_1, x_2, x_3, x'_3, \dots, x_{m+2}, x'_{m+2}, x'_{m+3}, \dots, x'_{n+2}\} \cup \{y_1, y_2, y_3, y'_3, \dots, y_{m+2}, y'_{m+2}, y'_{m+3}, \dots, y'_{n+2}\}.$$

We refer to the above list as the *list of variables* of the graph $B(n, m, K)$. There is a natural homomorphism $\phi^{m,n}$ from $D(K)$ onto $B(n, m, K)$ defined via the procedure of deleting those coordinates of the infinite points (x) and lines $[y]$ which do not belong to the above finite list. If $K = \mathbb{F}_q$ is the finite field of q elements, then we write $B(n, m, K) = B(n, m, q)$. In [30] it is stated that the projective limit of $B(n, m, q)$ as $m \rightarrow \infty$ is a forest.

In fact the graph $A(n, K) = B(n-2, 0, K)$ was defined in [37] (as the graph $E(n, K)$ in the notation of that paper). Some properties of $A(n, \mathbb{F}_q) = A(n, q)$ are considered in [36].

Note that the graph $B(n, m, K)$ is a homomorphic image of $D(n+m+2, K)$ under the homomorphism of deleting coordinates outside of the list of coordinates of $B(n, m, K)$. This homomorphism is a local isomorphism; this means that the second largest eigenvalue of a connected component $CB(n, m, \mathbb{F}_q)$ of $B(n, m, \mathbb{F}_q)$ is bounded by the second largest eigenvalue of $CD(n, \mathbb{F}_q)$. So from conjecture 3.1 about the second largest eigenvalue of $CD(n, q)$, it follows that graphs $CB(n, m, q)$ are almost Ramanujan. Note that besides the fact that $2\lfloor(n+5)/2\rfloor$ is a lower bound for the girth of $CD(n, K)$ in the general case of an integral domain K , the exact girth of these graphs are known in only a few special cases of the integral domain (see [10, 31]).

The computation of the girth of graphs $B(n, m, K)$ in the more general case of arbitrary n, m and integral domain K is a difficult and important task. This paper is dedicated to investigation of the girth and diameter of graphs $CD(n, K)$, $B(n, m, K)$ and some modifications of $CD(n, K)$. Computer experiments show that in many cases of integers n, m and prime powers q , the graphs $B(n, m, q)$ are not edge transitive.

Roots of \tilde{A}_1 and generalisation of graphs $B(n, m, K)$

The affine root system \tilde{A}_1 (see [4]) is the following totality of vectors in R^2 with the standard basis $e_1 = (1, 0)$ and $e_2 = (0, 1)$. It contains vectors $(1, 0), (0, 1), (i, i), (i, i+1), (i+1, i), i \geq 1$. All multiples of $(1, 1)$ are known as *imaginary roots*; other roots which have no multiples are known as *real roots*. We modify \tilde{A}_1 by adding copies $(i, i)'$ for each imaginary root $(i, i), i > 1$. So we obtain a set Root consisting of roots of \tilde{A}_1 and elements $(i, i)', i > 1$.

Let $R_1 = \text{Root} - \{(0, 1)\}$ and $R_2 = \text{Root} - \{(1, 0)\}$, and let K be a commutative ring with unity. We consider sets $L_i = K^{R_i}, i = 1, 2$ and the set of all functions f from R_i to $K, i = 1, 2$, such that for only a finite number of elements x from R_i is the value $f(x)$ different from zero. We write an element $X = (x)$ from $P = L_1$ as the tuple

$$(x) = (x_{1,0}, x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}, x'_{2,2}, \dots, x_{i,i+1}, x_{i+1,i}, x_{i+1,i+1}, x'_{i+1,i+1}, \dots)$$

where x_α is the value of X on the root α from \tilde{A}_1 and $x'_{i,i}$ is the value of X on $(i, i)', i > 1$.

Similarly we write an element $Y = [y]$ from $L = L_2$ as the tuple

$$[y] = [y_{0,1}, y_{1,1}, y_{1,2}, y_{2,1}, y_{2,2}, y'_{2,2}, \dots, y_{i,i+1}, y_{i+1,i}, y_{i+1,i+1}, y'_{i+1,i+1}, \dots]$$

where y_α is the value of Y on the root α from \tilde{A}_1 and $y'_{i,i}$ is the value of Y on $(i, i)', i > 1$. We introduce the incidence structure (P, L, I) as the following bipartite graph on $P \cup L$. A point (x) of this incidence structure I is incident with a line $[y]$, i.e. $(x)I[y]$, if their coordinates obey the following relations:

$$\begin{aligned} x_{i,i} - y_{i,i} &= x_{1,0}y_{i-1,i}, \\ x'_{i,i} - y'_{i,i} &= x_{i,i-1}y_{0,1}, \\ x_{i,i+1} - y_{i,i+1} &= x_{i,i}y_{0,1}, \\ x_{i+1,i} - y_{i+1,i} &= x_{1,0}y'_{i,i}. \end{aligned} \tag{1}$$

(These four relations are well defined for $i > 1, x_{1,1} = x'_{1,1}, y_{1,1} = y'_{1,1}$.)

Let us assume that elements of R_1 and R_2 of indices of points and lines of the bipartite graph $D(K)$ are written in their natural order, i.e. sequences:

$$((1, 0), (1, 1), (1, 2), (2, 1), (2, 2), (2, 2)', \dots) \text{ and } ((0, 1), (1, 1), (1, 2), (2, 1), (2, 2), (2, 2)', \dots).$$

Let ${}^k R_i, i = 1, 2$ be the list of the k first elements of $R_i, i = 1, 2$. The procedure of deleting coordinates of points and lines of $D(K)$ indexed by elements of $R_i - {}^k R_i$ defines the homomorphism of $D(K)$ onto the graph $D(k, K), k > 1$.

Recall that $D(k, \mathbb{F}_q)$ coincides with $D(k, q)$ of [18].

Graphs $A(m, K)$ were obtained in [37] as quotients of graphs $D(n, K)$. This incidence structure was defined in the following way.

Let K be an arbitrary commutative ring. We consider the totality P' of points of the form

$$x = (x) = (x_{1,0}, x_{1,1}, x_{1,2}, x_{2,2}, \dots, x_{i,i}, x_{i,i+1}, \dots), \text{ with coordinates from } K,$$

and the totality L' of lines of the form

$$y = [y] = [y_{0,1}, y_{1,1}, y_{1,2}, y_{2,2}, \dots, y_{i,i}, y_{i,i+1}, \dots].$$

We assume that tuples (x) and $[y]$ have finite support, and a point (x) is incident with a line $[y]$, i.e. xIy or $(x)I[y]$, if the following conditions are satisfied:

$$\begin{aligned} x_{i,i} - y_{i,i} &= y_{i-1,i}x_{1,0}, \\ x_{i,i+1} - y_{i,i+1} &= y_{0,1}x_{i,i}. \end{aligned} \tag{2}$$

We denote the graph of this incidence structure as $A(K)$. We consider the set Root of indices of points and lines of $A(K)$ as a subset of the totality of all elements $(i+1, i+1)$, $(i, i+1)$, $(i+1, i)$, $i \geq 0$ of the root system \tilde{A}_1 of affine type. We see that $\text{Root} = \{(1, 0), (0, 1), (1, 1), (1, 2), (2, 2), (2, 3), \dots\}$. So we introduce $R_{1,0} = \text{Root} - \{(0, 1)\}$ and $R_{0,1} = \text{Root} - \{(1, 0)\}$. This allows us to identify sets P' and L' with affine subspaces $\{f : R_{1,0} \rightarrow K\}$ and $\{f : R_{0,1} \rightarrow K\}$ of functions with finite supports.

It is easy to see that the procedure of deleting coordinates of points and lines of $D(K)$ indexed by $\text{Root} - R_{1,0}$ and $\text{Root} - R_{0,1}$ defines the homomorphism of $D(K)$ onto $A(K)$.

For each positive integer $k \geq 2$, we obtain an incidence structure (P_k, L_k, I_k) as follows. Firstly, P_k and L_k are obtained from P' and L' , respectively, by simply projecting each vector onto its k initial coordinates. The incidence I_k is then defined by imposing the first $k-1$ incidence relations and ignoring all the other ones. The incidence graph corresponding to the structure (P_k, L_k, I_k) is denoted by $A(k, K)$.

4 Results on the connected components of $B(n, m, K)$

Let us consider alternative notations for the graphs $B(n, m, K)$ where K is a commutative ring with unity. We associate with the graph $D(2k+1, K)$ the totality R_{2k+1} of roots to delete which is $\{(k-1, k-1), (k-1, k-2), (k-2, k-2), \dots, (2, 2), (2, 1)\}$ if k is odd and $\{(k, k-1), (k-1, k-1), \dots, (2, 1)\}$ if k is even. Let us assume that $R_{2k+1,s}$ is the set of elements of R_{2k+1} after deletion of s roots from the above list. Let $T(2k+1, s) = R_{2k+1} - R_{2k+1,s}$.

We consider the *chopped graph* $D_{2k+1,s}(K)$, $0 \leq s \leq k-1$, $k \geq 2$ as the totality of points and lines of $D(2k+1, K)$ with deleted coordinates indexed by elements of $T(2k+1, s)$ and deleted equations with the variables x_α, y_α , $\alpha \in T(2k+1, s)$. In fact the totality of elements $B(n, m, K)$ is a collection of graphs $D_{2k+1,s}(K)$ and graphs $D(2k, K)$. It is easy to see that $D_{2k+1,0}(K) = D(2k+1, K)$, and $D_{2k+1,k-1}(K) = A(k+2, K)$.

We introduce $I_{2k+1,s}$ to be the intersection of $R_{2k+1,s}$ with the set $\{(2, 2)', (3, 3)', \dots\}$. Let $d(2k+1, s)$ be the cardinality of this set. So $d(5, 0) = d(5, 1) = 0$, $d(7, 0) = 1$, $d(7, 1) = 0$.

Theorem 4.1.

(i) *Let K be a commutative ring of odd characteristic. Then the variety $V_{2k+1,s}(K)$ of connected components of the graph $D_{2k+1,s}(K)$ is isomorphic to $K^{d(2k+1,s)} = K^{I_{2k+1,s}}$. We assume that $K^0 = K^\emptyset$ is an empty set.*

(ii) *All elements of $V_{2k+1,s}(K)$ are isomorphic subgraphs $CD_{2k+1,s}(K)$ of $D_{2k+1,s}(K)$.*

This statement follows directly from the description of connected components of $D(k, K)$ given in [38].

We begin the description of connected graphs $V_{2k+1,s}(K)$ with the results on the connectivity invariants of $D(k, K)$. To facilitate notation in the future results on ‘‘connectivity invariants’’ of $D(n, K)$, it will be convenient for us to define $p_{-1,0} = l_{0,-1} = p_{1,0} = l_{0,1} = 0$, $p_{0,0} = l_{0,0} = -1$, $p'_{0,0} = l'_{0,0} = -1$, $p_{1,1} = p'_{1,1}$, $l_{1,1} = l'_{1,1}$ and to assume that our equations are defined for $i \geq 0$.

Graphs $CD(k, K)$ with $k \geq 6$ were introduced in [44] as induced subgraphs of $D(k, K)$ with vertices u satisfying the special equations

$$a_2(u) = 0, a_3(u) = 0, \dots, a_t(u) = 0, t = [(k+2)/4],$$

where $u = (u_\alpha, u_{1,1}, u_{1,2}, u_{2,1}, \dots, u_{r,r}, u'_{r,r}, u_{t,t+1}, u_{r,r+1}, u_{r+1,r}, \dots)$, $2 \leq r \leq t$, $\alpha \in \{(1, 0), (0, 1)\}$ is a vertex of $D(k, K)$ and

$$a_r = a_r(u) = \sum_{i=0}^r (u_{i,i} u'_{r-i,r-i} - u_{i,i+1} u_{r-i,r-i-1})$$

for every r from the interval $[2, t]$.

We set $a = a(u) = (a_2, a_3, \dots, a_t)$ and assume that $D(k, K) = CD(k, K)$ if $k = 2, 3, 4, 5$. It was proven in [37] that the graphs $D(n, K)$ are edge transitive. So their connected components are isomorphic graphs. Let ${}^v CD(k, K)$ be a solution set of the system of equations $a(u) = (v_2, v_3, \dots, v_t) = v$ for certain $v \in K^{t-1}$. It is proven that each ${}^v CD(k, K)$ is the disjoint union of some connected components of the graph $D(n, K)$. If K is a commutative ring with unity of odd characteristic, then ${}^v CD(k, K)$ is an actual connected component of the graph.

Proposition 4.2. *Let $D_{2k+1,s}(K)$ be a chopped graph of $D(2k+1, K)$ defined over an arbitrary commutative ring with unity K . Then the solution space C of the system $a_i(u) = b_i$, $(i, i)' \in I_{2k+1,s}$ for $u \in V(D_{2k+1,s}(K))$ is a union of connected components of the graph. If $\text{char}(K)$ is odd, then C is a connected component of the graph.*

Remark. If $K = \mathbb{F}_4$ then each C in Proposition 4.2 splits into 4 connected components of the graph.

Proposition 4.3. *Let K be a finite field of characteristic 2 with at least 4 nonzero elements. Then each C of Proposition 4.2 is an actual connected component of the graph $D_{2k+1,s}(K)$.*

This statement follows directly from the description of connected components of $D(n, \mathbb{F}_q)$, $q = 2^m$ given in [20].

Conjecture 4.4. *Let K be an integral domain with unity such that K^* contains more than two elements. Then the girth of $D_{2k+1,s}(K)$ is $2k - s + 6$ if s is even and $2k - s + 5$ or $2k - s + 7$ if s is odd.*

Proposition 4.5. *Let K be an integral domain. Then the girth of $D_{2k+1,s}(K)$ is $\geq 2k - 2s + 6$ if s is even and $\geq 2k - 2s + 5$ if s is odd.*

Corollary 4.6. *Let $k = cs + b$, where $c > 1$ and $b > 0$. Then the family of graphs $G(s, K) = D_{2k+1,s}(K)$, $s = 1, 2, \dots$, is a family of affine graphs over the integral domain K of large girth.*

Conjecture 4.7. *Let K be an integral domain. Then the depth of the graph $D_{2k+1,s}(K)$ is $\geq k + 2$.*

Proposition 4.8. *Let K be an integral domain with unity. Then the cycle indicator of the graph $D_{2k+1,s}(K)$ is $\geq 2k + 6$.*

Conjecture 4.9. *Let K be an integral domain with unity. Then the depth of the graph $D_{2k+1,s}(K)$ is $\geq k + 2$.*

Conjecture 4.10. *Let K be a field with at least 4 elements. Then the diameter of the graph $D_{2k+1,s}(K)$ is bounded from above by $2k + 6$.*

We introduce some additional graphs constructed from $D_{2k+1,s}(K) = {}^s D(2k+1, K)$. The cases of odd and even k will be considered separately.

If $n = 2k + 1$, then the coordinates of points and lines of $A(n, K)$ are indexed by $n + 1$ roots from the set ${}^n A = \{(1, 0), (0, 1), (1, 1), (1, 2), (2, 2), (2, 3), \dots, (k, k + 1)\}$.

If $n = 2k$, then the coordinates of $A(n, K)$ are indexed by $n + 1$ roots from the set ${}^n A = (1, 0), (0, 1), (1, 1), (1, 2), (2, 2), \dots, (k, k)$.

In the case of $n = 2k + 1$ we form the supplement ${}^{2k+1}A^*$ of nA consisting of the $2k$ roots

$$(2, 1), (2, 2)(3, 2), \dots, (k, k), (k + 1, k), (k + 1, k + 1).$$

We consider the containing graph $D(4k + 1, K)$, with the points and lines indexed by elements of ${}^{2k+1}A \cup {}^{2k+1}A^*$. Deletion of coordinates indexed by $(k + 1, k + 1)$ makes the quotient which is isomorphic to $D(4k, K)$.

For the set ${}^{2k+1}A^*$ we consider its difference ${}^{2k+1}A_s$ with the set $\Delta(2k + 1, s)$ of s senior roots $(k + 1, k + 1), (k + 1, k), (k, k), \dots$ of cardinality s , where $0 \leq s \leq 2k$. We already defined the chopped graph ${}^sD(4k + 1, K)$ obtained via deletion of coordinates of point and lines of $D(4k + 1)$ indexed by elements from $\Delta(2k + 1, s)$, and the deletion of corresponding equations of the incidence relation.

Let $J(2k + 1, s)$ be the intersection of ${}^{2k+1}A_s$ with the set of roots $(2, 2)', (3, 3)', \dots$. We can select some nonempty subset T of $J(2k + 1, s)$ such that $(i, i) \in T$ implies that $(i + 1, i) \in {}^{2k+1}A_s$, and make the following *truncation* procedure.

Delete coordinates of the vertices ${}^sD(4k + 1, K)$ indexed by $(i, i)'$ from T and change the equation indexed by $(i + 1, i)$ by replacing the variable indexed by $(i, i)'$ with the variable with index (i, i) . Let us denote the graph obtained as ${}^sD_T(4k + 1, K)$.

Conjecture 4.11. *Let K be an integral domain with unity. Then the depth of ${}^sD_T(4k + 1, K)$ is $\geq 2k + 1$.*

Conjecture 4.12. *Let K be an integral domain with unity such that K^* contains at least three elements. Then the depth of ${}^sD_T(4k + 1, K)$ is $2k + 1$.*

Proposition 4.13. *Let K be an integral domain with unity. Then the cycle indicator of ${}^sD(4k + 1, K)$ is at least $4k + 4$.*

Proposition 4.13 follows from the fact that the cycle indicator of $A(2k + 1, K)$, where K is an integral domain is at least $4k + 4$, (see IACR e-print archive [42]).

Conjecture 4.14. *Let K be an integral domain with unity such that K^* contains at least three elements. Then the cycle indicator of ${}^sD_T(4k + 1, K)$ is $4k + 4$.*

Conjecture 4.15. *Let K be an integral domain with unity. Then the girth of ${}^sD_T(4k + 1, K)$ is at least $2k + 6$.*

Let us consider the case of $n = 2k$.

We consider ${}^{2k}A = \{(1, 0), (0, 1), (1, 1), (1, 2), (2, 2), \dots, (k, k)\}$ of cardinality $2k + 1$ together with ${}^{2k}A^* = \{(2, 1), (2, 2)', (3, 2), \dots, (k, k)', (k + 1, k)\}$ of cardinality $2k - 1$. The set ${}^{2k}A \cup {}^{2k}A^*$ is the set of indices of the containing graph $D(4k - 1, K)$. Deletion of coordinates of points and lines indexed by $(k + 1, k)$ makes it isomorphic to $D(4k - 2, K)$.

Let ${}^{2k}A_s$ be the difference of ${}^{2k}A^*$ with the set $\Delta(2k, s)$ of the final s roots $(k + 1, k), (k, k)', \dots$ of ${}^{2k}A^*$ where $0 \leq s \leq 2k - 1$. We define the *chopped graph* ${}^sD(4k - 1, K)$ obtained via deletion of the coordinates of point and lines of $D(4k - 1)$ indexed by elements from $\Delta(2k, s)$ and the deletion of the corresponding equations of the incidence relation.

Let $J(2k, s)$ be the intersection of ${}^{2k+1}A_s$ with the set of roots $(2, 2)', (3, 3)', \dots$. We can select some nonempty subset T of $J(2k, s)$ such that $(i, i)' \in T$ implies that $(i + 1, i) \in {}^{2k}A_s$, and make the following truncation procedure.

Delete coordinates of the vertices ${}^sD(4k - 1, K)$ indexed by $(i, i)'$ from T , and change the equation indexed by $(i + 1, i)$ via the change of the variable indexed by $(i, i)'$ for the variable with index (i, i) .

Let us denote the graph obtained as ${}^sD_T(4k - 1, K)$.

Conjecture 4.16. *Let K be an integral domain with unity. Then the depth of ${}^sD_T(4k-1, K)$ is $\geq 2k$.*

Conjecture 4.17. *Let K be integral domain with unity such that K^* contains at least 3 elements. Then the depth of ${}^sD_T(4k-1, K)$ is $2k$.*

Proposition 4.18. *Let K be an integral domain with unity. Then the cyclic indicator of ${}^sD(4k+1, K)$ is at least $4k+2$.*

Conjecture 4.19. *Let K be integral domain with unity such that K^* contains at least 3 elements. Then the cycle indicator of ${}^sD_T(4k+1, K)$ is $4k+2$.*

Conjecture 4.20. *Let K be an integral domain with unity. Then the girth of ${}^sD_T(4k+1, K)$ is at least $2k+4$.*

Proposition 4.21. *Let (i, i) be the minimal root of T . There is a well defined homomorphism of ${}^sD_T(4k-1, K)$ onto $D(4i+1, K)$ obtained via the deletion of (i, i) together with higher roots of the graph.*

Corollary 4.22. *Let K be an integral domain. Then under the condition of the previous statement, the girth of the graph ${}^sD_T(4k-1, K)$ is at least $4i+6$.*

We denote the parameter i of the proposition as $m_T(k, s)$. Let us consider the family $G(k) = {}^{s(k)}D_T(k)(4k-1, K)$, $k = 1, 2, \dots$ such that for $t(k) = m_T(k)(k, s(k))$ the following condition holds: $t(k+1) > t(k)$. Then $G(k)$ is a family of graphs of unbounded girth. Note that if an increasing sequence of $t(k)$ is bounded below by ck where c , $0 < c < 4$ is positive constant, then $G(k)$ is a family of Jordan-Gauss graphs of large girth.

We can substitute graph $D(4k-1, K)$ for its connected component $C(4k-1, K)$ and apply the above procedures of deleting coordinates and modification of equations to C . Then we obtain the family $CG(k)$ of connected graphs of unbounded girth.

Conjecture 4.20 can be used for the following construction. Let K be an integral domain. Under the conjecture, the girth of $G(k) = {}^{s(k)}D_T(k)(4k-1, K)$ is at least $2k+4$. So the family $G(k)$ with arbitrarily chosen $s(k)$ and $T(k)$ is a family of large girth.

Remark. We can modify Proposition 4.21 and the following constructions via the change of $4k-1$ for $4k+1$.

Computer experiments support the conjecture that the second largest eigenvalues of graphs ${}^sD_T(4k-1, \mathbb{F}_q)$, ${}^sD(4k-1, \mathbb{F}_q)$, ${}^sD_T(4k+1, \mathbb{F}_q)$ and ${}^sD(4k+1, \mathbb{F}_q)$ are bounded above by $2\sqrt{q}$.

LDPC codes corresponding to members of family $A(n, \mathbb{F}_q)$ were investigated in [27] and [28]. Parameters of these codes turn out to be better than those of LDPC codes derived from graphs $CD(n, \mathbb{F}_q)$.

5 On homogeneous algebraic graphs of high girth

Let us start from the concept of an homogeneous algebraic graph. Let F be a field. Recall that a projective space over F is a set of elements constructed from a vector space over F such that a distinct element of the projective space consists of all non-zero vectors which are equal up to multiplication by a non-zero scalar. A subset Q is called a *quasiprojective variety* if it is the set of all solutions of some system of homogeneous polynomial equations and inequalities.

An algebraic graph Ψ over F consists of two things: the vertex set Q , being a quasiprojective variety over F of non-zero dimension; and the edge set being a quasiprojective variety Ψ in $Q \times Q$ such that (x, x) is not an element of Ψ for each x from Q , and $x\Psi y$ implies $y\Psi x$ (where $x\Psi y$ means (x, y) is an element of Ψ).

The graph Ψ is *homogeneous* (or N -homogeneous), if for each vertex w from Q , the set $\{x|w\Psi x\}$ is isomorphic to a quasiprojective variety $M(w)$ over F of a non-zero finite dimension N .

We further assume that each $M(w)$ contains at least 5 elements and the field F contains more than two elements. We refer to $\text{codim}(\Psi) = \dim(Q)/N$ as the *codimension* of an algebraic graph Ψ . The examples of affine algebraic graphs from the previous section in the case of the field K with at least 5 elements are examples of homogeneous algebraic graphs.

Studies of algebraic graphs with some restrictions on their cycles in the case of finite fields are motivated by extremal graph theory (see previous sections and corresponding references). Flag transitive geometries over arbitrary fields are classical objects of algebraic geometry; they are incidence graphs, i.e. simple graphs of binary relations defined over algebraic varieties over a field F such that their edge sets are also algebraic varieties over F . Rank two geometries are building bricks for geometries of higher rank. Their definitions are given in terms of girth and diameter. For example, the classical projective plane is a graph of girth 6 and diameter 3. Its vertex set is a disjoint union of one dimensional and two dimensional vector spaces of F^3 . Recall that J. Tits defined a *generalised m -gon* as a bipartite graph (or incidence structure) of girth $2m$ and diameter m [33].

It is noteworthy that geometries of Chevalley groups $A_2(F)$, $B_2(F)$ and $G_2(F)$ are generalised m -gons for $m = 3, 4$ and 6 .

Let us introduce some definitions of homogeneous algebraic graph theory. We refer to G as an *infinite algebraic graph* over K if G is a projective limit for the family G_i $i = 1, 2, \dots$ of k -homogeneous algebraic graphs for some positive integer k .

If G is a forest we say that the family G_i of k -homogeneous graphs is an *algebraic forest approximation* over the commutative ring K .

Let g_i stand for the girth of G_i . In the case where $g_i \geq cn_i$, where n_i are dimensions of the vertex sets $V(G_i)$ of the graphs G_i and c is some positive constant, we use the term *algebraic forest approximation of large girth*. If the G_i are connected, we use the term *algebraic tree approximation of large girth*.

In [31] it was proven that the girth of $D(n, F)$ defined over a field F of characteristic zero equals $2\lfloor(n+5)/2\rfloor$.

Other definitions of homogeneous algebraic graph theory are motivated by the following statement.

Theorem 5.1. [31] *Let G be a homogeneous algebraic graph over a field F with at least 5 elements of girth g such that the dimension of a neighbourhood for each vertex is $N, N \geq 1$. Then $\text{codim}(G) = \dim(Q)/N \geq \lfloor(g-1)/2\rfloor$.*

Note that the condition that the field contains at least five elements is important. The graph $D(4, \mathbb{F}_3)$ has codimension 4 and girth 12, so the inequality of the theorem does not hold in this case.

Theorem 5.2. *Let G be a homogeneous algebraic graph over a field F with at least 5 elements of depth k such that the dimension of a neighbourhood for each vertex is $N, N \geq 1$. Then $\text{codim}(G) = \dim(Q)/N \geq k$.*

Proof. Assume that the depth k is $> \dim(Q)/N$. Let v be a vertex of depth k and M be the variety of elements at distance k from v . The absence of cycles C_s , $1 \leq s \leq 2k$, means that each element from M is connected to v by a unique path of length k . Elements of M are in one to one correspondence with such paths. Let $N_v(F)$ be a neighbourhood of v . A path is a sequence v, u_1, u_2, \dots, u_k , where $u_1 \in N_v(F), u_2 \in N_{u_1}(F) - v, \dots, u_k \in N_{u_{k-1}}(F) - u_{k-2}$. So the dimension of M is $N \times k$. But $N \times k > \dim(Q)$ by our assumption, so we get a contradiction. \square

The natural analog of this theorem for finite simple graphs is the following statement.

Proposition 5.3. *Let $\text{dep}_k(m)$ be the minimal order of a k -regular graph with $k > 2$ of depth $m, m > 1$. Then $\text{dep}_k(m) \geq 1 + k + k(k-1) + k(k-1)^2 + \dots + k(k-1)^{m-1}$.*

The proof is obtained by considering a branching process starting from a vertex of maximal depth.

Conjecture 5.4. *Let $q, q > 3$ be a prime power. Then $\text{dep}_q(m) \leq 2q^m$.*

The above conjecture follows from the following assumption. We conjectured that the graph $A(n, q)$ of order $2q^n$ has depth n . Conjecture 5.4 follows from this assumption together with the following statement.

Conjecture 5.5. *Let $k, k > 2$ and $q = \mu(k)$ be a minimal prime power $\geq k$. Then $\text{dep}_k(m) \leq 2kq^{m-1}$.*

We say that a homogeneous algebraic graph G over a field F is a *deep algebraic graph* if its depth coincides with its codimension. Let $md(k), k \geq 2$ be the minimal codimension of a homogeneous algebraic graph of depth k .

Remark. Generalised m -gons of Chevalley graphs $A_2(F), B_2(F)$ and $G_2(F)$ are deep graphs of depth 2, 3 and 5 respectively.

Conjecture 5.6. *For each $k, k \geq 2$, the lower bound of Theorem 5.2 is sharp. So $md(k) = k$.*

Conjecture 5.7. *Graphs $A(n, F), n \geq 2$ defined over a field of cardinality at least 5 are deep Jordan-Gauss graphs.*

Theorem 5.8. *Graphs $A(n, F), n \leq 14$ defined over the field of cardinality 5 are deep Jordan-Gauss graphs.*

This result is obtained via computer calculation.

Corollary 5.9. *$md(k) = k$ for $k = 2, 3, \dots, 14$.*

We introduce $v(g)$ as the minimal value of $\text{codim}(G)$ for a homogeneous algebraic graph G defined over a field with at least 5 elements of girth g . We refer to $v(g)$ as the *algebraic rank* of girth g .

Corollary 5.10. *$v(g) \geq \lfloor (g-1)/2 \rfloor$.*

We refer to a graph G of girth g and $\text{codim}(G) = \lfloor (g-1)/2 \rfloor$ as an *algebraic cage*. In the case of a graph G of girth g and $\text{codim}(G) \leq \lfloor (g-1)/2 \rfloor$ we say that G is an *algebraic Moore graph*. We say that G is an *extraspecial algebraic Moore graph* if $\text{codim}(G) < \lfloor (g-1)/2 \rfloor$. (Such graphs can exist for $F = \mathbb{F}_3$ and $F = \mathbb{F}_4$. We have just one example: $D(4, \mathbb{F}_3)$ of girth 12.)

Theorem 5.11. (see [42]) Let $v(g)$ be the minimal codimension of a homogeneous algebraic graph of even girth $g = 2k + 2$, $k \geq 6$. Then $k \leq v(g) \leq (3k - 3 + e)/2$ where $e = 0$ if k is odd, and $e = 1$ if k is even. (Graphs $CD(n, F)$, $\text{char } F = 0$.)

Let $F \neq \mathbb{F}_2$ be a field. We define ${}^F v(g)$ as the minimal value of $\text{codim}(G)$ for an algebraic graph G over the field F with girth g . If $g \geq 6$ is even then ${}^F v(g)$ is at least $(g - 2)/2$, for each field F , $F \neq \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4$. The upper bound for ${}^F v(g)$ can be heavily dependent on the choice of field.

Theorem 5.12. (see [42]) There are algebraic Moore graphs of girth 6, 8, 10, 12 and 18 of codimensions 2, 3, 4, 5 and 8 respectively. (Regular generalised m -gons for $m = 3, 4, 6$ and graphs $A(4, 4), CD(9, 3)$.)

Remark. Instead of generalised triangles and quadrangles, one can take Jordan-Gauss graphs $D(2, F)$ and $D(3, F)$ (affine parts of generalised polygons).

Theorem 5.13. Let ${}^{\mathbb{F}_4} v(g)$ be the minimal codimension of a homogeneous algebraic graph defined over \mathbb{F}_4 of even girth $g = 2k + 2$, $k \geq 6$. Then ${}^{\mathbb{F}_4} v(g) \leq (3k - 3 + e)/2 - 1$ where $e = 0$ if k is odd, and $e = 1$ if k is even. (Graphs $C(n, \mathbb{F}_4)$ from [20].)

6 On the platforms of Noncommutative Cryptography formed by multivariate transformations

6.1 Some definitions

A classical multivariate public rule is a transformation of an n -dimensional vector space over a finite field \mathbb{F}_q which moves vector (x_1, x_2, \dots, x_n) to the tuple $(g_1(x_1, x_2, \dots, x_n), g_2(x_1, x_2, \dots, x_n), \dots, g_n(x_1, x_2, \dots, x_n))$, where the polynomials g_i are given in their standard forms, i.e. lists of monomial terms in the lexicographical order [14]. The degree of this transformation is the maximal value of $\text{deg}(g_i)$. Traditionally a public rule has degree 2 or 3. Degree 2 is preferable (RUOV algorithm claimed to provide ‘the shortest digital signatures’). Let us consider the following important object of Noncommutative Cryptography.

The Affine Cremona Semigroup ${}^n CS(K)$ is defined as the endomorphism group of the polynomial ring $K[x_1, x_2, \dots, x_n]$ over the commutative ring K (see [29] and further references). It is an important object of algebraic geometry (see [26] about the mathematics of Luigi Cremona, a prominent figure in algebraic geometry in the 19th century). An element σ of the semigroup can be given via its values on variables, i.e. as the rule $x_i \rightarrow f_i(x_1, x_2, \dots, x_n)$, $i = 1, 2, \dots, n$. This rule induces the map

$$\sigma : (a_1, a_2, \dots, a_n) \rightarrow (f_1(a_1, a_2, \dots, a_n), f_2(a_1, a_2, \dots, a_n), \dots, f_n(a_1, a_2, \dots, a_n))$$

on the free module K^n . Automorphisms of $K[x_1, x_2, \dots, x_n]$ form the affine Cremona Group ${}^n CG(K)$. In the case when K is a finite field, Boolean ring or arithmetic ring Z_m of residues modulo m , elements of affine Cremona Groups or Semigroups are used in algorithms of Multivariate Cryptography. Results about subsemigroups S of ${}^n CS(K)$ (or subgroups of ${}^n CG(K)$) such that computation of the superposition of arbitrary n elements can be completed in polynomial time can be used as so called *platforms of Noncommutative Cryptography*. One class of such objects is formed by stable subsemigroups of degree k , i.e. a subsemigroup S such that the maximal degree of its representative is bounded by the constant k . We will talk about Multiple Composition Computability (MCC) property. In the case of $k = 1$ one can take $AGL_n(K)$; stable subsemigroups of degree k in ${}^n CG(K)$ exist for each k , $k = 2, 3, \dots$

The Affine Cremona semigroup ${}^nCS(K)$ does not possess MCC. If one takes n quadratic elements randomly, their product (with probability close to 1) will have degree 2^n . So the computation is not feasible. We suggest the following stable cubical groups.

The families of graphs $D(n, K)$ defined over an arbitrary commutative ring K are linguistic bipartite graphs of type $(1, 1, n - 1)$ with partition sets which are two copies of K^n (see [43] or [37]), i.e. graphs with the incidence $I = I(K) = {}^nI(K)$ between points (x_1, x_2, \dots, x_n) and lines $[y_1, y_2, \dots, y_n]$ given by the system of equations

$$\begin{aligned} a_2x_2 - b_2y_2 &= f_2(x_1, y_1), \\ a_3x_3 - b_3y_3 &= f_3(x_1, x_2, y_1, y_2), \\ &\dots, \\ a_nx_n - b_ny_n &= f_n(x_1, x_2, \dots, x_{n-1}, y_1, y_2, \dots, y_{n-1}), \end{aligned}$$

where the parameters a_2, a_3, \dots, a_n and b_2, b_3, \dots, b_n are taken from the multiplicative group K^* of the commutative ring K .

Parameters $\rho((x_1, x_2, \dots, x_n)) = x_1$ and $\rho([y_1, y_2, \dots, y_n]) = y_1$ serve as *colours* of the point and the line. The following linguistic property holds: each vertex of the graph has a unique neighbour of the chosen colour. The following statement follows instantly from the definitions.

Proposition 6.1. *Let K be a commutative ring with unity. Then the Jordan-Gauss graphs ${}^sD_T(4k - 1, K)$, ${}^sD(4k - 1, K)$, ${}^sD_T(4k + 1, K)$, ${}^sD(4k + 1, K)$ are linguistic graphs of type $(1, 1, n)$ for $n = 4k - 2$ and $n = 4k$ respectively.*

Let us consider the general scheme of creating the cipher based on the family of linguistic graphs ${}^nI(K)$, $n = 2, 3, \dots$. Note that we can expand $I(K)$ as defined above to the infinite linguistic graph $I(K[x_1, x_2, \dots, x_n])$ defined over the ring $K[x_1, x_2, \dots, x_n]$ of all multivariate polynomials with coefficients from K and the variables x_i , $i = 1, 2, \dots, n$. So the points and lines of this graph are

$$\begin{aligned} X &= (X_1(x_1, x_2, \dots, x_n), X_2(x_1, x_2, \dots, x_n), \dots, X_n(x_1, x_2, \dots, x_n)) \text{ and} \\ Y &= [Y_1(x_1, x_2, \dots, x_n), Y_2(x_1, x_2, \dots, x_n), \dots, Y_n(x_1, x_2, \dots, x_n)]. \end{aligned}$$

The incidence of this bipartite graph is given by equations

$$\begin{aligned} a_2X_2 - b_2Y_2 &= f_2(X_1, Y_1), \\ a_3X_3 - b_3Y_3 &= f_3(X_1, X_2, Y_1, Y_2), \\ &\dots, \\ a_nX_n - b_nY_n &= f_n(X_1, X_2, \dots, X_{n-1}, Y_1, Y_2, \dots, Y_{n-1}), \end{aligned}$$

where the parameters $a_2, a_3, \dots, a_n, b_2, b_3, \dots, b_n$ and polynomials f_i , $i = 2, 3, \dots, n$ with coefficients from K are taken from the equations in the definition of the linguistic graph $I(K)$.

We define the polynomial map F from K^n to K^n via the following scheme (see [40]). Take the special point $X = (x_1, x_2, \dots, x_n)$ of $I(K[x_1, x_2, \dots, x_n])$ and consider the list of colours $g_1(x_1), g_2(x_1), \dots, g_t(x_1)$. We compute the path $v_0Iv_1Iv_2 \dots Iv_t$ where $v_0 = X$ and v_{i+1} is the neighbour of v_i with the colour $g_i(x_1)$, $i = 1, 2, \dots, t$ and $I = I(K[x_1, x_2, \dots, x_n])$. Then the destination point v_t of this path can be written as $(g_t(x_1), F_2(x_1, x_2), \dots, F_n(x_1, x_2, \dots, x_n))$. The map F is given by the rule $x_1 \rightarrow g_t(x_1)$, $x_2 \rightarrow F(x_1, x_2)$, \dots , $x_n \rightarrow F(x_1, x_2, \dots, x_n)$. It is easy to see that $F = F(g_1, g_2, \dots, g_t)$ is a bijective map if and only if the equations of the kind $g_t(x_1) = b$ have unique solutions for unknown x_1 for each b from K .

Let $S(I(K))$ be a subsemigroup of ${}^nSC(K)$ formed by transformations of the kind $F = F(g_1, g_2, \dots, g_t)$ and $G(I(K))$ be the subgroup of $S(I(K))$ formed by transformations of the

kind $F = F(g_1, g_2, \dots, g_t)$ for which $g_t \in {}^1SC(K)$ (see [40]).

Let $G_0(I(K))$ be the subgroup generated by transformations $F = F(g_1, g_2, \dots, g_t)$ with g_i of the kind $x_1 + c$ where $c \in K$. It is known that $G_0(D(n, K))$ and $G_0(A(n, K))$ are stable cubic subgroups of ${}^nCG(K)$ (see [47, 45] and [40]). Their applications to Noncommutative Cryptography can be found in [44] and [40]. Transformations from T_1GT_2 where G is $G_0(D(n, K))$ or $G_0(A(n, K))$ and $T_i, i = 1, 2$ can be used as encryption maps of Stream Ciphers. We prove that

Proposition 6.2. *Groups $G_0({}^sD(n, K))$, $n = 1$ or $3 \pmod{4}$ are stable cubic subgroups of ${}^{n-s}CG(K)$.*

Computer experiments support the following.

Conjecture 6.3. *Groups $G_0({}^sD_T(n, K))$, $n \equiv 1$ or $3 \pmod{4}$ are stable cubic subgroups of ${}^{n-s}CG(K)$.*

These two statements justify the use of transformations from the groups $G_0({}^sD(n, K))$ and $G_0({}^sD_T(n, K))$ in Noncommutative Cryptography and Symmetric Cryptography. For instance, we can modify the stream cipher of [44] via the change of encryption transformation from $G_0(D(n, K))$ for an element of $G_0({}^sD(n, K))$ or $G_0({}^sD_T(n, K))$. This obfuscation leads to an increase in the security level of the cipher.

We can obfuscate the key exchange protocol of Noncommutative Cryptography presented in [44] via the change of transformation group $G_0(D(n, K))$ for $G_0({}^sD(n, K))$ or $G_0({}^sD_T(n, K))$. This change allows us to work with the hidden platform of Noncommutative Cryptography instead of a known one. Various cryptographic algorithms based on graphs $D(n, K)$ and $A(n, K)$ can be found in [40]. Each of them can be obfuscated via the change of these graphs on ${}^sD(n, K)$ for ${}^sD_T(n, K)$.

Declarations

Competing interests

The authors have no relevant financial or non-financial interests to disclose.

Funding

This research is supported by British Academy/Cara/Leverhulme Research Support grant LTRSF\100333.

Data availability

The data sets generated in the course of this research are available on request from the corresponding author.

References

- [1] N. Biggs, *Algebraic graph theory*, Second Edition, Cambridge University Press, 1993.

- [2] B. Bollobás, *Extremal Graph Theory*, Academic Press, London, 1978.
- [3] B. Bollobás, *Random Graphs*, Academic Press, London, 1985.
- [4] N. Bourbaki, *Lie Groups and Lie Algebras*, Chapters 1 - 9, Springer, 1998-2008.
- [5] A. Brouwer, A. Cohen, A. Neumaier, *Distance regular graphs*, Springer, Berlin, 1989.
- [6] F. Buekenhout (Editor), *Handbook on Incidence Geometry*, North Holland, Amsterdam, 1995.
- [7] R. W. Carter, *Simple Groups of Lie Type*, Wiley, New York, 1972.
- [8] D. Charles, K. Lauter, and E. Z. Goren. *Cryptographic Hash Functions from Expander Graphs* Journal of Cryptology, 2008. doi: 10.1007/s00145-007-9002-x.
- [9] A. Costache, B. Feigon, K. Lauter, M. Massierer, A. Puskás *Ramanujan graphs in cryptography*, arXiv:1806.05709.
- [10] Z. Füredi, F. Lazebnik, A. Seress, V. A. Ustimenko, and A. J. Woldar, *Graphs of Prescribed Girth and Bi-degree*, J. of Combin. Theory Ser. B Vol. 64, No. 2, (1995) 228–239.
- [11] P. Guinand and J. Lodge, *Tanner Type Codes Arising from Large Girth Graphs*, Proceedings of the 1997 Canadian Workshop on Information Theory (CWIT 97), Toronto, Ontario, Canada, pp. 5–7, June 3–6, 1997.
- [12] P. Guinand and J. Lodge, *Graph Theoretic Construction of Generalized Product Codes*, Proceedings of the 1997 IEEE International Symposium on Information Theory (ISIT 97), Ulm, Germany, p. 111, June 29–July 4, 1997.
- [13] S. Hoory, N. Linial, and A. Wigderson, *Expander graphs and their applications*, Bulletin (New Series) of AMS, volume 43, N4, 439–461.
- [14] N. Koblitz, *Algebraic aspects of Cryptography*, in Algorithms and Computations in Mathematics, v. 3, Springer, 1998.
- [15] F. Lazebnik, V. Ustimenko, *Some Algebraic Constructions of Dense Graphs of Large Girth and of Large Size*, DIMACS series in Discrete Mathematics and Theoretical Computer Science , v. 10, (1993) 75–93.
- [16] F. Lazebnik, V. Ustimenko, *New Examples of Graphs without Small Cycles and of Large Size* Europ. J. of Combinatorics(1993) 14, 445–460.
- [17] F. Lazebnik, V. Ustimenko, *Explicit construction of graphs with arbitrary large girth and of large size*, Discrete Applied Mathematics 60 (1995), 275–284.
- [18] F. Lazebnik, V. Ustimenko, A. J. Woldar, *A new series of dense graphs of high girth*, Bull. Amer. Math. Soc. (N.S.) 32 (1995), no. 1, 73–79.
- [19] F. Lazebnik, V. Ustimenko and A. Woldar, *A Characterization of the Components of the graphs $D(k, q)$* , Discrete Math. 157 (1996), 271–283.
- [20] F. Lazebnik, R. Viglione, *On the connectivity of certain graphs of high girth*. Discrete Math., 277 (2004), 309–319.
- [21] A. Lubotzky, *Discrete Groups, Expanding graphs and invariant measures*, Progress in mathematics 125, Birkhauser, 1994.

- [22] A. Lubotzky, R. Phillips and P. Sarnak, *Ramanujan graphs*, *Combinatorica*, September 1988, Volume 8, Issue 3, 261–277.
- [23] G. A. Margulis, *Explicit construction of graphs without short cycles and low density codes*, *Combinatorica*, 2, (1982), 71–78.
- [24] D. J. C. MacKay, *Good error correcting codes based on very sparse matrices*, *IEEE Trans. Information Theory*, 399–431, March 1999.
- [25] D. MacKay and M. Postol, *Weakness of Margulis and Ramanujan Margulis Low Density Parity Check Codes*, *Electronic Notes in Theoretical Computer Science*, 74 (2003), 8 pp.
- [26] M. Noether, *Luigi Cremona*, *Mathematische Annalen*, 59 (1904), 1–19.
- [27] M. Polak, V. Ustimenko, *On LDPC Codes corresponding to affine parts of generalized polygons*, *Annales UMCS Informatica AI X1*, 2 (2011), 143–150.
- [28] M. Polak, V. Ustimenko, *On LDPC Codes Corresponding to Infinite Family of Graphs $A(k, K)$* , *Proceedings of the Federated Conference on Computer Science and Information System (FedCSIS)*, CANA 2012.
- [29] V. L. Popov, *Roots of the affine Cremona group*, in: *Affine Algebraic Geometry*, Seville, Spain, June 1821, 2003, *Contemporary Mathematics*, Vol. 369, American Mathematical Society, Providence, RI, 2005, 12–13.
- [30] U. Romanczuk, V. Ustimenko, *On regular forests given in terms of algebraic geometry, new families of expanding graphs with large girth and new multivariate cryptographical algorithms*, *Proceedings of Applications of Computer Algebra ACA 2013. M´alaga July 2nd-6th, 2013*, 144–147., <http://www.aca2013.uma.es/Proceedings.pdf>
- [31] T. Shaska, V. Ustimenko, *On the homogeneous algebraic graphs of large girth and their applications*, *Linear Algebra and its Applications Article*, Volume 430, Issue 7, 1 April 2009, Special Issue in Honor of Thomas J. Laffey.
- [32] R. Michiel Tanner, *A recursive approach to low density codes*, *IEEE Trans.on Info Th., IT*, 27(5), 533–547, Sept.1984
- [33] J. Tits, *Sur la trialite at certains groupes qui sen deduicent*, *Publ. Math. I.H.E.S.* 2 (1959), 15–20.
- [34] V. Ustimenko, *On a group theoretical construction of expanding graphs*, *Algebra and Discrete Mathematics*, Vol 2, No 3 (2003).
- [35] V. Ustimenko, *New results on algebraic graphs of large girth and their impact on Extremal Graph Theory and Algebraic Cryptography*, *IACR e-print archive*, 2022/1489.
- [36] V. Ustimenko, *On extremal graph theory and symbolic computations*, *Dopovidi National Academy of Sci, Ukraine*, -2013, N2, 42–49.
- [37] V. Ustimenko, *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, *Journal of Mathematical Sciences*, Springer, vol.140, N3 (2007), 412–434.
- [38] V. Ustimenko, *Algebraic groups and small world graphs of high girth*, *Albanian Journal of Mathematics*, 2009, 3 (1), 26–33.

- [39] V. Ustimenko, *CRYPTIM: Graphs as Tools for Symmetric Encryption*, Lecture Notes in Computer Science, Springer, LNCS 2227, Proceedings of AAECC-14 Symposium on Applied Algebra, Algebraic Algorithms and Error Correction Codes, November 2001, 278–286
- [40] V. Ustimenko, *Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world*, Maria Curie-Sklodowska University Publishers, 2022. ISBN 978-83-227-9655-9.
- [41] V. Ustimenko, *Coordinatisation of Trees and their Quotients*, in the Voronois Impact on Modern Science, Kiev, Institute of Mathematics, 1998, vol. 2, 125–152.
- [42] V. Ustimenko, *On the families of algebraic graphs with the fastest growth of cycle indicator and their applications*, ACR e-print archive, 2022/1668.
- [43] V. Ustimenko, *Maximality of affine group, hidden graph cryptosystem and graphs stream ciphers*, Journal of Algebra and Discrete Mathematics, 2005, vol.1, 51–65.
- [44] V. Ustimenko, M. Klisowski, *On new protocols of Noncommutative Cryptography in terms of homomorphism of stable multivariate transformation groups*, Journal of Algebra and Discrete Mathematics, 220–250, DOI: 10.12958/adm1523, <https://admjournal.luguniv.edu.ua/index.php/adm/issue/view/88>
- [45] V. Ustimenko, U. Romanczuk *On Extremal Graph Theory, Explicit Algebraic Constructions of Extremal Graphs and Corresponding Turing Encryption Machines*, in “Artificial Intelligence, Evolutionary Computing and Metaheuristics”, In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Vol. 427, Springer, January, 2013, 257–285.
- [46] B. L. Van Der Waerden, *Algebra*, Vol 1, Springer V, 2011.
- [47] A. Wroblewska, *On some properties of graph based public keys*, Albanian Journal of Mathematics, Volume 2, Number 3, 2008, 229–234.

Appendix — computational results

Field	Dimension	Components	Eccentricity	Depth	Local girth	λ_2	
\mathbb{F}_3	4	1	8	5	12	2.53209	
	5	1	12	5	12	2.71519	
	6	3	12	5	12	2.71519	
	7	3	12	5	12	2.78066	
	8	3	14	5	12	2.78205	
	9	3	17	8	18	2.78205	
	10	9	17	8	18	2.78205	
	11	9	22	8	18	2.82290	
	12	9	22	8	18	2.82290	
	13	9	24	8	18	2.84088	
	14	27	24	8	18	2.84088	
	15	27	26	9	20	2.84958	
	16	27	26	9	20	2.84958	
	17	27	28	11	24	2.84958	
	18	81	28	11	24		
	19	81	30	11	24		
	20	81	32	13	28		
	\mathbb{F}_4	4	4	6	3	8	2.82843
		5	4	8	4	10	3.16228
		6	16	8	4	10	3.16228
7		16	10	5	12	3.46410	
8		16	12	5	12	3.46410	
9		16	16	6	14	3.64575	
10		64	16	6	14	3.64575	
11		64	16	7	16	3.64575	
12		64	18	7	16	3.64575	
13		64	20	8	18	3.64575	
14		256	20	8	18	3.64575	
15		256	20	9	20	3.64575	
16		256	22	9	20		

Table 1: Properties of $D(n, q)$ for $q = 3, 4$

Field	Dimension	Components	Eccentricity	Depth	Local girth	λ_2
\mathbb{F}_5	4	1	8	3	8	3.61803
	5	1	12	4	10	4.03112
	6	5	12	4	10	4.03112
	7	5	12	5	12	4.03112
	8	5	12	5	12	4.03112
	9	5	14	6	14	4.03112
	10	25	14	6	14	4.03112
	11	25	15	7	16	4.03112
	12	25	16	7	16	4.06587
\mathbb{F}_7	4	1	8	3	8	4.74094
	5	1	10	4	10	4.81302
	6	7	10	4	10	4.81302
	7	7	11	5	12	4.93326
	8	7	12	5	12	4.93326
	9	7	14	6	14	5.19394
	10	49	14	6	14	
\mathbb{F}_8	4	1	8	3	8	5.65685
	5	1	10	4	10	5.65685
	6	8	10	4	10	5.65685
	7	8	11	5	12	5.65685
	8	8	12	5	12	5.65685
	9	8	14	6	14	
	10	64	14	6	14	
\mathbb{F}_9	4	1	8	3	8	5.22668
	5	1	10	4	10	6.00000
	6	9	10	4	10	6.00000
	7	9	11	5	12	6.00000
	8	9	12	5	12	6.00000
	9	9	14	6	14	
	10	81	14	6	14	

Table 2: Properties of $D(n, q)$ for $q = 5, 7, 8, 9$

Field	Dimension	# comp	Eccentricity		Depth		Local girth		
			min	max	min	max	min	max	
\mathbb{F}_3	4	1	8	8	3	4	8	12	
	5	1	12	12	5	5	12	12	
	6	1	12	13	5	6	12	14	
	7	1	15	16	5	7	12	16	
	8	1	16	18	5	8	12	18	
	9	1	18	20	7	8	16	20	
	10	1	20	22	7	9	16	20	
	11	1	22	22	7	10	16	24	
	12	1	23	24	7	11	16	24	
	13	1	25	26	9	12	20	28	
	14	1	27	27	9	13	20	28	
	15	1	28	29	9	14	20	30	
	16	1	30	32	9	15	20	32	
	17	1	32	33	11	14	24	32	
\mathbb{F}_4	4	1	8	8	4	4	10	10	
	5	1	10	10	5	5	12	12	
	6	1	12	12	5	6	12	14	
	7	1	12	14	6	7	14	16	
	8	1	14	16	6	7	14	16	
	9	1	16	18	7	9	16	20	
	10	1	16	20	7	10	16	22	
	11	1	18	22	8	11	18	24	
	12	1	20	23	8	11	18	24	
	13	1	22	25	9	12	20	26	
	14	1	22	27	9	11	20	24	
	\mathbb{F}_5	4	1	8	8	3	4	8	10
		5	1	8	10	4	5	10	12
		6	1	10	12	4	6	10	14
7		1	12	14	5	7	12	16	
8		1	12	16	5	7	12	16	
9		1	14	18	6	9	14	20	
10		1	16	19	6	8	14	18	
11		1	18	21	7	10	16	22	
12		1	18	22	7	9	16	20	
13		1	20	24	8	11	18	24	
\mathbb{F}_7	4	1	8	8	3	4	8	10	
	5	1	8	10	4	5	10	12	
	6	1	10	12	4	5	10	12	
	7	1	12	13	5	6	12	14	
	8	1	12	16	5	7	12	16	
	9	1	14	17	6	7	14	16	
	10	1	16	19	6	8	14	18	

Table 3: Properties of $A(n, q)$ for $q = 3, 4, 5, 7$

Field	Dimension			# comp	Eccentricity		Depth		Local girth	
	orig	chops	final		min	max	min	max	min	max
\mathbb{F}_3	7	1	6	1	12	12	5	5	12	12
	9	1	8	3	14	14	5	6	12	16
	9	2	7	1	14	14	5	6	12	16
	11	1	10	3	22	22	8	8	18	18
	11	2	9	3	17	18	7	7	16	16
	11	3	8	1	17	18	7	7	16	16
	13	1	12	9	22	22	8	8	18	18
	13	2	11	3	22	22	8	8	18	18
	13	3	10	3	20	20	7	8	16	18
	13	4	9	1	20	20	7	8	16	18
	15	1	14	9	26	26	9	9	20	20
	15	2	13	9	24	24	9	9	20	20
	15	3	12	3	24	24	9	9	20	20
	15	4	11	3	22	22	7	9	16	20
	15	5	10	1	22	22	7	9	16	20
	17	1	16	27	28	28	11	11	24	24
	17	2	15	9	28	28	11	11	24	24
	17	3	14	9	24	24	10	10	22	22
	17	4	13	3	24	24	10	10	22	22
	17	5	12	3	22	23	7	10	16	22
	17	6	11	1	22	23	7	10	16	22
	19	1	18	27	30	30	11	11	24	24
	19	2	17	27	28	28	11	11	24	24
	19	3	16	9	28	28	11	11	24	24
	19	4	15	9	26	26	11	11	24	24
	19	5	14	3	26	26	11	11	24	24
	19	6	13	3	23	24	9	11	20	24
	19	7	12	1	23	24	9	11	20	24
	21	1	20	81	30	31	11	12	24	28
	21	2	19	27	30	31	11	12	24	28
21	3	18	27	29	30	11	12	24	28	
21	4	17	9	29	30	11	12	24	28	
21	5	16	9	27	28	11	12	24	28	
21	6	15	3	27	28	11	11	24	24	
21	7	14	3	25	26	9	11	20	24	
21	8	13	1	25	26	9	11	20	24	

Table 4: Properties of chopped graphs for $q = 3$

Field	Dimension			# comp	Eccentricity		Depth		Local girth	
	orig	chops	final		min	max	min	max	min	max
\mathbb{F}_4	7	1	6	4	10	10	5	5	12	12
	9	1	8	16	12	12	5	6	12	14
	9	2	7	4	12	12	5	6	12	14
	11	1	10	16	16	16	7	7	16	16
	11	2	9	16	12	14	6	7	14	16
	11	3	8	4	12	14	6	7	14	16
	13	1	12	64	18	18	7	8	16	18
	13	2	11	16	18	18	7	8	16	18
	13	3	10	16	14	16	6	8	14	18
	13	4	9	4	14	16	6	8	14	18
	15	1	14	64	20	20	9	9	20	20
	15	2	13	64	18	20	8	9	18	20
	15	3	12	16	18	20	8	9	18	20
	15	4	11	16	16	18	7	9	16	20
	15	5	10	4	16	18	7	9	16	20
	17	1	16	256	20	22	9	10	20	22
	17	2	15	64	20	22	9	10	20	22
	17	3	14	64	19	22	8	10	18	22
	17	4	13	16	19	22	8	10	18	22
	17	5	12	16	16	20	7	10	16	22
	17	6	11	4	16	20	7	10	16	22
	19	3	16	64	22	24	10	11	22	24
	19	4	15	64	20	24	9	11	20	24
	19	5	14	16	20	24	9	11	20	24
	19	6	13	16	18	21	8	10	18	22
	19	7	12	4	18	21	8	10	18	22
	21	5	16	64	22	26	9	12	20	26
	21	6	15	16	22	25	9	11	20	24
	21	7	14	16	20	24	8	12	18	26
	21	8	13	4	20	23	8	10	18	22

Table 5: Properties of chopped graphs for $q = 4$

Field	Dimension			# comp	Eccentricity		Depth		Local girth	
	orig	chops	final		min	max	min	max	min	max
\mathbb{F}_5	7	1	6	1	12	12	5	5	12	12
	9	1	8	5	12	14	5	6	12	14
	9	2	7	1	12	14	5	6	12	14
	11	1	10	5	15	16	7	7	16	16
	11	2	9	5	14	16	6	7	14	16
	11	3	8	1	14	16	6	7	14	16
	13	1	12	25	16	18	7	8	16	18
	13	2	11	5	16	18	7	8	16	18
	13	3	10	5	15	18	6	8	14	18
	13	4	9	1	15	18	6	8	14	18
	15	1	14	25	20	20	9	9	20	20
	15	2	13	25	18	20	8	9	18	20
	15	3	12	5	18	20	8	9	18	20
	15	4	11	5	16	19	7	8	16	18
	15	5	10	1	16	20	7	9	16	20
	17	3	14	25	19	22	8	10	18	22
	17	4	13	5	19	22	8	10	18	22
	17	5	12	5	18	21	7	9	16	20
	17	6	11	1	18	22	7	10	16	22
	19	5	14	5	20	24	9	11	20	24
	19	6	13	5	19	23	8	10	18	22
19	7	12	1	19	24	8	11	18	24	
21	7	14	5	20	25	8	11	18	24	
21	8	13	1	21	25	8	11	18	24	

Table 6: Properties of chopped graphs for $q = 5$

Field	Dimension			# comp	Eccentricity		Depth		Local girth	
	orig	chops	final		min	max	min	max	min	max
\mathbb{F}_7	7	1	6	1	11	12	5	5	12	12
	9	1	8	7	12	14	5	6	12	14
	9	2	7	1	12	14	5	6	12	14
	11	1	10	7	15	16	7	7	16	16
	11	2	9	7	14	16	6	7	14	16
	11	3	8	1	14	16	6	7	14	16
	13	2	11	7	16	18	7	8	16	18
	13	3	10	7	15	17	6	7	14	16
	13	4	9	1	15	18	6	8	14	18
	15	4	11	7	16	20	7	9	16	20
	15	5	10	1	16	19	7	8	16	18
	17	6	11	1	18	20	7	8	16	18

Table 7: Properties of chopped graphs for $q = 7$

Field	Dimension			# comp	Eccentricity		Depth		Local girth	
	orig	trunc	final		min	max	min	max	min	max
\mathbb{F}_3	7	1	6	1	12	12	5	5	12	12
	8	1	7	1	14	14	5	5	12	12
	9	1	8	1	17	17	8	8	18	18
	10	1	9	1	20	20	8	8	18	18
	11	1	10	1	22	22	8	8	18	18
	11	2	9	1	22	22	8	8	18	18
	12	1	11	1	24	24	8	8	18	18
	12	2	10	1	22	22	8	8	18	18
	13	1	12	1	24	24	8	8	18	18
	13	2	11	1	24	24	8	8	18	18
	14	1	13	1	28	28	8	8	18	18
	14	2	12	1	24	24	8	8	18	18
	15	1	14	1	30	30	11	11	24	24
	15	2	13	1	26	26	9	9	20	20
	15	3	12	1	26	26	9	9	20	20
	16	1	15	1	30	30	11	11	24	24
	16	2	14	1	28	28	9	10	20	24
	16	3	13	1	26	26	9	9	20	20
	17	1	16	1	31	32	11	11	24	24
	17	2	15	1	29	29	11	11	24	24
	17	3	14	1	28	28	11	11	24	24
	18	1	17	1	34	34	11	11	24	24
	18	2	16	1	30	32	11	11	24	24
	18	3	15	1	28	29	11	11	24	24
	19	1	18	1	34	36	11	11	24	24
	19	2	17	1	32	32	11	11	24	24
	19	3	16	1	30	31	11	11	24	24
	19	4	15	1	29	30	11	11	24	24

Table 8: Properties of truncated graphs for $q = 3$

Field	Dimension			# comp	Eccentricity		Depth		Local girth	
	orig	trunc	final		min	max	min	max	min	max
\mathbb{F}_4	7	1	6	4	10	10	5	5	12	12
	8	1	7	4	12	12	5	5	12	12
	9	1	8	4	12	14	6	7	14	16
	10	1	9	8	14	16	6	7	14	16
	11	1	10	32	14	16	6	7	14	16
	11	2	9	16	12	14	6	7	14	16
	12	1	11	32	14	16	6	7	14	16
	12	2	10	16	14	16	6	7	14	16
	13	1	12	32	16	18	6	8	14	18
	13	2	11	16	16	18	6	8	14	18
	14	1	13	32	17	18	7	8	16	18
	14	2	12	16	16	18	6	8	14	18
	15	1	14	32	18	20	8	9	18	20
	15	2	13	16	18	19	8	8	18	18
	15	3	12	16	16	20	8	9	18	20
	16	1	15	32	20	20	8	9	18	20
	16	2	14	16	19	20	8	9	18	20
	16	3	13	16	18	20	8	9	18	20
	17	2	15	16	20	23	8	10	18	22
17	3	14	16	19	24	8	11	18	24	
18	3	15	16	20	23	8	10	18	22	
19	4	15	64	19	23	8	10	18	22	

Table 9: Properties of truncated graphs for $q = 4$

Field	Dimension			# comp	Eccentricity		Depth		Local girth	
	orig	trunc	final		min	max	min	max	min	max
\mathbb{F}_5	7	1	6	1	12	12	5	5	12	12
	8	1	7	1	12	12	5	5	12	12
	9	1	8	1	12	14	6	6	14	14
	10	1	9	1	14	14	6	6	14	14
	11	1	10	1	16	16	7	7	16	16
	11	2	9	1	14	16	7	7	16	16
	12	1	11	1	16	18	7	7	16	16
	12	2	10	1	16	16	7	7	16	16
	13	1	12	1	18	18	8	8	18	18
	13	2	11	1	16	18	7	8	16	18

Table 10: Properties of truncated graphs for $q = 5$