On new results on Extremal Algebraic Graph Theory and their connections with Algebraic Cryptography

Vasyl Ustimenko

Royal Holloway University of London
Institute of Telecommunication and Global Information Space, Kyiv, Ukraine
vasylustimenko@yahoo.pl

↪

Abstract. Homogeneous algebraic graphs defined over arbitrary field are classical objects of Algebraic Geometry. This class includes geometries of Chevalley groups $A_2(F)$, $B_2(F)$ and $G_2(F)$ defined over arbitrary field F. Assume that codimension of homogeneous graph is the ratio of dimension of variety of its vertices and the dimension of neighbourhood of some vertex. We evaluate minimal codimension $v(g)$ and $u(h)$ of algebraic graph of prescribed girth g and cycle indicator. Recall that girth is the size of minimal cycle in the graph and girth indicator stands for the maximal value of the shortest path through some vertex. We prove that for even h the inequality $u(h) \leq (h-2)/2$ holds. We define a class of homogeneous algebraic graphs with even cycle indicator h and codimension $(h-2)/2$. It contains geometries $A_2(F)$, $B_2(F)$ and $G_2(F)$ and infinitely many other homogeneous algebraic graphs.

Keywords: commutative integrity rings, homogeneous algebraic graphs, codimension, girth indicator, girth.

Funding: This research is supported by British Academy Fellowship for Researchers at Risk 2022.

1 On Turan type problems for finite simple graphs

The missing definitions of Graph Theory reader can find in [1] or [2]. We assume that all graphs under consideration are simple graphs, i. e. undirected graphs without loops and multiple edges.

Classical Extremal Graph Theory (see [1], [19]) developed by P. Erds' and his school had been started with the following problem formulated by Turan. What is the maximal value $ex(v, C_{2n})$ for the size (number of edges) of graph on v vertexes without cycles C_{2n} of length $2n$? Other important question is about maximal size $ex(v, C_3, C_4, \ldots, C_{2n}, C_{2n+1})$ of a graph of order v without cycles of length 3, 4, ..., $2n+1$, i.e. graphs of girth $\geq 2n+2$. Recall that girth of the graph is minimal length of its cycle. According to P. Erdős' Even Circuit Theorem $ex(v, C_{2n}) = O(v^{1+1/n})$.

Studies of lower bounds for $ex(v, C_{2n})$, $ex(v, C_3, C_4, \ldots, C_{2n}, C_{2n+1})$ or $ex(v, C_3, C_4, \ldots, C_{2n})$ form important direction of Extremal Graph Theory. Recall that the family G_i, $i = 1, 2, \ldots$ of k-regular simple graphs of increasing order v_i is a *family of graphs of large girth* if the girth $g(i)$ of graph G_i are at least $clog_{k-1}(v_i)$ for some independent positive constant c.

We refer to family G_i, $i = 1, 2, \ldots$ of k-regular simple graphs of increasing order v_i as a family of *small world graphs* if the diameter $d(i)$ of graph Gi are at most $clog_{k-1}(v_i)$ for some independent positive constant c. Noteworthy that there is exactly one known construction of finite regular family of finite small world graphs of large girth with an arbitrarily large degree q. This is the family $X(p, q)$ formed by Cayley graphs for $PSL_2(p)$, where p and q are primes, had been defined by G. Margulis [3] and investigated by A. Lubotzky, Sarnak and Phillips [4].

We say that family G_i of k-regular graphs of increasing girth is a *finite forest approximation* if there is a well defined projective limit of these graphs, i. e for each i, $i > 1$ there is a graph homomorphism of G_i onto G_{i-1}. Noteworthy that the projective limit G of these graphs is a k-regular forest.

If each G is a tree then each graph G_i is a connected graph. In this case we refer to the sequence G_i as tree approximation. First example of forest approximation was defined in [5], [6]. Corresponding sequence of edge transitive graphs form a family of large girth $D(n, q)$, $n = 2, 3, \ldots$ with projective limit $D(q)$. So all trees of the forest $D(q)$ are isomorphic. Description of the tree $CD(q)$ of this forest in terms of equations and its tree approximation $CD(n, q)$ are presented in [7] for the case of odd prime powers q. Family $CD(n, q)$, $n = 2, 3, \ldots$ is a family of large girth, correspondent constant c is evaluated as $4/3log_q(q-1)$. Noteworthy that projective limit of $X(p, q)$ does not exist, so these Cayley-Ramanujan graphs are not tree approximation of large girth and are not small world approximation of an infinite tree.

2 On special Turan type problems for homogeneous algebraic graphs

Let us start from the concept of 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 a multiplication by a non-zero scalar. Its subset 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 Φ 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 Φ in QQ such that (x, x) is not element of Φ for each x from Q, and $x\Phi y$ implies $y\Phi x$ ($x\Phi y$ means (x, y) is an element of Φ).

The graph Φ is homogeneous (or N-homogeneous), if for each vertex w from Q, the set $\{x|w\Phi x\}$ is isomorphic to some quasiprojective variety $M(w)$ over F of a non-zero dimension N. We further assume that each $M(w)$ contains

at least 3 elements and field F contains more than two elements. We refer to $codim(\Phi) = dim(Q)/N$ as codimension of an algebraic graph Φ.

Studies of algebraic graphs with some restrictions on their cycles (see [22]) are motivated by the following 3 areas in Mathematics.

Investigations in the case of finite case are motivated by Extremal Graph Theory.

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 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 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 [24]. J. Tits defined generalised m-gons as a bipartite graph of girth $2m$ and diameter m. These objects are constructing bricks for the creation of geometries over diagrams with more that two nodes (see [25], [26], [27], [28]). 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. Studies of families $G_i(F)$ of homogeneous algebraic graphs defined over the field F with well defined projective limits $G(F)$ when n tends to infinity form an interesting direction of Algebraic Geometry. The cases when $G(F)$ is a forest or a tree are especially important. Investigations of growth of order of maximal or minimal cycles in $G_i(F)$ are naturally required in this cases

In probability theory *branching process* is a special stochastic process corresponding to random walk on regular forest Forr, i. e. simple graph without cycles with vertexes of the same degree of finite or infinite of cardinality > 2. The genealogy of single vertex is a tree.

The forest Forr itself is a deterministic part of branching process.

A possibility to define Forr by system of equations over some field of special commutative ring K i.e. as a projective limit of homogeneous algebraic graphs G_i, $i = 1, 2, \ldots$ of increasing girth defined over K motivate special direction of Infinite Network Theory.

Let us introduce some definitions of homogeneous algebraic graph theory

We refer to G as infinite algebraic graph over K if G is a projective limit for the family G_i, $i = 1, 2, \ldots$ of k - homogeneous algebraic graphs.

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

Let g_i stands for the girth of G_i.

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

Let G be a connected graph and d_i stands for the diameter of G_i. In the case $d_i \leq cn_i$, where n_i are dimensions of the vertex sets $V(G_i)$ of the graph G_i and c is some positive constant we use term *algebraic G- approximation via small world graphs.*

The existence of tree approximations defined over arbitrary field is proven.

Noteworthy that the algebraic forest approximation over finite field is a family of finite graphs of large girth in the sense of P. Erdős'.

The first example of the family of graphs of large girth over arbitrary field was introduced in [8] where was stated that graphs $D(n, K)$ over arbitrary infinite integrity ring have girth $\geq 2[(n+5)/2]$. This fact was proven in [9]. A bit more compact prove without usage of terminology of linguistic dynamic systems theory is given recently in [10].

Noteworthy that together with $D(n, K)$, $n = 2, 3, \ldots$ one can consider another families $D(n, K[x_1, x_2, \ldots, x_m])$ for each parameter m. It opened a possibility to use extremal properties of these graphs in the Theory of Symbolic Computations. In [11] it was proven that the girth of $D(n, F)$ defined over the field F of characteristic zero equals $2[(n+5)/2]$.

Note that small world approximation of infinite algebraic graph over finite field is a family of small world graphs in sense of [12].

The first small world approximation of infinite algebraic graph was presented in [13], where projective limit of Wenger graph $W(n, F)$ where F is an infinite field was investigated.

Other definitions of Homogeneous Algebraic Graph Theory are motivated by the following statement.

THEOREM 2.1.[11]

Let G be the homogeneous algebraic graph over a field F of girth g such that the dimension of a neighbourhood for each vertex is N, $N \geq 1$. Then $codim(G) = dim(Q)/N \geq [(g-1)/2]$.

We introduce $v(g)$ as minimal value of $codim(G)$ for homogeneous algebraic graph G of girth g. We refer to $v(g)$ as *algebraic rank* of girth g.

COROLLARY 2.1.

$v(g) \geq [(g-1)/2]$

We refer to graph G of girth g and $codim(G) = v(g)$ as *algebraic cage.*

In the case of graph G of girth g and $codim(G) = [(g-1)/2]$ we say that G is *algebraic Moore graph.*

THEOREM 2. 2.

Let $v(g)$ be the minimal codimension of homogeneous algebraic graph of even girth $g = 2k+2$, $k \geq 6$. Then $k \leq v(g) \leq [3k/2+1]$.

Let F be a field $F \neq F_2$. We introduce $Fv(g)$ as minimal $codim(G)$ for algebraic graph G over the field F with girth g.

If g, $g \geq 6$ is even then ${}^F v(g)$ is at least $(g-2)/2$, for each field F, FF_2. The upper bound for ${}^F v(g)$ can be heavy dependable from the choice of field. For each even m we introduce $t(m)$ as minimal codimension of homogeneous algebraic graph without cycle C_m. Let ${}^F t(m)$ stands for the minimal codimension of the homogeneous algebraic graph defined over the field F Noteworthy that $t(m) \leq v(m+2)$. The following conjecture is motivated by Even Circuit Theorem.

CONJECTURE 2. 1.

The inequality $t(m) \geq m/2$ holds.

We refer to the written above inequality as Even Circuit Inequality (ECI).

THEOREM 2.3.

Let F be a field with at least 3 elements, $m = 2k$ be an even integer Assume that ${}^F\tilde{v}(m)$ be the minimal codimension of homogeneous algebraic graph over the field, m be an even integer ≥ 4 such that its girth is $> m$. Then ${}^F\tilde{v}(m) \leq [3k/2 + 1]$.

COROLLARY 2.2.

Let F be a field with at least 3 elements. Let ${}^Ft(m)$ be the minimal codimension of homogeneous algebraic graph without cycles of length $m = 2k$, $k \geq 6$. Then ${}^Ft(m) \leq [3k/2 + 1]$

Importance of rank 2 finite geometries over diagrams A_2, B_2 and G_2 for Extremal Graph Theory was noticed in [17]. The following statement follows instantly from the definition of algebraic Moore graphs and definitions of geometries of simple groups of Lie type (see [18]). Noteworthy that incidence graphs of geometries of Chevalley groups $A_2(F)$, $B_2(F)$ and $G_2(F)$ over arbitrary field F are algebraic Moore graphs.

In the next section the family $A(n, F)$ of 1-homogeneous algebraic bipartite graphs with partition sets F^n will be defined. The girth of $A(n, F_4)$ for $n = 4, 5, 6, 7, 8, 9$ was computed (see [16]). It turns out that $A(4, F_4)$ is algebraic Moore graph of girth 10. Some conjectures connected with these 4 exceptional graphs are formulated in [10].

Justification of Theorem 2.2 and 2.3 and some statements about ${}^Fv(m)$ will be given in Section 4.

3 Another optimization problem for finite or homogeneous algebraic graphs

Problems on evaluation of girth and diameter of k-regular simple graph with $k \geq 3$ are well known. Additionally we consider following optimization minimax problems for graphs.

(1) Investigate cycle indicator $h(v)$ of the vertex v of the k-regular graph G, i. e. the minimal length of cycle through this vertex v.

(2) Find the cycle indicator $h(G)$ of the graph which is maximal value of cycle indicators of vertexes of the graph.

As it instantly follows from the definitions $h(G) \geq g(G)$, where $g(G)$ stands for the girth of the graph, which is minimal size of a cycle of G.

We say that family G_i, $i = 1, 2, \ldots$ of increasing order v_i is a family with large girth indicator if cycle indicator $h(i)$ of graph G_i are at least $clog_{k-1}(v_i)$ for some independent positive constant c.

Similarly we say that family of homogeneous algebraic graphs G_i, $i = 1, 2, \ldots, n$ defined over the field F with increasing dimension d_i of vertex sets $V(G_i)$ such that the neighbourhood of each vertex of G_i. has fixed dimension N independent from parameter i is an algebraic family of graphs with large cycle indicator if cycle indicator $h(i)$ of graph G_i are at least cd_i for some positive constant i.

As it follows from definitions each family of graphs (or algebraic graphs) of large girth is a family of graphs (algebraic graphs) with large circle indicator. So

quite many examples of such families are known (see [7] and further references) In Section 1we introduce a family of algebraic graphs over arbitrary field F with the large circle indicator with constant $c = 2$. If $F = F_q$ this is the family of finite graphs with large circle indicator and constant $c = 2log_q(q-1)$.

Let G be k-homogeneous algebraic graph over field F with the vertex set $V(G)$ and with the girth indicator h Let ${}^F u(h)$, $h \geq 6$ be the minimal codimension for variety of such graphs defined over the field F. We consider $u(h)$ as minimal value of ${}^F u(h)$ via all fields F with at least 3 elements. Noteworthy that ${}^F u(h) \geq (h)$.

THEOREM 3.1.

For each even h, $h \geq 6$ the inequality $u(h) \leq (h-2)/2$ holds.

Justification of this statement will be given via evaluation of cycle indicator of graphs $A(n, F)$ defined below . The evaluations of ${}^F u(h)$ for special fields F are also given in the next section.

CONJECTURE 3.1.

The bound of Theorem 3.1 is sharp, i. e. $u(h) = (h-2)/2$ for even h, $h \geq 6$.

Let K be a commutative ring . We define $A(n, K)$ as bipartite graph with the point set $P = K^n$ and line set $L = K^n$ (two copies of a Cartesian power of K are used). We will use brackets and parenthesis to distinguish tuples from P and L.

So $(p) = (p_1, p_2, \ldots, p_n) \in P_n$ and $[l] = [l_1, l_2, \ldots, l_n] \in L_n$.

The incidence relation $I = A(n, K)$ (or corresponding bipartite graph I) is given by condition pIl if and only if the equations of the following kind hold.

$p_2 l_2 = l_1 p_1$,
$p_3 - l_3 = p_1 l_2$,
$p_4 l_4 = l_1 p_3$,
$p_5 l_5 = p_1 l_4$, (1)
$\ldots$,
$p_n l_n = p_1 l_{n-1}$ for odd n and $p_n l_n = l_1 p_{n-1}$ for even n.

We can consider an infinite bipartite graph $A(K)$ with points
$(p_1, p_2, \ldots, p_n, \ldots)$ and lines $[l_1, l_2, \ldots, l_n, \ldots]$.

We proved the following statement.

THEOREM 3.2. (see [10] and further references).

Let K be an integrity ring. Then for each odd $n \geq 3$ a cycle indicator of graph $A(n, K)$ is at least $2n + 2$.

In the case when K coincides with F_q graphs $A(n, F_q)$ are q-regular, they form a family of graphs with large cycle indicator, appropriate constant c can be written as $2log_q(q-1)$.

We prove inequality $h(A(n, K)) \geq 2n + 2$ via computation of $h(v)$ for the vertex v (point or line) given by the tuple (0, 0, $\ldots$, 0). Computer simulation indicates that if $n > 6$ then cycle indicators of 0-point and 0-line are different, one of them is $2n+2$ but other is $2n$. It means that graphs are not vertex transitive, their girth differs from the cycle indicator in investigated via computer simulation cases.

CONJECTURE 3.2.

Let F be a field with at least 3 elements. Then for each odd $n \geq 3$ a cycle indicator of graph $A(n, F)$ is $2n + 2$.

The inequality ${}^F u(h) \leq (h-2)/2$ for each even parameter h instantly follows from the Conjecture 3.2. The following statement supports Conjecture 3.2.

THEOREM 3. 3.

Let k , $k > 3$ be an odd number. There are infinitely many fields F such that girth indicator of $A(k, F)$ is $2k + 2$.

Justification of this statement is given in the next section.

Theorem 3.1 instantly follows from Theorem 3.3.

Let ${}^F\tilde{u}(m)$ be a minimal dimension of homogeneous algebraic graph over F with the girth indicator $> m$.

THEOREM 3. 4.

For each odd m of kind $2k+1$, $k \geq 1$ and each field F the following inequality holds. ${}^F\tilde{u}(m) \leq (m + 1)/2$

This statement instantly follows from Theorem 3.2

We refer to homogeneous algebraic graphs over field F with even cycle indicator h of codimension $(h - 2)/2$ as cyclonic graphs.

Class of cyclonic graphs contains geometries of Chevalley groups $A_2(F)$, $B_2(F)$, $G_2(F)$ (known flag transitive generalised m-gons for $m = 3, 4$ and 6 in the case of arbitrary field F). Other examples give some representatives of known family of graphs $A(n, F)$ defined above. Noteworthy that in the cases of generalised polygons their girth coincides with the cyclic indicator, but in well investigated via computer simulation cases of graphs $A(n, F_q)$, $q = 3$, $q = 4$ and $q = 5$ and odd parameters n from the intervals $[7, 27]$, $[7, 15]$ and $[7, 13]$ these parameters are distinct. Computer simulation was conducted by Prof. G. Erskine.

We define Cyclic gap of graph G as the difference between cycle indicator $Cind(G)$ and $Girth(G)$. Investigation of cyclic gaps of $A(n, F)$ is an interesting open problem of Algebraic Geometry.

4 On relations of $A(n, K)$ with other known families of graphs

Graphs $A(m, K)$ were obtained in [9] 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 kind

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

and the totality L' of lines of kind

$y = [y] = [y_{0,1}, y_{1,1}, y_{1,2}, y_{2,2}, \dots, y_{i,i}, y_{i,i+1}, \dots]$. We assume that tuples (x) and $[y]$ has 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:

$x_{i,i} - y_{ii} = y_{i-1,i}x_{1,0}$,

$x_{i,i+1} - y_{i,i+1} = y_{0,1}x_{i,i}$ (2)

where $i = 1, 2, \dots$.

We denote the graph of this incidence structure as $A(K)$. We consider the set *Root* of indexes 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 root system $\tilde{A}_1$ of affine type. We see that $Root = \{(1,0), (0,1), (11), (12), (22), (23), \dots\}$. So we introduce $R_{1,0} = Root - \{0,1\}$ and $R_{0,1} = Root - \{(1,0)\}$. It allows us to identify sets P' and L' with affine subspaces $\{f : R_{1,0} \to K\}$ and $\{f : R_{0,1} \to K\}$ of functions with finite supports.

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 $A'(k, K)$. The comparison of equations of $A'(k, K)$ and $A(k, K)$ allows to justify the isomorphism of these graphs. It is convenient for us to identify graphs $A(k, K)$ with incidence structures I_k defined via relations (2).

The procedure to delete last coordinates of points and lines of graph $A(n, K)$ defines the homomorphism ${}^n\Delta$ of $A(n, K)$ onto $A(n-1, K)$, $n > 2$. The family of these homomorphisms defines natural projective limit of $A(n, K)$ which coincides with $A(K)$. We introduce the colour function ρ on vertexes of graph $A(K)$ or $A(n, K)$ as x_{10} for the point $(x_{10}, x_{11}, x_{12}, \dots)$ and y_{01} for the line $[y_{01}, y_{11}, x_{12}, \dots]$. We refer to $\rho(v)$ for the vertex v as *colour* of vertex v.

As it follows directly from definitions for each vertex v and each colour $a \in K$ there is exactly one neighbour of v with the colour a. We refer to this fact as linguistic property of graphs $A(n, K)$ and $A(K)$. In fact such property were used for the definition of the class of linguistic graphs (see [9] and further references). The family of graphs $D(n, K)$, $n = 2, 3, \dots$ where K is arbitrary commutative ring defines the projective limit $D(K)$ with points $(p) = (p_{10}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, \dots, p'_{ii}, p_{ii+1}, p_{i+1,i}, p_{i+1,i+1}, \dots)$, and lines $[l] = [l_{01}, l_{11}, l_{12}, l_{21}, l_{22}, l'_{22}, \dots, l'_{ii}, l_{ii+1}, l_{i+1,i}, l_{i+1,i+1}, \dots]$.

which can be thought as infinite sequences of elements in K such that only finitely many components are nonzero.

A point (p) of this incidence structure I is incident with a line $[l]$, i.e. $(p)I[l]$, if their coordinates obey the following relations:

$$p_{i,i} - l_{i,i} = p_{1,0} l_{i-1,i},$$
$$p'_{i,i} - l'_{i,i} = p_{i,i-1} l_{0,1},$$
$$p_{i,i+1} - l_{i,i+1} = p_{i,i} l_{0,1}, \quad (3)$$
$$p_{i+1,i} - l_{i+1,i} = p_{1,0} l'_{i,i}.$$

(These four relations are well defined for $i > 1$, $p_{1,1} = p'_{1,1}$, $l_{1,1} = l'_{1,1}$.)

Let D be the list of indexes of the point of the graph $D(K)$ written in their natural order, i. e. sequence $(1,0)$, $(1,1)$, $(1,2)$, $(2,1)$, $(2,2)$,$(2,2)'$,$\dots$.$Let^k D$ be the list of k first elements of D. The procedure of deleting coordinates of points and lines of $D(k, K)$ indexed by elements of $D -^k D$ defines the homomorphism of $D(K)$ onto graph $D(k, K)$ with the partition sets isomorphic to the variety K^n and defined by the first $k-1$ equations from the list (3). We can see that the

procedure of deleting of coordinates indexed by elements $D - (Root - \{(0,1)\})$ defines the homomorphism of graph $D(K)$ onto $A(K)$.

Let us consider the set ${}^kA =^k D -^k D \cap Root$. The procedure of deleting coordinates of vertexes of $D(k,K)$ indexed by elements of ${}^kA$ defines the homomorphism η_k of $D(k,K)$ onto $A(m,k)$ where m is the cardinality of ${}^kD \cap Root$.

Let $k \geq 6$, $t = [(k+2)/4]$, and let $u = (u_i, u_{11}, \ldots, u_{tt}, u'_{tt}, u_{t,t+1}, u_{t+1,t}, ...)$ be a vertex of $D(k,K)$. We assume that $u_1 = u_{1,0}(u_{0,1})$ if u be a point (a line, respectively). It does not matter whether u is a point or a line. For every r, $2 \leq r \leq t$, let $a_r = a_r(u) = \Sigma_{i=0,r}(u_{ii}u'_{r-i,r-i}u_{i,i+1}u_{r-i,r-i-1})$ and $a = a(u) = (a_2, a_3, \ldots, a_t)$.

The following statement was proved in [7] for the case K = F_q. Its generalization on arbitrary commutative rings is straightforward, see [9].

PROPOSITION 4.1.

Let K be a commutative ring with unity and u and v be vertices from the same connected component of $D(k,K)$. Then $a(u) = a(v)$. Moreover, for any $t1$ ring elements $x_i \in K$, $2 \leq i \leq [(k+2)/4] = t$, there exists a vertex v of $D(k,K)$ for which $a(v) = (x_2, x_3, \ldots, x_t) = (x)$.

So the classes of equivalence for the relation$\tau = \{(u,v)|a(u) = a(v)\}$ on the vertexes of the graph. $D(n,K)$ are unions of connected components.

THEOREM 4.1 [9]. *For each commutative ring with unity, the graph $D(k,K)$ is edge transitive.*

Equivalences classes of τ form an imprimitivity systems of automorphism group of $D(k,K)$. Graph $C(n,K)$ was introduced in [8] as the restriction of incidence relation of $D(k,K)$ on a solution set of system of homogeneous equations $a_2(x) = 0$, $a_3(x) = 0$, ..., $a_t(x) = 0$. The dimension of this algebraic variety is $n - t = d$. Thus $d = [4/3n] + 1$ for $n = 0, 2, 3$ *mod* 4, $d = [4/3n] + 2$ for $n = 1$ *mod* 4. For convenience we assume that $C(n,K) = C_d(K)$ Symbol $CD(k,K)$ stands for the connected component of graph $D(k,K)$. The following statement was proven in [9].

THEOREM 4.2 [14].

The diameter of the graph $C_m(K)$, $m \geq 2$, K is a commutative ring with unity of odd characteristic is bounded by parameter $f(m)$ which does not depend on K defined by the following equations.

COROLLARY 4. 1.

If K is a commutative ring with unity then $CD(n,K) = C(n,K)$.

COROLLARY 4. 2.

For each natural n family $C(n,F_q)$ where q run through all odd prime powers is a family of small world graphs of unbounded degree, i.e. diameter of member of the family is bounded by some independent constant.

COROLLARY 4.3.

Let K be a commutative ring with unity of odd characteristic, then $\eta_k(D(k,K) = \eta_k(CD(k,K) = A(m,K)$, where m is cardinality of ${}^kD \cap Root$. So graphs $A(m,K)$ are connected.

The girth of graph $D(k,K)$ is computed only for special integrity ring with unity. The following two propositions are well known.

THEOREM 4. 3. ([15])

Let k be odd, and q be any prime power in the arithmetic progression $\{1 + n(k+5)/2\}$, $n = 1, 2, \ldots$. Then the girth of $D(k, F_q)$ is $k + 5$.

THEOREM 4. 4 ([11]).

Let k be odd, and Pbe the arithmetic progression $P = \{1 + n(k+5)/2\}$, $n = 1, 2, \ldots$. Then

(i) for each integrity ring F of prime characteristic $p \in P$ or 0 the girth of the graph $D(k, F)$ is $k + 5$;

(ii) there is an integer function $n(k)$ such that for each commutative integrity ring K with unity such that $char(K) \geq n(k)$ the girth of the graph $D(n, K)$ is $k + 5$.

Noteworthy that $D(m, F_q)$ is induced subgraph of $D(m, F_{q^s})$ and the following statement instantly follows from Theorem 4.3.

COROLLARY 4.4.

Let parameters m and q satisfy condition of Theorem 4. 3 and $s \geq 1$. Then the girth of $D(m, F_{q^s})$ is $m + 5$.

The usage of this corollary allows us to formulate the following statement on existence of infinitely many finite cyclonic graphs

THEOREM 4.5.

Let k be odd, and q be any prime power in the arithmetic progression $\{1 + n(k+5)/2\}$, $n = 1, 2, \ldots$ and s is integer ≥ 1. Then cycle indicator of $A(r, F_{q^s})$, $r = (k+3)/2$ is $2s + 2$.

Proof.

Let v be some vertex of $A(r, F_{q^s})$. Assume that u be a reimage of v for the homomorphism η_m of the graph $D(k, F_{q^s})$ onto $A(r, F_{q^s})$. Edge transitivity of $D(k, F_q)$ and Corollary 4.4 insure that there is a cycle C through the vertex u of length $m + 5$. The closed walk $\eta(C)$ contains vertex v. So cycle indicator of v has length $\leq 2r + 2 = k + 5$. Theorem 3.2 insures that cycle indicator equals $2r + 2$.

The following statement on the existence of other examples of cyclonic graphs can be deduced from the Theorem 4.2.

THEOREM 4. 6.

Let k be odd, and P be the arithmetic progression $P = \{1 + n(k+5)/2\}$, $n = 1, 2, \ldots$. Then

(i) for each integrity ring $F$of prime characteristic $p \in P$ or 0 the cycle indicator of $A(s, F)$ is $2s + 2$ where $s = (k+3)/2$.

(ii) there is an integer function $n(k)$ such that for each commutative integrity ring K with unity such that $char(K) \geq n(k)$ the girth indicator of the graph $A(s, F)$ is $2s + 2$.

The proof of this statement is similar to justification of Theorem 4.3. Theorem 3.3 follows instantly from Theorem 4.3. or Theorem 4.4.

Proof of Theorems 2.2 and 2.3.

Assume that n is integer ≥ 2. We know that girth of graph $D(n, K)$ defined over arbitrary integrity ring K is $\geq 2[(n+5)/2]$. As it follows from the edge transitivity of $D(n, K)$ vertex sets of graphs isomorphic to $C(n, K)$ forms par-

tition of $K^n \cup K^n$ into classes of equivalence relation τ . Each of these classes is a unions of several connected components of $D(n, K)$. Let C be a shortest cycle in $D(n, K)$. The connected component containing C belongs to some class. Thus without loss of generality we can assume that C belongs to $C(n, K)$. So we prove that the girth of $D(n, K)$ and $C(n, K)$ is the same even integer. Let K be a field. The set of vertices for $C(n, K)$ is a subvariety $K^n \cup K^n$ defined and $t-1$ equations of kind $a_2(x) = 0$, $a_3(x) = 0$, ..., $a_t(x) = 0$. It means that dimension of the vertex set of $C(n, K)$ is $n - t + 1$.

For simplicity we assume that parameter n is odd and K is the field different from F_2. So graph $C(n, K)$ does not contains cycles of length $n-3$, $n = 2k+1$, graph does not contain cycles of length $2k-2$. Its dimension coincides with the codimension and we obtain the upper bound for ${}^F t(2k-2)$. It gives us the proof of theorem 2.3. Now we take one of the fields for which the girth of $D(2k+1, F)$ is $2k+6$. We evaluate ${}^F v(2k+6)$ and use inequality $v(2k+6) {}^F v(2k+6)$.

THEOREM 4.7.

$6 \leq v(14) \leq {}^{F_4} v(14) \leq 7$

It follows from the fact that the girth of algebraic graph $A(7, F_4)$ equals to 14 (see [16]).

CONJECTURE 4.1.

$v(14) = 7$ *and* $A(7, F_4)$ *is an algebraic cage.*

5 On Extremal Algebraic Graphs and Cryptography based on multivariate maps over commutative rings

Extremal algebraic graphs were traditionally used for the construction of stream ciphers of multivariate nature (see [32] and further references, [33] and [16] where multivariate maps of unbounded degree were used). Described above graphs $D(n, K)$ and $A(n, K)$ were intensively used. Later first graph based multivariate public keys with injective encryption maps were suggested in [34], [35]. These constructions use graphs $A(n, K)$ and $D(n, K)$ together with Eulerian transformation of K^n to produce public rule as multivariate transformation of linear degree and polynomial density. So they differs from classical constructions of multivariate public rules of degree 2 or 3 which were investigated during NIST standartisation project started in 2017.

This project starts the standardisation process of possible Post-Quantum Public keys aimed for purposes to be (i) encryption tools, (ii) tools for digital signatures (see [29]).

In July 2020 the Third Round of the competition started. In the category of Multivariate Cryptography (MC) remaining candidates are easy to observe. For the task (i) multivariate algorithm was not selected, single multivariate candidate is "The Rainbow Like Unbalanced Oil and Vinegar" (RUOV) digital signature method. As you see RUOV algorithm was investigated as appropriate instrument for the task (ii). Due to this investigation RUOV was not selected for the next 4th round of NIST competition. In 2022 first 4 winners of the NIST competition

were selected. So NIST certification do not select any of algorithm of Multivariare Cryptography.

Noteworthy that all multivariate NIST candidates were presented by multivariate rule of degree bounded by constant (2 or 3) of kind $x_1 \to f_1(x_1, x_2, \ldots, x_n)$, $x_2 \to f_2(x_1, x_2, \ldots, x_n)$, $\ldots$, $x_n \to f_n(x_1, x_2, \ldots, x_n)$. In fact RUOV is given by quadratic system of polynomial equations.

We think that NIST outcomes motivate investigations of alternative options in Multivariate Cryptography oriented on encryption tools for

(a) the work with the space of plaintexts ${F_q}^n$ and its transformation G of linear degree cn, $c > 0$ on the level of stream ciphers or public keys

(b) the usage of protocols of Noncommutative Cryptography with platforms of multivariate transformations for the secure elaboration of multivariate map G from $End(F_q[x_1, x_2, \ldots, x_n])$ of linear or superlinear degree and density bounded below by function of kind cn^r, where $c > 0$ and $r > 1$.

We hope that these alternative options together with classical multivariate public key approach are able to bring reliable encryption algorithms.

Recall that the density is the number of all monomial terms in a standard form $x_i \to g_i(x_1, x_2, \ldots, x_n)$, $i = 1, 2, \ldots, n$ of multivariate map G, where polynomials g_i are given via the lists of monomial terms in the lexicographical order.

We use presented above family of small world graphs $A(n.q)$, connected graphs $CD(n, q)$ and their analogs $A(n, K)$ and $CD(n, K)$ defined over finite commutative ring K with unity for the construction of multivariate group $GA(n, K)$ of transformations of K^n.

It can be used as platform for postquantum protocols of Noncommutative Cryptography (see [30]) and creation of multivariate protocol based cryptosystems. This approach allows to convert graph based symmetric ciphers to protocol based asymmetric algorithms of El Gamal type (see [31]).

Presented above results on the girth of linguistic graphs $A(n, K)$ and $D(n, K)$ over commutative integrity ring can be used for investigation of groups $GA(n, K)$ and $GD(n, K)$ and other subgroups and subsemigroups of transformations of K^n defined via walks in graphs $A(n, K)$, $D(n, K)$ and $A(n, K[x_1, x_2, \ldots, x_n])$, $D(n, K[x_1, x_2, \ldots, x_n])$. Some statements about degrees of elements of these semigroups are already obtained. So studies of girth and girth indicators of graph $A(n, K)$ and $D(n, K)$ make essential impact on studies of corresponding graph based ciphers of Multivariate nature and properties of Asymmetric Cryptosystems which use these graphs.

1. B. Bolloba's, *Extremal Graph Theory*, London Math. Soc. Monograph, Academic Press, 1978.
2. A. Brower, A. Cohen, A. Nuemaier, *Distance Regular Graphs*, Springer, Berlin, 1989.
3. G. Margulis, *Explicit group-theoretical constructions of combinatorial schemes and their application to desighn of expanders and concentrators*, Probl. Peredachi Informatsii 24 (1) 5160. English translation: J. Prob. Inform. Trans., 1988, pp. 39–46.
4. A. Lubotsky, R. Philips, P. Sarnak, *Ramanujan graphs.* J. Comb. Theory, 1989, 115 (2), 62–89.

5. F. Lazebnik and V. A. Ustimenko, *New examples of graphs without small cycles and of large size*, European J. Combin., 14, 445–460 (1993).
6. F. Lazebnik and V. Ustimenko, *Explicit construction of graphs with an arbitrary large girth and of large size*, Discrete Appl. Math., 60, 275–284 (1995).
7. F. Lazebnik, V. A. Ustimenko, and A. J. Woldar, *A new series of dense graphs of high girth,* Bull. Amer. Math. Soc. (N.S.), 32, No. 1, 73–79 (1995).
8. V. A. Ustimenko, *Coordinatisation of regular tree and its quotients,* in: Voronois Impact on Modern Science, P. Engel and H. Syta (eds.), Book 2, National Acad. of Sci, Institute of Mathematics (1998).
9. V. Ustimenko, *On linguistic dynamical systems, graphs of large girth and cryptography,* J. Math. Sci. 140 (3) (2007) 412–434.
10. V. Ustimenko, *On the families of algebraic graphs with the fastest growth of cycle indicator and their applications*, IACR e-print Archive, 2022/1668.
11. T. Shaska, V. Ustimenko, *Linear Algebra and its Applications*, 430 (2009) 1826–1837.
12. B. Bollobas', *Random Graphs*, Academic Press, London, 1985.
13. V. Futorny, V. Ustimenko, *On small world semiplanes with generalised Schubert cells*, Acta Applicandae Mathematicae, 98, N1 (2007) 47–61.
14. V. Ustimenko, *Algebraic groups and small world graphs*, Albanian Journal of Mathematics,Volume 3, Number 1 (2009), Pages 25–33.
15. Z. Fu'redi, F. Lazebnik, A. Seress, V.A. Ustimenko, A.J. Woldar, *Graphs of prescribed Girth and Bi-Degree*, J. Combin. Theory, Ser. B 64 (2) (1995) 228–239.
16. Tymoteusz Chojecki, Vasyl Ustimenko , *On fast computations of numerical parameters of homogeneous algebraic graphs of large girth and small diameter and encryption of large files*, IACR e-print Archive, 2022/908.
17. C.T. Benson, *Minimal regular graphs of girth eight and twelve*, Canad. Journal of Mathematics, . 18. 1966. P. 1091–1094.
18. R. W. Carter, *Simple Groups of Lie Type*, Wiley, New York (1972).
19. M. Simonovits, *Extremal graph theory*, in: Selected Topics in Graph Theory, 2, L. W. Beineke and R. J. Wilson (eds.), Academic Press, London (1983), pp. 161–200.
20. P. Erdős' and H. Sachs, , *Regul are Graphen gegebener Taillenweite mit minimaler Knotenzahl,* Wiss. Z. Martin-Luther-Univ. Halle-Wittenberg Math.-Natur. Reihe, 12, 251–257 (1963).
21. J. A. Bondy and M. Simonovits, *Cycles of even length in graphs*, J. Combin.Theory. Ser. B. 16. 1974. P. 87–105.
22. N. Biggs, *Algebraic Graph Theory*, 2nd edition, Cambridge Univ. Press, Cambridge (1993).
23. N.Biggs, *Graphs with large girth*, Ars Combin., 25C, 73–80 (1988).
24. P. Dembovski, *Finite Geometries*, Springer, Berlin, 1968.
25. J.A. Thas, *Generalised polygons*, in: F. Buekenhout (Ed.), Handbook in Incidence Geometry, North-Holland, Amsterdam, 1995 (Chapter 9).
26. J. Tits, *Sur la trialite et certains groupes qui sen deduisent*, Publ. Math. I.H.E.S 2 (1959) 15–20.
27. J. Tits, R. Weiss, *Moufang Polygons*, Springer-Verlag, 2002.
28. F. Buekenhout (editor), *Handbook in Incidence Geometry*, Ch. 9, North Holland, Amsterdam, 1995.
29. *Post-Quantum Cryptography: Call for Proposals:https://csrc.nist.gov/*, Project: Post-Quantum-Cryptography-Standardization/Call-for-Proposals, Post-Quantum Cryptography: Round 2 Submissions.
30. Alexei G. Myasnikov; Vladimir Shpilrain; Alexander Ushakov. *Non-commutative Cryptography and Complexity of Group-theoretic Problems*. Amer. Math Soc. 2011.

31. V. Ustimenko, *On new symbolic key exchange protocols and cryptosystems based on hidden tame homomorphism*, Reports of. Nath. Acad. Sci. of Ukraine, 2018, n 10, pp. 26–36.
32. M. Polak, U. Romanczuk, V. Ustimenko and A. Wrblewska , *On the applications of Extremal Graph Theory to Coding Theory and Cryptography*, Erd' Centennial, Proceedings of Erdős' Centennial (EP 100), Electronic Notes in Discrete Mathematics,V43, P. 329–342, 2013.
33. V. Ustimenko, *Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world*, UMCS Editorial House, Lublin, 2022, 198 p.
34. V. Ustimenko, *On new multivariate cryptosystems based on hidden Eulerian equations over finite fields*, IACR e-print Atchive, 2017/093.
35. V. A. Ustimenko, *On new multivariate cryptosystems based on hidden Eulerian equations*, Reports of National Academy of Sci of Ukraine, N5, 2017.