On the families of algebraic graphs with the fastest growth of cycle indicator and their applications

Vasyl Ustimenko

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

↪

Abstract. Symbolic computations with the usage of bipartite algebraic graphs $A(n, F_q)$ and $A(n, F_q[x_1, x_2, \ldots, x_n])$ were used for the development of various cryptographic algorithms because the length of their minimal cycle (the girth) tends to infinity when n is growing. It motivates studies of graphs $A(n, K)$ defined over arbitrary integrity ring K. We show that the cycle indicator of $A(n, K)$, i. e. maximal value of minimal cycles through the given vertex is $\geq 2n + 2$. We justify that the girth indicator of line $[0, 0, \ldots, 0]$ of $A(n, K)$ is $> 2n$, the girth indicator of point $(0, 0, \ldots, 0)$ of this graph is at least $2n$. From this result instantly follows that the girth of known edge transitive graphs $D(n, K)$ defined over integrity ring K is at least $2([n + 5]/2)$. We consider some inequalities defined in terms of a girth, a diameter and the girth indicator of homogeneous algebraic graphs and formulate some conjectures.

1 Some corollaries and remarks on applications

Let K be commutative integrity ring containing at least two elements. We consider nonempty subsets R and S of $K[x_1, x_2, \ldots, x_n]$, $n \geq 1$ Let ${}^{R,S}A(n, K[x_1, x_2, \ldots, x_n]$ be the induced subgraph of $A(n, K)$ of all points and lines with colours from R and S respectively. According to famous result by D. Hilbert $K[x_1, x_2, \ldots, x_n]$ is also an integrity ring. So the girth of infinite graph A(n, K[$x_1, x_2, \ldots, x_n$]) is $\geq 2n$ and the following statement holds.

PROPOSITION 2.1.
The girth of graph ${}^{R,S}A(n, K[x_1, x_2, \ldots, x_n])$ *is at least* $2n$.

COROLLARY 2.1.
Let K *be a field* $\neq F_2$ *and subsets* R *and* S *contain the field of constants* K *then the girth indicator of graph* $\Gamma = {}^{R,S} A(n, K[x_1, x_2, \ldots, x_n])$ *is at least* $2n + 2$.

This statement follows from the fact that Γ contains induced subgraph $A(n, K)$ with girth indicator $> 2n$. Similarly we get the following statement.

COROLLARY 2.2.
Let K *be a field of odd characteric* p *and subsets* R *and* S *contain prime field* F_p *then the girth indicator of the graph* $\Gamma = {}^{R,S} A(n, K[x_1, x_2, \ldots, x_n])$ *is* $> 2n$

These results about the girth indicators of induced subgraphs can be used for further investigation of properties of cryptographic systems based on symbolic computations with usage of graphs $A(n, F_q[x_1, x_2, \ldots, x_n]$.
Low density parity check (LDPC) codes with the usage of graphs of large girth ([22], [23], [24], [25]) are successfully used in satellite communications.
LDPC codes constructed via induced subgraphs of $A(n, F_q)$ compare well with LDPC codes based on graphs $CD(n, q)$ or Cayley-Ramanujan graphs $X(p, q)$ (see [26], [27], [28], [29]). Cubical subgroups $GA(n, F)$ of affine Cremona group $CG_n(F)$ (see [30]) defined in t Symbolic computations with the usage of bipartite algebraic graphs $A(n, F_q)$ and $A(n, F_q[x_1, x_2, \ldots, x_n])$ were used for the development of various cryptographic algorithms because the length of their minimal cycle (the girth) tends to infinity when n is growing. It motivates studies of graphs $A(n, K)$ defined over arbitrary integrity ring K. The cycle indicator of $A(n, K)$, i. e. maximal value of minimal cycles through the given vertex is $\geq 2n + 2$. We prove that in the case when K is a field with more than two elements the value $2n + 2$ is the maximal possible cycle indicator of algebraic graph with n-dimensional variety of vertexes. We justify that the girth indicator of line $[0, 0, \ldots, 0]$ is $2n + 2$, the girth indicator of point $(0, 0, \ldots, 0)$ is at least $2n$. From this result instantly follows that girth of known graph D(n, K) is at least $2([n + 5]/2)$ where K is an integrity ring. We consider some inequalities defined in terms of a girth, a diameter and the girth indicator of homogeneous algebraic graphs and formulate some conjectures.

Keywords: Family of graphs with large girth indicator, commutative integrity rings, homogeneous algebraic graphs, codimension, girth indicator, girth, diameter.

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

2 Introduction

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

(1) Investigate cycle indicator $h(v)$ of the vertex 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 the 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 thelarge girth indicator if cycle indicators $h(i)$ of graph G_i are at least $c \times log_{k-1}(v_i)$ for some independent positive constant c.

The problems (1) and (2) can be investigated not only in the case of finite graphs. They can be considered for algebraic graphs defined over the field F, i. e. graphs such that their vertexes and edges form finite dimensional algebraic variety over F. We talk about homogeneous (or k-homogeneous) algebraic graphs if neighbourhoods of each vertex have the same dimension k, $k \geq 1$. One can use integrity ring K instead of the field F.

We assume that field F contains at least two elements and each vertex of algebraic graph has at least 3 elements.

We refer to a family G_i of k-homogeneous algebraic graphs with vertex sets $V_i = V(G_i)$ as an family with large cycle indicator if cycle indicators $h(G_i)$ are bounded from below by $c \times dim(V_i)/k$ for some positive constant c.

In this paper we investigate some properties of bipartite algebraic graphs $A(n, K)$ with partition sets isomorphic to K^n.

In Section 2 we prove that girth indicator of $A(n, K)$ is at least $2n + 2$. It means that in the case when K coincides with F_q graphs $A(n, F_q)$ are q-regular and they form a family of graphs with large cycle indicator and appropriate constant c can be written as $2log_q(q-1)$. If K is a field then these graphs form algebraic family of graphs with large cycle indicator ($c = 2$).

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 investigated graphs are not vertex transitive, their girth differs from the cycle indicator.

In Section 3 we consider a problem of evaluation of the girth and the girth indicator in the case of homogeneous algebraic graph defined over the field F. The vertex set and edge set of algebraic graph have to be quasiprojective varieties over F.

The codimension $codim(G)$ of homogeneous algebraic graph G is the ration of dimension of its vertex set and the dimension k of neighbourhood of some vertex. We evaluate the minimal codimension of algebraic graph with prescribed cycle indicator of algebraic graph over field F.

Previously known bound $[(g(G) - 2)/2] \leq codim(G)$ for the homogeneous algebraic graph G of girth G is used for the definition of *algebraic Moore graphs* which codimension is on this bound. Some examples of algebraic Moore graphs are given. For each field F we introduce ${}^F u(h)$ as minimal codimension of algebraic graph G with girth indicator h defined over the field F. Symbol $u(h)$ stands for the minimal value of ${}^F u$ for the totality of fields F with at least two elements. We justify that for even h values of ${}^F u(h)$ and $u(h)$ coincides with $[(h-2)/2]$.

In Section 4 we write lower bounds for the diameter of homogeneous algebraic graph and bipartite algebraic homogeneous graph. We introduce Tits graphs as bipartite algebraic Moore graphs of diameter d codimension $d - 1$. Some conjectures are formulated.

In Section 5 references on applications of grapha $A(n, K)$ to Algebraic Geometry, Coding Theory and Cryptography are given.

3 On lower bound for the girth indicator of graphs $A(n, K)$ over integrity ring K

All graphs Γ in this paper are symmetric antireflexive binary relations on the set of their vertices V, i.e Γ is a subset of Cartesian product V with itself, such that $(x, y) \in \Gamma$ implies $(y, x) \in \Gamma$, for each $x \in V$ element (x, x) does not belong to Γ (see [1]). Missing definitions of Graph Theory such as path in the graph, cycle of length m, neighbour of the vertex, bipartite graph and etc. can be also found in [1].

Definition of commutative ring, integrity ring K and ring of multivariate polynomials $K[x_1, x_2, \dots, x_n]$ reader can find in [2].

Let K be a commutative ring. We define $A(n, K)$ as a 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 $(p) = (p_1, p_2, \dots, p_n) \in P_n$ and $[l] = [l_1, l_2, \dots, l_n] \in L_n$. The incidence relation $I = A(n, K)$ (or the corresponding bipartite graph I) is given by condition (p) and $[l]$ are incident if and only if the equations of the following kind hold:

$p_2 - l_2 = l_1 p_1$,
$p_3 - l_3 = p_1 l_2$,
$\mathrm{p}_4 - l_4 = l_1 p_3$, (1)
$p_5 - l_5 = p_1 l_4$,
$\dots$,
$p_n - l_n = p_1 l_{n-1}$ for odd n and
$p_n - l_n = l_1 p_{n-1}$ for even n.

Graphs $A(m, K)$ were obtained in [3] 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. $xI'y$ 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 v. 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 [3] and further references).

Let us consider a special automorphisms of graphs $A(K)$ and $A(n, K)$ defined over arbitrary commutative ring K. We take the list L of coordinates of the point of incidence structure $A(K)$ consisting of (10), (11), (12), (22), ..., (ii), $(i, i+1)$, ... Let $<$ stands for the natural order on L presented in the written above sequence. Assume that n^L stands for the list of first n elements of L.

For each element α from L of kind (i, i) or $(1, 0)$ we introduce automorphism $T_{\alpha,t}$, $t \in K$ moving point $(p) = (p_{1,0}, p_{1,1}, p_{1,2}, \dots)$ to $(p') = (p'_{1,0}, p'_{1,1}, p'_{1,2}, \dots)$ and line $[l_{0,1}, l_{1,1}, l_{1,2}, \dots]$ to the line $[l'_{0,1}, l'_{1,1}, l'_{1,2}, \dots]$ accordingly to the following rules.

(1) If $\alpha = (k, k)$, $k > 0$ then $T_{\alpha,t}((p))$ has coordinates $\{p'_{1,0} = p_{10}$, $p'_{1,1} = p_{11}$, $\dots$, $p'_{k-1,k} = p_{k-1,k}$, $p'_\alpha = p_\alpha + t$, $p'_{i-1,i} = p_{i-1,i} - p_{i-k-1,i-k)t}$, $p'_{ii} = p_{ii} - p_{i-k,i-k}t$ for each i, $i > k$ and $T_{\alpha,t}([l])$ has coordinates $l'_{01} = l_{01}$, $l'_{11} = l_{11}$, $\dots$, $l'_{i-1,i} = l_{i-1,i}$, $l'_\alpha = l_\alpha + t$, $l'_{i-1,i} = l_{i-1,i} - l_{i-k-1,i-k}t$, $l'_{ii} = l_{ii} - l_{i-k,i-k}t$, $\dots$ for each i, $i > k$.

(2) In the case of $\alpha = (1, 0)$ has coordinates $T_{\alpha,t}((p))$ has coordinates $p_{1,0} + t$, p_{11}, p_{12}, $\dots$) and $T_{\alpha,t}([l])$ has l_{01}, $l_{11} - l_{0,1}t$, $\dots$, l_{i-1i}, $l_{i,i} - l_{i-1,i}t$, $\dots$, $i > 1$.

Direct check of incidence conditions for (p') ans $[l']$ allows us to formulate the following statement.

PROPOSITION 1.1.

Transformations $T_{\alpha,t}$ for $\alpha = (1, 0)$ or $\alpha = (i, i)$, $i \geq 1$ are automorphisms of the graph $A(K)$.

We consider transformations ${}^nT_{\alpha,t}$, $\alpha \in {}^nL$ which correspond to natural action of $T_{\alpha,t}$ on the vertices of graph $A(n, K)$. Similarly to previous statement we justify the following statement.

PROPOSITION 1. 2.

The transformation ${}^nT_{\alpha,t}$, $\alpha \in^n L$ of kind $(1, 0)$ or (i, i) are automorphisms of the graph $A(K)$.

As we mentioned above graph $A(n, K)$ satisfies to linguistic property. It means that the following statement holds.

LEMMA 1.1.

The path (0), v_1, v_2, $\ldots$, v_{n-1} *in the graph* $A(n,K)$ *are determined by colours* z_i *of elements* v_i, $i = 1, 2, \ldots, n-1$.

LEMMA 1. 2 (two numbers lemma).

Let $v_0, v_1, v_2, \ldots, v_{n-1}$ *be the path of* $A(n,K)$ *starting in zero point* $v_0 = (0,0,\ldots,0)$ *given by the tuple of colours* z_1, z_2, $\ldots$, z_{n-1}. *Then last two coordinates of* v_{n-1} *are* $z_1 z_2 (z_1 - z_3)(z_2 - z_4)\ldots(z_{n-3} - z_{n-1})$ *and* $z_{n-1} z_1 z_2 (z_1 - z_3)(z_2 - z_4)\ldots(z_{n-3} - z_{n-1})$. *The last two coordinates of* v_1, v_2, $\ldots$, v_{n-3} *equal to* 0.

The proof of this statement can be obtained via straight usage of mathematical induction. This statement was used in [3] for the prove of the fact that girth $D(n,K)$ is at least $2[(n+5)/2]$ in the case of integrity ring K.

COROLLARY 1. 1.

Let v_0, v_1, v_2, $\ldots$, v_{n-1} *be the path in the graph* $A(n-1,K)$ *with* $v_0 = (0,0,\ldots,0)$ *and* $\rho(v_i) = z_i$. *Then the last coordinate of the destination point* v_{n-1} *is* $z_1 z_2 (z_1 - z_3)(z_2 - z_4)\ldots(z_{n-3} - z_{n-1})$. *The last coordinate of* v_{n-2} *is zero.*

Noteworthy that for the path as above the conditions $z_i - z_{i+2} \neq 0$ and $z_2 \neq 0$ hold.

COROLLARY 1.2.

Assume that conditions of previous statement hold, z_1 *is not a zero and* K *is an integrity ring. Then the last coordinate of the tuple* v_{n-1} *is not a zero but the last coordinate of* v_{n-3} *is zero.*

As we mentioned above the procedure to cut the last coordinate of each vertex of graph $A(n,K)$ defines colour preserving homomorphism ${}^n\Delta$ from the graph $A(n,K)$ to $A(n-1,K)$. So if graph $A(n-1,K)$ has no cycles of length s then graph $A(n,k)$ does not have C_{2s} as well.

Let Γ be a graph. The *cycle indicator of a vertex* $v \in \Gamma$ is minimal length of the cycle through this vertex if such cycle exists or infinity in opposite case. The cycle indicator of Γ is maximal value of cycle indicator of vertexes of the graph. So the cycle indicator of the tree is infinity. If degree of each vertex of the finite graph is at least two then its cycle indicator is finite.

THEOREM 1.1.

Let K *be an integrity ring with more than two elements. Then the girth of point* $(0,0,\ldots,0)$ *of the graph* $A(n,K)$ *is at least* $2n$. *The girth indicator of line* $[0,0,\ldots,0]$ *is at least* $2n+2$.

Proof.

Each vertex of the graph $A(n,K)$ has at least two neighbours. So girth indicator of $A(n,K)$ is finite.

As it follows from the definitions of graphs $A(2,K)$ and $A(3,K)$ they are isomorphic to well investigated graphs $D(2,K)$ and $D(3,K)$ (see [3]). These graphs are edge transitive, their girth indicator equals to girth which is ≥ 6 and ≥ 8 respectively. It means that graphs $A(n,K)$, $n \geq 4$ do not contain cycles C_4 and C_6. So the the value of girth indicator of $(0,0,0,0)$ from $A(4,K)$ is at least 8. Let us consider graph $A(5,K)$ and assume that it has cycle C of length 8

starting in $(0,0,0,0,0)$. Let (p) be some point from this cycle. It is easy to see that C is formed by two paths of kind (0), $[v_1]$, (v_2), $[v_3]$, (v_4), $[v_5]$ of colours z_1, z_2, z_3, z_4, z_5 and (0), $[u_1]$, (u_2), $[u_3]$ of colours y_1, y_2, z_5 such that $[u_3] = [v_5]$. Noteworthy that $y_1 \neq z_1$. Without loss of generality we can assume that $z_1 \neq 0$. Then according to Corollary 1.2 the last coordinate of $[v_5]$ is different from zero but the last coordinate of $[u_3]$ equals 0. Thus we get a contradiction. So the graph $A(5,K)$ has no cycles C_4, C_6 and C_8 through the vertex $(0,0,0,0,0)$. It means that girth indicator of this vertex is ≥ 10 and vertex $(0,0,\ldots,0)$ of graphs $A(n,K)$, $n \geq 5$ is ≥ 10.

Assume that 0 point of the graph $A(6,K)$ has a cycle C of length 10 starting in this point. We can assume that $C$is formed by two paths of kind (0), $[v_1]$, (v_2), $[v_3]$, (v_4), $[v_5]$, (v_6) of colours z_i, $i = 1,2,\ldots,6$ with $z_1 \neq 0$ and (0), $[u_1]$, (u_2), $[u_3]$, (u_4) of colours y_1, y_2, y_3, z_6 such that $[u_4] = [v_6]$. According to the Corollary 1.2 last coordinate of v_6 is not zero but last coordinate of u_4 is 0. So we get a contradiction. Thus girth indicator of (0) point of $A(n,K)$, $n \geq 6$ is ≥ 12. Continuation of this process for $n = 7,8,\ldots$ justifies the statement.

Let us consider line $[0] = [0,0,\ldots,0]$ of $A(n,K)$ and cycle C through this vertex of even length $s < 2n+2$. Let u and w be neighbouring points of [0]. Existence of homomorphisms of kind $T_{(1,0),t}$ allows us to assume without loss of generality that $\rho(u) = 0$ but $\rho(w) \neq 0$. It means that $u = (0,0,\ldots,0)$. Let us assume that there is a cycle of length $2n$ through the edge (0), [0]. We can assume that it formed by two paths of kind (0), [0], v_2, v_3, $\ldots$, v_n and (0), u_1, u_2, $\ldots$, u_n with $\rho(u_1) \neq 0$ and $v_n = u_n$. Accordingly Lemma 1.2 last coordinate of v_1 is 0 but last coordinate of u_2 differs from zero. So we have a contradiction and cycles of length $2n$ trough $[0,0,\ldots,0]$ do not exist. Similarly we justify that $A(s,K)$, $s < n$ does not contains cycle of lrngth $2s$ through zero line. It means that $A(n,K)$ also does not contain cycles of length $2s$ through [0]. Thus we proved that cycle indicator of [0] is at least $2n+2$.

In the case of $K = F_q$ the theorem is proven in short note [4] where conjectuted that cycle indicator of $A(n,F_q)$ is $2n+2$.

The edge transitive group of automorphisms of graphs $D(n,K)$ where K is arbitrary commutative ring is presnted in [3]. From edge transitivity and Theorem 1.1 we obtained the following statement.

THEOREM 1. 2 (see [3])

Let K be an integrity ring and k, $k \geq 3$ is odd number. Then the girth of graph $D(k,K)$ is at least $k+5$.

The family of graphs $D(n,K)$, $n = 2,3,\ldots$ 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}, $\ldots$, p_{ii}, p_{ii+1}, $p_{i+1,i}$, $p_{i+1,i+1}$, $\ldots)$, and lines $[l] = [l_{01}$, l_{11}, l_{12}, l_{21}, l_{22}, l'_{22},$\ldots$,l'$_{ii}$, l_{ii+1}, $l_{i+1,i}$, $l_{i+1,i+1}$, $\ldots]$.

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:

$p_{i,i} - l_{i,i} = l_{1,0}p_{i-1,i}$,

$p'_{i,i} - l'_{i,i} = l_{i,i-1}p_{0,1}$,
$p_{i,i+1} - l_{i,i+1} = p_{i,i}l_{0,1}$, (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 $D(K)$ writtem in their natural order, i. e. sequence $(1,0)$, $(1,1)$, $(1,2)$, $(2,1)$, $(2,2)$,$(2,2)$',. . . .$Let^k D$ 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 ${}^kD \cap Root$.

Proof

Let $k = 4s - 3$. We partite the list the coordinates of point of the graph in different order and get list L_1 formed by $(1,0)$, $(1,1)$, $(1,2)$, $(2,2)$, $(2,3)$, $(3,3)$, . . . , $(s-1,s-1)$, $(s-1,s)$ of length $2s-1$ and list L_2 formed by $(2,1)$, $(2,2)'$, $(2,3)$, $(3,3'$, . . . , $(s-1,s-1)'$. The image of homomorphism η_k is $A(2s-1,K)$. Assume that $D(4s-3,K)$ has cycle of length $4s$

Assume that graph $D(4s-3,K)$ has cycle C of the length $4s$. Edge transitivity of the graph allow us to assume that C contains (0) point together with [0] line. Then $\eta_k(C)$ has to be a closed walk through [0] of length $2(2s_1)+2$. the neightbours of [0] have distict colurs of kind 0 and b, $b \neq 0$. Thus cycle indicator of $[0,0,\ldots,0]$ has to be $< 2(2s-1)+2$, but it contradics to Theorem 1.1.

In the case $k = 4s-1$ we add index (s,s) to list L_1 and $(s,s-1)$ to the list L_2 and repear written above arguments.

Let $H(n,K)$ be a group generated by transformations $T_{\alpha,t}$ of the vertex set of graph $A(n,K)$ introduced in the Proposition 1.2.

REMARK 1.1.

In fact Theorem 1. 2 is proven in [3] but the equivalent to this statement theorem is formulated in terms of linguistic dynamical systems.

REMARK 1.2.

Let $Orb_{(0)}$ and $Orb_{[0]}$ are orbits of graphs $A(n,K)$ containing zero point or zero line. These orbits are isomorphic to varieties K^{m+1} and K^m with $m = [n/2]$ for $n \geq 4$ respectively with $m = [n/2]$. Representatives of $Orb_{(0)}$ and $Orb_{[0]}$ have the same cycle indicators with (0) and [0].

4 On minimal codimensions of vertex sets of homogeneous algebraic graphs with the prescribed girth or girth indicator

Let us introduce 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 $Q \times Q$ 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 $codim() = dim(Q)/N$ as codimension of an algebraic graph Φ. Recall that the girth of the graph is the length of its minimal cycle.

THEOREM (see [5]).

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

We define codimension $codim(G)$ of homogeneoud graph G over a field F with vertex set Q such that the dimension of a neighbourhood for each vertex is N, $N \geq 1$ as papameter $dim(Q)/N$.

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.

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

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

In [6] the computer computations of girth of graphs $A(n, F_4)$ for parameters $n = 2, 3, 4, 5, 6, 7, 8$ are described. It was established that $g(A(2, F_4)) = 6$, $g(A(3, F_4)) = 8$, $g(A(4, F_4)) = 10$, $g(A(5, F_4)) = 12$ So graphs $A(n, F_4)$, $n = 2, 3, 4, 5$ are algebraic Moore graphs and the following statement holds.

PROPOSITION 2.1.

$v(6) = 2$, $v(8) = 3$, $v(10) = 4$ and $v(12) = 5$.

We introduce ${}^F v(g)$ as minimal codimension of homogeneous algebraic graph over field F, $F \neq F_2$ of girth g. As it follows from the written above Theorem ${}^F v(g) \geq [(g-1)/2]$.

Geometries of simple Chevalley groups $A_2(F)$, $B_2(F)$, $G_2(F)$ (see [7]) are bipartite homogeneous algebraic graphs over field F of codimension 1 of girth $6, 8$ and 12. So they are algebraic Moore graphs and the following statement holds.

PROPOSITION 2.2.

For each field F with more than two elements ${}^F v(6) = 2$, ${}^F v(8) = 3$, ${}^F v(12) = 5$.

I suggest to refer to homogeneous algebraic graph of girth 10 with codimension 4 as Chojecki graph, hope that following conjecture can attract attention of researchers.

CONJECTURE 2.1.

The totality of Chojecki graphs is a finite set.

Recall that the girth indicator $Cind(x)$ of a vertex x of the graph G as the minimal length of the cycle through x and introduce a cycle indicator $Cind(G)$ of the graph as the maximal value of $Cind(x)$ for its vertexes. The inequality $Cind(G) \geq g(G)$ follows directly from the definition.

5 On diameter, girth and girth indicator of homogeneous algebraic graphs.

Investigations of girth and diameter of finite graphs is an important core direction of Extremal Graph theory (see [8], [9]. [10], [11]. [12], [13], [14], [15]).

Studies of algebraic graphs over selected field with prescribed girth and diameter form classical direction of Geometry.

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 subspaces of vector space F^3 (see [16])

J. Tits defined generalised m-gons as a finite biregular bipartite graphs of girth $2m$ and diameter m (see [17], [18], [19]) . Noteworthy that geometries of Chevalley groups $A_2(F_q)$, $B_2(F_q)$ and $G_2(F_q)$ are $(q+1)$ regular generalised m-gons for $m = 3, 4$ and 6. Edge transitive generalised m-gons are "constructions bricks" for creation of Tits geometries over diagrams and buildings ([20], [21]).

LEMMA 3.1.

Let G be the homogeneous algebraic graph over a field F, $F \neq F_2$ of the diameter d such that the dimension of a neighbourhood for each vertex is N, $N \geq 1$. Then $d \geq codim(G) = dim(V(G))/N$.

Proof.

Let v be a vertex of G. Each other vertex u has to be connected with v via some path of kind v , u_1, u_2, ..., $u_s = u$ where $s \leq d$. Let M be the variety of vertexes u at maximal distance from v. The dimension of variety P of pathes of kind v , u_1, u_2, ..., $u_d = u$ has to satisfy condition $Nd \geq dim(P) \geq dim(M)$. Each vertex from $V = V(G)$ is located at the distance at most d from v. So $dim(M) = dim(V)$ and d is at least $dim(V)/N$.

For the case of bipartite graphs or graphs without even cycles the following stronger lower bound on the diameter holds.

$d \geq dim(V)/N + 1$ (3.1)

It can be justified via breadth-first search tree starting from the midpoint of a single edge.

We refer to bipartite homogeneous algebraic graph G as *algebraic Tuttes graph* if its diameter $d(G)$ coincides with $codim(G) + 1$.

In the case of algebraic Tuttes graphs which are also algebraic Moore graphs we use term *Tits graphs. It is clear that the diameter of Tits graph is a half of*

the girth. Obvious examples of Tits graphs are geometries of Chevalley groups $A_2(F)$, $B_2(F)$ and $G_2(F)$ over arbitrary field F. They have codimensions $2, 3$ and 5 and girth $6, 8, 12$ respectively.

CONJECTURE 3.1.

Tits graphs exist only in cases of codimensions $2, 3$ *and* 5. *(in a spirit of Feit-Higman Theorem).*

CONJECTURE 3.2.

Algebraic Moore graphs exist only in cases of codimensions $2, 3, 4$ *and* 5.

We introduce some integer function in terms of algebraic geometry which are extremely hard for computation in a following way. Parameter $g(d)$ is maximal girth of algebraic homogeneous graph of diameter d, $d \geq 3$. $d(g)$ is minimal diameter of algebraic homogeneous graphs of girth g, $g \geq 4$.

It is easy to see that $d(6) = 3$, $d(8) = 4$, $d(12) = 6$ and $g(3) = 6$, $g(4) = 8$, $g(6) = 12$.

From the result about girth and diameter of $A(4, 4)$ we get that $d(10) \leq 8$ and $g(8) \geq 10$. Recall that we introduce $v(n)$ as the minimal codimension of existing algebraic homogeneous graph of girth n. So $v(n) \geq [(n-1)/2]$. We define $w(d)$ as the maximal codimension of existing bipartite homogeneous algebraic graph of diameter d. So $w(d) \leq d - 1$.

6 Some corollaries and remarks on applications

Let K be commutative integrity ring containing at least two elements. We consider nonempty subsets R and S of $K[x_1, x_2, \ldots, x_n]$, $n \geq 1$. Let ${}^{R,S}A(n, K[x_1, x_2, \ldots, x_n]$ be the induced subgraph of $A(n, K)$ of all points and lines with colours from R and S respectively. According to famous result by D. Hilbert $K[x_1, x_2, \ldots, x_n]$ is also an integrity ring. So the girth indicator of infinite graph $A(n, K[x_1, x_2, \ldots, x_n])$ is $g > 2n$ and the following statement holds.

PROPOSITION 4.1.

The girth indicator of graph ${}^{R,S}A(n, K[x_1, x_2, \ldots, x_n])$ *is* $> 2n$.

COROLLARY 4.1.

Let K *be a field* $\neq F_2$ *and subsets* R *and* S *contain the field of constants* K *then the girth indicator of graph* $\Gamma = {}^{R,S} A(n, K[x_1, x_2, \ldots, x_n])$ *is at least* $2n + 2$.

This statement follows from the fact that Γ contains induced subgraph $A(n, K)$ with girth indicator $> 2n$. Similarly we get the following statement.

COROLLARY 4.2.

Let K *be a field of odd characteric* p *and subsets* R *and* S *contain prime field* F_p *then the girth indicator of the graph* $\Gamma = {}^{R,S} A(n, K[x_1, x_2, \ldots, x_n])$ *is* $> 2n$

These results about the girth indicators of induced subgraphs can be used for further investigation of properties of cryptographic systems based on symbolic computations with the usage of graphs $A(n, F_q[x_1, x_2, \ldots, x_n])$.

Low density parity check (LDPC) codes with the usage of graphs of large girth ([22], [23], [24], [25]) are successfully used in satellite communications.

LDPC codes constructed via induced subgraphs of $A(n, F_q)$ compare well with LDPC codes based on graphs $CD(n, q)$ or Cayley-Ramanujan graphs $X(p, q)$ (see [26], [27], [28], [29]). Cubical subgroups $GA(n, F)$ of affine Cremona group $CG_n(F)$ (see [30]) defined in terms of pair $(A(n, F)\ ,\ A(n, F[x_1, x_2, \ldots, x_n]))$ are interesting objects of Algebraic Geometry (see [31]). The usage of these groups in Non Commutative cryptography [32], Multivariate cryptography [33], Algebraic Cryptography [34] and Post-Quantum Cryptography [35] is described in [36].

Properties of graphs $A(n, K)$ and groups $GA(n, K)$ over finite commutative ring K have various applications to Symmetric and Postquantum Cryptographies (see [37], [38] and further references).

1. A. Brouwer, A. Cohen, A. Nuemaier, *Distance regular graphs*, Springer, Berlin,1989.
2. B. L, Van Der Waerden, *Algebra*, Vol 1, Springer V, 2011, 265 pp.
3. V. Ustimenko, *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Journal of Mathematical Sciences.- Springer. v.140. No.3. 2007. P. 412-434.
4. V. Ustimenko, *On the extremal graph theory and symbolic computations*, Reports of Nath. Acad. of Sci. of Ukraine, 2013, No. 2, P. 42-49.
5. T. Shaska, V. Ustimenko, *On the homogeneous algebraic graphs of large girth and their applications*, Linear Algebra Appl., 430, No. 7, 2009, pp. 1826-1837.
6. 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 Atchive, 2022/908.
7. R. W. Carter, *Simple Groups of Lie Type*, Wiley, New York (1972)
8. F. Lazebnik., V. A. Ustimenko and A. J. Woldar. *New Series of Dense Graphs of High Girth*, Bull (New Series) of AMS. v.32, No.1, 1995. P. 73-79.
9. B. Bolloba's, *Extremal Graph Theory.* London: Academic Press, 1978, 440 P.
10. J. A. Bondy and M. Simonovits, *Cycles of even length in graphs*, J. Combin.Theory. Ser. B. 16. 1974. P. 87-105.
11. W. Faudree, M. Simonovits. *On a class of degenerate extremal graph problems*, Combinatorica, 3 (1), 1983, P. 83-93.
12. P. Erdős', A. Renyi. and V. T.Sos, *On a problem of graph theory*, Studia. Sci. Math. Hungar. 1. 1966. P. 215-220.
13. P. Erdős', M. Simonovits *Compactness results in extremal graph theory*, Combinatorica. 2 (3). 1982. P. 275-288.
14. C.T. Benson, *Minimal regular graphs of girth eight and twelve*, Canad. Journal of Mathematics, . 18. 1966. P. 1091-1094.
15. W. G. Brown, *On graphs that do not contain Thomsen graph*, Canad. Math. Bull. 9. No.3. 1966. P. 281-285.
16. P. Dembovski, *Finite Geometries*, Springer, Berlin, 1968.
17. J. Tits, *Sur la trialite at certains groupes qui sen deduicent*, Publ. Math. I.H.E.S. 2 (1959), 15-20.
18. J. Tits, *Les groupes simples de Suzuki et de Ree*, Seminaire Bourbaki 13 (210), 1960/1961, 1-18.
19. J. A. Thas, *Generalised polygons*, in F. Buekenhout (ed), Handbook in Incidence Geometry, Ch. 9, North Holland, Amsterdam, 1995.
20. F. Buekenhout (editor), *Handbook in Incidence Geometry*, Ch. 9, North Holland, Amsterdam, 1995.

21. J. Tits, *Buildings of spherical type and Finite BN-pairs*, Lecture Notes in Math., Springer Verlag, 1074.
22. R. Michiel Tanner, *A recursive approach to low density codes*, IEEE Trans. on Info Th., IT, Sept. 1984, 27(5), 533-547.
23. 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.
24. 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.
25. Richardson, R. Urbanke, *Modern Coding Theory*, Cambridge University Press, 2008.
26. 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 systems (FedCSIS), 2012, Wroclaw, pp. 11-23.
27. D. J. C. MacKay, and M. S. Postol, M. S. *Weaknesses of Margulis and Ramanujan-Margulis low-dencity parity-check codes*, 2003, Electron. Notes Theor. Comput. Sci., 74, pp. 97-104
28. G. Margulis. *Explicit group-theoretical constructions of combinatorial schemes and their application to design of expanders and concentrators*, Probl. Peredachi Informatsii, 24 (1), 51–60. English translation publ. Journal of Problems of Information transmission. 1988, 39–46.
29. A. Lubotsky, R. Philips, P. Sarnak. *Ramanujan graphs*, J. Comb. Theory, 1989, 115 (2), 62–89.
30. 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, pp. 1213.
31. V. Ustimenko, U. Romaczuk, *On dynamical systems of large girth or cycle indicator and their applications to multivariate cryptography,* In Artificial intelligence, evolutionary computing and metaheuristics. Studies in Computational Intelligence (Vol. 427) (pp. 231-256). Berlin, Heidelberg: Springer, 2013.
32. Alexei G. Myasnikov, Vladimir Shpilrain, Alexander Ushakov. *Non-commutative Cryptography and Complexity of Group-theoretic Problems.* Amer. Math Soc. 2011.
33. Jintai Ding, Albrecht Petzoldt, Dieter S. Schmidt, *Multivariate Cryptography*, Springer Nature, 30 Sept 2020, 253 pages
34. Neal Koblitz,*Algebraic Aspects of Cryptography*, Springer Science Business Media, 6 Dec 2012, 206 pages.
35. Daniel J. Bernstein, Johannes Buchman, Erik Dahmen (Editors), *Post-Quantum Cryptography*, Springer, 2011.
36. V. Ustimenko, *Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world*, UMCS Editorial House, Lublin, 2022, 198 p.
37. M. Polak, U. Romanczuk, V. Ustimenko and A. Wrblewska, *On the applications of Extremal Graph Theory to Coding Theory and Cryptography*, Erdős' Centennial, Proceedings of Erdős' Centennial (EP 100), Electronic Notes in Discrete Mathematics, V.43, P. 329–342, 2013.
38. V. Ustimenko, U. Roman'czuk-Polubiec, A. Wroblewska, M. Polak, E. Zhupa, *On the constructions of new symmetric ciphers based on non-bijective multivariate maps of pre-scribed degree*, Security and Communication Networks , Volume (2019), Article ID 2137561, 15 pp.