New results on algebraic graphs of large girth and their impact on Extremal Graph Theory and Algebraic Cryptography

Vasyl Ustimenko

Royal Holloway University of London
Institute of Telecommunication and Global Information Space, Kyiv, Ukraine
vasylustimenko@yahoo.pl
https://itgip.org/security_en/

Abstract. For arbitrary finite field F_q, $q > 2$ we prove that known q-regular bipartite algebraic graphs $A(n, q)$ existence on $2q^n$ vertices have girth $2n$ or $2n + 2$. Similar result is formulated for more general graphs $A(n, K)$ defined over general commutative integrity ring K. The impact of these results on Extremal Graph Theory and graph based Algebraic Cryptography is discussed.

Keywords: Families of graphs of large girth, Extremal Graph Theory, Graph based Cryptography, Multivariate Cryptography, Noncommutative Cryptography

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

1 Some results of Extremal Graph Theory

Classical Extremal Graph Theory developed by Erdős' and his school had been started with the following problem formulated by Turan.

What is the maximal value $ex(v, C_n)$ for the size (number of edges) of simple graph on v vertices without cycles C_n of length n? (see [1], [2], [3], [4])

To discuss the behavior of function $ex(v, C_n)$ for large variable v we will use the following standard notations.

Let f and g be two real valued functions on (a, ∞).

1. $f(x) <=> g(x)$, $x \to \infty$ if $f(x)/g(x) \to 1$ for $x \to \infty$;

2. $f(x) = o(g(x))$, $x \to \infty$ if $f(x)/g(x) \to 0$ for $x \to \infty$;

3. $f(x) = O(g(x))$, $x \to \infty$ if there exist C and x_0 such that $|f(x)| < C|g(x)|$ for all $x > x_0$;

4. $f(x) = \Omega(g(x))$, $x \to \infty$ if there exist a $c > 0$ and a sequence $x_1, x_2, \ldots$ such that $|f(x_i)| \geq c|g(x_i)|$ for all $i \geq 1$.

If $n = 2k + 1$ is odd positive integer we can assume that positive integer v is even and take the complete bipartite graph with the partition sets of same cardinality $v/2$. It contains $v^2/4$ vertices, so $ex(v, C_{2k+1}) = O(v^2)$.

If n is even, then according to famous Erdős' Even Circuit Theorem $ex(v, C_{2k}) = O(v^{1+1/k})$. This proof was obtained by famous Erdős' probabilistic method. Recall that the upper bound of the theorem is known to be sharp $ex(v, C_{2k}) = \Omega(v^{1+1/k})$ for $k = 2, 3$ and 5 only (see [4], [5], [7] for $n = 2$ and [6] for $n = 3, 5$).

The girth $g(G)$ of the simple graph G is the length of its smallest cycle. The studies of maximal size $ex(v, C_3, C_4, \dots, C_n)$ for graph on v vertices without cycles $C_3, C_4, \dots, C_n$, i.e. graphs of girth $> n$ historically had been motivated by their applications to Telephone Networking. As it follows from Erdős' Even Circuit Theorem $ex(v, C_3, C_4, \dots, C_{2n}) = O(v^{1+1/n})$.

More precise evaluations lead to the following bounds:

$ex(v, C_3, C_4, \dots, C_{2k}, C_{2k+1}) \leq (1/2)^{1+1/k} v^{1+1/k} + o(v^{1+1/k})$ (1)

$ex(v, C_3, C_4, \dots, C_{2k}) \leq (1/2) v^{1+1/k} + o(v^{1+1/k})$ (2)

The inequality (1) is established in [5] for all integers $k \geq 2$. The upper bound (2) can be obtained by similar arguments.

Similar to the case of $ex(v, C_{2n})$ both bounds (1) and (2) are known to be sharp up to magnitude for $n = 2, 3$ and 5 only.

The first general lower bounds of kind

$ex(v, C_3, C_4, \dots, C_n) \geq \Omega(v^{1+c/n})$ (3)

where c is some constant was obtained in 50th by famous Erdos via studies of families of graphs of large girth, i.e. infinite families of simple regular graphs G_i of degree k, $k > 2$ and order v_i such that the girth $g(G_i)$ is $\geq \gamma log_{k-1}(v_i)$, where γ is the independent of i constant. We refer to γ as speed of growth of the family.

P.Erdős' proved the existence of such a family with arbitrary large but bounded degree k with $\gamma = 1/4$ by his famous probabilistic method.

Novadays several explicit families of graphs of large girth with unbounded girth and arbitrarily large k are known. Among them reader can find the family of Ramanujan-Cayley graphs $X(p, q)$ had been defined in [8] and investigated in [9], the family of bipartite algebraic graphs $CD(n, q)$ defined in [10].

Notice that $ex(v, C_{2k}) \geq ex(v, C_3, C_4, \dots, C_{2k+1})$. The best known lower bound for $k \neq 2, 3, 5$ was obtained in [10]:

$ex(v, C_3, C_4, \dots, C_{2k+1}) = \Omega(v^{1+2/(3k-3+e)})$ (4)

where $e = 0$ if k is odd, and $e = 1$ if k is even.

Family of graphs $CD(n, q)$ were used for the justification of this bound.

The main result of this paper which is essential improvement of bound (4). It is written below.

THEOREM 1.1.

$ex(v, C_3, C_4, \dots, C_{2k+1}) = \Omega(v^{1+1/(k+1)})$ (5)

COROLLARY 1.1.

$C' v^{1+1/(k+1)} \leq ex(v, C_{2k}) \leq C v^{1+1/k}$ for certain constants C and C'.

CONJECTURE 1.1.

(i) If $n = 4$ or $n > 6$ then $ex(v, C_{2n}) <=> c v^{1+1/(n+1)}$ for some constant c.

Noteworthy that for $n = 2, 3, 5$ the equivalence $ex(v, C_{2n}) <=> c v^{1+1/n}$ holds for some c.

Theorem 1.1 follows from the results on properties of the family of q-regular bipartite graphs $A(n,q)$ (see [11], [12], [13]) of order $2q^n$ and further investigation of their girths.

Noteworthy that speed of grows of girth of family of Cayley-Ramanujan graphs $X(p,q)$ of fixed degree p is $4/3$. The speed of growth of girth of q-regular graphs $CD(n,q)$ tends to $4/3$ from below when parameter q is growing. Alex Lubotzky conjectured that $4/3$ is the maximal possible speed of growth of the girth. The existence of graphs $A(n,q)$, $q \geq 4$ of girth $\geq 2n$ disproves this conjecture.

We can see that speed of growth of the girth of family $A(n,q)$, $n = 2,3,\dots$ tends to 2 when q is growing. Speed of girth grows for family of graphs $A(n,q)$, $n = 2,3,\dots$ is $> 4/3$ if q is at least 4.

As it formulated in [11] family $A(n,q)$, $q \geq 3$ like Cayley-Ramanujun graphs is a family of small world graphs of bounded degre and large girth, well defined projectibe limit $A(q)$ of $A(n,q)$ is isomorphic to q-regular tree T_q. Noteworthy that in the case of family of Cayley-Ramanujan graphs of large girth the projective limit does not exist.

Recall that the girth and diameter of a graph are the minimal length of its cycle and the maximal distance of the graph. We can consider the girth indicator $Cind(v)$ of a vertex v of the graph G as the minimal length of the cycle through v and introduce a cycle indicator $Cind(G)$ of the graph as the maximal value of $Cind(v)$ for its vertices. It was shown in [11] that graphs $A(n,q)$, $n = 2,3,\dots$ have maximal posible cycle indicator $2n+2$. We can prove that girth of the graph $A(n,q)$ is at most $2n$ for $n > 6$. So if $n > 6$ graphs $A(n,q)$ are not vertex transitive,

2 Case of algebraic graphs

The constructions of finite or infinite graphs with prescribed girth and diameter is an important and difficult task of the graph theory. Noteworthy that the incidence of the classical projective geometry over various fields is a graph of girth 6 and diameter 3.

J. Tits defined generalized m-gons as bipartite graphs of girth $2m$ and diameter m. Feit and Higman proved that finite generalized m-gons with bi-degrees > 2 exist only in the cases of $m = 3,4,6,8$, and 12. Geometries of finite simple groups of rank 2 are natural examples of generalized m-gons for $m = 3,4,6,8$. Classification of flag transitive generalized m-gons of the Moufang type were obtained by J. Tits and R. Weiss.

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 $x \in Q$ and $x\phi y$ implies $y\phi x$ ($x\phi y$ means $(x, y) \in \phi$).

The graph ϕ is homogeneous (or N-homogeneous), if for each vertex $u \in Q$, the set $\{x|u\phi x\}$ is some quasiprojective variety $M(u)$ over F of a non-zero constant dimension N independent on the choice of N. We further assume that each $M(u)$ contains at least 3 elements. We refer to $codim(\phi) = dim(V)/N$ as codimension of an algebraic graph ϕ.

THEOREM 2. 1. [14].

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

The following corollary is an analog of Even Circuit Theorem by Erdős'.

COROLLARY 2. 1.

Let Γ be a homogeneous graph over a field F, $F \neq F_2$ and let $E(\Gamma)$ be a variety of its edges. Then $dim(E(\Gamma)) \leq dim(V(\Gamma))(1 + [(g-1)/2]^{-1})$.

We introduce $v(g, F)$, $F \neq F_2$ as milimal value of $codim(\Gamma)$ for homogeneous algrbraic graph Γ over F of girth g. We refer to $v(g, F)$ as algebraic rank of girth g over field F. We introduce $v(g)$ as minimum $v(g, F)$ for various fields F, $F \neq F_2$ and refer to it as absolute rank of g.

COROLLARY 2.2.

$v(g, F) \geq [(g-1)/2]$ and $v(g) \geq [(g-1)/2]$.

THEOREM 2.2.

If g is even positive integer ≥ 4 and $F \neq F_2$ then $v(g, F) \in \{(g-2)/2, g/2\}$ for each field F..

COROLLARY 2.3.

$v(g) \in \{(g-2)/2, g/2\}$.

3 The construction of graphs $A(n, K)$ over commutatative ring K and their properties

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 $(p) = (p_1, p_2, \ldots, p_n) \in P_n$ and $[l] = [l_1, l_2, \ldots, l_n] \in L_n$. The incidence relation $I = A(n, K)$ (or the corresponding bipartite graph I) is given by condition p and l, 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$_4 - l_4 = l_1 p_3$, (6)
$p_5 - l_5 = p_1 l_4$,
$\ldots$,
$p_n - l_n = p_1 l_{n-1}$ for odd n and
$p_n - l_n = l_1 p_{n-1}$ for even n.

Graphs $A(m, K)$ were obtained in [11] as quotients of graphs $D(n, K)$ (see [10] and further references).

The graphs $A(n, K)$ obtained as special homomorphic images (see [11], [12] of graphs $D(n, K)$ (see [7]) which defines the projective limit $D(K)$ with points

$(p) = (p_{01}, p_{11}, p_{12}, p_{21}, p_{22}, p_{22}, \dots, p_{ii}, p_{ii+1}, p_{i+1,i}, p_{i+1,i+1}, \dots)$,

lines

$[l] = [l_{10}, l_{11}, l_{12}, l_{21}, l_{22}, l_{22}, \dots, l_{ii}, l_{ii+1}, l_{i+1,i}, l_{i+1,i+1}, \dots]$.

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

We now define an incidence structure $(P,\ L,\ I)$ with the partition sets P and L as follows. We say that a point (p) is incident with a line $[l]$, and write $(p)I[l]$, if their coordinates obey the following relations:

$l_{i,i}-p_{i,i}=l_{1,0}p_{i-1,i}$,
$l'_{i,i} - p'_{i,i} = l_{i,i-1}p_{0,1}$,
$l_{i,i+1} - p_{i,i+1} = l_{i,i}p_{0,1}$, (7)
$l_{i+1,i} - p_{i+1,i} = l_{1,0}p'_{i,i}$.

(These four relations are well defined for $i > 1$, $p_{1,1} = p'_{1,1}$, $l_{1,1} = l_{1,1}$.) This incidence structure (P, L, I) is denoted by $D(K)$.

We speak now of the incidence graph of (P, L, I) with vertex set $P \cup L$ and edge set consisting of all pairs $\{(p), [l]\}$ for which $(p)I[l]$. 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 $D(k, K)$.

These incidence relations are motivated by the linear interpretation of Lie geometries in terms of their Lie algebras [23] (see [24]).

Let us define the root subgroups U_α, where the root α belongs $\mathit{Root} = \tilde{A}_1 = \{(01), (11), (11), (12), (21), (22)', (22), \dots, (i, i), (ii)', (i, i+1), (i+1, i), \dots\}$. The group U_α is generated by the root transformations $t_\alpha(x)$, $x \in K$, of $P \cup L$, $\alpha \in \mathit{Root}$ were defined in the case of arbitrary commutative ring K in the [11]. The transformation $t_{0,1}(x)$ is an automorphism of $D(K)$ which transform point (p) as above to point with first coordinate $p_{01} + x$ and line $[l]$ to line with first coordinate l_{10}. Similarly the transformation $t_{1,0,}(x)$ is an automorphism of $D(K)$ which moves line $[l]$ to a line with first coordinate $l_{10} + x$ and point (p) to the poin with first coordinate p_{01}. Assume that elements of Root are listed above in the fixed natural order $<$. For α outside the set of simple roots (01) and (10) we consider graph automorphism $t_\alpha(x)$, $x \in K$ which leavs coordinate p_β of point (p) and l_β of line $[l]$ without change and moves p to $p_\alpha + x$ and l_α to $l_\alpha + x$. It is easy to see that group U generated by various U_α acts transitively on sets of points, lines and edges of the graph.

We define an incidence structure with point set P' and line set L' isomorphic to K^∞ which is a totality of tuples over K with a finite support. It will be convenient for us to denote vectors from P' as

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

and vectors from L as

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

We say that a point (x) is incident with a line $[y]$ and write xIy or $(x)I[y]$ if the following conditions are satisfied:

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

$y_{i,i+1} - x_{i,i+1} = x_{1,0}y_{i,i}$, (8)

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

We denote the graph of incidence relation of this incidence structure as $A(K)$.

We can identify the set of points P of graph $D(K)$ as function from $R_{0,1} = \mathit{Root} - \{(1,0)\}$ to K and the set of lines L with affine space of functions from $R_{1,0} = \mathit{Root} - \{(0,1)\}$ to K We consider the subsets $\mathit{Root}' = \{(01), (10), (11), (12), (22), (23), \ldots\}$, $R'_{0,1} = R_{0,1} \cap R'$ and $R'_{1,0} = R_{1,0,} \cap R'$ of *Root* of *Root*. It allows us to identify sets P' and L' with affine subspaces $\{f : R'_{0,1} \to K\}$ and $\{f : R'_{1,0} \to K\}$ of P and L respectively.

It is easy to see that restrictions of $R_{0,1)}$ and $R_{1,0}$ onto $R'_{0,1)}$ and $R'_{1,0}$ induce projections of affine spaces P anf L onto P' and L' and homomorphism η of graph $D(K)$ onto the graph $A(K)$.

We can check that element $t_\alpha(x)$, $\alpha \in R'_{0,1}$, $x \in K$ preserves affine subspaces P' and L'. Restriction of this transformation on $P' \cup L'$ is automorphism $\tilde{t_\alpha}$ of the graph $A(K)$,

PROPOSITION 3.1.

Group $\tilde{U}$ of automorphisms of $A(K)$ generated by various $\tilde{t_\alpha}(x)$, $\alpha \in R_{0,1}$, $x \in K t_\alpha(x)$, $\alpha \in R_{0,1}$, $x \in K$ acts transitively on the point set P'.

Let ${}^kR'_{0,1}$ be the set of first k elements of $R'_{0,1}$ accordingly to the chosen order. Symbol ${}^kR'_{1,0}$ stands for the set of first k elements of $R_{1,0}$. It is easy to see that restrictions of elements from P' and L' on ${}^kR'_{0,1}$ and ${}^kR'_{1,0}$ form affine spaces ${}^kP_k$ and ${}^kL$. We use ${}^kP$ and ${}^kL$ as partition set of incidence structute $I(k, K)$ with incidence relation defined by first $k-1$ equations of $A(K)$. It is possible to write points and lines simply as $(x_1, x_2, \ldots, x_k)$ and $[y_1, y_2, \ldots, y_k]$ and rerite equations in the form 6. So $I(k, K)$ are isomorphic to $A(k, K)$.

PROPOSITION 3.2.

Group ${}^k\tilde{U}$ of automorphisms of $A(k, K)$, $k \geq 2$ generated by various $\tilde{t_\beta}$, $\beta \in R'_{0,1}$, $x \in K$ acts transitively on the point set ${}^kP$.

LEMMA 3.1 (two numbers lemma accordingly [11]).

Let $(0)[{}^1y]I({}^2y)I\ldots I^ny$ be a path in the graph $A(n, K)$, $n \geq 4$, starting at the zero point $((0) = (0, 0, \ldots, 0))$ and determined by a sequence of colors $0, x_1, x_2, \ldots, x_{n-1}, x_n$. Then the last two components of the vertex ${}^ny$ are $\alpha = x_2(x_1 - x_3)\ldots(x_{n-3} - x_{n-1}(x_n - x_{n-2})$ and $\beta = -x_{n-1}\alpha$. where $x_2 \neq 0$, $x_i \neq x_{i+2}$, $i = 1, 2, \ldots, n-2$.

The fact that graphs $A(n, q)$, $q > 2$, $n = 2, 3, \ldots$ form a family of large girth was stated in [13] together with the first lower bound for the girth of $A(n, K)$ where K is a commutative integrity ring. The following statement essentially imroves this bound.

THEOREM 3.1.

Let K be a commutative integrity ring. Then the girth of graph $A(n, K)$ is $\geq 2n$. If K is a field then the girth of $A(n, K)$ is $2n$ or $2n + 2$.

PROOF. Graphs $A(2, K)$, and $A(3, K)$ are isomorphic to graphs $D(2, K)$ and $D(3, K)$ of girth at least 6 and 8 respectively. Let us consider graph $A(n, K)$, $n \geq 4$. Let us assume that it contains cycle C of length $2n - 2$. Automorphism group of $A(n, K)$ is point transitive. So without loss of generality we can assume that $(0, 0, \ldots, 0)$ is an element of C. It contains distinct neighbours $[x_1, 0, \ldots, 0]$ and $[\mathrm{y}_1, 0, \ldots, 0]$ of this point within the cycle C.

We can assume that one of the colours say x_1 differs with 0.

Then cycle contains the path $(0, 0, \ldots, 0)$, $[x_1, 0, 0, \ldots, 0]$, $(x_2, -x_1x_2 \ldots, 0)$, $\ldots$, v_n. Last two coordinates of v_n are $\alpha = x_2(x_1 - x_3) \ldots (x_{n-3} - x_{n-1})(x_n - x_{n-2})$ and $\beta = -x_{n-1}\alpha$ accordingly to previous lemma.

Noteworthy that conditions $x_2 \neq 0$ $x_i \neq x_{i+2}$, $i = 1, 2, \ldots, n - 2$ insure that all vertices of the path are different. The cycle C of length $2n - 2$ has to be complited by adding the chainn with starting vertex $[y_1, 0, \ldots, 0]$ and elements of colour y_2, y_3, $\ldots$, y_{n-2}. We can check that last vertex u of this chain will be the vertex with list of coordinates of kind $y_{n-2}, \ldots, 0, 0$. To make a cycle we need $u = v$ but $n - 1$-th coordinate of v differs from zero. So we get a contrudiction. We prove absence of cycles of kind C_{2n-2} in $A(n, K)$.

Noteworthy that absence of Cycles C_{2n-2s} in $A(n-s, K)$ insures that $A(n, K)$ does not have cycles of length $2n - 2s$.

So girth of $A(n, K)$ is $> 2n - 2$. Let us assume that K is a field and girth of graph $A(n, K)$ is $> 2n + 2$. Then $codim(A(n, K) < [(g - 1)/2]$ and it contradict to Theorem 2.1. So $g(A(n, K)$ is $2n$ or $2n + 2$.

REMARK. *Theorems 1.1 and 2.2 follow directly from Theorem 3.1.*

4 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 [18] and further references, [19] and [22] where multivariate maps of unbounded degree 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 [20],[21]. These constructions use graphs $A(n, K)$ and 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 degre 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 [15]).

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 $x_1 \to f_1(x_1, x_2, \dots, x_n)$, $x_2 \to f_2(x_1, x_2, \dots, x_n)$, …, $x_n \to f_n(x_1, x_2, \dots, x_n)$. 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 $End(F_q[x_1, x_2, \dots, x_n])$ 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 $x_i \to g_i(x_1, x_2, \dots, x_n)$, $i = 1, 2, \dots, n$ 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 $A(n.q)$ and their analogs $A(n, K)$ 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 [16]) 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 [17]).

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

1. Bolloba's B. *Extremal Graph Theory.* London: Academic Press, 1978, 440 P.
2. Bondy J.A. and Simonovits M.*Cycles of even lengthgin graphs*, J. Combin.Theory. Ser. B. 16. 1974. P. 87-105.
3. Faudree W., Simonovits M. *On a class of degenerate extremal graph problems*, Combinatorica. 3 (1). 1983, P. 83-93.
4. Erdős', Renyi A. and Sos V.T. *On a problem of graph theory*, Studia. Sci. Math. Hungar. 1. 1966. P. 215-220.
5. Erdős', Simonovits M. *Compactness results in extremal graph theory*, Combinatorica. 2 (3). 1982. P. 275-288.
6. Benson C.T.*Minimal regular graphs of girth eight and twelve*, Canad. Journal of Mathematics, . 18. 1966. P. 1091-1094.

7. Brown W.G. *On graphs that do not contain Thomsen graph*, Canad. Math. Bull. 9. No.3. 1966. P. 281-285.
8. Margulis G. *Explicit construction of graphs without short cycles and low density codes*, Combinatorica. 2. 1982, P. 71-78.
9. Lubotsky A., R. Philips R. and Sarnak P.*Ramanujan graphs*, J. Comb. Theory. 115, No.2. 1989. P. 62-89.
10. Lazebnik F., Ustimenko V.A. and Woldar A.J. *New Series of Dense Graphs of High Girth*, Bull (New Series) of AMS. v.32. No.1. 1995. P. 73-79.
11. Ustimenko V. Linguistic Dynamical Systems, *Graphs of Large Girth and Cryptography*, Journal of Mathematical Sciences.- Springer. v.140. No.3. 2007. P. 412-434.
12. V. Ustimenko, *On the extremal graph theory and symbolic computations*, Reports of Nath. Acad. of Sci. of Ukraine, 2013, No. 2, P. 42-49.
13. V. Ustimenko, *On new results on Extremal Graph Theory*, Theory of Algebraic Graphs and their applications in Cryptography and Coding Theory. Reports of Nath. Acad. of Sci. of Ukraine, 2022, No. 4, P. 42-49 (see IACR e-print Archive 2022/296). (PDF).
14. Shaska, T., Ustimenko, V. (2009). On the homogeneous algebraic graphs of large girth and their applications. Linear Algebra Appl., 430, No. 7, 2009, pp. 1826-1837.
15. *Post-Quantum Cryptography: Call for Proposals:https://csrc.nist.gov/*, Project: Post-Quantum-Cryptography-Standardization/Call-for-Proposals, Post-Quantum Cryptography: Round 2 Submissions.
16. Alexei G. Myasnikov; Vladimir Shpilrain; Alexander Ushakov. *Non-commutative Cryptography and Complexity of Group-theoretic Problems*. Amer. Math Soc. 2011.
17. 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.
18. 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,V43, P. 329–342, 2013.
19. V. Ustimenko, *Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world*, UMCS Editorial House, Lublin, 2022, 198 p.(to appear).
20. V. Ustimenko, *On new multivariate cryptosystems based on hidden Eulerian equations over finite fields*, IACR e-print Atchive, 2017/093.
21. Ustimenko V. A., *On new multivariate cryptosystems based on hidden Eulerian equations*, Reports of National Academy of Sci of Ukraine, N5, 2017.
22. 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.
23. V. A. Ustimenko, *Linear interpretation of Chevalley group flag geometries*, Ukraine Math. J. 43, Nos. 7,8 (1991), pp. 1055-1060.
24. V. A. Ustimenko,*On some properties of Chevalley groups and their generalisations*, In: Investigations in Algebraic Theory of Combinatorial objects, Moskow, Institute of System Studies, 1985, 134 - 138 (in Russian), Engl.trans.: Kluwer, Dordrecht, 1992, pp. 112-119.