On new results on Extremal Graph Theory, Theory of Algebraic Graphs and their applications in Cryptography and Coding Theory.

Vasyl Ustimenko

Institute of Telecommunications and the Global Information Space of the National Academy of Sciences of Ukraine, https://itgip.org/security/ and University of Maria Curie-Sklodowska (Poland, , Lublin 20036, vasyl@hektor.umcs.lublin.pl or E-mail: vasylustimenko@yahoo.pl

Abstract. *New explicit constructions of infinite families of finite small world graphs of large girth with well defined projective limits which is an infinite tree are described. The applications of these objects to constructions of LDPC codes and cryptographic algorithms are shortly observed.*

We define families of homogeneous algebraic graphs of large girth over commutative ring K.

For each commutative integrity ring K with |K|>2 we introduce a family of bipartite homogeneous algebraic graphs of large girth over K formed by graphs with sets of points and lines isomorphic K^n, n>1 and cycle indicator $\geq 2n+2$ such that their projective limit is well defined and isomorphic to an infinite forest.

***Key words**: family of graphs of large girth, small world graphs, cryptographic algorithms, LDPC codes.*

1. Introduction.

Girth and diameter of a graph are the minimal length of its cycle and the maximal distance of the graph. We can consider girth indicator *Cind(v)* of vertex *v* of the graph Γ as the minimal length the cycle through *v* and introduce cycle indicator *Cind(*Γ*)* of the graph as the maximal value of *Cind*(v) for its vertices.

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 classical projective geometry over various fields is a graph of girth 6 and diameter 3. J. Tits defined generalised m-gons as bipartite graphs of girth *2m* and diameter *m*. Feit and Higman proved that finite generalised 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 generalised m-gons for *m=3,4,6, 8*. Classification of flag transitive generilised *m*-gons of Moufang type were obtained by J. Tits and R.Weiss.

Infinite families of graphs of large girth of bounded degree are important objects of Extremal Graph Theory which were introduced by P. Erdős'. He proved the existence of such families via his well-known probabilistic method. Nowadays few explicit constructions of such families are known. The concept of infinite family of small world graphs of bounded degree turns out to be very important for various applications of graph theory.

Noteworthy that only one family of small world graphs of large girth is known. This is the family $X(p, q)$ of Ramanujan graphs introduced by Gregory Margulis [1] and investigated via the computation of their girth, diameter and the second largest eigenvale by A. Lubotsky, R.Phillips and P.Sarnak [2].

We have to admit that studies of families of graphs Γ_i with well defined projective limit Γ, which is isomorphic to infinite tree, is well motivated.

We refer to such family as tree approximation. There is only one approximation by finite graphs which is a family of large girth. This is the family of $CD(n, q)$ defined by F.Lazebnik, V. Ustimenko and A.Woldar [3].

The question whether or not $CD(n, q)$ form a family of small world graphs has been still open since 1995.

In 2013 the tree approximation by finite graphs $A(n,q)$ which is a family of small world graphs was presented (see [4]). It was proven that the graph from the family has maximal possible cycle indicator (in fact $Cind\ (A(n, q))=2n+2$).

One of the main statements of this paper is $A(n, q)$ where $n=2, 3,....$ is a family of large girth.

We generalise these results in terms of the theory of algebraic graphs defined over arbitrary field and consider properties and applications of above mentioned graphs.The paper is accepted for publication in Dopovidi Nath. Acad. Sci of Ukraine. Hope it appears shortly after the defeat of Russian state terroristic attack on Ukraine.

2. Case of finite simple graphs.

All graphs we consider are simple, i. e. undirected without loops and multiple edges. Let $V(\Gamma)$ and $E(\Gamma)$ denote the set of vertices and the set of edges of Γ, respectively. The parameter $|V(\Gamma)|$ is called the order of Γ, and |E(G)| is called the size of Γ. A path in Γ is called simple if all its vertices are distinct. When its convenient we shall identify Γ with the corresponding antireflexive binary relation on $V(\Gamma)$, i.e. $E(\Gamma)$ is a subset of $V(\Gamma)\times V(\Gamma)$. The length of a path is a number of its edges. The girth of a graph Γ, denoted by $g=g(\Gamma)$, is the length of the shortest cycle in Γ. Let $k\geq 3$ and $g\geq 3$ be integers. The distance between vertices v and u of the graph Γ is a minimal length of the path between them. The diameter of the graph is maximal distance between its vertices.

Graph is connected if its diameter is finite. Graph is k-regular if each vertex of the graph is incident exactly to k other vertexes. A tree is a connected graph which does not contain cycles

(1) An infinite family of simple regular graphs Γ_i of constant degree k and order v_i such that $diam(\Gamma_i) \leq c \log_{k-1}(v_i)$, where c is the independent of i constant and $diam(\Gamma_i)$ is diameter of Γ_i , is called a *family of small world graphs.*

(2) Recall that infinite families of simple regular graphs Γ_i of constant degree k and order v_i such that $g(\Gamma_i) \geq c \log_{k-1}(v_i)$,where $\boldsymbol{c}$ is the independent of i constant and $g(\Gamma_i)$ is a girth of Γ_i are called *families of graphs of large girth*.

Let Γ be a simple graph. Assume that $Cind(x)$ is the minimal length of cycle through vertex x of the graph Γ . Let C$ind(G)$ stand for the maximal *value* of $Cind(x)$ via all vertices x of Γ. We refer to parameter $Cind(G)$ as a cycle indicator of Γ.

One of the main purposes of the paper is to present a special interpretations of q-regular tree (q -regular simple graph without cycles) in terms of algebraic geometry over finite field F_q .

THEOREM 1. *For each prime power q, q>2 there is a family of q –regular graphs Γ_i satisfying following properties*

(i) Γ_i *is a family of small world graphs,*

(ii) Γ_i *is a family of large girth,*

(iii) Projective limit of graphs Γ_i *is well defined and coincides with q-regulat tree* T_q.

(iv) $Cind\ \Gamma_i = 2 \log_q(v_i/2)+2$.

We refer to family of graphs Γ_i satisfying condition (iii) as *tree approximation*.

The prove of Theorem 1 is given via explicit construction of graphs $\Gamma_i = A(i,q),\ i \geq 2$ satisfying requirements of the statement.

Noteworthy that $A(i,q)$ is a unique known example of the family satisfying conditions (i), (ii) an (iii).

In fact, there is exactly one other known construction of the q regular family satisfying (i) and (ii), i.e. explicit construction of the family of regular simple small world graphs of large girth and with an arbitrarily large degree q.

This family $X(p, q)$ formed Cayley graphs for $PSL_2(p)$, where p and q are primes, had been defined by G. Margulis [1] and investigated by A. Lubotzky, Sarnak and Phillips [2]. As it is easy to see the projective limit of $X(p, q)$ does not exist.

The construction of *A(n, q)*.

Let K be a finite field F_q.

We define $A(n, K)=A(n,q)$ 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 $(p)=(p_1, p_2, \dots, p_n) \in P_n$ and $[l]=[l_1, l_2, \dots, l_n] \in L_n$.

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

$p_2 - l_2=l_1p_1$,

$p_3 - l_3= p_1 l_2$,

$p_4 - l_4 = l_1p_3$,

$p_5 - l_3 = p_1 l_4$,

$\dots$,

$p_n - l_n = p_1 l_{n-1}$ for odd n and $p_n - l_n = l_1 p_{n-1}$ for even n.

We can consider an infinite bipartite graph $A(K)$ with points

$(p_1, p_2 ,\dots, p_n ,\dots)$ and lines $[l_1 , l_2 ,\dots,l_n , \dots]$.

PROPOSITION 1 [4]. *If $K=F_q$, $q>2$ then $A(n, F_q)$ is a family of small world graphs and tree approximation with $Cind(A(n, F_q))=2n+2$.*

Let K be an arbitrary field. We define $A(n, K)$ via simple change of F_q on K and announce the following statement

PROPOSITION 2.
Let K be a field. Then the girth of A(n,K) is $\geq 2[n/2]+2$.

Symbol $[\ x\ ]$ stands for the flow function from $\boldsymbol{x}$. Theorem 1 follows from propositions 1 and 2.

3. Case of algebraic graphs.

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 nonzero dimension and the edge set being a quasiprojective variety φ in Q × Q such that (x, x) is not element of φ for each $x \in Q$ and $x\varphi y$ implies $y\varphi x$ ($x\varphi y$ means $(x, y) \in \varphi$). The graph φ is homogeneous (or M-homogeneous) if for each vertex $v \in Q$ the set $\{x \mid v\varphi x\}$ is isomorphic to some quasiprojective variety M over F of nonzero dimension. We further assume that M contains at least 3 elements.

Theorem [5]. *Let Γ be homogeneous algebraic graph over a field F of girth g such that the dimension of neighborhood for each vertex is N, $N \geq 1$. Then $[(g - 1)/2] \leq dim(V)/N$.*

The following corollary is an analog of Even Circuit Theorem by Erdős' for finite simple graphs.

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

We announce a stronger statement.

Theorem 2. *Let Γ be homogeneous algebraic graph over a field F with cycle indicator z such that the dimension of neighborhood for each vertex is N, $N \geq 1$. Then $[(z - 1)/2] \leq dim(V)/N$.*

We refer to a family of homogeneous algebraic graphs φ_n for which dimension of neighborhood for each vertex is independent constant N, $N \geq 1$ as a family of *small world graphs* if diameter of each graph φ_n is bounded from above by linear function $\alpha n + \beta$ defined by constants α and β.

We refer to a family of homogeneous algebraic graphs φ_n for which the dimension of neighborhood for each vertex is independent constant N, $N \geq 1$ as a *family of large girth* if girth of each graph φ_n is bounded from below by linear function $\alpha n + \beta$ defined by constants α and β .

We refer to a homogeneous algebraic graph as algebraic forest if it does not contain cycles. Their term algebraic tree stands for the connected algebraic forest.

We say that family of homogeneous algebraic graphs φ_n is a forest (tree) approximation if projective limit of φ_n is an algebraic forest (tree) and formulate thaw following statement.

Theorem 3. *For each field F, F≠ F_2 there exists a tree approximation which is a family φ_n of small world algebraic graphs of large girth with the vertex set of dimension n and cycle indicator 2n+2.*

Family of graphs $\varphi_n=A(n, F)$ provides explicit construction of objects described in the theorem. As it follows from Theorem 2 homogeneous algebraic graphs $A(n, F)$ form a family with maximal possible girth indicator**.**

REMARK. Graphs $A(n, F_2)$ are disconnected. So they are disjoint union of cycles. Graph $A(F_2)$ is 2-regular forests with trees presented on the following diagram …. -----*-----*-----*--- .... .

Girth indicator of $A(n, F_2)$ coincides with its girth of size **≥ *2n+2.*** So, formally $A(n, 2)$ are algebraic graphs of large girth.

Noteworthy that cycles can be defined via the system of equations.

4. Some properties of *A(n,K)* and some their applications.

Graphs $A(n,q)$ obtained as homomorphic images of graphs $D(n,q)$ which defines projective limit $D(q)$ with points

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

lines

$[l]=[l_{19}, l_{11}, l_{12}, l_{21}, l_{22}, l'_{22}, \ldots, l'_{ii}, l_{i\,i+1}, l_{i+1,i}, l_{+i+1,i+1} \ldots]$

and incidence relation given by equations

l_{ii}-$p_{ii}=l_{10}\, p_{i-1,i}$;

$l'_{ii} - p'_{ii} = l_{i,i-1}\, p_{01}$;

$l_{i,i+1} - p_{i,i+1} = l_{ii}\, p_{01}$;

$l_{i+1i} - p_{i+1,i} = l_{10} p'_{ii}$.

This four relations are defined for $i\geq 1$, ($p'_{11}= p_{11}$, $l'_{11}= l_{11}$).

REMARK. *You can see that indexes of vectors correspond to coordinates of positive roots of root system A_1 with a wave.*

Historically graph *D(q)* is not the first example of description of *q*-regular forest in terms of Algebraic Geometry. Geometries of buildings (see [3], [4]) corresponding to extended Dynkin diagram A_1 as incidence structures are *q+1*-regular trees or *q+1*-regular forests. As a result we get a description of a tree in group theoretical terms.

In [6] it was noticed that the restriction of this incidence relation on orbits of Borel subgroup B^- acting on maximal parabolics are *q*-regular bipartite graphs. So we get a description of a *q*-regular tree in terms of positive roots of A_1 with a wave.

In [7] authors proved that *D(n,q)* defined via first *n-1*equations of *D(q)* form a family of graphs of large girth.

Unexpectedly we discover that these graphs are disconnected if $n \geq 6$**.** So forest *D(q)* contains infinitely many trees and the diameter is an infinity. F. Lazebnik conjectured that connected components of graphs *D(n,q), n =3,4*, … form a family of small world graphs. This conjecture is still open.

In 1994 we found out how to describe connected components *CD(n, q)* of graphs *D(n, q)* in terms of equations (see [4],]8]).

Graphs *A(n, q)* were obtained in 2007 as homomorphic images of graphs *D(n, q)* ([9]). Corresponding homomorphism $\acute{\eta}$ is a procedure to delete coordinates of points and lines with indexes *(i+1, i)* and *(i,i)'*.

The self importance of these graphs have been justified in my joint research with U. Romanczuk (see [10] and further references) and M. Polak [11] via applications to Cryptography and Coding Theory.

In the case of families of graphs of large girth we would like to have " speed of growth" *c* of the girth "as large as it is possible".

P. Erdos' proved the existence of such a family with arbitrary large but bounded degree *k* with *c=1/4* by his probabilistic method.

In the case of families $X(p,q)$ and $CD(n,q)$ the constant c is $4/3$. In the case of $A(n,q)$ we just get inequality $1 \leq c < 2$. So exact computation of the girth is the area of the future research.

There are essential differences between family of graphs $X(p, q)$ and tree approximations. Recall that the projective limit of $X(p, q)$ does not exist.

We prove that bipartite graphs $A(n,q)$ are not edge-transitive and not vertex transitive (transitivity on points and intransitivity on lines) Noteworthy that their projective limit T (the tree) is obviously an edge-transitive infinite graph.

The usage of generalizations and modifications of graphs $A(n,q)$ allows us to construct postquantum cryptosystem of El Gamal type with encryption procedure for potentially infinite vector from F_q with the execution speed $O(n^{1+2/n})$ (see [16]).

In fact the diameter of $A(n,q)$ is growing slower than diameter of $X(p,q)$. So, $A(n,q)$ are the best known small world graphs among known families of large girth. Recall the girth of $A(n,q)$ is not yet computed precisely.

So, the comparison of growth of the girth for $A(n,q)$ and $X(p,q)$ is the interesting task for the future research.

In the case of finite fields both families are expanding graphs, the second largest eigenvalue of $A(n, q)$ tends to $2q^{1/2}$, they are not Ramanujan graphs for which the second largest eigenvalue has to be bounded above by $2(q-1)^{1/2}$.

The family $X(p,q)$ is formed by Ramanujan graphs, so they are better expanding graphs than $A(n, K)$.

Families $X(p,q)$, $CD(n,q)$ and $A(n,q)$ can be used for the constructions of LDPC codes for noise protection in satellite communications. D. MacKay and M. Postol [12] proved that $CD(n, q)$ based LDPC codes have better properties than those from $X(p,q)$ for the constructions of LDPC codes.

Together with Monika Polak we proved that $A(n,q)$ based LDPC codes even better than those from $CD(n,q)$ (see [11]).

Cayley nature of $X(p,q)$ does not allow to use these graphs in cryptography. Various applications of graphs $D(n,q)$, $CD(n,q)$ and $A(n,q)$ have been known since 1998.

The most recent postquantum cryptosystem based on noncommutative multivariate group associated with $A(n,q)$ is described in [13], IACR e-print Archive 2021/1466. .

This algorithm can be used for the encryption of potentially infinite vectors from $(F_q)^n$ in time $O(n^{1+2/n})$. So it can work with Big Data files.

5. The case of integrity rings.

Let K stand for an arbitrary commutative ring.

Noteworthy that graphs $A(n, K)$ are defined over arbitrary commutative ring K have been already defined. Graphs $D(k,K)$ over K are considered in [14]
where graphs $CD(k,K)$ with $k \geq 6$ were introduced for as induced subgraphs of $D(k,K)$ with vertices u satisfying special equations $a_2(u)=0$, $a_3(u)=0,\ldots$, $a_t(u)=0$, $t=[(k+2)/4]$, where $u = (u_\alpha, u_{11}, u_{12}, u_{21}, \ldots, u_{r,r}, u'_{r,rt}, u_{t\,t+1}\, u_{r,r+1}, u_{r+1,r}, \ldots)$,

$2 \leq r \leq t$, $\alpha \in \{(1, 0), (0,1)\}$ is a vertex of $D(k, K)$ and

$a_r = a_r(u)=\Sigma_{i=0,r}(u_{ii}\, u' - u_{i,i+1}\, u_{r-i,r-i-1})$ for every r from the interval $[2,t]$.

We set $a=a(u)=(a_2, a_3, \ldots, a_t)$ and assume that $D(k, K)=CD(k,K)$ *if* $k=2,3,4,5$.

As it was proven in [9] graphs $D(n,K)$ are edge transitive. So their connected components are isomorphic graphs. Let ${}^vCD(k,K)$ be a solution set of system of equations $a(u)=(v_2,v_3,\ldots,v_t)=v$ for certain $v \in K^{t-1}$. It is proven that each ${}^vCD(k,K)$ is the disjoint union of some connected components of graph $D(n,K)$.

It is easy to see that sets of vertices of ${}^vCD(k,K)$, $v \in K^{t-1}$ form a partitions of the vertex set of $D(n,K)$.

The concept of quasiprojective variety over commutative ring K can be introduced via simple substitution of K instead of field F. It leads to concepts of homogeneous algebraic graphs over K, forest and tree approximations and families of graphs of large girth over K. It was proven that for the case of commutative ring K with unity of odd characteristic graphs $CD(n,K)$ are connected (see [15]). So graph $CD(n,q)=CD(n, F_q)$ for odd q is a connected component of $D(n,q)$.

As it follows from definitions the image of restriction of homomorphism ή from $D(n, K)$ onto $CD(n, K)$ coincides with $A(n, K)$.

So graphs *A(n,K)* are connected for the case of *K* with unity of an odd characteristic.

Theorem 4. *For each commutative integrity ring K the families of graphs CD(n, K), n=2,3,… and A(n, K),n=2,3,.. are forest approximations and families of graphs of large girth.*

The content of the paper was present as a talk at the international conference " At the End of Year 2021", Kyiv. The talk was dedicated to the memory of Volodymyr Vasilievich Sergeichuk (1949-2021), who was a prominent member of algebraic community of Ukraine.

REFERENCES

1. G. Margulis(1988). Explicit group-theoretical constructions of combinatorial schemes and their application to desighn of expanders and concentrators, Probl. Peredachi Informatsii, 24, No. 1, p.51-60.
2. A. Lubotsky, R. Philips, P. Sarnak (1989). Ramanujan graphs, J. Comb. Theory, 115, No. 2, p. 62-89. https://doi.org/10.1007/BF02126799
3. Lazebnik F., Ustimenko V. A. and Woldar A. J (1995). New Series of Dense Graphs of High Girth //Bull (New Series) of AMS, 32, No. 1, p. 73-79. https:/doi.org/10.1090/S0273-0979-1995-00569-0
4. V. A. Ustimenko (2013). On the extremal graph theory and symbolic computations, Dopovidi National Academy of Sci, Ukraine, No. 2, p. 42-49.
5. T. Shaska, V. Ustimenko (2009). On the homogeneous algebraic graphs of large girth and their applications, Linear Algebra and its Applications, 430, No. 7, p. 1826-1837. https:/doi.org/10.1016/j.laa.2008.08.023
6. V. Ustimenko (1989). Affine system of roots and Tits geometries, Voprosy teorii grupp i gomologicheskoy algebry, Yaroslavl, p.155-157 (in Russian).
7. F. Lazebnik, V.Ustimenko (1993). Some Algebraic Constractions of Dense Graphs of Large Girth and of Large Size, DIMACS series in Discrete Mathematics and Theoretical Computer Science, 10, p.75-93. https:/doi.org/10.1090/dimacs/010/07

8. F.Lazebnik, V. Ustimenko and A. J. Woldar (1996). A characterisation of the components of the graphs D(k,q), Discrete Mathematics,157, p. 271-283. https:/doi.org/10.1016/S0012-365X(96)83019-6
9. V.Ustimenko (2007). Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography, Journal of Mathematical Sciences, Springer, 140, No. 3, p. 412-434. https:/doi.org/ 10.1007/s10958-007-0453-2
10. V. A. Ustimenko, U. Romanczuk (2012). On Dynamical Systems of Large Girth or Cycle Indicator and their applications to Multivariate Cryptography, in "Artificial Intelligence, Evolutionary Computing and Metaheuristics ", In the footsteps of Alan Turing Series: Studies in Computational Intelligence, 427, p. 257-285. https:/doi.org/ 10.1007/978-3-642-29694-9_10
11. M. Polak, V. A. Ustimenko (2012). On LDPC Codes Corresponding to Infinite Family of Graphs A(k,K). Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS), CANA , Wroclaw, p. 11-23.
12. D. MacKay and M. Postol (2003). Weakness of Margulis and Ramanujan - Margulis Low Dencity Parity Check Codes, Electronic Notes in Theoretical Computer Science, 74, p.97-104. https:/doi.org/ 10.1016/S1571-0661(04)80768-0
13. Vasyl Ustimenko (2021). On semigroups of multivariate transformations constructed in terms of time dependent linguistic graphs and solutions of Post Quantum Multivariate Cryptography, IACR e-print archive 2021/1466.
14. V. Ustimenko (1998). Coordinatisation of Trees and their Quotients, in the Voronoj's Impact on Modern Science, Kiev, Institute of Mathematics, 2, p. 125-152.
15. V. Ustimenko (2009). Algebraic groups and small world graphs of high girth, Albanian Journal of Mathematics,3, No. 1, p. 25-33