IWONT, 21.07.2023

On families of homogeneous algebraic graphs of large girth and corresponding polynomial transformation of free modules.

Vasyl Ustimenko [1,2]

[1]*Royal Holloway University of London*

[2]*Institute of telecommunication and global information space, NAS of Ukraine*

E - mail: Vasyl.Ustymenko@rhul.ac.uk,

Abstract.

Homogeneous algebraic graphs defined over an arbitrary field are classical objects of Algebraic Geometry. 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 the minimal codimension $v(g)$ of an algebraic graph of prescribed girth g.

We use known constructions of families of homogeneous bipartite algebraic graphs of increasing girth defined over arbitrary integrity domain K for the constructions of families of polynomial transformations of affine varieties K^n (free modules over K), $n=1,2,\dots$ of polynomial degree $k=2, 3$. Some applications of these families of groups to Theoretical Computer Science will be discussed.

1. On special optimisation problem 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 $\boldsymbol{F}$ is a set of elements constructed from a vector space over $\boldsymbol{F}$ 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 $\boldsymbol{Q}$ is called a *quasiprojective variety*, if it is the set of all solutions of some system of homogeneous polynomial equations and inequalities.

If $\boldsymbol{F}$ is a field than we can define a dimension ***dim Q*** of $\boldsymbol{Q}$ as maximal dimension of subvariety isomorphic to $\boldsymbol{F}^n$.

EXAMPLES.

1) If $Q=F^n$ then dimension of Q is n.

2) If Q is Grassmanian , i. e. the totality of m-dimensional subspaces of F^n. Then Q is subdivided into orbits $C_n{}^m$ of group $UT_n(F)$ unitriangular matrices of kind F^i, $i\geq 0$. The maximal orbit is a vector space of dimension $m(n-m)$. So $dim(Q)=m(n-m)$.

3) Let us consider generalised m-gons corresponding to Chevalley groups $A_2(F)$, $B_2(F)$ and $G_2(F)$, $m=3, 4, \ldots, 5$ respectively Borel subgroups has orbits on partition sets of these bipartite graph of kind F^i, $i\geq 0$, $i=0, 1,\ldots, m-1$. So the dimension of the vertex set of this thick generalise m-gon is $m-1$.

An algebraic graph ψ over F consists of two things: the vertex set Q being a quasiprojective

variety over F of non-zero dimension and the edge set being a quasiprojective variety ψ in $Q \times Q$

such that (x, x) is not element of ψ for each x from Q,

and $x \ \psi \ y$ implies $y \ \psi \ x$ ($x \ \psi \ y$ means (x, y) is an element of ψ.

The graph ψ is homogeneous (or N-homogeneous), if for each vertex w from Q, the set $\{x \mid w \ \psi \ x\}$ is

isomorphic a quasiprojective variety $M(w)$ over F of a non-zero finite 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(ψ)=dim(Q)/N*** as codimension of an algebraic graph ***ψ***.

One of natural generalisation is homogeneous algebraic graph over commutative ring K can be obtained via straightforward change of field ***F*** for ***K.***

Studies of algebraic graphs with some restrictions on their cycles are motivated by the following 3 areas in Mathematics.

1) Investigations in the case of finite case are motivated by Extremal Graph Theory. WE HAVE NICE INVITED TALK BY FELIX LAZEBNIK few minutes ago.

2) 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. J. Tits defined generalised ***m***-gons as a bipartite graph of girth ***2m*** and diameter ***m*.**

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***.

3) 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 minimal cycles in ***$G_i(F)$*** are naturally required in this cases

A possibility to define ***For*** 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.***

4) Studies of walks on homogeneous algebraic graphs over rings ***$K[x_1, x_2, \ldots, x_n]$*** motivated by the THEORY OF SYMBOLIC COMPUTATIONS.

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.***

The first example of the family of graphs of large girth over arbitrary field was introduced in [1998] where was stated that graphs $D(n,K)$ over arbitrary infinite integrity domain have girth $\geq 2[(n+5)/2]$. This fact was proven in [Ustimenko, Journal of Math Sci, 2007]. A bit more short prove without usage of terminology of linguistic dynamic systems theory is given in [IACR e-print archive, https://eprint.iacr.org/2022/1668.pdf].

In [T. Shaska , Ustimenko] it was proven that the girth of ***D(n, F)*** defined **over the field *F* of characteristic zero** equals 2***[***(***n+5)/2].***

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

Theorem [T. Shaska, V. Ustimenko, Lin. Alg and its Appl].

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 ≥1.*** Then ***codim(G) = dim(Q)/N ≥[(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.

v(g) ≥ [(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 1.

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

$$k \leq v(g) \leq (3k-3+e)/2$$ where $e = 0$ if k is odd, and $e = 1$ if k is even.

*(graphs **CD(n,F)**)*

Let F be a field $F \neq F_2$. We introduce ${}^{F}v(g)$ 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, $F \neq F_2$.

The upper bound for ${}^{F}v(g)$ can be heavy dependable from the choice of field.

THEOREM 2.

There are algebraic Moore graphs of girth 6, 8, 10, 12

C_4, C_6, C_8 , C_{10} of codimensions 3, 4, 5 and 6 respectively.

(regular generalised **m**-gons for ***m=3, 4 , 6*** and graph ***A(4, 4)).***

REMARK. Instead of generalised triangles and quadrangles one can take **graphs *D(2, F)* and *D(3, F)* (affine parts of generalised polygons).**

THEOREM.

$$\mathbf{6 \leq \nu(14) \leq {}^{F}\nu(14) \leq 7}$$

It follows from the fact that the girth of algebraic graph ***A(7, F$_4$)*** equals to

14 .

CONJECTURE.

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

2. **OTHER OPTIMISATION PROBLEMS FOR 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 $c\log_{k-1}(v_i)$ 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 dimensions 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. In the case of intransitive graphs the re is an interesting problem of computing CYCLIC GAP which is the DIFFERENCE between cycle indicator and girth. Some results can be found via the link
https://grahameerskine.co.uk/OU/Slides/Ustimenko.pdf

PROBLEMS.

We can look at

1) minimal codimensions of homogeneous algebraic graphs without CYCLES ***C_{2n}* ,**

2) minimal codimensions of homogeneous algebraic graphs with CYCLE INDICATOR ***2n*,**

3) maximal codimension of bipartite homogeneous graph ***cod*** of diameter ***d*.**

***cod≤d-1*.**

(generalised m-gons are optimal points of this optimisation problem,

cod=m-1 and diameter m)

EXAMPLE OF FAMILIES are BELOW

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 ***$(p)=(p_1, p_2, \dots , p_n) \in P_n$*** 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.

$p_2 - l_2 = l_1 p_1,$

$p_3 - l_3 = p_1 l_2,$

$p_4 - l_4 = l_1 p_3,$

$p_5 - l_5 = p_1 l_4,$

$\dots,$

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

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

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

We proved that for each odd ***n*** girth indicator of ***A(n, K)*** is at least ***2n+2.***

FOR THE COMPARISON look at the following edge transitive graphs.

GRAPHS *D(n, K)*

The following interpretation of a family of graphs ***D(n. K)*** in case of general commutative ring ***K*** is convenient for the computations. Let us use the same notations for points and lines as in previous case of graphs ***A(n, K).***

Points and lines are elements of two copies of the affine space over

K. Point $(p)=(p_1, p_2, \dots , p_n)$ is incident with the line $[l]=[l_1, l_2 , \dots , l_n]$ if the following relations between their coordinates hold:

$p_2 - l_2=l_1p_1,$

$p_3 - l_3= p_1 l_2,$

$p_4 - l_4 = l_1p_3,$

$\dots,$

$l_i-p_i=p_1l_{i-2}$ if i congruent to 2 or 3 modulo 4,

$\boldsymbol{l_i - p_i = l_1 p_{i-2}}$ if ***i*** congruent to ***1*** or ***0*** modulo ***4.***

APPLICATIONS OF GRAPHS OVER COMUTATIVE RINGS TO THEORY OF SYMBOLIC COMPUTATIONS AND POSTQUANTUM CRYPTOGRAPHY.

Postquantum Cryptography is searching for security protection algorithms with resistance to adversarial attacks with the usage of Quantum Computer. In ALGEBRAIC PC the usage of SYMBOLIC COMPUTATION and symbolic transformations of affine space K^n , K is a commutating ring, of kind $x_i \to f_i(x_1, x_2, \ldots, x_n), i=1, 2, \ldots, n$ where f_i are nonlinear elements of $K[x_1, x_2, \ldots, x_n]$ is looking promising. WHY?

Let us compare Deterministic Turing machine and strange probabilistic Quantum Computer, which does not allow to repeat the computation twice.

1.Quantum Computer (QC) can factor number essentially faster than Turing machine. Here problem of impossibility to repeat the Quantum computation twice is not so important. One can check whether or not outcome of QC computation is right on ordinary PC which can multiply numbers fast. Similar situation is with Discrete Logarithm Problem.

2.We can form the list of problems for which QC has advantage in a comparison with including Fourier transform or Grover search techniques in information space, Optimisation problems with easily computable aim functions, and etc. But the area of Symbolic Computations looks like definite area where Turing Machine has advantage.

The verification of symbolic computations obtained via QC looks like almost impossible task.

because if we recompute written above symbolic computation second time then all coefficients of f_i will be changed. So symbolic computations can bring promising implementations of schemes from Noncommutative Cryptography or Multivariate Cryptography.

Let us consider the following important object of Algebraic Geometry.

Affine Cremona Group ${}^{n}CG(K)$ is defined as endomorphism group of polynomial ring

$K[x_1, x_2,..., x_n]$ over the commutative ring K. It is an important object of Algebraic Geometry (see Max Noether paper [Math Annales 1904] about mathematics of Luigi Cremona - prominent figure in Algebraic Geometry in XIX).

Element of the group

σ can be given via its values on variables, i. e. as the rule $x_i \to f_i(x_1, x_2, \ldots, x_n)$, $i=1, 2,\ldots, n$. This rule induces the map $\sigma': (a_1, a_2,.., a_n) \to (f_1(a_1, a_2,.., a_n), f_2(x_1, x_2, \ldots, x_n),\ldots, f_n(x_1, x_2,\ldots, x_n))$.

In the case when K is a finite field or arithmetic ring Z_m of residues modulo m elements of affine Cremona Groups or Semigroups are used in encryption algorithms of Multivariate Cryptography.

Let us assume that element σ is given via so called standard form, i. e. monomial terms of each f_i are listed in the lexicographical order.

We define degree of σ as maximal degree of f_i .

We say that the piece of information T is a *trapdoor accelerator* for nonlinear σ if the knowledge of T allows us to compute the reimage of given value b in time $O(n^2)$.

Of course it is just an instrument to search for practical trapdoor functions for which without knowledge of secret T the computation of reimage in polynomial time is impossible.

The existence of theoretical trapdoor functions is closely related to the open conjecture that $P \neq NP$.

The following *inverse problem* is an interesting for applications. Assume that σ_n is a family of quadratic or cubic elements of ${}^{n}CG(K)$ given in the standard form and it has hidden trapdoor accelerator. Find some trapdoor accelerator for this map.

We define degree of subgroup G of ${}^{n}CG(K)$ as maximal degree of representatives of G.

Theorem 1. For each commutative ring K cardinality ≥ 3 with unity, each positive integer n, $n \geq 2$, $k = 2, 3$ there is noncommutative subgroup ${}^{k}G(n, K)$ of degree k in ${}^{n}CG(K)$ such that each nonlinear element of ${}^{n}G(K)$ has a trapdoor accelerator.

Remark 1. We can change group ${}^{k}G(n, K)$ of Theorem 1 for ${}^{n}L\,{}^{k}G(n, K)\,{}^{n}L^{-1}$, where ${}^{n}L \in AGL_n(K)$ is some family of affine transformations of K^n.

In fact two versions ${}^{k}GD(n, K)$ *and* ${}^{k}GA(n, K)$ *of a family of subgroups* ${}^{k}G(n, K)$, $n = 2, 3, \ldots$ *as in Theorem 1 were defined constructively in terms of walks on graphs* $D(n, K)$ *and* $A(n,K)$.

If K *is a finite commutative ring then constructed versions of* ${}^{k}G(n, K)$ *are* **‘’LARGE’’:** *the projective limit of these* ${}^{k}G(n, K)$ *is well defined for each* K *and resulting group is an infinite one.*

REMARK 2.

Theorem 1 is far for trivial. Let us consider the affine Cremona Semigroup ${}^{1}CS(K)$.
We see that the product of two maps $x \to x^2$ and $x \to x^3$ will be the map of degree 6.
In fact it holds for vast majority of pairs of endomorphisms of $K[x_1, x_2, ..x_n]$. We have to multiply the degrees.

So elements as in Theorem 1 are very special, the product of two quadratics elements is a quadratic map again. Similarly the product of two cubic elements is a cubic transformation again.

Clearly that symbolic computations in groups ${}^{3}G(n, K)$ are feasible.

That is why they can be used as platforms for protocols of Noncommutative Cryptography.

Theorem 2. For each $n \geq 2$ affine Cremona group ${}^{n}CG(F_q)$, $q=2^s$ contains quadratic automorphism σ with trapdoor accelerator and the inverse of degree $\geq 2^{s-1}$.

Theorem 3. Let $K= F_q$, $q=2^s$ and ${}^{2}G(n, K)$ be one of the groups ${}^{2}GD(n, K)$ and ${}^{2}GD(n, K)$. *If* σ_1 is nonlinear representative of ${}^{2}G(n, K)$ and σ_2 such as in Theorem 2 then $\sigma_1\sigma_2$ is also quadratic and its inverse has degree at least 2^{s-1}.

Example. In the case of $q=2^{64}$ the degree of inverse is at least 2^{63}.

Applications of these statement to CRYPTOLOGY can be found in my recorded talk by July 3, 2023 , Sumy Ukraine , Int. Ukrainian Algebraic Conference 2023

https://sites.google.com/view/iacu2023

or my talk at Linz (Austria) by July 4 , 2023 at Central European Conference on Cryptology

https://secsys.lit-systems.jku.at/cecc2023/

Application to construction of pseudorandom real sequences were presented at https://www.newton.ac.uk/event/FD2W02/,

CAMBRIDGE, March 2022

ONE OF THE CONSTRUCTIONS.

Let $\Gamma(n, K)$ be one of the graphs $D(n, K)$ or $A(n, K)$ with points $x=(x_1, x_2,\dots, x_n)$ and lines $y=[y_1, y_2, \dots, y_n]$ with colours $c(x)=x_1 \epsilon K$ and $c(y)=y_1 \epsilon K$.

Each vertex has exactly one neighbour of this bipartite graph of selected colour. So the path in the graph is uniquely defined by initial vertex and the sequence of consecutive colours.

So we consider $\Gamma(n, K[x_1, x_{2.},\dots, x_n])$ and the chain with initial point

$(x_1, x_2,\dots, x_n)$ and colours $x_1+\alpha_1, x_1+\alpha_2,\dots. , x_t+\alpha_{2t}$

The destination point of this chain will be point $(x_t+\alpha_{2t}, g_2, g_3,\dots,g_n)$

where g_i are cubical polynomials from $K[x_1, x_2,\dots,x_n]$).

We consider automorphism $\sigma= \sigma(a_1, a_2, \dots, a_{2t})$:

$x_1 \to x_t + \alpha_{2t},\ x_2 \to g_2(x_1, x_2, \ldots, x_n),\ x_3 \to g_3(x_1, x_2, \ldots, x_n),\ \ldots,\ x_n \to g_n(x_1, x_2, \ldots, x_n).$

of affine Cremona Group ${}^{n}CG(K)$.

Various automorphisms of kind $\sigma(a_1, a_2, \ldots, a_t)$, $t=O(n)$ generate subgroup

${}^{3}G(n, K)$ such as in Theorem 1.

The tuple $\alpha_1, \alpha_2, \ldots., \alpha_{2t}$ can be considered as a trapdoor accelerator of the map σ

written in its standard form.

REMARK.

Noteworthy that groups $GD(n, K)$ are much different from

$Aut\ D(n, K)$. They are acting of different sets P and PUL respectively.

Number of ***GD(n, K)*** orbits on ***K^n*** coincides with the number of connected components of ***D(n, K)*** but group ***Aut D(n, K)*** is vertex and edge transitive.

Let ***$K \neq F_2$*.** Group ***GA(n, K)*** acting on ***K^n*** is transitively put transformation group ***Aut A(n. K)*** is intransitive on ***PUL.***

Quite large subgroup of ***Aut A(n. K)*** are described in my reprint

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

https://eprint.iacr.org/2022/1668.pdf

THANK YOU FOR YOUR ATTENTION