On geometries of Kac-Moody groups and Symbolic Computations.

Vasyl Ustimenko[1,2]

[1] Institute of telecommunications and global information space, Kyiv, Ukraine

[2] Royal Holloway University of London, United Kingdom.

1. On the generalisations of the geometries of Chevalley groups.

The incidence system is the triple (Γ, I, t) where I is a symmetric antireflexive relation (simple graph) on the vertex set Γ, $t : \Gamma \to N$ is a type function onto the set of types N such that $\alpha I \beta$ and $t(\alpha) = t(\beta)$ implies $\alpha = \beta$.

An important example of the incidence system as above is the so-called *group incidence system* $\Gamma(G, G_s), s \in S$. Here G is the abstract group and $G_s, s \in S$ is the family of distinct subgroups of G.

The elements of $\Gamma(G, G_s), s \in S$ are the left cosets of G_s, in G for all possible $s \in S$. Cosets α and β are incident precisely when

$|\alpha \cap \beta| \neq 0$. The type function is defined by $t(\alpha)=s$ where $\alpha = gG_s$ for some $s \in S$.

Let (W, S) be Coxeter system, i.e. W is a group with a set of distinguished generators given by $S=\{s_1, s_2, \dots, s_l\}$ and generic relation $(s_i s_j)^{m(i,j)}=e$. Here $M=(m(i,j))$ is a symmetrical l times l matrix with $m(i,i)=1$ and off-diagonal entries satisfying $m(i,j) \geq 2$.

Let us take $W_i = \langle S-\{s_i\} \rangle, 1 \leq i \leq l$ and consider a group incidence system $\Gamma(W)=\Gamma(W, W_i), 1 \leq i \leq l$. This geometry is called Coxeter geometry of W. Then W_i are referred to as the maximal standard subgroups of W.

Geometries of BN-pairs.

Let G be a group, B and N subgroups of G, and S be a collection of cosets of $B \cap N$ in N. We call

(G, B, N, S) *Tits system* (or we say that G has a BN-*pair*) if

(i) $G=\langle B, N \rangle$ and $B \cap N$ is normal in N,

(ii) S is a set of involutions which generate $W=N/(B \cap N)$,

(iii) sBw is a subset in $BuB \cap BswB$ for any $s \in S$ and $w \in W$,

(iv) (iv) $sBs \neq B$ for all s from S.

Properties (1)-(iv) imply that (W, S) is a Coxeter system.

Whenever (G,B, N, S) is Tits system we call the group W by Weyl group of the system or more usually Weyl group of G.

The subgroups P_i of G defined by BW_iB are called the *standard maximal parabolic subgroups* of G.

The group incidence system $\Gamma(G) = \Gamma(G, P_i), \{1 \leq i \leq l\}$ is commonly referred to as *Lie geometry* of G.

Kac – Moody group G is a group with BN pairs defined via the pair (A, F) where A is generalised Cartan matrix and F is the field.

Recall that A is a square matrix with diagonal entries 2 and negative integers in other entries. It defines Coxeter-Dynkin diagram $X_l=X_l(A)$.

(1) Definition of Kac-Moody Lie Algebra $L(A, F)$.
(2) Take inner automorphism of $L(A, F)$ and construct Kac Moody group $G=G(A, F)$ with the Tits system (G, B, N, S).

Generalised Cartan matrix defines the Weyl group $W(A)$ of the BN-pair G.

If $W(A)$ is a finite irreducible Coxeter group then G is Chevalley group over the field F with associated with Coxeter - Dynkin diagram X_l which belongs to the list $A_n, n\geq 2$, $B_n, n\geq 2$, $C_n, n\geq 2$, $D_n, n\geq 4$, G_2, F_4, E_6, E_7, E_8.

Let us fix Kac-Moody group $G(F)=X_l(F)$ with corresponding Weyl group W.

Let us consider the description of the geometry $\Gamma(G(F))$ as algebraic variety in sense of Zariski topology.

The following bipartite graphs are analogue of planar ternary rings introduced by M. Hall for the description of Projective Planes.

Let K be a commutative ring with the unity.

Jordan-Gauss graph over K is an incidence structures with partition sets P (points) and L (lines) isomorphic to affine spaces V_1 and V_2 over K such that the incidence relation is given by special quadratic equations over the commutative ring K with unity such that the neighbour of each vertex is defined by the system of linear equation given in its row-echelon form.

We assume that V_i, $i=1,2$ are finite dimensional spaces of kind K^n or infinite dimensional affine spaces formed tuples with finite support.

The formal description follows.

Jordan-Gauss graph $J(K)$ is the special case of linguistic graph of type (s, r) given by the following way.
We identify points with tuples of kind $(x)=(x_1, x_2,\ldots, x_n,\ldots)\epsilon V_1$ and lines with tuples $[y] =[y_1, y_2,\ldots, y_n,\ldots] \epsilon V_2$. Brackets and parenthesis are convenient to distinguished type of the vertex of the graph. If (x) and $[y]$ are incident $(x)I[y]$ if and only if the following relations hold.

$$a_1x_{s+1}-b_1y_{r+1}=f_1 (x_1, x_2 ,\ldots , x_s, y_1, y_2, \ldots , y_r),$$
$$a_2x_{s+2}-b_2y_{r+2}=f_2 (x_1, x_2 ,\ldots , x_s, x_{s+1}, x_{s+1}, y_1, y_2, \ldots , y_r, y_{r+1}), (1)$$
$$\ldots$$
$$a_mx_{s+m}-b_my_{r+m}=f_m(x_1, x_2 ,\ldots ,x_s, x_{s+1},\ldots, x_{s+m-1}, y_1, y_2, \ldots , y_r, y_{r+1}, \ldots,y_{r+m-1})$$
$$\ldots.$$

where a_j, and b_j, $j=1,2,\ldots,m$ are not zero divisors, and f_j are quadratic multivariate polynomials with coefficients from K.
We assume that f_j are given in their standard form , i. e. the list of monomial terms ordered lexicographically.

We say that two Jordan graphs $J_1(K)$ and $J_2(K')$ are symbolically equivalent if they are given by the system of kind (1) with the same number of equations over commutative rings K and K' where quadratic polynomials f_j have the same list of monomial terms with nonzero coefficients.

Let Γ be an incidence system with partition sets Γ_i, $i=1,2,\ldots, m$ and incidence relation I. We say that partition of Γ into sets J_k, $k=1, 2, \ldots, l$ is Jordan-Gauss equivalence over commutative ring K if for incident elements α and β there is a Jordan - Gauss graph $J(k(\alpha), k(\beta))$ over K with sets of points $J(\alpha)=J_{k(\alpha)}$ and lines $J(\beta)= J_{k(\beta)}$ such that $\alpha\epsilon J(\alpha)$, $\beta\epsilon J(\beta)$ and α, β form an edge of J_l.

Theorem 1. *Let F be a field, $G(F)$ be a Kac-Moody group and $\Gamma(G(F))$ be a Kac -Moody geometry of $G(F)$. Then there is Jordan-Gauss partition of $\Gamma(G(F))$ defined over F.*

Let B^+ and B^- be Borel subgroups containing root subgroups corresponding positive and negative roots respectively. Let P_i , $i=1, 2,..., n$ are standard maximal parabolic subgroups, i. e maximal subgroups of G containing B^+.

Recall that the geometry $\Gamma(G(F))$ is the disjoint union of $(G(F):P_i)$ *with the type function* $t(gP_i)=i$ and incidence relation $I : \alpha I \beta$ if and only if $\alpha \cap \beta$ is not an empty set.

Proposition 1. Orbits of B^- form the classes of Jordan-Gauss equivalence relation.

Definition. Let $\Gamma = \Gamma(G(F))$ be the geometry of Kac-Moody group with the Coxeter-Dynkin diagram X_l. We take the partition of Γ onto the classes of Jordan-Gauss equivalence relation of Proposition 1. For each pair of classes J_s, $J_{s'}$ which defines nontrivial induced graph $J(s, s')$ defined over F we select Jordan-Gauss graph ${}^{s,s'}J(K)$ over the commutative ring K with unity such that $J(s, s')$ and ${}^{s,s'}J(K)$ are symbolically equivalent. Let D be the data of our selection of graphs.

The substitution of ${}^{s,s'}J(K)$ instead of $J(s, s')$ accordingly selected data D will produce incidence system ${}^{D}\Gamma(X_l, K)$.

We refer to it as *Jordan-Gauss geometry* with the diagram X_l over commutative ring K based on the symbolic data D.

As it follows from the definition there is a Jordan-Gauss equivalence on the set of elements of this incidence structure.

The set of classes of this equivalence relations are in natural one to one correspondence R with the set of elements of Weyl geometry $\Gamma(W)$, where W corresponds to Dynkin-Coxeter diagram X_l.

2. Applications of Jordan-Gauss geometries in Algebraic Geometry.

Let us consider an affine Cremona semigroup ${}^{n}CS(K)$ of all endomorphisms of multivariate ring $K[x_1, x_2, ..., x_n]$. Endomorphism F can be given by its values $F(x_1)=f_1, F(x_2)=f_2, ..., F(x_n)=f_n$ on the variables $x_i, i=1, 2,..., n$.

We can assume that polynomials f_i are given in their standard form i.e. sum of monomial terms ordered in lexicographical order.

Endomorphism F induces the map $F' : x_1 \to f_1(x_1, x_2, ..., x_n)$,

$x_2 \to f_1(x_1, x_2, ..., x_n), ..., x_n \to f_n(x_1, x_2, ..., x_n)$ of the affine space K^n into itself.

We define degree $deg(F)$ as maximal value of $deg\ (f_i)$. The density $den\ f_i(x_1, x_2, ..., x_n)$ is its number of monomial terms

. We define density $den(F)$ of F as maximal value of $den\ (f_i)$, $i=1, 2, ..., n$ and identify endomorphism F with the tuple $(f_1(x_1, x_2, ..., x_n), f_2(x_1, x_2, ..., x_n), ..., f_n(x_1, x_2, ..., x_n))$.

We use walks on incidence structure ${}^D\Gamma(X_l, K[x_1, x_2, ..., x_n])$ in the case of $X_l = A_l$ and natural colourings of their Jordan-Gauss graphs for the explicit constructions of groups supporting the following statement of Computational Algebraic Geometry.

Theorem 2. *Let K be commutative ring with unity. For each positive integer $n, d, d \geq 2$ and $s \geq 0$ there is a noncommutative subgroup H of affine Cremona semigroup ${}^nCS(K)$ of all endomorphisms of $K[x_1, x_2, ..., x_n]$ such that maximal degree of representative of H is d and the densities of elements from H are of size $O(n^s)$.*

Remark. *There is a large subsemigroup $H', H' > H$ of ${}^nCS(K)$ of prescribed degree d and density $O(n^s)$.*

H an H' can serve as platforms of Noncommutative Cryptography for the implementation of postquantum secure protocols which are generalisations of Diffie – Hellman protocol.

Note that the constructions of subgroups or subsemigroups of affine Cremona group of bounded degree is not an easy task because the product of two nonlinear elements of degree t and s in general position will have degree ts.

We assume that multivariate map F of K^n onto K^n is given in its standard form of kind $x_i \to f_i(x_1, x_2, \dots, x_n)$, $i=1, 2, \dots, n$ where polynomials f_i are given in the form of the some of monomial terms

listed in the lexicographical order. We assume that monomial term M is written in the form $a(x_1)^{t(1)}(x_2)^{t(2)}\dots(x_n)^{t(n)}$, where $t(i)$ are elements of Z_m, m is the order of multiplicative group K^*.

The trapdoor accelerator T of F is a piece of information such the knowledge of T allows us to compute the reimage of F in polynomial time. We say that T is a *computational accelerator* of speed α if its knowledge allows to compute the reimage of F and its value on given element in time $O(n^{\alpha})$.

Theorem 3. *For each parameters* $n, d, d\geq 2$ and $\alpha, \alpha\leq d$ *there is a bijective polynomial map* F *of* K^n *onto* K^n *of degree* d, *density of size* $O(n^{\alpha})$ *with the computational accelerator of speed* $O(n)$.

We say that polynomial map F of K^n onto K^n has a multiplicative computational accelerator T of speed α if the restriction of F on $(K^*)^n$ is the injective one and the knowledge *of* T allows to compute the reimage of $b \in F((K^*)^n)$ and the image of $p\in(K^*)^n$ in time $O(n^{\alpha})$.

Theorem 4. *For each parameters* n, *and* $\alpha, \alpha\geq 0$ *there is a polynomial map* F *of* K^n *onto* K^n *of the density of size* $O(n^{\alpha})$ *with the multiplicative computational accelerator of speed* $O(n)$.

Public keys based on this statement for $\alpha=3$ were proposed in **2017** Reports of Nath. Acad. Sci. of Ukraine (cases $K=Z_q$ and $K=F_q$). Other cryptographic applications of maps of unbounded degree can be found in

V. Ustimenko, On Eulerian semigroups of multivariate transformations and their cryptographic applications. European Journal of Mathematics 9, 93 (2023), https://doi.org/10.1007/s40879-023-00685

APPENDIX. The constructions of polynomial maps.

Let us consider the incidence system $\Gamma = {}^{D}\Gamma(X_l, K')$. Assume that X_l **d**efines finite Weyl group W. We take one of the Jordan-Gauss graphs

$J(K')$ of Γ with partition set J_k ***(points***) and J_m ***(lines)*** such that $R(J_k)$ and $R(J_m)$ from $\Gamma(W)$ contain the Coxeter element g of Coxeter system (W, S). It means that g has the maximal length of its irreducible representations as the word of generators from S.

Assume that $J_k = (K')^n$. We select K' in a form of $K[x_1, x_2, ..., x_n]$. So points of $J(K')$ are tuples of kind

$(f_1(x_1, x_2, ..., x_n), f_2(x_1, x_2, ..., x_n), ..., f_n(x_1, x_2, ..., x_n))$.

We take the special point $X=(x_1, x_2, \ldots, x_n)$ of $J(K')$ and consider the walk in ${}^D\Gamma(X_l, K'])$ of kind

$X, a_1, a_2, ..., ..., a_l, a_{l+1}$ where (X, a_1) is an edge of $J(K')$, $a_l \in J_m$ and $a_{l+1} \in J_k$. The destination point a_{l+1} is the tuple $(g_1, g_2, \ldots, g_n)$ where $g_i \in K[x_1, x_2, \ldots, x_n]$.

We investigate transformations of K^n of kind

$x_1 \to g_1(x_1, x_2, \ldots, x_n)$,

$x_2 \to g_2(x_1, x_2, \ldots, x_n)$,

…

$x_1 \to g_1(x_1, x_2, \ldots, x_n)$.

Thus we can

1. **consider the semigroup of such maps and its special subsemigroups**
2. **investigate when this transformation is bijective and information on the walk defines trapdoor accelerator.**

THANK YOU VERY MUCH FOR YOUR ATTENTION !