ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 4, Pages 135–145
ISSN 1930-1235: (2010)

SCHUBERT CELLS IN LIE GEOMETRIES AND KEY EXCHANGE VIA SYMBOLIC COMPUTATIONS

VASYL USTIMENKO

Abstract. We propose some cryptographical algorithms based on finite BN-pair G defined over the fields F_q. We convert the adjacency graph for maximal flags of the geometry of group G into a finite Tits automaton by special colouring of arrows and treat the largest Schubert cell Sch $= {F_q}^N$ on this variety as a totality of possible initial states and a totality of accepting states at a time. The computation (encryption map) corresponds to some walk in the graph with the starting and ending points in Sch. To make algorithms fast we will use the embedding of geometry for G into Borel subalgebra of corresponding Lie algebra. We consider the induced subgraph of adjacency graph obtained by deleting all vertices outside of largest Schubert cell and corresponding automaton (Schubert automaton). We consider the following symbolic implementation of Tits and Schubert automata. The symbolic initial state is a string of variables x_α, where roots α are listed according Bruhat order, choice of label will be governed by linear expression in variables x_α, where α is a simple root.

Conjugations of such nonlinear map with element of affine group acting on ${\mathrm{F_q}}^N$ can be used in Diffie-Hellman key exchange algorithm based on the complexity of group theoretical discrete logarithm problem in case of Cremona group of this variety. We evaluate the degree of these polynomial maps from above and the maximal order of this transformation from below. For simplicity we assume that G is a simple Lie group of normal type but the algorithm can be easily generalised on wide classes of Tits geometries. In a spirit of algebraic geometry we generalise slightly the algorithm by change of linear governing functions for rational linear maps.

1. Introduction

According to Hilbert's approach to Geometry it is a special incidence system (or multipartite graph). Felix Klein thought that the Geometry was a group and proposed his famous Erlangen program. J. Tits combined those two ideas for the development of concept of a BN-pair, its geometry and flag system [28]. [29]. He created an axiomatic closure for such objects based on the definition of building [30].

Finite geometries $\Gamma(G(q))$ of BN-pair $G(q)$ with Weyl group W defined over finite field F_q, $q \to \infty$ form a family of small world graphs. Really, the diameters of the incidence graphs for $\Gamma(G(q))$ coincide with the diameter of Weyl geometry $\Gamma(W)$, but average degree is growing with the growth of parameter q. The problem

Key words and phrases. small world graphs, Lie geometries, symbolic computations, walks on graphs, Schubert cells, automata, cryptography, key exchange protocols.

Research supported by a project "Human - The Best Inwestment". The project is co-funded from the sources of the European Union within the European Social Fund.

of constructing infinite families of small world graphs has many remarkable applications in economics, natural sciences, computer sciences and even in sociology. For instance, the "small world graph" of binary relation "two person shake hands" on the set of people in the world has small diameter.

The algorithm of finding the shortest pass between two arbitrarily chosen vertexes of $\Gamma(G(q))$ is much faster than the action of general Dijkstra algorithm. One can find the pass in $\Gamma(G(q))$ for the time c, where c is a constant independent on q. Regular graphs of simple groups of Lie type of normal type of rank 2 (generalised m-gons for $m \in \{3, 4, 6\}$ support the sharpness of Erdös' bound from Even Circuit Theorem in cases of cycles of length $4, 6$ and 10 (see [3]).

One of the constructions which provide for each $k_0 \geq 2$ the infinite family of regular graphs of degree $k, k \geq k_0$ of large girth (length of minimal cycle) is based on the properties of the geometry of Kac-Moody BN-pair $G(q)$ with diagram $\tilde{A}_1$ (see [16], [17], [18])

The geometries of finite BN-pairs are traditionally used in classical Coding Theory. Foundations of this theory are based on the concept of finite distance-transitive or distance-regular metrics (distance regular and distance transitive graphs in other terminology [6]). Large number of known families of distance transitive graphs are constructed in terms of the incidence geometry of BN-pair or geometry of its Weyl group. Known constructions of families of distance - regular but not distance transitive graphs are also based on the properties of BN-pair geometries (see [6], [32]). Linear codes are just elements of projective geometry and all applications of Incidence Geometries to Coding Theory are hard to observe (see [12], [20], [22] and further references). Notice that some nonclassical areas like LDPS codes and turbocodes use objects constructed via BN-pair geometries: for the first constructions of LDPS codes Tanner [27] used finite generalised m-gons, the infinite family of graphs of large girth defined in [16] have been applied to constructions of the LDPS codes ([15], [13], [14], [25], [26] and further references)

Quite recent development gives an application of linear codes and their lattices to cryptography. Incidence geometries were used in [1] and [36] for the development of cryptographical algorithms (see also a [5], [20]).

In the paper we generalise some encryption algorithms of [36], [35] and consider the key exchange protocols based on geometries of BN-pairs.

2. Basic definitions in theory of BN-pairs, their geometries and flag systems

2.1. Graphs and incidence system. The missing definitions of graph-theoretical concepts which appears in this paper can be found in [2] or [3]. All graphs we consider are simple, i.e. undirected without loops and multiple edges. Let $V(G)$ and $E(G)$ denote the set of vertices and the set of edges of G, respectively. Then $|V(G)|$ is called the *order* of G, and $|E(G)|$ is called the *size* of G. When it is convenient, we shall identify G with the corresponding anti-reflexive binary relation on $V(G)$, i.e. $E(G)$ is a subset of $V(G) \times V(G)$ and write vGu for the adjacent vertices u and v (or neighbours). The sequence of distinct vertices $v_0, v_1, \ldots, v_t$, such that $v_i G v_{i+1}$ for $i = 1, \ldots, t-1$ is the pass in the graph. The length of a pass is a number of its edges. The distance $\mathrm{dist}(u, v)$ between two vertices is the length of the shortest pass between them. The diameter of the graph is the maximal distance between two vertices u and v of the graph. Let C_m denote the cycle of length m i.e.

the sequence of distinct vertices $v_0, \ldots, v_m$ such that $v_i G v_{i+1}$, $i = 1, \ldots, m-1$ and $v_m G v_1$. The girth of a graph G, denoted by $g = g(G)$, is the length of the shortest cycle in G. The degree of vertex v is the number of its neighbours.

The incidence structure is the set V with partition sets P (points) and L (lines) and symmetric binary relation I such that the incidence of two elements implies that one of them is a point and another is a line. We shall identify I with the simple graph of this incidence relation (bipartite graph). If number of neighbours of each element is finite and depends only from its type (point or line), then the incidence structure is a tactical configuration in the sense of Moore (see [7]). An incidence structure is a semiplane if two distinct lines are intersecting not more than in one point and two distinct points are incident not more than one line. As it follows from the definition, graphs of the semiplane have no cycles C_3 and C_4.

The graph is k-regular if each of its vertex has degree k, where k is a constant.

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

The flag F is a nonempty subset in Γ such that $\alpha, \beta \in F$ implies $\alpha I \beta$. We assume that $t(F) = \{t(x) | x \in F\}$

We assume that two flags F_1 and F_2 are incident ($F_1 I F_2$) if $F_1 \cup F_2$ is also a flag and $t(F_1) \cap t(F_2) = \emptyset$. Let $GF(\Gamma)$ be the incidence graph of the incidence relation defined on the set of all flags from Γ, $GF_{I,J}(\Gamma)$, $I \cap J = \emptyset$ be the totality of flags of type I or J with the restriction of flag incidence on it. The type function is defined by $t(\alpha) = s$, where $\alpha = gG_s$ for some $s \in S$.

2.2. **Groups, Coxeter systems and BN-pairs.** 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 objects 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 $\alpha \cap \beta \neq \emptyset$. The type function is defined by $t(\alpha) = s$ where $\alpha = gG_s$ for some $s \in S$.

Let (W, S) be a Coxeter system, i.e. W is a group with set of distinguished generators given by $S = \{s_1, s_2, \ldots, s_l\}$ and generic relation $(s_i \times s_j)^{m_{i,j}} = e$. Here $M = (m_{i,j})$ is a symmetrical $l \times l$ matrix with $m_{i,i} = 1$ and off-diagonal entries satisfying $m_{i,j} \geq 2$ (allowing $m_{i,j} = \infty$ as a possibility, in which case the relation $(s_i \times s_j)^{m_{i,j}} = e$ is omitted). Letting $W_i = < S - \{s_i\} >$, $1 \leq i \leq l$ we obtain a group incidence system $\Gamma_W = \Gamma(W, W_i)_{1 \leq i \leq l}$ called the Coxeter geometry of W. The W_i are referred to as the *maximal standard subgroups* of W (see [8]).

Let G be a group, B and N subgroups of G, and S a collection of cosets of $B \cap N$ in N. We call (G, B, N, S) a *Tits system* (or we say that G *has a BN-pair*) if

(i) $G = < B, N >$ 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 $BuB \cup BswB$ for any $s \in S$ and $w \in W$,

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

Properties (1)-(iv) imply that (W, S) is a Coxeter system (see [7], [8]). Whenever (G, B, N, S) is a Tits system, we call the group W the Weyl group of the system, or more usually the 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 $\Gamma_G = \Gamma(G, P_i)_{1 \leq i l e l}$ is commonly referred to as the *Lie geometry* of G (see [6]). Note that the Lie geometry of G and the Coxeter geometry of the corresponding Weyl group have the same rank. In fact there is a type preserving morphism from Γ_G onto Γ_W given by $gP_i \to wW_i$, where w is determined from the equality $BgP_i = BwP_i$. This morphism is called a *retraction* (see [30]).

3. Tits and Schubert automata and for symbolic computations

3.1. **Definitions of automata.** The geometry $\Gamma(G)$ of BN-pair G is the set of all left cosets by the standard maximal subgroups i.e. maximal subgroups P_i, $i = 1, 2, \ldots, n$i of G containing standard Borel subgroup B. Two cosets $C_1 = gP_i$ and $C_2 = hP_j$ are incident $C_1 I C_2$ if and only if their intersection is not empty. It is clear, that $gP_i \cap hP_j \neq 0$ implies $i \neq j$. The maximal flag of the geometry is a subset $F = \{C_1, C_2, \ldots, C_n\}$ such that $C_i I C_j$ for each pair (i, j), $i \neq j$. Maximal flags form the set $\mathrm{F}\Gamma(G)$, they are in one to one correspondence with the left cosets by standard Borel subgroup. The largest Schubert cell Sch is the orbit of B acting on $\mathrm{F}\Gamma(G)$ containing largest number of elements. In case of group of normal type variety $\mathrm{Sch} = \mathrm{Sch}(G)$ is isomorphic to vector space ${F_q}^N$, where N is the number of positive roots.

We assume that two maximal flags F_1 and F_2 are adjacent if their intersection contains $n-1$ elements of geometry. Let $AF(G)$ be the simple graph of symmetric adjacency relation (flag graph for $\Gamma(G)$. The order of this simple regular graph is $|(G : B)|$, the degree is nq and diameter is n. Let us restrict the adjacency relation as above on the largest Schubert cell $\mathrm{Sch}(G)$. We obtain new graph $AS(G)$ which is a regular induced subgraph of $AF(G)$ of order q^N and degree $q-1$. We refer to $AS(G)$ as Schubert subgraph of the flag graph.

We convert the directed graph of adjacency relation of flags into the following automaton.

Let (F_1, F_2) be the ordered pair of adjacency flags such that $t(F_1 \cap F_2) = \{1, 2, \ldots, n\} - \{s\}$. So flags differs by geometry elements $C_1 = {C_s}^1$ and $C_2 = {C_s}^2$ of type s from (F_1, F_2), respectively. The following situations are possible.

(i) Element C_1 and C_2 are from the same Schubert cell. In that case there unique a transformation $u = x_\alpha(t)$, $t \neq 0$, shifting C_1 to C_2. Root α depends on $\mathrm{Retr}(F_1)$ only.

(ii) Elements C_1 and C_2 are from different Schubert cells and there is a group U_α such that $(F_1 \cap F_2) \cup \{u(C_2)\}$ is an adjacent flag to F_1 for each $u = x_\alpha(t)$. Notice, that case $t = 0$ is a possibility here. Root α depends on $\mathrm{Retr}(F_1)$ again.

(iii) Elements C_1 and C_2 are from different Schubert cells and Schubert cell contains C_2 as unique representative C such that flag $(F_1 \cap F_2) \cup \{C\}$ is adjacent to F_1.

Let us consider the following labelling of $F_1 \to F_2$ for cases of (i), (ii) and (iii) separately:

(i) put the label (s, t). where $t \neq 0$.

(ii) the label is (s, t), where $t \in F_q$ is defined by condition $x_\alpha(t)\mathrm{Retr}(C_2) = C_2$

(iii) put the label ∞.

So for fixed F_1 and fixed type s the label (s, t) in direction to s-adjacency flag is defined by parameter t taken from the "acceptable" set $\mathrm{Ac}(F_1) = F_q \cup \{\gamma\}$ where γ is one of the symbols 0 and ∞. We add the formal loop on state F_1 labelled by the unique symbol from $\{0, \infty\} - \{\gamma\}$.

So the transition function $T_{s,t}$ of taking the s-adjacent element of colour (s, t) for general flag is defined for each $t \in F_q \cup \{\infty\}$ We assume that the initial state can be any flag from the largest Schubert cell Sch and this cell is the totality of all accepting states.

So algorithm can be given by the string of labels $(s_1, t_1), (s_2, t_2), \ldots, (s_d, t_d)$ such that the composition $T = T(s_1, t_1)T(s_2, t_2)T(s_d, t_d)$ maps Sch into itself. We are interested only in irreducible computations for which $s_i \neq s_{i+1}$ for $i = 1.2, \ldots d-1$

In case of group of normal type the alphabet contains exactly $n(q + 1)$ symbols. The computation corresponds to special walks in the graph $AF(G)$ with the starting and ending point in Sch(G). Notice that C may be not a bijection. For instance $T(s, O)$, which image for Sch lays outside of the largest large Schubert cell, is not invertible.

We refer to such automaton as *Tits automaton* for group G. We would like to use it as tool for symbolic computations.

The unipotent group U acts regularly on Sch. So we can identify $v \in$ Sch with certain product of $X_\alpha(t_\alpha)$, and positive roots $\alpha \in$ Root are taken in Bruhat order. In fact, we identify the string v $= t_\alpha \in F_q$, $\alpha \in \mathrm{Root}^+$ with the accepting state v.

We refer to the list $(t_{\alpha_1}, t_{\alpha_2}, \ldots, t_{\alpha_n})$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ is the set of all simple roots, as the color of v from plainspace. So we are colouring accepting states now but not arrows.

Let us consider irreducible computation within Tits automaton of kind $v \to v_s$, $v_1 = T(i_1, a_1)(v)$, $v_2 = T(i_2, a_2)(v_1), \ldots, v_s = T(i_s, a_s)(v_{s-1})$, where $i_k \neq i_{k+1}$, $k = 1, \ldots, s-1$, $a_k \in F_q \cup \infty$, element $\mathrm{Retr}(v) = \mathrm{Retr}(v_s)$ equals to the element $w \in W$ of maximal length. Notice, that in the sequence $\mathrm{Retr}(v_1), \mathrm{Retr}(v_2), \ldots, \mathrm{Retr}(v_k)$ consecutive elements are adjacent in $\mathrm{F}\Gamma(W)$ or equal.

The computation is conducted into several steps. Each time we have one of the situations i, (ii) or (iii). In cases of kind (i) and (ii) when the corresponding root α is simple parameters a_j will be chosen as linear functions of kind $l(t_{\alpha_1}, t_{\alpha_2}, \ldots t_{\alpha_n}) = c_1 t_{\alpha_1} + c_2 t\alpha_2 \ldots, c_n t_{\alpha_n} + b$, where $c_1, c_2, \ldots, c_n$ and b are elements of F_q and $(t_{\alpha_1}, t_{\alpha_2}, \ldots, t_{\alpha_n})$ is a colour of our initial state. If α is not a simple root, we choose a_j as $c_j t_{\beta_j} + f_j((t_{\alpha_1}, t_{\alpha_2}, \ldots t_{\alpha_n})$, where $c_j \neq 0$.

After the completion of our computation we get the accepting state $u = v_s$. It has a colour $(d_{\alpha_1}, d_{\alpha_2}, \ldots, d_{\alpha_n}) = (t_{\alpha_1}, t_{\alpha_2}, \ldots t_{\alpha_n})A + (b_1, b_2, \ldots, b_n)$, where

the matrix A is defined by some linear expressions of kind $a_i = l_i(l(t_{\alpha_1}, t_{\alpha_2}, \ldots t_{\alpha_n})$, which we used during the computation. We will require that the matrix A is invertible. Notice that we may use symbol ∞, where the design of algorithm allows such option.

After the completion of algorithm we obtain accepting state of colour $(d_{\alpha_1}, d_{\alpha_2}, \ldots, d_{\alpha_n})$. The invertibility of A allows us to compute $(t_{\alpha_1}, t_{\alpha_2}, \ldots t_{\alpha_n})$ as $((d_{\alpha_1}, d_{\alpha_2}, \ldots d_{\alpha_n}) - (b_1, b_2, \ldots, b_n))A^{-1}$. So we can compute all parameters a_i and create the reverse walk in the graph and compute the inverse map T^{-1} which sends the final accepting state to initial state.

Let us restrict Tits automaton on the largest Schubert cell, i. e delete all states outside Sch(G) together with corresponding output arrows. We obtain Schubert automaton over the alphabet (i, a), where $a \in F_q$, $1 \leq i \leq n$. Notice, that $a = 0$ corresponds to taking the loop.

3.2. **Tits and Schubert automata and related symmetric encryption.** Correspondents Alice and Bob may use the following symmetric encryption based on the Tits automaton. The plainspace is a vector space Sch $= {F_q}^N$. The plaintext p we identify with the string v= $t_\alpha \in F_q$, $\alpha \in \mathrm{Root}^+$. We may think that this is a function p : $Root^+ \to F_q$. Alice has to compute the restriction of this function onto subsets of all simple roots and get the colour $(t_{\alpha_1}, t_{\alpha_2}, \ldots, t_{\alpha_d})$ of the plainspace.

Correspondents share symbolic string of labels $(s_1, l_1), (s_2, l_2), \ldots, (s_d, l_d)$, where $l_i.i = 1, 2, \ldots, d$ is a linear expression of formal variables z_α, for each simple root α or ∞ and two affine invertible transformations τ_1 and τ_2. The vector space of all maps from the totality of simple roots to F_q has to be not invariant subspace for τ_i, $i = 1, 2$. Alice executing the specialization $z_\alpha = p_\alpha$ computing Corresponding numerical string t $= (t_1, t_2, \ldots, t_d)$. She has to hide that string by applications of affine maps τ_i. So she is adding to symbolic key two invertible Linear transformations τ_1 and τ_2 of the plainspace ${F_q}^N$ and compose τ_1, the automaton map corresponding to t and τ_2.

She sends to Bob the ciphertext

$$\mathrm{c} = \tau_1(T(s_1, t_1)T(s_2, t_2) \ldots T(s_d, t_d)(\tau_1(\mathrm{p}))$$

Bob decrypt applying to c consequently ${\tau_2}^{-1}$, T^{-1}, where $T = T(s_1, t_1)T(s_2, t_2) \ldots T(s_d, t_d)$ and ${\tau_1}^{-1}$,

Remark 1. If correspondents do not use ∞ in the shared symbolic key then T is the computation in Schubert automaton. Bob can simply compute T^{-1} as $T(s_d, -t_d)T(s_{d-1}, -t_{d-1}) \ldots T(s_1, -t_1)$.

Remark 2. We may generalise the above algorithms by changing affine maps τ_1, τ_2 and $(t_1, t_2, \ldots, t_n) \to (t_1, t_2, \ldots, t_d)A + (b_1, b_2, \ldots, b_n)$ for general invertible polynomial maps.

4. Key exchange protocols based on incidence geometries

The automata as above can be considered over the general ground field F We can see that the computations in both automata do not use division. What is going on during the computations on a symbolic level. Let us assume now that the initial state is a formal string of variables x_α, where α is running throw the list of all positive roots. It is convenient for us to expand the ground field F_q to the field R of rational functions $r(x_1, x_2, \ldots, x_N) = f(x_1, x_2, \ldots, x_N)/g(x_1, x_2, \ldots, x_N)$, where f and g are elements $F_q[x_1, x_2, \ldots, x_N]$ Formal variables x_α and governing linear expressions $l(x_{\alpha_1}, x_{\alpha_2}, \ldots, x_{\alpha_n}, x_\alpha)$, where α is not a simple root are elements of subring $F_q[x_1, x_2, \ldots, x_N]$ in R. During its work Tits automaton newer use division. So after getting accepting state over R we got the vector of dimension N with polynomial components f_α. So the numerical encryption map is regular automorphism of ${F_q}^N$ (element of Cremona group for ${F_q}^N$) of kind.

$$x_i \to f_i(x_1, x_2, \ldots, x_N), i = 1, 2, \ldots, N$$

Special choice of symbolic key guarantee that the above transformation is bijective. Symbol ∞ play just formal role. Linearity of governing functions leads to rather small degree of the nonlinear map.

Such a walk produces a bijective transformation T of variety Sch(G) which is its regular automorphism (polynomial map of the variety into itself such that its inverse is also polynomial). We will conjugate T by invertible affine transformation $\tau \in AGL_N(F_q)$ and use $Y = \tau^{-1}T\tau$ as the instrument for the key exchange based in modified Diffie - Hellman method. So the Alice is computing a standard from for Y

$t_1 = f_1(t_1, t_2, \ldots, t_N), t_2 = f_2(t_1, t_2, \ldots, t_N), \ldots, t_N = f_N(t_1, t_2, \ldots, t_N)$, where $f_i \in F_q[t_1, t_2, \ldots, t_N]$, $i = 1, 2, \ldots, N$, and sending the map to Bob via open communication channel. Correspondents Alice and Bob (as usually) are choosing their keys k_A and k_B, respectively. They are executing computations $D_A = Y^{k_A}$ and $D_B = Y^{k_B}$. They exchange the outputs via the open channel.

Finally Alice and Bob are computing collision maps ${D_B}^{k_A}$ and ${D_A}^{k_B}$. So correspondents are getting common element.

We can modify the above scheme:

Alice chooses the maximal flag F from the largest large Schubert cell Sch(G) and sends it to Bob via open channel. Correspondence may use common flag ${D_A}^{k_B}(F) = {D_B}^{k_A}(F)$ as the key for their private key algorithm.

The security of the above key exchange algorithm based on the complexity of discrete logarithm problem for the Cremona group of variety Sch(G). In case of finite field F_q this group coincides with the symmetric group S_{q^N}. it is important that we use description of permutations in terms of polynomial algebra. So related discrete logarithm problem is formulated in terms of algebraic geometry.

Method allows various modification: we can use nonlinear invertible maps instead of affine transformation τ, the base of discrete logarithm can be non invertible polynomial map and etc. An interesting modifications can be obtained if we will allow noninvertible transformations of the variety. For instance we may consider fractional linear governing function l_i for the step i looks like $(a_1 X_{\alpha 1} + a_2 x_\alpha 2 + \ldots a_{\alpha_n} x_{\alpha_n})/(b_1 X_{\alpha 1} + b_2 x_\alpha 2 + \ldots b_{\alpha_n} X_{\alpha_n})$ if the root α on step i is simple, and l_i is a fraction of two linear combinations of x_α, $\alpha \in \mathrm{Root}^+$ if α is not a simple root. In case of such governing functions we refer to corresponding automata as birational Tits and Schubert automaton, respectively.

5. Embedding of the flag variety into the Lie Algebra and some complexity estimates

Throughout this section (G, B, N, S) is a Tits system which arises in connection with Chevalley group G, although we point that the results of this section remain valid in a far more general setting (see [30],[7], [8]). We write $G = X_l(K)$ to signify that G is the Chevalley group over the field K, with associated Dynkin diagram X_l. We are most interested in the case when K is finite, and we shall write $X_l(q)$ instead of $X_l(F_q)$ in that case.

So, fix Chevalley group $G = X_l(K)$ with corresponding Weyl group W. As in the previous section Γ_W and Γ_G their associated Coxeter and Lie geometries. Let $L = H + L^+ + L^-$ be the Lie algebra corresponding to G.

Following convention, we refer to H, L^+, L^- and $H + L^+$ as, respectively, the *Cartan subalgebras, positive root space, negative root space* and *Borel subalgebra* with respect to the given decomposition of L. We also use the familiar bracket notation $[,]$ to indicate Lie product [4], [24],

Below we turn out our attention to a method of embedding Γ_W and Γ_G in L. As the reader shall see, this method actually embeds Γ_W in the Cartan subalgebra H of L. Let us consider the embedding more precisely.

Let $A = (a_{i,j})$ be the Cartan matrix corresponding to the root system Ω of W. We consider the lattice R which is generated by simple roots $\alpha_1, \alpha_2, \ldots, \alpha_l$ and the reflection $r_1, r_2, \ldots r_l$ of R defined by the equality $(\alpha_i)^{r_j} = \alpha_i - a_{i,j}\alpha_j$.

Let $S = \{r_1, r_2, \ldots, r_l\}$ is the set of Coxeter generators of Weyl group W. Let ${\alpha_1}^*, {\alpha_2}^*, \ldots, {\alpha_l}^*$ be a dual basis of $\alpha_1, \alpha_2, \ldots, \alpha_l$, i.e. ${\alpha_i}^*$ is the linear functional on R which satisfies $\alpha_i{}^*(\alpha_j) = \delta_{i,j}$. We define the action of W on the dual lattice R^* by $l(x)^s = l(x^s)$, where $l(x) \in \mathrm{R}^*$ and $s \in S$.

Consider the orbit $H_i = \{\alpha_i{}^{*w} | w \in W\}$ of permutation group (W, R^*), which contains $\alpha_1{}^*$. Let H be the disjoint union of H_i. We give the set H the structure of an incidence system as follows. Linear functionals $l_1(x)$ and $l_2(x)$ are incident if and only if products $l_1(\alpha)l_2(\alpha) \geq 0$ for all $\alpha \in \Omega$. The type function t is defined by $t(l(x)) = i$ where $l(x) \in H_i$. It can be shown that (H, I, t) is isomorphic to Coxeter geometry Γ_W. (In fact there is a unique isomorphism of Γ_W with (H, I, t) which sends W_i to α_i, $1 \leq i \leq l$.) This gives the desired embedding since H is a subset in R^* and $\mathrm{R}^* \subset L_0$. Moreover this embedding still valid for a field K of sufficiently large characteristic, since, in that case H is a subset of $\mathrm{R} \times K = L_0$.

We now consider an analogous embedding of the Lie geometry Γ_G into the Borel subalgebra $U = L_0 + L^+$ of L. Let $d = \alpha_1{}^* + \alpha_2{}^* + \dots \alpha_l{}^*$. Than we can take $\Omega^+ = \{\alpha \in \Omega | d(\alpha) \geq 0\}$ to be our set of positive roots in Ω. For any $l(x) \in \mathrm{R}^*$ define $\eta^-(L) = \alpha \in \Omega^+ | l(\alpha) < 0$.

Let L_α be the root space corresponding to positive root α. For each $h \in H$ we define the subalgebra L_h as the sum of L_α, $\alpha \in \eta^-(h)$. Let $U_i = \{h + v | h \in H_i, v \in L_h\}$ and U is a disjoint union of U_i. We give U the structure of an incident system as follows. Elements $h_1 + v_1$ and $h_2 + v_2$ are incident if and only if each of the following hold:

(i) $h_1(\alpha)h_2(\alpha) \geq 0$ for all $\alpha \in \Omega$, i.e. h_1 and h_2 are incident in (H, I, t).

(ii) $[h_1 + v_1, h_2 + v_2] = 0$

Element $h + v$ has type i if $h + v \in U_i$.

In [38] it is shown that this newly defined incident system is isomorphic to the Lie geometry Γ_G, provided that the characteristic of K is zero or sufficiently large to ensure the isomorphism at the level of the subgeometries (H, I, t) and Γ_W. Then analogous to the Weyl case, there exists a unique isomorphism Retr of $\Gamma(G)$ into (U, I, t) which sends P_i to α_i, $1 \leq i \leq l$.

Proposition 5.1. *Let $\Gamma = \Gamma(G)$ be the geometry of group $G = X_n(q)$. The above interpretation of $\Gamma(G)$ allows*

(i) generate Γ in $O(|\Gamma|)$ elementary steps and check whether or not two elements of Γ are incident for time $O(N^2)$, where N is the number of positive roots.

(ii) complete the computation in Tits and Schubert automaton consisting of k elementary steps for time $O(kN)$

Graphs of degree q and $SF(X_n(q)$, $q \geq 4$ of degree $q-1$ have orders $|X_n(q)|/|B|$ and q^N, respectively. They form families of small world graphs depending on two parameters n and q.

6. On the discrete logarithm problem with polynomial or birational base

Let F_p, where p is prime. be a finite field. Affine transformations $\mathrm{x} \to A\mathrm{x} + b$, where A is invertible matrix and $b \in (F_p)^n$, form an affine group $AGL_n(F_p)$ acting on ${F_p}^n$. It is known that polynomial transformation of kind $x_1 \to g_1(x_1, x_2, \dots, x_n), x_2 \to g_2(x_1, x_2, \dots, x_n), \dots, x_n \to g_n(x_1, x_2, \dots, x_n)$ form a symmetric group S_{p^n}.

In the simplest case F_p, affine transformations form an affine group $AGL_n(F_p)$ of order $(p^n-1)(p^n-p)\dots(p^n-p^{n-1})$ in the symmetric group S_{p^n} of order $(p^n)!$. In [19] the maximality of $AGL_n(F_p)$ in S_{p^n} was proven. So we can present each permutation π as a composition of several "seed" maps of kind $\tau_1 g \tau_2$, where $\tau_1, \tau_2 \in AGL_n(F_p)$ and g is a fixed map of degree ≥ 2. One may choose quadratic map of Imai - Matsumoto algorithm in case $p = 2$ (see [10], [21] for its description and cryptanalysis by J. Patarin) or graph based cubical maps [31] for general p.

We can choose the base of ${F_p}^n$ and write each permutation $g \in S_{p^n}$ as a "public rule":

$x_1 \to g_1(x_1, x_2, \ldots, x_n), x_2 \to g_2(x_1, x_2, \ldots, x_n), \ldots, x_n \to g_n(x_1, x_2, \ldots, x_n)$.

Let $g^k \in S_{p^n}$ be the new public rule obtained via iteration of g. Discrete logarithm problem of finding solution for k for $g^k = b$ can be difficult if the order of g is "sufficiently large". We have to avoid the linear growth of the degree g^k, when k is growing. Obvious bad example is the following: g sends x_i into ${x_i}^t$ for each i. In this case the solution is just a ratio of deg$b$ and deg$g$.

Let us consider the Cremona group $C(n, q)$ of all invertible polynomial automorphisms of the vector space ${F_q}^n$, where $q = p^m$, the semigroups $PC(n, q)$ and $BC(n, q)$ of polynomial and birational maps of ${F_q}^n$ into itself, respectively.

To avoid such trouble one can look at families of subgroups of increasing order G_n, $n \to \infty$ of S_{p^n} such that maximal degree of its element equals c, where c is independent constant (groups of degree c or groups of stable degree). We refer to an element g such that all its nonidentical powers are of degree c as element of stable degree.

It is clear that the family of affine subgroup $AGL_n(p)$ is a subgroup of stable degree for $c = 1$ and all nonidentical affine transformations are of stable degree. Notice that if g is a linear diagonalisable element of $AGL_n(p)$, then discrete logarithm problem for base g is equivalent to the classical number theoretical problem.

One can take a subgroup H of $AGL_n(p)$ and consider its conjugation with nonlinear bijective polynomial map f. Of course the group $H' = f^{-1}Hf$ will be also a stable group, but for most pairs f and H group H' will be of degree degf $\times$ deg$f^{-1} \geq 4$ because of nonlinearity f and f^{-1}. So the problem of construction an infinite families of subgroups G_n in S_p^n of degree 2 and 3 may attract some attention.

The following questions are important because of Diffie Hellman type protocols (see [9]).

$Q1$; How to construct stable subgroups C of small degree c ($c = 2$ and $c = 3$ especially) of increasing order in $C(n, q)$?

We say refer to a semigroup Se generated by single elements as monogenetic semigroup of order |Se|.

$Q2$; How to construct stable monogenetical subsemigroups in $PC(n, q)$ and $BC(n, q)$ of small degree c ($c = 2$ and $c = 3$ especially) of increasing order in $C(n, q)$ of large order?

Finally, we announce the following statement

Theorem 6.1. *Let $X_n(F)$, $n \geq 2$ be a simple group of Lie type over the field F. Let $L(X_n(q)$ be a group of all invertible computations in Schubert automaton.*

In case of classical groups (diagrams A_n, B_n, C_n and D_n) groups $L(X_n(F))$, $n \to \infty$ form families of stable degree.

Remark: Groups $L(X_n(F))$ are of degree 3 in case of diagram B_n, C_n and D_n, and $L(A_n(F))$ are groups of degree 2.

We can demonstrate the existence of elements in $L(X_n(q))$ of rather large order. Really, take a permutation $i_1, i_2, \ldots, i_n$ on the nodes of Dynkin diagram and compute a composition g of generators $Z^{i_1}(l_1(x)), Z^{i_2}(l_2(x)), \ldots Z^{i_n}(l_n(x))$, where $l_i(x)$

are linear forms corresponding to the rows of Singer cycle matrix of order $q^n - 1$ (see, for instance, [11]). As it follows from the description of algorithm the order of g will be at least $q^n - 1$.

Similarly we can use Singer cycle to generate by Tits automata a stable monogenetic subgroup in $PC(n, q)$ and $BC(n, q)$.

References

[1] A. Beutelspachera, Enciphered Geometry. Some Applications of Geometry To Cryptography, Annals of Discrete Mathematics, V.37, 1988, 59-68.

[2] N. Biggs, *Algebraic Graph Theory* (2nd ed), Cambridge, University Press, 1993.

[3] B. Bollobás, *Extremal Graph Theory*, Academic Press, 1972.

[4] N. Bourbaki, *Lie Groups and Lie Algebras*, Chapters 1 - 9, Springer, 1998-2008.

[5] A. A. Bruen , D. L. Wehlau, *Error-Correcting Codes, Finite Geometries and Cryptography*, AMS, 2010.

[6] A. Brower, A. Cohen, A. Nuemaier, *Distance regular graphs*, Springer, Berlin, 1989.

[7] F. Buekenhout (Editor), *Handbook on Incidence Geometry*, North Holland, Amsterdam, 1995.

[8] R. W. Carter, *Simple Groups of Lie Type*, Wiley, New York 1972.

[9] N. Coblitz, *A Course in Number Theory and Cryptography*, Second Edition, Springer, 1994, 237 p.

[10] N. Coblitz, *Algebraic Aspects of Cryptography*, Springer, 1998, 198 p.

[11] A. Cossidente, M. J. de Ressmine, *Remarks on Singer Cycle Groups and Their Normalizers*, Desighns, Codes and Cryptography, 32, 97-102, 2004.

[12] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.

[13] , 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.

[14] 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.

[15] Jon-Lark Kim, U. N. Peled, I. Perepelitsa, V. Pless, S. Friedland, *Explicit construction of families of LDPC codes with no 4-cycles* , Information Theory, IEEE Transactions, 2004, v. 50, Issue 10, 2378 - 2388.

[16] F. Lazebnik and V. Ustimenko, *Some Algebraic Constructions of Dense Graphs of Large Girth and of Large Size*, DIMACS series in Discrete Mathematics and Theoretical Computer Science, V. 10 (1993), 75-93.

[17] F. Lazebnik, V. Ustimenko, *Explicit construction of graphs with an arbitrary large girth and of large size*, Discrete Appl. Math. , 60, (1995), 275 - 284.

[18] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *A New Series of Dense Graphs of High Girth*, Bull (New Series) of AMS, v.32, N1, (1995), 73-79.

[19] B. Mortimer, *Permutation groups containing affine transformations of the same degree*, J. London Math. Soc., 1972, 15, N3, 445-455.

[20] H. Niederreiter, Chaoping Xing, *Algebraic Geometry in Coding Theory and Cryptography*, Princeton University Press, 2009).

[21] J. Patarin, *Cryptoanalysis of the Matsumoto and Imai public key scheme of the Eurocrypt '88*, Advances in Cryptology, Eurocrypt '96, Springer Verlag, 43-56.

[22] T. Richardson, R. Urbanke, *Modern Coding Theory* Cambridge University Press, 2008.

[23] , T. Shaska , W C Huffman, D. Joyner, V Ustimenko (Editors), Advances in Coding Theory and Crytography (Series on Coding Theory and Cryptology) World Scientific Publishing Company, 2007.

[24] J. P. Serre, *Lie Algebras and Lie groups*, N. Y., Lectures in Math., Springer, Berlin, 1974.

[25] T. Shaska, V. Ustimenko, *On the homogeneous algebraic graphs of large girth and their applications*, Linear Algebra and its Applications Article, Volume 430, Issue 7, 1 April 2009, Special Issue in Honor of Thomas J. Laffey.

[26] T. Shaska and V. Ustimenko, *On some applications of graph theory to cryptography and turbocoding*, Special issue of Albanian Journal of Mathematics:Proceedings of the NATO Advanced Studies Institute "New challenges in digital communications", May 2008, University of Vlora, 2008, v.2, issue 3, 249-255.
[27] R. Michiel Tanner, *A recursive approach to low density codes*, IEEE Trans. on Info Th., IT, 27(5):533-547, Sept.1984.
[28] J. Tits, *Sur la trialite at certains groupes qui s'en deduicent*, Publ. Math. I.H.E.S. 2 (1959), 15-20.
[29] J. Tits, *Les groupes simples de Suzuki et de Ree*, Seminaire Bourbaki 13 (210), 1960/1961, 1-18.
[30] J. Tits, *Buildings of spherical type and Finite* BN*-pairs, Lecture Notes in Math*, Springer Verlag, 1074.
[31] V. Ustimenko, *CRYPTIM: Graphs as Tools for Symmetric Encryption*, in Lecture Notes in Computer Science, Springer, 2001, v. 2227, 278-287.
[32] 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
[33] V. A. Ustimenko, *Linear interpretation of Chevalley group flag geometries*, Ukraine Math. J. 43, Nos. 7,8 (1991), pp. 1055–1060 (in Russian).
[34] V. A. Ustimenko, *Geometries of twisted simple groups of Lie type as objects of linear algebra*, in Questions of Group Theory and Homological Algebra, University of Jaroslavl, Jaroslavl, 1990, 33-56 (in Russian).
[35] V. A. Ustimenko, *On the Varieties of Parabolic Subgroups, their Generalizations and Combinatorial Applications*, Acta Applicandae Mathematicae 52 (1998): pp. 223–238.
[36] V. A. Ustimenko, *Graphs with Special Arcs and Cryptography*, Acta Applicandae Mathematicae, vol. 71, N2, November 2002, 117-153.

Vayl Ustimenko, University of Maria Curie Sklodovska in Lublin
E-mail address: `vasyl@hekor.umcs.lublin.pl`