Algebra and Discrete Mathematics
Volume **19** (2015). Number 1, pp. 130–144
© Journal "Algebra and Discrete Mathematics"

RESEARCH ARTICLE

On the flag geometry of simple group of Lie type and multivariate cryptography

Vasyl Ustimenko

Communicated by V. I. Sushchansky

Abstract. We propose some multivariate cryptosystems 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 isomorphic to vector space over F_q 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 also consider the notion of symbolic Tits automata. The symbolic initial state is a string of variables $t_\alpha \in F_q$, where roots α are listed according Bruhat's order, choice of label will be governed by special multivariate expressions in variables t_α, where α is a simple root.

Deformations of such nonlinear map by two special elements of affine group acting on the plainspace can produce a computable in polynomial time nonlinear transformation. The information on adjacency graph, list of multivariate governing functions will define invertible decomposition of encryption multivariate function. It forms a private key which allows the owner of a public key to decrypt a ciphertext formed by a public user. We also estimate a polynomial time needed for the generation of a public rule.

Key words and phrases: Multivariate Cryptography, flag variety, Geometry of Simple Group of Lie type, Schubert cell, symbolic walks.

1. Introduction

Linear codes over finite field F_q are subspaces of ${F_q}^n$. The subspaces form a finite projective geometry of dimension $n-1$, which is a very important object of Pure Mathematics and Classical Coding Theory. Since late 80th some other applications of Finite Projective Geometry to Information Security have appeared (see [3], [4], devoted to Network Coding). In particular, it was used in Cryptography (see [5], where projective geometry were used for audentification protocols, or [6], [7], where it was used for the symmetric encryption and key exchange protocols respectively). Finite geometries now are widely used as tools for secret sharing. In current article we will introduce a new public key algorithms based on finite Lie geometries of normal and twisted type over the Coxeter Dynkin diagrams A_n, B_n, C_n and D_n. Public key algorithm of Multivariate Cryptography [1] based on finite projective geometry already was introduced recently at the conference Algebraic Combinatoric and Applications 2015 (ALCOMA 2015, Kloster Banz, Germany , see the program and book of abstracts on its web). In this paper we are going to present more general cryptosystem corresponding to the geometry of a finite simple group of rank $n \geqslant 2$.

In section 2 we present the concepts of a family of multivariate maps with polynomially invertible decomposition and its applications to cryptography.

In section 3 symbolic Tits automaton for the case of variety of maximal flags of the geometry of finite simple group will be defined. Its computations are polynomial maps of the vector space ${F_q}^N$, where N is a number of positive roots in corresponding root system. In fact, some special Tits automata over various diagrams have been used for the construction of key exchange protocols [7].

In section 3 we also consider the invertibility conditions for the map produced by Tits automaton.

We show that the polynomial map produced by Tits automaton can be treated as the polynomial map with invertible decomposition.

In section 4 we consider an interpretation of the geometry of simple Lie group of normal type and its flag system in terms of linear algebra. We will use the approach suggested in [9], [10], [11] for the description of the geometry of Shevalley group and the work of corresponding Tits automaton.

Conclusions are in section 5. The complexity estimates for the public key algorithm based on flag variety of geometry of Simple Group of Lie type are presented there.

2. On the general scheme for a cryptosystem based on a family of multivariate maps with an invertible decomposition

Multivariate cryptography (see [1]) is one of the directions of Postquantum Cryptography, which concerns with algorithms resistant to hypothetic attacks conducted by Quantum Computer. The encryption tools of Multivariate Cryptography are nonlinear multivariate transformations of affine space K^n, where K is a finite commutative ring.

Recall that affine *Cremona group* $C(K^n)$ is a totality of invertible maps f of affine space K^n over a Commutative ring K into itself, such that the inverse map f^{-1} is also a polynomial one.

Let us refer to the sequence of maps $f(n)$ from $C(K^n)$, $n = 1, 2, \ldots$ as *a family of polynomial degree* if the degree of each transformation is a parameter s of the size $O(n^t)$.

We say that a family $f(n) \in C(K^n)$ has a polynomially invertible decomposition if $f(n)$ can be written as a composition of elements $f^1(n), f^2(n), \ldots, f^{k(n)}(n)$ and the knowledge on this decomposition will allow us to compute the value of $y = f(x)$ and the re-image of given y in polynomial time $k(n)O(n^d)$ (see [2]).

We can create a new encryption map $h(n)$ as a deformation $\tau_L f(n)\tau_R$ of $f(n)$ with special invertible affine transformations τ_L and τ_R of K^n. If the family $h(n)$ on a symbolic level is presentable in a computable form and the value of $h(n)$ in given point of affine space is computable in polynomial time, then $h(n)$ is also a map with polynomially invertible decomposition.

Let $f(n) \in C(K^n))$ be a family of transformations with polynomially invertible decomposition. Then the following public key can be implemented.

Alice chooses parameter n. She knows the decomposition $f(n) = f(n,1)\ f(n,2) \ldots f(n,k(n))$. Notice that some transformations $f(n,i)$ can be not a bijective. Additionally she chooses an invertible monomial linear transformations τ_L of kind $x_i \to \lambda_i x_\pi(i)$, where π is a permutation on the set $\{1, 2, \ldots, n\}$. Alice also takes a bijective affine transformation τ_R of kind $\mathrm{x} \to \mathrm{x}A + \mathrm{b}$, where A is a non-singular matrix.

She computes the transformation $G = \tau_L f(n)\tau_R$ in affine Cremona group and writes it in the standard form $\mathrm{x}_i \to g_i(x_1, x_2, \ldots, x_n)$, $i = 1, 2, \ldots, n$.

Assume that public rules g_i are governed by the lists of monomial terms, written in some chosen order.

Notice, that the left application of τ_L does not change the number of monomial terms. The right application of τ_R can increase the number of monomial terms in n times. So the density $\mathrm{den}(\tau_L f(n)\tau_R)$ is $O(n^{d+1})$.

A public user (Bob) gets symbolic transformation $G = G(n)$ in the form of public rule $\mathrm{x}_i \to g_i(x_1, x_2, \ldots, x_n)$. He can encrypt by computation of the value of G on his plaintext $(x_1, x_2, \ldots, x_n)$ in $O(n^{s+d+1})$.

Alice keeps the decomposition $f(n) = f(n,1)f(n,2)\ldots f(n,k(n))$ as a deep secret. It allows her to decrypt Bob's ciphertext for $k(n)O(n^{t+3})$ elementary steps, because applications of known ${\tau_L}^{-1}$ and ${\tau_R}^{-1}$ cost $O(n)$ and $O(n^2)$, respectively. If Bob does not have an additional information on the transformation G then he has a difficult task of computation G^{-1}.

3. Symbolic Tits automata and bijective multivariate maps

Below we consider an abstract scheme for cryptosystem for special class of geometrical maps corresponding to the geometry of finite simple group $G = X_n(q)$ of rank $n \geqslant 2$. In this article we assume that $X_n(q)$ is a Shevalley group (in other terminology a simple group of normal type).

This group corresponds to Coxeter-Dynkin diagram X_n which also defines Weyl group W corresponding to root system Ω. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the list of simple roots, Ω^+ and Ω^- correspond to the list of sets of positive and negative roots. We assume that $|\Omega^+| = |\Omega^-| = N$. For each $\beta \in \Omega$ subgroup $U_\beta =< x_\beta(t) | t \in F_q >$ is isomorphic to additive group F_q (see [12]). Group G is generated by U_β, $\beta \in \Omega$, its unipotent subgroup $U =< U_\beta | \beta \in \Omega^+ >$ is a Sylow p subgroup of $X_n(q)$, $q = p^m$ for prime integer p. In fact, $|U| = q^N$.

Let $P_1, P_2, \ldots, P_n$ be the list of maximal parabolic subgroups of G corresponding to nodes of diagram X_n, then the Borel subgroup $P_1 \cap P_2 \cap \ldots P_n$ coincides with the normaliser $N_G(U)$ of the unipotent subgroup U.

The geometry of G is a totality $\Gamma(G)$ of all left cosets gP_i, where $g \in G$, $1 \leqslant i \leqslant n$ with the type function t, such that $t(gP_i) = i)$, and symmetric and irreflexive incidence relation I, such that $a, b \in \Gamma(G)$ if and only if $t(a) \neq t(b)$ and the intersection of left cosets is nonempty. Let $\Gamma_i(G) = \{a \in \Gamma(G) | t(a) = i\}$. We refer to a subset F of $\Gamma(G)$ as a flag of the geometry if each pair of elements from F is incident. We assume that $t(F) = \{t(a) | a \in F\}$. In case of maximal flag $t(F) = \{1, 2, \ldots, n\} = M$.

Let $GF(G)$ be the totality of maximal flags of $\Gamma(G)$ with the partition onto large Schubert cells, i. e. orbits of unipotent subgroup U on this set. In fact there is the unique largest Schubert cell of size q^N on which the unipotant group acts regularly.

Assume that for a flag F its type is $t(F) = M - \{i\}$. The residue $Res(F) = \{x \in \Gamma_i | xIa, a \in F\}$. We assume that $Ext(F)$ is the totality of all flags of kind $F \cup \{x\}$, $x \in ResF$. In fact $|Ext(F)| = |Res(F)| = q + 1$. The elements of $Ext(F)$ are from two different Schubert cells S_0 and S_1 such that $Ext(F) \cap S_0$ and $Ext(F) \cap S_1$ have cardinalities 1 and q. If $F \cup \{y\}$, where $y \in Res(F)$ is located in Schubert cell S_0 then we join F and maximal flag $F \cup \{y\}$ by a directed arrow labeled by pair (i, ∞), where ∞ is a formal symbol. If $y \in S_1$, then there is a unique root subgroup $U_\beta = \{x_\beta(t) | t \in F_q\}$ which acts regularly on $Ext(F) \cap S_1$. Element $z = F \cup \{y\}$ from S_1 can be identified with corresponding element $x_r(t) \in U$ and with parameter $\mu(z) = t \in F_q$. We join F and z by an arrow with the label $(i, \mu(z))$ in that case.

Let F be a maximal flag. For each $i \in \{1, 2, \ldots, n\}$ we consider a subflag F^i of type $M - \{i\}$ and join F and representative y from $Ext(F^i)$ by an arrow with the label $(i, \mu(y))$, where $\mu(y) \in \{\infty\} \cup F_q$. So we constructed a labeled directed graph $T(G)$ on the set of maximal flags with $n(q + 1)$ output arrows for each vertex, n of them are loops.

We convert $T(G)$ to Tits automaton by an announcement that the initial and accepting states of this automaton have to be elements of the largest Schubert cells.

If we ignore labels and loops of $T(G)$, this graph can be identified with the directed graph of adjacency relation : *two flags are adjacent if their intersection has cardinality* $n - 1$. The action of unipotant subgroup U defines the partition on the large Schubert cells and labeling of $T(G)$.

Let F, F' be flags joined by an arrow of $T(G)$ labeled by (i, a), $i \in M$,$a \in \infty \cup F_q$. The transition function ${T^i}_a$ sends F to F' for each pair of flags joined by arrow with the label (i, a). The regular computation of Tits automaton is the composition E of ${T^{i_1}}_{a_1}, {T^{i_2}}_{a_2}, \ldots, {T^{i_r}}_{a_r}$, where $i_l \neq i_{l+1}$, $l = 1, 2, \ldots, r-1$ which sends flag from the largest Schubert cell to another element of this cell. As it follows from the definition of Tits automaton its computation is not a bijective linear map on the vector space of the largest Schubert cell. The existence of the reverse directed walk from the image to the initial state insures that the initial state is uniquely defined by its projection on tangent space and the computation.

We also define a Schubert automaton $Sch(G)$ as one obtained from Tits automaton for $T(G)$ by deleting all flags located outside of the largest Schubert cell together with input and output arrows and their labels.

The regular action of unipotent subgroup U on the largest Schubert cell $Sch(G)$ allows us to identify $Sch(G)$ with ${F_q}^N$.

Finally we define symbolic Tits automaton with the symbolic initial state $(t_1, t_2, \ldots, t_N)$, where t_i are variables corresponding to roots from Ω^+ and parameters $a_j \neq \infty$ are polynomials in N variables $t_{i_1}, t_{i_2}, \ldots, t_{i_n}$ related to simple roots. The computation of a symbolic Tits automaton induces polynomial transformation E_n of ${F_q}^N$. The map E_n corresponds to a "symbolic walk" $S_{n,m}$ of length m in $A_n(q)$. The map E_n appears together with their decomposition on "symbolic transition functions". The infinite families of highly nonlinear bijective computable transformations E_n with polynomially invertible decompositions have been introduced. So the described above (section 1) scheme can be implemented to create a cryptosystem in the case of groups of normal type $A_n(q), B_n(q), C_n(q), D_n(q)$ and twisted groups ${}^2A_n(q)$.

Symbolic Tits automata of groups of restricted rank $E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, $G_2(q)$, ${}^2E_6(q)$, ${}^2F_4(q)$, $q = 2^{2l+1}$, ${}^2D_4(q)$, ${}^3D_4(q)$ (see [12]) can be used for the construction of S-boxes and hash functions.

Special Tits automata can be a base for stream ciphers (see [8]).

Let us consider a regular computation of symbolic Tits automaton with the symbolic initial state $(t_1, t_2, \ldots, t_N)$, where t_i, $i = 1, 2, \ldots, N$ are variables, defined by putting labels from $F_q[t_{i_1}, t_{i_2}, \ldots, t_{i_n}] \cup \{\infty\}$. The specialization of symbolic initial state $t_1 = a_1, t_2 = a_2, \ldots, t_N = a_N$ produces the computation of Tits automaton with initial state $(a_1, a_2, \ldots, a_N) \in {F_q}^N$. Let $e_1, e_2, \ldots, e_N$ be the fixed basis which we use for writing elements of ${F_q}^N$ as tuples.

We refer to the symplectic subspace S of all tuples of kind e_{i_1},e_{i_2},$\ldots$,e_{i_n} as a tangent subspace of the largest Schubert cell. The computation in a symbolic Tits automaton sends a symbolic initial state t $= (t_1, t_2, \ldots, t_N)$ into $E(\mathrm{t})$, where E is a polynomial multivariate map of ${F_q}^N$ into itself. Tangent subspace is invariant subspace for a transformation E. Let $(j_1, f_1), (j_2, f_2), \ldots, (j_k, f_k)$ be the sequence of the labels such that $f_i \in F_q[t_{i_1}, t_{i_2}, \ldots, t_{i_n}] \cup \infty$ for the computation of a symbolic Tits automaton.

We assume that $j_s \neq i_{s+1}$, $s = 1, 2, \ldots, k-1$. The computation E is the composition of symbolic transition functions ${G_{i_1}}^{f_{i_1}}, {G_{i_2}}^{f_{i_2}}, \ldots, {G_{i_m}}^{f_{i_m}}$. Recall, that the resulting state of our computation is the flag of the largest Schubert cell.

Let E' be the restriction of E on S.

Proposition 3.1. The map E is a bijection if and only if its restriction E' on the tangent space is one to one correspondence.

Proof. Let us assume that b_β, $\beta \in \Omega^+$ are coordinates of the image of the vector t. The bijective map E' can be written in the form $h_i(t_{\alpha_1}, t_{\alpha_2}, \dots t_{\alpha_n}) = b_i$, $i = 1, 2, \dots, n$.

Theoretically we can solve this system and find $t_{\alpha_1} = a_1$, $t_{\alpha_2} = a_2$, $\dots$, $t_{\alpha_n} = a_n$. After that we can compute $c_j = f_j(a_1, a_2, \dots, a_n)$ for $j = 1, 2, \dots, m$. The map E acts outside of tangent space as $t_\beta \to {G_{i_1}}^{c_1} {G_{i_2}}^{c_2} \dots {G_{i_m}}^{c_m}(\mathrm{t})$ for nonsimple root β. It is a linear map depending on $N - n$ variable. Notice that alternatively we can consider the specialisation $t_{\alpha_1} = a_1$, $t_{\alpha_2} = a_2$, $\dots$, $t_{\alpha_n} = a_n$ of standard presentation of E which exists and write linear equations. We can take a unique solution of system ${G_{i_1}}^{c_1} {G_{i_2}}^{c_2} \dots {G_{i_m}}^{c_m}(\mathrm{t}) = b_\beta$ for variables t_β, $\beta \in \Omega^+ - \{\alpha_1, \alpha_2, \dots, \alpha_n\}$. So we get the well defined unique re-image t. □

The map E corresponds to a *symbolic walk* of a length k in a symbolic Tits automaton.

Proposition 3.2. Let map E be a bijection defined by Tits automaton and it is computable in a given vector from ${F_q}^N$ in a polynomial time. Assume that a tangent space is known and the reimage of E' in a given point is also computable in a polynomial time. Then the reimage of E in a given point is computable in a polynomial time.

Proof. The restriction of map E on symplectic subspace S is the map $t_{\alpha_r} \to a_{j_r}[t_{\alpha_1}, t_{\alpha_2}, \dots, t_{\alpha_n}] = t'_{\alpha_r}$, $r = 1, 2, \dots, n$, where j_r is the last appearance of r as a first coordinate of label (r, a_l), $a_l \in F[t_{\alpha_1}, t_{\alpha_2}, \dots, t_{\alpha_n}]$ if such appearance exists. In the opposite case we have simply $t_{\alpha_r} \to t_{\alpha_r}$.

We refer to expressions $a_{j_r}[t_{\alpha_1}, t_{\alpha_2}, \dots, t_{\alpha_n}]$ as tangent coordinates of the walk (or computation).

The computation of the inverse for $E|_S$ in polynomial time will allow us to solve the system of equations $a_{j_r}[t_{\alpha_1}, t_{\alpha_2}, \dots, t_{\alpha_n}] = t'_{\alpha_r}$ for $t_{\alpha_i} = {t^*}_i$, $i = 1, 2, \dots, n$. It gives us an opportunity to compute parameters $a_s = f_{i_s}({t^*}_1, {t^*}_2, \dots {t^*}_{n-1})$, $s = 1, 2, \dots, m$.

After that we can consider the computation of Tits automaton ${G_{i_1}}^{a_1} {G_{i_2}}^{a_2} \dots {G_{i_m}}^{a_m}$ sending vector with coordinates t_β onto the known image of E. Recall that t_{α_i} coincides with ${t^*}_i$, $i = 1, 2, \dots, n$. So, we have system of $N - n$ linear equations in $N - n$ variables, which has a unique solution. It is clear that we can solve this system for polynomial time $O(N^3)$ and get the re-image of the map E. Notice, that we can get system of linear equations with $N - n$ variable via specialisation $t_{\alpha_i} = {t^*}_i$, $i = 1, 2, \dots, n$ of polynomial map E. □

Corollary 3.3. Under the conditions of previous statement the map E is a map with the polynomially invertible decomposition $E = {G_{i_1}}^{f_{i_1}} {G_{i_2}}^{f_{i_2}} \dots {G_{i_m}}^{f_{i_m}}$.

We say that the computation of Tits automaton is a *tame* one if it corresponds to symbolic walk given by $(j_1, f_1), (j_2, f_2), \dots, (j_k, f_k)$, $f_i \in F_q[x_{i_1}, x_{i_2}, \dots, x_{i_m}] \cup \infty$, for $i = 1, 2, \dots, k$, $j_s \neq j_{s+1}$, $s = 1, 2, \dots, k-1$, each $r \in M$ appears in the list $j_1, j_2, \dots, j_k$ not more than $O(1)$ times and degree of each f_i is bounded by $O(n)$ and density $O(1)$.

In the last section of the paper we show that the following statement holds.

Lemma 3.4. Let E_n be the map corresponding to tame computation of Tits automaton. Then it has a polynomial density and a polynomial degree bounded by $O(n^3)$ and $O(n^2)$ respectively.

Example. Polynomially invertible E_n corresponding to the tame computation of Tits automaton can be constructed by the following method.

We choose the length of the walk m as a linear expressions from n. We assume additionally that the restriction E' of E onto S is the bijective map $t_{i_s} \to b_{i_s} {t_{\mu(i_s)}}^{k_{i_s}} + d_{i_s}$, $s \in \{1, 2, \dots, n\}$, where μ is a permutation on $\{i_1, i_2, \dots, i_n\}$, and b_{i_s}, d_{i_s} are constants from F_q and k_{i_s} are constant integers such that the equation of kind $z^{k_{i_s}} = b$ have unique solution. We assume that the field F_q is fixed. It means that the re-image for E' in given vector can be computed for $O(n)$ elementary steps.

Notice that functions f_{j_s} which are not a tangent coordinates can be arbitrary polynomials of degree $O(n)$ and density $O(1)$.

We refer to such invertible map E' as invertible tame map. We can use more general maps of kind $E' = \tau_1 H \tau_2$ where $\tau_i(x) = xA_i + c_i$, $i = 1, 2$ where rows and columns of invertible $n \times n$ matrices A_i have finite number of nonzero entries and H is an invertible tame map. Natural example of tame computation is the following.

Let $E : {F_q}^N \to {F_q}^N$ be the polynomial map induced by a regular tame computation of symbolic Tits automaton, such that different from ∞ labels are "shifted" monomial terms of kind $at_{i_1}^{s_1(n)} t_{i_2}^{s_2(n)}, \dots, t_{i_n}^{s_n(n)} + b$, where a and b are constants, parameters $s_i(n)$, $i = 1, 2, \dots, n$ are linear expressions in n, such that $s_1(n) + s_2(n) + \dots + s_{n-1}(n)$ is also a linear expression. We choose the length of the walk k as a linear expressions from n.

Remark. Let us consider the deformation $\tilde{E_n} = \tau_1 E_n \tau_2$ of Δ, where τ_1 is invertible monomial transformation $t_i \to \lambda_i t_{\pi(i)}$, $\lambda_i \in F_q^*$, $i = 1, 2, \ldots, N$, π is a permutation on $\{1, 2, \ldots, N\}$, τ_2 is a general bijective affine map of ${F_q}^N$ into itself.

For the deformation $\tilde{E}$ of E the equality $\deg(\tilde{E}) = \deg(E)$ holds. Transformations E and $\tau_1 E$ have the same densities. Density of $E\tau_2$ is at most n^2 times larger than the density of E.

Let us evaluate the complexity of the multivariate cryptosystem based on tame computation of the Tits automaton.

Notice that evaluations of degree and density shows that Bob can compute the value of $\tilde{E}$ in a given point for $O(n^7) = O(N^{3+1/2})$ elementary steps.

We can use invertible tame computations defined in the Example above. The time of its generation and the time of the computation of its inverse will be evaluated in the last section.

4. On the interpretation of Lie geometry and Tits automaton in terms of linear algebra

4.1. Graphs and incidence system

The missing definitions of graph-theoretical concepts which appear in this paper can be found in [13], [14] or [16]. Simple graphs are undirected graphs 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 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 one 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 on its type (point or line), then the incidence structure is a tactical configuration in the sense of Moore (see [15]).

The graph is k-regular if each of its vertices 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 $t(F) = \{t(x) | x \in F\}$

4.2. 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 $\alpha \cap \beta \neq \varnothing$. 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 a set of distinguished generators given by $S = \{s_1, s_2, \ldots, s_l\}$ ana 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 $m_{i,j} \geqslant 2$ (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 $W_i =< S - \{s_i\} >$, $1 \leqslant i \leqslant l$ we obtain a group incidence system $\Gamma_W = \Gamma(W, W_i)_{1 \leqslant i \leqslant l}$ is called the Coxeter geometry of W. The W_i are referred to as the *maximal standard subgroups* of W (see [17]).

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) *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 (i)–(iv) imply that (W, S) is a Coxeter system (see [17] or [12]). Whenever (G, B, N, S) is Tits system, we call the group W 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 $\Gamma_G = \Gamma(G, P_i)_{1 \leqslant i \leqslant l}$ is commonly referred to as *Lie geometry* of G (see [16]). Note that Lie geometry of G and 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 *Ret* is called a *retraction* (see [18]).

Throughout this section (G, B, N, S) is 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 [18],[12], [17]). We write $G = X_l(K)$ to signify that G is 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 are associated Coxeter and Lie geometries.

4.3. On the embeddings of geometries into Lie algebra

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

Let $S = \{r_1, r_2, \dots, r_l\}$ be the set of Coxeter generators of Weyl group W. Let $\alpha_1{}^*, \alpha_2{}^*, \dots, \alpha_l{}^*$ be a dual basis of $\alpha_1, \alpha_2, \dots, \alpha_l$, 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 $l_1(\alpha)l_2(\alpha) \geqslant 0$ 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, $1 \leqslant i \leqslant l$.) This gives the desired embedding since H is a subset in R^*.

We now consider an analogous embedding of Lie geometry Γ_G into Borel subalgebra $U = L_0 + L^+$ of L. Let $d = \alpha_1{}^* + \alpha_2{}^* + \dots \alpha_l{}^*$. Then we can take $\Omega^+ = \{\alpha \in \Omega | d(\alpha) \geqslant 0\}$ 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 be 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 holds:

(i) $h_1(\alpha)h_2(\alpha) \geqslant 0$ 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 [10] (see [11]) it is shown that this newly defined incident system is isomorphic to Lie geometry Γ_G, provided that the characteristic of K is zero or sufficiently large one to ensure the isomorphism at the level of the subgeometries (H, I, t) and Γ_W. Then analogous to Weyl case there exists a unique isomorphism Retr of $\Gamma(G)$ into (U, I, t) which sends P_i to α_i, $1 \leqslant i \leqslant l$.

Proposition 4.1. 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) evaluate the degree and density of a deformation of tame computation of Tits automaton as values of size $O(n^2)$ and $O(n^3)$ respectively.

(iii) generate a tame computation of Tits automaton consisting of k elementary steps for time $O(n^5)$.

Proof. The part (i) is straightforward. Let us discuss point (ii). Let us consider the tame computation corresponding to the password $\mathrm{p} = (j_1, f_1)$, (j_2, f_2), …, (j_k, f_s), where $f_i \in F_q[t_{i_1}, t_{i_2}, \ldots t_{i_n}] \cup \infty$.

The maximal flag F of the $\Gamma(G)$ can be treated as sequence (h_1, v^1), (h_2, v^2), … (h_n, v^n) of elements of geometry of type $1, 2, \ldots, n$ such $\{h_1, h_2, \ldots h_n\}$ is a flag in Weyl geometry and $[h_i + v^i, h_j + v^j] = 0$, $i, j \in M$. We refer to such a sequence as *expanded data* of the flag.

Let us denote $\eta(h_i)$ as D_i and treat vectors from L_{h_i} as functions from D_i to F_q.

It is easy to see that the flag is uniquely defined by the flag h_1,h_2,…,h_n of Weyl geometry, vector v^1, $v^2|D_2 - D_1$, $v_3|(D_3 - (D_1 \cup D_2))$, …, $v_n|(D_n - (D_1 \cup D_2 \cdots \cup D_{n-1}))$. We refer to such a data of the flag as *compressed data* of the flag. We assume that the projection of vector on empty set is the formal symbol ∞.

We have the following interpretation of Tits automaton.

Assume that a flag F' of type $M-\{i\}$ is a subset of F of type M as above. The residue $Res(F')=\{x\in\Gamma_i|xIa, a\in F\}$. There are two elements h, h' of type i such that sets $S_1=\{h+x|x\in L_h\}$ and $S_0=\{h'+x'|x'\in L_{h'}$ have nonempty intersections with $Res(F')$ of type i of cardinality q and 1.

Then we join flags F and $\tilde{F}$ of kind $(h_1+v^1),(h_2+v^2),\ldots,(h_{i-1}+v^{i-1}),(h+x),(h_{i+1}+v^{i+1}),\ldots,(h_n+v^n)$, $h+x\in Res(F)$ by (i,a_i), $a_i=x|\eta(h)-((D_1\cup D_2\cdots\cup D_n)-D_i)$. Additionally we join F and $F'\cup S_0\cap Res(F')$ by symbol (i,∞). We have to do such labeling for each subset of F' of cardinality $n-1$. Repetition of this procedure for each maximal flag bring us Tits automaton for which elements from the largest Schubert cells are accepting states. An initial state also has to be chosen as element of the largest Schubert cell.

Let us consider the tame computation corresponding to the password p $=(j_1,f_1)$, (j_2,f_2), $\ldots$, (j_k,f_s), where $f_i\in F_q[x_1,x_2,\ldots,x_n]\cup\infty$.

We define a type Sig(p) o as sequence $(\sigma_1,\sigma_2,\ldots,\sigma_k)$, where $\sigma_i=1$ if $a_i\neq\infty$ and $\sigma_i=\infty$ in remaining cases.

Let F be an initial state. Notice that for symbolic transition functions produces the chain $F=F_0, F_1={G_{j_1}}^{f_1}(F), F_2={G_{j_2}}^{f_2}(F_1),\ldots F_k={G_{j_k}}^{f_{i_k}}(F_{k-1})$.

The sequence $R_i=Res(F_i)$, $i=0,1,2,\ldots,k$ does not depend on the choice of different from ∞ functions $f_1,f_2,\ldots,f_k$ or their specialisations. It depends only on sequences $(j_1,j_2,\ldots,j_k)$ and $(\sigma_1,\sigma_2,\ldots,\sigma_k)$. Consequtive elements R_i and R_{i+1}, $i=0,1,\ldots,k-1$ are adjacent elements of $\Gamma(W)$ or $R_i=R_{i+1}$. Recall that $R_0=R_k$, corresponds to element of group W with the maximal length of irreducible representation in generators from S (Coxeter element).

So the map E is a composition of multivariate maps ${G_{j_1}}^{f_1}: L_{R_0}\rightarrow L_{R_1}$, ${G_{j_2}}^{f_2}: L_{R_1}\rightarrow L_{R_2}$, $\ldots$, ${G_{j_k}}^{f_k}: L_{R_{k-1}}\rightarrow L_{R_k}$.

The best way to compute is a consequtive computation of F_1, F_2,$\ldots$,F_k. We assume that F_0 is given in its compressed form. For $O(n^3)$ operations we can convert compressed data into the expanded form. Further, we make all steps of Tits computation and present the final data in compressed form. Each step gives us addition of $O(n^2)$ new monomial terms, number of steps is $O(n)$.

It means that we can evaluate the density as $O(n^3)$. During the computation a monomial terms of degree $O(n^2)$ will appear. So we justify (ii). The computation of each monomial term costs $O(n^2)$. The product of two monomial terms can be done in time $O(n^2)$. Each step of computation costs $O(n^2)$ operations and the number of terms is n. It means that the generation of the map in the standard form costs $O(n^5)$ and we prove (iii). □

5. Conclusion and complexity estimates

Let us consider the deformation $\tilde{E_n} = \tau_1 E_n \tau_2$ of Δ, where τ_1 is invertible monomial transformation $t_i \to \lambda_i t_{\pi(i)}$, $\lambda_i \in F_q^*$, $i = 1, 2, \ldots, N$, π is a permutation on $\{1, 2, \ldots, N\}$, τ_2 is a general bijective affine map of ${F_p}^N$ into itself.

Recall that for the deformation $\tilde{E}$ of E the equality $\deg(\tilde{E}) = \deg(E)$ holds. Transformations E and $\tau_1 E$ have the same densities. Density of $E\tau_2$ is at most n^2 times larger than the density of E.

Let us evaluate the complexity of the multivariate cryptosystem based on tame computation of Tits automaton.

Notice that evaluations of degree and density shows that Bob can compute the value of $\tilde{E}$ in a given point for $O(n^7)$ elementary steps. Alice can use described above method of proposition 4.1 as algorithm for the decryption of ciphertext c given by Bob. The application of τ_2^{-1} to c costs $O(N^2) = O(n^4)$. The solution of the nonlinear equations and the computation of E' costs $O(n)$. The solution of linear system costs $O(N^3) = O(n^6)$. So re-image of E can be computed for $O(n^7)$. The application of known ${\tau_1}^{-1}$ costs $O(N)$. It means that for $O(n^{13})$ Alice can decrypt.

Generation of E costs $O(n^5)$, its deformation by τ_1 and τ_2 need $O(n^2)$ and $O(n^4)$ operations, respectively. So generation of $\tilde{E}$ costs $O(n^{11})$.

As usually, we have to evaluate complexity as function from the dimension N of plainspace. So Bob applies public rule for $O(N^{3+1/2})$. Alice can decrypt in time $0(N^{6+1/2})$. The generation of public key costs $O(N^{5+1/2})$.

The paper is dedicated to the memory of my teacher Lev Kaluzhnin. His wide mathematical vision brought us, participants of his Seminar, the light of Modern Algebra.

References

[1] Ding J., Gower J. E., Schmidt D. S., *Multivariate Public Key Cryptosystems*, 260. Springer, Advances in Information Security, v. 25, (2006).

[2] V. Ustimenko, On Multivariate Cryptosystems Based on Computable Maps with Invertible Decompositions, Annales of UMCS, Informatica, volume 14 (2014) , Special issue "Proceedings of International Conference Cryptography and Security Systems", pp. 7-18.

[3] Anton Betten, Mihael Braun, Adalbert Kerber, Axel Kohnert, Alfred Wasserman *Error Correcting Linear Codes Isometry and Applications*, Springer, 2006.

[4] Andreas Stephan Essenhans, Axel Kohnert, Alfed Wassermann, *Constructions of codes for Network Coding*, arXiv:1005, 2839[cs].

[5] A. Beultespacher, *Enciphered Geometry, Some Applications of Geometry to Cryptography*, Annals of Discrete Mathematics, v. 37, 1988, 59-68.

[6] V. A. Ustimenko, *Graphs with Special Arcs and Cryptography*, Acta Applicandae Mathematicae, vol. 71, N2, November 2002, 117-153.

[7] V. Ustimenko, *Schubert cells in Lie geometries and key exchange via symbolic computations*, Proceedings of the International Conference ”Applications of Computer Algebra, ACA 2010”, Vlora, Albanian Math. J., 2010, Vol 4, n. 4, 135-145.

[8] V. Ustimenko, *On walks of variable length in Schubert incidence systems and multivariate flow ciphers*, Dopovidi of Nathional Acad. Sci. of Ukraine, 2014, No 3, P. 55 - 150.

[9] 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

[10] V. A. Ustimenko, *Linear interpretation of Chevalley group flag geometries*, Ukraine Math. J. 43, Nos. 7,8 (1991), pp. 1055–1060 (in Russian).

[11] V. A. Ustimenko, *On the Varieties of Parabolic Subgroups, their Generalizations and Combinatorial Applications*, Acta Applicandae Mathematicae 52 (1998): pp. 223–238.

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

[13] F. Harary, *Graph Theory*, Addison-Wesley Publishing Co, Reading, MA (1966).

[14] R. Wilson, *Introduction to Graph Theory*, Oliver & Boyd, Edinburg, (1972).

[15] E. Moore, *Tactical Memoranda 1-3*, Amer. J. of Math., vol. 18, n3 (1896), 264-29o.

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

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

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

Contact information

Vasyl Ustimenko
University of Maria Curie Skłodowska, Pl. Maria Curie Skłodowska 1, pok. 323, 20-931, Lublin, Poland
E-Mail(s): vasyl@hektor.umcs.lublin.pl

Received by the editors: 23.01.2015
and in final form 21.02.2015.