On linguistic dynamical systems, families of graphs of large girth and cryptography

Vasiliy A. Ustimenko

April 15, 2005

Kiev Mohyla Academy (Ukraine) and IME (University of Sao Paulo, Brasil), e-mails: vasyl@mail.kar.net, ustimenk@ime.usp.br

Abstract

Paper is devoted to studies of linguistic dynamic system of dimension $n \geq 2$ over arbitrary commutative ring K, i.e. family F of nonlinear polynomial maps $f_\alpha : K^n \to K^n$ depending on "time" $\alpha \in \{K - 0\}$ such that ${f_\alpha}^{-1} = f_{-\alpha}$ and $f_{\alpha_1}(x) = f_{\alpha_2}(x)$ for some $x \in K^n$ implies $\alpha_1 = \alpha_2$, each map f_α has no invariant points.

The neighbourhood $\{f_\alpha(v) | \alpha \in K - \{0\}\}$ of element v defines the graph $\Gamma(F)$ of a dynamical system on the vertex set K^n.

We shall refer to F as linguistic dynamical system of rank $d \geq 1$ if for each string $\mathrm{a} = (\alpha_1, \ldots, \alpha_s)$, $s \leq d$, where $\alpha_i + \alpha_{i+1}$, is not a zero divisor for $i = 1, \ldots d-1$, vertices v and $v_\mathrm{a} = f_{\alpha_1} \times \ldots \times f_{\alpha_s}(v)$ in the graph are connected by a unique pass.

For each commutative ring K and even integer number $n \neq 0 \bmod 3$ there is family of linguistic dynamical system $L_n(K)$ of rank $d \geq 1/3n$. Let $L(n, K)$ be the graph of a dynamical system $L_n(q)$.

If $K = F_q$ graphs $L(n, F_q)$ form a new family of graphs of large girth. The projective limit $L(K)$ of $L(n, K)$, $n \to \infty$ is well defined for each commutative ring K, in case of integral domain K graph $L(K)$ is a forest, if K has zero divisors the girth of K is dropping to 4.

We introduce some other families of graphs of large girth related to the dynamical systems $L_n(q)$ in case of even . The dynamical systems and related graphs can be used for the development of symmetric or asymmetric cryptographical algorithms. These graphs allow us to establish the best known upper bounds on the minimal order of regular graphs without cycles of length $4n$, n is odd ≥ 3.

Key Words: Infinite groups acting on graphs, dynamical systems, graphs with memory, assymptotic combinatorics, families of graphs of large girth, cryptography.

1 Introduction

It is well known that a continuous bijection of the interval $[a, b]$ has a fixed point. In case of open variety K^n, where K is commutative ring situation is different. For each pair (K, n), $n \geq 3$ and each $t \in K - \{0\}$ we shall construct a linguistic dynamical system, i.e family $F = F_n(K) = \{f_t\}$ of invertible nonlinear polynomial maps $f_t : K^n \to K^n$ without fixed points ($f_t(x) \neq x$ for each $x \in K^n$), such that ${f_t}^{-1} = f_{-t}$ and $t_1 \neq t_2$ implies $f_{t_1}(x) \neq f_{t_2}(x)$ for each x.

Foe each sting $\mathrm{a} = (a_1, \ldots a_s$ we consider the composition $G_\mathrm{a} = f_{a_1} \times f_{a_2} \times f_{a_s}$ of transformations f_{a_i}, $i = 1, \ldots, s$.

We shall refer to a string $\mathrm{a} = (a_1, \ldots, a_s)$ with regular elements (not zero divisors) $a_i + a_{i+1}$, $i = 1, \ldots, s-1$ as regular string of length s. Let $R_s = R_s(K)$ be the totality of all regular string of length s.

The level $d = d(F)$, $d \geq 1$ of linguistic dynamical system F is the maximal number s such that for each $\mathrm{a} \in R_s$ condition $G_\mathrm{a}(x) = G_\mathrm{b}(x)$, $\mathrm{b} \in K - \{0\}^s$ for some $x \in K^n$ implies $\mathrm{a} = \mathrm{b}$.

The rank $r = r(F)$, $r \geq 1$ of linguistic dynamical system F is the maximal number s such that for each $\mathrm{a} \in R_s$ the condition $G_\mathrm{a}(x) = G_\mathrm{b}(x)$, $\mathrm{b} \in K - \{0\}^l$, $l \leq s$ implies $\mathrm{a} = \mathrm{b}$. Let us consider simple graph $\Gamma = \Gamma(F)$ of the dynamical system F with the vertex set $V = K^n$ such that $u \in V$ and $v \in V$ are connected by edge if and only $f_t(u) = v$ for some $t \in K$.

The property $d(F) \geq s$ means that for each vertex x and "regular" string $\mathrm{a} = (\mathrm{a}_1, \ldots, \mathrm{a}_\mathrm{s})$, $s \leq d$ as above x and $F_\mathrm{a}(x) = f_{a_1} \times \ldots \times f_{a_s}(x)$ are not included together in a cycle of even length $\leq 2d$ in the graph $\Gamma(F)$.

The property $r(F) \geq s$ means that for each vertex x and $\mathrm{a} \in R_s$ vertices x and $G_\mathrm{a}(x)$ are connected by the unique pass of length $\leq s$.

Recall that the girth $g = g(\Gamma)$ of the graph Γ is the length of its smallest cycle.

Property $r(F) \geq s$ implies that in case of integral domain K the girth g of the graph $\Gamma(F)$ is $> 2s$.

In section 4 we construct explicitly the family of dynamical systems $L_n(K)$, $n \neq 0(\mathrm{mod})\ 3$ is even number ≥ 2 of rank $r \geq 1/3n$ and level $d \geq 2/3n$. It means that the family

$L(n,q) = L(n,F_g)$ of graphs of dynamical systems $L_n(q)$ of fixed degree $q-1$ satisfies to the inequality $g(L(n,q)) \geq \gamma \log_{q-2} q^n$, where constant γ does not depend on n, its value is approximately $2/3\log_{q-2} q$. So they form a family of graphs of large girth in sense of N. Biggs [2] for each prime power q. We shall construct other family of graphs of large girth $B(n,q)$, related to $L_n(q)$, $n = 4, \ldots$ for each even prime power q.

Essential algorithmic advantage of new families from the family of Cayley graphs $X(p,q)$, constructed by G.Margulis, is the following : the set of vertices for $X(p,q)$ is the group $PSL(2,q)$, which is algebraic manifold over prime field F_q of dimension bounded by constant, while sets of vertices for graphs $L(n,q)$ and $B(n,q)$ are varieties ${F_q}^n$ and ${F_q}^* {F_q}^{n-1}$ of dimension n over F_q. It means that algorithms related to new families graphs can be done by Turing machine of algebraic transformations of the potentially infinite text over the fixed alphabet F_q. Graphs $L(n,q)$ ad $B(n,q)$ are not bipartite in the difference with members of other known family $CD(n,q)$ ([16]) of graphs of large girth. There is a canonical map of $L(n+2,K)$ $(B(n,q))$ onto $L(n,K)$ $(B(n,q))$ and the projective limit $L(K)$ $(B(K))$ of $L_(n,K)$ $(B(n,q)$, respectively) is well defined.

Mentioned above four families give us the full list of families of graphs of large girth with unbounded degree. They satisfy to inequality $g \geq clog_{k-1}(v)$, where g, k, v are girth, degree and order, of the graph from the family, where the "velocity of logarithmic growth of girth" c is constant.

We consider the definition of *arithmetical dynamical system* $F = \{f_\alpha | \alpha \in Q\}$ simply via consideration of quasi projective manyfold M of K^n instead of K^n and requirement $f_\alpha \in F$ instead of ${f_\alpha}^{-1} = f_{-\alpha}$ f$_{-\alpha}$, Q is just a subset of K. Major justification of *arithmetical graphs* related to such dynamical systems is that they are examples of *graphs with memory* (see [29]) because we can not only consider such a graph as finite automaton where states v and $f_\alpha(v)$ are connected by the arrow with the labl α, but each state v is a string of characters from the alpabet K.

We consider explicit construction of arithmetic dynamical systems $D_n(K)$ and $C_n(K)$ on $K^n \cup K^n$ related to permutational representations of infinite group $U(K)$ and $CU(K)$ defined over arbitrary commutative ring, if K is an integral domain than $CU(K)$ is a free product $K^+ * K^+$, where K^+ is an additive group of the ring, well defined projective limit of graphs $\Gamma(C_n(K))$ is an infinite tree. If K has zero divisors, then the girth of each graph $\Gamma C_n(K))$ and their projective limit is dropping to 4 (see section 4).

The ideas on applications of graphs of large girth and dynamical systems as above to Cryptography are considered in section 3.

Section 5 devoted to graphs and dynamical systems related to polarities of graphs $\Gamma(D_n(K))$ and $\Gamma(C_n((K))$. It contains explicit construction of family $L_n(K)$.

2 Cages, regular graphs without even cycles and families of graphs of large girth

The missing definitions of graph-theoretical concepts which appears in this paper can be found in [6] or [28]. 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. $|V(G)|$ is called the *order* of G, and $|E(G)|$ is called the *size* of G. A path in G is called *simple* if all its vertices are distinct. When its convenient, we shall identify G with the corresponding antireflexive binary relation on $V(G)$, i.e. $E(G)$ is a subset of $V(G) \times V(G)$. The length of a pass is a number of its edges.

The girth of a graph G, denoted by $g = g(G)$ is the length of the shortest cycle in G. Let $k \geq 3$ and $g \geq 3$ be in integers. A (k, g)-graph is a k-regular graph with girth exactly g. A $(k, g) -$ cage is a (k, g)-graph of minimal order. The problem of determining the $v(k, g)$ of a (k, g)-cage is unsolved for most pairs (k, g) and is extremely hard in general case. By counting the number of vertices in the breadth-first-search tree of a (k, g)-graph, one easily establishes the following lower bounds for $v(k, g)$:

$v(k, g) \geq k(k-1)^{(g-1)/2}/(k-2)$ for g odd, $k \geq 4$

$v(k, g) \geq 2(k-1)^{g/2-2}/(k-2)$ for g even, $k \geq 4$

The problem of determining $v(k, g)$ was posed in 1959 by F. Kartesi who observed that $v(3, 5) = 10$ was realized by the Petersen graph (see [9]). The above lower bound had been established by Tutte [30].

Let us consider the family of graphs G_i of degree l_i and unbounded girth g_i such that

$$g_i \geq \gamma \log_{l_i-1}(v_i) \tag{1}$$

The last formula means that G_i, $i = 1, \ldots$ form an infinite *family of graphs of large girth* in the sense of N. Biggs [3].

The order of graphs from such a family is close to the lower bound on $v(k, g)$, this bound shows that $\gamma \leq 2$ but no family has been found for which $\gamma = 2$. Bigger γ's correspond to the larger girth.

For many years the only significant result were the theorems of Erdø"s' and Sachs [10], [25] and its improvement by Sauer [26], Walther [40], [41], and

others (see [7] for more details and references), who using nonconstructive methods proved the existence of infinite families with $\gamma = 1$. The first explicit examples of families with large girth were given by Margulis [21] with $\gamma = 0.44$ for some infinite families with arbitrary large valency, and $\gamma = 0.83$ for an infinite family of graphs of valency 4. The constructions were Cayley graphs of $SL_2(Z_p)$ with respect to special sets of generators. Imrich [13] was able to improve the result for an arbitrary large valency, $\gamma = 0.48$, and to produce a family of cubic graphs (valency 3) with $\gamma = 0.96$. A family of geometrically defined cubic graphs, so called sextet graphs, was introduced by Biggs and Hoare [5]. They conjectured that these graphs have large girth. Weiss [42] proved the conjecture by showing that for the sextet graphs (or their double cover) $\gamma \geq 4/3$. Then independently Margulis [21, 22, 23] and Lubotsky, Phillips, and Sarnak [24] came up with similar examples of graphs (graphs $X^{p,q}$) with $\gamma \geq 4/3$ and arbitrary large valency (they turned out to be, additionally, so-called Ramanujan graphs). In [4] Biggs and Boshier showed that that γ is asymptotically $4/3$ for graphs from [21, 22, 23]. The graphs $X^{p,q}$ are Cayley graphs of the group $PSL_2(Z_q)$ with respect to a set of $p+1$ generators (p and q are primes congruent to 1 mod4).

The problem of estimation of order of cages is dual to problem on the maximal size of graphs on girth g.

Let $v(k, C_{2n}$ be the minimal order of k-regular graph without cycles of the length $2n$.The problem to evaluate $v(k, C_{2n})$ is dual to famous problem on the maximal size of the graph on v vertices without even cycles C_{2n} by Erdø"s' (see [8]). AS it follows from definitions

$v(k, C_{2n}) \leq v(k, 2n+1)$ and $v(k, C_{2n}) \leq v(k, 2n+2)$. The construction of graphs $L(n, q)$ and $B(n, q)$ implies the following result (the best known upper bounds on $v(k, C_{4n})$.

Theorem 2.1 *Let $k \geq 2$ and $g \geq 5$ be integers, and let q denote the smallest prime power for which $k < q$, let b be the smallest power of 2 for which $k \leq q$.*

Then the following upper bounds hold

$$v(k, C_{4n}) \leq (k+1)q^{(3/4)n-2} \tag{2}$$

$$v(k, C_{4n}) \leq kb^{(3/4)n-2} \tag{3}$$

It is clear, that for some very special k the bound (3) is better then (2).

By Chebyshev's Theorem for a fixed integer $k \geq 3$ there is always a prime between k and $2k-2$. For any $e \geq 0$ and $k > k_0(e)$, this interval can be narrowed to $[k, k + k^{2/3+e}]$, see [24], p.131.

The best known bound for $v(k, 2n)$, n is odd, follows from the bound on $v(k, 2n)$ ([17]):

Let $k \geq 2$ and $g \geq 5$ be integers, and let q denote the smallest odd prime power for which $k \leq q$. Then

$$v(k, g) \leq 2kq^{(3/4)g-\alpha} \tag{4}$$

where $\alpha = 4, 11/4, 7/2, 13/4$ for $g = 0, 1, 2, 3 \bmod 4$, respectively.

It is clear that bound (2) on $v(k, C_{4n})$ is always better then (4).

3 Graphs with special walks and Cryptography

Graphs of large girth are applied tools in Networking (see [1]), other application is Cryptography (see [32], [34], [35] for theoretical studies and [36], [37], [38] [39] for the computer implementation.

The general idea of such a graph theoretical approach is considering the set of vertices as the plainspace and the pass in the graph as an encryption tool (password). In case of the graph of girth g distinct passes of length s, $s \leq [(g-1)/2]$ starting from given vertex produce different verices-ciphertexts. In the case of parallelotopic graphs ([32], [34]) or Cayley graphs we have a nice parametrisation of walks and passes by strings over some alphabet (set of colours for parallelotopic graphs and set of generators for Cayley graphs). In case of (k, g)-graphs and encryption by passes of length s, $s \leq (g-1)/2$ the size of the key-space is $k(k-1)^{s-1}$, the vertex-plaintext and the vertex ciphertext are joint by the unique pass. It means that if adversary has access only to encrypted communications, he or she can use only brut-force search to recover plaintext. The encryption by walks on the graph has a certain resistance in other situation when adversary knows several pairs (plaintext-ciphertext) and trying to get the password for the control of communication channel. Such resistance is increasing with the grows of the girth (see [34], [35]). Thus families of (k, g)-graphs of increasing girth, especially parallelotopic graphs or Cayley graphs, are valuable tools for the encryption. If such graphs form the family of graphs of large girth we have the following theoretical advantage: size of the key space is comparable with the size of the plainspace.

The advantage of families $D(n,q)$, $CD(n,q)$ and new graphs related to dynamical systems $L_n(F_q)$, $B_n(F_q)$ in comparison with Cayley graphs $X(p,q)$ is the possibility to work with the "potentially infinite" plaintext as a string over the fixed alphabet F_q like in the case of affine encryption or real block ciphers DES, AES, NEST and many others (see [27] or [12]). In the encryption process via graphs $X(p,q)$ we need change the size of the alphabet F_q with the grows of the information volume because of the dimension of the plainspace $PSL_n(q)$ over F_q is constant.

Affine encryption is used not only for finite field F_q but in the case of general commutative rings (see unit "Enciphering matrices" in the Koblitz book [11]). The idea to investigate girth of graphs related to invertible dynamical systems over rings with zero divisors is natural but difficult one. Instead of girth investigation we can justify existence of many pairs of vertices joint by the unique pass. More precisely, we can consider pairs $(v, u = F_{\alpha_1}(F_{\alpha_2} \dots (F_{\alpha_k}(v)) \dots)$, where v is arbitrary vertex of the graph related to invertible dynamical system F_x of level k over commutative ring K, $\alpha_i + \alpha_{i+1}$ are regular elements of K. We can treat v as a plaintext, u as a ciphertext, string $(\alpha_1, \alpha_2, \dots, \alpha_k)$ as a password and the transformation $G = F_{\alpha_1} \dots \times F_{\alpha_k}$ as encryption rule.

The idea to combine such symmetric encryption N via graphs with two affine transformation A and B over K or its proper subring (use ANB) for the public key encryption (for the case of integrity rings see [36]).

Combination of encryption base on families of graphs $D_n(K)$, $C_n(K)$, $L(n,K)$, $B(n,K)$ with appropriate affine transformations A and B can be useful also in symmetric mode algorithms. Such an encryption schemes are not block ciphers, change of one character in the plaintext leeds to change of entire ciphertext, not just one block of it.

Important to notice that choice $K = Z_{2^n}$ instead of $K = F_{2^n}$ leads to essential speed up of the encryption because of multiplication of numbers are faster than multiplication of polynomials, but the key space remains to be rather large: zero divisors are odd classes and strings of alternating even and odd classes are appropriate passwords.

4 Transformation groups of incidence structures defined over commutative rings

We need the following well known results on groups acting on graphs.

Let G be a group with proper distinct subgroups G_1 and G_2. Let us

consider the incidence structure with the point set $P = (G : G_1)$ and the line set $(G : G_2)$ and incidence relation $I : \alpha I \beta$ if and only if the set theoretical intersection of cosets α and β is nonempty set. We shall not distinguish the incidence relation and corresponding graph $\Gamma(G)_{G_1,G_2}$.

Lemma 4.1 *Graph I is connected if and only if $< G_1, G_2 >= G$.*

Let $A =< a_1, \ldots, a_n | R_1(a_1, \ldots, a_n), \ldots, R_d(a_1, \ldots, a_n) >$ and
$B =< b_1, \ldots b_m | S_1(b_1, \ldots b_m), \ldots, S_t(b_1, \ldots, b_m) >$ are subgroups with generators a_i, $i = 1, \ldots, n$ and b_j, $j = 1, \ldots, m$ and generic relations R_i, $i = 1, \ldots, d$ and S_j, $j = 1, \ldots, t$, respectively. Free product $F = A * B$ of A and B be the subgroup $< a_1, \ldots, a_n, b_1, \ldots, b_m | R_1, \ldots R_d, S_1, \ldots, S_t >$ (see [20]).

The definition of an operation of free product F_H of groups A and B amalgamated at common subgroup H can be found in [20]. If $H =< e >$, then $F_H = A * B$.

Theorem 4.2 *(see, for instance [20]) Let G acts edge transitively but not vertex transitively on a tree T. Then G is the free product of the stabilizers G_a and G_b of adjacent vertices a and b amalgamated at their intersection.*

Corollary 4.3 *Let G acts edge regularly on the tree T, i. e. $|G_a \cap G_b| = 1$. Then G is the free product $G_a * G_b$ of groups G_a and G_b.*

We define the family of graphs $D(k, K)$, where $k > 2$ is positive integer and K is a commutative ring, such graphs have been considered in [15] for the case $K = F_q$ (some examples are in [14]).

let P and L be two copies of Cartesian power K^N, where K is the commutative ring and N is the set of positive integer numbers. Elements of P will be called *points* and those of L *lines*.

To distinguish points from lines we use parentheses and brackets: If $x \in V$, then $(x) \in P$ and $[x] \in L$. It will also be advantageous to adopt the notation for co-ordinates of points and lines introduced in [15] for the case of general commutative ring K:

$$(p) = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \ldots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \ldots),$$

$$[l] = [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l'_{2,2}, l_{2,3}, \ldots, l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,i}, \ldots].$$

The elements of P and L can be thought as infinite ordered tuples of elements from K, such that only finite number of components are different from zero.

We now define an incidence structure (P, L, I) as follows. We say the point (p) is incident with the line $[l]$, and we write $(p)I[l]$, if the following relations between their co-ordinates hold:

$$\begin{aligned} l_{i,i} - p_{i,i} &= l_{1,0}p_{i-1,i} \\ l'_{i,i} - p'_{i,i} &= l_{i,i-1}p_{0,1} \\ l_{i,i+1} - p_{i,i+1} &= l_{i,i}p_{0,1} \\ l_{i+1,i} - p_{i+1,i} &= l_{1,0}p'_{i,i} \end{aligned} \tag{6}$$

(This four relations are defined for $i \geq 1$, $p_{1,1} = p_{1,1}, l`_{1,1} = l_{1,1)}$). This incidence structure (P, L, I) we denote as $D(K)$. We speak now of the *incidence graph* of (P, L, I), which has the vertex set $P \cup L$ and edge set consisting of all pairs $\{(p), [l]\}$ for which $(p)I[l]$.

For each positive integer $k \geq 2$ we obtain an incidence structure (P_k, L_k, I_k) as follows. First, P_k and L_k are obtained from P and L, respectively, by simply projecting each vector onto its k initial coordinates. The incidence I_k is then defined by imposing the first $k-1$ incidence relations and ignoring all others. The incidence graph corresponding to the structure (P_k, L_k, I_k) is denoted by $D(k, K)$.

To facilitate notation in future results, it will be convenient for us to define $p_{-1,0} = l_{0,-1} = p_{1,0} = l_{0,1} = 0$, $p_{0,0} = l_{0,0} = -1$, $p'_{0,0} = l'_{0,0} = -1$, and to assume that (6) are defined for $i \geq 0$.

Notice that for $i = 0$, the four conditions (6) are satisfied by every point and line, and, for $i = 1$, the first two equations coincide and give $l_{1,1} - p_{1,1} = l_{1,0}p_{0,1}$.

The incidence relation motivated by the linear interpretation of Lie geometries in terms their Lie algebras [31] (see [33]). Let us define the "root subgroups" U_α, where the "root" α belongs to the root system Root $= \{(10), (01), (11), (12), (21), (22), (22)' \ldots, (i, i), (ii)', (i, i{+}1), (i{+}1, i) \ldots\}$. Group U_α generated by the following "root transformations" $t_\alpha(x)$, $x \in K$ of the $\mathrm{P} \cup \mathrm{L}$:

1) $\mathrm{l}^{t_{1,0}(x)} = [l_{1,0} + x, l_{1,1}, l_{2,1} - l_{1,1}x, l_{1,2}, l_{2,2}, \ldots, l'_{s,s} + l_{s-1,s}x, l_{s+1,s} + l_{s,s}x, l_{s,s+1}, l_{s+1,s+1}, \ldots]$;

1') $\mathrm{p}^{t_{1,0}(x)} = (p_{0,1}, p_{1,1} - p_{0,1}x, p_{2,1} - 2p_{1,1} + p_{0,1}x^2, p_{1,2}, p_{2,2} + p_{1,2}x, \ldots, p_{s+1,s} - (p_{s,s} + p'_{s,s})x + p_{s-1,s}x^2, p_{s,s+1}, p_{s+1,s+1} - p_{s,s+1}x, \ldots)$

2) $\mathrm{l}^{t_{0,1}(x)} = [l_{1,0}, l_{1,1} + l_{1,0}x, l_{1,2} + 2l_{1,1}x + l_{1,0}x^2, l_{2,1}, l_{2,2} + l_{2,1}x, \ldots, l'_{s,s} + l_{s,s-1}x, l_{s,s+1} + (l_{s,s} + l'_{s,s})x + l_{s,s-1}x^2, l_(s + 1, s, l_{s,s} + l_{s,s-1}x, \ldots$

2') $(\mathrm{p})^{t_{0,1}(x)} = (p_{0,1} + x, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, \ldots)$

3) $\mathrm{l}^{t_{1,1}(x)} = [l_{1,0}, l_{1,1} + x, l_{1,2}, l_{2,1} + l_{1,0}x, l_{2,2} - l_{1,1}x, l'_{2,2} + l_{1,1}x, \ldots, l_{s,s} - l_{s-1,s-1}x, l'_{s,s} + l_{s-1,s-1}x, l_{s,s+1} - l_{s-1,s}x, l_{s+1,s} + l_{s,s-1}x, \ldots]$

3') $\mathrm{p}^{t_{1,1}(x)} = (p_{0,1}, p_{1,1}+x, p_{1,2}-p_{0,1}x, p_{2,1}, p_{2,2}-p_{2,1}x, \ldots, p_{s,s}-p_{s-1,s-1}x, p'_{s,s}-p'_{s-1,s-1}x, p_{s,s+1} - p_{s-1,s}, p_{s+1,s} + p_{s,s-1}x, \ldots$

The transformations $t_{m+1,m}(x)$, m ≥ 1 acts on the coordinates of l and p by the following rules.

(a) $l_{m+1,m} \to l_{m,m+1} + x$, $p_{m,m+1} \to p_{m,m+1} + x$.

(b) $l'_{m+1,m+1} \to l'_{m+1,m+1}$,

$p'_{m+1,m+1} \to p'_{m+1,m+1} + p_{0,1}x$

(c) $l'_{m+r,m+r} \to l'_{m+r,m+r} - l_{r-1,r}x$, $p'_{m+r,m+r} \to p'_{m+r,m+r} - p_{r-1,r}x$, $r \geq 2$.

(d) $l_{m+r+1,m+r} \to l_{m+r+1,m+r} - l_{r,r}x$, $pm+r+1, m+r \to p_{m+r+1,m+r} - p_{r,r}x$, $r \geq 2$.

(e) All other components are unchanged.

The transformation $t_{m,m+1}(x)$, $m \geq 1$ is defined by following rules.

(a)$l_{m,m+1} \to l_{m,m+1} + x$, $p_{m_m+1} \to p_{m,m+1} + x$.

(b) $l_{m+1,m+2} \to l_{m+1,m+2} + l_{1,1}x$, $p_{m+1,m+2} \to p_{m+1,m+2} + p_{1,1}x$.

(c) $l_{m+1,m+1} \to l_{m+1,m+1} + l_{1,0}x$.

(d) $l_{m+r,m+r+1} \to l_{m+r,m+r+1} + l'_{r,r}x$, $r \geq 2$.

(e) All other components are unchanged.

The transformation $t'_{m,m}(x)$ acts on vertices of $D(K)$ by the following rules.

(a) $l'_{m,m} \to l'_{m,m} + x$, $p'_{m,m} \to p'_{m,m} + x$.

(b) $l_{m+1,m} \to l_{m+1,m} + l_{1,0}x$.

(c) $l_{m+1,m+1} \to l_{m+1,m+1} + l_{1,1}x$, $p_{m+1,m+1} \to l_{m+1,m+1} + p_{1,1}x$

(d) $l_{m+r,m+r} \to l_{m+r,m+r} + l'_{r,r}x$, $p_{m+r,m+r} \to p_{m+r,m+r} + p'_{r,r}x$, $r \geq 2$.

(e) $l_{m+r+1,m+r} \to l_{m+r+1,m+r} + l_{r+1,r}x$, $p_{m+r+1,m+r} \to p_{m+r+1,m+r} + p_{r+1,r}x$, $r \geq 2$.

(f) All other components are unchanged.

The transformation $t_{m,m}(x), m \geq 1$ act on coordinates of vertices by the following rules.

(a) $l_{m,m} \to l_{m,m} + x$, $p_{m,m} \to p_{m,m} + x$.

(b) $p_{m,m+1} \to p_{m,m+1} - p_{0,1}x$.

(c) $l_{m+r,m+r} \to l_{m+r,m+r} - l_{r,r}x$, $p_{m+r,m+r} \to p_{m+r,m+r} - p_{r,r}x$, $r \geq 1$.

(d) All other components are unchanged.

Note that action of each transformation above on the n-s component of a vertex from $P \cup L$ depends only from this component itself and previous

components. Thus we can define a natural projection of this transformation onto the graph $\mathrm{D}(n, K)$.

Proposition 4.4 (i)*For each pair* (α, x), $\alpha \in$ Root, $x \in K$ *the transformation* $t_\alpha(x)$ *are automorphisms of* $D(K)$. *The projections of these maps onto the graph* $D(n, K)$, $n \geq 2$ *are elements of* $Aut(D(n, K))$.

(ii) *Group* $\mathrm{U}(K)$ *acts edge regularly on the vertices of* $\mathrm{D}(K)$.

(iii) *Group* $\mathrm{U}(n, K)$ *generated by projections of* $t_\alpha(x)$ *onto the set of vertices* V *of* $\mathrm{D}(n, K)$ *acts edge regularly on* V.

Proof:

Statement (i) follows directly from the definitions of incidence and closed formulas of root transformations $t_\alpha(x)$. Let $<$ be the natural lexicographical linear order on roots of kind (i, j), where $|i-j| \leq 1$. Let us assume additionally that $(i, i) < (i, i)' < (i, i+1)$. Then by application of transformations $t_\alpha(x_\alpha)$, $\alpha \neq (0, 1)$ to a point (p) consecutively with respect to the above order, where parameter x_α is chosen to make α component of the image equals zero, we are moving point (p) to zero point (0). A neighbour $[a, 0, \ldots, 0]$ of the zero point can be shifted to the line $[0]$ by the transformation $t_{(1,0)}(-a)$. Thus each pair of incident elements can be shifted to $((0), [0])$ and group U acts edge regularly on vertices of $D(K)$. This action is regular $((ii))$ because the stabilizer of the edge $(0), [0]$ is trivial. Same arguments about the action of $U(n, K)$ justify (iii).

•

Lemma 4.5 *Let* ϕ_a *be a binary relation : "difference of colours of the same type is a". Then group* U $(U(n, K))$ *preserves* ϕ_a.

Proof:

Transformations t_α , $\alpha \neq (0, 1), (1, 0)$ preserves colours of vertices. Maps $t_{(0,1)}(x)$ and $t_{(1,0)}(x)$ preserve the binary relation ϕ_a for each $a \in K$.

•

Let $k \geq 6$, $t = [(k+2)/4]$, and let $u = (u_\alpha, u_{11}, \cdots, u_{tt}, u'_{tt}, u_{t,t+1}, u_{t+1,t}, \cdots)$ be a vertex of $\mathrm{D}(k, K)$ ($\alpha \in \{(1, 0), (0, 1)\}$, it does not matter whether u is a point or a line). For every r, $2 \leq r \leq t$, let

$a_r = a_r(u) = \sum_{i=0,r} (u_{ii} u'_{r-i,r-i} - u_{i,i+1} u_{r-i,r-i-1})$,

and $a = a(u) = (a_2, a_3, \cdots, a_t)$.

Proposition 4.6 *(i) The classes of equivalence relation* $\tau = \{(u,v)|a(u) = a(v)\}$ *form the imprimitivity system of permutation groups* $\mathrm{U}(K)$ *and* $\mathrm{U}(n,K)$

(ii) For any $t-1$ *ring elements* $x_i \in K$*),* $2 \leq t \geq [(k+2)/4]$*, there exists a vertex* v *of* $\mathrm{D}(k,K)$ *for which*

$a(v) = (x_2, \ldots, x_t) = (x)$.

(iii) The equivalence class C *for the equivalence relation* τ *on the set* $K^n \cup K^n$ *is isomorphic to the affine variety* $K^t \cup K^t$ *,* $t = [4/3n] + 1$ *for* $n = 0, 2, 3 \bmod 4$*,* $t = [4/3n] + 2$ *for* $n = 1 \bmod 4$*.*

Proof:

Let C be the equivalence class on τ on the vertex set $\mathrm{D}(K)$ ($\mathrm{D}(n,K)$ then the induced subgraph, with the vertex set C is the union of several connected components of $\mathrm{D}(K)$ ($\mathrm{D}(n,K)$).

Without loss of generality we may assume that for the vertex v of $C(n,K)$ satisfying $a_2(v) = 0, \ldots a_t(v) = 0$. We can find the values components $v'_{i,i)}$ from this system of equations and eliminate them. Thus we can identify P and L with elements of K^t, where $t = [3/4n] + 1$ for $n = 0, 2, 3 \bmod 4$, and $t = [3/4n] + 2$ for $n = 1 \bmod 4$.

•

We shall use notation $C(t,K)$ ($C(K)$) for the induced subgraph of $D(n,K)$ with the vertex set C.

Remark.

If $K = F_q$, q is odd, then the graph $C(t,k)$ coincides with the connected component $CD(n,q)$ of the graph $D(n,q)$ (see [18]), graph $C(F_q)$ is a q-regular tree. In other cases the question on the connectedness of $C(t,K)$ is open. It is clear that $g(C(t,F_q))$ is $\geq 2[2t/3] + 4$.

We define an incidence structure with point set P' and line set L'. It will be convenient for us to denote vectors from P' as

x $= (x) = (x_{0,1}, x_{1,1}, x_{1,2}, x_{2,2}, \ldots x_{i,i}, x_{i,i+1} \ldots,)$ and vectors from L' as y $= [y_{1,0}, y_{1,1}, y_{1,2}, y_{2,2}, \ldots, y_{i,i}, y_{i,i+1}, \ldots]$.

We say that point (x) is incident with the line $[y]$ and we write it xJy or (x)J$[y]$ if and only if the following condition are satisfied:

$$y_{i,i} - x_{ii} = x_{i-1,i} y_{1,0}$$

$$y_{i,i+1} - x_{i,i+1} = x_{1,0} y_{i,i}$$

where $i = 1, 2, \ldots$.

Let $\mathrm{E}(K)$ be the incidence graph of the incidence graph of the incidence structure $\Gamma(K) = (P', L', J')$. For each integer $k \geq 2$ let $\Gamma(k,q) =$

$(P'(k), L'(k), J(k))$ be the incidence system, where $P(k)$ and $L(k)$ are images of P and L under the projection of these spaces on the first k -coordinates and binary relation $J(k)$ is defined by the first k equations. Finally, let E(k, K) be the incidence graph for $\Gamma(k, K)$.

Similarly we can define an incidence structure $E'(K)$ with points of kind (x) = $(x_{0,1}, x_{1,1}, x_{2,1}, \ldots, x'_{i,i}, x_{i+1,i}, \ldots)$, $i \geq 2$, lines of kind [y] = $[y_{1,0}, y_{1,1}, y_{2,1}, \ldots y'_{i,i}, y_{i+1,i}, \ldots]$ and the incidence relation given by equations

$$y'_{i,i} - x'_{i,i} = y_{i,i-1}x_{1,0}$$

$$y_{i+1,i} - x_{i+1,i} = y_{1,0}x'_{i,i}.$$

By projections of the point space and the line space on the first k components we get the quotient graph $E'(n, K)$. It is easy to see that graphs $E(K)$ and $E'(K)$ ($E(n, K)$ and $E'(n, K)$) are isomorphic.

Let G be the graph with the colouring $\rho : V(G) \to C$ of the set of vertices $V(G)$ into colours from C such that the neighbourhood of each vertex looks like rainbow, i.e. consists of $|C|$ vertices of different colours. In case of pair (G, ρ) we shall refer to G as *parallelotopic graph* with the local projection ρ (see [36] and further references).

It is obvious that parallelotopic graphs are k-regular with $k = |C|$. Linguistic graphs are just bipartite parallelotopic graphs of order $2q^t$ and degree $q = p^s$ where p is a prime number.

If C' is a subset of C, then induced subgraph $G^{C'}$ of G which consists of all vertices with colours from C' is also a parallelotopic graph. It is clear that connected component of the parallelotopic graph is also a parallelotopic graph.

The *arc* of the graph G is a sequence of vertices $v_1, \ldots, v_k$ such that $v_i I v_{i+1}$ for $i = 1, \ldots, k-1$ and $v_i \neq v_{i+2}$ for $i = 1, \ldots, k-2$. If $v_1, \ldots, v_k$ is an arc of the parallelotopic graph (G, ρ) then $\rho(v_i) \neq \rho(v_{i+2})$ for $i = 1, \ldots, k-2$.

The *trail* of the graph G is the sequence of vertices $v_1, \ldots, v_k$, such that $\mathrm{v}_i \neq v_{i+1}$, $i = 1, \ldots, k-1$ and $v_1 = v_k$.

If (G_1, ρ_1) and (G_2, ρ_2) be two parallelotopic graphs over the same set of colours. We say that graph homomorphism $\phi : G_1 \to G_2$ is a parallelotopic morphism if $\rho_1(v) = \rho_2(\phi(v))$ for each vertex v of the graph G_1.

Parallelotopic morphism moves arc of the graph G_1 into the arc of graph G_2.

Examples. Let $\Gamma = \Gamma_k(K)$ be one graph among the graphs $D(k, K)$, $CD(k, K)$ and $E(k, K)$. Γ with the colouring $\rho([\mathrm{x}]) = x_1$, $\rho((\mathrm{x})) = \mathrm{x}_1$ is a parallelotopic graph. If $K = F_q$, then it is q-regular bipartite graph with $2q^k$

vertices. The map η_s of deleting the s last components of the tuple-vertex (point or line) of $\Gamma_{k+s}(q)$ is a parallelotopic morphism onto $\Gamma_k(q)$.

Let ϕ be a map of deleting of coordinates with indices $(i, i+1)$, $(i,i)'$ for vertices of $D(K)$ (or $CD((K))$. Then ϕ is a parallelotopic morphism onto the graph $E(K)$. It is preserves not only colours but all components $x_\alpha, \alpha \in$ Root$'$, where Root$'$ contains exactly $(1,0),(0,1),(i,i),(i,i+1)$, $i = 1, \ldots$.

We can consider the map ϕ_n (ϕ'_n)on the set of vertices of the graph $D(n,K)$. The image of this parallelotopic morphism belongs to the family $E(k,K)$ ($E'(k,K)$, respectively).

Let $U_\alpha =< t_\alpha(x) | x \in K >$ be a subgroup of $U(K)$. It is isomorphic to the additive group K^+ of the ring K. Let U^C be subgroup generated by $t_\alpha(x)$, $x \in K$, $\alpha \in \{(0,1,(1,0),\ldots,(i,i),(i,i+1),\ldots\}$. Let ${U_n}^C$ be the subgroup generated by transformations $t_\alpha(x)$ from U^C onto the graph $D(n,K)$ (or $C(n,K)$).

(i) The connected component $CD(n,K)$ of the graph $D(n,K)$ (or its induced subgraph $C(t,K)$) is isomorphic to $\Gamma(U_n)^C)_{U_{(0,1)},U_{(1,0)}}$.

(ii) Projective limit of graphs $D(n,K)$ (graphs $C(t,K)$, $CD(n,K)$) with respect to paralletopic morphisms of $D(n+1,K)$ onto $D(n,K)$ (their restrictions on induced subgraphs) equals to $D(K)$ ($C(K)$, $CD(K) = {U^C}_{U_{(0,1)},U_{(1,0)}}$, respectively).

Remark. Let $v_1, v_2, \ldots v_k$ be the pass in the parallelotopic graph G, then it is uniquely determined by the starting point v_1 of the colour c_1 and the sequence of colours $c_2, \ldots c_k$ of colours of vertices $v_2, \ldots, v_k$, respectively. We have $c_i \neq c_{i+2}$, for $i = 1, \ldots, k-2$.

The following statement can be proven by straightforward induction on n.

Lemma 4.7 *(two numbers lemma)*

Let $[\mathrm{y}_1]I(\mathrm{y}_2)I \ldots I\mathrm{y}_n$ *be the pass in the graph* $E(n,K)$, $n \geq 4$ *starting from the zero point* ($\mathrm{y}_1 = 0$) *defined by the sequence of colours* $0, x_1, x_2, \ldots x_{n-1}$.

Then two last components of the vertex y_n *are* $\alpha = x_1x_2(x_1 - x_3)\ldots(x_{n-3} - x_{n-1})$, *and* $\beta = -x_{n-2}\alpha$.

Theorem 4.8 *Let* $N_x(\mathrm{v})$ *be the operator of taking the neighbour of the vertex* $\mathrm{v} = (v_1, v_2, \ldots, v_s)$ *of the colour* $v_1 + x$ *in the graph* $D(n,K)$.

Then operator it defines an arithmetical dynamic system $D_n(K)$ *on* $K^n \cup K^n$ *of level* $d = [(n+5)/2] - 1$.

Proof:

Let us consider the action of operator $F_d = N_{t_1} N_{t_2} \dots N_{t_d}$, where $t_i + t_{i+2}$ are regular elements of K, on the vertex u.

Consecutive applications of N_{t_i} produce the walk

$\mathrm{u} = \mathrm{u}_0, \mathrm{u}_1 = N_{t_1}(u_0), \dots, \mathrm{u}_d = N_{t_d}(u_{d-1})$, where the difference of colours for elements u_i and u_{i+2} is $t_i + t_{i+1}$. The group $U(n, K)$ acts transitively on the vertex set of $D(n, K)$ and preserves difference of colours for elements of same type. Thus without loss of generality we may assume that u is zero point.

We can apply map ϕ_n (or ϕ'_n) to u_d and compute the common for u_d and its image component α via two numbers lemma. It is product of regular elements and one nonzero element. Thus it differs from zero. Let us assume that $F'_s(\mathrm{u}) = N_{t'_1} \dots N_{t'_s}(\mathrm{u}) = F_d(\mathrm{u})$. Without loss of generality we may assume that $t'_i \neq t'_{i+1}$, $i = 1, \dots, s-1$. If $s \leq d$, the component with number α for $F(\mathrm{u}) = 0$ according to the 2 numbers lemma and we are getting a contradiction. So $s = d$ and consecutive execution of transformation $N_{t'_i}, (i = 1, \dots, d)$ produces the walk $\mathrm{u}'_1, \dots \mathrm{u}'_d$. Let $t_1 \neq t'_1$. Then we can apply operator $t_{0,1}(-t')$ to each element u_i, u'_i, $i = 1, \dots, d$ and get elements v_i, v'_i, $i = 1, \dots, d$, respectively. Conditions $\mathrm{u}_d = \mathrm{u}'_d$ and $\mathrm{v}_d = \mathrm{v}'_d$ are equivalent.

According to two numbers lemma component α of v'_d equals zero but same component of v_d is not a product of regular and nonzero elements. Thus $t_1 = t'_1$. Application of same argument to the sequence $\mathrm{u}_i, \dots \mathrm{u}_d$, $i = 1, \dots, d-1$ gives us $t_i = t'_i$ for $i = 2, \dots d$.

•

Operator N_x preserves connected components of $D(n, K)$ and blocks of equivalence relation τ.

Corollary 4.9 *Let $N'_x(v)$, $t \in K$ be the operator of taking the neighbour of the vertex* v *of the colour $v_1 + x$ in the graph $C(t, K)$, which is the restriction of operator $N_x(v)$ on the equivalence class C. Then it defines arithmetical dynamic system $C_t(K)$ on $K^t \cup K^t$ over $Q = K$ of rank $d = [2/3t] + 1$.*

If K is an integrity domain, then $D(K)$ and $CD(K)$ are forests. Let C be the connected component, i.e tree.

Group U^C acts regularly on $CD(K)$. So we can apply theorem on group acting regular on the tree and get the following statement.

Proposition 4.10 *If K is integrity domain then group $U^C(K)$ is isomorphic to the free product of two copies of K^+.*

5 Polarities of incidence structures and related dynamical systems

Let P and L be disjoint sets, the elements of which we call *points* and *lines*, respectively. A subset I of $P \times L$ is called an *incidence relation* on the pair (P, L). The *incidence graph* Γ of geometry (P, L, I) is defined to be the bipartite graph with vertex set $P \cup L$ and edge set $\{\{p, l\} | p \in P, l \in L, (p, l) \in L\}$.

Let $\pi : P \cup L \to P \cup L$ be a bijection for which the following hold

(1) $P^\pi = L$ and $L^\pi = P$,

(ii) for all $p \in P$, $l \in L$ (l^π,p$^\pi$) $\in I$ if and only if $(p, l) \in I$,

(iii) $\pi^2 = 1$.

We call such π a polarity of the incidence structure (P, L, I). Note that π induces an order two automorphism of the incidence graph Γ which interchanges the bipartition sets P and L. We shall use the term "polarity" and the notation "π" for the graph automorphism as well.

We now define the polarity graph Γ^π of the structure (P, L, I) with respect to polarity π. It is the graph with the vertex set $V(\Gamma^\pi) = P$ and edge set $E(\Gamma^\pi) = \{\{p_1, p_2\}\} | p_1, p_2 \in P, p_1 \neq p_2, (p_1, {p_2}^\pi) \in I\}$.

Finally, we call point $p \in P$ an *absolute point* of the polarity π provided (p, p^π) in I.

Let N_π denote the number of absolute points of π.

Proposition 5.1 *(see, for instance [18])*

Let π be be a polarity of the finite incidence structure (P, L, I) and let Γ and Γ^π be the correspondent incidence and polarity graphs.

*(*a*)* $\deg_{\Gamma^\pi} = \deg_{\Gamma^\pi} - 1$ *if p is an absolute point of π, and* $\deg_{\Gamma\pi} = \deg_\Gamma$ *otherwise.*

*(*b*)* $|V(\Gamma)^\pi| = 1/2|V(\Gamma)|$, $|E(\Gamma^\pi)| = |E(\Gamma)| - N_\pi$,

*(*c*) If Γ^π contains a $(2k+1)$-cycle then Γ contains a $(4k+2)$ cycle.*

*(*d*) If Γ^π contains a $2k$-cycle then Γ contains two vertex disjoint $2k$ cycles C and C' such that $C^\pi = C'$. Consequently, if Γ is $2k$-cycle-free then so is Γ^π.*

*(*e*) The girth of the two graphs are related by $g(\Gamma^\pi) \geq 1/2 g(\Gamma)$.*

It is clear that statements (c) , (d) and (e) are valid for an infinite incidence structure with polarities.

Let us consider the case of the incidence structure with paralleloopic graph (Γ, ρ) with the polarity π which is the parallelotopic morphism. We

call such π a *parallelotopic polarity*. In that case we can define the *regular folding graph* $\mathrm{R}\Gamma = \mathrm{R}(\Gamma^\pi) = \{(p.p')|\rho(p) \neq \rho(p'), (p,p') \in E(\Gamma^\pi)\}$.

Let us consider the case when the set B of colours of the absolute points is a proper subset of the set of all colours C. In that case we can define an induced subgraph $\mathrm{I}\Gamma = \mathrm{I}\Gamma^\pi$ with the set of vertices $\{v \in \Gamma^\pi | \rho(v) \in C - B\}$ Directly from the definitions and above proposition we are getting the following statement.

Lemma 5.2 *Let P, L, I be the incidence structure with the k-regular parallelotopic incidence graph Γ and parallelotopic polarity $\pi : \Gamma \to C$. Then $\mathrm{R}(\Gamma^\pi)$ is $k-1$-regular graph of girth g, where $g \geq g(\Gamma^\pi) \geq g(\Gamma)$.*

If the set B of colours for absolute points of π is different from C, then $\mathrm{I}\Gamma$ is $|C-B|$-regular graph and $g(\mathrm{I}\Gamma)) \geq g(\Gamma^\pi) \geq g(\Gamma)$.

Remark *1:*

Graph $\mathrm{I}\Gamma$ is a parallelotopic graph. Let S be a finite proper subset of $C-B$ of cardinality s. Then the graph $\mathrm{I}\Gamma^S$ has valency s and $g(\mathrm{I}\Gamma^S) \geq g(\mathrm{I}\Gamma)$.

Remark *2:*

Graph $R\Gamma$ is not a parallelotopic graph because of sets of colours from tne neighbourhoods differs from vertex to vertex. Let S, $|S| = s$ be a subset of the colour set C of the parallelotopic graph Γ. Then parallelotopic polarity π induces a parallelotopic polarity π of $R\Gamma^S$. The graph $\mathrm{R}\Gamma^S$ shall be a graph of valency $s-1$ and $g(\mathrm{R}\Gamma^S) \geq g(\Gamma^S) \geq g(\Gamma)$.

Proposition 5.3 *The map π given by the close formula*

$\mathrm{p}^\pi = [p_{10}, -p_{11}, p_{21}, p_{12}, -p'_{22}, -p_{22}, \ldots, -p'_{ii}, -p_{ii}, p_{i+1,i}, p_{i,i+1}, \ldots]$,

$\mathrm{l}^\pi = (l_{01}, -l_{11}, l_{21}, l_{12}, -l'_{22}, -l_{22}, \ldots, -l'_{ii}, -l_{ii}, l_{i+1,i}, l_{i,i+1}, \cdots)$

is a parallelotopic polarity of $D(n,K)$. It preserves blocks of the equivalence relation τ. It is restriction on $V(\mathrm{CD}(n,K))$ is a parallelotopic polarity of $\mathrm{CD}(n,K)$.

Let $L(n,K)$ be regular folding graph corresponding to the parallelotopic polarity π induced on the vertices of the graph $C(n,K)$. In case of $\mathrm{char}K = 2$ the colours of absolute points of the polarity graph of $C(n,K)$ corresponding to the polarity π form the set $B = \{x|x^2 = 0\}$. Thus colours of the vertices of $B(n,K)$ are elements of $K - B$.

Directly from the fact $g(D(n,F_q)) \geq 2[(n+5)/2]$, proposition 6.1 and lemma 6.2 we are getting

Proposition 5.4 *(i) The girth of the graph $L(n,F_q) = L(n,q)$ and $B(n,F_q) = B(n,q)$, q is even is, at least $2[(n+5)/2]$. They are regular graphs of degrees $q-1$ and q^t with q^t and $(q-1)q^{t-1)}$ vertices , respectively.*

(ii) For each q they form a families of graphs of large girth with the $\gamma = 2/3\log_{q-1}(q)$.

(3i) Let S be a subset of nonzero elements of F_q, $|S| = s$ then $L(n, F_q)^S$ and $B(n, F_q)^S$ (q is even) are graphs of the order sq^{t-1}, girth $\geq 2[(n+5)/2]$ and degrees $s-1$ and s, respectively.

Theorem 2.1 follows directly from the statement (3i) of the Proposition 5.4.

The proposition 5.4 can be obtained alternatively as the corollary of the two following theorems.

Theorem 5.5 *(i) Let $N_x(v)$, $x \in \{K-0\}$ be the operator of taking the neighbour of the vertex $v \in V(\mathrm{RC}(t,K)) = K^t$, of colour $v_{1,0}+x$, then it defines the linguistic dynamical system $L_t(K)$ on K^t, $t \geq 2$ of level $d = [2/3t]+1$ and rank $r \geq [1/3t]$*

(ii) Let $\mathrm{char}K = 2$, B is the set of roots for the equation $x^2 = 0$, $N_x(v)$, $x + \rho(v) \neq y$, $y \in B$ be the operator of taking the neighbour of $v \in V(\mathrm{IC}(n,K)) = (K-B) \times K^{t-1}$ of the colour $v_{1,0}+x$, then it defines an arithmetical dynamic system $B_n(K)$ of level $d = [2/3t]+1$ and rank $r = [1/3t]+1$.

Proof:

Let $G(K)$ be one of the systems $L_n(K)$, $B_n(K)$. Let us consider the action of operator $F_d = N_{t_1}N_{t_2}\dots N_{t_d}$, where $t_i + t_{i+2}$ are regular elements of K, on the vertex u.

Consecutive applications of N_{t_i} produce the walk

$\mathrm{u} = \mathrm{u}_0, \mathrm{u}_1 = N_{t_1}(\mathrm{u}_0), \dots, \mathrm{u}_d = N_{t_d}(\mathrm{u}_{d-1})$*, where the difference of colours for elements u_i and u_{i+2} is $t_i + t_{i+1}$. Let us consider the -dynamic equation- $F_s(\mathrm{u}) = F_d(\mathrm{u})$, where*

$F_s(\mathrm{u}) = N_{t'_1}\dots N_{t'_s}(\mathrm{u}) = F_d(\mathrm{u})$*. Without loss of generality we may assume that $t'_i \neq t'_{i+1}$, $i = 1, \dots, s-1$.*

Consecutive execution of transformation $N_{t'_i}$, $i = 1, \dots, s$ produces the walk $\mathrm{u}'_1, \dots, \mathrm{u}'_s$. So we are getting -the dynamical trail-: $u_0, \dots u_d, u'_{s-1}, \dots, u'_1$, where u'_1 is adjacent to u_0. We can consider elements of the trail as points in $D(n,K)$. Then $u_0, \pi(u_1), u_2, \pi(u_3), \dots$ is a dynamical trail in $D(n,K)$ corresponding to the same dynamical equation. But the only trail in $D(n,K)$ can be related to the sequence of colours $x, x+t_1, x+t_1+t_2, \dots x+t_1+\dots t_d, x+t_1+\dots t_{d-1}, x+t_1$, where x is the colour of u*. Thus $s = d$, tuple $(t_1, \dots, t_d)^* = (t'_1, \dots t'_d)$ and $G(K)$ is an invertible dynamical system of level d.*

Let us investigate possible odd cycles in the graph. If $N_{t_s} \dots N_{t_1}(x) = x$ *and* $p_l = N_{t_{l-1}}$, $l = 2, \dots, 2k = 1$. *Then* $p_1, (p_2)^\pi, \dots, p_{2k+1}, (p_1)^\pi \dots (p_{2k+1})^\pi$ *are consecutive verices of a (4k+2)-cycle in the bipartite graph. Half of this cycle has colours from the regular string.*

•

It is clear that theorems 2.1 is direct corollary of theorem 5.5.

References

*[1] F. Bien,*Constructions of telephone networks by group representations), Notices Amer. Mah. Soc., 36 (1989), 5-22.

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

[3] N.L. Biggs, *Graphs with large girth*, Ars Combinatoria, 25C (1988), 73–80.

[4] N.L. Biggs and A.G. Boshier, *Note on the Girth of Ramanujan Graphs*, Journal of Combinatorial Theory, Series **B 49**, pp. 190–194 (1990).

[5] N.L. Biggs and M.J. Hoare, *The sextet construction for cubic graphs*, Combinatorica **3** (1983), 153–165.

[6] B. Bollobás, *Extremal Graph Theory*, Academic Press, London, 1978.

[7] B. Bollobás, *Random Graphs*, Academic Press, London, 1985.

[8] J. A. Bondy and M. Simonovits, *Cycles of even length in graphs*, J. Combinatorial Theory (B), **16** (1974), pp. 97–105.

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

[10] P. Erdös' and H. Sachs, *Regulare Graphen gegebener Taillenweite mit minimaler Krotenzahl, Wiss. Z. Univ. Halle Martin Luther, Univ. Halle-Wittenberg, Math. Natur. Reine 12 (1963), 251-257.*

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

[12] N. Koblitz, Algebraic aspects of Cryptography, in Algorithms and Computations in Mathematics, v. 3, Springer, 1998.

[13] W. Imrich, Explicit construction of graphs without small cycles*, Combinatorica* **2** *(1984) 53–59.*

[14] F. Lazebnik, V. A. Ustimenko, New Examples of graphs without small cycles and of large size*, Europ. J. of Combinatorics, 14 (1993) 445-460.*

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

[16] 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.*

[17] Lazebnik, F., Ustimenko, V.A. and A.J. Woldar, New upper bounds on the order of cages*, Electronic J. Combin. 14 R13 (1997), 1–11.*

[18] F. Lazebnik, V. A. Ustimenko, A. Woldar, Polarities and $2k$-cycle-free graphs*, Discrete Mathematics, 197/198 (1999), 503-513.*

[19] A. Lubotsky, R. Philips, P. Sarnak, Ramanujan graphs*, J. Comb. Theory., 115, N 2., (1989), 62-89.*

[20] W. Magnus, A. Karrass, D. Solitar, Combinatorial group theory*, Interscience publ., 1966.*

[21] G. A. Margulis, Explicit construction of graphs without short cycles and low density codes*, Combinatorica, 2, (1982), 71-78.*

[22] G. Margulis, Explicit group-theoretical constructions of combinatorial schemes and their application to desighn of expanders and concentrators*, Probl. Peredachi Informatsii., 24, N1, 51-60. English translation publ. Journal of Problems of Information transmission (1988), 39-46.*

[23] M. Margulis, Arithmetic groups and graphs without short cycles*, 6th Intern. Symp. on Information Theory, Tashkent, abstracts, vol. 1, 1984, pp. 123-125 (in Russion).*

[24] H. L. Montgomery, Topics in Multiplicative Number Theory*, Lecture Notes in Mathematics 227, Springer Verlag, New York, 1971.*

[25] H. Sachs, Regular graphs with given girth and restricted circuits*, J. London. Math. Soc. 38 (1963), 423-429.*

[26] N. Sauer. Extermaleigenschaften regularer Graphen gegebener Taillenweite*, 1, 2, Osterreich. Acad. Wiss. Math. Natur. Kl. S. -B 2, 176 (1967), 9-25, 27-43.*

[27] J. Seberry, J. Pieprzyk, Cryptography: An Introducion to Computer Security*, Prentice Hall 1989, 379 p.*

[28] M. Simonovitz, Extermal Graph Theory *, In "Selected Topics in Graph Theory", 2, edited by L. W. Beineke and R. J. Wilson, Academic Press, London, 1983, pp. 161-200.*

[29] J.Spencer, The strange logic of random graphs*, Springer Verlag, 2001.*

[30] W. Tutte, A family of cubical graphs*, Proc. Cambridge Philos. Soc. 43 (1945).*

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

[32] V. A. Ustimenko, Coordinatisation of regular tree and its quotients*, in "Voronoi's impact on modern science, eds P. Engel and H. Syta, book 2, National Acad. of Sci, Institute of Matematics, 1998, 228p.*

[33] V. A. Ustimenko, On the varieties of parabolic subgroups, their generalizations and combinatorial applications*, Acta Applicandae Mathematicae, 52 (1998), 223-238.*

[34] V. Ustimenko, Graphs with Special Arcs and Cryptography*, Acta Applicandae Mathematicae, 2002, vol. 74, N2, 117-153.*

[35] V. Ustimenko, CRYPTIM: Graphs as tools for symmetric encryption*, In Lecture Notes in Comput. Sci., 2227, Springer, New York, 2001.*

[36] V. Ustimenko, Maximality of affine group and hidden graph cryptsystems*, Journal of Algebra and Discrete Mathematics, October, 2004.*

[37] V. A. Ustimenko, D. Sharma, CRYPTIM: system to encrypt text and image data*, Proceedings of International ICSC Congress on Intelligent Systems 2000, Wollongong, 2001, 11pp.*

[38] V. Ustimenko, A. Touzene, CRYPTALL:system to encrypt all types of data*, Notices of Kiev-Mohyla Academy, v 23, June , 2004, pp. 12-15.*

[39] Yu. Khmelevsky , V. A. Ustimenko, Practical aspects of the Informational Systems reengineering*, The South Pacific Journal of Natural Science, volume 21, 2003, www.usp.ac.fj(spjns).*

[40] H.Walther, Eigenschaften von regularen Graphen gegebener Taillenweite und Minimaler Knotzenzahl, Wiss. Z. Illmenau 11 (1965), 167-168.

[41] H. Walther, *Uber regulare Graphen gegebener Taillenweite und minimaler Knotenzahl*, Wiss. Z. Techn Hochsch. Ilmenau 11 (1965), 93-96.

[42] A. L. Weiss, *Girth of bipartite sextet graphs*, Combinatorika 4 (2-3) 1984, 241-245.