On graphs of large size without small cycles and commutative diagrams and their applications

Vasyl Ustimenko

Institute of Mathematics
Maria Curie-Skłodowska University in Lublin, Poland

The 6th International workshop on Optimal Network Topologies

Recall that a girth is the length of a minimal cycle in a simple graph. Studies of maximal size $ex(C_3, C_4, \ldots, C_{2m}, v)$ of the simple graph on v vertices without cycles of length $3, 4, \ldots, 2m$, i. e. graphs of girth $> 2m$, form an important direction of Extremal Graph Theory.

As it follows from the famous Even Circuit Theorem by P. Erdős' we have inequality

$$ex(C_3, C_4, \ldots, C_{2m}, v) \leq cv^{1+1/n},$$

where c is a certain constant.

The bound is known to be sharp only for $n = 4, 6, 10$. The first general lower bounds of kind $ex(v, C_3, C_4, \ldots C_n) = \Omega(v^{1+c/n})$, where c is some constant $< 1/2$ were obtained in the 50th by Erdős' via studies of **families of graphs of large girth**, i.e. infinite families of simple regular graphs Γ_i of degree k_i and order v_i such that $g(\Gamma_i) \geq c\log_{k_i} v_i$, where c is the independent of i constant. Erdős' proved the existence of such a family with arbitrary large but bounded degree $k_i = k$ with $c = 1/4$ by his famous probabilistic method.

Only two explicit families of regular simple graphs of large girth with unbounded girth and arbitrarily large k are known: the family $X(p,q)$ of Cayley graphs for $PSL_2(p)$, where p and q are primes, had been defined by G. Margulis [12] and investigated by A. Lubotzky, Sarnak [13] and Phillips and the family of algebraic graphs $CD(n,q)$ [14]. Graphs $CD(n,q)$ appears as connected components of graphs $D(n,q)$ defined via system of quadratic equations. The best known lower bound for $d \neq 2,3,5$ had been deduced from the existence of above mentioned families of graphs $ex(v, C_3, C_4, \ldots, C_{2d}) \geq cv^{1+2/(3d-3+e)}$ where $e = 0$ if d is odd, and $e = 1$ if d is even.

Recall, that family of regular graphs Γ_i of degree k_i and increasing order v_i is a **family of graphs of small world** if $\mathrm{diam}(\Gamma_i) \leq c\log_{k_i}(v_i)$ for some independent constant c, $c > 0$, where $\mathrm{diam}(\Gamma_i)$ is diameter of graph G_i. The graphs $X(p.q)$ form a unique known family of large girth which is a family of small world graphs at the same time. There is a conjecture known from 1995 that the family of graphs $CD(n, q)$ for odd q is another example of such kind. Currently. it is proven that the diameter of $CD(n, q)$ is bounded from above by polynomial function $d(n)$, which does not dependent from q.

Expanding properties of $X(p,q)$ and $D(n,q)$ can be used in Coding Theory (magnifiers, super concentrators, etc). The absence of short cycles and high girth property of both families can be used for the construction of LDPC codes [15]. This class of error correcting codes is an important tool of security for satellite communications. The usage of $CD(n,q)$ as Tanner graphs producing LDPC codes lead to better properties of corresponding codes in the comparison to usage of Cayley - Ramanujan graphs $X(p,q)$(see [16]).

Both families $X(p,q)$ and $CD(n,q)$ consist of edge transitive graphs. Their expansion properties and the property to be graphs of a large girth hold also for random graphs, which have no automorphisms at all. To make better deterministic approximation of random graph we can look at regular expanding graphs of a large girth without edge transitive automorphism group.

We consider below optimisation problem for simple graphs which is similar to a problem of finding maximal size for a graph on v vertices with the girth $\geq d$.

Let us refer to the minimal length of a cycle, through the vertex of given vertex of the simple graph Γ as *cycle indicator of the vertex*. The **cycle indicator of the graph** $\mathrm{Cind}(\Gamma)$ will be defined as the maximal cycle indicator of its vertices. Regular graph will be called **cycle irregular graph** if its indicator differs from the girth (the length of the minimal cycle). The solution of the optimization problem of computation of the maximal size $e = e(v, d)$ of the graph of order v with the size greater than d, $d > 2$ has been found very recently.

It turns out that

$$e(v, d) \Leftrightarrow O(v^{1+[2/d]})$$

and this bound is always sharp (see [17] or [18] and further references).

We refer to the family of regular simple graphs Γ_i of degree k_i and order v_i as the **family of graphs of large cycle indicator**, if

$$\mathrm{Cind}(\Gamma_i) \geq c\log_{k_i}(v_i)$$

for some independent constant c, $c > 0$. We refer to the maximal value of c satisfying the above inequality as **speed of growth** of the cycle indicator for the family of graphs Γ_i. As it follows from the written above evaluation of $e(v, d)$ the speed of growth of the cycle indicator for the family of graphs of constant but arbitrarily large degree is bounded above by 2.

We refer to such a family as a *family of cyclically irregular graphs of large cycle indicator* if almost all graphs from the family are cycle irregular graphs.

THEOREM 1

There is a family of cyclically irregular graphs of large cycle indicator with the speed of cycle indicator 2, which is a family of graphs of small word graphs.

The explicit construction of the family $A(n, q)$ like in previous statement is given in [17], [18]. Notice, that members of the family of cyclically irregular graphs are not edge transitive graphs. The LDPC codes related to new families are presented in [19], computer simulations demonstrate essential advantages of the new codes in comparison to those related to $CD(n, q)$ and $D(n, q)$.

Graphs $D(n,q)$ and $CD(n,q)$ have been used in symmetric cryptography together with their natural analogs $D(n,K)$ and $CD(n,K)$ over general finite commutative rings K since 1998 (see [6]). The theory of directed graphs and language of dynamical system were very useful for studies of public key and private key algorithms based on graphs $D(n,K)$, $CD(n,K)$ and $A(n,K)$ (see [21], [23], [20], [25] and further references).

There are several implementations of symmetric algorithms for cases of fields (starting from [7]) and arithmetical rings ([22], in particular). Some comparison of public keys based on $D(n,K)$ and $A(n,K)$ are considered in [24].

The missing theoretical definitions on directed graphs the reader can find in [16].

Let ϕ be an irreflexive binary relation over set M, i.e. ϕ be a subset of $M \times M$ which does not contain elements of kind (x, x). We write $x \to y$ or $x\phi y$ for $(x, y) \in \phi$ and identify binary relation ϕ with the corresponding **directed graph** or shortly **digraph**. The **pass of a digraph** is a sequence $x_0 \to x_1 \to x_2 \to \cdots \to x_s$. We refer to a parameter s as the **length of the pass.**

We refer to a pair of passes $x_0 \to x_1 \to x_2 \cdots \to x_s$ and $y_0 \to y_1 \to y_2 \to \cdots \to y_r$ of length s as **commutative diagram** $O_{s,r}$ if $x_0 = y_0$, $x_s = y_r$, and $x_i \neq y_j$ for $0 < i < s$ and $0 < j < r$.

We refer to the parameter $\max(r, s)$ as the **rank** of $O_{s,r}$. Notice that the digraph may have a **directed cycle** $O_s = O_{s,0}$: $v_0 \to v_1 \to \dots v_{s-1} \to v_0$, where v_i, $i = 0, 1, \dots, s-1$, $s \geq 2$ are distinct vertices.

We will count directed cycles as **commutative diagrams**.

We refer to a digraph as a **diagram free one** if it does not contain digraph of rank ≥ 2.

We use term **balanced digraph** for the digraph Γ corresponding to irreflexive binary relation ϕ over finite set V such that for each $v \in V$ sets $\{x|(x, v) \in \phi\}$ and $\{x|(v, x) \in \phi\}$ have the same cardinality.

We say that balanced digraph Γ is k-**regular** if for each vertex $v \in \Gamma$ the cardinality of $\{x|(v, x) \in \phi\}$ is k.

Notice that each k-regular simple forest is a diagram free digraph. A simplest examples of diagram free digraph which is not simple graph is a balanced digraph of degree 1:

$$\ldots x_{-2} \to x_{-1} \to x_{-0} \to x_1 \to x_{-} \ldots .$$

As it follows instantly from definitions a diagram free k-regular balanced digraph for $k \geq 2$ is an infinite one.

For the investigation of commutative diagrams we introduce **girth indicator** gi, which is the minimal value for the rank of commutative diagram $O_{s,t}$, $s + t \geq 3$. Notice that two vertices v and u at distance $< \mathrm{gi}$ are connected by unique pass from u to v of length $< \mathrm{gi}$.

In case of symmetric binary relation $\mathrm{gi} = d$ implies that the girth of the graph is $2d$ or $2d-1$. It does not contain even cycle $2d-2$. In general case $\mathrm{gi} = d$ implies that $g \geq d+1$. So in the case of family of graphs with unbounded girth indicator, the girth is also unbounded. We also have $\mathrm{gi} \geq g/2$.

We assume that the **girth** $g(\Gamma)$ of directed graph Γ with the girth indicator $d+1$ is $2d+1$ if it contains commutative diagram $O_{d+1,d}$. If there are no such diagrams we assume that $g(\Gamma)$ is $2d+2$.

In the case of symmetric irreflexive relations the above mentioned general definition of the girth agrees with the standard definition of the girth of simple graph, i.e the length of its minimal cycle.

We will use the term *family of graphs of large girth* for the family of balanced directed regular graphs Γ_i of degree k_i and order v_i such that $\mathrm{gi}(\Gamma_i)$ is $\geq c\log_{k_i} v_i$, where c' is the independent of i constant.

As it follows from the definition $g(\Gamma_i) \geq c'\log_{k_i}(v_i)$ for appropriate constant c'. So, it agrees with the well known definition for the case of simple graphs.

We refer to a **family of balanced directed graphs as a family of graphs of increasing girth** if $\mathrm{gi}(\Gamma_i)$ is unbounded function in variable i and $\mathrm{gi}(\Gamma_i) \leq \mathrm{gi}(\Gamma_{i+1})$ for every i.

The **diameter** is the maximal length d of the minimal shortest directed pass $a = x_0 \to x_1 \to x_2 \cdots \to x_d$ between two vertices a and b of the directed graph. Digraph of finite diameter is called **a strongly connected one**.

Recall that balanced digraph is k-**regular**, if each vertex of G has exactly k outputs. Let G be the infinite family of finite k_i regular digraphs G_i of order v_i and diameter d_i.

We say, that F is a **family of small world graphs** if $d_i \leq C\log_{k_i}(v_i)$, $i = 1, 2, \ldots$ for some independent on i constant C. The definition of small world simple graphs and related explicit constructions the reader can find in [3]. For the studies of small world simple graphs without small cycles see [9], [20] and [33].

Let us refer to the minimal girth indicator, through the vertex of the directed balanced Γ as **diagram indicator of the vertex**. The **diagram indicator of the graph** $\mathrm{Dind}(\Gamma)$ will be defined as the maximal diagram indicator of its vertices. We refer to the family of regular balanced digraphs Γ_i of degree k_i and order v_i as the **family of digraphs with large diagram indicator**, if $\mathrm{Dind}(\Gamma_i) \geq c\log_{k_i}(v_i)$ for some independent constant c, $c > 0$.

Let F be a list of directed graphs and P be some graph theoretical property. By $\mathrm{Ex}_P(v, F)$ we denote the greatest number of arrows of F-free directed graph on v vertices satisfying property P (graph without subgraphs isomorphic to graph from F). We will omit the index P in this section if P is just a property to be a balanced directed graph.

The maximal size $\mathrm{E}(d, v)$ (number of arrows) of the balanced binary relation graphs with the girth indicator $> d$ coincides with $\mathrm{Ex}(v, O_{s,t}, s + t \geq 2 \leq s \leq d)$.

Let $\mathrm{Ex}^{2d+1}(v))$ be the maximal size of the balanced directed graph of girth $> 2d + 1$, then this number coincide with $\mathrm{Ex}(v, O_{d+1,d}, O_{s,t} \geq 3. \leq s \leq d)$.

The following analogue of (1.1) has been stated in [23].

THEOREM 2

$$E(d, v) <=> v^{1+1/d} \tag{2.1}$$

The proof of this statement the reader can find in [23]. The analogue of this statements for graphs, such that number of outputs for each vertex is the same, has been formulated in [25].

Remark 1. Let $E_P(d, v)$ be the maximal size (number of arrows) for the balanced graph on v vertices with the girth indicator $> d$ satisfying the graph theoretical property P. If P is the property to be a graph of symmetric irreflexive relation then $E_P(d, v) = 2\mathrm{ex}(v, C_3, \ldots, C_{2d-1}, C_{2d})$ because undirected edge of the simple graph corresponds to two arrows of symmetric balanced directed graph. So the bound (1.5) implies the inequality (1.2).

Remark 2. The precise computation of $E(d, v)$ does not provide the sharpness of (1.2). So the questions on the sharpness of (1.1) and (1,2) up to magnitude for $n \neq 3, 4$ and 5 are still open and the lower bound (1.5) is still the best known.

Remark 3 Balanced digraph Γ be extremal graph of order v with the girth indicator gi with maximal possible $E(d, v)$ if and only if girth of the graph equals $2d + 1$.

The above Theorem is analogue of bound (1.2) for balanced directed graphs. The following analogue of (1.1) was introduced also in lecture notes [34].

THEOREM 3

$$\mathrm{Ex}^{2d+1}(v) <=> (1/2)^{1/d} v^{1+1/d} \tag{2.2}$$

Remarks

(i) Let $E_P^{2d+1}(v)$ be the maximal size (number of arrows) for the balanced graph on v vertices with the girth $> 2d+1$ satisfying the graph theoretical property P. If P is the property to be a graph of symmetric irreflexive relation, then $E_P^{2d+1}(v) = 2\mathrm{ex}(v, C_3, \ldots, C_{2d}, C_{2d+1})$ because undirected edge of the simple graph corresponds to two arrows of symmetric balanced directed graph. So, Theorem 2.1 implies the inequality (1.1).

(ii) The sharpness of the bound (1.1) does not follow from the above mentioned theorem. The function $\mathrm{ex}(v, C_3, \ldots, C_{2d}, C_{2d+1})$ is computed up to the magnitude for $d = 2, 3, 5$.

(iii) Balanced digraph Γ be extremal graph of order v with the girth indicator gi with maximal possible $Ex(2d+1, v)$ if and only if girth of the graph equals $2d+2$.

We consider a family $\Gamma(K)$ of simple bipartite graphs $\Gamma(K)$ of the incidence structure with the point set

$$P = \{(x_1, x_2, \dots, x_n, \dots) | x_i \in K, i = 1, 2, \dots\} = K^{\infty},$$

the line set

$$L = \{[y_1, y_2, \dots, y_n, \dots] | y_i \in K, i = 1, 2, \dots\} = K^{\infty}$$

and incidence relation I such that $(\mathrm{x}) = (x_1, \dots, x_n, \dots)$ and $[\mathrm{y}] = [y_1, \dots, y_n, \dots]$ are incident if and only if

$$\begin{aligned} x_2 - y_2 &= x_1 y_1, \\ x_i - y_i &= x_1 y_{s(i)} e_i + y_1 x_{s(i)}(1 - e_i), \quad i = 2, 3, \dots, \end{aligned}$$

where $e_i \in \{0, 1\}$, integer function $s(i)$ satisfies inequality $s(i) < i$.

Let $\rho((\mathrm{x})) = x_1$ and $\rho([\mathrm{y}]) = y_1$ be the colour of the point and colour of the line, respectively. As it follows from definition every vertex has exactly one neighbour of given color (paralelotopic property or rainbow like property). So, if K is a finite ring and $|K| = k$ then $\Gamma(K)$ is a k-regular simple bipartite graph.

We refer to defined above simple graph $\Gamma(K)$ as a **bivariate graph** over commutative ring K.

Let $F = \{\{p, l\} | (p, l) \in P \times L | p\ I\ l\}$ a be the sets of flags of incidence structure P, L, I.

We say that two flags are adjacent if their intersection has cardinality one.

Let us assume that $\Gamma(K)$ be a family of bivariate graphs over a general ring K (or incidence structure). Assume that $F(K)$ is the corresponding set of flags. Notice, that $F(K)$ is a variety isomorphic to K^{∞}. For a flag $\{p, l\}$ we consider adjacent flag $NP_{\alpha}(\{p, l\})$, $\alpha \neq 0$ which consist on the line l and point p' of colour $\rho(p) + \alpha$ which is incident to l.

Similarly, we introduce the flag $NL_{\alpha}(\{p, l\})$, which is adjacent to $\{p, l\}$ and contains the line l' of colour $\rho(l) + \alpha$.

Let us consider two copies $F_1(K)$ and $F_2(K)$ of the flag set $F(K)$ We say that a subset S of commutative ring K is a multiplicative one if zero does not belong to S and the subset is closed under multiplication.

For every multiplicative subset S of K we introduce a digraph $D_S(K)$ with a vertex set $F_1(K) \cup F_2(K)$, such that $a \to b$ means $a \in F_1(K)$ and $b = NP_\alpha(a)$ for some $\alpha \in S$ or $a \in F_2(K)$ and $b = NL_\alpha(a)$, $\alpha \in S$.

We refer to $\Gamma(K)$ as **bivariate free graph** over K if for every multiplicative subset S of K a digraph $D_S(\Gamma(K))$ is a diagram free one.

Notice, that if K is a field that bivariate free graph $\Gamma(K)$ is a simple forest.

If graph $\Gamma(K)$ is a bivariate free graph for each commutative ring K we say that family $\Gamma(K)$ is a tree approximation. Notice, that tree approximation has been defined as functor from the category of pairs K, S to the category of directed graphs.

PROPOSITION 1.

Let $\Gamma(K)$ be bivariate graph. Then the transformations of kind $NP_{\alpha_1}NL\alpha_2NP_{\alpha_3}NL\alpha_4\ldots NP_{\alpha_{2k-1}}NL\alpha_{2k}$ and $NL_{\alpha_1}NP\alpha_2NL_{\alpha_3}NP\alpha_4\ldots NL_{\alpha_{2k-1}}NP\alpha_{2k}$, where α_i are elements of some multiplicative subset of K, are bijective transformations of K^{∞} of infinite order.

The existence of tree approximation has been proved (graphs $D(n, K)$).

Let $\Gamma(K)$ be bivariate graph. Let us consider simple graph $\Gamma_n(K)$ defined in the following way. It is bipartite graph of the incidence structure P_n, L_n, I_n with the pointset $P_n = K^n = \{\mathrm{x} = (x_1, x_2, \ldots, x_n) | x_i \in K\}$ and line set $L_n = K^n = \{\mathrm{y} = [y_1, y_2, \ldots, y_n] | y_i \in K\}$ and Incidence relation I_n such that $(x_1, x_2, \ldots, x_n) I_n [y_1, y_2, \ldots, y_n]$ if and only if first $n-1$ relation of $*$ hold.

We consider a graph homomorphism ψ_n of $\Gamma(K)$ onto $\Gamma_n(K)$ which acts on vertices (x) and $[\mathrm{y}]$ by deleting of coordinates x_i and y_i with $i \geq n+1$. We have also a well defined natural homomorphism $\psi(n, n-1) : \Gamma_n(K) \to \Gamma_{n-1}(K)$, $n \geq 3$. which acts by deleting of last coordinates of points and lines. So, the natural projective limit of $\Gamma_n(K)$ is well defined. It is coincides with $\Gamma(K)$. Notice, that the maps ψ_n and $\psi(n, n-1)$ are local isomorphisms, they induce homomorphism from $D_S(\Gamma(K))$ onto $D_S(\Gamma_n(K))$ and from $D_S(\Gamma_n(K))$ onto $D_S(\Gamma_{n-1}(K))$, respectively.

We assume, that $\rho((x_1, x_2, \ldots, x_n)) = x_1$ and
$\rho([y_1, y_2, \ldots, y_n] = y_1$
We say that a subset S of commutative ring K is a multiplicative set of generators if its multiplicative closure is a multiplicative subset of the ring K.

PROPOSITION

Let $\Gamma(K)$ be a free bivariate graph. For each multiplicative set of generators S digraphs $D_S(\Gamma_n(K))$ form a family of increasing girth.

COROLLARY

For each finite field F graphs $\Gamma_n(F)$ form a family of simple graphs of increasing girth.

THEOREM 1

There is a tree approximation $\Gamma(K)$, such that

(i) for every finite commutative ring R and every multiplicative subset S of cardinality ≥ 2 digraphs $D_S(\Gamma_n(K))$ form a family of digraphs of large girth

(ii) for each finite field F_q, $q > 2$ simple graphs $\Gamma_n(F_q)$ form a family of graphs of large girth.

The tree approximation of theorem 1 can be defined explicitly as projective limit $D(K)$ of graphs $D(n, K)$, $n \to \infty$, where K is a general commutative ring.

THEOREM 2

There is a tree approximation $\Gamma(K)$, such that

(i) for every finite commutative ring R and each subset S of multiplicative generators of cardinality ≥ 2 digraphs $D_S(\Gamma_n(K))$ form a family of digraphs with large diagram indicator

(ii) for every field F_q, $q \neq 2$ and graphs $\Gamma_n(F))$ form a family of algebraic small world graphs which is also a family of graphs with large cycle indicator

(iii) for each finite field F_q, $q > 2$ simple graphs $\Gamma_n(F_q)$ form a family of simple small world graphs.

The tree approximation of theorem 2 can be defined explicitly as projective limit $A(K)$ of graphs $A(n, K)$, $n \to \infty$, where K is a general commutative ring.

Let $\Gamma_n(K)$ be a family of graphs associated with bivariate free graph $\Gamma(K)$. Then the transformations of kind $NP_{\alpha_1}NL_{\alpha_2}NP_{\alpha_3}NL_{\alpha_4}\dots NP_{\alpha_{2k-1}}NL_{\alpha_{2k}}$ and $NL_{\alpha_1}NP_{\alpha_2}NL_{\alpha_3}NP_{\alpha_4}\dots NL_{\alpha_{2k-1}}NP_{\alpha_{2k}}$, where α_i are elements of some multiplicative subset of K, , where α_i are elements of some multiplicative subset of K, are bijective transformations of K^{n+1} of increasing order.

(A) We can identify K^{n+1} with the plaintext and consider $E = NP_{\alpha_1}NL_{\alpha_2}NP_{\alpha_3}NL_{\alpha_4}\dots NP_{\alpha_{2k-1}}NL_{\alpha_{2k}}$ as encryption map corresponding to password $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \dots, \alpha_{2k-1}, \alpha_{2k})$.
So, we are getting private key symmetric algorithms. In case of bivariate graphs of Theorem 1 and Theorem 2 we are getting stream ciphers

(B) We proved that multivariate transformations $E : K^{n+1} \to K^{n+1}$ independently on the choice of password are stable cubical maps. So they can be used as bases of Diffie Hellman algorithm in Cremona group. One can use a symbolic El Gamal version described above to get a cryptosystem.

(C) Transformation $E = NP_{\alpha_1} NL\alpha_2 NP_{\alpha_3} NL\alpha_4 \dots NP_{\alpha_{2k-1}} NL\alpha_{2k}$ is an example of polynomial transformation with invertible transposition. Really, ${NP_\alpha}^{-1} = NP_{-\alpha}$ and ${NL_\alpha}^{-1} = NL_{-\alpha}$. The problem of its usage for the public key is the following: the inverse of E is also cubical. It means that the adversary can conduct linearisation attacks to break the system.

To make a good candidate for the encryption map of multivariate cryptosystem we can use the following deformation of E
Let a point (x) and line $[\mathrm{y}]$ of colours x_1 and y_1 form an initial flag h. The computation of E can be computed recurrently
$h \to h_1 = NP_{\alpha_1}(h), h_2 = NL_{\alpha_2}, \dots h_{2k-1} = NP_{\alpha_{2k-1}}(h_{2k-2}), h_{2k} = NL_{\alpha_{2k}}(n_{2k-1})$.
We can modify map E in the following way.

Instead of $h_1 = NP_{\alpha_1}(h)$ we compute a flag $h'_1 = NP(a_1, \alpha_1, \beta_2, \gamma_1)$ adjacent to h such that colour of h' is $a_1 {x_1}^{\beta_1} {y_1}^{\gamma_1} + \alpha_1$. Instead of $h_2 = NL_{\alpha_2}(h_1)$ we compute $h'_2 = NL(a_2, \alpha_2, \beta_2, \gamma_2)(h'_1)$ which is adjacent to h'_1 and its colour of the line is $a_2 {x_1}^{\beta_2} {y_1}^{\gamma_2} + \alpha_2$.
Continue this process we get deformed map $\tilde{E}$ together with its decomposition into factors of kind $NP(a_{2i-1}, \alpha_{2i-1}, \beta_{2i-1}, \gamma_{2i-1})$ (the operator of computing adjacent flag with the colour of the point $a_{2i-1} {x_1}^{\beta}_{2i-1} {y_1}^{\gamma_{2i-1}} + \alpha_1 + \alpha_3 + \cdots + \alpha_{2i-1}$) and $NL(\alpha_{2i}, \beta_{2i}, \gamma_{2i})$ (the operator of computing adjacent flag with the colour of the point $a_{2i} {x_1}^{\beta_{2i}} {y_1}^{\gamma_{2i}} + \alpha_2 + \alpha_4 + \cdots + \alpha_{2i}$.

If the system of equations

$$a_{2i-1}x_1^{\beta_{2i-1}}y_1^{\gamma_{2i-1}} + \alpha_1 + \alpha_2 + \cdots + \alpha_{2i-1} = c_1$$

$$a_{2i}x_1^{\beta_{2i}}y_1^{\gamma_{2i}} + \alpha_2 + \alpha_4 + \cdots + \alpha_{2i} = c_2$$

with various c_1 and c_2 has at most one solution then $\tilde{E}$ is invertible. Our map has invertible decomposition.

THEOREM

Let us consider transformations $\tilde{E}_n$ and E_n acting on the set K^{n+1} of flags of $\Gamma_n(K)$. Then their order is going to infinity with the growth of n.

Both transformations have the same density which is $O(n^4)$.

This way allows us to construct a symmetric and asymmetric maps of polynomial degree $O(n^t)$. Notice that we can use integer parameters β, γ and k which are functions from n.
Finally, for the construction of public maps one can use compositions of kind $\tau_1\tilde{E}_n\tau_2$ where τ_1 are monomial linear transformation and τ_2 is general affine transformation.
Polynomial density of $\tau_1\tilde{E}_n\tau_2$ is $O(n^{t+1})$.

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

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

[3] P. Erdös', A. R'enyi and V. T. S'oc,
On a problem of graph theory,
Studia. Sci. Math. Hungar. 1 (1966), 215-235.

[4] P. Erdös', M. Simonovits,
Compactness results in extremal graph theory,
Combinatorica 2 (3), 1982, 275-288.

 [5] 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.

 [6] Ustimenko V.,
Coordinatisation of Trees and their Quotients,
In the "Voronoj's Impact on Modern Science", Kiev, Institute of Mathematics, 1998, vol. 2, 125-152.

 [7] Ustimenko V.,
CRYPTIM: Graphs as Tools for Symmetric Encryption,
Lecture Notes in Computer Science, Springer, v. 2227, 278-287 (2001)

 [8] Ustimenko V.,
Maximality of affine group and hidden graph cryptosystems
J. Algebra Discrete Math. -2005 ., No 1,-P. 133–150.

 [9] A. Wróblewska,
On some properties of graph based public keys,
Albanian Journal of Mathematics, Volume 2, Number 3, 2008, 229-234, NATO Advanced Studies Institute: "New challenges in digital communications".

 [10] V. Ustimenko, A. Wróblevska,
On some algebraic aspects of data security in cloud computing,
Proceedings of International conference "Applications of Computer Algebra", Malaga, 2013, p. 144-147.

 [11] U.Romańczuk, V. Ustimenko,
On regular forests given in terms of algebraic geometry, new families of expanding graphs with large girth and new multivariate cryptographical algorithms,
Proceedings of International conference "Applications of Computer Algebra", Malaga, 2013, p. 135-139.

 [12] 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.

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

 [14] 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.

 [15] P. Guinand, J. Lodge,
Tanner type codes arising from large girth graphs,
Canadian Workshop on Information Theory CWIT '97,
Toronto, Ontario, Canada (June 3-6 1997):5–7.

 [16] D. MacKay and M. Postol,
Weakness of Margulis and Ramanujan - Margulis Low Dencity Parity Check Codes,
Electronic Notes in Theoretical Computer Science, 74 (2003), 8pp.


[17]V. Ustimenko,
On some optimisation problems for graphs and multivariate cryptography (in Russian),
In Topics in Graph Theory: A tribute to A.A. and T. E. Zykova on the ocassion of A. A. Zykov birthday, pp 15-25, 2013, www.math.uiuc.edu/kostochka.


[18] Ustimenko V. A.
On extremal graph theory and symbolic computations,
Dopovidi National Academy of Sci of Ukraine, N2 (in Russian), 42-49 (2013)


[19] M. Polak, V. A. Ustimenko,
On LDPC Codes Corresponding to Infinite Family of Graphs A(n,K),
Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS), CANA, Wroclaw, September, 2012 , pp 11-23.

 [20] V. Ustimenko,
On the extremal graph theory for directed graphs and its cryptographical applications
In: T. Shaska, W.C. Huffman, D. Joener and V. Ustimenko, Advances in Coding Theory and Cryptography, Series on Coding and Cryptology, vol. 3, 181-200 (2007).

 [21]J. Kotorowicz, V. Ustimenko,
On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings,
Condenced Matters Physics, Special Issue: Proceedings of the international conferences "Infinite particle systems, Complex systems theory and its application", Kazimerz Dolny, Poland, 2006, 11 (no. 2(54)) (2008) 347–360.


[22]V. A. Ustimenko, U. Romańczuk,
On Extremal Graph Theory, Explicit Algebraic Constructions of Extremal Graphs and Corresponding Turing Encryption Machines,
in "Artificial Intelligence, Evolutionary Computing and Metaheuristics ", In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Vol. 427, Springer, January, 2013, 257-285.


[23] V. A. Ustimenko, U. Romańczuk,
On Dynamical Systems of Large Girth or Cycle Indicator and their applications to Multivariate Cryptography,
in "Artificial Intelligence, Evolutionary Computing and Metaheuristics ", In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Volume 427/January 2013, 257-285.


[24] M.Klisowski, V. A. Ustimenko,
On the Comparison of Cryptographical Properties of Two Different Families of Graphs with Large Cycle Indicator,
Mathematics in Computer Science, 2012, Volume 6, Number 2, Pages 181-198.


[25]V. A. Ustimenko,
On the cryptographical properties of extreme algebraic graphs,
in Algebraic Aspects of Digital Communications, IOS Press (Lectures of Advanced NATO Institute, NATOScience for Peace and Security Series - D: Information and Communication Security, Volume 24, July 2009, 296 pp.

Thank you for your attention!