ALBANIAN JOURNAL
OF MATHEMATICS
Volume 1, Number 4, Pages 283–295
ISSN 1930-1235: (2007)

ON THE EXTREMAL REGULAR DIRECTED GRAPHS WITHOUT COMMUTATIVE DIAGRAMS AND THEIR APPLICATIONS IN CODING THEORY AND CRYPTOGRAPHY

V. A. USTIMENKO

Abstract. We use term regular directed graph (r. d. g.) for the graph of irreflexive binary relation with the constant number outputs (or inputs) for each vertex. The paper is devoted to studies of maximal size $E_R(d,v)$ of r. d. g. of order v without commutative diagrams formed by two directed passes of length $< d$ with the common starting and ending points. We introduce the upper bound for $E_R(d,v)$, which is one of the analogs of well known Even Circuit Theorem by P. Erdös'. The Erdös' theorem establish the upper bound on maximal size of simple graphs without cycles of length $2n$. It is known to be sharp for the cases $n = 2, 3 and 5$ only. The situation with the upper bound for $E_d(v)$ is different: we prove that it is sharp for each $d \geq 2$. We introduce the girth of directed graph and establish tight upper and lower bounds on the order of directed cages, i.e. directed regular graphs of given girth and minimal order. The studies of regular directed graphs of large size (or small order) without small commutative diagrams, especially algebraic explicit constructions of them, are motivated by their applications to the design of turbo codes in Coding Theory and cryptographical algorithms. We introduce several new algebraic constructions of directed extremal graphs based on biregular generalized polygons, family of directed graphs of large girth with fixed degree.

1. Introduction

According to Bourbaki the graph (or directed graph) is the pair V (vertex set) and subset Φ in the Cartesian product $V \times V$ (see [24] for more general definitions). We refer to element $v \in V$ as vertex (state in automata theory).

We use term arc (or arrow as in automata theory) for the element $(a,b) \in \Phi$. We refer to $(a,b) \in \Phi$ as arc (arrow) from a to b, Element a and b are starting and ending vertex of the arc (a,b). We say that (a,b) is output of vertex a and b is input of b. As it follows from above definition graph has no multiple arcs. The cardinalities of V and Φ are the order and size of the graph, respectively.

Graph is simple if Φ is symmetric and anti-reflexive relation. The information about simple graph can be given by edge i. e. set of kind $\{a,b\}$, where (a,b) is an arc. Graphically simple graph has no loops and multiple edges. In case of simple graph term size used for the number of edges within the graph.

The classical extremal graph theory studies extremal properties of simple graphs. Let F be family of graphs none of which is isomorphic to a subgraph of the graph Γ. In this case we say that Γ is F-free. Let P be certain graph theoretical property.

Key words and phrases. directed cages, directed graphs of large girth, directed small world graphs, bounds on order of directed cages, turbo codes, graph based cryptography.

By $\mathrm{ex}_P(v,F)$ we denote the greatest number of edges of F-free graph on v-vertices, which satisfies property P. If P is just a property to be simple graph we omit index P and write $\mathrm{ex}(v,F)$. The missing definitions in extremal graph theory the reader can find in [3].

This theory contains several important results on $\mathrm{ex}(v,F)$, where F is a finite collection of cycles of different length [3], [25]. The following statement had been formulated by P. Erdös'.

Let C_n denote the cycle of length n. Then

$$\mathrm{ex}(v,C_{2k}) \le Cv^{1+1/k} \tag{1.1}$$

where C is independent positive constant. For the proof of this result and its generalizations see [5], [8]. In [7] the upper bound

$$\mathrm{ex}(v,C_3,C_4,\dots,C_{2k},C_{2k+1}) \le (1/2)^{1+1/k}v^{1+1/k} + O(V) \tag{1.2}$$

had been established for all integers $k \ge 1$.

Both bounds are known to be sharp for $k = 2,3,5$ in other cases the question on the sharpness is open (see [3], [1] and further references).

The girth of the simple graph is the minimal length of its cycle. So the above bound is the restriction on the size of the graph on v vertices of girth $\ge n$. Graphs of high girth, i.e. graphs which size is close to the above upper bounds can be used in Networking and Operation Research (see [3]) and Cryptography.

The generalizations (or analogs) of classical extremal graph theory on directed graphs require certain restrictions on inputs or outputs of the graph. Really, the graph DK_v: $P \cup L = V$, $P \cap L = \emptyset$, $|V| = v$, $\Phi = P \times L$ of order $O(v^2)$ has no directed cycles or commutative diagrams.

In [38] the above results on maximal size of the graphs generalized on the case of balanced graphs, when for each vertex $a \in V$ cardinalities of $\mathrm{id}(v) = \{x \in V | (a,x) \in \phi\}$ and $\mathrm{od}(v) = \{x \in V | (x,a) \in \phi\}$ are same. We refer to numbers $\mathrm{id}(v)$ and $\mathrm{od}(v)$ as input degree and output degree of vertex v in the graph, respectively.

Let Γ be directed graph. The *pass* between vertices a and b is the sequence $a = x_0 \to x_1 \to \dots x_s = b$ of length s, where x_i, $i = 0,1,\dots,s$ are distinct vertices. We refer to he minimal s among all passes between a and b as output distance $\mathrm{odist}(a,b)$. we assume $\mathrm{odist}(a,b) = \infty$ in case of absence of passes from a to b.

We say that the pair of passes $a = x_0 \to x_1 \to \dots \to x_s = b$, $s \ge 1$ and $a = y_0 \to y_1 \to \dots \to y_t = b$, $t \ge 1$ form an (s,t)- commutative diagram $O_{s,t}$ if $x_i \ne y_j$ for $0 < i < s$, $0 < j < t$. Without loss of generality we assume $s \ge t$ and refer to the number s as the rank of $O_{s,t}$. The directed cycle with s arrows we denote as $O'_{s,0}$. We will count directed cycles as commutative diagram.

The minimal parameter $s = \max(s,t)$ of the commutative diagram $O_{s,t}$ with $s + t \ge 3$ in the binary relation graph Γ we call the *girth indicator* of the Γ and denote it as $\mathrm{gi}(\Gamma)$. It can be infinity as in case of DK_v.

Notice that directed graph does not contain diagrams $O_{1,1}$, because there are no multiple edges.

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 it agrees with the standard definition of the girth of simple graph i.e the length of its minimal cycle.

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 to property P (graph without subgraphs isomorphic to graph from F).

Let $\mathrm{E}_P = \mathrm{E}_P(d,v) = \mathrm{Ex}_P(v, O_{s,t}, s+t \geq 3 | 2 \leq s \leq d)$ be the maximal size (number of arrows) of the balanced binary relation graphs with the girth indicator $> d$.

The main result of [38] is the following statement. If B be the property to be the balanced directed graph, then

$$v^{1+1/d} - O(v) \leq \mathrm{E}_B(d,v) \leq v^{1+1/d} + O(v) \tag{1.3}$$

Notice, that the size of symmetric irreflexive relation is the double of the size of corresponding simple graph. because undirected edge of the simple graph corresponds to two arrows (arcs) of $O_{2,0}$.

If P is the property to be a graph of symmetric irreflexive relation then

$$\mathrm{Ex}_P(v, O_{s,t}, s+t \geq 3 | 2 \leq s \leq d) = 2\mathrm{ex}(v, C_3, \ldots, C_{2d-1}, C_{2d}),$$

because undirected edge of the simple graph corresponds to two arrows of $O_{2,0}$. So equality (1, 3) implies the following inequality

$$\mathrm{ex}(v, C_3, C_4, \ldots, C_{2k}) \leq (1/2)v^{1+1/k} + O(V) \tag{1.4}$$

we evaluate the maximal size of the directed graph of order v with the girth indicator $> d$ which does not contain commutative diagrams $O_{d+1,d}$, as well. The inequality (1.2) is the corollary from such evaluation.

We can see that studies of extremal properties of balanced graphs with the high girth indicator and studies of $ex(v, C_3, \ldots, C_n)$ are far from being equivalent. Really, the sharpness of the Erdös' bound (1.1) and bounds (1.2) and (1.4) up to magnitude for $k = 8$ and $k \geq 12$ are old open questions (see [1], [3]) .

The regularity R of graph (V, Φ) means that either for each vertex $a \in V$ sets $\{x | (v,x) \in \Phi\}$ are same or for each $a \in V$ set $\{x | (x,v) \in \Phi\}$ are same. We will prove that substitution of property R instead of B leads to correct inequality:

$$v^{1+1/d} - O(v) \leq \mathrm{E}_R(d,v) \leq v^{1+1/d} + O(v) \tag{1.5}$$

The family of directed graphs G_i, $i = 1, \ldots$ with average output degree k_i and order is the family of large girth if the girth indicator of G_i is $\geq \log_{k_i}(v)$. It agrees well with the standard definition for the simple graphs. In case of balanced or regular graphs of large girth their size is close to the upper bounds (1. 3) and (1. 5). The following directions of applied data security are motivations of studies of extremal properties of regular or balanced graphs of large girth.

1.1. **LDPS and Turbo Codes and graphs of large girth.** Low-density parity-check (LDPC) codes were originally introduced in his doctoral thesis by Gallager in 1961 [11]. Since the discovery of Turbo codes in 1993 by Berrou, Glavieux, and Thitimajshima [4], and the rediscovery of LDPC codes by Mackay and Neal in 1995 [21], there has been renewed interest in Turbo codes and LDPC codes, because their error rate performance approaches asymptotically the Shannon limit. Much research is devoted to characterizing the performance of LDPC codes and designing codes that have good performance. Commonly, a graph, the Tanner graph (see [26] and further references), is associated with the code and an important parameter affecting the performance of the code is the girth of its Tanner graph. In [23], [12],

[13] authors consider the design of structured regular LDPC codes whose Tanner graphs have large girth. The regularity and structure of LDPC codes utilize memory more efficiently and simplify the implementation of LDPC coders. The Tanner graph is a special type of graph, a bipartite graph, where the nodes divide into two disjoint classes with edges only between nodes in the two different classes. The impotence of the studies of undirected regular bipartite graphs with large girth for the design of turbo codes is discussed in [23].

Large girth speeds the convergence of iterative decoding and improves the performance of LDPC codes, at least in the high SNR range, by slowing down the on setting of the error floor. Large size of such graphs implies fast convergence.

1.2. **Cryptography.** The cryptographical properties of infinite families of simple graphs of large girth with the special coloring of vertices during the last 10 years (see [31],[34], [33], [35] and further references). Such families can be used for the development of cryptographical algorithms (on symmetric or public key modes). Only few families of simple graphs of large unbounded girth and arbitrarily large degree are known.

Paper [35], [38] is devoted to the more general theory of directed graphs of large girth and their cryptographical applications. It contains new explicit algebraic constructions of infinite families of such graphs. It is shown that they can be used for the implementation of secure and very fast symmetric encryption algorithms. The symbolic computations technique allow us to create a public key mode for the encryption scheme based on algebraic graphs. The information on the implementations if such algorithms can be found in [30],[34], [15], [29] (case of simple graphs) and [35], [37], [16]. Last two papers compare speed of the graph based algorithms with the speed of RC4 and DES.

2. On the upper bounds for size of the regular graphs the with high girth indicator

Let Γ be the graph of irreflexive binary relation Φ on the vertex set V and the following property R holds:

for each vertex $v \in V$ the input degrees $\mathrm{id}(v) = |\{x|(x,v) \in \Phi\}| = k$ or $\mathrm{od}(v) = |\{x|(v,x) \in \Phi\}| = k$ for some positive number $k \geq 2$.

As it follows from property B for balanced graph Φ the cardinality $\{(x,y,z)|(x,y) \in \Phi and (y,z) \in \Phi\}$ is $D = \sum_{v \in V} ({k_v}^2)$. So the number of random walk with two arrows from random vertex v is D/v. Any random walk in this graph can be viewed as the branching process with $\sqrt{(}D/v)$ branches from each node.

The bound $\mathrm{E}_B(d,v) \leq v^{1+1/d} + O(v)$ is based on the studies of such branching process corresponding to the passes of length $\leq d$ of the rooted tree. The definitions of such branching process, expectation operator and the confidence interval the reader can find in the book [14] by Karlin and Taylor.

In our case of regular graphs we can use straightforward combinatorial counting.

Theorem 1.

$$\mathrm{E}_R(d,v) \leq v^{1+1/d} + O(v) \tag{2.1}$$

$$\mathrm{Ex}_R(v, O_{d+1,d}, O_{s,t} | 3 \leq s \leq d) \leq (1/2)^{1/d} v^{1+1/d} + O(v) \tag{2.2}$$

Proof. Let $\Gamma = \Gamma_i$, $i = 1, \dots, v$ be the family of regular graphs corresponding to irreflexive binary relations $\phi = \phi_i$ with the girth indicator i which is $> d$ and maximal possible number of edges on $v = v_i$ vertices. Without loss of generality we may assume $od(v) = k$ for each vertex of Γ. Let us chose the vertex x_0 and consider the totality V_r of all vertices from Γ, such that $r = \mathrm{odist}(x_o, v) \leq d$. We can use the branching process in counting of $v_r = |V_r|$: graph has no loops, so v_1 is k. One link of the vertex $x \in V_2$ may correspond to diagram $O_{2,0}$ so $v_2 \geq k(k-1)$. Induction on i we are getting $v_i = k(K-1)^{i-1}$ for $i = 1, \dots, d$.

We have $(k-1)^d \leq k(k-1)^d \leq v_d \leq v$. Thus, $(k-1)^d \leq v$, $(k-1) \leq v^{1/d}$ $E(\Gamma) = v \times (k \leq v \times (v^{1/d} + 1) = v^{1+1/d} + v$. So we proved (2.1).

Let us assume now that graphs Γ_i, $i = 1, \dots$ do not contain commutative diagrams $O_{d+1,d}$. Let us consider the arc $v_1 \to v_2$ in the graph Γ and two rooted trees T_1 and T_2 with roots v_1 and v_2, respectively. Let P_i be the sets of vertices at the distance d and from the vertex v_i, $i = 1, 2$ The absence of commutative diagrams listed in the theorem insure that $|P_1 \cap P_2| = 0$ and $|P_1 \cup P_2| = (k-1)^d$. Thus $2(q-1)^d \leq v$. So for the size of the graph $E(\Gamma)$ is $\leq v \times ((v/2)^d + 1) = (1/2)^d v^d + v$. □

3. On the sharpness of the bound

The diameter is the minimal length d of the 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. We will say that graph is k-regular, if each vertex of G has exactly k outputs. Let F be the infinite family of k_i regular graphs G_i of order v_i and diameter d_i. We say, that F is a family of small world graphs if $d_i \leq C\log_{k_i}(v_i)$, $i = 1, \dots$ for some independent on i constant C. The definition of small world graphs and related explicit constructions the reader can find in [3]. For the studies of simple small world graphs without small cycles see [10].

Let M be a finite set, $m = |M| \geq 2$. We define M_k, $m \geq k+2$ as the totality of tuples $(x_1, x_2, \dots x_k) \in M^k$, such that $x_i \neq x_j$ for each pair $(i, j) \in M^2$. Let us consider the binary relation $\phi = \phi_k(m)$ on M_k consisting of all pairs of tuples $((x_1, \dots, x_m)\ , (y_1, \dots, y_m))$, such that $y_i = x_{i+1}$ for $i = 1, \dots, k-1$ and $y_m \neq x_i$ for each $i \in \{1, \dots, k\}$. The corresponding directed graph $\Gamma = \Gamma_i(m)$ has order $m(m-1)\dots(m-k+1)$, each vertex has $m-k$ input and output arrows.

Proposition 2. *The girth indicator and diameter of the graph $\Gamma_k(m)$ is $k+1$ and $2k$, respectively. The girth of the graph is $2d+1$*

Proof. Let us consider the $O_{s,t}$, $0 \leq t \leq s \leq k$, $s \geq 1$ of the graph $\Gamma_k(m)$ with the starting point a $= (a_1, a_2, \dots, a_k)$. Let $\mathrm{a}_x = (a_2, a_3, \dots, a_k, x)$ be the neighbor of $\tilde{a}$ within the pass P_x of the diagram of length s. Notice that x is different from a_i, $i = 1, 2, \dots, k$. Let P be other pass of the diagram. If length t of P is zero, we assume that P consist of one vertex a. The first component of ending point w of the P_x equals to x. But the first component of each vertex for each vertex of the pass P is either element of $\{a_1, a_2, \dots, a_k\}$ (case $t < s$ or element y, $y \neq x$ (case $t = s$). But w has to be the vertex of P as well. So we are getting a contradiction. Thus, we proved that the girth indicator of the graph is $> k$.

Notice that w $= (x, x_1, \dots, x_{k-1})$, where $x \neq a_i$, $i = 1, \dots, k$, $x_i \neq a_j$, $J = i+1, i+2, \dots, k$, $j = 1, \dots, k-1$. We can add vertex $(x_1, x_2, \dots, x_{k_1}, x_k)$, consider

the following specialization of variables $x_i = a_i$ for $i = 1, 2, \dots, k$ and obtain the diagram $O'_{0,k+1}$. So the girth indicator of the graph is $k+1$.

Let us consider the pass of length $2k$ starting from a and going throw w and $(x_1, x_2, \dots, x_k)$ as above. It contains the following tuples:

$$(x_2, \dots, x_k, y_1),\ (x_3, \dots, x_k, y_1, y_2), \dots (x_k, y_1, \dots, y_{k-1}).$$

The only requirement on distinct elements $X_k, Y_1, \dots, y_k$ is x_k *nex* and x can be arbitrarily element from the complement of $\{a_1, \dots, a_k\}$. If $m \geq k+2$, then arbitrary point of M_k can be reached from a via the pass as above and diameter of the graph is bounded by $2k$. It is clear that there is no pass of length $2k-1$ between a and element of kind $(Z_1, \dots, z_{k-1}, a_k)$. So $\mathrm{diam}(\Gamma_k(m)) = 2m$.

□

Corollary 3. *Let F be the family of graphs $\Gamma_m(k)$, $m = k+2, k+3, \dots$. Then it is a family of directed small world graphs, the size of the members of this family is on the bound (2.1) of theorem 1.*

Really, $\Gamma_m(k)$ has degree $m-k$, order $v = m(m-1)\dots(m-k+1)$. So $\log_{m-k}(v)$ is some constant $> k$. So diameter of graphs from the family is bounded by $2\log_{m-k}(v)$. The size of $\Gamma_m(k)$ is $v(m-k)$. We have $(m)^k \geq V$. So $E(\Gamma_m(k)) \geq v[(v^{1/k}) - k] = v^{1+1/k} - kv$.

Let us consider the bipartite analog $\Gamma' = \Gamma'_k(m)$ of the graph $\Gamma = \Gamma_k(m)$ Let M be a finite set, $m = |M| \geq 2$. Let P (point set) and L (line set) are two copies of the vertex set M_k, $m \geq k+2$ of the graph Γ. We will use the brackets and parenthesis for the tuples from P and L, respectively.

Let$\Gamma' = \Gamma'_k(m)$ be the graph of binary relation on $P \cup L$ consisting of all pairs of tuples $((x_1, \dots, x_m), [y_1, \dots, y_m)$ or $(x_1, \dots, x_m, (y_1, \dots, y_m))$, such that $y_i = x_{i+1}$ for $i = 1, \dots, k-1$ and $y_m \neq x_i$ for each $i \in \{1, \dots, k\}$. The corresponding directed graph $\Gamma' = \Gamma'_k(m)$ has order $2m(m-1)\dots(m-k+1)$, each vertex has $m-k$ input and output arrows.

Proposition 4. *The girth indicator and diameter of the graph $\Gamma'_k(m)$ is $k+1$ and $2k+1$, respectively. The graph does not contain commutative diagram $O_{k+1,k}$.The girth of the graph is $2d+2$.*

Proof. The graph does not contain $O_{k+1,k}$ because of the ending point of the diagram can not be point and line at same time.The evaluation of the girth indicator and diameter can be done similarly to the evaluation in the proof of proposition 1. □

Corollary 5. *Let F' be the family of graphs $\Gamma'_m(k)$, $m = k+2, k+3, \dots$. Then it is a family of directed small world graphs, the size of the members of this family is on the bound (2.2) of theorem 1.*

Really, $\Gamma'_m(k)$ has degree $m-k$ and order $v = 2m(m-1)\dots(m-k+1)$. We have $(m-k)^K \leq m(m-1)\dots(m-k+1)$. So $k \leq \log_{m-k}(m(m-1)\dots(m-k+1))$. Thus $2k+1 < 3k \leq 3\log_{m-k}(m(m-1)\dots(m-k+1)) < 3\log 2m(m-1)\dots(m-k+1) = 3\log_{m-k}(v)$

The size of $\Gamma'_m(k)$ is $v(m-k)$. We have $(m)^k \geq m(m-1)\dots(m-k+1) = v/2$. So $m > (1/2)^k v^{1/k}$. Thus $E(\Gamma'_m(k)) \geq v((1/2)^{1/k} v^{1/k}) - k] = (1/2)^{1/k} v^{1+1/k} - kv$.

4. On the directed graphs without commutative diagrams of rank $< d$ of minimal order

Recall that (k,g)-cage is a simple graph of degree k, girth g of minimal order $v(k,g)$. The following objects are analogies of classical cages.

Definition 6. *We refer to the directed graph with the girth g, output degree k and minimal order $u(k,g)$ as directed (k,g)-cage.*

As it follows from the definition of directed (k,g)-cage

Theorem 7. *The following hold:*

$$(k+d)(k+d-1)\dots k \geq u(2k+1,d) \geq 1+k(k-1)+\dots k(k-1)^{d-1},$$

$$2[(k+d)(k+d-1)\dots k] \geq u(2k+2,d) \geq (1+(k-1)+\dots (k-1)^d)+(k-1)^d$$

Proof. Let Γ be directed graph with k-outputs for each vertex and girth indicator d, then the branching process Branch starting with the chosen vertex a gives $s = 1+k+k^(k-1)+\dots k(k-1)^d$ different vertices. So we prove (i).

Let b satisfies to $a \to b$. We can consider $K-1$ output arcs (a,x) from a, which are different from (a,b). The branching process starting from each element x b gives at least $(K-1)+\dots (k-1)^{d-1}$ passes of length $\leq d-1$. This way we are getting set T of elements of distance $(d-1)$ from a. Let us consider arcs of kind (b,y), $y \neq a$. The branching process from y gives us $(q-1)+(q-1)^{d-1}$ at distance $d-2$ from y. Together with b we have $1+(q-1)+\dots (q-1)^{d-1}$ elements at distance $\leq d-1$ from b. This set has empty intersection with T because of absence of commutative diagrams $O_{d+1,d}$. So we have at least $(1+(k-1)+\dots (k-1)^d)+(k-1)^d$ different vertices of the graph.

□

Proposition 8. *Let Γ be directed cage with the output degree ≥ 3 of order v and girth indicator d.*

(i) If its girth is $2d+1$, then the size E of the graph satisfies to the following inequality

$$v^{1+1/d} - kv \leq E \leq v^{1+1/d} + v$$

(ii) if its girth is $2d+2$, then the size E of the graph satisfies to the following inequality

$$(1/2)^{1/d}v^{1+1/d} - kv \leq E \leq (1/2)^{1/d}v^{1+1/d} + v$$

Let P be some property of directed regular graphs and $u_P(k,g)$ be the minimal order of graph with the output degree K and the girth indicator g. It is clear that $U_P(k,g) \geq U(k,g)$. So $v(m,g) \geq u(m,g)$, in particular. The following statement follows immediately from the above inequalities.

Corollary 9. *Let s be the property to be simple graph. Then*

a) $v(k,2d+1) = u_S(k,2d+1) \geq u(k,2d+1) \geq 1+k+k(k-1)+\dots+k(k-1)^{d-1}$,

b) $v(k,2d+2) = u_s(k,2d+2) \geq U(k,2d+2) \geq (1+(k-1)+\dots+(k-1)^d)+(k-1)^d$

The above lower bound for $g = 2d+2$ can be improved by Tutte inequality $v(k,2d+2 \geq 2(1+(k-1)+\dots(k-1)^d)$ (see [BCN]). The Tutte's lover bound for $v(k,2d+2)$ is same with (b). The upper and lower bound for $U(k,g)$ are quite tight, both of them are given by polynomial expression in variable k of kind $k^d + f(k)$, where $d = [(q-1)/2]$ and $\deg f(x) \leq d-1$. The situation with the known upper

bound on the order of cages is different, such bound is quite far from the lower one (see [18]).

Cages of odd girth with the order on the Tutte's bound are known as Moore graphs. There are only finite examples of Moore graphs. Well known finite generalized m-gons are examples of cages of even girth (see next section of the paper).

From the existence of the k-regular Moore graph of girth $2d+1$ $(2d+2)$ follows $U(k,d) = v(k,2d+1) = 1 + k(k-1) + \dots k(k-1)^{d-1}$ $(u(k,d) = v(k,2d+1) = 2(1 + (k-1) + \dots (k-1)^d)$, respectively.

There is a finite number of Moore graphs of order v of odd girth. Some infinite families of Moore graphs of even girth are known (see [6] or next section).

Proposition 10. *Let A be the property to be the graph of antisymmetric relation Φ i.e. $(a,b) \in \Phi$ implies that $(b.a)$ is not in Φ. Then*
(i) $(k+d)(k+d-1)\dots k \geq u_A(2k+1,d) \geq 1 + k + k^2 + \dots k^{d-1}$,
(ii) $2[(k+d)(k+d-1)\dots k] \geq u_A(2k+2,d) \geq [1+k+k^2+\dots k^{d-1}]+(k-1)k^{d-1}$.

The bounds (i) and (ii) are valid for balanced antisymmetric regular graphs.

5. Algebraic explicit constructions of extremal regular directed graphs with the fixed girth indicator

We shall use term of *algebraic graph* for the of graph $\Gamma(K)$ of binary relation Φ, such that the vertex set $V(\Gamma) = V(K)$ is an algebraic variety over commutative ring K of dimension ≥ 1 and for each vertex $v \in V$ the neighborhoods $\mathrm{In}(v) = \{x|(x,v) \in V\}$ and $\mathrm{Ou}(v) = \{x|(v,x) \in V\}$ are algebraic varieties over K of dimension ≥ 1 as well (see [2] for the case of simple graphs).

We shall use term *the family of directed graphs of large girth* for the family of regular graphs Γ_i with output degree k_i and order v_i such that their girth indicator $d_i = \mathrm{gi}(\Gamma_i)$ are $\geq c \log_{k_i}(v_i)$, where c is the independent on i constant. So the size of such graphs is quite close to the bound (2.1) or (2.2).

We say that Γ_i form a family of asymptotical directed cages of odd (even) girth if $v_i = ki^{d_i} + o(ki^{d_i})$ ($v_i = 2ki^{d_i} + o(ki^{d_i})$. It is clear that asymptotical cages of even or odd girth are families of graphs of large girth.

In this section we consider examples of families of algebraic graphs of large girth with fixed girth indicator, asymptotical directed cages of odd and even girth, in particular.

E. Moore [11] used term *tactical configuration* of order (s,t) for biregular bipartite simple graphs with bidegrees $s+1$ and $r+1$. It corresponds to incidence structure with the point set P, line set L and symmetric incidence relation I. Its size can be computed as $|P|(s+1)$ or $|L|(t+1)$.

Let $F = \{(p,l)|p \in P, l \in L, pIl\}$ be the totality of flags for the tactical configuration with partition sets P (point set) and L (line set) and incidence relation I. We define the following irreflexive binary relation ϕ on the set F:

$((l_1,p_1),(l_2,p_2)) \in \phi$ if and only if $p_1 I l_2$, $p_1 \neq p_2$ and $l_1 \neq l_2$. Let $F(I)$ be the binary relation graph corresponding to ϕ. The order of $F(I)$ is $|P|(s+1)$ (or $|L|(t+1)$ We refer to it as *directed flag graph* of I.

Lemma 11. *Let (P,L,I) be a tactical configuration with bidegrees $s+1$ and $t+1$ of girth $g \geq 4k$. Then the girth indicator of directed graph $F(I)$ with the output an input degree st is $> k$.*

Let (P, L, I) be the incidence structure corresponding to regular tactical configuration of order t.

Let $F_1 = \{(l, p) | l \in L, p \in P, lIp\}$ and $F_2 = \{[l, p] | l \in L, p \in P, lIp\}$ be two copies of the totality of flags for (P, L, I). Brackets and parenthesis allow us to distinguish elements from F_1 and F_2. Let $DF(I)$ be the directed graph (double directed flag graph) on the disjoint union of F_1 with F_2 defined by following rules:

$(l_1, p_1) \to [l_2, p_2]$ if and only if $p_1 = p_2$ and $l_1 \neq l_2$,
$[l_2, p_2] \to (l_1, p_1)$ if and only if $l_1 = l_2$ and $p_1 \neq p_2$.

Lemma 12. *Let (P, L, I) be a regular tactical configuration of degrees s of girth $g \geq 2m$. Then the girth indicator of double directed graph $DF(I)$ with the output an input degree s is $> m$.*

Generalized m-gons $GP_m(r, s)$ of order (r, s) were defined by J. Tits in 1959 (see [15], [16] and survey [14]) as tactical configurations of order (s, t) of girth $2m$ and diameter m. According to well known Feit - Higman theorem a finite generalized m-gon of order (s, t) has $m \in \{3, 4, 6, 8, 12\}$ unless $s = t = 1$.

The known examples of generalized m-gons of bidegrees ≥ 3 and $m \in \{3, 4, 6, 8\}$ include rank 2 incidence graphs of finite simple groups of Lie type (see [4]). The regular incidence structures are $I_{1,1}(3, q)$ for $m = 3$ (groups $A_2(q)$), $I_{1,1}(4, q)$, $m = 4$ (groups $B_2(q)$) and $I_{1,1}(6, q)$, $m = 6$ (group $G_2(q)$). In all such cases $s = t = q$, where q is prime power.

The biregular but not regular generalized m-gons have parameters $s = q^\alpha$, $t = q^\beta$, where q is a prime power. The list is below: relation $I_{2,1}(4, q)$, $s = q^2, t = q$, q is arbitrary large prime power for $m = 4$; $I_{3,2}(6, q)$, $s = q^3, t = q^2$, where $q = 3^{2k+1}$, $k > 1$ for $m = 6$; $I_{2,1}(8, q)$, $s = q^2, t = q$, $q = 2^{2k+1}$ for $m = 8$. For each triple of parameters (m, s, t) listed above there is an edge transitive generalized m-gon of order (s, t) related to certain finite rank 2 simple group of Lie type. in case of $m = 3$ (projective planes. in particular) and $m + 4$ (generalized quadragons) some infinite families of graphs without edge transitive automorphism group are known. The following two lemmas can be obtained immediately from the axioms of generalized polygon.

Lemma 13. *Let (P, L, I) be the generalized $2k$-gon of order (r, s). Then*
$|P| = \sum_{t=0,k-1} (r^t s^t + r^{t+1} s^t)$, $|L| = \sum_{t=0,k-1} (s^t r^t + s^{t+1} r^s)$.

Lemma 14. *Let (P, L, I) be regular generalized m-gon of degree $q+1$. Then $|P| = |L| = 1 + q + \cdots + q^{m-1}$.*

Corollary 15. *For each $m = 3, 4, 6$ and prime p the family $F_m(q)$, $q = p^n$, $n = 1, \ldots$ of edge transitive polygons is an algebraic family over F_p of cades of girth $2m$ of degree $q + 1$ with the order on the Tutte's lower bound.*

Let (P, L, I) be generalized m-gon of order (s, t), $s \geq 2$, $t \geq 2$ and $e = \{(p, l\}$, $(p \in P, l \in L, pIl)$ be chosen edge of this simple graph.

Let $\mathrm{S}_e = \mathrm{Sch}_e(I)$ be the restriction of incidence relation I onto $P' \cup L'$ where P' (L') is the totality of points (lines) at maximal distance from p (l, respectively). It can be shown that (P', L', S_e) is a tactical configuration of degree $(s - 1, t - 1)$. Let us refer to (P', L', S_e) as Schubert graph. If the generalized polygon is edge-transitive its Schubert graph is unique up to isomorphism. In this case Schubert

graph corresponds to the restriction of incidence relation onto the union of two "largest large Schubert cells", i. e. orbits of standard Borel subgroups of highest dimension.

Proposition 16. *For each $S_m(p)$ $m = 3, 4, 6$ and prime p the family of Schubert graphs $S_m(p)$ of regular generalized m-gons $F_m(q)$ is algebraic over F_p family of asymptotical cages of even girth with the order $2q^{m-1}$ and degree q.*

The extremal properties of finite generalized polygons, their Schubert graphs and some of their induced subgraphs have been considered in [32].

Remark. The girth of $S_m(q)$ is $2m$ for "sufficiently large" parameter q.

Let (P, L, I) be a regular tactical configuration of order (t, t). The *double configuration* $I' = DT(I)$ is the incidence graph of the following incidence structure $(P', L', I') : P' = F(I) = \{(p, l)|p \in P, l \in L, pIl\}$, $L' = P \cup L$, $f = (p, l)Ix$, $x \in L'$ if $p = x$ or $l = x$. It is clear that the order of tactical configuration I' is $(1, t)$. If (P, L, I) is a generalized m-gon, then (P', L', I') is a generalized $2m$-gon.

Proposition 17. *(i) If the girth of regular tactical configuration (P, L, I) of degree $s + 1$ is $2t$, then the girth of $DT(I)$ is $4t$. The order of $DT(I)$ is $(s, 1)$.*

(ii) Let (P, L, I) be regular generalized m-gon, then $DT(I)$ is generalized $2m$-gom.

Corollary 18. *The configurations $DT(I) = I^2(m, q)$ for known regular m-gons, $m = 3, 4, 6$ of degree $q + 1$, q is a prime power, are generalized $2m$-gons of order $(1, q)$.*

Theorem 19. *(i) Let $I_{s.t}(m, q)$, $m \geq 4$ be the incidence relation of one of the known edge transitive m-gons defined over the field F_q, $q = p^n$, p is prime number.*

Then for each tuple (m, s, t, p) the family of directed flag-graphs $F^n(m, s, t, p)$ for generalized m-gon of order $(q^s, q^t$ is an algebraic over F_p family of asymptotic cages of odd girth. The girth indicator of each graph from the family is $m/2 + 1$ and the girth is $m + 1$ $(5, 7, 9)$.

(ii) Let $S_{s.t}(m, q)$, $m \geq 4$ be the Schuberst graph of the incidence relation $I_{s.t}(m, q)$ of one of the known edge transitive m-gons defined over the field F_q, $q = p^n$, p is prime number.

Then for each tuple (m, s, t, p) the family of directed flag-graphs $SF^n(m, s, t, p)$ for $S_{s.t}(m, q)$ is an algebraic over F_p family of asymptotic cages of odd girth. The girth indicator of each graph from the family is $m/2 + 1$ and the girth is $m + 1$.

(iii) Let $I_{1.1}(m, q)$ be the incidence relation of one of the known edge transitive regular m-gons defined over the field F_q, $q = p^n$, p is prime number. Then for each pair (m, p) the family $DF(m, p)$ of double flag graphs $DF(m, i) = DF(I_{1.1}(m, p^i))$, $i = 1, \ldots$ is an algebraic over F_p family of directed asymptotic cages of even girth. The girth indicator of each $DF(m, s)$ is $m + 1$ and the girth is $2m + 2$ $(8, 10.14)$.

(4i) Let $I^2(m, q)$ be the incidence relation of double tactical configuration of regular generalized m gon defined over F_q, $q = p^n$, p is prime. Then for each pair (m, p) the family $F(m, p)$ of directed flag-graphs $F^n(m, p)$, $n = 1, \ldots$ is an algebraic over F_p family of directed graphs of large girth. The girth indicator of each graph is $m + 1$ and girth is $2m + 1$ $(7, 9, 13)$.

Regular finite generalized polygons have been used in works of R. Tanner on Coding Theory. The applications of biregular generalized polygons and their Schubert graphs to Cryptography the reader can find in [33]. Paper [37] devoted to

cryptographical algorithms based on nonsymmetric directed asymptotical cages as above.

6. On the constructions of families of nonsymmetric directed graphs of large girth with fixed degree

The concept of family of simple graphs of large girth of fixed degree had been introduced by P. Erdös' in the late 50th.

The first explicit examples of families of simple graphs with large girth of arbitrary large degree were given by Margulis. The constructions were Cayley graphs $X^{p,q}$ of group $SL_2(Z_q)$ with respect to special sets of $q+1$ generators, p and q are primes congruent to 1 mod4. The family of $X^{p,q}$ is not a family of algebraic graphs because the neighborhood of each vertex is not an algebraic variety over F_q. For each p, graphs $X^{p,q}$, where q is running via appropriate primes, form a family of small world graph of unbounded diameter (see [19],[20]).

The fist family of connected algebraic simple graphs over F_q of large girth and arbitrarily large degree had been constructed in [17]. These graphs $CD(k,q)$, k is an integer ≥ 2 and q is odd prime power had been constructed as connected component of graphs $D(k,q)$ defined earlier. For each q graphs $CD(k,q)$, $k \geq 2$ form a family of large girth with $\gamma = 4/3\log_{q-1}q$.

Two new examples of families of simple algebraic graphs of large girth and arbitrary large degree the reader can find in [36]. Papers [34], [30], [15], [29] devoted to software packages of cryptographical algorithms based on simple graphs.

For each commutative ring the infinite family of directed graphs of large girth with fixed degree has been constructed in [34]. The cryptographical algorithms based on such directed graphs the reader can find in [34], [36]. Paper [15] devoted to implementations of graph based fast stream ciphers corresponding to antisymmetric relations.

References

[1] C.T. Benson, *Minimal regular graphs of girth eight and twelve*, Canadien Journal of Mathematics, (18):1091- 1094, 1966.

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

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

[4] C. Berrou, A. Glavieux and P. Thitimajshima, *Near Shannon limit errorcorrectingcoding and decoding: turbocodes*, ICC 1993, Geneva, Switzerland, pp. 10641070, May 1993.

[5] J.A. Bondy and M.Simonovits, *Cycles of even length in graphs*, J. Combin.Theory, Ser. B, 16 (1974) 87-105.

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

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

[8] W. Faudree, M. Simonovits, *On a class of degenerate extremal graph problems*, Combinatorica 3 (1), 1983, 83-93.

[9] W. Feit, D. Higman *The nonexistence of certain generalised polygons*, J. of Algebra 1 (1964), 114-131.

[10] V. Futorny, V. Ustimenko, *On Small World Semiplanes with Generalised Schubert Cells*, Acta Applicandae Mathematicae, N4, 2007 (already available online).

[11] R. G. Gallager, Lowdensity paritycheck codes, IRE Transactions on Information Theory, vol. IT8, pp. 2128, Jan. 1962.

[12] P. Guinand and J. Lodge, "Tanner Type Codes Arising from Large Girth Graphs", Proceedings of the 1997 Canadian Workshop on Information Theory (CWIT '97), Toronto, Ontario, Canada, pp. 5-7, June 3-6, 1997.

[13] P. Guinand and J. Lodge, *Graph Theoretic Construction of Generalized Product Codes*, Proceedings of the 1997 IEEE International Symposium on Information Theory (ISIT '97), Ulm, Germany, p. 111, June 29-July 4, 1997.

[14] S. Karlin, H.M. Taylor, *A first course in stochastic processes*, Academic Press, New York, 1975.

[15] Yu Khmelevsky, V Ustimenko, Practical aspects of the Informational Systems reengineering, The South Pacific Journal of Natural Science, volume 21, 2003, p.75-21 (together with Yu. Khmelevsky), www.usp.ac.fj/spjns/volume21

[16] J. Kotorowich, V. Ustimenko, *On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings*, Proceedings of the international conferences "Infinite particle systems, Complex systems theory and its application, Kazimerz Dolny, Poland, 2005-2006 (to appear).

[17] 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.

[18] (with F. Lazebnik and A. Woldar) New upper bound on the order of cages, Electronic Journal of Combinatorics, Volume 4 (1997), No. 2, Paper R13.

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

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

[21] D. J. C. MacKay and R. N. Neal, *Good Codes based on very sparse matrices*, In "Cryptography and Coding", 5th IMA Conference, Lecture Notes in Computer Science, v. 1025, 1995, pp. 110-111.

[22] E. H. Moore, *Tactical Memoranda*, Amer. J. Math., v.18, 1886, 264-303.

[23] Jose M. F. Moura, Jin Lu, and Haotian Zhang, *Structured LDPC Codes with Large Girth*, IEEE Signal Processing Magazine, vol. 21:1, pp.42-55, January 2004. Included in Special Issue on Iterative Signal Processing for Communications

[24] R. Ore, *Graph Theory*, Wiley, London, 1971.

[25] M. Simonovits *Extremal Graph Theory*, Selected Topics in Graph Theory 2 (L.W. Beineke and R.J. Wilson, eds), Academic Press, London, 1983, 161-200.

[26] R. Michiel Tanner, *A recursive approach to low density codes*, IEEE Trans. on Info Th., IT, 27(5):533-547, Sept.1984.

[27] J. A. Thas, *Generalised polygons*, in F. Buekenhout (ed), Handbook in Incidence Geometry, Ch. 9, North Holland, Amsterdam, 1995.

[28] J. Tits, *Sur la trialite et certains groupes qui s'en deduisent*, Publ. Math. I.H.E.S, 2 (1959), 15-20.

[29] A. Touzene, V. Ustimenko, *Graph Based Private Key Crypto System*, International Journal on Computer Research, Nova Science Publisher, volume 13 (2006), issue 4, 12p.

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

[31] 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.

[32] V. Ustimenko, A. Woldar, *Extremal properties of regular and affine generalised polygons as tactical configurations*, 2003, European Journal of Combinatorics, 24, 99-111.

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

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

[35] 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 Theory and Cryptology, vol. 3, 181-200 (2007).

[36] V. A. Ustimenko, *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Journal of Mathematical Sciences, Springer, vol. 140, N3 (2007), pp 412-434.

[37] V. Ustimenko *On the graph based cryptography and symbolic computations*, Serdica journal of computing, N1, 2007 (to appear).

[38] V. Ustimenko *On the extremal balanced binary relation graphs of high girth*, Proceedings of the international conferences "Infinite particle systems", Complex systems theory and its application, Kazimerz Dolny, Poland, 2005-2006 (to appear).

Vasyl Ustimenko
University of Maria Curie-Sklodowska
Lublin, Poland
Email: vasyl@golem.umcs.lublin.pl