

On the extremal graphs, their automata, dynamical systems and cryptography

V. A. Ustimenko

February 13, 2007

University of Maria Curie-Sklodowska, Poland, e-mail: vasyk@golem.umcs.lublin.pl

Abstract

The girth $g = g(G)$ of the simple graph G is the smallest length of its cycle. One of the analogs of Erdős's Even Cycle Theorem gives the following upper bound on the size $e(G)$ (number of edges) of the simple graph G of order v and girth $g \geq 2n$: $e(G) \leq Cv^{1+1/n}$, where C is the independent on n constant.

It is known that size of members of the family of k -regular random graphs of girth $g \geq c \log(v)$, $c \leq 2$ is on the above upper bound, they form the family of small world graphs. The deterministic approximation of such a combinatorial chaos is a difficult problem, very few explicit constructions of k -regular infinite families of large girth i.e. graphs with the girth $\geq \log(v)$, are known.

Notice that well known "real-life examples" of small world graphs, including the graph of binary relation "two persons on the earth know each other" contains cliques, so they have cycles of order 3 or 4. So they are different from graphs of large girth.

Simple graphs of large girth turn out to be useful in Networking and other problems of Computer Science. Special importance have algebraic graphs, i.e. graphs for which the vertex set and neighbourhoods of each vertex are algebraic varieties defined over the commutative ring K . In fact we can define families of algebraic graphs of large girth and small world graphs over the general (even infinite) commutative ring.

Here cases of complex number C , real numbers R , p -adic numbers are of special importance because we can define graph-based dynamical systems depending on time for classical analytical varieties (R^n , C^n , in particular) and study effects of synchronization and desynchronization for such varieties. Computational applications require naturally not necessarily simple graphs but graphs of binary relations, because of finite automata are roughly directed graphs with special colouring of

edges. That is why we generalise the elements of extremal graph theory on the case of directed graphs:

The girth of a directed graph (girth indicator) is defined via its smallest commutative diagram. More precicely:

We use term *binary relation graph* for the graph Γ of 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 same cardinality.

We say that the pair of passes $a = x_0 \rightarrow x_1 \rightarrow \dots \rightarrow x_s = b$, $s \geq 1$ and $a = y_0 \rightarrow y_1 \rightarrow \dots \rightarrow y_t = b$, $t \geq 1$ form an (s, t) - commutative diagram $O_{s,t}$ if $x_i \neq y_j$ for $0 < i < s$, $0 < j < t$. Without loss of generality we assume $s \geq t$ and refer to the number s as the rank of $O_{s,t}$. The directed cycle with s arrows we denote as $O_{s,0}$. The minimal parameter $s = \max(s, t)$ of the commutative diagram $O_{s,t}$ with $s+t \geq 3$ in the binary relation graph Γ we call the *girth indicator* of the Γ and denote it as $gi(\Gamma)$.

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

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 of $O_{2,0}$. We obtain the following bound: $E_d(v) \leq v^{1+1/d} + O(v)$.

Via explicit constructions we find out that for $d = 2, 3, 4, 5$ and 6 the bound (1) is sharp up to magnitude.

It indicates that studies of extremal properties of graphs of binary relations with the high girth indicator and studies of $\text{ex}(v, C_3, \dots, C_n)$ are far from being equivalent. Really, the sharpness of the $\text{ex}(v, n)$ for $n = 8$ and $n = 12$ are old open questions (similar to cases of cycles C_8 and C_{12} in Erdős' Even Circuit Theorem).

Size of members of infinite family of directed regular graphs of high girth is close to an upper bound. New explicit construction of infinite families of such algebraic graphs defined over the arbitrarily chosen ring will be given. Finite automata related to members of such a family can be used effectively for the design of cryptographical algorithm for different problems of data security (stream ciphers, data base encryption, public key mode and digital signatures).

References

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