ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 3, Pages 249–255
ISSN 1930-1235: (2008)

# ON SOME APPLICATIONS OF GRAPHS TO CRYPTOGRAPHY AND TURBOCODING

Tanush Shaska

*Department of Mathematics*
*Oakland University*
*shaska@oakland.edu*

V. Ustimenko

*University of Maria Curie-Sklodowska ( Poland)*
and *Institute of telecommunications and global information space (Ukraine)*
*vasyl@golem.umcs.lublin.pl*

Abstract. Families of simple graphs of high girth had been used for the development of algorithms in Cryptography and Turbocoding. Recent results in that directions show the interest of applied researchers to "families of directed graphs of high girth", but the concept of the girth for the directed graphs is not well established. We discuss one of the possible definition. It agrees well with the classical definition in the case of simple graph and allows to create the analog of Extremal graph theory for simple graphs without small cycles for the class of balanced graphs i.e. directed graphs without multiple arrows such that each vertex has same number of inputs and outputs. Finally we discussed some explicit construction of simple and directed graphs which can be applicable to Turbocoding and Cryptography.

## 1. Introduction

Various applications of graph theory to Coding Theory are hard to observe. We just mention that the code is just subset in finite metric space defined via distance regular graph (see [8], [7], [1]) and xpanding graphs (superconcentrators, magnifyers) had been used for the design of important codes (see [14], [26], [20], [19]).

Similar situation is in Cryptography: each computation can be defined in terms of finite automaton, roughly directed graph with labels on arrows, various applications of automata theory to cryptography are very hrd to observe. We just mention [38]( see also further references in this survey).

In this note we mentioned just some traditional applications of families of simple graphs of large girth to construction of LDPS and Turbo Codes (see [25], last chapter of [15], [29], [23], [12], [13]) and Cryptography (see surveys [33], [35], [37]).

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 [5], and the rediscovery of LDPC codes by Mackay and Neal in 1995 [22], 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 [29],[25] 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 based on Tanner graphs of 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.

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 onsetting of the error floor. Large size of such graphs implies fast convergence.

On the web page of Professor Moura (see also [23]) one can find the following text: "Commonly, a graph, the Tanner graph, is associated with the code and an important parameter affecting the performance of the code is the girth of its Tanner graph. In our work, we 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 problem we have been considering is a generic problem in graph theory, namely, that of designing bipartite graphs with large girth. We actually have studied a more special class of this generic problem, in particular, the design of undirected regular bipartite graphs with large girth".

So here we can see clearly two ideas:

(i) new families of bipartite simple graphs of large girth can be used as families of Tanner's graphs

(ii) for the constructions of LDPS codes and turbo codes we can use directed graphs which are analogs of bipartite graphs of large girth.

In the cryptography shift to directed graphs of large girth is very natural because of the finite automaton is directed graphs. Last results demonstrated that choice of appropriate directed graphs lead to very fast graph based encryption algorithms (see [35], [16]). The new algorithms are much faster than encryption schemes [30], [31], [32] corresponding to simple graphs.

## 2. On the classical extremal graph theory for graphs without prescribed cycles and its modification

According to Bourbaki the graph (or directed graph) is the pair $V$ (vertex set) and subset $\Phi$ 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 $\Phi$ are the order and size of the graph, respectively.

Graph is simple if $\Phi$ 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 is 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 $\Gamma$. In this case we say that $\Gamma$ is $F$-free. Let $P$ be certain graph theoretical property. 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 [4].

This theory contains several important results on $\mathrm{ex}(v, F)$, where $F$ is a finite collection of cycles of different length [4], [28]. The following statement had been formulated by P. Erdös'.

Let $C_n$ denote the cycle of length $n$. Then

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

where $C$ is independent positive constant.

For the proof of this result and its generalizations see [6], [10].

In [9] the upper bound

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

was established for all integers $k \geq 1$.

Both bounds are known to be sharp for $k = 2, 3, 5$ in other cases the question on the sharpness is open (see [4], [2] 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 $\geq n$. 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 [4]) 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 $DK_v$ of binary relation $\phi$: $P \cup L = V$, $P \cap L = \emptyset$, $|P| = |L|$, $|V| = v$, $\phi = P \times L$ of order $O(v^2)$ has no directed cycles or commutative diagrams.

In [33], [37] 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 $\Gamma$ be directed graph. The *pass* between vertices $a$ and $b$ is the sequence $a = x_0 \to x_1 \to \ldots x_s = b$ of length $s$, where $x_i$, $i = 0, 1, \ldots, s$ are distinct vertices. We refer to the 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 $a = x_0 \to x_1 \to \cdots \to x_s = b$, $s \geq 1$ and $a = y_0 \to y_1 \to \cdots \to y_t = b$, $t \geq 1$ 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 that $s \geq t$ and refer to the number $s$ as the rank of $O_{s,t}$. The directed cycle with $s$ arrows we denote as $O_{s,0}$. We will count directed cycles as commutative diagram.

The minimal parameter $s = \max(s,t)$ of the commutative diagram $O_{s,t}$ with $s+t \geq 3$ in the binary relation graph $\Gamma$ we call the *girth indicator* of the $\Gamma$ 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 $\Gamma$ 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 [37] is the following statement. If $B$ is 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 problems (see [2], [4]) .

The regularity $R$ of graph $(V, \Phi)$ 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.

The family of directed graphs $G_i$, $i = 1, \ldots$ with average output degree $k_i$ and order $v_i$ is the family of graphs of large girth if the girth indicator of $G_i$ is $\geq c \times \log_{k_i}(v_i)$. 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).

## 3. Explicit constructions of Tanner graphs

3.1. **Some suggestions in case of simple graphs.** The induced biregular bipartite subraphs of graphs $D(n,q)$ (see [17] and further references) of order $2q^n$, degree $q$ and girth $\geq n+4$ or their connected components $CD(d,q)$had been used

by Guinnand and Lodge for the construction of turbocodes. The description of the class of biregular subgraphs of the above graphas the reader can find in [18]. The parameters of related codes are very close to the Shannon bound.

We notice that the family of graphs $D(n,q)$ depending on two parameters $n$ and $q=p^m$, where $p$ is prime, is not the unique known family of graphs of unbounded degree and arbitrarily large girth. For "sufficiently large $p$" the exact girth is computed in [27].

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 [21],[19]).

Of course Cayley graph corresponding to finite group $G$ and symmetrical set of generators $S$ ( $s\in S$ leads to $s^{-1}\in S$ is not a bipartite graph. But we can take it bipartite analog - the graph of incidence structure $I=I(G,S)$for which the point set $P$ and line set $L$ are two distinct copies of $G$ and $p\in P$ is incident to $l\in L$ if and only if $ps=l$ in group $G$ for some generator $s\in S$.

Let $R$ be arbitrary subset of $S$ containing at least 3 elements, $G_R$ be the group generated by $R\cup R^{-1}$ and $G_R<H<G$.

We can consider the bipartite graph $I'=I(H,R)$ with the partition sets $P'=P\ capH$ and $L'=L\cap H$ such that $p\in P'$ and $l\in L'$ are incident ($pI'l$ or $lI'p$) if and only if $ps=l$ for some $s\in R$. Notice, that last condition is equivalent to $ls=p$ for some $s\in R^{-1}$.

We set the Cayley graph corresponding to $G,S$ is $X^{p,q}$. then $g(I(H,R)$ is larger than the girth of $X^{p,q}$. So $I(H,R)$ can be used as Tanner graph.

Some other regular graphs of high girth the reader can find in [34].

3.2. **Examples of directed bipartite graphs with large girth indicators.** Let $M_k$, $m\geq k+2$ 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 1.** *The girth indicator and diameter of the graph $\Gamma_k(m)$ is $k+1$ and $2k$, respectively. The girth of the graph is $2d+1$.*

The reader can find the proof in [36].

Let us consider the bipartite version $\Gamma'=\Gamma'_k(m)$ 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 $\Gamma$. 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 2.** *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* $2d+2$*.*

So one can use these directed bipartite regular graphs as directed Tanner graphs.

## References


[1] E. Bannai, T. Ito, *Algebraic Combinatorics 1: Association Schemes*, Benjumin-Cummings Lecture Notes, Ser. 58, London, 1984.

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

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

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

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

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

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

[8] Ph. Delsarte, *An algebraic approach to the association schemes of coding theory*, Phillips Research Reports Suppl., 10 (1973).

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

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

[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. Hoory, N. linial and A. Widgerson, *Expander graphs and their applications* Bulletin (New series) od the American Mathematical Society, volume 43, N4,2006, 439-561.

[15] W. C. Huffman and V. Pless, Fundamentals of Error Correcting Codes, Cambridge University Press, 2003, 646 pp.

[16] J. Kotorowicz, V. A. 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.

[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] F. Lazebnik, V. A. Ustimenko 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] A Lubotsky, *Discrete Groups, Expanding Graphs and Invariant Measures*, Progres in Math., Birkhauser, 1994.

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

[22] 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.

[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] T. Richardson, R. Urbanke, *Modern Coding Theory*, Cambridge University Press, 2008, 592 pp.
[26] P. Sarnak, *What is an expander?*, Notices of AMS, 2004, 762-763. Linear Algebra and its Applications Article in Press, Corrected
[27] T. Shaska, V. Ustimenko, *On the homogeneous algebraic graphs of large girth and their applications*, Linear Algebra and its Applications Article in Press, 2008 (in press, available on line).
[28] 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.
[29] R. Michiel Tanner, *A recursive approach to low density codes*, IEEE Trans. on Info Th., IT, 27(5):533-547, Sept.1984.
[30] 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.
[31] V. Ustimenko, *Graphs with Special Arcs and Cryptography*, Acta Applicandae Mathematicae, 2002, vol. 74, N2, 117-153.
[32] V. Ustimenko, *CRYPTIM: Graphs as tools for symmetric encryption*, In Lecture Notes in Comput. Sci., 2227, Springer, New York, 2001.
[33] 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).
[34] V. A. Ustimenko, *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Journal of Mathematical Sciences, Springer, vol. 140, N3 (2007), pp 412-434.
[35] V. Ustimenko *On the graph based cryptography and symbolic computations*, Serdica journal of computing, N1, 2007, 131-156.
[36] V. A. Ustimenko, *On the extremal regular directed graphs without commutative diagrams and their applications in coding theory and cryptography*, Albanian. J. of Mathematics, Special Issue "Algebra and Computational Algebraic Geometry", vol. 1, N4, 387-400, 2007.
[37] V. Ustimenko, *On the cryptographical properties of extremal algebraic graphs*, In Publisher: IOS Press Title: Mathematics and Communications Editors: T. Shaska, E. Hasimaj, IOS Press, 2008 (to appear).
[38] S. Wolfram, *Cryptography with cellular automata* , Lecture notes in computer sciences, 218 (1985) (Advances in cryptology-CRYPTO 85, Santa Barbara, California), 429 - 432.