# On LDPC codes corresponding to new families of regular expanding graphs of large girth

Monika Polak, Vasyl Ustimenko
Maria Curie-Sklodowska University (Poland)

monika.katarzyna.polak@gmail.com

**Abstract**

We are testing correcting properties of LDPC codes connected with the new families of regular graphs of bounded degree and increasing girth. They form a family of expanding graphs, some of them are in fact Ramanujan graphs. In the difference with previously known graphs of large girth graphs from new families are not edge transitive. We compare spectral gaps and key parameters of LDPC codes for new graphs with previously known results. Some codes have visible advantage in comparison with codes obtained by Guinand and Lodge corresponding to connected components of family $D(n,q)$ [1].

There are many different algorithms in everyday life where graphs are used. One of the most interesting features of the new graphs is their expansion property. This property seems to be significant in a lot of mathematical, computational and physical contexts. Another interesting property of our graphs is the property of being a family of graphs of increasing girth. Such graphs are used for example for constructions of error correcting codes. Basically, only two explicit constructions of families of connected graphs of large girth and superlinear size are known (Ramanujan-Cayley graphs [2], algebraic graphs $CD(n,q)$) given by the nonlinear system of equations over finite field $F_q$). Lubotzky, Phillips and Sarnak [3] proved that Ramanujan - Cayley graphs $X(p,q)$, where $p$ and $q$ are primes, introduced by G. Margulis [4] satisfy the Ramanujan graphs definition.

In this peper we present a method to obtain a new families of graphs with specific properties required in practical applications. We describe properties of obtained new families $A'(n,q)$ and $D'(n,q)$ in comparison to previously known families such as $A(n,q)$ ([5]) and $D(n,q)$ which has been known since 1995 [6]. However the main goal is to show how they can be used in practice for the creation of error correcting codes.

By the theorem of Alon and Boppana, large enough members of an infinite family of $q$-regular graphs with constant $q$ satisfy the inequality $\lambda \geq 2\sqrt{d-1}-o(1)$, where $\lambda$ is the second largest eigenvalue in absolute value. Ramanujan graphs are $d$-regular graphs for which the inequality $\lambda \leq 2\sqrt{d-1}$ holds. We say that a family of regular graphs of bounded degree $q$ of increasing order $n$ *has an expansion constant* $c$, $c > 0$ if for each subset $A$ of the vertex set $X$, $|X| = n$ with $|A| \leq n/2$ the inequality $|\partial A| \geq c|A|$ holds. The expansion constant of the family of $q$-regular graphs can be estimated via upper limit $q - \lambda_n$, $n \to \infty$, where $_n$ is the second largest eigenvalue of family representative of order $n$. It is clear that a family of Ramanujan graphs of bounded degree $q$ has the best expansion constant.

Family of graphs $G_n$ is a family of graphs of increasing girth if $g(G_n)$ goes to infinity with the growth of $n$. The *family of graphs of large girth* is an infinite family of simple regular graphs $\Gamma_i$ of degree $k_i$ and order $v_i$ such that: $g(\Gamma_i) \geq \gamma \log_{k_i} v_i$, where $c$ is independent of $i$ constant.

Let $F_q$, where $q$ is prime power, be a finite field. $CD(n,q)$ (connected components of $D(n,q)$) and $A(n,q)$ are connected, biregular, bipartite $V = P \cup L$ families of graphs of increasing girth. Sets $P$ and $L$ can be consider as two copies of Cartesian power ${F_q}^n$, where $n \geq 2$ is a integer. Graphs $D(n,q)$, $n \geq 2$ of fixed degree $q$ form a family of expanders with the second largest eigenvalue bounded from above by $2\sqrt{q}$. A family $A(n,q)$ of increasing girth, superlinear size and degree $q$ is given by the nonlinear system of equations. If $q$ is fixed then the second largest eigenvalue of $A(n,q)$is also bounded by $2\sqrt{q}$. So, families $A(n,q)$ and $D(n,q)$ consist of "almost Ramanujan graphs". Graphs $A(n,q)$ are not edge transitive. They are connected if $q \geq 2$. In fact, $A(n,q)$ form a family of small world graphs. There is a conjecture that $CD(n,q)$ is another family of small world graphs.

Described families of graphs can be use to obtain new families with different structures. It can be done by use of simple cubical operator on the vertex set of graph from one of the family, such operator allow us to define a new relations. Let $(v) = (v_1, v_2, ...v_n)$ denote point,

$[v] = [v_1, v_2, ...v_n]$ denote line and $N_t(v)$ be the operator of taking neighbor of vertex $v$ where first coordinate is $v_1 + t$: $N_t(v_1, v_2, v_3, ...v_n) \to [v_1 + t, *, *, ..., *]$, $N_t[v_1, v_2, v_3, ...v_n] \to (v_1 + t, *, *, ..., *)$. The remaining coordinates can be determined uniquely using original relations defining used graph. As it follows from the equations each vertex has exactly one neighbor of chosen color $t$. It is easy to see that $N_t$ is invertible operator on the set of vertices. To create a new family we can use the composition of two such operators $N_t \circ N_0$ on two copies of the same graph ( it is also possibility to take other composition of such operators). For arbitrary graph $G$ described above let $I'$ denote the incidence relation defined by using composition $N_t \circ N_0$. Take two copies of $G$ and denote point in first copy by (p) and in second by $\langle z \rangle$. $(p)I' \langle z \rangle$ if for some $t \in F_q$ relations $(p)I[l]I \langle z \rangle$ hold, where $I$ is the incidence relation in based graph: $A(n, q)$ or $D(n, q)$ described by system of equations ([5]), ([6]). Graph defined by new binary relation on two copies of graph $D(n, q)$ or $A(n, q)$: $(p)I' \langle z \rangle$ we denote $D'(n, q)$ or $A'(n, q)$ accordingly, with the notation for point and line as for $D(n, q)$ ([6]) or $A(n, q)$ ([5]) . Above constructions form a simple undirected families of graphs. Expansion and other properties of this new families are very interesting. We have following propositions:

1. Families $A'(n, q)$ and $D'(n, q)$ are expanders.
2. Families $A'(n, q)$ and $D'(n, q)$ for $q = 3$ are $q$-regular Ramanujan graphs $\lambda_1 \leq 2\sqrt{3-1}$ and they density is $\frac{4}{3(3^{n+1}-1)}$.
3. Families $A'(n, q)$ and $D'(n, q)$ are families of graphs of increasing girth (with growing $n$). For all $n \geq 2$ there is no cycles of length 4. $D'(n, q)$ form a family of a large girth.
4. There is no transitive groups defined on the graphs $A'(n, q)$ and $D'(n, q)$.

Presented construction leads us to families of graphs that can be successfully used in coding theory to create LDPC codes. Since 1997 when the first time graphs $CD(n, q)$ have been used to create LDPC codes, which are applied by NASA there were no results, that would indicate a weak properties of codes derived from them. Therefore very good and economic codes can be obtained by studying algebraic structures with similar properties.

Let consider the minimum distance analysis for described codes. Presented families of graphs have increasing girth so we can construct LDPC codes with arbitrary large girth. Combining Proposition 3 and lower bound on $d_{min}$ given by Tanner in [7], we see that LDPC codes, corresponding to presented families of graphs, can be designed to have arbitrarily large minimum distance $d_{min}$. We were testing LDPC codes corresponding to designed families of graphs by using BPSK modulation over AWGN channel and simple MAP decoder implementation. Our simulations showed that codes, based on representatives of new described families, have most frequently better error correcting properties than codes based on $D(n, q)$. This fact is supported by many simulations conducted for randomly chosen parameters.

**Keywords**

LDPC codes, expanding graphs, large girth, spectral gap

# References

[1] 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.

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

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

[4] G. A. Margulis. Explicit group-theoretic constructions of com- binatorial schemes and their applications in the construction of expanders and concentrators. Problemy Peredachi Informatsii, 24(1):5160, 1988

[5] V. A. Ustimenko, U. Roamńczuk and M. Klisowski, The implementation of cubic public keys based on a new family of algebraic graphs, Annales UMCS Informatica AI XI, 2 (2011) 127141.

[6] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, A new series of dense graphs of high girth , Bulletin (New Series) of the AMS Vol. 32, Number 1 (1995):73–79.

[7] R. M. Tanner, A recursive approach to low density codes, IEEE Transactions on Information Theory IT 27(5) (1984):533–547.