 DOI: 10.1515/umcsinfo-2015-0006

Algorithms for generation of Ramanujan graphs, other Expanders and related LDPC codes

Monika Polak[1*], Vasyl Ustimenko[1†]

[1] *Institute of Mathematics, Maria Curie-Sklodowska University, pl. M. Curie-Sklodowskiej 5, 20-031 Lublin, Poland.*

Abstract – Expander graphs are highly connected sparse finite graphs. The property of being an expander seems significant in many of these mathematical, computational and physical contexts. For practical applications it is very important to construct expander and Ramanujan graphs with given regularity and order. In general, constructions of the best expander graphs with a given regularity and order is no easy task. In this paper we present algorithms for generation of Ramanujan graphs and other expanders. We describe properties of obtained graphs in comparison to previously known results. We present a method to obtain a new examples of irregular LDPC codes based on described graphs and we briefly describe properties of this codes.

(*Received: 07.07.2015; Revised: 29.09.2015; Published: 10.11.2015*)

1 Introduction

The property of being an expander seems to be very significant. In fact the known families of Ramanujan graphs of unbounded degree play an important role in theory of finite geometries and have many practical applications for example in Internet network, cryptography, car navigation systems, sociology, mobile robotics and construction of class of error correcting codes so called LDPC codes. What's more expander graphs are used to efficient error reduction in probabilistic algorithms. Algorithms that use the random input (is not easy to collect a reasonable collection of random bits) to reduce the expected running time or memory usage have a chance of producing an incorrect result. Using expander walks allows to achieve the same error probability, with much fewer random bits. The exact form of the exponential decay in error using expander walks and its dependence on the spectral gap was found by Gillman [**1**].

Graphs used in this paper were introduced in [**2**]. Other constructions based on similar idea were presented in [**3**]. However, the girth of presented graphs is 6 and 8 (Theorem 1 and Theorem 2, [**2**]) and the girth of graphs presented in [**3**] is 6. This allow us to construct LDPC codes from presented graphs. Theorem introduced in [**2**] were included without proofs. We introduce this theorems with proofs in Section 3. It is very important for construction of LDPC codes that graphs which we use must have girth $g \geq 6$.

Throughout this paper only undirected, simple graphs without loops or multiple edges are considered. A graph is connected if for arbitrary pair of vertices v_1, v_2 there is a path from v_1 to v_2. The length g of the shortest cycle in a graph is called a *girth*, [**4**]. Bipartite graph is a graph whose vertices set V can be divided into two disjoint subsets V_1 and V_2 such that every edge connects a vertex in V_1 to one in V_2. We refer to bipartite graph $\Gamma(V_1 \cup V_2, E)$ as biregular one if the number of neighbours for vertices from each partition sets are constants s and t (bidegrees). We call a graph regular in the case $s = t$. Missing definitions can be found in [**5, 6**].

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, [**7**]. The expansion constant of the family of q-regular graphs can be estimated via upper limit $q - \lambda_n$, $n \to \infty$, where λ_n is the second largest eigenvalue of family representative of order n. The first explicit expander graph family was constructed by Gregory Margulis in the 1970's via studies of Cayley graphs of large girth [**8**].

By the theorem of Alon and Boppana, large enough members of an infinite family of d-regular graphs with constant d satisfy the inequality $\lambda \geq 2\sqrt{d-1} - o(1)$, where λ 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. It is clear that a family of Ramanujan graphs of bounded degree q has the best expansion constant, [**9**].

Regular generalized polygons are one of the best expanders. They are regular tactical configurations of diameter m and girth $2m$. For each parameter m, a regular generalized m-gon has degree $q+1$ and order $2(1+q+...+q^{m-1})$, [**10**].

However, according to the famous Feit-Higman theorem the regular thick (i.e. degree ≥ 3) generalized regular m-gons exist only for $m = 3, 4$ and 6, [**11**]. Thus Generalized Pentagon does not exist, in particular. We have the following properties of generalized regular polygons:

*monika.katarzyna.polak@gmail.com
†vasyl@hektor.umcs.lublin.pl

- the incidence graph of a projective plane $PG(2,q)$ has $|V| = \nu(q+1,6) = 2(1+q+q^2)$ and $g = 6$,
- the incidence graph of a generalized quadrangle $GQ(q,q)$ has $|V| = \nu(q+1,8) = 2(1+q+q^2+q^3)$ and $g = 8$,
- the incidence graph of a generalized hexagon $GH(q,q)$ has $|V| = \nu(q+1,12) = 2(1+q+q^2+q^3+q^4+q^5)$ and $g = 12$.

By $\nu(q,g)$ we denote a Moore graph which is a regular graph of vertex degree $q > 2$ and girth g that contains the maximum possible number of nodes. For practical applications it is very important to create families of expander graphs with other parameters. For now we create a families of expander graphs of unbounded degree but only two of them are investigated until now. In [**2**] we introduced this new structures. This construction can be extended for arbitrary large parameter n which yield us to connected $q+1$ regular graphs of order $2(1+q+...+q^{n-1})$.

2 Construction of the families

In [**12**] the incidence structures corresponding to generalized polygons were considered. Recently we use the concept of a *root system* ϕ which is a configuration of vectors in a Euclidean space satisfying certain geometrical properties. In [**2**] we created a graphs having interesting properties by using root system and special binary operation, we only consider cases for $n = 3,4,5$ and for $n \geq 6$ the work is in progress.

In our construction we simplify the concept used in [**12**]. We redefined used operators and introduced new algorithm to choose a set of positive roots. There is only one 3-element set $\phi_3^+ = \{\alpha_1, \alpha_2, \alpha_1+\alpha_2\}$. The sets ϕ_4^+ consisting four elements are two: $\{\alpha_1, \alpha_2, \alpha_1+\alpha_2, 2\alpha_1+\alpha_2\}$ and $\{\alpha_1, \alpha_2, \alpha_1+\alpha_2, \alpha_1+2\alpha_2\}$, but they are symmetric and give the same results. There are three ways to choose non-symmetric sets ϕ_5^+: $\{\alpha_1, \alpha_2, \alpha_1+\alpha_2, 2\alpha_1+\alpha_2, \alpha_1+2\alpha_2\}$, $\{\alpha_1, \alpha_2, \alpha_1+\alpha_2, 2\alpha_1+\alpha_2, 2\alpha_1+2\alpha_2\}$, $\{\alpha_1, \alpha_2, \alpha_1+\alpha_2, 2\alpha_1+\alpha_2, 3\alpha_1+\alpha_2\}$. For $n = 3$ this construction yields projective plane which is commonly known. For $n = 4$ the set of roots is the same as for generalized quadrangle but we obtain two structures witch different properties. For $n = 5$ the set ϕ_5^+ can not be derived from Cartan matrix and we obtained over a dozen new structures with different properties.

Before we introduce incidence relations in obtained graphs we will describe the set of vertices. Let $\Gamma(n, \phi_n^+, \mathbb{F}_q)$ denote bipartite graph obtained by using n-element set ϕ_n^+, scalars from $\mathbb{F}_q$ and binary operator $\langle\cdot,\cdot\rangle$. Traditionally in geometrical bipartite graphs one set of vertices is called set of points P and another one set of vertices is called set of lines L.

First, let us consider an ordinary n-gon as a bipartite graph with vertex set $V = P \cup L = \{(1),(2),\ldots,(n)\} \cup \{[1,2],[2,3],\ldots,[n-1,n],[n,1]\}$. We can write the incidence relation I in n-gon as follows:

$$(m)I[s,t] \Longleftrightarrow m = s \vee m = t.$$

A line is incident with point if this point belong to this line. Let vertex of type t_i be define as vertex corresponding to i-element subset of ϕ_n^+, $i = 0,1,2,...,n-1$ and let A_i denote i-element closed subset of ϕ_n^+. We create two ascending sequences of closed subset of ϕ_n^+. Second element of first sequence is $\{\alpha_1\}$ and for second sequence second element is $\{\alpha_2\}$:

$$A_0 = \{\emptyset\} \subset A_1 = \{\alpha_2\} \subset A_2 \subset A_3 ... \subset A_{n-1} = \phi_n^+ \backslash \{\alpha_1\},$$

$$B_0 = \{\emptyset\} \subset B_1 = \{\alpha_1\} \subset B_2 \subset B_3 ... \subset B_{n-1} = \phi_n^+ \backslash \{\alpha_2\}.$$

For bigger n set ϕ_n^+ has more roots and above sequences can be chosen in many ways. Now, we choosing elements from this two sequences alternately we create set of points and set of lines. For lines we choose a sets: $B_0 = \{\emptyset\}, A_1 = \{\alpha_2\}, B_2, A_3, ..., \phi_n^+ \backslash \{\alpha_j\}$ and for points $A_0 = \{\emptyset\}, B_1 = \{\alpha_1\}, A_2, B_3, ..., \phi_n^+ \backslash \{\alpha_i\}$, where $i = 1$ and $j = 2$ if n is odd and $i = 2$ and $j = 1$ if n is even. Let F_q, where q is prime power, be a finite field. The the number of vertices in obtained graph $\Gamma(n, \phi_n^+, \mathbb{F}_q)$ is $|V| = 2(1+q+q^2+\ldots+q^{n-1})$. The graph is bipartite $V = P \cup L$ and set V consist of:

2 elements of type t_0–$((1), \alpha_1^*)$ and $[[1,2], \alpha_2^*]$,

$2q$ elements of type t_1–$((2), \alpha_1^* + p_1\alpha_1)$ and $[[1,2], \alpha_2^* + l_1\alpha_2]$,

$2q^2$ elements of type t_2–$((n), \alpha_2^* + \sum_{\alpha \in A_2} p_\alpha \alpha)$ and $[[2,3], \alpha_1^* + \sum_{\alpha \in B_2} l_\alpha \alpha]$,

$\vdots$

$2q^{n-1}$ elements of type t_{m-1}–$((\lceil \frac{n+2}{2} \rceil) + \sum_{\alpha \in \phi_n^+ \backslash \{\alpha_i\}} p_\alpha \alpha)$ and

$[[\lfloor \frac{n+2}{2} \rfloor, \lfloor \frac{n+4}{2} \rfloor] + \sum_{\alpha \in \phi_n^+ \backslash \{\alpha_j\}} l_\alpha \alpha]$,

where $i = 1$ and $j = 2$ if n is odd and $i = 2$ and $j = 1$ if n is even and p_α, $l_\alpha \in \mathbb{F}_q$. Brackets and parenthesis will allow the reader to distinguish points $(\cdot)$ and lines $[\cdot]$. The set of edges consisting of all pairs $\{(p),[l]\}$ for which $(p)I_\Gamma[l]$. The incidence relation I_Γ for the graph $\Gamma(n, \phi^+, \mathbb{F}_{\shortparallel})$ are defined as follows. Let ψ_1 and ψ_2 be a closed subset of the set of positive roots ϕ^+ and let Σ_p and Σ_l be a linear combination of elements of set ψ_1 and ψ_2 accordingly, with scalars from $\mathbb{F}_{\shortparallel}$. Point $(p) = ((m), \alpha_i^* + \Sigma_p)$ is incident to line $[l] = [[s,t], \alpha_j^* + \Sigma_l]$ (we denote it by (p)I [l]) if and only if

$$(m = s \vee m = t) \wedge (\langle \alpha_i^* + \Sigma_p, \alpha_j^* + \Sigma_l \rangle_{|\psi_1 \cap \psi_2} = 0).$$

It is easy to see that this is symmetric incidence relation (the graphs are simple). This construction allowed us to

obtain new structures similar in some aspect to generalized polygons but in general with different properties.

In Table 2 we present incidence relations for graph $\Gamma(4,\phi_4^+,\mathbb{F}_q)$ when sequences of closed set are following $\{\alpha_1\}\subset\{\alpha_1,2\alpha_1+\alpha_2\}\subset\{\alpha_1,2\alpha_1+\alpha_2,\alpha_1+\alpha_2\}$, $\{\alpha_2\}\subset\{\alpha_1,\alpha_1+\alpha_2\}\subset\{\alpha_2,\alpha_1+\alpha_2,2\alpha_1+\alpha_2\}$.

In Table 3 we present incidence relations for graph $\Gamma(5,\{\alpha_1\},\{\alpha_1+\alpha_2\},\{2\alpha_1+\alpha_2\},\{\alpha_1+2\alpha_2\},\mathbb{F}_q)$ and sequences: $\{\alpha_1\}\subset\{\alpha_1,2\alpha_1+\alpha_2\}\subset\{\alpha_1,2\alpha_1+\alpha_2,\alpha_1+\alpha_2\}\subset\{\alpha_1,2\alpha_1+\alpha_2,\alpha_1+\alpha_2,\alpha_1+2\alpha_2\}$ and $\{\alpha_2\}\subset\{\alpha_1,\alpha_1+2\alpha_2\}\subset\{\alpha_2,\alpha_1+2\alpha_2,\alpha_1+\alpha_2\}\subset\{\alpha_2,\alpha_1+2\alpha_2,\alpha_1+\alpha_2,2\alpha_1+2\alpha_2\}$ In this case we obtained $\lambda_1<2\sqrt{q}$. For this chooses we obtained better results than other possibilities and only their are in consideration in this article.

TABLE 1. Incidence relations for graph $\Gamma(3,\phi_3^+,\mathbb{F}_q)\cong PG(2,q)$

	$((1),\emptyset)$	$((2),p_1)$	$((3),p_1,p_2)$
$[[1,2],\emptyset]$	+	+	−
$[[3,1],l_1]$	+	−	$+:p_1=l_1$
$[[2,3],l_1,l_2]$	−	$+:p_1=l_1$	$+:l_2-p_2=l_1p_1$

TABLE 2. Incidence relations for graph $\Gamma(4,\phi_4^+,\mathbb{F}_q)$

	$((1),\emptyset)$	$((2),p_1)$	$((4),p_1,p_2)$	$((3),p_1,p_2,p_3)$
$[[1,2],\emptyset]$	+	+	−	−
$[[4,1],l_1]$	+	−	$+:l_1=p_1$	−
$[[2,3],l_1,l_2]$	−	$+$ $p_1=l_1$	−	$+\ p_1=l_1$ $p_2-l_2=p_3l_1$
$[[3,4],l_1,l_2,l_3]$	−	−	$+:p_1=l_1,$ $p_2=l_2$	$+:l_2-p_2=p_1l_1,$ $l_3-p_3=p_1l_2$

TABLE 3. Incidence relations for graph $\Gamma(5,\phi_5^+,\mathbb{F}_q)$

	$((1),\emptyset)$	$((2),p_1)$	$((5),p_1,p_2)$	$((3),p_1,p_2,p_3)$	$((4),p_1,p_2,p_3,p_4)$
$\begin{bmatrix}[1,2]\\ \emptyset\end{bmatrix}$	+	+	−	−	−
$\begin{bmatrix}[1,5]\\ l_1\end{bmatrix}$	+	−	$+:p_1=l_1$	−	−
$\begin{bmatrix}[2,3]\\ l_1\\ l_2\end{bmatrix}$	−	$+:$ $p_1=l_1$	−	$+:p_1=l_1$ $p_2-l_2=p_3l_1$	−
$\begin{bmatrix}[4,5]\\ l_1\\ l_2\\ l_3\end{bmatrix}$	−	−	$+:p_1=l_1,$ $p_2-l_2=p_1l_3$	−	$+:p_1=l_1,$ $p_2-l_2=p_1l_3+p_3l_1$ $p_3=l_3$
$\begin{bmatrix}[3,4]\\ l_1\\ l_2\\ l_3\\ l_4\end{bmatrix}$	−	−	−	$+:p_1=l_1,$ $p_2-l_2=p_1l_3+p_3l_1$ $p_3=l_3$	$+:p_2-l_4=l_3p_1,$ $p_3-l_3=l_1p_1$ $p_4-l_2=l_1p_3$

3 Comparison with previously known results

Expanding and other properties are following. The families $\Gamma(n,\phi_n^+,\mathbb{F}_q)$ consist of bipartite graphs with $|V|=2(1+q+q^2+\ldots+q^n)$ vertices and $(q+1)(1+q+q^2+\ldots+q^n)$ edges. A sparse graph has a small number of edges in comparison to the number of vertices. A simple relationship describing the density of the graph $\Gamma(V,E)$ is

$$D=\frac{2|E|}{|V|(|V|-1)}, \tag{1}$$

where $|E|$ is the number of edges of graph Γ and $|V|$ is the number of vertices. The maximal density is $D=1$ when a graph is complete and the minimal density is 0 (Coleman & Moré 1983).

TABLE 4. Comparison between presented families and generalized regular polygons for $n=3,4,5$

Graph	Regularity	|V|	Girth	λ_1
$PG(2,q)\cong$ $\Gamma(3,\phi_3^+,\mathbb{F}_q)$	$q+1$	$2(1+q+q^2)$	6	$\sqrt{q}$
$GQ(q,q)$	$q+1$	$2(1+q+q^2+q^3)$	8	$\sqrt{2q}$
$\Gamma(4,\phi_4^+,\mathbb{F}_q)$	$q+1$	$2(1+q+q^2+q^3)$	6	$\sqrt{3q}$
generalized pentagon	do not exist			
$\Gamma(5,\phi_5^+,\mathbb{F}_q)$	$q+1$	$2(1+q+q^2+q^3+q^4)$	8	$\leq 2\sqrt{q}$

$\Gamma(n,\phi_n^+,\mathbb{F}_q)$ are $q+1$-regular, sparse graphs and the density according to (1) is

$$\frac{q+1}{2(q+\ldots+q^n)+1}.$$

Each of the representatives of the presented family is $q+1$-regular graph so the first eigenvalue of the adjacency matrix, corresponding to this graph, is $\lambda_0=q+1$. Let us denote the second eigenvalue by $\lambda_1=\max_{\lambda_i\neq q+1}|\lambda_i|$. Tab. 4 present comparison between presented families and generalized regular polygons for $n=3,4,5$.

The graphs $\Gamma(4,\phi_4^+,\mathbb{F}_q)$ have a structure which is some aspects similar to generalized quadrangle. They are $q+1$ regular graphs and have the same number of vertices. However, he constructed graphs for $n=4$ are not isomorphic to generalized quadrangles. In [**2**] we showed that second largest eigenvalue of graph $\Gamma(4,\phi_4^+,\mathbb{F}_q)$ is $\sqrt{3q}$ (for $q=3,4,5,7,8,9,11,13,16,17,19,23$). The second largest eigenvalue of regular generalized quadrangle is $\sqrt{2q}$ for arbitrary q. What's more generalized quadrangle has girth 8 and graphs $\Gamma(4,\phi_4^+,\mathbb{F}_q)$ has girth 6. There is an conjecture that $\lambda_1=\sqrt{3q}$ for graph $\Gamma(4,\phi_4^+,\mathbb{F}_q)$ for arbitrary large q, [**2**]. The following conclusion can be drawn from this observation.

Corollary 1. The graphs $\Gamma(4,\phi_4^+,\mathbb{F}_q)$ are not isomorphic to generalized quadrangles.

Let us prove the theorems introduced in [**2**].

Theorem 1. Family of graphs $\Gamma(4, \phi_4^+, \mathbb{F}_q)$ is a family of graphs of girth 6.

Proof. Graphs $\Gamma(4, \phi_4^+, \mathbb{F}_q)$ are bipartite so there is no cycle C_3 and C_5. Each vertex of type t_k have q neighbours of type t_{k+1} and one each vertex have four neighbour of type t_{k-1}, for $k = 1, 2$. Each vertex of type t_3 have q neighbours of type t_3 and one each vertex have four neighbour of type t_2. Because of the structure of this family we can consider only three possibilities of form of the cycle C_4:

(1) There exist a cycle C_4 passing through two points of type t_3 and two lines of type t_3. Let us note that incidence relations among vertices of type t_3 are the same as incidence relations among vertices in graph $D(3, q)$, [**13**]. From [**13**] we know that the girth of graphs $D(3, q)$ is 8 so cycle of such type do not exist.

(2) There exists two points $(\dot{p})$ of type t_2 and $(\ddot{p})$ of type t_3 which have two common neighbours of type t_3: $[\dot{l}]$, $[\ddot{l}]$, such that $[\dot{l}] \neq [\ddot{l}]$. Cycle C_4 has a form $(\dot{p})I[\dot{l}]I(\ddot{p})I[\ddot{l}]I(\dot{p})$. If cycle of such type exist then:

$$(\dot{p})I[\dot{l}] \Leftrightarrow ((4), \dot{p_1}, \dot{p_2})I[[3,4], \dot{l_1}, \dot{l_2}, \dot{l_3}] \Leftrightarrow \dot{p_1} = \dot{l_1} \wedge \dot{p_2} = \dot{l_2},$$

$$(\dot{p})I[\ddot{l}] \Leftrightarrow ((4), \dot{p_1}, \dot{p_2})I[[3,4], \ddot{l_1}, \ddot{l_2}, \ddot{l_3}] \Leftrightarrow \dot{p_1} = \ddot{l_1} \wedge \dot{p_2} = \ddot{l_2},$$

$$(\ddot{p})I[\dot{l}] \Leftrightarrow ((3), \ddot{p_1}, \ddot{p_2}, \ddot{p_3})I[[3,4], \dot{l_1}, \dot{l_2}, \dot{l_3}] \Leftrightarrow$$

$$((3), \ddot{p_1}, \ddot{p_2}, \ddot{p_3})I[[3,4], \dot{p_1}, \dot{p_2}, \dot{l_3}] \Leftrightarrow$$

$$\begin{cases} \dot{p_2} - \ddot{p_2} &= \ddot{p_1}\dot{p_1} \\ \dot{l_3} - \ddot{p_3} &= \ddot{p_1}\dot{p_2} \end{cases} \Rightarrow$$

$$\dot{l_3} = \ddot{p_1}\dot{p_2} + \ddot{p_3},$$

$$(\ddot{p})I[\ddot{l}] \Leftrightarrow ((3), \ddot{p_1}, \ddot{p_2}, \ddot{p_3})I[[3,4], \ddot{l_1}, \ddot{l_2}, \ddot{l_3}] \Leftrightarrow$$

$$((3), \ddot{p_1}, \ddot{p_2}, \ddot{p_3})I[[3,4], \dot{p_1}, \dot{p_2}, \ddot{l_3}] \Leftrightarrow$$

$$\begin{cases} \dot{p_2} - \ddot{p_2} &= \ddot{p_1}\dot{p_1} \\ \ddot{l_3} - \ddot{p_3} &= \ddot{p_1}\dot{p_2} \end{cases} \Rightarrow$$

$$\ddot{l_3} = \ddot{p_1}\dot{p_2} + \ddot{p_3}.$$

We obtain dependence $\dot{l_1} = \ddot{l_1} \wedge \dot{l_2} = \ddot{l_2} \wedge \dot{l_3} = \ddot{l_3} \Leftrightarrow [\dot{l}] = [\ddot{l}]$. This contradicts our assumption that $[\dot{l}] \neq [\ddot{l}]$. Therefore the initial assumption that such type of cycle C_4 exist must be false.

(3) There exists two lines $[\dot{l}]$ of type t_2 and $[\ddot{l}]$ of type t_3 which have two common neighbors of type t_3: $(\dot{p})$, $(\ddot{p})$, such that $(\dot{p}) \neq (\ddot{p})$. Cycle C_4 has a form $[\dot{l}]I(\dot{p})I[\ddot{l}]I(\ddot{p})I[\dot{l}]$ If cycle of this type exist then:

$$[\dot{l}]I(\dot{p}) \Leftrightarrow [[2,3], \dot{l_1}, \dot{l_2}]I((3), \dot{p_1}, \dot{p_2}, \dot{p_3}) \Leftrightarrow$$

$$\dot{l_1} = \dot{p_1} \wedge \dot{p_2} - \dot{l_2} = \dot{p_3}\dot{l_1},$$

$$[\dot{l}]I(\ddot{p}) \Leftrightarrow [[2,3], \dot{l_1}, \dot{l_2}]I((3), \ddot{p_1}, \ddot{p_2}, \ddot{p_3}) \Leftrightarrow$$

$$\dot{l_1} = \ddot{p_1} \wedge \ddot{p_2} - \dot{l_2} = \ddot{p_3}\dot{l_1},$$

$$[\ddot{l}]I(\dot{p}) \Leftrightarrow [[3,4], \ddot{l_1}, \ddot{l_2}, \ddot{l_3}]I((3), \dot{p_1}, \dot{p_2}, \dot{p_3}) \Leftrightarrow$$

$$[[3,4], \ddot{l_1}, \ddot{l_2}, \ddot{l_3}]I((3), \dot{l_1}, \dot{p_2}, \dot{p_3}) \Leftrightarrow$$

$$\begin{cases} \ddot{l_2} - \dot{p_2} &= \ddot{l_1}\dot{l_1} \\ \ddot{l_3} - \dot{p_3} &= \ddot{l_2}\dot{l_1} \end{cases} \Leftrightarrow$$

$$\begin{cases} \dot{p_2} &= \ddot{l_2} - \ddot{l_1}\dot{l_1} \\ \dot{p_3} &= \ddot{l_3} - \ddot{l_2}\dot{l_1} \end{cases},$$

$$[\ddot{l}]I(\ddot{p}) \Leftrightarrow [[3,4], \ddot{l_1}, \ddot{l_2}, \ddot{l_3}]I((3), \ddot{p_1}, \ddot{p_2}, \ddot{p_3}) \Leftrightarrow$$

$$[[3,4], \ddot{l_1}, \ddot{l_2}, \ddot{l_3}]I((3), \dot{l_1}, \ddot{p_2}, \ddot{p_3}) \Leftrightarrow$$

$$\begin{cases} \ddot{l_2} - \ddot{p_2} &= \ddot{l_1}\dot{l_1} \\ \ddot{l_3} - \ddot{p_3} &= \ddot{l_2}\dot{l_1} \end{cases} \Leftrightarrow$$

$$\begin{cases} \ddot{p_2} &= \ddot{l_2} - \ddot{l_1}\dot{l_1} \\ \ddot{p_3} &= \ddot{l_3} - \ddot{l_2}\dot{l_1} \end{cases}$$

We obtain dependence $\dot{p_1} = \ddot{p_1} \wedge \dot{p_2} = \ddot{p_2} \wedge \dot{p_3} = \ddot{p_3} \Leftrightarrow (\dot{p}) = (\ddot{p})$ This contradicts our assumption that $(\dot{p}) \neq (\ddot{p})$. Therefore the initial assumption that such C_4 exist must be false.

For an arbitrary prime power q in $\Gamma(4, \phi_4^+, \mathbb{F}_q)$ there is a cycle of length 6:

$$[[3,4], 0, 0, 1]I((4), 0, 0)I[[3,4], 0, 0, 0]I((3), 0, 0, 0)$$

$$I[[2,3], 0, 0]I((3), 0, 0, 1)I[[3,4], 0, 0, 1].$$

□

Analogous proof can be performed for the graph $\Gamma(5, \phi_5^+, \mathbb{F}_q)$.

Theorem 2. Family of graphs $\Gamma(5, \phi_5^+, \mathbb{F}_q)$ is a family of graphs of girth 8.

Proof. Graphs $\Gamma(5, \phi_5^+, \mathbb{F}_q)$ are bipartite so there is no cycle C_3, C_5 and C_7. This graphs have representation as symmetric adjacency matrices so without loss of generality we can consider only two possibilities of form of the cycle C_4:

(1) There exist a cycle C_4 passing through two points of type t_4 and two lines of type t_4. However, if we rewrite relations among vertices of type t_4 as follows: $p_3 := p_2$, $p_2 := p_4$, $p_4 := p_3$, $l_3 := l_2$, $l_2 := l_3$ we obtain the same relations as among vertices in graph $D(4, q)$, [**13**]. From [**13**] we know that the girth f graphs $D(4, q)$ is 8 so cycle of this type do not exist.

(2) There exist a cycle C_4 passing through two points of type t_3 and two lines of type t_4. Let us note that incidence relations among vertices of type t_3 are the same as incidence relations among vertices in graph $D(3, q)$, [**13**]. From [**13**] we know that the girth f graphs $D(n, q)$ is 8 so cycle of such type do not exist.

$$(\dot{p})I[\dot{l}] \Leftrightarrow ((3), \dot{p_1}, \dot{p_2}, \dot{p_3})I[[3,4], \dot{l_1}, \dot{l_2}, \dot{l_3}, \dot{l_4}] \Leftrightarrow$$

$$\begin{cases} \dot{p_1} &= \dot{l_1} \\ \dot{p_2} - \dot{l_2} &= \dot{p_1}\dot{l_3} + \dot{p_3}\dot{l_1} \\ \dot{p_3} &= \dot{l_3} \end{cases}$$

$$(\dot{p})I[\ddot{l}] \Leftrightarrow ((3), \dot{p_1}, \dot{p_2}, \dot{p_3})I[[3,4], \ddot{l_1}, \ddot{l_2}, \ddot{l_3}, \ddot{l_4}] \Leftrightarrow$$

$$\begin{cases} \dot{p_1} &= \ddot{l_1} \\ \dot{p_2} - \ddot{l_2} &= \dot{p_1}\ddot{l_3} + \dot{p_3}\ddot{l_1} \\ \dot{p_3} &= \ddot{l_3} \end{cases}$$

Hence $\dot{l_1} = \ddot{l_1}$, $\dot{l_3} = \ddot{l_3}$ and $\dot{l_2} = \ddot{l_2} = \hat{l_2}$.

$$(\ddot{p})I[\dot{l}] \Leftrightarrow ((4), \ddot{p_1}, \ddot{p_2}, \ddot{p_3})I[[3,4], \dot{l_1}, \dot{l_2}, \dot{l_3}, \dot{l_4}] \Leftrightarrow$$

$$((4), \ddot{p_1}, \ddot{p_2}, \ddot{p_3})I[[3,4], \dot{p_1}, \hat{l_2}, \dot{p_3}, \dot{l_4}] \Rightarrow$$

$$\ddot{p_2} - \dot{l_4} = \ddot{p_1}\dot{p_3}$$

$$(\ddot{p})I[\ddot{l}] \Leftrightarrow ((4), \ddot{p_1}, \ddot{p_2}, \ddot{p_3})I[[3,4], \ddot{l_1}, \ddot{l_2}, \ddot{l_3}, \ddot{l_4}] \Leftrightarrow$$

$$((4), \ddot{p_1}, \ddot{p_2}, \ddot{p_3})I[[3,4], \dot{p_1}, \hat{l_2}, \dot{p_3}, \ddot{l_4}] \Rightarrow$$

$$\ddot{p_2} - \ddot{l_4} = \ddot{p_1}\dot{p_3}$$

We obtain dependence $\dot{l_1} = \ddot{l_1} \wedge \dot{l_2} = \ddot{l_2} \wedge \dot{l_3} = \ddot{l_3} \wedge \dot{l_4} = \ddot{l_4} \Leftrightarrow [\dot{l}] = [\ddot{l}]$. This contradicts our assumption that $[\dot{l}] \neq [\ddot{l}]$. Therefore the initial assumption that such type of cycle C_4 exist must be false.

Because of the symmetric nature of this family we can consider only four possibilities of form of the cycle C_6:

(1) There exist a cycle C_6 passing through three points of type t_4 and three lines of type t_4. However, if we rewrite relations among vertices of type t_4 as follows: $p_3 := p_2$, $p_2 := p_4$, $p_4 := p_3$, $l_3 := l_2$, $l_2 := l_3$ we obtain the same relations as among vertices in graph $D(4,q)$, [**13**]. From [**13**] we know that the girth f graphs $D(4,q)$ is 8 so cycle of this type do not exist.

(2) There exist cycle C_6 contained point $(p) = ((3), p_1, p_2, p_3)$ of type t_3, two points $(\dot{p})$ and $(\ddot{p})$ $((\dot{p}) \neq (\ddot{p}))$ of type t_4 and three different lines $[l], [\dot{l}], [\ddot{l}]$ of type t_4. Cycle C_6 has a form $(p)I[\dot{l}](\dot{p})I[l]I(\ddot{p})I[\ddot{l}]I(p)$. If cycle of this type exist then:

$$(p)I[\dot{l}] \Leftrightarrow ((3), p_1, p_2, p_3)I[[3,4], \dot{l_1}, \dot{l_2}, \dot{l_3}, \dot{l_4}] \Leftrightarrow$$

$$\begin{cases} p_1 &= \dot{l_1} \\ p_2 - \dot{l_2} &= p_1\dot{l_3} + p_3\dot{l_1} \\ p_3 &= \dot{l_3} \end{cases},$$

$$(p)I[\ddot{l}] \Leftrightarrow ((3), p_1, p_2, p_3)I[[3,4], \ddot{l_1}, \ddot{l_2}, \ddot{l_3}, \ddot{l_4}] \Leftrightarrow$$

$$\begin{cases} p_1 &= \ddot{l_1} \\ p_2 - \ddot{l_2} &= p_1\ddot{l_3} + p_3\ddot{l_1} \\ p_3 &= \ddot{l_3} \end{cases},$$

and we see that $\dot{l_1} = \ddot{l_1} = p_1$, $\dot{l_2} = \ddot{l_2} = \hat{l_2}$, $\dot{l_3} = \ddot{l_3} = p_3$.

$$[l]I(\dot{p}) \Rightarrow [[3,4], l_1, l_2, l_3, l_4]I((4), \dot{p_1}, \dot{p_2}, \dot{p_3}, \dot{p_4}) \Leftrightarrow$$

$$\begin{cases} \dot{p_2} - l_4 &= \dot{p_1}l_3 \\ \dot{p_3} - l_3 &= \dot{p_1}l_1 \\ \dot{p_4} - l_2 &= \dot{p_3}l_1 \end{cases},$$

$$[l]I(\ddot{p}) \Rightarrow [[3,4], l_1, l_2, l_3, l_4]I((4), \ddot{p_1}, \ddot{p_2}, \ddot{p_3}, \ddot{p_4}) \Leftrightarrow$$

$$\begin{cases} \ddot{p_2} - l_4 &= \ddot{p_1}l_3 \\ \ddot{p_3} - l_3 &= \ddot{p_1}l_1 \\ \ddot{p_4} - l_2 &= \ddot{p_3}l_1 \end{cases},$$

$$(\dot{p})I[\dot{l}] \Leftrightarrow ((4), \dot{p_1}, \dot{p_2}, \dot{p_3}, \dot{p_4})I[[3,4], \dot{l_1}, \dot{l_2}, \dot{l_3}, \dot{l_4}] \Leftrightarrow$$

$$((4), \dot{p_1}, \dot{p_2}, \dot{p_3}, \dot{p_4})I[[3,4], p_1, \hat{l_2}, p_3, \dot{l_4}] \Leftrightarrow$$

$$\begin{cases} \dot{p_2} - \dot{l_4} &= \dot{p_1}p_3 \\ \dot{p_3} - p_3 &= \dot{p_1}p_1 \\ \dot{p_4} - \hat{l_2} &= \dot{p_3}p_1 \end{cases},$$

$$(\ddot{p})I[\ddot{l}] \Leftrightarrow ((4), \ddot{p_1}, \ddot{p_2}, \ddot{p_3}, \ddot{p_4})I[[3,4], \ddot{l_1}, \ddot{l_2}, \ddot{l_3}, \ddot{l_4}] \Leftrightarrow$$

$$((4), \ddot{p_1}, \ddot{p_2}, \ddot{p_3}, \ddot{p_4})I[[3,4], p_1, \hat{l_2}, p_3, \ddot{l_4}] \Leftrightarrow$$

$$\begin{cases} \ddot{p_2} - \ddot{l_4} &= \ddot{p_1}p_3 \\ \ddot{p_3} - p_3 &= \ddot{p_1}p_1 \\ \ddot{p_4} - \hat{l_2} &= \ddot{p_3}p_1 \end{cases},$$

We can write variables $\dot{p_3}$ and $\ddot{p_3}$ in two ways:

$$\dot{p_3} = l_3 + \dot{p_1}l_1 = p_3 + \dot{p_1}p_1,$$

$$\ddot{p_3} = l_3 + \ddot{p_1}l_1 = p_3 + \ddot{p_1}p_1,$$

It is easy to see that $\dot{p_1} = \ddot{p_1}$ and $\dot{p_3} = \ddot{p_3}$. Therefore $\dot{p_2} = \ddot{p_2}$, $\dot{p_4} = \ddot{p_4}$. We obtain that $(\dot{p}) = (\ddot{p})$. This contradicts our assumption that $(\dot{p}) \neq (\ddot{p})$. Therefore the initial assumption that such C_6 exist must be false.

(3) Between point $(p) = ((3), p_1, p_2, p_3)$ of type t_3 and line $[l] = [[4,5], l_1, l_2, l_3]$ of type t_3 there exist two different paths: $[l]I(\dot{p})I[\dot{l}]I(p)$ and $[l]I(\ddot{p})I[\ddot{l}]I(p)$, where $(\dot{p}) \neq (\ddot{p})$, $[\dot{l}] \neq [\ddot{l}]$ and $(\dot{p}), (\ddot{p}), [\dot{l}], [\ddot{l}]$ are of type t_4. Cycle C_6 has a form $[l]I(\dot{p})I[\dot{l}]I(p)I[\ddot{l}]I(\ddot{p})I[l]$. If cycle of this type exist then:

$$[l]I(\dot{p}) \Leftrightarrow [[4,5], l_1, l_2, l_3]I((4), \dot{p_1}, \dot{p_2}, \dot{p_3}, \dot{p_4}) \Leftrightarrow$$

$$\begin{cases} \dot{p_1} &= l_1 \\ \dot{p_2} - l_2 &= \dot{p_3}l_1 + \dot{p_1}l_3 \\ \dot{p_3} &= l_3 \end{cases},$$

$$[l]I(\ddot{p}) \Leftrightarrow [[4,5], l_1, l_2, l_3]I((4), \ddot{p_1}, \ddot{p_2}, \ddot{p_3}, \ddot{p_4}) \Leftrightarrow$$

$$\begin{cases} \ddot{p_1} &= l_1 \\ \ddot{p_2} - l_2 &= \ddot{p_3}l_1 + \ddot{p_1}l_3 \\ \ddot{p_3} &= l_3 \end{cases},$$

and we see that $\dot{p_1} = \ddot{p_1} = l_1$, $\dot{p_2} = \ddot{p_2} = \hat{p_2}$, $\dot{p_3} = \ddot{p_3} = l_3$.

$$(p)I[\dot{l}] \Leftrightarrow ((3), p_1, p_2, p_3)I[[3,4], \dot{l_1}, \dot{l_2}, \dot{l_3}, \dot{l_4}] \Leftrightarrow$$

$$\begin{cases} p_1 &= \dot{l_1} \\ p_2 - \dot{l_2} &= p_3\dot{l_1} + p_1\dot{l_3} \\ p_3 &= \dot{l_3} \end{cases},$$

$$(p)I[\ddot{l}] \Leftrightarrow ((3), p_1, p_2, p_3)I[[3,4], \ddot{l_1}, \ddot{l_2}, \ddot{l_3}, \ddot{l_4}] \Leftrightarrow$$

 DOI: 10.1515/umcsinfo-2015-0006

$$\begin{cases} p_1 &= \ddot{l_1} \\ p_2 - \ddot{l_2} &= p_3\ddot{l_1} + p_1\ddot{l_3} \\ p_3 &= \ddot{l_3} \end{cases},$$

and we see that $\dot{l_1} = \ddot{l_1} = p_1$, $\dot{l_2} = \ddot{l_2} = \hat{l_2}$, $\dot{l_3} = \ddot{l_3} = p_3$.

$(\dot{p})I[\dot{l}] \Leftrightarrow ((4), \dot{p_1}, \dot{p_2}, \dot{p_3}, \dot{p_4})I[[3,4], \dot{l_1}, \dot{l_2}, \dot{l_3}, \dot{l_4}] \Leftrightarrow$

$((4), l_1, \hat{p_2}, l_3, \dot{p_4})I[[3,4], p_1, \hat{l_2}, p_3, \dot{l_4}] \Rightarrow$

$$\begin{cases} \hat{p_2} - \dot{l_4} &= l_1 p_3 \\ \dot{p_4} - \hat{l_2} &= l_3 p_1 \end{cases},$$

$(\ddot{p})I[\ddot{l}] \Leftrightarrow ((4), \ddot{p_1}, \ddot{p_2}, \ddot{p_3}, \ddot{p_4})I[[3,4], \ddot{l_1}, \ddot{l_2}, \ddot{l_3}, \ddot{l_4}] \Leftrightarrow$

$((4), l_1, \hat{p_2}, l_3, \ddot{p_4})I[[3,4], p_1, \hat{l_2}, p_3, \ddot{l_4}] \Rightarrow$

$$\begin{cases} \hat{p_2} - \ddot{l_4} &= l_1 p_3 \\ \ddot{p_4} - \hat{l_2} &= l_3 p_1 \end{cases}$$

We obtain that $\dot{p_4} = \ddot{p_4}$, $\dot{l_4} = \ddot{l_4}$ so $(\dot{p}) = (\ddot{p})$ and $[\dot{l}] = [\ddot{l}]$. This contradicts our assumptions that $(\dot{p}) \neq (\ddot{p})$ and $[\dot{l}] \neq [\ddot{l}]$. Therefore the initial assumption that such C_6 exist must be false.

(4) There exists point $(p) = ((5), p_1, p_2)$ of type t_2, which is connected with two lines of type t_3: $[\dot{l}]$, $[\ddot{l}]$ ($[\dot{l}] \neq [\ddot{l}]$) and line $[l] = [[3,4], l_1, l_2, l_3, l_4]$ of type t_4 which is connected with two points of type t_4: $(\dot{p})$, $(\ddot{p})$ ($(\dot{p}) \neq (\ddot{p})$). We have $(\dot{p})I[\dot{l}]$ and $(\ddot{p})I[\ddot{l}]$. Cycle C_6 has a form $(p)I[\dot{l}]I(\dot{p})I[l]I(\ddot{p})I[\ddot{l}]I(p)$. If cycle of this type exist then:

$(p)I[\dot{l}] \Leftrightarrow ((5), p_1, p_2)I[[4,5], \dot{l_1}, \dot{l_2}, \dot{l_3}] \Leftrightarrow$

$$\begin{cases} p_1 &= \dot{l_1} \\ p_2 - \dot{l_2} &= \dot{l_3} p_1 \end{cases},$$

$(p)I[\ddot{l}] \Leftrightarrow ((5), p_1, p_2)I[[4,5], \ddot{l_1}, \ddot{l_2}, \ddot{l_3}] \Leftrightarrow$

$$\begin{cases} p_1 &= \ddot{l_1} \\ p_2 - \ddot{l_2} &= \ddot{l_3} p_1 \end{cases},$$

$[\dot{l}]I(\dot{p}) \Leftrightarrow [[4,5], \dot{l_1}, \dot{l_2}, \dot{l_3}]I((4), \dot{p_1}, \dot{p_2}, \dot{p_3}, \dot{p_4}) \Leftrightarrow$

$$\begin{cases} \dot{p_1} &= \dot{l_1} \\ \dot{p_2} - \dot{l_2} &= \dot{p_3}\dot{l_1} + \dot{p_1}\dot{l_3} \\ \dot{p_3} &= \dot{l_3} \end{cases},$$

$[\ddot{l}]I(\ddot{p}) \Leftrightarrow [[4,5], \ddot{l_1}, \ddot{l_2}, \ddot{l_3}]I((4), \ddot{p_1}, \ddot{p_2}, \ddot{p_3}, \ddot{p_4}) \Leftrightarrow$

$$\begin{cases} \ddot{p_1} &= \ddot{l_1} \\ \ddot{p_2} - \ddot{l_2} &= \ddot{p_3}\ddot{l_1} + \ddot{p_1}\ddot{l_3} \\ \ddot{p_3} &= \ddot{l_3} \end{cases},$$

From the above equations we obtain $\dot{p_1} = \ddot{p_1} = \dot{l_1} = \ddot{l_1} = p_1$.

$[l]I(\dot{p}) \Leftrightarrow [[3,4], l_1, l_2, l_3, l_4]I((4), \dot{p_1}, \dot{p_2}, \dot{p_3}, \dot{p_4}) \Leftrightarrow$

$[[3,4], l_1, l_2, l_3, l_4]I((4), p_1, \dot{p_2}, \dot{p_3}, \dot{p_4}) \Leftrightarrow$

$$\begin{cases} \dot{p_2} - l_4 &= l_3 p_1 \\ \dot{p_3} - l_3 &= l_1 p_1 \\ \dot{p_4} - l_3 &= l_1 \dot{p_3} \end{cases}$$

$[l]I(\ddot{p}) \Leftrightarrow [[3,4], l_1, l_2, l_3, l_4]I((4), \ddot{p_1}, \ddot{p_2}, \ddot{p_3}, \ddot{p_4}) \Leftrightarrow$

$[[3,4], l_1, l_2, l_3, l_4]I((4), p_1, \ddot{p_2}, \ddot{p_3}, \ddot{p_4}) \Leftrightarrow$

$$\begin{cases} \ddot{p_2} - l_4 &= l_3 p_1 \\ \ddot{p_3} - l_3 &= l_1 p_1 \\ \ddot{p_4} - l_3 &= l_1 \ddot{p_3} \end{cases}$$

We see that $(\dot{p_2} = \ddot{p_2} \wedge \dot{p_3} = \ddot{p_3}) \Rightarrow \dot{p_4} = \ddot{p_4}$ and so $(\dot{p}) = (\ddot{p})$. This contradicts our assumption that $(\dot{p}) \neq (\ddot{p})$. Therefore the initial assumption that such C_6 exist must be false.

Graph $D(5,q)$ is a subgraph of $\Gamma(5, \phi_5^+, \mathbb{F}_q)$. For an arbitrary $q \geq 2$ graph the girth of graph $D(5,q)$ is 8 and so the girth of graph $\Gamma(5, \phi_5^+, \mathbb{F}_q)$ is 8 and it has a cycle of length 8. □

The graphs $\Gamma(n, \phi_n^+, \mathbb{F}_q)$ for arbitrary n, q are connected. What more we have conjecture that the families is $q+1$-connected, namely highly connected. A graph is said to be k-connected when there does not exist a set of $k-1$ vertices whose removal disconnects the graph. The connectivity of graphs is important property used in many practical and theoretical aspects. If (for fixed n) we remove vertices of type t_n from graph $\Gamma(n, \phi_n^+, \mathbb{F}_q)$ we obtain a tree.

4 Corresponding LDPC codes

An error-correcting code is an algorithm for expressing a sequence of numbers such that any errors which are introduced can be detected and corrected based on the remaining numbers. This techniques enable reliable delivery of digital data over unreliable communication channels. To a k bits message are added r extra bits-redundant data. As a result of this action we get the codewords $y \in C$ of the length N. Such a code has $r = N - k$ parity checks equations and is denoted by $[N, k]$. The ratio k/N is called code rate and is denoted by R_C.

LDPC code is one of the powerful class of error correcting codes, which was discovered by Robert Gallanger in his work Low-Density Parity-Check Codes [**14**]. They were forgotten for twenty years to get back in the nineties, for example see [**15, 16, 17**]. The ability to use graphs in construction of LDPC was first discussed by [**18**]. Construction of Tanner type codes based on the expander graphs was considered for example by Sipser and Spielman [**17**], Guinanad and Lodge [**19**]. In this paper we present irregular low-density parity-check (LDPC) codes which exhibit a performance extremely close to the Shannon limit. Irregular LDPC codes were introduced in [**20, 21**] and were further studied in [**22, 23**]. For such an irregular LDPC code, the degrees of each set of nodes are chosen according to some distribution. In case of regular LDPC codes the degree of each variable node is equal r and the degree of each check node is equal s. The corresponding Tanner graph is biregular (r, s). In the case of irregular codes the weight of rows and columns are varied.

An irregular LDPC code might have a graphical representation in which the set of variable nodes or the set of constraint nodes may be divided into subsets of different degree.

There are three ways to represent linear error correcting code allowing us to obtain LDPC codes: generator matrix G, parity check matrix H or Tanner graph $\Gamma(V, E)$. There is a standard way to create LDPC codes from bipartite, Tanner graph. Parity check matrix H and adjacency matrix A for used graph are dependent:

$$A = \begin{pmatrix} 0 & \mathrm{H} \\ H^T & 0 \end{pmatrix}.$$

Presented construction leads us to families of graphs that can be successfully used in coding theory to create LDPC codes because they: are simple undirected graphs, do not have cycles of length less than 8, have structures that allow us to obtain arbitrary code rate R_C, work with existing decoding algorithm, have representation as very sparse matrices H.

Our simulations were done using BPSK modulation over AWGN channel and simple belief-propagation (BP) decoder implementation with 10 iterations. Efficacy BP algorithm is only slightly worse than the optimum MAP decoding. Let y be the received codeword. MAP decoder works accordingly to the rule which returns an output value $\hat{x}$ of a code word x for which the *a posteriori* probability $P = (x|y, H)$ is maximized. BP algorithm consists in calculating the approximate values of the *a posteriori* probabilities $P = (x_i|y, H)$ for the different receiver bits of the codeword x until the hard decisions taken on the basis of these probabilities will indicate one of the possible code words or the maximum number of iterations will be reached. The use of iterative decoding is especially useful in the case of LDPC codes as the computational complexity of the decoding process for sparse matrix depends linearly on the length of the codeword.

Obtained graphs are $q+1$ regular and $|P| = |L|$. To create LDPC code the number of vertices in one partition set should be much less than the in second one (for example $|P| \leq |L|$). We can use method described in **[24]** for graphs $D(n, q)$. To obtain bipartite graph with $|P| \leq |L|$ we must put restriction on coordinates of points. Let $E \subset \mathbb{F}_q$ be an e-element subset respectively and let V_P and V_L be sets of points and lines in a new bipartite graph. They are the following sets:

$$V_P = \{(p) \in P | p_2 \in E\},$$
$$V_L = \{[l] \in L | \deg([l]) \geq 2\}.$$

The bigger set V_L corresponds to codeword bits and the smaller V_P to parity checks. By this algorithm we obtain irregular LDPC codes. This irregular LDPC codes have a graphical representation in which one part of variable nodes have degree $|E|$,second part have degree $|E|+1$ and third part have degree $q+1$.

TABLE 5. Properties of graphs used for presented in figures sample codes if $p_2 \in E$

Initial graph	E	Number of lines in used subgraph	Number of points in used subgraph	Code rate
$\Gamma(4, \phi_4^+, \mathbb{F}_5)$	$\{0, 1\}$	138	66	≈ 0.52
$\Gamma(4, \phi_4^+, \mathbb{F}_7)$	$\{0, 1\}$	360	120	0.(6)
$\Gamma(4, \phi_4^+, \mathbb{F}_7)$	$\{0, 1, 2\}$	368	176	≈ 0.52
$\Gamma(4, \phi_4^+, \mathbb{F}_{11})$	$\{0, 1, 2, 3, 4\}$	1392	672	0.52
$\Gamma(5, \phi_5^+, \mathbb{F}_5)$	$\{0, 1\}$	682	311	≈ 0.55
$\Gamma(5, \phi_5^+, \mathbb{F}_7)$	$\{0, 1\}$	2516	806	≈ 0.68
$\Gamma(5, \phi_5^+, \mathbb{F}_7)$	$\{0, 1, 2\}$	2573	1205	≈ 0.53

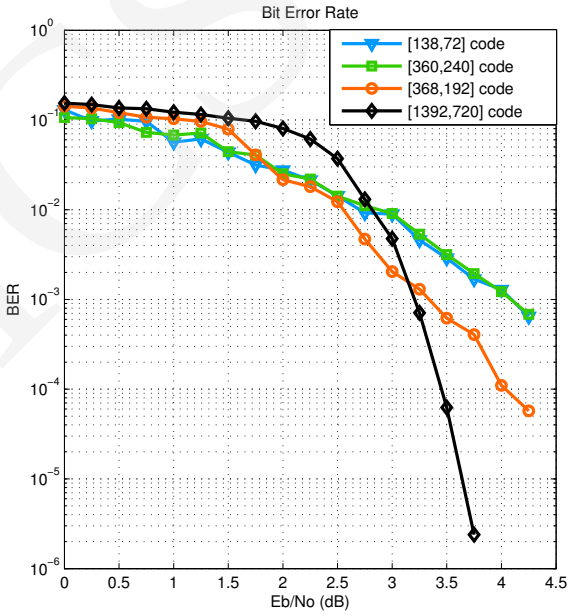

FIGURE 1. Bit error rate for codes based on $\Gamma(4, \phi_4^+, \mathbb{F}_q)$

Bidegree reduction can only increase the girth so there is no short cycles. After bidegree reduction the graph may be disconnected and divided into several components. To create a parity check matrix we use only one component. We decide to put one or zero in a parity check matrix by checking if relations presented in Tab. 2 or Tab. 3 among coordinates for each point and line are satisfied. Tab. 5 presents properties of example codes obtained from graphs $\Gamma(4, \phi_4^+, \mathbb{F}_q)$ and $\Gamma(5, \phi_5^+, \mathbb{F}_q)$. Fig. 1 and Fig. 2 show Bit Error Rate for this representatives.

 DOI: 10.1515/umcsinfo-2015-0006

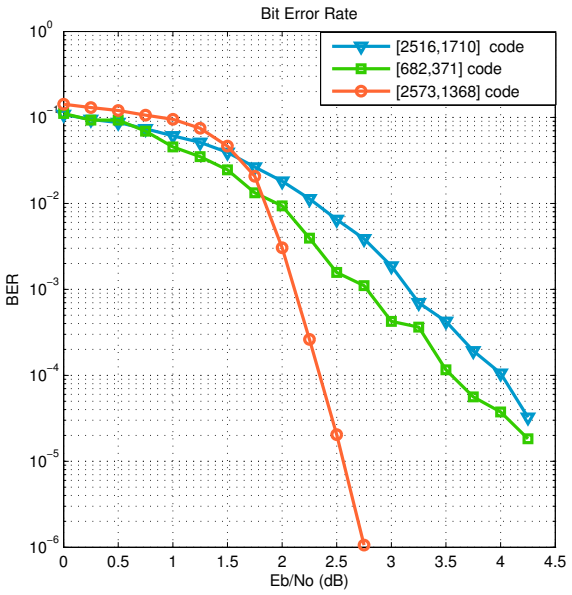

FIGURE 2. Bit error rate for codes based on $\Gamma(5, \phi_5^+, \mathbb{F}_q)$

References

[1] D. Gillman, A Chernoff bound for random walks on expander graphs, SIAM J. Comput. 27 (4) (1998): 1203.

[2] M. Polak, V. Ustimenko, On new expanders of unbounded degree for practical applications in Informatics, Dopovidi Nacionalńoj Akademii Nauk Ukrain 12 (2014): 44.

[3] M. Polak, V. Ustimenko, Examples of Ramanujan and expander graphs for practical applications, Proceedings of the 2013 Federated Conference on Computer Science and Information Systems (2013): 499.

[4] B. Bollobas, Extremal Graph Theory, Academic Press (1978).

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

[6] A. Brouwer, A. Cohen, A. Neumaier, Distance-Regular Graphs, Springer-Verlag (1989).

[7] S. Hoory, N. Linial, A. Wigderson, Expander graphs and their applications, Bulletin (New Series) of the American Mathematical Society 43 (2006): 439.

[8] G.A. Margulis, Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators, Problemy Peredachi Informatsii 24 (1) (1988): 51.

[9] A. Lubotsky, R. Philips, P. Sarnak, Ramanujan graphs, Combinatorica 9 (1988): 261.

[10] R. Weiss, Distance transitive graphs and generalised polygons, Arch. Math 45 (1985): 186.

[11] W. Feit, D. Higman, The nonexistence of certain generalised polygons, J. of Algebra 1 (1964): 114.

[12] V. A. Ustimenko, On some properties of geometries of the Chevalley groups and their general- izations, Studies in Algebraic Theory of Combinatorial Objects, Moskow; English transl, Kluwer Publ., Dordresht (1991): 112.

[13] F. Lazebnik, V. A. Ustimenko, A. J. Woldar, A new series of dense graphs of high girth, Bulletin (New Series) of the AMS 32 (1995): 73.

[14] R. G. Gallager, Low-Density Parity-Check Codes, Monograph, M.I.T. Press (1963).

[15] M. Luby, M. Mitzenmacher, M. A. Shokrollahi, D. A. Spielman, Improved Low-Density Parity- Check Codes Using Irregular Graphs and Belief Propagation, ISIT 98-IEEE International Symposium of Information Theory, Cambridge, USA (1998): 171.

[16] D. J. C. MacKay, Good error-correcting codes based on very sparse matrices, Information Theory, IEEE Transactions 45 (2) (1999): 399.

[17] M. Sipser, D. A. Spielman, Expander codes, IEEE Trans on Info Theory, 42 (6) (1996): 1710.

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

[19] P. Guinand, J. Lodge, Tanner type codes arising from large girth graphs, in Canadian Workshop on Information Theory CWIT, Toronto, Ontario, Canada (1997): 5.

[20] M. Luby, M. Mitzenmacher, M. A. Shokrollahi, D. A. Spielman, and V. Stemann, Practical loss-resilient codes, Proc. 29th Annu. ACM Symp. Theory of Computing (1997): 150.

[21] M. Luby, M. Mitzenmacher, M. A. Shokrollahi, D. A. Spielman, Analysis of low density codes and improved designs using irregular graphs, Proc. 30th Annu. ACM Symp. Theory of Computing (1998): 249.

[22] D. MacKay, S. Wilson, M. Davey, Comparison of constructions of irregular Gallager codes, IEEE Trans. Commun. 47 (Oct. 1999): 1449.

[23] M. Luby, M. Mitzenmacher , M. A. Shokrollahi , D. A. Spielman, and V. Ste- mann, Practical loss-resilient codes, IEEE Trans. Inform. Theory 47 (2001): 569.

[24] F. Lazebnik, V. A. Ustimenko, Explicit construction of graphs with an arbitrary large girth and of large size, Discrete Applied Mathematics 60 (1995): 275.