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

Monika Polak¹,*, Vasyi Ustimenko¹†

¹Institute of Mathematics, Maria Curie-Skłodowska University,
pl. M. Curie-Skłodowskiej 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 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 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

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

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 bipartite one if the number of neighbours for vertices from each partition sets are constants $s$ and $t$ (idegrees). 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 $\theta$ 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 $\theta$-regular graphs can be estimated via upper limit $q - \lambda_n, n \to \infty$, where $\lambda_n$ 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 $\theta$-regular graphs with constant $\theta$ satisfy the inequality $\lambda \geq 2\sqrt{\theta - 1} - o(1)$, where $\lambda$ is the second largest eigenvalue in absolute value. Ramanujan graphs are $\theta$-regular graphs for which the inequality $\lambda \leq 2\sqrt{\theta - 1}$ holds. It is clear that a family of Ramanujan graphs of bounded degree $\theta$ 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 $\geq 3$) 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:
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
expaneder 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 to
connected $q+1$ regular graphs of order $2(1+q+\ldots+q^{n-1})$.

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 $\phi$ which is a configuration of vec-
tors in a Euclidean space satisfying certain geometrical
properties. In [2] we created a graph 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 algo-
rithm to choose a set of positive roots. There is only one
3-element set $\phi^+_3 = \{a_1, a_2, a_1 + a_2\}$. The sets $\phi^+_n$
consisting four elements are two: $\{a_1, a_2, a_1 + a_2, 2a_1 + a_2\}$
and $\{a_1, a_2, a_1 + a_2, 2a_1 + a_2\}$, but they are symmetric
and give the same results. There are three ways to choose
non-symmetric sets $\phi^+_n$: $\{a_1, a_2, a_1 + a_2, 2a_1 + a_2\}$
and $\{a_1, a_2, a_1 + a_2, 2a_1 + a_2\}$, but they are symmetric
and give the same results. There are three ways to choose
non-symmetric sets $\phi^+_n$: $\{a_1, a_2, a_1 + a_2, 2a_1 + a_2\}$
and $\{a_1, a_2, a_1 + a_2, 2a_1 + a_2\}$. 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 with different properties.
For $n = 5$ the set $\phi^+_n$ 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
$\Gamma(n,\phi^+_n, F_q)$ denote bipartite graph obtained by using
$n$-element set $\phi^+_n$, scalars from $F_q$ and binary operator
$\langle, \cdot \rangle$. 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 $V = P \cup L = \{1, 2, \ldots, n\}$
and $\{[1, 2], [2, 3], \ldots, [n-1, n], [n, 1]\}$. We can write the inci-
dence relation $I$ in $n$-gon as follows:

$$(m)I[s, t] \leftrightarrow m = s \lor m = t.$$ 

A line is incident with point if this point belong to this
line. Let vertex of type $t_i$ be define as vertex correspond-
ing to $e$-subset of $\phi^+_n$, $i = 0, 1, 2, \ldots, n-1$ and
let $A_i$ denote $e$-element closed subset of $\phi^+_n$. We create
two ascending sequences of closed subset of $\phi^+_n$.
Second element of first sequence is $\{a_1\}$ and for second sequence
element second is $\{a_2\}$:

$A_0 = \{\emptyset\} \subset A_1 = \{a_2\} \subset A_2 \subset A_3 \ldots \subset A_{n-1} = \phi^+_n \setminus \{a_1\}$,
$B_0 = \{\emptyset\} \subset B_1 = \{a_1\} \subset B_2 \subset B_3 \ldots \subset B_{n-1} = \phi^+_n \setminus \{a_2\}$.

For bigger $n$ set $\phi^+_n$ 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:
$B_0 = \{\emptyset\}, A_1 = \{a_2\}, B_2, A_3, \ldots, \phi^+_n \setminus \{a_1\}$ and for points
$A_0 = \{\emptyset\}, B_1 = \{a_1\}, A_2, B_3, \ldots, \phi^+_n \setminus \{a_2\}$, 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 $\Gamma(n,\phi^+_n, F_q)$ 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 $\ell_n-(1, a_1^\ast)$ and $[[1, 2], a_2^\ast]$

$2q$ elements of type $t_1-(2, a_1^\ast + p_{i_1} a_1)$ and $[[1, 2], a_2^\ast + l_{i_2} a_2]$,

$2q^2$ elements of type $t_2-(n, a_2^\ast + \sum_{a \in A_2} p_a a)$ and
$[[2, 3], a_1^\ast + \sum_{a \in B_2} l_{a} a]$,

$2q^{n-1}$ elements of type $t_{n-1}-(\sum_{a \in \phi^+_n \setminus \{a_i\}} \sum_{a \in \phi^+_n \setminus \{a_i\}} p_{a} a)$
and $\sum_{a \in \phi^+_n \setminus \{a_i\}} l_{a} a$,

where $i = 1$ and $j = 2$ if $n$ is odd and $i = 2$ and $j = 1$
in $n$ is even and $n = 2$ and $n = 2$ in $F_q$. Brackets and parenthesis
will allow the reader to distinguish points ($i$) and lines
$[i]$. The set of edges consists of all pairs $\{(p), [l]\}$ for
which $(p)I[l]$. The incidence relation $I_{\Gamma}$ for
the graph $\Gamma(n,\phi^+_n, F_q)$ is defined as follows. Let $v_1$ and $v_2$
be a closed subset of the set of positive roots $\phi^+_n$ and
let $\Sigma_p$ and $\Sigma_l$ be a linear combination of elements
of set $\psi_1$ and $\psi_2$ accordingly, with scalars from $F_q$.
Point $(p) = ([m], a_1^\ast + \Sigma_p)$ is incident to line $[l] = ([s, t], a_2^\ast + \Sigma_l)$
(we denote it by $(p)I[l]$) if and only if

$$(m = s \lor m = t) \land ([a_1^\ast + \Sigma_p, a_2^\ast + \Sigma_l])_{\psi_1 \cap \psi_2} = 0.$$ 

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 $\Gamma(4, \phi^+_3, \mathbb{F}_q)$ 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 $\Gamma(5, \{\alpha_1\}, \{\alpha_1 + \alpha_2\}, \{2\alpha_1 + \alpha_2\}, \{3\alpha_1 + \alpha_2\}, \mathbb{F}_q)$ and sequences: $\{\alpha_1\} \subset \{\alpha_1, 2\alpha_1 + \alpha_2\} \subset \{\alpha_1, 2\alpha_1 + \alpha_2, \alpha_1 + \alpha_2\}$ and $\{\alpha_2\} \subset \{\alpha_1, \alpha_1 + \alpha_2\} \subset \{\alpha_2, \alpha_1 + \alpha_2, 2\alpha_1 + \alpha_2\}$ 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 $\Gamma(3, \phi^+_3, \mathbb{F}_q) \cong PG(2, q)$

<table>
<thead>
<tr>
<th>$((1), \emptyset)$</th>
<th>$((2), p_1)$</th>
<th>$((3), p_1, p_2)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(1, 2), \emptyset$</td>
<td>$+$</td>
<td>$+$</td>
</tr>
<tr>
<td>$(3, 1), 1_1$</td>
<td>$+$</td>
<td>$-$</td>
</tr>
<tr>
<td>$(2, 3), 1_1, 1_2$</td>
<td>$-$</td>
<td>$+$</td>
</tr>
</tbody>
</table>

Table 2. Incidence relations for graph $\Gamma(4, \phi^+_3, \mathbb{F}_q)$

<table>
<thead>
<tr>
<th>$((1), \emptyset)$</th>
<th>$((2), p_1)$</th>
<th>$((3), p_1, p_2)$</th>
<th>$((4), p_1, p_2, p_3)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(1, 2), \emptyset$</td>
<td>$+$</td>
<td>$+$</td>
<td>$-$</td>
</tr>
<tr>
<td>$(4, 1), 1_1$</td>
<td>$+$</td>
<td>$-$</td>
<td>$+$ : $p_1 = 1_1$</td>
</tr>
<tr>
<td>$(2, 3), 1_1, 1_2$</td>
<td>$-$</td>
<td>$+$</td>
<td>$+$ : $p_1 = 1_1$, $p_2 - p_1 = 1_1 p_1$</td>
</tr>
<tr>
<td>$(3, 4), 1_1, 1_2, 1_3$</td>
<td>$-$</td>
<td>$-$</td>
<td>$+$ : $p_1 = 1_1$, $p_2 - p_1 = 1_1 p_1$, $p_3 - p_2 = 1_1 p_2$</td>
</tr>
</tbody>
</table>

Table 3. Incidence relations for graph $\Gamma(5, \phi^+_3, \mathbb{F}_q)$

<table>
<thead>
<tr>
<th>$((1), \emptyset)$</th>
<th>$((2), p_1)$</th>
<th>$((3), p_1, p_2)$</th>
<th>$((4), p_1, p_2, p_3)$</th>
<th>$((5), p_1, p_2, p_3, p_4)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(1, 2), \emptyset$</td>
<td>$+$</td>
<td>$+$</td>
<td>$-$</td>
<td>$-$</td>
</tr>
<tr>
<td>$(2, 3), 1_1$</td>
<td>$+$</td>
<td>$-$</td>
<td>$+$ : $p_1 = 1_1$</td>
<td>$-$</td>
</tr>
<tr>
<td>$(3, 3), 1_1, 1_2$</td>
<td>$-$</td>
<td>$+$</td>
<td>$+$ : $p_1 = 1_1$, $p_2 - p_1 = 1_1 p_1$</td>
<td>$-$</td>
</tr>
<tr>
<td>$(4, 4), 1_1, 1_2, 1_3$</td>
<td>$-$</td>
<td>$-$</td>
<td>$+$ : $p_1 = 1_1$, $p_2 - p_1 = 1_1 p_1$, $p_3 - p_2 = 1_1 p_2$, $p_4 - p_3 = 1_1 p_3$</td>
<td>$-$</td>
</tr>
<tr>
<td>$(5, 5), 1_1, 1_2, 1_3, 1_4$</td>
<td>$-$</td>
<td>$-$</td>
<td>$+$ : $p_1 = 1_1$, $p_2 - p_1 = 1_1 p_1$, $p_3 - p_2 = 1_1 p_2$, $p_4 - p_3 = 1_1 p_3$, $p_5 - p_4 = 1_1 p_4$</td>
<td>$-$</td>
</tr>
</tbody>
</table>

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

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

where $|E|$ is the number of edges of graph $\Gamma$ 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 & More 1983).

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

| Graph | Regularity | $|V|$ | Girth | $\lambda_1$ |
|-------|------------|------|-------|------------|
| $PG(2, q) \cong \Gamma(3, \phi^+_3, \mathbb{F}_q)$ | $q + 1$ | $2(1 + q + q^2)$ | 6 | $\sqrt{q}$ |
| $GQ(q, q)$ | $q + 1$ | $2(1 + q + q^2 + q^3)$ | 8 | $\sqrt{2q}$ |
| $\Gamma(4, \phi^+_4, \mathbb{F}_q)$ | $q + 1$ | $2(1 + q + q^2 + q^3 + q^4)$ | 6 | $\sqrt{2q}$ |
| generalized pentagon | do not exist | | | |
| $\Gamma(5, \phi^+_5, \mathbb{F}_q)$ | $q + 1$ | $2(1 + q + q^2 + q^3 + q^4 + q^5)$ | 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

$$ q + 1 \quad 2(q + \ldots + q^n) + 1. $$

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 $\lambda_1 = q + 1$. Let us denote the second eigenvalue by $\lambda_2 = \max_{\lambda, \varphi q + 1} |\lambda_i|$. 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, the 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 $\sqrt{5q}$ 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 $\lambda_1 = \sqrt{5q}$ 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 neighbours of type $t_{k-1}$, for $k = 1, 2$. Each vertex of type $t_3$ have $q$ neighbours of type $t_4$ and one each vertex have four neighbours 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 exists a cycle $C_4$ passing through two points of type $t_3$ and two lines of type $t_2$.
2. There are two points ($\bar{p}$) of type $t_2$ and ($\bar{q}$) of type $t_3$ which have two common neighbours of type $t_4$: $[\bar{l}], [\bar{l}]$, such that $[\bar{l}] \neq [\bar{l}]$. Cycle $C_4$ has a form $([l])I([p])I([q])I(\bar{l})$. If cycle of such type exist then:

$$(\bar{p})I([l]) \leftrightarrow ((4), \bar{p}_1, \bar{p}_2)I[[3, 4], \bar{l}_1, \bar{l}_2, \bar{l}_3] \leftrightarrow \bar{p}_1 = \bar{l}_1 \land \bar{p}_2 = \bar{l}_2,$$

$$(\bar{q})I([l]) \leftrightarrow ((4), \bar{q}_1, \bar{q}_2)I[[3, 4], \bar{l}_1, \bar{l}_2, \bar{l}_3] \leftrightarrow \bar{q}_1 = \bar{l}_1 \land \bar{p}_2 = \bar{l}_2,$$

$$(\bar{p})I([l]) \leftrightarrow ((3), \bar{p}_1, \bar{p}_2, \bar{p}_3)I[[3, 4], \bar{l}_1, \bar{l}_2, \bar{l}_3] \leftrightarrow \begin{cases} \bar{p}_2 - \bar{p}_2 = \bar{p}_1 \bar{p}_1 \\ \bar{l}_3 - \bar{p}_3 = \bar{p}_1 \bar{p}_2 \\
\bar{l}_3 = \bar{p}_1 \bar{p}_2 + \bar{p}_3, \end{cases}$$

$$(\bar{q})I([l]) \leftrightarrow ((3), \bar{q}_1, \bar{q}_2, \bar{q}_3)I[[3, 4], \bar{l}_1, \bar{l}_2, \bar{l}_3] \leftrightarrow \begin{cases} \bar{q}_2 - \bar{p}_2 = \bar{p}_1 \bar{p}_1 \\ \bar{l}_3 - \bar{p}_3 = \bar{p}_1 \bar{p}_2 \\
\bar{l}_3 = \bar{p}_1 \bar{p}_2 + \bar{p}_3, \end{cases}$$

We obtain dependence $\bar{l}_1 = \bar{l}_1 \land \bar{l}_2 = \bar{l}_2 \land \bar{l}_3 = \bar{l}_3 \leftrightarrow [l] \neq [l]$. This contradicts our assumption that $[l] \neq [l]$. Therefore the initial assumption that such type of cycle $C_4$ exist must be false.

3. There exists two lines $[l]$ of type $t_3$ and $[l]$ of type $t_2$ which have two common neighbours of type $t_4$: ($\bar{p}$), ($\bar{q}$), such that ($\bar{p}) \neq (\bar{q})$. Cycle $C_4$ has a form $[[l]]I(\bar{p})I([l])I([q])I([l])$ If cycle of this type exist then:

$$[[l]]I(\bar{p}) \leftrightarrow [[2, 3], \bar{l}_1, \bar{l}_2]I((3), \bar{p}_1, \bar{p}_2, \bar{p}_3) \leftrightarrow \bar{l}_1 = \bar{p}_1 \land \bar{l}_2 = \bar{p}_3 \bar{l}_1,$$

$$[[l]]I(\bar{q}) \leftrightarrow [[2, 3], \bar{l}_1, \bar{l}_2]I((3), \bar{q}_1, \bar{p}_2, \bar{p}_3) \leftrightarrow \bar{l}_1 = \bar{p}_1 \land \bar{l}_2 = \bar{p}_3 \bar{l}_1,$$

$$[[l]]I(\bar{p}) \leftrightarrow [[3, 4], \bar{l}_1, \bar{l}_2, \bar{l}_3]I((3), \bar{p}_1, \bar{p}_2, \bar{p}_3) \leftrightarrow \begin{cases} \bar{l}_1 - \bar{p}_2 = \bar{l}_1 \bar{l}_1 \\ \bar{l}_3 - \bar{p}_3 = \bar{l}_1 \bar{l}_2 \\
\bar{p}_2 = \bar{l}_2 - \bar{l}_1 \bar{l}_1 \\
\bar{l}_3 = \bar{l}_3 - \bar{l}_1 \bar{l}_1 \\
\bar{l}_1 = \bar{p}_1 \land \bar{l}_2 = \bar{p}_3 \bar{l}_1, \end{cases}$$

We obtain dependence $\bar{l}_1 = \bar{l}_1 \land \bar{l}_2 = \bar{l}_2 \land \bar{l}_3 = \bar{l}_3 \leftrightarrow [l] \neq [l]$. This contradicts our assumption that $[l] \neq [l]$. Therefore the initial assumption that such type of cycle $C_4$ 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 exists 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 vertices in graph $D(4, q)$, [13]. From [13] we know that the girth of graphs $D(n, q)$ is 8 so cycle of this type do not exist.

2. There exists 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 of graphs $D(n, q)$ is 8 so cycle of such type do not exist.

$$(\bar{p})I([l]) \leftrightarrow ((3), \bar{p}_1, \bar{p}_2, \bar{p}_3)I[[3, 4], \bar{l}_1, \bar{l}_2, \bar{l}_3, \bar{l}_4] \leftrightarrow \begin{cases} \bar{l}_1 - \bar{p}_2 = \bar{l}_1 \bar{l}_1 \\ \bar{l}_3 - \bar{p}_3 = \bar{l}_1 \bar{l}_2 \\
\bar{p}_2 = \bar{l}_2 - \bar{l}_1 \bar{l}_1 \\
\bar{l}_3 = \bar{l}_3 - \bar{l}_1 \bar{l}_1 \\
\bar{l}_1 = \bar{p}_1 \land \bar{l}_2 = \bar{p}_3 \bar{l}_1, \end{cases}$$
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 $t_3$ 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 of 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 $(\dot{p}) ((\dot{p}) \neq (\dot{p}))$ of type $t_4$ and three different lines $[\dot{l}], [l_1], [l_2], [l_3]$ of type $t_4$. Cycle $C_6$ has a form $(p)I[\dot{l}][p)I[\dot{l}][p)I(p)$. If cycle of this type exist then:

\[
\begin{align*}
(p)I[\dot{l}] & \iff ((3), p_1, p_2, p_3)I[[3,4], l_1, l_2, l_3, l_4] \\
\begin{cases}
p_1 &= l_1 \\
p_2 - l_2 &= p_1 l_3 + p_3 l_1 \\
p_3 &= l_3
\end{cases}
\]

\[
([\dot{l}])I(\dot{p}) \Rightarrow [[3,4], l_1, l_2, l_3, l_4]I((4), \dot{p}_1, \dot{p}_2, \dot{p}_3, \dot{p}_4) \iff
\begin{cases}
p_2 - l_4 &= \dot{p}_1 l_3 \\
p_3 - l_3 &= \dot{p}_1 l_1 \\
p_4 - l_2 &= \dot{p}_3 l_4
\end{cases}
\]

Hence $l_1 = l_1$, $l_3 = l_3$ and $l_2 = l_2 = l_2$.

\[
(p)I[\dot{l}] \iff ((4), p_1, p_2, p_3)I[[3,4], l_1, l_2, l_3, l_4] \\
\begin{cases}
p_1 &= \dot{l}_1 \\
p_2 - l_2 &= \dot{p}_1 l_3 + \dot{p}_3 l_1 \\
p_3 &= l_3
\end{cases}
\]

\[
((p)I[\dot{l}] \iff ((4), p_1, p_2, p_3, p_4, l_1, l_3, l_2, l_4]) \\
\begin{cases}
p_2 - l_4 &= \dot{p}_1 l_3 \\
p_3 - l_3 &= \dot{p}_1 l_1 \\
p_4 - l_2 &= \dot{p}_3 l_4
\end{cases}
\]

We obtain dependence $l_1 = l_1 \land l_2 = l_2 \land l_3 = l_3 \land l_4 = l_4 \iff [\dot{l}] = [\dot{l}]$. This contradicts our assumption that $[\dot{l}] \neq [\dot{l}]$. Therefore the initial assumption that such type of cycle $C_6$ exist must be false.

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

\[
\begin{align*}
(p)I[\dot{l}] & \iff ((3), p_1, p_2, p_3)I[[3,4], l_1, l_2, l_3, l_4] \\
\begin{cases}
p_1 &= l_1 \\
p_2 - l_2 &= p_1 l_3 + p_3 l_1 \\
p_3 &= l_3
\end{cases}
\]

\[
([\dot{l}]I(\dot{p}) \Rightarrow [[3,4], l_1, l_2, l_3, l_4]I((4), \dot{p}_1, \dot{p}_2, \dot{p}_3, \dot{p}_4) \iff
\begin{cases}
p_2 - l_4 &= \dot{p}_1 l_3 \\
p_3 - l_3 &= \dot{p}_1 l_1 \\
p_4 - l_2 &= \dot{p}_3 l_4
\end{cases}
\]

It is easy see that $p_1 = \dot{p}_1$ and $p_3 = \dot{p}_3$. Therefore $p_2 = \dot{p}_2, p_4 = \dot{p}_4$. We obtain that $(\dot{p}) = (\dot{p})$. This contradicts our assumption that $(\dot{p}) \neq (\dot{p})$. Therefore the initial assumption that such $C_6$ exist must be false.

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

\[
\begin{align*}
(p)I[\dot{l}] & \iff ((3), p_1, p_2, p_3)I[[3,4], l_1, l_2, l_3, l_4] \\
\begin{cases}
p_1 &= l_1 \\
p_2 - l_2 &= p_1 l_3 + p_3 l_1 \\
p_3 &= l_3
\end{cases}
\]

\[
([\dot{l}]I(\dot{p}) \Rightarrow [[3,4], l_1, l_2, l_3, l_4]I((4), \dot{p}_1, \dot{p}_2, \dot{p}_3, \dot{p}_4) \iff
\begin{cases}
p_2 - l_4 &= \dot{p}_1 l_3 \\
p_3 - l_3 &= \dot{p}_1 l_1 \\
p_4 - l_2 &= \dot{p}_3 l_4
\end{cases}
\]

We can write variables $p_2$ and $p_3$ in two ways:

\[
\begin{align*}
p_3 &= l_3 + \dot{p}_1 l_4 = p_3 + \dot{p}_1 p_1 \\
p_3 &= l_3 + \dot{p}_1 l_4 = p_3 + \dot{p}_1 p_1
\end{align*}
\]

\[
\begin{align*}
p_3 &= l_3 + \dot{p}_1 l_4 = p_3 + \dot{p}_1 p_1 \\
p_3 &= l_3 + \dot{p}_1 l_4 = p_3 + \dot{p}_1 p_1
\end{align*}
\]
\[ p_1 = \hat{l}_1 \]
\[ p_2 - \hat{l}_2 = p_3 \hat{l}_3 + p_1 \hat{l}_3 , \]
\[ p_3 = \hat{l}_3 \]

and we see that \( \hat{l}_1 = \hat{l}_1 = p_1, \hat{l}_2 = \hat{l}_2, \hat{l}_3 = \hat{l}_3 = p_3 \).

\((\hat{p}) I[\hat{l}] \Leftrightarrow ((4), \hat{p}_1, \hat{p}_2, \hat{p}_3, \hat{p}_4) I[[3, 4], \hat{l}_1, \hat{l}_2, \hat{l}_3] \Leftrightarrow \]
\[ ((4), l_1, \hat{p}_2, l_3, \hat{p}_4) I[[3, 4], p_1, l_2, p_3, l_4] \Rightarrow \]
\[ \begin{cases} p_2 - l_4 = l_3 p_1 \\ p_4 - l_2 = l_3 p_1 \end{cases} \]

\((\hat{p}) I[\hat{l}] \Leftrightarrow ((4), \hat{p}_1, \hat{p}_2, \hat{p}_3, \hat{p}_4) I[[3, 4], \hat{l}_1, \hat{l}_2, \hat{l}_3] \Leftrightarrow \]
\[ ((4), l_1, \hat{p}_2, l_3, \hat{p}_4) I[[3, 4], p_1, l_2, p_3, l_4] \Rightarrow \]
\[ \begin{cases} p_2 - l_4 = l_3 p_1 \\ p_4 - l_2 = l_3 p_1 \end{cases} \]

We obtain that \( \hat{p}_4 = \hat{p}_4, \hat{l}_4 = \hat{l}_4 \) so \((\hat{p}) = (\hat{p})\) and \([\hat{l}] = [\hat{l}]\). This contradicts our assumptions that \((\hat{p}) \neq (\hat{p})\) and \([\hat{l}] \neq [\hat{l}]\). Therefore the initial assumption that such \( C_6 \) exist must be false.

Graph \( D(5, q) \) is a subgraph of \( \Gamma(5, \phi_n^+, F_q) \). For an arbitrary \( q \geq 2 \) graph the girth of graph \( D(5, q) \) is 8 and so the girth of graph \( \Gamma(5, \phi_n^+, F_q) \) is 8 and it has a cycle of length 8.

The graphs \( \Gamma(n, \phi_n^+, F_q) \) for arbitrary \( n, q \) are connected. What more we have conjecture that the families are \( q + 1 \)-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 \( \Gamma(n, \phi_n^+, F_q) \) 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 technique 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 Gallager 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]. Guaninan 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:

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

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 $P(x|y,H)$ 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 $p_2 \in E$

<table>
<thead>
<tr>
<th>Initial graph</th>
<th>$E$</th>
<th>Number of lines in used subgraph</th>
<th>Number of points in used subgraph</th>
<th>Code rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Gamma(4, \phi_5^*, F_5)$</td>
<td>(0, 1)</td>
<td>138</td>
<td>66</td>
<td>$\approx 0.52$</td>
</tr>
<tr>
<td>$\Gamma(4, \phi_5^*, F_7)$</td>
<td>(0, 1)</td>
<td>300</td>
<td>120</td>
<td>0.6</td>
</tr>
<tr>
<td>$\Gamma(4, \phi_5^*, F_7)$</td>
<td>(0, 1, 2)</td>
<td>368</td>
<td>176</td>
<td>$\approx 0.52$</td>
</tr>
<tr>
<td>$\Gamma(4, \phi_5^*, F_11)$</td>
<td>(0, 1, 2, 3, 4)</td>
<td>1392</td>
<td>672</td>
<td>0.52</td>
</tr>
<tr>
<td>$\Gamma(5, \phi_5^*, F_5)$</td>
<td>(0, 1)</td>
<td>682</td>
<td>311</td>
<td>$\approx 0.55$</td>
</tr>
<tr>
<td>$\Gamma(5, \phi_5^*, F_7)$</td>
<td>(0, 1)</td>
<td>2516</td>
<td>806</td>
<td>$\approx 0.68$</td>
</tr>
<tr>
<td>$\Gamma(5, \phi_5^*, F_7)$</td>
<td>(0, 1, 2)</td>
<td>2573</td>
<td>1205</td>
<td>$\approx 0.53$</td>
</tr>
</tbody>
</table>

### Figure 1. Bit error rate for codes based on $\Gamma(4, \phi_5^*, F_q)$

Bit degree reduction can only increase the girth so there is no short cycles. After bit degree 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 $\Gamma(4, \phi_5^*, F_q)$ and $\Gamma(5, \phi_5^*, F_q)$. Fig. 1 and Fig. 2 show Bit Error Rate for this representatives.
Figure 2. Bit error rate for codes based on $\Gamma(5, \phi, F_q)$.

References