Linear and Nonlinear Analysis
Volume 5, Number 1, 2019, 1–11
Yokohama Publishers
ISSN 2188-8167

PSEUDORANDOM NUMBER GENERATOR BY p-ADIC CHAOS AND RAMANUJAN EXPANDER GRAPHS

KOICHIRO NAITO

Dedicated to Professor Jong Soo Jung for his 65th happy birthday

Abstract. In our previous paper, applying chaotic properties of the p-adic dynamical system given by the p-adic logistic map, we constructed a new pseudorandom number generator. In this paper, using the pseudorandom sequences given by this generator, we construct random adjacency matrices and their random graphs. Then we numerically show that the eigenvalue distributions of these random matrices have the characteristical properties of the adjacency matrices of Ramanujan graphs.

1. Introduction

Expander graphs are highly connected sparse graphs, which have been of great interest with many applications in computer science; from the design and analysis of communication networks to the theory of error correcting codes and the theory of pseudorandomness. Especially, Ramanujan graphs, known as the best expanders, not only play an important role in computer science as basic building blocks for network constructions, but the researches on the Ramanujan graphs are deeply related to various branches of pure mathematics; number theory, representation theory and algebraic geometry, and also, probability theory.

In our previous paper [8], applying chaotic properties of the p-adic dynamical system given by the p-adic logistic map or the p-adic Smale horseshoe map (cf. [9]) and estimating the invariants between the p-adic dynamical system and the symbolic dynamical system, we constructed pseudorandom number generators. Furthemore, we numerically estimated the randomness of the generated pseudorandom numbers by the statistical method, derived from the Random Matrix Theory, called RMT test (see [10]). In this paper, using the pseudorandom sequences given by this generator and the LLL algorithm, we construct the sequences of pseudorandom small numbers $\{-1, 0, 1\}$. Furthemore, we investigate the randomness of the generated pseudorandom numbers by the RMT test. Then, using these pseudorandom sequences, we construct random adjacency matrices and their random graphs. Finally, we numerically show that the eigenvalue distributions of these random matrices have the characteristical properties of the adjacency matrices of non-regular Ramanujan graphs.

2010 *Mathematics Subject Classification.* 60B20,05C80, 37B10, 11E95, 14G50, 65C10.

Key words and phrases. Random matrices, random graphs, p-adic theory, cryptography, random number generation.

Our plan of this paper is as follows. In section 2 we introduce the definitions of expander graph and Ramanujan graph by usign the properties of eigenvalues of these adjacency matrices. In section 3 we give some genelarized non-regular Ramanujan graphs and classify them according to upper bounds of their nontrivial eigenvalues. In section 4, using the pseudorandom number generator and the LLL algorithm, we construct the sequences of pseudorandom small numbers and we numerically estimate the randomness of the generated pseudorandom numbers by the RMT test. In section 5, using the pseudorandom numbers obtained in section 4, we construct non-regular Ramanujan graphs and we investigate the eigenvalue distributions of their adjacency matrices.

2. Ramanujan graph

Let $X = (V, E)$ be a graph where $V = \{v_1, v_2, ..., v_n\}$ is the set of vertices and E is the set of edges. Let a_{ij} be the number of edges joining v_i to v_j, then the adjacency matrix of the graph X is given by $A = (a_{ij})$. We assume that (i) X is simple; there is at most one edge joining adjacent vertices, $a_{ij} \in \{0, 1\}$ for every i, j, (ii) X has no loops; $a_{ii} = 0$ for every $v_i \in V$ and (iii) X is undirected; A is a $n \times n$ symmetric matrix.

Let $k \geq 2$ be an integer and the graph X be k-regular, that is, for every $v_i \in V$,

$$\sum_{v_j \in V} a_{ij} = k.$$

Since A is an n-by-n symmetric matrix, it had n real eigenvalues, counting multiplicities,

$$\mu_0 \geq \mu_1 \geq \cdots \geq \mu_{n-1}.$$

The following proposition is easily obtained (cf. [2]).

Proposition 2.1. *Let X be a finite connected k-regular graph with n vertices. Then*

- $\mu_0 = k$;
- $|\mu_i| \leq k, \quad 1 \leq i \leq n-1$.

For a graph $X = (V, E)$ and $F \subset V$, define the boundary ∂F of F by the set of edges with one extremity in F and the other in $V - F$, that is, ∂F is the set of edges connecting F to $V - F$.

Definition 2.2. The expanding constant $h(X)$ of the graph X is defined by

$$h(X) = \inf\{\frac{|\partial F|}{\min\{|F|, |V - F|\}} : \ F \subset V, \ 0 < |F| < +\infty\}.$$

For the relation between the nontrivial eigenvalue $\mu \neq k$ and the expanding constant $h(X)$ Dodziuk has shown the following estimates.

Proposition 2.3 ([3])**.** *Let $X = (V, E)$ be a finite, connected, k-regular simple graph. Let μ_1 be the first nontrivial eigenvalue of X. Then*

$$\frac{k - \mu_1}{2} \leq h(X) \leq \sqrt{2k(k - \mu_1)}.$$

Let $\{X_m\}$ be a family of finite, connected, k-regular graphs with $|V_m| \to +\infty$ as $m \to +\infty$.

$\{X_m\}$ is called a family of expanders if there exists a constant $\varepsilon > 0$ such that

$$h(X_m) \geq \varepsilon, \quad \forall m \geq 1.$$

It follows from Proposition 2.3 that we can easily obtain an equivalent condition for the existence of a family of expanders.

Corollary 2.4. *Let $\{X_m\}$ be a family of finite, connected, k-regular simple graphs with $|V_m| \to \infty$ as $m \to \infty$. Then, $\{X_m\}$ is a family of expanders if and only if there exists a constant $\varepsilon > 0$ such that*

$$k - \mu_1(X_m) \geq \varepsilon, \quad \forall m \geq 1.$$

For the asymptotic behaviors of these eigenvalues the following Alon-Boppana theorem is well known.

Theorem 2.5 ([1])**.** *Let $\{X_m\}$ be a family of finite, connected, k-regular simple graphs with $|V_m| \to +\infty$ as $m \to +\infty$. Then,*

$$\liminf_{m \to +\infty} \mu_1(X_m) \geq 2\sqrt{k-1}.$$

Here we give the definition of Ramanujan graph.

Definition 2.6. A finite, connected k-regular graph X is a Ramanujan graph if for every nontrivial eigenvalue $\mu (\neq \pm k)$ of X,

$$|\mu| \leq 2\sqrt{k-1}.$$

Since an expander constant of a regular graph is greater than or equal to $(k - \mu_1)/2$, making μ_1 as small as possible gives us good expander graphs. However, by the Alon-Boppana theorem, we cannot do better than

$$\liminf_{m \to +\infty} \mu_1(X_m) \geq 2\sqrt{k-1}.$$

Hence, Ramanujan graphs make good expanders.

It is very difficult to construct a family of Ramanujan graphs of fixed degree with number of vertices going to infinity. Only a few examples of these explicit constructions have been known ([6], [7]). On the other hand, for random graphs, J. Friedman has shown in [4] that for fixed degree k and $\varepsilon > 0$, the probability that nontrivial eigenvalues satisfy

$$|\mu| \leq 2\sqrt{k-1} + \varepsilon$$

approaches 1 as $n \to \infty$. In Section 5, considering the above results on random graphs, we numerically construct Ramanujan graphs by using pseudorandom sequences.

3. Non-regular Ramanujan graph

In view of practical applications it is important to study non-regular type graphs and recently, various generalized Ramanujan graphs have been proposed by many authors (cf. [11]). While in case of k-regular graphs the maximal eigenvalue μ_0 is equal to k and the definition of the Ramanujan graph is given by

$$|\mu| \leq 2\sqrt{k-1}$$

for every nontrivial eigenvalue $\mu(\neq \pm k)$, the following genelarized Ramanujan graphs have been defined.

We say that a non-regular graph X is a naive Ramanujan graph if

$$|\mu| \leq 2\sqrt{\sigma_X - 1}$$

for every nontrivial eigenvalue $\mu(\neq \sigma_X)$ where σ_X is the largest absolute value of eigenvalues of the adjacency matrix A,

$$\sigma_X = \max\{|\mu| : \mu \in \mathrm{Spectrum} A\}.$$

The degree of a vertex v_i in the graph X is the number of edges joining v_i,

$$\sum_{v_j \in V} a_{ij}, \quad a_{i,j} \in \{0,1\}.$$

Let $\overline{d_X}$ be the average degree of the vertices of X. We say that a non-regular graph X is a weak Ramanujan graph if

$$|\mu| \leq 2\sqrt{\overline{d_X} - 1}$$

for every nontrivial eigenvalue $\mu(\neq \sigma_X)$.

In our numerical experiments, using the maximal degree D_X, we say that a non-regular graph X is a mild Ramanujan graph if the following inequality hold

$$|\mu| \leq 2\sqrt{D_X - 1}$$

for every nontrivial eigenvalue $\mu(\neq \sigma_X)$.

In the histograms showing the distributions of the eigenvalues we plot these upper bound values colored as follows:

$2\sqrt{D_X - 1}$: mild Ramanujan bounds (green)
$>$ $2\sqrt{\sigma_X - 1}$: naive Ramanujan bounds (red)
$>$ $2\sqrt{\overline{d_X} - 1}$: weak Ramanujan bounds (blue).

4. Pseudorandom number generator

Here we construct a new pseudorandom number generator by applying our pervious method in [8] as follows.

(1): Choose a seed, a p-adic integer number, $\xi \in \mathbb{Z}_p$.

(2): For an integer $n \sim 50$ and $l \sim 100$, construct a sequence $\{\xi_k\}_{k=1}^{L}$, $L = n \times l$, by a p-adic logistic map l_p, defined by

$$l_p(x) = \frac{x^p - x}{p} \qquad \text{for } x \in \mathbb{Z}_p,$$

$$\xi_1 = \xi,\ \xi_2 = l_p(\xi_1), ..., \xi_n = l_p(\xi_{n-1}), ...$$

In [8] we have taken their modulo p: $\xi_{k,p} = \xi_k \pmod p$ and we have shown the randomness of the sequence by RMT test.

(3): For an integer $m \sim 10$, a precision order, we calculate the approximate sequence $\{\xi_{k,m}\}$ of $\{\xi_k\}$, given by

$$\xi_{k,m} = \sum_{j=0}^{m-1} a_j p^j \in \mathbb{Z}, \quad k = 1, ..., L$$

where each ξ_k has a p-adic expansion

$$\xi_k = \sum_{j=0}^{\infty} a_j p^j \in \mathbb{Z}_p, \quad a_j \in \{0, 1, ..., p-1\}$$

(4): Construct the following knapsack type matrices $A_m^{(i)}, i = 0, .., l-1$ given by

$$A_m^{(i)} = \begin{pmatrix} p^m & 0 & 0 & \dots & 0 \\ \xi_{1+i,m} & 1 & 0 & \dots & 0 \\ \xi_{2+i,m} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_{n+i,m} & 0 & 0 & \dots & 1 \end{pmatrix}, \quad i = 0, 1, ..., l-1$$

Each matrix $A_m^{(i)}$ generates a lattice and it is known that, if the sequences $\{\xi_{k,m}\}$ are random, their lattices are randomly distributed in the set of lattices, the determinants of which have the same value p^m (see [5]).

(5): We apply the LLL reduction algorithm to each matrix $A_m^{(i)}$. Then we have reduced matrices $B_m^{(i)},\ i = 0, ..., l-1$, with small integer elements.

(6): By connecting each rows of $B_m^{(i)}$ from $i = 0$ to $i = l-1$, we have the sequence P_l of pseudorandom numbers with its length $(n+1)^2 \times l \sim 250000$, sufficient for the RMT test ([10]).

(7): (RMTtest) We cut P_l into N pieces of equal length L, then shape them in an $N \times L$ matrix $C = (c_{ij})$ by placing the first L elements in the first row and the next elements in the 2nd rows $\cdots$.

$$C = \begin{pmatrix} c_{11} & \cdots & c_{1L} \\ \vdots & \ddots & \vdots \\ c_{N1} & \cdots & c_{NL} \end{pmatrix}$$

Then we normalize each row with zero mean and unit variance to have the normalized matrix D and we calculate the correlation matrix

$$G = \frac{1}{L} D\ {}^tD.$$

Compare the eigenvalue distribution of G to the corresponding theoretical distribution, called Marchenko-Pastur curve.

$$MP(\lambda) = \frac{Q}{2\pi\lambda}\sqrt{(\lambda_+ - \lambda)(\lambda - \lambda_-)}, \quad \lambda_\pm = \left(1 \pm \sqrt{\frac{1}{Q}}\right)^2$$

where $Q = L/N$. According to Random Matrix Theory, Marchenko-Pastur distribution describes the asymptotic behavior of eigenvalue distributions of large rectangular random matrices. If the two distributions match, our data passes the RMT test, and if they do not match, our data fails the RMT test.

Here we show some results of numerical experiments given by the seed: $p = 17,\ l = 100,\ n = 49,\ m = 7,\ \xi = 13^{\frac{1}{103}}$.

$$A_m^{(10)} = \begin{pmatrix} 410338673 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 180361593 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 402872406 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ \vdots & & & & & \ddots & & & & & \vdots \\ 180685084 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 & 0 \\ 310632419 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (50 \times 50)$$

$\longrightarrow$ LLL reduction algorithm $\longrightarrow$

$$B_m^{(10)} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & \cdots \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & \cdots \\ \vdots & & & & & \vdots & & & & & \vdots & \\ 0 & -1 & 0 & 0 & 0 & -1 & 1 & -1 & -1 & 0 & 0 & \cdots \\ 1 & -1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & \cdots \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & \cdots \end{pmatrix} \quad (50 \times 50)$$

The length of the pseudorandom numbers is 250000. Using the sequence of these pseudorandom numbers, we operate the following RMT tests.

The 1st RMT test is given by the parameters, $m = 7, l = 100, L = 625,\ N = 400,\ \ Q = L/N = 1.5625$ and the 2nd RMT test is given by the parameters, $m = 30, l = 144, L = 900,\ N = 400,\ \ Q = L/N = 2.778$.

The following graphs (Fig.1, Fig.2) show that these two tests are passed.

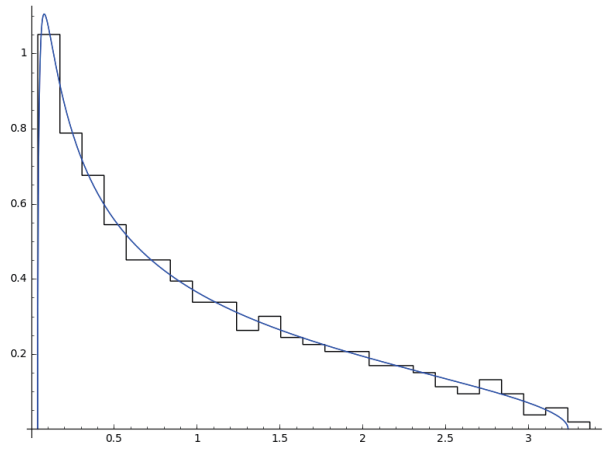

FIGURE 1. 1st RMT test

Next we show the result of the 3rd RMT where we directly use the sequence of pseudorandom numbers $\{\xi_{k,p}\}_{k=1}^{750000}$ given by the p-adic logistic map without LLL algorithms. The following graph (Fig.3) shows that this test is also passed where $p = 17,\ \xi = 13^{\frac{1}{103}}, L = 1500,\ N = 500,\ \ Q = L/N = 3$

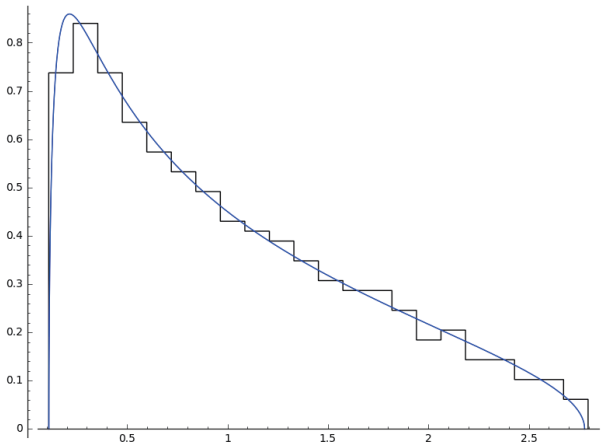

FIGURE 2. 2nd RMT test

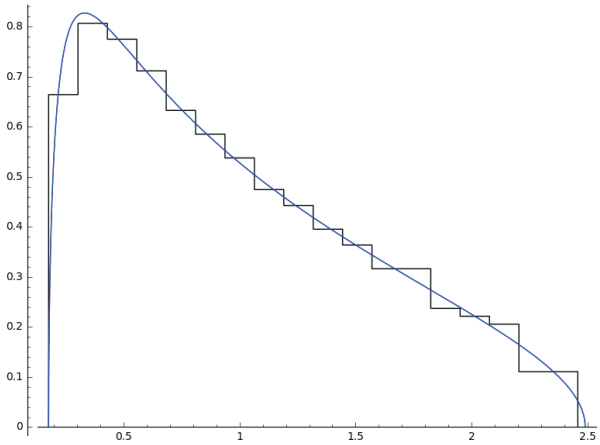

FIGURE 3. 3rd RMT test

5. Construction of non-regular Ramanujan graph

Using the pseudorandom sequence P_l generated in the previous section, we give the two construction methods to draw the mild, naive or weak Ramanujan graphs. These two methods have the following common part:

For an integer q : $q^2 \leq l \times (n+1)^2$ (= the length of P_l), we take the string with its length q^2 from P_l and we cut this into q pieces of equal length q, then we shape them into a $q \times q$ square matrix S.

Following the common proccess, we apply the first method (I) as follows:
(I)-(1) Construct an upper triangle matrix S_u, which has the upper triangle part of S with 0 diagonal elements.
(I)-(2) Calculate $T = S_u + {}^t S_u$, which is the adjacency matrix of our Ramanujan graph.

The second method is also given as follows:
(II)-(1) Calculate $T = S + {}^tS$.
(II)-(2) (by sage command)
C_g = Graph(T): C_g is the graph given by the adjacency matrix T.
C_g.remove_loops: the loops of C_g are deleted.
C_g.remove_multiple_edges: only one edge is remained.
Then we have the simple graph C_g without loops and mutiple edges.

If the number of vertices is large over 500, the shape of its graph is condensed and not clear (see Fig.6, Fig.8). First we show a graph of 50 vertices which is obtained by the method (II) for a 50×50 matrix generated in the proccess of the pseudorandom number generator (Fig. 4).

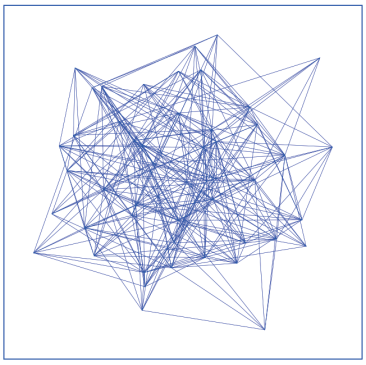

FIGURE 4. Graph of 50x50 Adj. Matrix

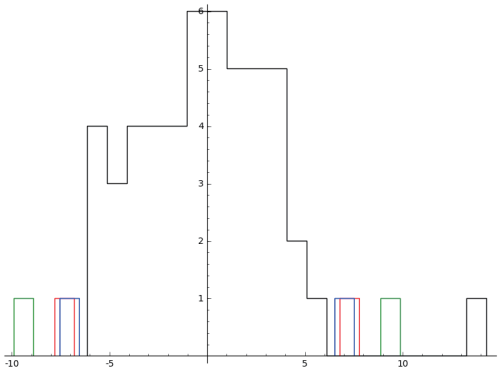

FIGURE 5. eigenvalue distribution: 50x50

Next we calculate the eigenvalues and plot the histograms of their distributions (Fig.5). Their 20 eigenvalues from the largest absolute value are
14.30, -6.13, 5.25,-5.51,-5.37, -5.25, -5.04, 4.86,-4.56, 4.54
-4.27, -3.96, -3.75, 4.05, 3.85 -3.50, -3.10, -2.97, -2.64, -2.58, ...
and the upper bound values of the almost Ramanujan graphs are
$2\sqrt{D_X - 1}$: mild Ramanujan bound = 9.38,
$2\sqrt{\sigma_X - 1}$: naive Ramanujan bound = 7.29,
$2\sqrt{d_X - 1}$: weak Ramanujan bound = 7.03.
We can see that all absolute values of nontrivial eigenvalues are smaller than the upper bound of each almost Ramanujan bound.

Now we use the same parameters and the pseudorandom numbers as in the RMT test 1st case (resp. 2nd case),
$p = 17, l = 100$, (resp. $l = 144$), $n = 49, m = 7$, (resp. $m = 30$), $\xi = 13^{\frac{1}{103}}$,
we construct the adjacency matrices: 500×500 (resp. 600×600) by the (I) method, drawing its graph, and we calculate the eigenvalues and plot the histograms of their distributions.

For the 1st case the 10 eigenvalues from the largest absolute value are

114.09, -21.59, 20.12, 18.21, 18.05, 17.78, 17.12, 17.09, 16.93, 16.80, ...
and the upper bound values of the almost Ramanujan graphs are
mild Rmj bd: 25.46, naive Rmj bd: 21.27, weak Rmj bd: 20.68.

We can see that all absolute values of nontrivial eigenvalues are smaller than the upper bound of the mild Ramanujan bound and almost all nontrivial eigenvalues, exactly, with the probability of 498/499, are also under the upper bounds of the naive and weak Ramanujan bounds.

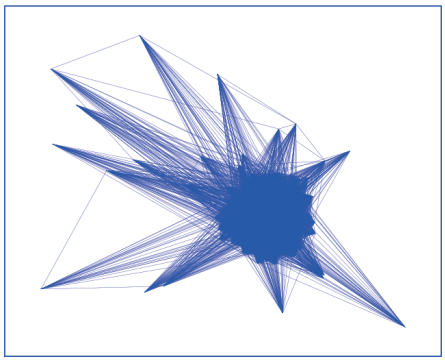

FIGURE 6. Graph of 1st case

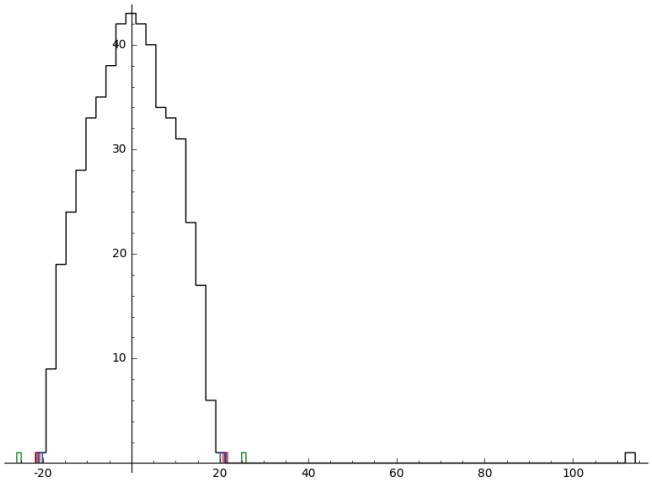

FIGURE 7. Eigenvalues distribution of 1st case

For the 2nd case, the parameters are

$p = 17,\ l = 144,\ n = 49,\ m = 30,\ \xi = 13^{\frac{1}{103}}$.

The 10 eigenvalues of the 600×600 adjacency matrix from the largest absolute value are

134.80, -25.52, 22.09, 20.11, 19.61, 19.32, 19.02, 18.973, 18.82, 18.64, ...

and the upper bound values of the almost Ramanujan graphs are

mild Rmj bd: 28.57 , naive Rmj bd: 23.13, weak Rmj bd: 22.45

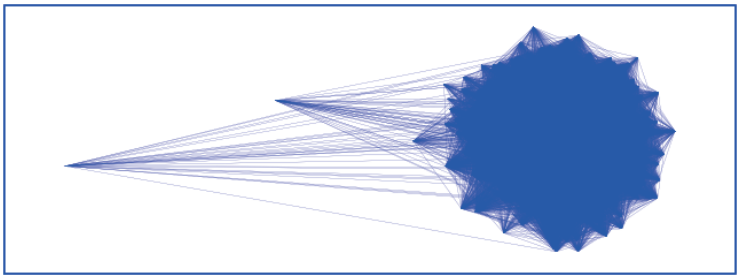

FIGURE 8. Graph of 2nd case

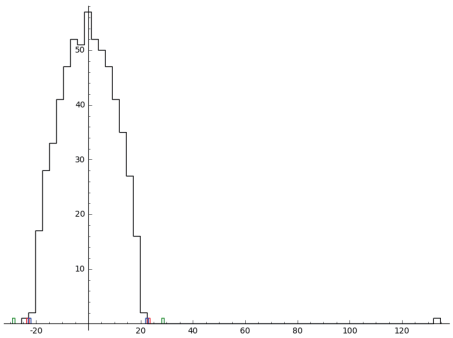

FIGURE 9. Eigenvalues distribution of 2nd case

We can see that all absolute values of nontrivial eigenvalues are smaller than the upper bound of the mild Ramanujan bound and almost all nontrivial eigenvalues, exactly, with the probability of 598/599, are also under the upper bounds of the naive and weak Ramanujan bounds.

CONCLUDING REMARKS

- Pseudorandom number generators have great potential for applications to cryptography. Since we can generate pseudorandom numbers with seeds of small sizes, we can prepare small size keys in cryptography.
- We can see that the RMT tests provide convenient and easy methods for randomness tests.

- **Future Problems**
  - Applications to cryptography.
  - Further numerical tests on randomness; the moment method in RMT test, NIST, ... etc.
  - Theoretical proof on randomness of our p-adic random lattices, using the results in [5].
  - Investigation on the relations between the almost Ramanujan graph and the weak (graph theory) Riemann Hypothesis in [11].
  - Another most important property of expander graphs is "sparse". The boundedness of degrees or the small order growth rate of degrees $O(n^{\varepsilon})$ as $n \to \infty$ should be considered in our improved construction methods of almost Ramanujan random graphs.

References

[1] N. Alon, *Eigenvalues and expanders*, Combinatorica **6** (1986), 83–96.

[2] N. Biggs, *Algebraic Graph Theory*, Cambridge University Press, 1994.

[3] J. Dodziuk, *Difference equations, isoperimetric inequality and transience of certain random walks*, Trans. Amer. Math. Soc. **284** (1984), 787–794.

[4] J. Friedman, *A Proof of Alon's Second Eigenvalue Conjecture and Related Problems*, Memoirs of the American Mathematical Society **910**, A.M.S. 2008.

[5] D. Goldstein and A. Mayer, On the equidistribution of Hecke points, Formu Math. *15* (2003), 165–189.

[6] A. Lubotzky, R. Phillips and P. Sarnak, *Ramanujan graphs*, Combinatorica **8** (1988), 261–277.

[7] G. A. Margulis, *Explicit groups-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators*, Problems of Information Transmission **24** (1988), 39–46.

[8] K. Naito, *Randomness of p-adic discrete dynamical systems and its applications to cryptosystems*, to appear in Proc. 10th International Conference on Nonlinear Anal. Convex Anal. 2017.

[9] N. P. Smart and C. F. Woodcock, *p-adic chaos and random number generation*, Experiment. Math. **7** (1998), 333–342.

[10] X. Yang, R. Itoi, and M. Tanaka, *Testing Randomness by Means of Random Matrix Theory*, Progress of Theoretical Physics, Supplement **194** (2012), 73–83.

[11] A.Terras, *Zeta functions of graphs: A stroll through the garden*, Cambridge Studies in Advanced Mathematics **128**, Cambridge University Press 2011.

Manuscript received 28 February 2019
revised 6 April 2019

Koichiro Naito
Department of Applied Mathematics, Kumamoto University, Chuo-ku, Kurokami, 2-39-1, Kumamoto, Japan
E-mail address: knaito@gpo.kumamoto-u.ac.jp