Linear and Nonlinear Analysis
Volume 6, Number 1, 2020, 143–152
Yokohama Publishers
ISSN 2188-8167

GRAPH RIEMANN HYPOTHESIS AND IHARA ZETA FUNCTION OF NONREGULAR RAMANUJAN GRAPH GENERATED BY p-ADIC CHAOS

KOICHIRO NAITO

Dedicated to the memory of Professor Hang-Chin Lai

Abstract. In our previous papers, 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 sequences of these pseudorandom numbers given by this generator, we construct some pseudorandom adjacency matrices and their graphs. Since the regular Ramanujan graph satisfies the Graph Riemann Hypothesis, we numerically investigate our pseudorandom nonregular graphs by calculating the distributions of poles of the Ihara zeta functions, which are obtained by substituting our pseudorandom adjacency matrices into the Ihara determinant formula.

1. Introduction

Expander graphs, especially, Ramanujan graphs as the best expanders, 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. On the other hand, the researches on the Ramanujan graphs are deeply related to various branches of pure mathematics such as number theory, representation theory and algebraic geometry, and also, probability theory. In the relation between the number theory and the graph theory, the following equivalence relation is significant. A regular graph is Ramanujan if and only if the Ihara zeta function of this graph satisfies the Riemann hypothesis.

For the k-regular graph the Ramanujan graph is defined by the nontrivial eigenvalues $\mu(\neq k)$ satisfying

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

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 ([8], [9]). On the other hand, for the random graphs, J. Friedman has shown in [5] that for fixed degree k and $\varepsilon > 0$, the probability that nontrivial eigenvalues satisfy $|\mu| \leq 2\sqrt{k-1} + \varepsilon$ approaches 1 as $n \to \infty$.

For the nonregular Ramanujan graphs the various definitions of 'almost' Ramanujan graphs have been proposed by using the eigenvalue distributions of their

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.

adjacency matrices. In our previous paper [10], using the sequences of the pseudorandom numbers given by the generator, proposed in [11], we construct some pseudorandom adjacency matrices with their graphs and we numerically investigate these graphs by calculating the eigenvalue distributions whether they have the properties of the Ramanujan graph. In this paper, since the regular Ramanujan graph satisfies the graph Riemann Hypothesis, we numerically investigate our pseudorandom nonregular graphs by calculating the distributions of poles of the Ihara zeta functions, which are obtained by substituting our pseudorandom adjacency matrices into the Ihara determinant formula.

Our plan of this paper is as follows. In section 2 we introduce the notations of the graph theory and the properties of regular Ramanujan graphs. In section 3 we give the definition of the Ihara zeta function and the equivalence relation between the Ramanujan graph and the graph Riemann Hypothesis. In section 4 we give the construction method for the pseudorandom graphs given by our pseudorandom number generator. In section 5 and 6 we show the numerical results, the distribution of the eigenvalues which specifies the almost Ramanujan properties, and the distribution of poles of the Ihara zeta functions, which also shows the properties of the almost Ramanujan graphs corresponding to the graph Riemann Hypothesis.

2. Regular 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. [3]).

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 ([4])**.** *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.

3. Ihara zeta function

For a graph $X = (V, E)$ and a path $C = a_1 a_2 \cdots a_s$ where a_j is an oirented edge of X, we say that it has a backtrack if $a_{j+1} = a_j^{-1}$ for some $j = 1, ..., s-1$ and a tail if $a_s = a_1^{-1}$. The length of C is $s = \nu(C)$ and C is called a closed path or cycle if the starting vertex is the same as the terminal vertex.

The closed path $C = a_1 \cdots a_s$ is called a primitive or prime path if it has no backtrack or tail and $C \neq D^n$, $n \geq 2$. For the closed path $C = a_1 \cdots a_s$, the equivalence class $[C]$ is the following set

$$[C] = \{a_1 \cdots a_s,\ a_2 \cdots a_s a_1,\ ...,\ a_s a_1 \cdots a_{s-1}\}.$$

A prime in the graph X is an equivalent class $[C]$ of prime paths. The length of the path C is denoted by $\nu(C) = s$.

Definition 3.1. The Ihara zeta function for a finite connected graph without 1-degree vertices is defined to be the following function o the complex number u, with $|u|$ sufficiently small,

$$\zeta_X(u) = \prod_{[P]} (1 - u^{\nu(P)})^{-1}$$

where the product is over all the primes $[P]$ in X.

Definition 3.2. The radius of the largest circle o f convergence of $\zeta_X(u)$ is denoted by R_X.

When X is a $(q+1)$-regular graph, $R_X = 1/q$.

Definition 3.3. Let X be a connected $(q+1)$-regular graph. We say that the Ihara zeta function $\zeta_X(q^{-s})$ satisfies the Riemann Hypothesis iff, when $0 < \text{Re } s < 1$,

$$\zeta_X(q^{-s})^{-1} = 0 \Rightarrow \text{Re } s = \frac{1}{2}.$$

If $u = q^{-s}$, Re $s = \frac{1}{2}$ means that $|u| = 1/\sqrt{q}$.

The following theorem shows the deep and significant relation between the Ramanujan graph and the number theory (cf. [14]).

Theorem 3.4. *For a connected $(q+1)$-regular graph X, $\zeta_X(u)$ satisfies the Riemann Hypothesis if and only if the graph X is Ramanujan.*

4. Pseudorandom number generator

In this section we construct the adjacency matrices of nonregular Ramanujan graphs, using the pseudorandom number generator given in [11] and following the method in [10].

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

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

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

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

(see [12]). In [11] 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 (cf. [13]).
(3): For an integer $m \sim 10$, a precision order, we calculate the approximate sequence $\{\xi_{k,m}\}$ of $\{\xi_k\}$, given by

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

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 given by

$$A_m = \begin{pmatrix} p^m & 0 & 0 & \dots & 0 \\ \xi_{1,m} & 1 & 0 & \dots & 0 \\ \xi_{2,m} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_{n-1,m} & 0 & 0 & \dots & 1 \end{pmatrix},$$

The matrix A_m 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 [6]).
(5): We apply the LLL reduction algorithm to the matrix A_m. Then we have reduced matrices B_m with small integer elements.
(6): By connecting each rows of B_m, we have the sequence P_l of pseudorandom numbers with its length $(n+1)^2 \sim 10000$.

Furthermore, from this reduced matrix B_m we construct the adjacency matrix for the nonregular Ramanujan graph.
(7): Take the absolute values of elements of B_m.
(8): Construct an upper triangle matrix S_u of B_m, which has the upper triangle part of B_m with 0 diagonal elements.
(9): Calculate $T = S_u + {}^t S_u$.

When the graph given by the adjacency matrix is not simple, we apply the following sage commands, ".remove_loops" and ".remove_multiple_edges" and then we have the simple graph without loops and mutiple edges.

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

$$A_m = \begin{pmatrix} 410338673 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 43730889 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 234660880 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ \vdots & & & & & \ddots & & & & & \vdots \\ 63551984 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 & 0 \\ 68674355 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (50 \times 50)$$

$\longrightarrow$ LLL reduction algorithm $\longrightarrow$

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

$\longrightarrow$ construction of adjacency matrix $\longrightarrow$

$$T_{adj} = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & \cdots & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \cdots & 1 & 1 & 1 & 0 \\ \vdots & & & & \vdots & & & & & \vdots & & \vdots & & \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & \cdots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & \cdots & 0 & 1 & 0 & 0 \end{pmatrix} \quad (50 \times 50).$$

5. almost Ramanujan graph

In the previous section we construct the adjacency matrix for the nonregular Ramanujan graph, using the reduced matrix B_m. Following our previous paper ([10]), we define the various type of 'almost' Ramanujan graphs by using the upper bounds of 'nontrivial' eigenvalues of their adjacency matrices. Correponding to the regular graph case, here in the nonregular case the trivial eigenvalue is the one which has the largest absolute value.

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 $\mu : |\mu| \lneqq \sigma_X$ 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 $\mu : |\mu| \lneqq \sigma_X$.

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 $\mu : |\mu| \lneqq \sigma_X$.

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 diamond marker)
$> 2\sqrt{\sigma_X - 1}$: naive Ramanujan bounds (red diamond marker)
$> 2\sqrt{d_X - 1}$: weak Ramanujan bounds (blue diamond marker).

Next we calculate the eigenvalues and plot the histograms of their distributions (Fig. 2, Fig. 4, Fig. 6. We can see that all absolute values of nontrivial eigenvalues are smaller than the upper bound of each almost Ramanujan bound.

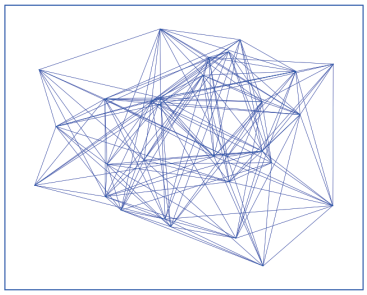

FIGURE 1. Graph:30×30 Adj.Matrix

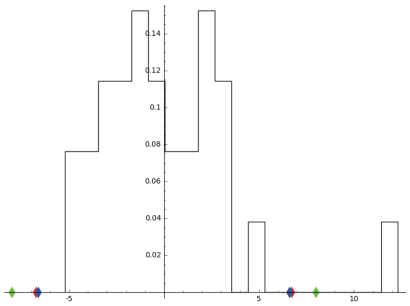

FIGURE 2. eigenval.dist. n=30

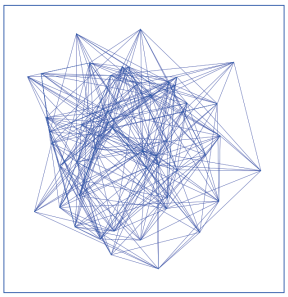

FIGURE 3. Graph:50×50 Adj.Matrix

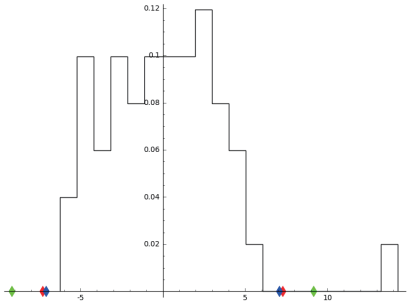

FIGURE 4. eigenval.dist. n=50

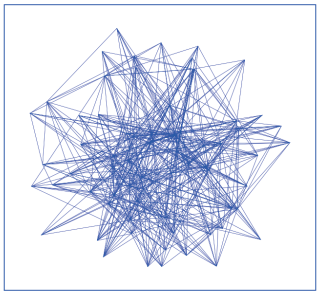

FIGURE 5. Graph:70×70 Adj.Matrix

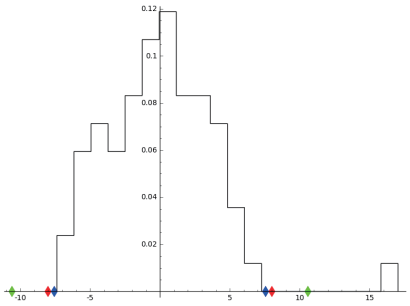

FIGURE 6. eigenval.dist. n=70

6. Weak graph Riemann hypothesis

In Section 3 for the regular graph case we see that the poles of the Ihara zeta function $\zeta_X(u)$, $u = q^{-s} = R_X^s$, satisfies Graph Riemann Hypothesis, that is, they are just on the circle $|u| = \sqrt{R_X}$, Re $s = 1/2$, when $0 <$ Re $s < 1$. In this section we numerically calculate the distribution of poles of $\zeta_X(u)$ for our nonregular pseudorandom graphs, using the determinant formula given by Bass in [2]. We use the same notations and the definitions as those in Section 2, but here we consider the nonregular graphs.

Theorem 6.1 ([2])**.** *Let A be the adjacency matrix of X and Q the diagonal matrix with jth diagonal entry q_j such that q_j+1 is the degree of the jth vertex of X. Then we have the Ihara three-term determinant formula*

$$\zeta_X(u)^{-1} = (1-u^2)^{r-1} \det(I - Au + Qu^2)$$

where r is the rank of th fundamental group of X; $r - 1 = |E| - |V|$.

Following the results obtained by Kotani and Sunagawa in [7] on nonregular graphs, we investigate the 'weak Graph Riemann Hypothesis'.

Theorem 6.2 ([7])**.** *Suppose that a graph X has vertices with maximum degree $q+1$ and minimum degree $p+1$. Then*

(1) *Every pole of $\zeta_X(u)$ satisfies $R_X \le |u| \le 1$ and*

$$q^{-1} \le R_X \le p^{-1}. \tag{6.1}$$

(2) *Every non-real pole of $\zeta_X(u)$ satisfies the inequality*

$$\frac{1}{\sqrt{q}} \le |u| \le \frac{1}{\sqrt{p}}. \tag{6.2}$$

We use the same cases where the vertices numbers are $n = 30, 50, 70$ and the same numerical parameters as those in the previous section. Here we use the floating-point complex numbers with 120 bits precision.

In [14] Terras defined the graph theory Riemann Hypothesis by the following pole free region of $\zeta_X(u)$,

$$R_X < |u| < \sqrt{R_X}.$$

and the weak graph theory Riemann Hypothesis by the following pole free region of $\zeta_X(u)$,

$$R_X < |u| < \frac{1}{\sqrt{q}}.$$

We plot the four circles colored by green, purple, red and blue as follows.

- The green circle is $|u| = R_X$.
- T The purple circle is $|u| = 1/\sqrt{q}$.
- T The red circle is $|u| = \sqrt{R_X}$.
- T The blue circle is $|u| = 1/\sqrt{p}$.

The following inequalities

$$R_X < \frac{1}{\sqrt{q}} < \sqrt{R_X} < \frac{1}{\sqrt{p}}$$

hold.

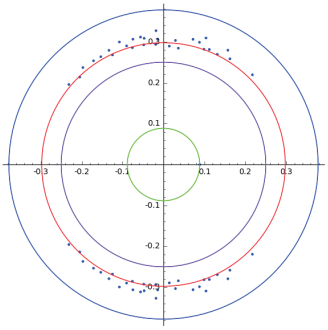

FIGURE 7. PseudoRandomGr:$n30$

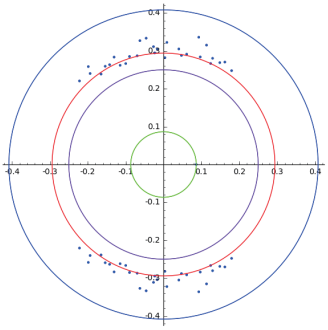

FIGURE 8. RandomGr:$n30$

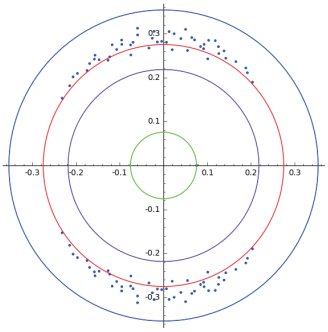

FIGURE 9. PseudoRandomGr:$n50$

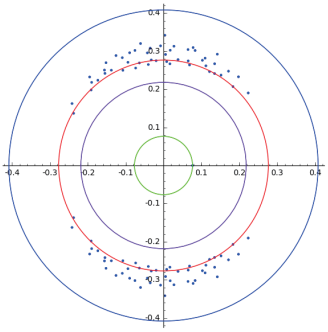

FIGURE 10. RandomGr:$n50$

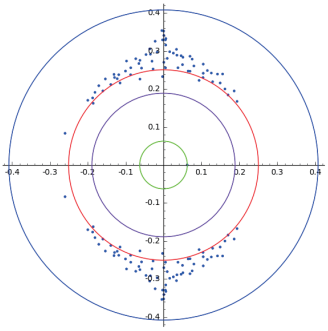

FIGURE 11. PseudoRandomGr:$n70$

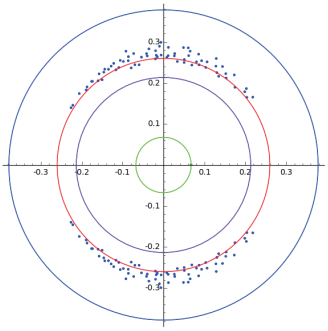

FIGURE 12. RandomGr:$n70$

For the random graphs obtained by using the sage command "graphs.RandomGNM" or "graphs.RandomGNP" we can see that these random graphs have the almost same distributions of poles as those of our pseudorandom graphs. Here we use the

command "graphs.RandomGNM", giving the same numbers of vertices and edges as those in our pseudorandom cases. We can compare the pseudorandom graph to the random graph in each case, n=30, 50, 70.

Remark 6.3. The poles of the zeta functions in the three cases $n = 30, 50, 70$ satisfy the weak GRH and approximately satisfy the GRH. It seems that the larger the degrees of the polynomials given by the determinant formula become, the more these poles be spreading apart from the red circle with its radius $\sqrt{R_X}$, which shows the Riemann Hypothesis. The inequalities (6.2) are satisfied in all cases.

References

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

[2] H. Bass, *The Ihara-Selberg zeta function of a tree lattice*, International. J. Math. **3** (1992), 717–797.

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

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

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

[6] Daniel Goldstein and Andrew Mayer, *On the equidistribution of Hecke points*, Formu Math **15** (2003), 165–189.

[7] M.Kotani and T.Sunagwa, *Zeta functions of finite graphs*, J. Math. Sci. Univ. Tokyo **7** (2000), 7–25.

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

[9] 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.

[10] K. Naito, *Pseudorandom number generator by p-adic chaos and Ramanujan expander graphs*, linear and Nonlinear Analysis **5** (2019), 1–11.

[11] 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.

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

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

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

Manuscript received 9 November 2019
revised 14 April 2020

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