A NOTE ON THE RELATION BETWEEN TWO PROPERTIES OF RANDOM GRAPHS

SHOHEI SATAKE

Abstract. The $t$-existentially closed (t-e.c.) property and pseudo-random property are properties which random graphs asymptotically almost surely satisfy. In this note, by constructing explicit infinite families of graphs without probabilistic arguments, we show that the $t$-e.c. property does not necessarily imply the best possible pseudo-random property. We also discuss the relation between $t$-e.c. graphs and expander graphs.

1. Introduction

Erdős-Rényi random graphs (or random graphs) are graphs on the vertex set $\{1,2,\ldots,n\}$ which can be obtained by choosing edges independently with probability $p$ (for details, see e.g. [8 Chapter 11]). The probability $p$ is called edge probability. For a property $P$, we say that random graphs asymptotically almost surely (a.a.s) satisfy $P$ if the probability of the event that graphs satisfy $P$ tends to 1 when $n$ goes to infinity. In graph theory, the properties which random graphs a.a.s. satisfy have been investigated. In this note, we deal with two such properties, namely, the $t$-existentially closed (t-e.c.) property and best pseudo-random property. The $t$-e.c. property is defined as a prescribed adjacency property for each positive integer $t$. And graphs satisfying the best pseudo-random property are best possible, in the sense of the description in Krivelevich-Sudakov [11, Section 2.2], among pseudo-random graphs. We give the definitions in Section 2.

There seem to be many constructions of the best pseudo-random graphs which are not $t$-e.c. graphs. In fact, Cameron-Stark [6] described graphs which are best pseudo-random but not $t$-e.c. for any $t \geq 4$, which implies that the best pseudo-random graphs are not necessarily $t$-e.c. graphs. On the other hand, there seem only few explicit constructions (without probabilistic arguments) of infinite families of $t$-e.c. graphs. And known infinite families of $t$-e.c. graphs are also best pseudo-random or quite unclear whether they are best pseudo-random or not. (see e.g. [3]). For example,
Paley graphs of sufficiently large order are $t$-e.c. for each $t \geq 1$ (see [3]) and they are also the best pseudo-random graphs (see e.g. [11, Section 2.5]). Now it seems natural to consider the following question.

**Problem 1.1.** For each $t \geq 1$, are there $t$-e.c. graphs which are not the best pseudo-random graphs?

In this note, by giving an explicit construction, we prove that the answer is “Yes” for any $t \geq 1$. The rest of this note is organized as follows. In Section 2 we give the definitions of the $t$-e.c. property and best pseudo-random property. In Section 3 we construct infinite families of $t$-e.c. graphs which are not best pseudo-random for every $t \geq 1$ without probabilistic arguments. Here we develop the method applied for Paley graphs by combining some elementary number-theoretic observations. In Section 4 based on our construction, we discuss the relation between $t$-e.c. graphs and expander graphs which are closely related to the best pseudo-random graphs.

2. **The $t$-e.c. Property and Best Pseudo-Random Property**

In this section, we give the definitions of the $t$-e.c. property and best pseudo-random property and introduce some related facts.

Let $t$ be a positive integer. A graph is called a \textit{t-existentially closed (t-e.c.) graph} if for any two disjoint subsets of vertex set, say $A$ and $B$, satisfying $|A \cup B| = t$, there exists a vertex $z \notin A \cup B$ such that $z$ is adjacent to all vertices of $A$ but no vertices of $B$. Here $A$ or $B$ may be empty set. We also call this adjacency property the \textit{t-e.c. property}. This property was originally come from a result in Erdős-Rényi [9] showing the characteristic property of the countable random graph (see [5]). And a simple probabilistic argument shows that random graphs with constant edge probability a.a.s. satisfy the $t$-e.c. property for any $t \geq 1$ (see e.g. [4]). As noted in Blass-Harary [2], the $t$-e.c. property gives much information of random graphs, for example, diameter and connectivity.

Let $0 < p(n) < 1 \leq \alpha$. A graph is called a \textit{(p(n), \alpha)-jumbled graph} if for any subset $U$ of vertex set,

$$
|e(U) - p(n) \cdot \binom{|U|}{2}| \leq \alpha \cdot |U|.
$$

(2.1)

This notion was defined by Thomason [15] and [16]. In this note, we deal with the following property as the best possible property among jumbled graphs (for details and background, see [11, Section 2.2]). We call graphs with $n$ vertices the \textit{best pseudo-random graphs} if they are $(p(n), \alpha)$-jumbled and $\alpha = O(\sqrt{n \cdot p(n)})$ as $n \to \infty$, where $e(U)$ is the number of edges of the subgraph induced by $U$. We also call this property the \textit{best pseudo-random property}. And, as noted in [11, Section 2.2], random graphs with edge probability $p = p(n)$ a.a.s. satisfy the best pseudo-random property.
This property also provides some non-trivial estimations of, for example, independence number and connectivity (see [11]).

We note that, for regular graphs, the best pseudo-random property can be described by using the eigenvalues of its adjacency matrix. Here the adjacency matrix of a graph on the vertex set \( \{1, 2, \ldots, n\} \) is the \((0, 1)\)-square matrix of order \( n \) such that the \((i, j)\)-entry is 1 if and only if \( i \) and \( j \) are adjacent. Let \( G \) be a \( d(n) \)-regular graph with \( n \) vertices and suppose that \( d(n) = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \) are eigenvalues of its adjacency matrix. And let \( \lambda(G) = \max\{\lambda_2, -\lambda_n\} \). Then, the expander-mixing lemma (see e.g. [1, Chapter 9]) tells us that \( G \) is \((d(n)/n, \lambda(G))\)-jumbled. Thus, we see that a \( d(n) \)-regular graph \( G \) is best pseudo-random if \( \lambda(G) = O(\sqrt{d(n)}) \) as \( n \to \infty \). Roughly speaking, this implies that the best pseudo-random \( d(n)\)-regular graphs behave like random graphs with edge probability \( p = d(n)/n \) (see also [11, Section 2.4]). We note that if \( d(n) \leq (1 - \delta)n \) for some \( \delta > 0 \), then \( \lambda(G) \geq \Omega(\sqrt{d(n)}) \) as shown in [11, Section 2.4]. Thus the best pseudo-random regular graphs are best possible up to constant in the sense of graph eigenvalues.

### 3. An explicit construction

In this section, we construct infinite families of \( t \)-e.c. graphs which do not have the best pseudo-random property. Let \( q \equiv 1 \pmod{4} \) be a prime and \( e \geq 1 \) be an odd integer. We construct Cayley graphs over the additive group of the residue ring \( \mathbb{Z}_{q^e} := \mathbb{Z}/q^e\mathbb{Z} \) as follows.

**Definition 3.1.** The graph \( G_{q^e} \) is the graph with vertex set \( \mathbb{Z}_{q^e} \) and edge set \( \{(x, y) \mid \chi_{q^e}(x - y) = 1\} \), where \( \chi_{q^e}(x) := (\frac{x}{q^e})_q \), where \( (\frac{x}{q}) \) is the Legendre symbol.

Since \( q \) satisfies \( q \equiv 1 \pmod{4} \), \( G_{q^e} \) is well-defined. And when \( e = 1 \), the graph \( G_q \) is the Paley graphs with \( q \) vertices. Moreover, by the following proposition, we see that \( G_{q^e} \) is a special case of quadratic unitary Cayley graphs defined by Liu-Zhou [12].

**Proposition 3.2.** \( G_{q^e} \) is the Cayley graphs defined by the set of non-zero unit squares \( S := \{u^2 \mid u \in \mathbb{Z}_{q^e}^*\} \) where \( \mathbb{Z}_{q^e}^* \) is the multiplicative group of \( \mathbb{Z}_{q^e} \). That is, two distinct vertices \( x \) and \( y \) are adjacent in \( G_{q^e} \) if and only if \( x - y \in S \).

**Proof.** By the definition of \( G_{q^e} \), two distinct vertices \( x \) and \( y \) are adjacent in \( G_{q^e} \) if and only if \( \chi_{q^e}(x - y) = 1 \). Since \( e \) is odd, \( \chi_{q^e}(x - y) = 1 \) if and only if \( (\frac{x-y}{q}) = 1 \), that is, \( x - y \) is a nonzero square modulo \( q \). Finally, from the Hensel's lemma (see e.g. [14, Chapter 13]), \( x - y \) is a nonzero square modulo \( q \) if and only if \( x - y \in S \). \( \square \)

By Definition 3.1 and Proposition 3.2, we see the following proposition.

**Proposition 3.3.** (1) \( G_{q^e} \) has \( q^e \) vertices.
(2) $G_{q^e}$ is a $(q^e - q^{e-1})/2$-regular graph.

Proof. (1) is directly obtained from Definition 3.1. We prove (2). By Proposition 3.2, we see that $G_{q^e}$ is $|S|$-regular and so we shall compute the size of $S$. Note that $\mathbb{Z}_{q^e}^*$ is the cyclic group of order $\varphi(q^e) = q^e - q^{e-1}$ where $\varphi$ is the Euler’s totient function. Let $x$ be a generator of $\mathbb{Z}_{q^e}^*$. Clearly, $S = \{x^{2a} \mid 1 \leq a \leq (q^e - q^{e-1})/2\}$, completing the proof. \hfill \Box

The following theorem is our main result.

**Theorem 3.4.** For every $t \geq 1$, $G_{q^e}$ is $t$-e.c. if $q$ and $e$ satisfy

\[(3.1) \quad q^e - (t2^{t-1} - 2^t + 1)q^{e-\frac{t}{2}} - t2^tq^{e-1} + t2^{t-1} > 0.\]

To prove the Theorem 3.4, we apply for the method used in [3]. Based on their discussion, we shall prove that

\[(3.2) \quad f(A, B) := \sum_{z \in \mathbb{Z}_{q^e} \setminus Z_{A,B}} \prod_{a \in A} \{1 + \chi_{q^e}(z - a)\} \prod_{b \in B} \{1 - \chi_{q^e}(z - b)\} > 0
\]

for all disjoint subsets $A, B \subset \mathbb{Z}_{q^e}$ such that $|A \cup B| = t$ if (3.1) holds. Here $Z_{A,B}$ is the set of elements $z$ such that $z - c = qv$ for some $c \in A \cup B$ and $v \in \mathbb{Z}_{q^e}$. Remark that, in the range of $z$ in the first sum, we must exclude the elements of $Z_{A,B}$ since, if $z - c = qv$ for some $c \in A \cup B$ and $v \in \mathbb{Z}_{q^e}$, then $z$ cannot satisfy the definition of the $t$-e.c. property. In fact, if so, from the definition of $\chi_{q^e}$, $z$ cannot be adjacent to any $c \in A \cup B$ in $G_{q^e}$. Now let $Z_{A,B}^* = Z_{A,B} \setminus (A \cup B)$ and

\[g(A, B) := \sum_{z \in \mathbb{Z}_{q^e} \setminus Z_{A,B}^*} \prod_{a \in A} \{1 + \chi_{q^e}(z - a)\} \prod_{b \in B} \{1 - \chi_{q^e}(z - b)\}.\]

Note that, in the range of $z$ in the first sum, the set $A \cup B$ is added. To obtain (3.2), we shall obtain a lower bound of $g(A, B)$. To explain why, let

\[h(A, B) := \sum_{z \in A \cup B} \prod_{a \in A} \{1 + \chi_{q^e}(z - a)\} \prod_{b \in B} \{1 - \chi_{q^e}(z - b)\}.\]

Then we can easily see that

\[(3.3) \quad h(A, B) \leq t2^{t-1}.\]

And we also see that

\[(3.4) \quad f(A, B) = g(A, B) - h(A, B)\]

since $\mathbb{Z}_{q^e} \setminus Z_{A,B} = (\mathbb{Z}_{q^e} \setminus Z_{A,B}^*) \setminus (A \cup B)$. So, by combining that lower bound of $g(A, B)$, (3.3) and (3.4), we will get (3.2). To get a lower bound of $g(A, B)$, at first, we give the following character sum estimation over $\mathbb{Z}_{q^e}$ by combining a known character sum estimation and elementary number-theoretic observations.
Lemma 3.5. Let $k \geq 1$ be a integer and $a_1, a_2, \ldots, a_k$ be distinct elements of $\mathbb{Z}_{q^e}$. Then,
\begin{equation}
\sum_{x \in \mathbb{Z}_{q^e}} \chi_{q^e}(x - a_1) \cdots \chi_{q^e}(x - a_k) \leq (k - 1)q^{e-\frac{1}{2}}.
\end{equation}

Proof of Lemma 3.5. We shall prove that
\begin{equation}
\sum_{x \in \mathbb{Z}_{q^e}} \chi_{q^e}(x - a_1) \cdots \chi_{q^e}(x - a_k) = q^{e-1} \sum_{x \in \mathbb{Z}_q} \chi_{q}(x - a_1) \cdots \chi_{q}(x - a_k)
\end{equation}
since we can use the following Burgess’s estimation (see e.g. [13, Chapter II.2]);
\begin{equation}
\sum_{x \in \mathbb{Z}_q} \chi_{q}(x - a_1) \cdots \chi_{q}(x - a_k) \leq (k - 1)\sqrt{q}.
\end{equation}

First, $\chi_{q^e}$ is a Dirichlet character modulo $q^e$ of conductor $q$, that is, $\chi_{q^e}(x) = \chi_{q^e}(y)$ whenever $x \equiv y \pmod{q}$. So $\chi_{q^e}$ can be regarded as the primitive Dirichlet character $\chi_q$ modulo $q$. Next observe that, for any $x \in \mathbb{Z}_{q^e}$, there uniquely exist $a_0, a_1, \ldots, a_{e-1} \in \mathbb{Z}_q$ such that $x = a_0 + a_1q + a_2q^2 + \cdots + a_{e-1}q^{e-1}$. Therefore, for any $a \in \mathbb{Z}_q$, there are $q^{e-1}$ elements $x \in \mathbb{Z}_{q^e}$ such that $\chi_{q^e}(x) = \chi_{q^e}(a)$, completing the proof.

Now we can get the following lower bound of $g(A, B)$.

Lemma 3.6.
\begin{equation}
g(A, B) \geq q^e - (t2^{t-1} - 2t + 1)q^{e-\frac{1}{2}} - t2^{t}q^{e-1} + t2^t.
\end{equation}

Proof of Lemma 3.6. First, we obtain that
\begin{equation}
\sum_{z \in \mathbb{Z}_{q^e} \setminus Z_{A,B}^*} 1 \geq q^e - tq^{e-1} + t
\end{equation}
since $|Z_{A,B}| \leq t(q^e - \phi(q^e)) = tq^{e-1}$ and $\mathbb{Z}_{q^e} \setminus Z_{A,B}^*$ contains $A \cup B$.

Now let $A \cup B = \{c_1, c_2, \ldots, c_t\}$. From the definition of $g(A, B)$ and the triangle inequality, we see that
\begin{equation}
\bigg| g(A, B) - \sum_{z \in \mathbb{Z}_{q^e} \setminus Z_{A,B}^*} 1 \bigg| = \bigg| \sum_{1 \leq k \leq t} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq t} \chi_{q^e}(z - c_{i_1}) \cdots \chi_{q^e}(z - c_{i_k}) \bigg|
\end{equation}
For each $1 \leq k \leq t$ and $1 \leq i_1 < i_2 < \cdots < i_k \leq t$, we obtain
\begin{equation}
\bigg| \sum_{z \in \mathbb{Z}_{q^e} \setminus Z_{A,B}^*} \chi_{q^e}(z - c_{i_1}) \cdots \chi_{q^e}(z - c_{i_k}) \bigg| \leq (k - 1)q^{e-\frac{1}{2}} + tq^{e-1} - t.
\end{equation}
In fact, we get (3.11) since
\[
\sum_{\mathbf{z} \in \mathbf{Z} \setminus \mathbf{Z}_{A,B}^*} \chi_{q^e}(\mathbf{z} - c_{i_1}) \cdots \chi_{q^e}(\mathbf{z} - c_{i_k}) = \sum_{\mathbf{z} \in \mathbf{Z}_{q^e}} \chi_{q^e}(\mathbf{z} - c_{i_1}) \cdots \chi_{q^e}(\mathbf{z} - c_{i_k})
\]
\[ - \sum_{\mathbf{z} \in \mathbf{Z}_{A,B}^*} \chi_{q^e}(\mathbf{z} - c_{i_1}) \cdots \chi_{q^e}(\mathbf{z} - c_{i_k}),
\]
and from Lemma 3.5 and the fact that \(|\mathbf{Z}_{A,B}^*| = |\mathbf{Z}_{A,B}| - |A \cup B| \leq tq^{e-1} - t\). Thus, by (3.10) and (3.11),
\[
(3.12)
\]
\[
\left| g(A, B) - \sum_{\mathbf{z} \in \mathbf{Z}_{q^e} \setminus \mathbf{Z}_{A,B}^*} 1 \right| \leq \sum_{1 \leq k \leq t} \left( \begin{pmatrix} t \end{pmatrix} \right) \{(k - 1)q^{e-\frac{1}{2}} + tq^{e-1} - t\}
\]
\[ = q^{e-\frac{1}{2}}t \sum_{0 \leq k \leq t-1} \left( \begin{pmatrix} k \end{pmatrix} \right) + (tq^{e-1} - t - q^{e-\frac{1}{2}}) \sum_{1 \leq k \leq t} \left( \begin{pmatrix} t \end{pmatrix} \right)
\]
\[ = t2^{t-1}q^{e-\frac{1}{2}} + (2^t - 1)(tq^{e-1} - t - q^{e-\frac{1}{2}})
\]
\[ = (t2^{t-1} - 2^t + 1)q^{e-\frac{1}{2}} + t(2^t - 1)q^{e-1} - t(2^t - 1).
\]
By (3.9) and (3.12), we get (3.8).

We remark that a slightly weaker statement also can be obtained by estimating the quadratic Gauss sum over \(\mathbf{Z}_{q^e}\).

At last, we note that Chung-Graham-Wilson [7] showed the mutually equivalence of some properties which random graphs a.a.s. satisfy. Such properties are simply called the quasi-random property. Proposition 3.3 and Theorem 3.7 show that the graph \(G_{q^e}\) also shares the quasi-random property.
4. A remark on $t$-e.c. graphs and expander graphs

In this section, we discuss the relation between $t$-e.c. graphs and expander graphs. Here we define expander graphs following the manner in [10]. For a graph $G = (V,E)$, the edge expansion ratio $h(G)$ is defined by

$$h(G) := \min \left\{ \frac{|\partial(Y)|}{|Y|} \mid Y \subset V, |S| \leq \frac{|Y|}{2} \right\}.$$  

Here $\partial(Y)$ is the set of edges $e \in E$ such that one end is in $Y$ and another end is in $V \setminus Y$. A graph $G$ is called a expander graph if $h(G) \geq \varepsilon$ holds for some $\varepsilon > 0$. We may say that expander graphs satisfying $h(G) \geq \varepsilon$ for large $\varepsilon$ are “highly connected”. For $d(n)$-regular graphs $G$ on $n$ vertices, the Cheeger type inequality shows that $h(G) \geq (d(n) - \lambda_2)/2$ (see e.g. [10]). So regular graphs whose the spectral gap $d(n) - \lambda_2$ is large (or equivalently $\lambda_2$ is small) will be good expander graphs. Especially the best pseudo-random regular graphs form very good expander graphs in the above sense (see also [1, Chapter 9], [14]).

On the other hand, $t$-e.c. graphs are connected from the definition and moreover, as shown in [2, Corollary 14], they are $\lfloor t/2 \rfloor$-(vertex and edge)-connected. Thus, expander regular graphs with large spectral gap and $t$-e.c. graphs for large $t$ possibly have “high connectivity”.

However Theorem 3.4 and 3.7 show that there exist infinite families of $t$-e.c. graphs which are not the best pseudo-random graphs for all $t \geq 1$. Moreover, for each $e \geq 3$, $\lambda_2$ of $G_{pe}$ is greater than the order of $\sqrt{\text{degree}}$. Thus we see that for any $t$, $t$-e.c. graphs do not necessarily ensure that they are the expander graphs with the largest spectral gap (up to constant).

Acknowledgements. First, we would like to appreciate Masanori Sawa for introducing the concept of $t$-e.c. graphs. We also would like to give special thanks to Gary Greaves for his comments leading to Section 4. At last, we would like to appreciate Sanming Zhou for telling us the paper [12].

References

[1] N. Alon, J. H. Spencer, The Probabilistic Method. Fourth edition, John Wiley & Sons, Inc., 2016.
[2] A. Blass, F. Harary, Properties of almost all graphs and complexes. J. Graph Theory 3(3): 225–240, 1979.
[3] A. Blass, G. Exoo, F. Harary, Paley graphs satisfy all first-order adjacency axioms. J. Graph Theory 5(4): 435–439, 1981.
[4] A. Bonato, The search for $N$-e.c. graphs, Contrib. Discrete Math. 4(1): 40–53, 2009.
[5] P. Cameron, The random graph. In The mathematics of Paul Erdős II, volume 14 of Algorithms Combin., pages 333–351. Springer, 1997.
[6] P. J. Cameron, D. Stark, A prolific construction of strongly regular graphs with the $n$-e.c. property. Electron. J. Combin., 9(1): #31, 2002.
[7] F. R. K. Chung, R. L. Graham, R. M. Wilson, Quasi-random graphs. Combinatorica, 9(4): 345–362, 1989.
[8] R. Diestel, Graph Theory. Fourth edition, Springer, 2010.
[9] P. Erdős, A. Rényi, Asymmetric graphs. *Acta Math. Acad. Sci. Hungar.*, 14: 295–315, 1963.
[10] S. Hoory, N. Linial, A. Wigderson, Expander graphs and their applications. *Bull. Amer. Math. Soc. (N.S.)* 43(4): 439–561, 2006.
[11] M. Krivelevich, B. Sudakov, Pseudo-random graphs. In *More sets, graphs and numbers*, pages 199–262. Springer-Verlag, 2006.
[12] X. Liu, S. Zhou, Quadratic unitary Cayley graphs of finite commutative rings. *Linear Algebra Appl.*, 479: 73–90, 2015.
[13] W. M. Schmidt, Equations over Finite Fields : An Elementary Approach. Springer-Verlag, 1976.
[14] T. Szabó, On the spectrum of projective norm-graphs. *Inform. Process. Lett.*, 86(2): 71–74, 2003.
[15] A. Thomason, Pseudorandom graphs. *Ann. Discrete Math.*, 33: 307–331, 1987.
[16] A. Thomason, Random graphs, strongly regular graphs and pseudorandom graphs. In *Surveys in combinatorics 1987*, Volume 123 of *London Math. Soc. Lecture Note Ser.*, pages 173–195, Cambridge Univ. Press, 1987.
[17] Z.-X. Wan, Finite Fields and Galois Rings. World Scientific Publishing Co. Pte. Ltd., 2012.

Graduate School of System Informatics, Kobe University, Rokkodai 1-1, Nada, Kobe, 657-8501, JAPAN

E-mail address: 155x601x@stu.kobe-u.ac.jp