Yoshiharu Kohayakawa; Vojtěch Rödl; Mathias Schacht
Discrepancy and eigenvalues of Cayley graphs

Czechoslovak Mathematical Journal, Vol. 66 (2016), No. 3, 941–954

Persistent URL: `http://dml.cz/dmlcz/145881`

Czechoslovak Mathematical Journal, 66 (141) (2016), 941–954

DISCREPANCY AND EIGENVALUES OF CAYLEY GRAPHS

Yoshiharu Kohayakawa, São Paulo, Vojtěch Rödl, Atlanta,
Mathias Schacht, Hamburg

(Received February 5, 2016)

Dedicated to the memory of Professor Miroslav Fiedler

Abstract. We consider quasirandom properties for Cayley graphs of finite abelian groups. We show that having uniform edge-distribution (i.e., small discrepancy) and having large eigenvalue gap are equivalent properties for such Cayley graphs, even if they are sparse. This affirmatively answers a question of Chung and Graham (2002) for the particular case of Cayley graphs of abelian groups, while in general the answer is negative.

Keywords: eigenvalue; discrepancy; quasirandomness; Cayley graph

MSC 2010: 05C50, 05C80

1. Introduction

Professor Miroslav Fiedler discovered a very fruitful relationship between connectivity properties of graphs and their spectra. Among other things, his works [15], [14] from the 1970s, together with an other pioneering work [18], [13], [12], gave birth to what is now known as *spectral partitioning of graphs.* Fiedler considered the so called combinatorial Laplacian $L(G)$ of graphs G and their spectra $0 = \lambda_1 \leqslant \lambda_2 \leqslant \ldots \leqslant \lambda_n$ ($n = |V(G)|$). Generalizing the fact that G is connected if and only if $\lambda_2 > 0$, Fiedler named λ_2 the *algebraic connectivity* of G and went on to prove that λ_2 is a lower bound for the standard connectivity of G (unless G is the complete graph).

The first author was supported by FAPESP (2013/03447-6, 2013/07699-0), CNPq (459335/2014-6, 310974/2013-5) and Project MaCLinC/USP. The second author was supported by NSF grant DMS 1301698. The third author was supported through the *Heisenberg-Programme* of the DFG. The collaboration of the first and third authors is supported by CAPES/DAAD PROBRAL project 430/15.

Furthermore, he also considered partitioning the vertex set of G by considering the coordinates of the eigenvector belonging to λ_2. The algebraic connectivity of a graph is now sometimes referred to as the *Fiedler value* and the associated eigenvector is referred to as the *Fiedler vector*. Alon [1] and Sinclair and Jerrum [26] later proved that graphs with small Fiedler value can be partitioned according to the Fiedler vector in a direct way to produce a cut that is small in relative terms (that is, in terms of the ratio of the number of cut edges to the number of separated vertices).

While a small Fiedler value tells us that the graph in question may be split along a "small cut", a large Fiedler value implies that the graph is an *expander*, that is, it has no cuts that are "small", see [4], [29]. In this paper, we investigate the relation between such "edge-distribution properties" and spectra, but focusing on the case of "uniform edge-distribution", by which we mean the *quasirandom* case, in the sense of Chung, Graham and Wilson, see [9][1]. Since we shall be concerned with Cayley graphs, which are regular graphs, for simplicity, we shall work with adjacency matrices and *not* with combinatorial Laplacians.

Let an n-vertex graph G be given. The *eigenvalues* of G are simply the eigenvalues of the n by n, 0–1 adjacency matrix of G, with 1 indicating edges. Let $\lambda_k = \lambda_k(G)$ be the kth largest eigenvalue of G, in absolute value. Recall that G is said to be "quasirandom" if the edges of G are "uniformly distributed" (we postpone the precise definition; see Definition 1.1). A fundamental result relating the λ_i to quasirandomness states that there is a large gap between λ_1 and λ_k, $k \geqslant 2$, *if and only if* G is quasirandom.

The assertion above may be turned precise in different ways. We are interested in the form given by Chung, Graham, and Wilson, see [9]. Recall that [9] presents a "theory of quasirandomness" for graphs, exhibiting several, quite disparate almost sure properties of graphs that are, quite surprisingly, equivalent in a deterministic sense. Earlier work in this direction is due to Thomason [30] (see also [31]), and also Alon [1], Alon and Chung [2], Frankl, Rödl and Wilson [16], and Rödl [24]. One of the so-called "quasirandom properties" that is presented in [9] is the "eigenvalue gap" between λ_1 and λ_k, $k \geqslant 2$.

Chung and Graham in [8] set out to investigate the extension of the results in [9] to *sparse graphs*, that is, graphs with vanishing edge-density. As it turns out, a naïve approach to such a project is doomed to fail, as the results in [9] *do not* generalize to the "sparse case" in the expected manner (for a thorough discussion on this point, the interested reader is referred to [8] and also to [3], [7], [10], [19], [20], [21]). In particular, having succeeded in proving that eigenvalue gap does imply uniform

[1] Owing to this focus, spectral graph partitioning will not be discussed here; the interested reader is referred to, e.g., Spielman [27] and Spielman and Teng [28].

distribution of edges in the sparse case, Chung and Graham asked whether the converse also holds (see [8], page 230). An affirmative answer to this question would fully generalize the relationship between these two concepts to the sparse case.

However, Krivelevich and Sudakov in [21] showed that the answer to the question posed by Chung and Graham is negative, by constructing a suitable family of counterexamples. Here, our aim is to show that *the answer is affirmative if one considers Cayley graphs of finite abelian groups, regardless of the density of the graph.* It is worth noting that several explicit constructions of quasirandom graphs are indeed Cayley graphs (see, e.g., [31] and [21], Section 3).

We use the following notation. If $G = (V, E)$ is a graph, we write $e(G)$ for the number of edges $|E|$ in G. If $U \subset V$ is a set of vertices of G, then $G[U]$ denotes the subgraph of G induced by U. Furthermore, if $W \subset V$ is disjoint from U, then we write $G[U, W]$ for the bipartite subgraph of G naturally induced by the pair (U, W). We also sometimes write $E(U, W) = E_G(U, W)$ for the edge set of $G[U, W]$.

If $\delta > 0$, we write $x \sim_\delta y$ to mean that

$$(1 - \delta)y \leqslant x \leqslant (1 + \delta)y.$$

Moreover, sometimes it will be convenient to write $O_1(\delta)$ for any term β that satisfies $|\beta| \leqslant \delta$. Observe that, clearly, $x \sim_\delta y$ is equivalent to $x = (1 + O_1(\delta))y$.

Definition 1.1 (DISC(δ)). Let $0 < \delta \leqslant 1$ be given. We say that an n-vertex graph G ($n \geqslant 2$) satisfies property DISC(δ) if the following assertion holds: for all $U \subset V(G)$ with $|U| \geqslant \delta n$, we have

$$e_G(U) = e(G[U]) \sim_\delta e(G)\binom{|U|}{2}\Big/\binom{n}{2}.$$

The following concept of DISC_2 is very much related to DISC, as we shall see next.

Definition 1.2 ($\mathrm{DISC}_2(\delta')$). Let $0 < \delta' \leqslant 1$ be given. We say that an n-vertex graph G ($n \geqslant 2$) satisfies property $\mathrm{DISC}_2(\delta')$ if the following assertion holds: for all disjoint U and $W \subset V(G)$ with $|U|$, $|W| \geqslant \delta' n$, we have

$$e_G(U, W) = e(G[U, W]) \sim_{\delta'} e(G)|U||W|\Big/\binom{n}{2}.$$

The following fact is very easy to prove and we omit its proof.

Fact 1.3. *For any* $0 < \delta' \leqslant 1$, *there is* $0 < \delta = \delta(\delta') \leqslant 1$ *such that any graph that satisfies* DISC(δ) *must also satisfy* $\mathrm{DISC}_2(\delta')$.

Given a graph G, let $\mathbf{A} = (a_{uv})_{u,v \in V(G)}$ be the 0–1 adjacency matrix of G, with 1 denoting edges. The *eigenvalues* of G are simply the eigenvalues of $\mathbf{A}$. Since $\mathbf{A}$ is symmetric, its eigenvalues are real. As usual, we adjust the notation so that these eigenvalues are such that

$$\lambda_1 \geqslant |\lambda_2| \geqslant \ldots \geqslant |\lambda_n| \tag{1.1}$$

(the fact that $\lambda_1 \geqslant 0$ follows, for instance, from the fact that the sum of the λ_i's is equal to the trace of $\mathbf{A}$, which is 0).

Definition 1.4 (EIG(ε))**.** Let $0 < \varepsilon \leqslant 1$ be given. We say that an n-vertex graph G satisfies property EIG(ε) if the following holds. Let $\bar{d} = \bar{d}(G) = 2e(G)/n$ be the average degree of G, and let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of G, with the notation adjusted in such a way that (1.1) holds. Then

(i) $\lambda_1 \sim_\varepsilon \bar{d}$,
(ii) $|\lambda_i| \leqslant \varepsilon \bar{d}$ for all $1 < i \leqslant n$.

Finally, we define Cayley graphs.

Definition 1.5 (Cayley graph $G(\Gamma, A)$)**.** Let Γ be an abelian group and suppose that $A \subset \Gamma \setminus \{0\}$ is symmetric, that is, $A = -A$. The *Cayley graph* $G = G(\Gamma, A)$ is defined to be the graph on Γ, with two vertices γ and $\gamma' \in \Gamma$ adjacent in G if and only if $\gamma' - \gamma \in A$.

We only consider finite graphs and finite abelian groups. The main aim is to answer the question of Chung and Graham from [8] in the affirmative for an interesting class of graphs.

Theorem 1.6. *For every $\varepsilon > 0$, there exist $\delta > 0$ and n_0 such that the following holds. Let $G = G(\Gamma, A)$ be a Cayley graph for some abelian group Γ with $n = |\Gamma| \geqslant n_0$ elements and a symmetric set $A = -A \subseteq \Gamma \setminus \{0\}$. If G satisfies property* DISC(δ)*, then G satisfies* EIG(ε)*.*

The proof of this theorem is given in Section 2. We close this introduction with a few remarks concerning Theorem 1.6.

We first observe that Theorem 1.6, together with the results of Chung and Graham in [8], implies that properties DISC and EIG are equivalent for Cayley graphs. More precisely, by "DISC *implies* EIG *for Cayley graphs*" we mean the following: for every $\varepsilon > 0$ there is a $\delta = \delta(\varepsilon) > 0$ such that, for any sequence of positive integers $(n_k)_k$ with $n_k \to \infty$ as $k \to \infty$, and any sequence $(G_k)_k$ of Cayley graphs with $|V(G_k)| = n_k$, we have that *if all but finitely many graphs G_k satisfy* DISC(δ)*, then all but finitely many G_k satisfy* EIG(ε). Theorem 1.6 tells us that DISC implies EIG for sequences of Cayley graphs. In [8], Theorem 1, it is proved that EIG implies DISC in the same sense for sequences of arbitrary graphs with average degree tending to infinity. This establishes the equivalence of the properties DISC and EIG for Cayley graphs with diverging average degree.

Secondly, we note that in general it is not true that DISC implies EIG for arbitrary sequences of graphs. This was already pointed out by Krivelevich and Sudakov in [21]. For every $\varepsilon > 0$ and every $\delta > 0$, they constructed an infinite sequence of graphs that satisfy DISC(δ) but fail to satisfy (i) in the definition of EIG(ε) (see Definition 1.4).

The following example is a different probabilistic construction: For $p = p(n) \to 0$ with $pn \gg 1$ as $n \to \infty$, consider the graph G given by the union of the random graph $G(n,p)$ and a disjoint clique of size αpn for some constant $\alpha > 0$. Such a graph G has density $(1 + o(1))p$ and for every fixed $\delta > 0$ with high probability it satisfies DISC(δ). However, $\alpha pn - 1$ is one of the eigenvalues of its adjacency matrix and, hence, G fails to satisfy (ii) in the definition of EIG(ε) for any fixed $\varepsilon \in (0, \alpha)$.

We also remark that in [8] it is proved that, under some additional conditions, DISC implies EIG for sequences of sparse graphs. This additional assumption combined with DISC implies that almost every graph in the sequence contains the "expected number" of closed walks of length l for some even $l \geqslant 4$. More precisely, for a sequence of graphs G_n with average degree $\bar{d}_n$ we say that it satisfies CIRCUIT$_l$ if the number of closed walks of length l in G_n is $(1 + o(1))(\bar{d}_n)^l$. We remark that Theorem 1.6 is not a consequence of the result of Chung and Graham, since there exist sequences of Cayley graphs satisfying DISC, and hence by Theorem 1.6 also EIG, but fail to have CIRCUIT$_l$ for any fixed even $l \geqslant 4$. We next sketch the construction of such a sequence.

Let

$$p = p(n) = \frac{\log^2 n}{n}$$

and consider the random cyclic Cayley graph $\mathcal{C}_{n,p} = G(\mathbb{Z}/n\mathbb{Z}, A)$, where independently for every $a \in (\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$ both elements a and $-a$ are included in A with probability $p/2$. It follows from standard Chernoff-type estimates that asymptotically almost surely $\mathcal{C}_{n,p}$ satisfies DISC and has average degree $\bar{d}_n = (1 + o(1))pn$. Consequently, by Theorem 1.6 it also satisfies EIG.

On the other hand, owing to the choice of p we have

$$pn^2 \gg (pn)^l$$

for every fixed even $l \geqslant 4$ and sufficiently large n. Hence, for every even $l \geqslant 4$ in expectation the number of "degenerated walks" which only use one edge is much bigger than $(\bar{d}_n)^l$. This implies that with positive probability $\mathcal{C}_{n,p}$ satisfies DISC and EIG, but fails to satisfy $\mathrm{CIRCUIT}_l$ for every even $l \geqslant 4$. Using appropriate blowups of such graphs yields sequences of Cayley graphs with these properties for any density p with $\log^2 n/n \ll p \ll 1$.

Finally, we remark that very recently Conlon and Zhao [11] extended in Theorem 1.6 for Cayley graphs to arbitrary (not necessarily abelian) finite groups.

Historical remark

The proof of Theorem 1.6 presented here is based on an idea of Tim Gowers, see [17]. The authors proved this result with a longer combinatorial argument (which can be found in the appendix of the arXiv version of this article). On learning about the result, Tim Gowers suggested the alternative, elegant proof given below. We are grateful to him for letting us include his proof here.

2. Proof of the main result

2.1. Eigenvalues of Cayley graphs of abelian groups. Theorem 2.1 below tells us how to compute the eigenvalues of Cayley graphs of abelian groups (Theorem 2.1 follows from a more general result due to Lovász, see [23]; see also [22], Exercise 11.8 and [6]).

Before we state Theorem 2.1, we recall some basic facts about group characters (for more details see, e.g., Serre [25]). Let Γ be a finite abelian group. In this case, an *irreducible character* χ of Γ may be viewed as a group homomorphism $\chi\Gamma \to S^1$, i.e., $\chi(a+b) = \chi(a)\chi(b)$ for all a, $b \in \Gamma$, where S^1 is the multiplicative group of complex numbers of absolute value 1. If Γ has order n, then there are n irreducible characters, say, $\chi_1, \dots, \chi_n$, and these characters satisfy the following *orthogonality property*:

$$\langle \chi_i, \chi_j \rangle = \sum_{\gamma\in\Gamma} \chi_i(\gamma)\chi_j(\gamma) = 0 \tag{2.1}$$

for all $i \neq j$. These facts and a simple computation suffice to prove the following well known result, the short proof of which we include for completeness. We shall use the following notation: if X is a set, we also write X for the $\{0,1\}$-indicator function of X, so that $X(a) = 1$ if $a \in X$ and $X(a) = 0$ otherwise.

Theorem 2.1. *Let $G = G(\Gamma, A)$ be a Cayley graph for some finite abelian group Γ and a symmetric set $A = -A \subseteq \Gamma \setminus \{0\}$. For any character $\chi\Gamma \to S^1$ of Γ, put*

$$\lambda^{(\chi)} = \langle A, \chi\rangle = \sum_{a\in A} \chi(a). \tag{2.2}$$

Then the eigenvalues of G are the $\lambda^{(\chi)}$, where χ runs over all $n = |\Gamma|$ irreducible characters of Γ.

Proof. Let $\chi\Gamma \to S^1$ be an irreducible character of Γ. Let $\lambda^{(\chi)}$ be as defined in (2.2). Consider the vector $\mathbf{v}^{(\chi)} = (\chi(\gamma))^{\mathrm{T}}_{\gamma\in\Gamma}$, with entries indexed by the elements of $\Gamma = V(G)$. Let $\mathbf{A} = (a_{\gamma\gamma'})_{\gamma,\gamma'\in\Gamma}$ be the adjacency matrix of G.

Fix $\gamma \in \Gamma$. Observe that the γ-entry $(\mathbf{Av}^{(\chi)})_\gamma$ of the vector $\mathbf{Av}^{(\chi)}$ is

$$(\mathbf{Av}^{(\chi)})_\gamma = \sum_{a\in A} \chi(\gamma - a) = \sum_{a\in A} \chi(\gamma + a) = \Big(\sum_{a\in A} \chi(a)\Big)\chi(\gamma) = \lambda^{(\chi)}\chi(\gamma),$$

and hence $\mathbf{Av}^{(\chi)} = \lambda^{(\chi)}\mathbf{v}^{(\chi)}$; that is, $\mathbf{v}^{(\chi)}$ is an eigenvector of $\mathbf{A}$ with an eigenvalue $\lambda^{(\chi)}$.

Let $\chi_j\,\Gamma \to S^1$, $1 \leqslant j \leqslant n$, be the irreducible characters of Γ and set $\mathbf{v}_j = \mathbf{v}^{(\chi_j)}$ for all $1 \leqslant j \leqslant n$. By (2.1), $\langle \mathbf{v}_j, \mathbf{v}_{j'}\rangle = 0$ if $j \neq j'$. Therefore, the $\mathbf{v}_j$, $1 \leqslant j \leqslant n$, form an orthogonal basis of eigenvectors of the matrix $\mathbf{A}$ and, hence, $\lambda^{(\chi_j)}$, $j = 1, \dots, n$ are indeed all the eigenvalues of G. $\square$

Remark 2.2. The eigenvalue $\lambda_1 = d = |A|$ may be obtained from (2.2) by letting χ be the trivial character $\chi(x) = 1$ for all $x \in \Gamma$.

2.2. Proof. We shall prove that $\neg\,\mathrm{EIG}(\varepsilon) \Rightarrow \neg\,\mathrm{DISC}(\delta)$. By Theorem 2.1 and Remark 2.2, our assumption implies that there is a character $\chi \not\equiv 1$ such that

$$|\lambda^{(\chi)}| = |\langle A, \chi\rangle| \geqslant \varepsilon|A|. \tag{2.3}$$

We shall fix this χ and use it to construct sets X and $Y \subset V(G)$ that "witness" the fact that $\neg\,\mathrm{DISC}(\delta)$ holds.

We introduce some notation. Let $0 \leqslant \chi_{\arg}(\gamma) < 2\pi$ be defined by $\chi(\gamma) = \mathrm{e}^{\mathrm{i}\chi_{\arg}(\gamma)}$. For $\gamma \in \Gamma$, let

$$c(\gamma) = \mathrm{Re}(\chi(\gamma)) = \cos(\chi_{\arg}(\gamma))$$

and

$$s(\gamma) = \mathrm{Im}(\chi(\gamma)) = \sin(\chi_{\arg}(\gamma)).$$

Applying the orthogonality relation (2.1) to χ and the trivial character $\chi \equiv 1$, denoted below by $\mathbf{1}$, gives us that

$$0 = \langle \mathbf{1}, \chi \rangle = \sum_{\gamma \in \Gamma} \mathrm{e}^{\mathrm{i}\,\chi_{\arg}(\gamma)} = \sum_{\gamma \in \Gamma} (c(\gamma) + \mathrm{i}\,s(\gamma)).$$

Consequently,

$$\sum_{\gamma \in \Gamma} c(\gamma) = \sum_{\gamma \in \Gamma} s(\gamma) = 0. \tag{2.4}$$

Given two functions f and $g\colon\ \Gamma \to \mathbb{C}$, let $f * g\colon\ \Gamma \to \mathbb{C}$ be their *convolution*, given by

$$(f * g)(\alpha) = \sum_{\gamma \in \Gamma} f(\alpha - \gamma) g(\gamma).$$

In what follows, we let m be the cardinality of the image of χ:

$$m = |\{\chi(\gamma)\colon\ \gamma \in \Gamma\}|.$$

Since $\chi \not\equiv 1$, we have $m > 1$. We shall need the following fact.

Lemma 2.3. *We have*

(i)

$$\sum_{\gamma \in \Gamma} c^2(\gamma) = \begin{cases} n & \textit{if } m = 2, \\ n/2 & \textit{if } m > 2; \end{cases}$$

(ii)

$$\Big\langle A, \frac{1}{2}(1 + c) * \frac{1}{2}(1 + c) \Big\rangle = \frac{1}{4} n|A| + \frac{1}{4} \langle A, c * c \rangle \tag{2.5}$$

$$= \begin{cases} \dfrac{1}{4} n|A| + \dfrac{1}{4} n \langle A, c \rangle & \textit{if } m = 2, \\ \dfrac{1}{4} n|A| + \dfrac{1}{8} n \langle A, c \rangle & \textit{if } m > 2. \end{cases} \tag{2.6}$$

We postpone the proof of Lemma 2.3 to Section 2.3, and proceed to prove our main theorem. Let $-X$ and $Y \subset \Gamma$ be generated at random as follows: we include $\gamma \in \Gamma$ in $-X$ with probability $p(\gamma) = (1 + c(\gamma))/2$ and we include $\gamma \in \Gamma$ in Y with the same probability $p(\gamma)$, with all these events independent.

By (2.4) we have $\sum_{\gamma \in \Gamma} p(\gamma) = n/2$. Therefore, by a Chernoff type inequality (see, e.g., Alon and Spencer [5], Theorem A.1.4), we have

$$\mathbb{P}\Big(|X| = \Big(\frac{1}{2} + o(1) \Big) n \Big) = 1 - o(1) \tag{2.7}$$

and

$$\mathbb{P}\Big(|Y| = \Big(\frac{1}{2} + o(1)\Big)n\Big) = 1 - o(1). \tag{2.8}$$

In view of Lemma 2.3 (i), we have

$$\sum_{\gamma\in\Gamma} p(-\gamma)p(\gamma) = \sum_{\gamma\in\Gamma} p^2(\gamma) = \frac{1}{4}\sum_{\gamma\in\Gamma}(1+c(\gamma))^2 \overset{(2.4)}{=} \frac{1}{4}n + \frac{1}{4}\sum_{\gamma\in\Gamma} c(\gamma)^2 = \frac{3}{8}n$$

if $m > 2$ and $\sum_{\gamma\in\Gamma} p(-\gamma)p(\gamma) = n/2$ if $m = 2$. Consequently, if $m > 2$, we have

$$\mathbb{P}\Big(|X\cap Y| = \Big(\frac{3}{8} + o(1)\Big)n\Big) = 1 - o(1)$$

and hence, in view of (2.7) and (2.8), we have

$$\mathbb{P}\Big(|X\cup Y| = \Big(\frac{5}{8} + o(1)\Big)n\Big) = 1 - o(1). \tag{2.9}$$

Similarly, if $m = 2$, we have

$$\mathbb{P}\Big(|X\cap Y| = \Big(\frac{1}{2} + o(1)\Big)n\Big) = 1 - o(1) \tag{2.10}$$

and

$$\mathbb{P}\Big(|X\cup Y| = \Big(\frac{1}{2} + o(1)\Big)n\Big) = 1 - o(1). \tag{2.11}$$

On the other hand, in view of our assumption (2.3) and $A = -A$ we have

$$\varepsilon|A| \leqslant |\langle A, \chi\rangle| = |\langle A, c\rangle|.$$

Recall that $p(\gamma) = (1 + c(\gamma))/2$ is the probability that we include γ in $-X$ and in Y. By the linearity of the expectation and the independence, we have[2]

$$\begin{aligned} \mathbb{E}(\langle A, (-X) * Y\rangle) &= \mathbb{E}\Big(\sum_{a\in A}\sum_{\gamma\in\Gamma}(-X)(a-\gamma)Y(\gamma)\Big) \\ &= \sum_{a\in A}\sum_{\gamma\in\Gamma}\mathbb{E}((-X)(a-\gamma))\mathbb{E}(Y(\gamma)) \\ &= \sum_{a\in A}\sum_{\gamma\in\Gamma} p(a-\gamma)p(\gamma) \\ &= \Big\langle A, \frac{1}{2}(1+c) * \frac{1}{2}(1+c)\Big\rangle. \end{aligned} \tag{2.12}$$

[2] In (2.12), we write $(-X)$ for the characteristic function of the set $-X = \{-x\colon\ x \in X\}$.

By Lemma 2.3 (ii), we thus have

$$\left|\mathbb{E}(\langle A, (-X) * Y\rangle) - \frac{1}{4}n|A|\right| \geqslant \frac{1}{8}n|\langle A, c\rangle| \geqslant \frac{1}{8}\varepsilon n|A|. \tag{2.13}$$

On the other hand,

$$\langle A, (-X) * Y\rangle = \sum_{a\in A}\sum_{\gamma\in\Gamma}(-X)(a-\gamma)Y(\gamma) = \sum_{a\in A}\sum_{\gamma\in\Gamma}X(-a+\gamma)Y(\gamma) = e(X,Y),$$

with the edges in $X \cap Y$ counted twice. Since $0 \leqslant e(X,Y) \leqslant n|A|$, the random variable

$$\eta = \eta(X,Y) = \langle A, (-X) * Y\rangle - \frac{1}{4}n|A| = e(X,Y) - \frac{1}{4}n|A|$$

satisfies

$$-\frac{1}{4}n|A| \leqslant \eta \leqslant \frac{3}{4}n|A|. \tag{2.14}$$

Let q be the probability that $|\eta| \leqslant \varepsilon n|A|/16$. Then, by (2.13) and (2.14),

$$\frac{1}{8}\varepsilon n|A| \leqslant |\mathbb{E}(\eta)| \leqslant \mathbb{E}(|\eta|) \leqslant \frac{1}{16}\varepsilon n|A|q + \frac{3}{4}n|A|(1-q),$$

and, consequently,

$$\mathbb{P}\Big(|\eta| \leqslant \frac{1}{16}\varepsilon n|A|\Big) = q \leqslant \frac{1-\frac{1}{6}\varepsilon}{1-\frac{1}{12}\varepsilon} \leqslant 1 - \frac{1}{12}\varepsilon. \tag{2.15}$$

First consider the case in which $m > 2$. Putting together (2.7)–(2.9) and (2.15) we see that there are sets X and $Y \subset \Gamma$ for which we have

$$\begin{aligned} |X| &= \Big(\frac{1}{2} + o(1)\Big)n, & |Y| &= \Big(\frac{1}{2} + o(1)\Big)n,\\ |X \cap Y| &= \Big(\frac{3}{8} + o(1)\Big)n, & |X \cup Y| &= \Big(\frac{5}{8} + o(1)\Big)n, \end{aligned}$$

and

$$\left|e(X,Y) - \frac{1}{4}n|A|\right| \geqslant \frac{1}{16}\varepsilon n|A|. \tag{2.16}$$

Fix such sets X and Y. Suppose that none of the sets $X\setminus Y$, $Y\setminus X$, $X\cup Y$, and $X\cap Y$ violates DISC(δ). Then for sufficiently large n we have

$$\left|e(X\setminus Y) - \frac{1}{128}n|A|\right| < \frac{2}{128}\delta n|A|, \qquad \left|e(Y\setminus X) - \frac{1}{128}n|A|\right| < \frac{2}{128}\delta n|A|,$$

and

$$\left|e(X\cap Y)-\frac{9}{128}n|A|\right|<\frac{10}{128}\delta n|A|,\qquad \left|e(Y\cup X)-\frac{25}{128}n|A|\right|<\frac{26}{128}\delta n|A|.$$

Since

$$e(X,Y)=e(X\cup Y)-e(X\setminus Y)-e(Y\setminus X)+e(X\cup Y), \tag{2.17}$$

we infer that

$$\left|e(X,Y)-\frac{32}{128}n|A|\right|<\frac{40}{128}\delta n|A|,$$

which contradicts (2.16) if $\delta\leqslant\varepsilon/5$. The proof for the case $m>2$ is complete.

The case $m=2$ is similar. Putting together (2.7), (2.8), (2.10), (2.11), and (2.15) we see that there are sets X and $Y\subset\Gamma$ for which we have

$$|X|=\Big(\frac{1}{2}+o(1)\Big)n,\qquad |Y|=\Big(\frac{1}{2}+o(1)\Big)n,$$
$$|X\cap Y|=\Big(\frac{1}{2}+o(1)\Big)n,\qquad |X\cup Y|=\Big(\frac{1}{2}+o(1)\Big)n,$$

and, moreover, with X and Y satisfying (2.16). Fix such sets X and Y. Note that, then,

$$e(X\setminus Y)=o(n|A|)\quad\text{and}\quad e(Y\setminus X)=o(n|A|).$$

Suppose that neither $X\cup Y$ nor $X\cap Y$ violates DISC(δ). Then for sufficiently large n we have

$$\left|e(X\cap Y)-\frac{1}{8}n|A|\right|<\frac{2}{8}\delta n|A|\quad\text{and}\quad\left|e(Y\cup X)-\frac{1}{8}n|A|\right|<\frac{2}{8}\delta n|A|.$$

Using (2.17) again, we infer that

$$\left|e(X,Y)-\frac{1}{4}n|A|\right|<\frac{5}{8}\delta n|A|,$$

which contradicts (2.16) if $\delta\leqslant\varepsilon/10$, completing the proof in the case $m=2$.

2.3. Proof of Lemma 2.3. We start with the following fact (Fact 2.4 (i) below is simply Lemma 2.3 (i)).

Fact 2.4. *We have*

(i)

$$\sum_{\gamma\in\Gamma}c^2(\gamma)=\begin{cases} n & \textit{if } m=2,\\ \frac{1}{2}n & \textit{if } m>2;\end{cases} \tag{2.18}$$

(ii)

$$\sum_{\gamma\in\Gamma} s(\gamma)c(\gamma) = 0; \tag{2.19}$$

(iii) *for any* $a \in \Gamma$

$$(c * c)(a) = \begin{cases} nc(a) & \textit{if } m = 2, \\ \frac{1}{2}nc(a) & \textit{if } m > 2. \end{cases} \tag{2.20}$$

P r o o f. (i) We start by observing that

$$\sum_{0\leqslant l<m} \cos\frac{4\pi l}{m} = \begin{cases} 2 & \text{if } m = 2, \\ 0 & \text{if } m > 2. \end{cases} \tag{2.21}$$

Indeed, if $m > 2$, then the sum in (2.21) is

$$\operatorname{Re} \sum_{0\leqslant l<m} \mathrm{e}^{4\pi l\mathrm{i}/m} = \operatorname{Re} \frac{1-\mathrm{e}^{4\pi\mathrm{i}}}{1-\mathrm{e}^{4\pi\mathrm{i}/m}} = 0.$$

If $m = 2$, then the sum in (2.21) is easily seen to be 2. We now observe that

$$\sum_{\gamma\in\Gamma} c^2(\gamma) = \frac{n}{m} \sum_{0\leqslant l<m} \cos^2\frac{2\pi l}{m} = \frac{n}{2m} \sum_{0\leqslant l<m} \Big(1 + \cos\frac{4\pi l}{m}\Big).$$

It now suffices to recall (2.21) to deduce (2.18); assertion (i) is therefore proved.

Now we prove (ii). Note that

$$\sum_{0\leqslant l<m} \sin\frac{4\pi l}{m} = 0.$$

Therefore,

$$\sum_{\gamma\in\Gamma} s(\gamma)c(\gamma) = \frac{n}{m} \sum_{0\leqslant l<m} \sin\Big(\frac{2\pi l}{m}\Big) \cos\Big(\frac{2\pi l}{m}\Big) = \frac{n}{2m} \sum_{0\leqslant l<m} \sin\frac{4\pi l}{m} = 0,$$

as required.

For the proof of (iii), we start by noticing that

$$\begin{aligned} c(a-\gamma) &= \cos(\chi_{\arg}(a-\gamma)) = \cos(\chi_{\arg}(a) - \chi_{\arg}(\gamma)) \\ &= \cos\chi_{\arg}(a)\cos\chi_{\arg}(\gamma) + \sin\chi_{\arg}(a)\sin\chi_{\arg}(\gamma) = c(a)c(\gamma) + s(a)s(\gamma). \end{aligned}$$

Therefore,

$$\begin{aligned}(c*c)(a) &= \sum_{\gamma\in\Gamma} c(a-\gamma)c(\gamma) = \sum_{\gamma\in\Gamma}(c(a)c(\gamma)+s(a)s(\gamma))c(\gamma)\\ &= \sum_{\gamma\in\Gamma}(c(a)c^2(\gamma)+s(a)s(\gamma)c(\gamma)) = c(a)\sum_{\gamma\in\Gamma}c^2(\gamma)+s(a)\sum_{\gamma\in\Gamma}s(\gamma)c(\gamma).\end{aligned}$$

Equation (2.20) follows from (2.18) and (2.19) and (iii) is proved. □

Proof of Lemma 2.3. Lemma 2.3 (i) has already been proved. We now turn to (ii). The left-hand side of (2.5) is

$$\begin{aligned}(2.22)\qquad \frac{1}{4}\sum_{a\in A}\sum_{\gamma\in\Gamma}&((1+c)(a-\gamma))((1+c)(\gamma))\\ &= \frac{1}{4}\sum_{a\in A}\sum_{\gamma\in\Gamma}(1+c(a-\gamma))(1+c(\gamma))\\ &= \frac{1}{4}n|A| + \frac{1}{4}\sum_{a\in A}\sum_{\gamma\in\Gamma}(c(a-\gamma)+c(\gamma)) + \frac{1}{4}\sum_{a\in A}\sum_{\gamma\in\Gamma}c(a-\gamma)c(\gamma)\\ &= \frac{1}{4}n|A| + \frac{1}{4}\sum_{a\in A}\sum_{\gamma\in\Gamma}c(a-\gamma)c(\gamma) = \frac{1}{4}n|A| + \frac{1}{4}\langle A, c*c\rangle,\end{aligned}$$

which verifies (2.5). Clearly, Fact 2.4 (iii) and (2.22) imply (2.6). □

References

[1] *N. Alon*: Eigenvalues and expanders. Combinatorica *6* (1986), 83–96.
[2] *N. Alon, F. R. K. Chung*: Explicit construction of linear sized tolerant networks. Discrete Math. *72* (1988), 15–19.
[3] *N. Alon, A. Coja-Oghlan, H. Hàn, M. Kang, V. Rödl, M. Schacht*: Quasi-randomness and algorithmic regularity for graphs with general degree distributions. SIAM J. Comput. *39* (2010), 2336–2362.
[4] *N. Alon, V. D. Milman*: λ_1, isoperimetric inequalities for graphs, and superconcentrators. J. Combin. Theory Ser. B *38* (1985), 73–88.
[5] *N. Alon, J. H. Spencer*: The Probabilistic Method. Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons, Hoboken, 2008.
[6] *L. Babai*: Spectra of Cayley graphs. J. Comb. Theory, Ser. B *27* (1979), 180–189.
[7] *Y. Bilu, N. Linial*: Lifts, discrepancy and nearly optimal spectral gap. Combinatorica *26* (2006), 495–519.
[8] *F. Chung, R. Graham*: Sparse quasi-random graphs. Combinatorica *22* (2002), 217–244.
[9] *F. R. K. Chung, R. L. Graham, R. M. Wilson*: Quasi-random graphs. Combinatorica *9* (1989), 345–362.
[10] *D. Conlon, J. Fox, Y. Zhao*: Extremal results in sparse pseudorandom graphs. Adv. Math. *256* (2014), 206–290.
[11] *D. Conlon, Y. Zhao*: Quasirandom Cayley graphs. Available at ArXiv: 1603.03025 [math.CO].

[12] *W. E. Donath, A. J. Hoffman*: Lower bounds for the partitioning of graphs. IBM J. Res. Dev. *17* (1973), 420–425.
[13] *W. E. Donath, A. J. Hoffman*: Algorithms for partitioning of graphs and computer logic based on eigenvectors of connection matrices. IBM Techn. Disclosure Bull. *15* (1972), 938–944.
[14] *M. Fiedler*: A property of eigenvectors of nonnegative symmetric matrices and its application to graph theory. Czech. Math. J. *25* (1975), 619–633.
[15] *M. Fiedler*: Algebraic connectivity of graphs. Czech. Math. J. *23* (1973), 298–305.
[16] *P. Frankl, V. Rödl, R. M. Wilson*: The number of submatrices of a given type in a Hadamard matrix and related results. J. Comb. Theory, Ser. B *44* (1988), 317–328.
[17] *W. T. Gowers*: Personal communication.
[18] *K. M. Hall*: R-dimensional quadratic placement algorithm. Management Science Series A (Theory) *17* (1970), 219–229.
[19] *Y. Kohayakawa, V. Rödl*: Regular pairs in sparse random graphs I. Random Struct. Algorithms *22* (2003), 359–434.
[20] *Y. Kohayakawa, V. Rödl, P. Sissokho*: Embedding graphs with bounded degree in sparse pseudorandom graphs. Isr. J. Math. *139* (2004), 93–137.
[21] *M. Krivelevich, B. Sudakov*: Pseudo-random graphs. More Sets, Graphs and Numbers (E. Györi, ed.). Bolyai Society Mathematical Studies 15, Springer, Berlin, 2006, pp. 199–262.
[22] *L. Lovász*: Combinatorial Problems and Exercises. AMS Chelsea Publishing, Providence, 2007.
[23] *L. Lovász*: Spectra of graphs with transitive groups. Period. Math. Hung. *6* (1975), 191–195.
[24] *V. Rödl*: On universality of graphs with uniformly distributed edges. Discrete Math. *59* (1986), 125–134.
[25] *J.-P. Serre*: Linear Representations of Finite Groups. Graduate Texts in Mathematics 42, Springer, New York, 1977.
[26] *A. Sinclair, M. Jerrum*: Approximate counting, uniform generation and rapidly mixing Markov chains. Inf. Comput. *82* (1989), 93–133.
[27] *D. Spielman*: Spectral graph theory. Combinatorial Scientific Computing. Chapman & Hall/CRC Comput. Sci. Ser., CRC Press, Boca Raton, FL, 2012, pp. 495–524.
[28] *D. A. Spielman, S.-H Teng*: Spectral partitioning works: planar graphs and finite element meshes. Linear Algebra Appl. *421* (2007), 284–305.
[29] *R. M. Tanner*: Explicit concentrators from generalized N-gons. SIAM J. Algebraic Discrete Methods *5* (1984), 287–293.
[30] *A. Thomason*: Pseudo-random graphs. Random graphs '85. Ann. Discrete Math. 33, North-Holland, Amsterdam, 1987, pp. 307–331.
[31] *A. Thomason*: Random graphs, strongly regular graphs and pseudo-random graphs. Surveys in Combinatorics 1987. Cambridge Univ. Press, Cambridge, 1987, pp. 173–195.

Authors' addresses: Yoshiharu Kohayakawa, Instituto de Matemática e Estatística, Universidade de São Paulo, R. do Matão, 1010 – Vila Universitaria, 05508-090 São Paulo, Brazil, e-mail: `yoshi@ime.usp.br`; Vojtěch Rödl, Department of Mathematics and Computer Science, Emory University, 400 Dowman Dr., 30307 Atlanta, Georgia, USA, e-mail: `rodl@mathcs.emory.edu`; Mathias Schacht, Fachbereich Mathematik, Universität Hamburg, Bundesstrasse 55, 20146 Hamburg, Germany, e-mail: `schacht@math.uni-hamburg.de`.