

DISCREPANCY AND EIGENVALUES OF CAYLEY GRAPHS

Y. KOHAYAKAWA, V. RÖDL, AND M. SCHACHT

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 Cayley graphs, even if they are *sparse*. This positively answers a question of Chung and Graham [“Sparse quasi-random graphs”, *Combinatorica* **22** (2002), no. 2, 217–244] for the particular case of Cayley graphs, while in general the answer is negative.

1. INTRODUCTION

Our aim in this paper is to investigate certain delicate aspects of a well known connection between the eigenvalue gap property and quasirandomness of graphs.

Thanks to the work of Tanner [20], Alon and Milman [3] and Alon [1] (see also Alon and Spencer [4, Chapter 9]) it is well known that a *gap* between the largest and the second largest eigenvalue of a graph G is related to the quasirandomness of G . Here, the concept of “quasirandomness” will be that of Chung, Graham, and Wilson [9].

Let an n -vertex graph G be given. Recall that the eigenvalues of G are simply the eigenvalues of the n by n , 0–1 adjacency matrix of G , with 1 indicating edges. As usual, let $\lambda_k = \lambda_k(G)$ be the k th 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). A fundamental result relating the λ_i to quasirandomness states that *there is a large gap between λ_1 and λ_k ($k \geq 2$) 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 [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 [21] (see also [22]), and also Alon [1], Alon and Chung [2], Frankl, Rödl and Wilson [10], and Rödl [18]. One of the so-called “quasirandom properties” that is presented in [9] is the eigenvalue gap between λ_1 and λ_k ($k \geq 2$).

Date: April 17, 2003.

1991 Mathematics Subject Classification. Primary: 05C50. Secondary: 05C80.

Key words and phrases. Eigenvalues, discrepancy, quasirandomness, Cayley graphs.

The first author was on leave from Instituto de Matemática e Estatística, Universidade de São Paulo, Rua do Matão 1010, 05508–090 São Paulo, Brazil, and was partially supported by FAPESP (Proj. 96/04505–2), by MCT/CNPq through ProNEx Proj. 107/97, and by CNPq (Proc. 300334/93–1). The second author was partially supported by NSF Grant 0071261. The collaboration between the authors is supported by an NSF/CNPq joint grant.

More recently, Chung and Graham [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* generalise 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 [13, 14]). In particular, having succeeded in proving that eigenvalue gap does imply uniform distribution of edges in the sparse case, Chung and Graham ask whether the converse also holds (see [8, p. 230]). An affirmative answer to this question would fully generalise the relationship between these two concepts to the sparse case.

However, Krivelevich and Sudakov [15] discovered that, unfortunately, the answer to the question posed by Chung and Graham is negative, by constructing a suitable family of counterexamples (see Section 3 for a different construction). Here, our aim is to show that *the answer is positive if one considers Cayley graphs of finite abelian groups, regardless of the density of the graph*. We leave the non-abelian case as an open question. It is worth noting that several explicit constructions of quasirandom graphs are indeed Cayley graphs (see, e.g., [22] and [15, Section 3]).

Before we proceed to state our result precisely, we mention that our proof method also sheds some light on the investigation of quasirandom subsets of $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, in the spirit of Chung and Graham [7], in the *sparse case* (and for general abelian groups, as suggested in [7, p. 85]). We shall come back to this topic in the near future.

1.1. Statement of the main result. 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

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

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

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

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

The concept of DISC₂ is very much related to DISC, as we shall see next.

Definition 2 (DISC₂(δ')). *Let $0 < \delta' \leq 1$ be given. We say that an n -vertex graph G ($n \geq 2$) satisfies property DISC₂(δ') if the following assertion holds: for all disjoint U and $W \subset V(G)$ with $|U|, |W| \geq \delta n$, we have*

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

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

Fact 3. *For any $0 < \delta' \leq 1$, there is $0 < \delta = \delta(\delta') \leq 1$ such that any graph that satisfies $\text{DISC}(\delta)$ must also satisfy $\text{DISC}_2(\delta')$.*

Given a graph G , let $\mathbf{A} = (a_{\gamma\gamma'})_{\gamma, \gamma' \in \Gamma}$ 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

$$\lambda_1 \geq |\lambda_2| \geq \cdots \geq |\lambda_n| \quad (1)$$

(the fact that $\lambda_1 \geq 0$ follows, for instance, from the fact that \mathbf{A} has no negative entries and, as it turns out, $\lambda_1 = \max\{\langle \mathbf{A}\mathbf{v}, \mathbf{v} \rangle : \|\mathbf{v}\| = 1\}$).

Definition 4 ($\text{EIG}(\varepsilon)$). *Let $0 < \varepsilon \leq 1$ be given. We say that an n -vertex graph G satisfies property $\text{EIG}(\varepsilon)$ if the following holds. Let $\bar{d} = \bar{d}(G) = 2e(G)/n$ be the average degree of G , and let $\lambda_1, \dots, \lambda_n$ be the eigenvalues of G , with the notation adjusted in such a way that (1) holds. Then*

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

Finally, we define Cayley graphs.

Definition 5 (Cayley graph $G = G(\Gamma, A)$). *Let Γ be an abelian group, and suppose $A \subset \Gamma \setminus \{0\}$ 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 $\gamma' - \gamma \in A$.*

In this paper, we only consider finite graphs and finite abelian groups.

The main aim of this paper is to answer a question of Chung and Graham from [8] in the positive for an interesting class of graphs.

Theorem 6. *For any $\varepsilon > 0$, there are constants $\delta > 0$ and $n_0 \geq 1$ for which the following holds. If $G = G(\Gamma, A)$ is a Cayley graph for some abelian group Γ and symmetric set $A = -A \subseteq \Gamma \setminus \{0\}$, the number of vertices $n = |\Gamma|$ of G satisfies $n \geq n_0$, and G satisfies property $\text{DISC}(\delta)$, then G satisfies $\text{EIG}(\varepsilon)$.*

We give the proof of this theorem in Section 2.

1.2. Remarks on the main result. Before we proceed, let us discuss some points concerning Theorem 6; more technical details are given in Section 3.

We first observe that Theorem 6, together with the results of Chung and Graham [8], imply that properties DISC and EIG are equivalent for Cayley graphs. We say that DISC implies EIG for Cayley graphs if for every $\varepsilon > 0$ there is a $\delta = \delta(\varepsilon) > 0$ such that, for any sequence of n -vertex d_n -regular Cayley graphs G_n with d_n tending to infinity as $n \rightarrow \infty$, the following holds: *if all but finitely many graphs G_n satisfy $\text{DISC}(\delta)$, then all but finitely many G_n satisfy $\text{EIG}(\varepsilon)$.* Theorem 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.

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 [15]. For every $\varepsilon > 0$ and every $\delta > 0$, they constructed an infinite sequence of graphs that satisfy $\text{DISC}(\delta)$ but fail to satisfy (i) in the definition of $\text{EIG}(\varepsilon)$ (see Definition 4). A different construction to be presented in Section 3 (see Fact 25) gives additional control over a constant number of the largest eigenvalues.

At last, we wish to compare our main result, Theorem 6, with the earlier work of Chung and Graham [8]. Let us consider the following property.

Definition 7 (CIRCUIT $_t(\xi)$). *Let $0 < \xi \leq 1$ and an integer $t \geq 3$ be given. We say that an n -vertex graph G with average degree $\bar{d}(G)$ satisfies property CIRCUIT $_t(\xi)$ if the number of t -circuits C_t^* in G , i.e., closed walks of length t , satisfies*

$$\#\{C_t^* \hookrightarrow G\} \sim_\xi \bar{d}(G)^t.$$

In [8], it is proved that, under some additional conditions, DISC implies EIG (see Theorem 6 in [8]). These additional conditions, combined with DISC, also imply CIRCUIT $_{2\ell}$ for some $\ell > 1$. The following fact shows that Theorem 6 in [8] does not imply our main result, as it says that there are sequences of Cayley graphs that satisfy both DISC and EIG, but fail to meet CIRCUIT $_{2\ell}$ for every $\ell > 1$.

Fact 8. *There is an infinite sequence G_N of N -vertex Cayley graphs ($N \rightarrow \infty$) for which the following holds:*

- (i) *for every $\delta > 0$ all but finitely many graphs G_N satisfy DISC(δ),*
- (ii) *for every $\varepsilon > 0$ all but finitely many graphs G_N satisfy EIG(ε),*

and

- (iii) *for every integer $\ell > 1$ and every $\xi > 0$ only finitely many graphs G_N satisfy CIRCUIT $_{2\ell}(\xi)$.*

We outline the proof of Fact 8 in the last section, Section 3.

2. PROOF OF THE MAIN RESULT

2.1. Eigenvalues of Cayley graphs of abelian groups. The eigenvalues of Cayley graphs of abelian groups may be determined easily, as shows Theorem 9 below. Theorem 9 follows from a more general result due to Lovász [16] (see also [17, Exercise 11.8] and [5]).

Before we state Theorem 9, we recall some basic facts about group characters (for more details see, e.g., Serre [19]). Let Γ be a finite abelian group. In this case, an *irreducible character* χ of Γ may be viewed as a group homomorphism $\chi: \Gamma \rightarrow S^1$, 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, χ_1, \dots, χ_n , and these characters satisfy the following *orthogonality property*:

$$\sum_{\gamma \in \Gamma} \chi_i(\gamma) \chi_j(\gamma) = 0 \tag{2}$$

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.

Theorem 9. *Let $G = G(\Gamma, A)$ for some finite abelian group Γ and symmetric set $A = -A \subseteq \Gamma \setminus \{0\}$. For any character $\chi: \Gamma \rightarrow S^1$ of Γ , put*

$$\lambda^{(\chi)} = \sum_{a \in A} \chi(a). \tag{3}$$

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

Proof. Let $\chi: \Gamma \rightarrow S^1$ be an irreducible character of Γ . Let $\lambda^{(\chi)}$ be as defined in (3). Consider the vector $\mathbf{v}^{(\chi)} = (\chi(\gamma))_{\gamma \in \Gamma}^T$, 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 $(\mathbf{A}\mathbf{v}^{(\chi)})_\gamma$ of the vector $\mathbf{A}\mathbf{v}^{(\chi)}$ is

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

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

Let $\chi_j: \Gamma \rightarrow S^1$ ($1 \leq j \leq n$) be the irreducible characters of Γ . By (2), $\langle \mathbf{v}_j, \mathbf{v}_{j'} \rangle = 0$ if $j \neq j'$. Therefore, the \mathbf{v}_j ($1 \leq j \leq n$) form an orthogonal basis of eigenvectors of the matrix \mathbf{A} and, hence, $\lambda^{(\chi_j)}$ ($j = 1, \dots, n$) are indeed the eigenvalues of G . \square

2.2. Proof of the main theorem. We shall now present the proof of Theorem 6. Let a constant $\varepsilon > 0$ be given. The aim is to find some $\delta > 0$ for which property $\text{DISC}(\delta)$ implies $\text{EIG}(\varepsilon)$ for any Cayley graph $G = G(\Gamma, A)$. Let us once and for all fix an abelian group Γ and a symmetric set $A \subseteq \Gamma \setminus \{0\}$. In what follows, we write G for the Cayley graph $G(\Gamma, A)$. We shall always write n for the number of vertices in G , i.e., $n = |\Gamma| = |V(G)|$. We also let $|A| = \alpha n$.

Clearly, our graph G is $|A|$ -regular. Therefore, the density of the graph G is

$$e(G) \Big/ \binom{n}{2} = \frac{|A|}{n-1}. \quad (4)$$

Moreover, as is well known, condition (i) of Definition 4 is automatically fulfilled. We should therefore consider condition (ii) of that definition. Because of Theorem 9, our task is to estimate the $\lambda^{(\chi)}$ given in (3). More precisely, we have to show that if $\chi \neq 1$, then

$$|\lambda^{(\chi)}| = \left| \sum_{a \in A} \chi(a) \right| \leq \varepsilon |A|. \quad (5)$$

Thus, let $\chi: \Gamma \rightarrow S^1$ be a fixed, non-constant irreducible character of Γ . We shall estimate $\lambda^{(\chi)}$ in two different ways, according to the cardinality of $\text{im } \chi = \{\chi(\gamma): \gamma \in \Gamma\}$. In what follows, we always write m for $|\text{im } \chi|$. We also use the bijection $e^{\theta i}$, mapping every θ in $\mathbb{R}/2\pi\mathbb{R}$ to $e^{\theta i}$ in S^1 . We define

$$\chi_{\text{ARG}}: \Gamma \rightarrow \mathbb{R}/2\pi\mathbb{R}$$

to be the homomorphism such that for every $\gamma \in \Gamma$

$$\chi_{\text{ARG}}(\gamma) = \arg(\chi(\gamma)) \quad \text{and} \quad \chi(\gamma) = e^{\chi_{\text{ARG}}(\gamma) i}.$$

Furthermore, we let $\Omega: \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{R}/2\pi\mathbb{R}$ be the homomorphism

$$\Omega(s) = \frac{2\pi}{m} s \quad \text{for} \quad s \in \mathbb{Z}/m\mathbb{Z}.$$

We also have a homomorphism $\varrho: \Gamma \rightarrow \mathbb{Z}/m\mathbb{Z}$ for which $\chi_{\text{ARG}} = \Omega\varrho$ holds, so that $\chi_{\text{ARG}}(\gamma) = 2\pi\varrho(\gamma)/m$ for every γ in Γ . Summarising the above, from now on we will work with the following setup.

Setup 10. Let $G = G(\Gamma, A)$ be the Cayley graph given by the abelian group Γ and the symmetric set $A = -A \subseteq \Gamma \setminus \{0\}$. The graph G is of order $n = |\Gamma|$, every vertex has degree $|A| = \alpha n$, and the density of the graph is $|A|/(n-1)$.

Fix an irreducible character $\chi \neq 1$, set $m = |\text{im } \chi|$, and let χ_{ARG} , Ω , and ϱ (depending on χ) be group homomorphisms such that the following diagram commutes:

$$\begin{array}{ccc} \Gamma & \xrightarrow{\chi} & S^1 \subset \mathbb{C} \\ \varrho \downarrow & \searrow \chi_{\text{ARG}} & \uparrow e^{\theta i} \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\Omega} & \mathbb{R}/2\pi\mathbb{R} \end{array}$$

As mentioned above we consider two cases for the proof of Theorem 6. In the first case m will be small. The following lemma will handle that case.

Lemma 11. *For every $\delta' > 0$ there is an $n_0 \geq 0$ such that if $|\Gamma| = n \geq n_0$, $m \leq 1/\delta'$, and $G = G(\Gamma, A)$ satisfies $\text{DISC}_2(\delta')$, then*

$$|\lambda^{(\chi)}| \leq 2\delta'|A|.$$

For the other case (m large), we shall need three auxiliary lemmas to verify (5). The proofs of these three lemmas, as well as the proof of Lemma 11, are given in Sections 2.3.2–2.3.4. We start with two definitions.

Definition 12 (\mathbb{Z} -INT-DISC($\varrho; \eta, \sigma$)). *For positive reals η and σ , we say that A satisfies \mathbb{Z} -INT-DISC($\varrho; \eta, \sigma$) if for all integers $0 \leq D_1 < D_2 \leq \lfloor m/2 \rfloor + 1$ such that $D_2 - D_1 \geq \eta m$ we have*

$$|A \cap \varrho^{-1}([D_1, D_2])| \sim_{\sigma} \frac{D_2 - D_1}{m} |A|. \quad (6)$$

Roughly speaking, a set A satisfies \mathbb{Z} -INT-DISC if its image under ϱ intersects “large” intervals uniformly. Next we define a very similar property for A with respect to χ_{ARG} and intervals in $\mathbb{R}/2\pi\mathbb{R}$.

Definition 13 (S^1 -ARC-DISC($\chi_{\text{ARG}}; \eta, \sigma$)). *For positive reals η and σ , we say that A satisfies S^1 -ARC-DISC($\chi_{\text{ARG}}; \eta, \sigma$) if for all reals $0 \leq \theta_1 < \theta_2 \leq \pi$ such that $\theta_2 - \theta_1 \geq 2\pi\eta$ we have*

$$|A \cap \chi_{\text{ARG}}^{-1}([\theta_1, \theta_2])| \sim_{\sigma} \frac{\theta_2 - \theta_1}{2\pi} |A|. \quad (7)$$

Basically, the next three lemmas give the following implications for large m :

$$\text{DISC} \implies \mathbb{Z}\text{-INT-DISC} \implies S^1\text{-ARC-DISC} \implies \text{EIG}.$$

These lemmas are stated under the assumptions of Setup 10; in particular, we recall that ϱ and χ_{ARG} depend on the fixed, non-constant character χ .

Lemma 14. *For all positive reals η and σ , there are $\delta = \delta(\eta, \sigma) > 0$ and $n_0 \geq 0$ such that if $|\Gamma| = n \geq n_0$, $m > 1/\delta$, and $G = G(\Gamma, A)$ satisfies $\text{DISC}(\delta)$, then A satisfies \mathbb{Z} -INT-DISC($\varrho; \eta, \sigma$).*

Lemma 15. *For all positive reals $\eta \leq 1$ and $\sigma \leq 1$ such that $m\eta\sigma \geq 3$, the following holds. If A satisfies property \mathbb{Z} -INT-DISC($\varrho; \eta/2, \sigma/3$), then A satisfies property S^1 -ARC-DISC($\chi_{\text{ARG}}; \eta, \sigma$).*

Lemma 16. *For every real $\varepsilon > 0$, there are reals $\eta = \eta(\varepsilon) > 0$ and $\sigma = \sigma(\varepsilon) > 0$ for which the following holds. If A satisfies S^1 -ARC-DISC($\chi_{\text{ARG}}; \eta, \sigma$), then*

$$|\lambda^{(\chi)}| = \left| \sum_{a \in A} \chi(a) \right| \leq \varepsilon |A|. \quad (8)$$

We now assume Lemma 11, 14, 15, and 16 and give the proof of Theorem 6. (We present the proofs of those auxiliary results in Section 2.3.)

Proof of Theorem 6. Let $\varepsilon > 0$ be given. We apply Lemma 16, which yields the positive constants $\eta = \eta(\varepsilon)$ and $\sigma = \sigma(\varepsilon)$. Then Lemma 14 gives $\delta_{14} = \delta_{14}(\eta/2, \sigma/3)$. We set

$$\delta' = \min \left\{ \delta_{14}, \frac{\eta\sigma}{3}, \frac{\varepsilon}{2} \right\}.$$

We now choose δ promised by Theorem 6 to be

$$\delta = \min\{\delta_3(\delta'), \delta_{14}\},$$

where $\delta_3(\delta')$ is given by Fact 3. Finally, let n_0 be as large as required by Lemmas 11 and 14. We claim that this choice for δ and n_0 will do, and proceed to check this claim.

Suppose $\text{DISC}(\delta)$ holds for some Cayley graph $G = G(\Gamma, A)$ with $|\Gamma| \geq n_0$ and let $\chi \neq 1$ be given (the notation here follows the notation set out in Setup 10). We consider two cases.

Suppose first that $m \leq 1/\delta'$. Fact 3 tells us that $\text{DISC}_2(\delta')$ holds for G . Since $m \leq 1/\delta'$, Lemma 11 tells us that $|\lambda^{(\chi)}| \leq \varepsilon|A|$ by the choice of $\delta' \leq \varepsilon/2$. For the other case, namely, $m > 1/\delta'$, we first observe that $\text{DISC}(\delta_{14})$ holds since $\delta \leq \delta_{14}$ and that $m > 1/\delta' \geq 1/\delta_{14}$. Moreover, the choice of $\delta' \leq \eta\sigma/3$ yields $m\eta\sigma > \eta\sigma/\delta' \geq 3$, making Lemma 15 applicable. Our claim is now a consequence of the following implications coming from Lemmas 14–16:

$$\begin{aligned} \text{DISC}(\delta_{14}) &\implies \mathbb{Z}\text{-INT-DISC} \left(\varrho; \frac{\eta}{2}, \frac{\sigma}{3} \right) \\ &\implies S^1\text{-ARC-DISC}(\chi_{\text{ARG}}; \eta, \sigma) \implies |\lambda^{(\chi)}| \leq \varepsilon|A|, \end{aligned}$$

and hence Theorem 6 is proved. \square

2.3. Auxiliary lemmas.

2.3.1. *An auxiliary weighted graph.* The homomorphism ϱ (see Setup 10 for details), defines a weighted graph \tilde{G} on $\mathbb{Z}/m\mathbb{Z}$ in a natural way. The symmetry of this graph will be useful in the proofs of Lemmas 11 and 14.

Definition 17. We let (under the assumptions of Setup 10) $\tilde{G} = \tilde{G}(\varrho) = (\mathbb{Z}/m\mathbb{Z}, w)$ be the weighted graph on $\mathbb{Z}/m\mathbb{Z}$, with weights assigned to the edges and vertices, with the weight function

$$w: \binom{\mathbb{Z}/m\mathbb{Z}}{2} \cup \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}$$

given by

$$w(\{r, s\}) = e(G[\varrho^{-1}(r), \varrho^{-1}(s)]), \quad (9)$$

for all distinct r and $s \in \mathbb{Z}/m\mathbb{Z}$, and

$$w(r) = e(G[\varrho^{-1}(r)]), \quad (10)$$

for all $r \in \mathbb{Z}/m\mathbb{Z}$.

For convenience, if X and $Y \subset \mathbb{Z}/m\mathbb{Z}$ are two disjoint sets, we put

$$w(X, Y) = \sum \left\{ w(\{x, y\}) : (x, y) \in X \times Y \right\} = e(\varrho^{-1}(X), \varrho^{-1}(Y)). \quad (11)$$

In Lemma 18 below, we make the definition of \tilde{G} more concrete, computing the values in (9) and (10). Let us observe that Lemma 18 shows that the weighted graph \tilde{G} has a “cyclic” structure, that is, the cyclic permutation $\tau: s \mapsto s + 1$ is an “automorphism” of \tilde{G} .

Lemma 18. *For all distinct r and $s \in \mathbb{Z}/m\mathbb{Z}$, we have*

$$w(\{r, s\}) = e(G[\varrho^{-1}(r), \varrho^{-1}(s)]) = \frac{n}{m} |A \cap \varrho^{-1}(r - s)|, \quad (12)$$

and for all $r \in \mathbb{Z}/m\mathbb{Z}$ we have

$$w(r) = e(G[\varrho^{-1}(r)]) = \frac{n}{2m} |A \cap \varrho^{-1}(0)|. \quad (13)$$

Proof. Let r and s be arbitrary, not necessarily distinct members of $\mathbb{Z}/m\mathbb{Z}$. For every γ in $\varrho^{-1}(s)$, consider the neighbourhood $N_r(\gamma)$ of γ in G restricted to $\varrho^{-1}(r)$. It is easy to see that

$$N_r(\gamma) = \{A \cap \varrho^{-1}(r - s)\} + \gamma$$

for every $\gamma \in \varrho^{-1}(s)$. Since $|\varrho^{-1}(s)| = n/m$, this implies, for $s \neq r$, that

$$e(G[\varrho^{-1}(r), \varrho^{-1}(s)]) = |\varrho^{-1}(s)| \cdot |A \cap \varrho^{-1}(r - s)| = \frac{n}{m} |A \cap \varrho^{-1}(r - s)|,$$

and therefore (12) holds. Similarly, (13) follows from the case $r = s$. \square

2.3.2. The small m case. The proof given in this section is fairly simple. It is based on (12) combined with an application of DISC_2 .

Proof of Lemma 11. Let $\delta' > 0$ be given. We choose n_0 large enough such that $n \sim_{\delta'/2} (n - 1)$ for every $n \geq n_0$.

Now assume $G = G(\Gamma, A)$ with $|\Gamma| \geq n_0$ satisfying $\text{DISC}_2(\delta')$ is given. Using that $1/m \geq \delta'$, we deduce from $\text{DISC}_2(\delta')$ and (12) that for all $r \in \mathbb{Z}/m\mathbb{Z}$

$$|A \cap \varrho^{-1}(r)| = \frac{m}{n} e(G[\varrho^{-1}(r), \varrho^{-1}(0)]) \sim_{\delta'} \frac{n|A|}{(n - 1)m},$$

and hence, by the choice of n_0 ,

$$|A \cap \varrho^{-1}(r)| \leq (1 + 2\delta') \frac{|A|}{m}. \quad (14)$$

We then set $\omega = e^{2\pi i/m}$ and use (14) to infer

$$|\lambda^{(x)}| = \left| \sum_{a \in A} \chi(a) \right| = \left| \sum_{r=0}^{m-1} (|A \cap \varrho^{-1}(r)| \cdot \omega^r) \right| \leq \frac{|A|}{m} \left(\left| \sum_{r=0}^{m-1} \omega^r \right| + 2\delta' m \right),$$

which yields $|\lambda^{(x)}| \leq 2\delta'|A|$, because

$$\sum_{r=0}^{m-1} \omega^r = 0.$$

\square

2.3.3. *DISC implies \mathbb{Z} -INT-DISC for m large.* The aim of this section is to verify \mathbb{Z} -INT-DISC($\varrho; \eta, \sigma$) for a graph that satisfies DISC(δ) for sufficiently small δ . We therefore want to link properties of the edge-distribution of G with the quantities

$$|A \cap \varrho^{-1}(I)| = \sum_{f \in I} |A \cap \varrho^{-1}(f)|,$$

where I is a sufficiently large interval in $\mathbb{Z}/m\mathbb{Z}$. A first step towards this goal is the following lemma.

Lemma 19. *Let ℓ, s , and t be integers, and suppose that*

$$0 \leq s < s + \ell \leq t < t + \ell \leq m/2.$$

Then for $d_1 = t - s - \ell$ and $d_2 = t - s + \ell$

$$\begin{aligned} \frac{m}{n} w([s, s + \ell), [t, t + \ell)) &= \sum \{ |A \cap \varrho^{-1}(f)| (f - d_1) : d_1 < f < t - s \} \\ &+ \sum \{ |A \cap \varrho^{-1}(f)| (d_2 - f) : t - s \leq f < d_2 \}. \end{aligned} \quad (15)$$

We later may control the left-hand side of (15) by DISC (or, more precisely, by DISC₂). On the other hand, we may interpret the right-hand side as a “weighted version” of $|A \cap \varrho^{-1}([d_1, d_2])|$ where the “multiplicity” for each f in $[d_1, d_2]$ is given by a piecewise linear function depending on d_1 and d_2 (see Figure 1).

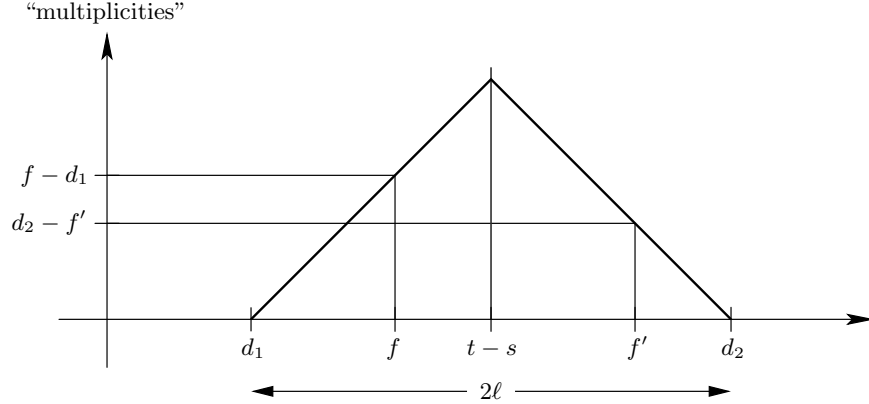


FIGURE 1. Distribution of “multiplicities”

Proof of Lemma 19. We have

$$w([s, s + \ell), [t, t + \ell)) = \sum \{ w(e) : e \in E_{\tilde{G}}([s, s + \ell), [t, t + \ell)) \}. \quad (16)$$

The integers f that arise as differences $t' - s'$ with $t' \in [t, t + \ell)$ and $s' \in [s, s + \ell)$ are in the interval

$$d_1 = t - s - \ell < f < t - s + \ell = d_2. \quad (17)$$

Intuitively speaking, these are the “lengths” of the edges in $E_{\tilde{G}}([s, s + \ell), [t, t + \ell))$. A moment’s thought (see Figure 2) shows that assertions (I) and (II) given below hold.

- (I) If f is in the interval $d_1 = t - s - \ell < f < t - s$, then $f - d_1$ edges in $E_{\tilde{G}}([s, s + \ell), [t, t + \ell))$ have length f .

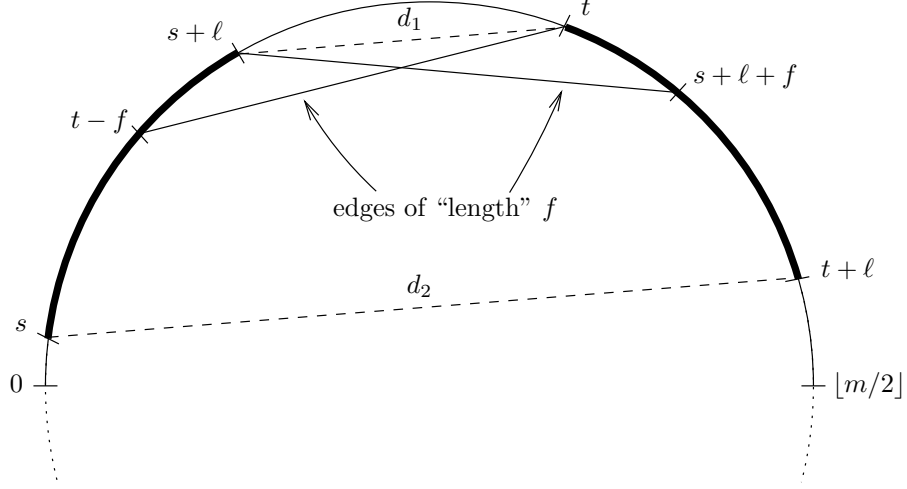


FIGURE 2. Edges in \tilde{G} of “length” $d_1 < f < t - s$ appear between $[t - f, s + \ell)$ and $[t, s + \ell + f)$

(II) If f is in the interval $t - s \leq f < d_2 = t - s + \ell$, then $d_2 - f$ edges in $E_{\tilde{G}}([s, s + \ell), [t, t + \ell))$ have length f .

In other words, the lengths f in the interval $(d_1, t - s)$ occur $f - d_1$ times and the lengths f in the interval $[t - s, d_2)$ occur $d_2 - f$ times in the sum in (16). Each occurrence of f contributes to (16) a weight of

$$\frac{n}{m} |A \cap \varrho^{-1}(f)| \quad (18)$$

(see (12)). Therefore, putting (I), (II), and (18) together, identity (15) follows. \square

The next step towards verifying \mathbb{Z} -INT-DISC is to dispose of the “multiplicities” of type $d_1 - f$ and $d_2 - f$ in (15). For this we use Lemma 19, and compare $w([s - d, s + \ell), [t - d, t + \ell))$ with $w([s, s + \ell), [t, t + \ell))$. By (15) these two terms (appropriately scaled) correspond to two “weighted versions” of $|A \cap \varrho^{-1}([d'_1, d'_2])|$ and $|A \cap \varrho^{-1}([d_1, d_2])|$, for some appropriate d'_1, d'_2, d_1 , and d_2 depending on d, s, t , and ℓ . As it turns out, the difference between these two “weighted versions” yields a “weighted version” of $|A \cap \varrho^{-1}([d'_1, d'_2])|$ with constant multiplicity d for the main part of the interval $[d'_1, d'_2]$, i.e., in between d_1 and d_2 (see Figure 3). This way we derive a useful estimate for $|A \cap \varrho^{-1}([d_1, d_2])|$.

Lemma 20. *Let d, ℓ, s , and t be positive integers, δ' a real number such that $0 < \delta' \leq 1$, and suppose that*

- (i) $0 \leq s - d < s + \ell \leq t - d < t + \ell \leq m/2$,
- (ii) $\text{DISC}_2(\delta')$ holds for $G = G(\Gamma, A)$,
- (iii) $\ell - d \geq \delta' m$, and
- (iv) $n \sim_{\delta'/2} (n - 1)$.

Then, for $d_1 = t - s - \ell$ and $d_2 = t - s + \ell$, we have

$$\left| |A \cap \varrho^{-1}([d_1, d_2])| - 2\ell \frac{|A|}{m} \right| \leq \frac{|A|}{m} \left(d + \frac{2\delta'}{d} ((\ell + d)^2 + \ell^2) \right). \quad (19)$$

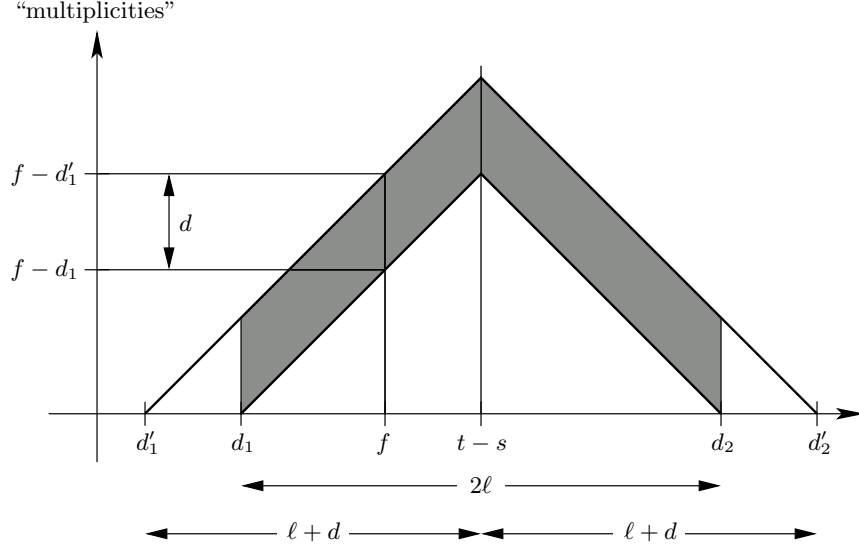


FIGURE 3. Difference between “multiplicities”

Proof. Let $d'_1 = (t-d) - s - \ell = d_1 - d$ and $d'_2 = t + \ell - (s-d) = d_2 + d$. Applying Lemma 19 to $w([s-d, s+\ell], [t-d, t+\ell])$, we get that

$$\begin{aligned} & \frac{m}{n} w([s-d, s+\ell], [t-d, t+\ell]) \\ &= \sum \{|A \cap \varrho^{-1}(f)|(f-d'_1) : d'_1 < f < t-s\} \\ & \quad + \sum \{|A \cap \varrho^{-1}(f)|(d'_2-f) : t-s \leq f < d'_2\}. \end{aligned}$$

We then apply Lemma 19 again, now to $w([s, s+\ell], [t, t+\ell])$, and observe that

$$\begin{aligned} & \frac{m}{n} \left(w([s-d, s+\ell], [t-d, t+\ell]) - w([s, s+\ell], [t, t+\ell]) \right) \\ &= d \sum \{|A \cap \varrho^{-1}(f)| : d_1 \leq f < d_2\} \\ & \quad + \sum \{|A \cap \varrho^{-1}(f)|(f-d'_1) : d'_1 < f < d_1\} \\ & \quad + \sum \{|A \cap \varrho^{-1}(f)|(d'_2-f) : d_2 \leq f < d'_2\}. \end{aligned} \tag{20}$$

The “main term” on the right-hand side of (20) will turn out to be

$$d \sum \{|A \cap \varrho^{-1}(f)| : d_1 \leq f < d_2\} = d |A \cap \varrho^{-1}([d_1, d_2])|. \tag{21}$$

We now use $\text{DISC}_2(\delta')$ to estimate the left-hand side of (20). By the definition of w (see Definition 17), we have

$$w([s, s+\ell], [t, t+\ell]) = e(G[\varrho^{-1}([s, s+\ell]), \varrho^{-1}([t, t+\ell])]).$$

Therefore, by $\text{DISC}_2(\delta')$, using that

$$|\varrho^{-1}([s, s+\ell])| = |\varrho^{-1}([t, t+\ell])| = \frac{n}{m} \ell \geq \delta' n,$$

we have that

$$\begin{aligned} w([s, s + \ell], [t, t + \ell]) &= e(G[\varrho^{-1}([s, s + \ell]), \varrho^{-1}([t, t + \ell])]) \\ &\sim_{\delta'} \frac{|A|}{n-1} \left| \varrho^{-1}([s, s + \ell]) \right| \left| \varrho^{-1}([t, t + \ell]) \right| = \frac{|A|}{n-1} \left(\frac{n}{m} \ell \right)^2. \end{aligned} \quad (22)$$

Similarly, we have that

$$w([s-d, s + \ell], [t-d, t + \ell]) \sim_{\delta'} \frac{|A|}{n-1} \left(\frac{n}{m} (\ell + d) \right)^2. \quad (23)$$

From (22), (23), and (iv) we deduce that the left-hand side of (20) satisfies

$$\begin{aligned} &\frac{m}{n} \left(w([s-d, s + \ell], [t-d, t + \ell]) - w([s, s + \ell], [t, t + \ell]) \right) \\ &= (1 + O_1(2\delta')) \frac{|A|}{m} (\ell + d)^2 - (1 + O_1(2\delta')) \frac{|A|}{m} \ell^2 \\ &= \frac{|A|}{m} (2\ell d + d^2 + O_1(2\delta') ((\ell + d)^2 + \ell^2)). \end{aligned} \quad (24)$$

Therefore, replacing the left-hand side of (20) by (24) and using (21) immediately yields

$$\begin{aligned} &d|A \cap \varrho^{-1}([d_1, d_2])| \\ &\quad + \sum \{ |A \cap \varrho^{-1}(f)| (f - d'_1) : d'_1 < f < d_1 \} \\ &\quad + \sum \{ |A \cap \varrho^{-1}(f)| (d'_2 - f) : d_2 \leq f < d'_2 \} \\ &= \frac{|A|}{m} (2\ell d + d^2 + O_1(2\delta') ((\ell + d)^2 + \ell^2)). \end{aligned} \quad (25)$$

Clearly, (25) implies that

$$d|A \cap \varrho^{-1}([d_1, d_2])| \leq \frac{|A|}{m} (2\ell d + d^2 + O_1(2\delta') ((\ell + d)^2 + \ell^2)). \quad (26)$$

Moreover, we observe that

$$\begin{aligned} d|A \cap \varrho^{-1}([d_1, d_2])| &\geq d|A \cap \varrho^{-1}([d_1 + d, d_2 - d])| \\ &\quad + \sum \{ |A \cap \varrho^{-1}(f)| (f - d_1) : d_1 \leq f < d_1 + d \} \\ &\quad + \sum \{ |A \cap \varrho^{-1}(f)| (d_2 - f) : d_2 - d \leq f < d_2 \} \\ &= \frac{m}{n} \left(w([s, s + \ell], [t, t + \ell]) - w([s + d, s + \ell], [t + d, t + \ell]) \right), \end{aligned}$$

where the last identity follows from Lemma 19 in the same way that equation (20) follows from that lemma. Then essentially the same calculations as in (24) give

$$\begin{aligned} &\frac{m}{n} \left(w([s, s + \ell], [t, t + \ell]) - w([s + d, s + \ell], [t + d, t + \ell]) \right) \\ &= \frac{|A|}{m} (2(\ell - d)d + d^2 + O_1(2\delta') (\ell^2 + (\ell - d)^2)), \end{aligned}$$

and hence

$$d|A \cap \varrho^{-1}([d_1, d_2])| \geq \frac{|A|}{m} (2\ell d - d^2 + O_1(2\delta') (\ell^2 + (\ell - d)^2)). \quad (27)$$

Inequality (19) follows from (26) and (27), and thus Lemma 20 is proved. \square

We prove a simple corollary of Lemma 20 that allows us to rewrite the conditions of Lemma 20 in terms of d_1 and d_2 . Moreover, the hypotheses of Lemma 20 imply that $d_2 - d_1 = 2\ell$ is even. The following corollary overcomes this shortcoming.

Corollary 21. *Let d , d_1 , and d_2 be positive integers, δ' a real number such that $0 < \delta' \leq 1$, and suppose that*

- (i) $0 < d \leq d_1 < d_2 - 1 < d_2 + 1 \leq \frac{1}{2}m - d$,
- (ii) $\text{DISC}_2(\delta')$ holds for $G = G(\Gamma, A)$,
- (iii) $\frac{1}{2}(d_2 - d_1 - 1) - d \geq \delta'm$,
- (iv) $n \sim_{\delta'/2} (n - 1)$.

Then

$$\left| |A \cap \varrho^{-1}([d_1, d_2])| - \frac{d_2 - d_1}{m} |A| \right| \leq \frac{|A|}{m} \left(d + 1 + \frac{\delta'}{d} \cdot \frac{m^2}{4} \right). \quad (28)$$

Proof. We distinguish two cases depending on the parity of $d_2 - d_1$. We later reduce the second case ($d_2 - d_1$ odd) to the first case ($d_2 - d_1$ even). In order to be prepared for this we are going to show a stronger statement for the first case.

Case 1 ($d_2 - d_1$ is even). Let us consider the following weaker conditions (i') and (iii') instead of (i) and (iii):

- (i') $0 < d \leq d_1 < d_2 \leq \frac{m}{2} - d$,
- (iii') $\frac{1}{2}(d_2 - d_1) - d \geq \delta'm$.

We are now going to show a stronger conclusion than (28) under these weaker assumptions. In particular, we shall verify

$$\left| |A \cap \varrho^{-1}([d_1, d_2])| - \frac{d_2 - d_1}{m} |A| \right| \leq \frac{|A|}{m} \left(d + \frac{\delta'}{d} \cdot \frac{m^2}{4} \right). \quad (29)$$

For this we want to apply Lemma 20 for the “right” choice of s , t , and ℓ . First, note that (ii) and (iv) are the same in Lemma 20 and Corollary 21. We set

$$s = d, \quad \ell = \frac{1}{2}(d_2 - d_1), \quad \text{and} \quad t = s + \ell + d_1.$$

Simple calculations using (i') and (iii') show that

$$0 = s - d < s + \ell \leq t - d < t + \ell \leq \frac{1}{2}m \quad \text{and} \quad \ell - d \geq \delta'm,$$

and hence (i) and (iii) of Lemma 20 hold for this particular choice of s , t , and ℓ . Moreover, $t - s - \ell = d_1$ and $t - s + \ell = d_2$, thus Lemma 20 implies

$$\left| |A \cap \varrho^{-1}([d_1, d_2])| - \frac{2\ell}{m} |A| \right| \leq \frac{|A|}{m} \left(d + \frac{2\delta'}{d} ((\ell + d)^2 + \ell^2) \right),$$

which, combined with

$$\ell^2 \leq (\ell + d)^2 = \frac{(d_2 - d_1 + 2d)^2}{4} = \frac{((d_2 + d) + (d - d_1))^2}{4} \leq \frac{(m/2)^2}{4} = \frac{m^2}{16},$$

gives inequality (29).

Case 2 ($d_2 - d_1$ is odd). The hypotheses of Lemma 20 unfortunately always imply $\ell = d_2 - d_1$ is even. In order to get a bound for intervals $[d_1, d_2]$ of odd length we “sandwich” $|A \cap \varrho^{-1}([d_1, d_2])|$ as follows:

$$|A \cap \varrho^{-1}([d_1, d_2 - 1])| \leq |A \cap \varrho^{-1}([d_1, d_2])| \leq |A \cap \varrho^{-1}([d_1, d_2 + 1])|. \quad (30)$$

Now we apply Case 1 twice to derive the upper and lower bounds in (28). For the upper bound, we set

$$d_2^U = d_2 + 1.$$

Then conditions (i) and (iii) of Corollary 21 are “strong” enough to imply (i') and (iii') of Case 1, applied to d_2^U instead of d_2 . Thus, by (29), we may bound the right-hand side of (30) from above by

$$\begin{aligned} |A \cap \varrho^{-1}([d_1, d_2 + 1])| &= |A \cap \varrho^{-1}([d_1, d_2^U])| \\ &\leq \frac{|A|}{m} \left(d + \frac{\delta'}{d} \cdot \frac{m^2}{4} \right) + \frac{d_2^U - d_1}{m} |A| \\ &= \frac{|A|}{m} \left(d + 1 + \frac{\delta'}{d} \cdot \frac{m^2}{4} \right) + \frac{d_2 - d_1}{m} |A|. \end{aligned}$$

Hence, the upper bound for $|A \cap \varrho^{-1}([d_1, d_2])|$ in (28) follows. The lower bound necessary to complete the proof of Corollary 21 may be verified by the same kind of argument applied to $d_2^L = d_2 - 1$ instead of d_2^U . \square

Corollary 21 above gives us control over

$$|A \cap \varrho^{-1}([d_1, d_2])|,$$

as long as d_1 and d_2 are bounded away from 0 and $m/2$. The following two lemmas consider the quantities

$$|A \cap \varrho^{-1}([0, d])| \quad \text{and} \quad \left| A \cap \varrho^{-1} \left(\left[\left\lfloor \frac{m}{2} \right\rfloor - d - 1, \left\lfloor \frac{m}{2} \right\rfloor + 1 \right] \right) \right|. \quad (31)$$

Lemma 22. *Suppose $0 < \delta \leq 1/3$, $d \geq \delta m/2$, and $n \geq 4$. If $\text{DISC}(\delta)$ holds for $G = G(\Gamma, A)$, then*

$$|A \cap \varrho^{-1}([0, d])| \leq 4 \frac{d}{m} |A|. \quad (32)$$

Proof. Let $\delta > 0$ and d be as in the statement of the lemma, and assume that G satisfies $\text{DISC}(\delta)$. Let us estimate from above the number of edges induced by

$$U = \varrho^{-1}([0, 2d])$$

in G . We have $|U| = 2dn/m \geq \delta n$. Invoking $\text{DISC}(\delta)$, using that $0 < \delta \leq 1/3$ and $n \geq 4$, and recalling that $|A| = \alpha n$, we obtain that

$$e(G[U]) \leq (1 + \delta) \frac{|A|}{n-1} \binom{|U|}{2} \leq 4\alpha \left(\frac{dn}{m} \right)^2. \quad (33)$$

On the other hand, by Lemma 18, we have

$$e(G[U]) = \sum_{r=0}^{2d-1} \sum_{s=r+1}^{2d-1} w(\{r, s\}) + \sum_{r=0}^{2d-1} w(r) \geq \sum_{r=0}^{d-1} \sum_{s=r+1}^{r+d-1} w(\{r, s\}) + \sum_{r=0}^{2d-1} w(r). \quad (34)$$

Now fix $0 \leq r < d$. If $r < s < r + d$, then $0 < s - r < d$, and, by (12) of Lemma 18, we have

$$\begin{aligned} \sum_{s=r+1}^{r+d-1} w(\{r, s\}) &= \frac{n}{m} \sum_{s=r+1}^{r+d-1} |A \cap \varrho^{-1}(s-r)| \\ &= \frac{n}{m} \sum_{f=1}^{d-1} |A \cap \varrho^{-1}(f)| = \frac{n}{m} |A \cap \varrho^{-1}([1, d])|. \end{aligned} \quad (35)$$

Also, by (13),

$$w(r) = \frac{n}{2m} |A \cap \varrho^{-1}(0)|,$$

and we may conclude from (34) that

$$e(G[U]) \geq d \frac{n}{m} |A \cap \varrho^{-1}([1, d])| + 2d \frac{n}{2m} |A \cap \varrho^{-1}(0)| = d \frac{n}{m} |A \cap \varrho^{-1}([0, d])|. \quad (36)$$

Comparing (33) and (36), inequality (32) follows and our lemma is proved. \square

Our next lemma concerns the second interval in (31).

Lemma 23. *Suppose $0 < \delta' \leq 1/3$, $d \geq \delta' m$, and $n \geq 4$. If $\text{DISC}_2(\delta')$ holds for $G = G(\Gamma, A)$, then*

$$\left| A \cap \varrho^{-1} \left(\left[\left\lfloor \frac{m}{2} \right\rfloor - d - 1, \left\lfloor \frac{m}{2} \right\rfloor + 1 \right) \right) \right| \leq 4 \frac{d+1}{m} |A|. \quad (37)$$

Proof. Let $\delta' > 0$ and d be as in the statement of the lemma, and assume that G satisfies $\text{DISC}_2(\delta')$. Let us estimate from above the number of edges in the bipartite graph induced by the vertex classes

$$U = \varrho^{-1}([0, d]) \quad \text{and} \quad W = \varrho^{-1}(\left[\lfloor m/2 \rfloor - d - 1, \lfloor m/2 \rfloor + d \right])$$

in G . We have $|U| = dn/m \geq \delta' n$ and $|W| = (2d+1)n/m > \delta' n$. Invoking $\text{DISC}_2(\delta')$ and using that $0 < \delta' \leq 1/3$ and $n \geq 4$, we obtain that

$$e(G[U, W]) \leq (1 + \delta') \frac{|A|}{n-1} |U||W| \leq 4\alpha \frac{d(d+1)n^2}{m^2}. \quad (38)$$

On the other hand, by Lemma 18, we have

$$\begin{aligned} e(G[U, W]) &\geq \sum_{r=0}^{d-1} \sum \left\{ w(\{r, s\}) : \left\lfloor \frac{m}{2} \right\rfloor - d - 1 + r \leq s < \left\lfloor \frac{m}{2} \right\rfloor + 1 + r \right\} \\ &= \sum_{r=0}^{d-1} \frac{n}{m} \sum \left\{ |A \cap \varrho^{-1}(f)| : \left\lfloor \frac{m}{2} \right\rfloor - d - 1 \leq f < \left\lfloor \frac{m}{2} \right\rfloor + 1 \right\} \\ &= d \frac{n}{m} |A \cap \varrho^{-1} \left(\left[\left\lfloor \frac{m}{2} \right\rfloor - d - 1, \left\lfloor \frac{m}{2} \right\rfloor + 1 \right) \right)|. \end{aligned} \quad (39)$$

Comparing (38) and (39), we deduce (37). Lemma 23 is proved. \square

We may now prove Lemma 14.

Proof of Lemma 14. Let positive reals $\eta \leq 1$ and $\sigma \leq 1$ be given. We may assume that $\sigma\eta \leq 1/2$. We set

$$\delta' = \frac{(\eta\sigma)^2}{240} \leq \frac{1}{3}, \quad (40)$$

and we let δ be sufficiently small (as given by Fact 3), so that $\text{DISC}(\delta)$ implies $\text{DISC}_2(\delta')$. Again, without loss of generality, we may assume $\delta \leq \delta'$. We let $n_0 \geq 4$ be sufficiently large so that $n \sim_{\delta'/2} (n-1)$ for every $n \geq n_0$. We shall now show that this choice of constants will do. Thus, let $G = G(\Gamma, A)$ with $|\Gamma| = n \geq n_0$ and $m > 1/\delta$ be given (we follow the notation in Setup 10), and suppose that G satisfies $\text{DISC}(\delta)$.

Let $0 \leq D_1 < D_2 \leq \lfloor m/2 \rfloor + 1$ be such that $D_2 - D_1 \geq \eta m$. We fix

$$d = \left\lfloor \frac{\eta\sigma m}{60} \right\rfloor \geq \left\lfloor \frac{\eta\sigma}{60\delta} \right\rfloor \geq \left\lfloor \frac{4}{\eta\sigma} \right\rfloor \geq 4,$$

and

$$d_1 = \max\{D_1, d\} \quad \text{and} \quad d_2 = \min\left\{D_2, \left\lfloor \frac{m}{2} \right\rfloor - d - 1\right\}.$$

Using $m > 1/\delta \geq 1/\delta' = 240/(\eta\sigma)^2$, $2\eta\sigma \leq 1$, and $d + 1 \leq 3d/2$, we see that

$$1 < \delta m \leq \delta' m \leq \frac{\delta' m}{2\eta\sigma} = \frac{\eta\sigma m}{480} \leq d < d + 1 \leq \frac{\eta\sigma m}{40} \quad (41)$$

and

$$D_2 - D_1 - 2(d + 1) \leq d_2 - d_1 \leq D_2 - D_1. \quad (42)$$

Now we check that the assumptions of Corollary 21, Lemma 22, and Lemma 23 hold simultaneously. It is obvious that the conditions in Lemma 22 and 23 hold by our choice of δ , δ' , n_0 , and the inequalities in (41). Moreover, conditions (ii) and (iv) of Corollary 21 hold by the definition of δ (yielding $\text{DISC}_2(\delta')$ for G), and n_0 . It remains to verify (iii) and (i) in Corollary 21. We start with condition (iii). For this we note that, by the left-hand side of (42) and by (41),

$$d_2 - d_1 \geq \eta m - \frac{\eta\sigma m}{20}.$$

Using $1 < \delta m$, (41), and $\delta \leq \delta' \leq \eta/6$ (see (40)), we verify (iii):

$$\begin{aligned} \frac{1}{2}(d_2 - d_1 - 1) - d &\geq \frac{1}{2}\left(\eta m - \frac{\eta\sigma m}{20} - \delta m - \frac{\eta\sigma m}{20}\right) \\ &\geq \frac{1}{2}\left(\frac{\eta m}{2} - \delta m\right) \geq \frac{3\delta' m - \delta' m}{2} = \delta' m. \end{aligned}$$

Moreover, the last inequality implies $d_2 - 1 - d_1 > 1$ (using $\delta' m > 1$) and thus (i) of Corollary 21 follows as well.

Having verified the assumptions of Corollary 21, Lemma 22, and Lemma 23, we use these lemmas to verify the claim of Lemma 14, i.e.,

$$|A \cap \varrho^{-1}([D_1, D_2])| \sim_{\sigma} \frac{D_2 - D_1}{m} |A|. \quad (43)$$

We first derive the upper bound in (43). Note that

$$\begin{aligned} |A \cap \varrho^{-1}([D_1, D_2])| &\leq |A \cap \varrho^{-1}([0, d])| + |A \cap \varrho^{-1}([d_1, d_2])| \\ &\quad + |A \cap \varrho^{-1}([\lfloor m/2 \rfloor - d - 1, \lfloor m/2 \rfloor + 1])|. \end{aligned}$$

Applying Lemma 22, Corollary 21, and Lemma 23 to the first, second, and third terms, of the right-hand side of the above inequality, respectively, yields

$$\begin{aligned} |A \cap \varrho^{-1}([D_1, D_2])| &\leq 4\frac{d}{m}|A| + \left(\frac{|A|}{m} \left(d + 1 + \frac{\delta' m^2}{4d}\right) + \frac{d_2 - d_1}{m}|A|\right) + 4\frac{d+1}{m}|A| \\ &\leq \frac{|A|}{m} \left(10(d+1) + \frac{\delta' m^2}{4d}\right) + \frac{d_2 - d_1}{m}|A|. \end{aligned}$$

Using (40), (41), and (42), we can bound this last expression further by

$$\frac{|A|}{m} \left(\frac{\sigma\eta m}{4} + \frac{\sigma\eta m}{2}\right) + \frac{D_2 - D_1}{m}|A|,$$

and, finally, $D_2 - D_1 \geq \eta m$ gives

$$|A \cap \varrho^{-1}([D_1, D_2])| \leq (1 + \sigma) \frac{D_2 - D_1}{m}|A|. \quad (44)$$

It is left for us to show the lower bound in (43). Note

$$|A \cap \varrho^{-1}([D_1, D_2])| \geq |A \cap \varrho^{-1}([d_1, d_2])|,$$

and hence Corollary 21 implies

$$|A \cap \varrho^{-1}([D_1, D_2])| \geq \frac{d_2 - d_1}{m}|A| - \frac{|A|}{m} \left(d + 1 + \frac{\delta' m^2}{4d}\right). \quad (45)$$

Similar calculations to the ones above, based on (42), (40), and (41), show that

$$\begin{aligned} \frac{d_2 - d_1}{m}|A| - \frac{|A|}{m} \left(d + 1 + \frac{\delta' m^2}{4d}\right) &\geq \frac{D_2 - D_1}{m}|A| - \frac{|A|}{m} \left(3(d+1) + \frac{\delta' m^2}{4d}\right) \\ &\geq \frac{D_2 - D_1}{m}|A| \left(1 - \frac{\sigma\eta m}{10(D_2 - D_1)} - \frac{\sigma\eta m}{2(D_2 - D_1)}\right). \end{aligned} \quad (46)$$

Again, since $D_2 - D_1 \geq \eta m$, it follows from (45) combined with (46) that

$$|A \cap \varrho^{-1}([D_1, D_2])| \geq (1 - \sigma) \frac{D_2 - D_1}{m}|A|. \quad (47)$$

Finally, (44) and (47) imply (43), and therefore Lemma 14 is proved. \square

2.3.4. \mathbb{Z} -INT-DISC implies EIG. In this section we give the proofs of Lemmas 15 and 16. We start with the proof of Lemma 15, which “translates” the results of Lemma 14 for ϱ and $\mathbb{Z}/m\mathbb{Z}$ to χ_{ARG} and $\mathbb{R}/2\pi\mathbb{R}$.

Proof of Lemma 15. Let σ and η be as in the statement of Lemma 15, and suppose A satisfies \mathbb{Z} -INT-DISC($g; \eta/2, \sigma/3$). Let $0 \leq \theta_1 < \theta_2 \leq \pi$ with $\theta_2 - \theta_1 \geq 2\pi\eta$ be given. Our aim is to show (7), i.e.,

$$|A \cap \chi_{\text{ARG}}^{-1}([\theta_1, \theta_2])| \sim_{\sigma} \frac{\theta_2 - \theta_1}{2\pi}|A|.$$

Recall we have $\varrho: \Gamma \rightarrow \mathbb{Z}/m\mathbb{Z}$ and $\Omega: \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{R}/2\pi\mathbb{R}$ such that $\chi_{\text{ARG}} = \Omega\varrho$ (see Setup 10). Put

$$D_1 = \left\lceil m \frac{\theta_1}{2\pi} \right\rceil \quad \text{and} \quad D_2 = \left\lceil m \frac{\theta_2}{2\pi} \right\rceil + 1.$$

Observe that

$$\frac{2\pi}{m} \left(\left\lceil \frac{m\theta_1}{2\pi} \right\rceil - 1 \right) < \theta_1 \leq \frac{2\pi}{m} \left\lceil \frac{m\theta_1}{2\pi} \right\rceil,$$

and hence we have

$$\frac{2\pi}{m} \left(\left\lceil \frac{m\theta_1}{2\pi} \right\rceil - 1 \right) = \Omega(D_1 - 1) < \theta_1 \leq \Omega(D_1) = \frac{2\pi}{m} \left\lceil \frac{m\theta_1}{2\pi} \right\rceil.$$

Similarly, one may check that $\Omega(D_2 - 1) \leq \theta_2 < \Omega(D_2)$, and consequently

$$\Omega^{-1}([\theta_1, \theta_2]) = [D_1, D_2].$$

We now observe that

$$D_2 - D_1 = \left\lfloor m \frac{\theta_2}{2\pi} \right\rfloor + 1 - \left\lfloor m \frac{\theta_1}{2\pi} \right\rfloor = \frac{m}{2\pi} (\theta_2 - \theta_1) + O_1(1).$$

Using that $m\eta \geq m\eta\sigma \geq 3$, we deduce that

$$D_2 - D_1 \geq \frac{m}{2\pi} (\theta_2 - \theta_1) - 1 \geq \eta m - 1 \geq \frac{1}{2} \eta m.$$

Hence, by property \mathbb{Z} -INT-DISC($\varrho; \eta/2, \sigma/3$), we have

$$\begin{aligned} |A \cap \chi_{\text{ARG}}^{-1}([\theta_1, \theta_2])| &= |A \cap \varrho^{-1}([D_1, D_2])| \\ &\sim_{\sigma/3} \frac{1}{m} (D_2 - D_1) |A| \\ &= \frac{1}{m} \left(m \frac{\theta_2}{2\pi} - m \frac{\theta_1}{2\pi} + O_1(1) \right) |A| \\ &= \frac{1}{2\pi} \left(\theta_2 - \theta_1 + O_1 \left(\frac{2\pi}{m} \right) \right) |A|, \end{aligned} \tag{48}$$

which, using that $m\eta\sigma \geq 3$, is

$$\frac{1}{2\pi} \left(1 + O_1 \left(\frac{\sigma}{3} \right) \right) (\theta_2 - \theta_1) |A|. \tag{49}$$

We conclude from (48) and (49) that

$$|A \cap \chi_{\text{ARG}}^{-1}([\theta_1, \theta_2])| \sim_{\sigma} \frac{(\theta_2 - \theta_1)}{2\pi} |A|,$$

as required. The proof of Lemma 15 is complete. \square

Finally, we prove the last auxiliary lemma, Lemma 16, used in the proof of the main theorem, Theorem 6.

Proof of Lemma 16. Let $0 < \varepsilon \leq 1$ be given. We define the constants η and $\sigma > 0$ as follows.

$$\eta = \frac{\varepsilon}{8\pi} < \frac{1}{16} \quad \text{and} \quad \sigma = \frac{1}{8}\varepsilon. \tag{50}$$

In the remainder of the proof, we show that the above choice for the constants η and $\sigma > 0$ will do. Thus, let us suppose that the set $A \subseteq \Gamma \setminus \{0\}$ satisfies property S^1 -ARC-DISC($\chi_{\text{ARG}}; \eta, \sigma$). Our aim is to show that (8) holds, i.e.,

$$|\lambda^{(x)}| = \left| \sum_{a \in A} \chi(a) \right| \leq \varepsilon |A|.$$

For a complex number $z \in \mathbb{C}$, in what follows, we write $\Re(z)$ for the real and $\Im(z)$ for the imaginary part of z . Let us first observe that, owing to the fact that the eigenvalues of an undirected graph are real and that $A = -A$, we have

$$\begin{aligned} \lambda^{(\chi)} &= \sum_{a \in A} \chi(a) = \Re\left(\sum_{a \in A} \chi(a)\right) \\ &= 2\Re\left(\sum_{a \in A} \{\chi(a) : \Im(\chi(a)) > 0\}\right) + \Re\left(\sum_{a \in A} \{\chi(a) : \Im(\chi(a)) = 0\}\right). \end{aligned} \quad (51)$$

Moreover, it follows from S^1 -ARC-DISC $(\chi_{\text{ARG}}; \eta, \sigma)$ that

$$\begin{aligned} |A \cap \chi^{-1}(1)| &= |A \cap \chi_{\text{ARG}}^{-1}(0)| \leq |A \cap \chi_{\text{ARG}}^{-1}([0, 2\pi\eta])| \\ &\leq (1 + \sigma)\eta|A| \leq 2\eta|A| \leq \frac{1}{4}\varepsilon|A|. \end{aligned}$$

Similarly, we observe that $|A \cap \chi^{-1}(-1)| = |A \cap \chi_{\text{ARG}}^{-1}(\pi)| \leq (1/4)\varepsilon|A|$ and thus

$$\left| \Re\left(\sum_{a \in A} \{\chi(a) : \Im(\chi(a)) = 0\}\right) \right| = \left| |A \cap \chi^{-1}(1)| - |A \cap \chi^{-1}(-1)| \right| \leq \frac{1}{4}\varepsilon|A|.$$

Therefore, we infer from (51) that

$$|\lambda^{(\chi)}| \leq 2 \left| \Re\left(\sum_{a \in A} \{\chi(a) : \Im(\chi(a)) \geq 0\}\right) \right| + \frac{1}{4}\varepsilon|A|. \quad (52)$$

Thus, we are interested in $\Re(\chi(a))$ ($a \in A$, $\Im(\chi(a)) \geq 0$).

Put

$$k = \left\lfloor \frac{\pi/2}{4\pi\eta} \right\rfloor = \left\lfloor \frac{1}{8\eta} \right\rfloor \quad \text{and} \quad \phi = \frac{\pi}{2k}. \quad (53)$$

Observe for later reference that by (50) and (53)

$$4\pi\eta \leq \phi \leq 8\pi\eta = \varepsilon. \quad (54)$$

We shall subdivide the upper half of S^1 into $2k$ arcs, symmetric with respect to the imaginary axis (in fact, \mathbf{i} will be left out). The endpoints of the arcs will be $0, \phi, 2\phi, \dots, \pi$. Let us in fact denote by I_j^+ the arc of the $z = \exp(\theta\mathbf{i}) \in S^1$ with

$$(j-1)\phi \leq \theta < j\phi, \quad (55)$$

for all $1 \leq j \leq k$. Similarly, we let I_j^- be the arc of the $z = \exp(\theta\mathbf{i}) \in S^1$ with

$$\pi - j\phi < \theta \leq \pi - (j-1)\phi, \quad (56)$$

for all $1 \leq j \leq k$. Clearly, if $a \in \Gamma$ is such that $\chi(a) \in I_j^+$ ($1 \leq j \leq k$), then

$$\cos(j\phi) < \Re(\chi(a)) \leq \cos((j-1)\phi). \quad (57)$$

Similarly, if $a \in \Gamma$ is such that $\chi(a) \in I_j^-$ ($1 \leq j \leq k$), then

$$-\cos((j-1)\phi) < \Re(\chi(a)) \leq -\cos(j\phi). \quad (58)$$

We now state and prove the following claim.

Claim 24. *For all $1 \leq j \leq k$ and both $*$ $\in \{+, -\}$, we have*

$$|A \cap \chi^{-1}(I_j^*)| \sim_{2\sigma} \frac{\phi}{2\pi} |A|. \quad (59)$$

Proof. This claim follows easily from S^1 -ARC-DISC($\chi_{\text{ARG}}; \eta, \sigma$). Let $0 \leq \psi_1 < \psi_2 \leq \pi$ be such that

$$\psi_2 - \psi_1 \geq 4\pi\eta. \quad (60)$$

We shall show that

$$|A \cap \chi_{\text{ARG}}^{-1}([\psi_1, \psi_2])| \sim_{2\sigma} \frac{1}{2\pi}(\psi_2 - \psi_1)|A|. \quad (61)$$

One may similarly show that

$$|A \cap \chi_{\text{ARG}}^{-1}((\psi_1, \psi_2])| \sim_{2\sigma} \frac{1}{2\pi}(\psi_2 - \psi_1)|A|. \quad (62)$$

Claim 24 follows from (61) and (62). In particular (61) with $\psi_1 = (j-1)\phi$ and $\psi_2 = j\phi$ gives the claim for intervals of the type I_j^+ and similarly (62) yields (59) for intervals of the type I_j^- .

To prove (61), observe first that there is a $\xi > 0$ such that

$$A \cap \chi_{\text{ARG}}^{-1}([\psi_1, \psi_2]) = A \cap \chi_{\text{ARG}}^{-1}([\psi_1, \psi_2 - \xi]). \quad (63)$$

Moreover, we may clearly assume that

$$\frac{\xi}{4\pi\eta} \leq \frac{\sigma}{2}. \quad (64)$$

Then $\psi_2 - \psi_1 - \xi \geq 2\pi\eta$, and hence we may apply S^1 -ARC-DISC($\chi_{\text{ARG}}; \eta, \sigma$) to deduce that

$$|A \cap \chi_{\text{ARG}}^{-1}([\psi_1, \psi_2 - \xi])| \sim_{\sigma} \frac{1}{2\pi}(\psi_2 - \psi_1 - \xi)|A|, \quad (65)$$

and, by (60) and (64), we have

$$\frac{1}{2\pi}(\psi_2 - \psi_1 - \xi)|A| \sim_{\sigma/2} \frac{1}{2\pi}(\psi_2 - \psi_1)|A|. \quad (66)$$

Relation (61) follows from (63), (65), and (66), by

$$A \cap \chi_{\text{ARG}}^{-1}([\psi_1, \psi_2]) = A \cap \chi_{\text{ARG}}^{-1}([\psi_1, \psi_2 - \xi]) \sim_{2\sigma} \frac{1}{2\pi}(\psi_2 - \psi_1)|A|. \quad \square$$

Claim 24 and inequalities (57) and (58) may now be used to estimate the sum in (52). We have

$$\Re\left(\sum_{a \in A} \{\chi(a) : \Im(\chi(a)) \geq 0\}\right) = \Re\left(\sum_{j=1}^k \sum_{a \in A} \{\chi(a) : \chi(a) \in I_j^+ \cup I_j^-\}\right). \quad (67)$$

Fix $1 \leq j \leq k$. We have, by Claim 24 and inequalities (57) and (58),

$$\begin{aligned} & \Re\left(\sum_{a \in A} \{\chi(a) : \chi(a) \in I_j^+ \cup I_j^-\}\right) \\ & \leq \frac{\phi}{2\pi}|A|\left((1+2\sigma)\cos((j-1)\phi) - (1-2\sigma)\cos(j\phi)\right). \end{aligned} \quad (68)$$

Using that $\cos((j-1)\phi) - \cos(j\phi) \leq \phi$, we observe that the right-hand side of (68) is smaller than

$$\frac{\phi}{2\pi}|A|\left(\phi + 4\sigma\right). \quad (69)$$

Therefore, from (68) and (69) we deduce that the expression in (67) is, in absolute value, at most

$$k \frac{\phi}{2\pi} |A| (\phi + 4\sigma) = \frac{1}{4} |A| (\phi + 4\sigma) \leq \frac{1}{4} |A| \left(\varepsilon + \frac{1}{2} \varepsilon \right) = \frac{3}{8} \varepsilon |A|, \quad (70)$$

where in this inequality we used (50) and (54). Combining (70) with (52), we infer that

$$|\lambda^{(x)}| \leq 2 \frac{3}{8} \varepsilon |A| + \frac{1}{4} \varepsilon |A| = \varepsilon |A|,$$

as claimed in Lemma 16. \square

3. FURTHER DISCUSSION ON THE MAIN RESULT

We now expand on the comments made in Section 1.2. First, we describe our construction that shows that DISC does not imply EIG for sequences of arbitrary graphs. We start by setting out some notation. Let integers $1 \leq k \leq l$ and reals $0 < \varepsilon < 1$, $0 < \delta < 1$, and $0 < \vartheta < 1$ be given. For all integers i and j with $1 \leq i < k < j \leq l$, let functions

$$\Phi_i, \phi_j: \mathbb{N} \rightarrow \mathbb{N} \text{ and } p: \mathbb{N} \rightarrow (0, 1)$$

be given, and suppose further that we have

$$(i) \quad \lim_{m \rightarrow \infty} p(m) = 0 \quad \text{and} \quad p(m) \geq m^{\vartheta-1},$$

$$(ii) \quad \sum_{i=1}^{k-1} \Phi_i^2(m) + \sum_{i=k+1}^l \phi_i^2(m) = o(p(m) \cdot m^2),$$

and, for every integer m ,

$$(iii) \quad \Phi_1(m) \geq \dots \geq \Phi_{k-1}(m) \geq (1 + 2\varepsilon)p(m) \cdot m > \\ > (1 - 2\varepsilon)p(m) \cdot m \geq \phi_{k+1}(m) \geq \dots \geq \phi_l(m).$$

Fact 25. *Let $k, l, \varepsilon, \delta, \vartheta, \Phi_i$, and ϕ_j , and p be as above. Then there exists an integer $m_0 \geq 1$ such that for every $m \geq m_0$ there is a graph G on $n = m + \sum_{i=1}^{k-1} (\Phi_i(m) + 1) + \sum_{i=k+1}^l (\phi_i(m) + 1)$ vertices with average degree $\bar{d} = \bar{d}(G) \sim_{\varepsilon/2} p(m)m$ having the following properties:*

$$(a) \quad G \text{ satisfies } \text{DISC}(\delta)$$

and after ordering the eigenvalues $\lambda_1 \geq |\lambda_2| \geq \dots \geq |\lambda_n|$

$$(b) \quad \lambda_i \begin{cases} = \Phi_i(m) & \text{for } 1 \leq i < k \\ \sim_{\varepsilon} \bar{d} & \text{for } i = k \\ = \phi_i(m) & \text{for } k < i \leq l \\ \leq \varepsilon \bar{d} & \text{for } l < i \leq n. \end{cases}$$

Fact 25 immediately implies that Theorem 6 does not hold for all graphs. Set, e.g., $k = 1$, $l = 2$, $\phi_2(m) = \lfloor (1/2)p(m)m \rfloor$, and $\varepsilon = 1/10$. Then a statement such as the one Theorem 6 fails. In particular, for every $\delta > 0$ Fact 25 yields a graph G that satisfies $\text{DISC}(\delta)$, but $\lambda_2(G) = \phi_2(m) = \lfloor (1/2)p(m)m \rfloor > \varepsilon \bar{d}$.

Proof of Fact 25. Let the numbers $k, l, \varepsilon, \delta, \vartheta$, and functions Φ_i, ϕ_i , and p be given. Let m be sufficiently large and consider the binomial random graph $\mathbb{G}(m, p)$ on m vertices and two vertices of $\mathbb{G}(m, p)$ adjacent with probability $p = p(m)$ (for more details about random graphs see, e.g., the excellent monographs [6] and [12]). Let G be the disjoint union

$$G = \bigcup_{i=1}^{k-1} K^{\Phi_i(m)+1} \cup \bigcup_{i=k+1}^l K^{\phi_i(m)+1} \cup \mathbb{G}(m, p),$$

where K^t denotes the complete graph on t vertices. We claim the graph G satisfies the conclusion of Fact 25 asymptotically almost surely (a.a.s.), i.e. with probability tending to 1, as m tends to infinity.

First we observe that (ii) and the Cauchy–Schwarz inequality imply that

$$n \sim_{\varepsilon/6} m \tag{71}$$

for m sufficiently large. It also follows from (ii) and the properties of the binomial distribution that a.a.s.

$$e(G) \sim_{\varepsilon/6} \frac{1}{2} p(m) m^2,$$

which combined with (71) yields

$$\bar{d}(G) \sim_{\varepsilon/2} p(m) m.$$

Furthermore, it is easy to check that, owing to (i) and (ii), $\text{DISC}(\delta)$ holds for arbitrary $\delta \geq 0$ and sufficiently large m depending on δ .

On the other hand, $\mathbb{G}(m, p)$ has, a.a.s., an eigenvalue $\sim_{\varepsilon/2} p(m) m$, with multiplicity 1, and the remaining eigenvalues of $\mathbb{G}(m, p)$ are $o(p(m) m)$. (Much stronger estimates are known, even for smaller values of p ; see, e.g., Remark 1 in Section 3 of [15], which is based on [11].) The only non-zero eigenvalues of the complete graphs (again with multiplicity 1) are $\Phi_i(m)$ and $\phi_j(m)$ for $1 \leq i < k < j \leq l$. This clearly implies Fact 25 for sufficiently large m . \square

We close this paper with an outline of a proof of Fact 8.

Proof of Fact 8 (sketch). Let $0 < p(n) < 1$ be an arbitrary function such that $p(n) = o(1)$ and $p(n)n/(\log(1/p(n)))^2 \rightarrow \infty$ as $n \rightarrow \infty$. For every integer n let $q(n)$ be the prime closest to

$$\frac{(\log(1/p(n)))^2}{p(n)}$$

and set

$$s(n) = \left\lfloor \frac{n}{q(n)} \right\rfloor \quad \text{and} \quad N(n) = s(n)q(n).$$

We observe that $q(n)$ and $s(n)$ tend to infinity as $n \rightarrow \infty$. It follows that

$$N(n) = (1 + o(1))n. \tag{72}$$

For every n consider the cyclic group $\mathbb{Z}/q(n)\mathbb{Z}$. We choose uniformly at random a symmetric subset $A_{q(n)} \subseteq \mathbb{Z}/q(n)\mathbb{Z}$ by including a and $-a$ with probability $p(n)/2$ for $0 < a < q(n)/2$. The random Cayley graph $H_{q(n)} = G(\mathbb{Z}/q(n)\mathbb{Z}, A_{q(n)})$ is a.a.s. $(1 + o(1))p(n)q(n)$ -regular. Let us argue that $H_{q(n)}$ satisfies $\text{EIG}(\varepsilon)$ a.a.s. for every fixed $\varepsilon > 0$. Fix some irreducible character $\chi \neq 1$. Note that $|\text{im } \chi| = q(n)$, since $q(n)$ is chosen to be a prime. Consider the corresponding homomorphism $\varrho =$

$\varrho_\chi: \mathbb{Z}/q(n)\mathbb{Z} \rightarrow \mathbb{Z}/q(n)\mathbb{Z}$ (see Setup 10). By standard large deviation inequalities, using $p(n)q(n) \gg \log(q(n))$, one sees that $A_{q(n)}$ satisfies \mathbb{Z} -INT-DISC($\varrho; \eta, \sigma$) with probability $1 - o(1/n)$ for any fixed positive η and σ . It follows from Lemma 15 and 16 that for every fixed $\varepsilon > 0$ and for all $\chi \neq 1$ a.a.s. $|\lambda^{(\chi)}| \leq \varepsilon|A|$ and, hence, $H_{q(n)}$ a.a.s. has EIG(ε).

We now consider the Cayley graph

$$G_{N(n)} = G(\mathbb{Z}/q(n)\mathbb{Z} \oplus \Gamma_{s(n)}, A_{q(n)} \times \Gamma_{s(n)}) ,$$

where $\Gamma_{s(n)}$ is any arbitrary abelian group of order $s(n)$. One may see that $G_{N(n)}$ is a “blow-up” of $H_{q(n)}$, where each vertex in $H_{q(n)}$ is replaced by an independent set of size $s(n)$ and two such independent sets are completely joined whenever the corresponding vertices are adjacent in $H_{q(n)}$. The “blow-up” of a vertex in $H_{q(n)}$ is simply its preimage under the projection map $\mathbb{Z}/q(n)\mathbb{Z} \oplus \Gamma_{s(n)} \rightarrow \mathbb{Z}/q(n)\mathbb{Z}$.

It is very easy to see that $G_{N(n)}$ has eigenvalues $s(n)\lambda_1, \dots, s(n)\lambda_{q(n)}$, where $\lambda_1, \dots, \lambda_{q(n)}$ are the eigenvalues of $H_{q(n)}$, and the remaining $(s(n) - 1)q(n)$ eigenvalues of $G_{N(n)}$ are 0. Since, $H_{q(n)}$ a.a.s. satisfies EIG(ε) for every constant $\varepsilon > 0$, so does $G_{N(n)}$. By Theorem 1, of [8], a.a.s. $G_{N(n)}$ also has property DISC(δ) for every fixed $\delta > 0$.

On the other hand, it is easy to see that for every fixed integer $\ell > 1$ and every positive ξ the graph $G_{N(n)}$ does not satisfy CIRCUIT $_{2\ell}(\xi)$ if $N(n)$ is sufficiently large. Indeed, counting only the circuits in which the first and every second vertex comes from the same “blown-up” vertex, we may bound the number $\#\{C_{2\ell}^* \hookrightarrow G_{N(n)}\}$ of 2ℓ -circuits in $G_{N(n)}$ from below by

$$N(n) \cdot d_{N(n)}^\ell \cdot s(n)^{\ell-1} ,$$

where $d_{N(n)}$ is the degree of every vertex in $G_{N(n)}$. By (72), $p(n) = o(1)$, and $d_{N(n)} = (1 + o(1))p(n)N(n)$ a.a.s., it follows that for some constant $c = c(\ell) > 0$, a.a.s.,

$$\#\{C_{2\ell}^* \hookrightarrow G_{N(n)}\} \geq c \frac{N(n)d_{N(n)}^{2\ell-1}}{(\log(1/p(n)))^{2(\ell-1)}} \gg d_{N(n)}^{2\ell} = \bar{d}(G_{N(n)})^{2\ell} .$$

□

REFERENCES

1. N. Alon, *Eigenvalues and expanders*, *Combinatorica* **6** (1986), no. 2, 83–96, Theory of computing (Singer Island, Fla., 1984). [1](#)
2. N. Alon and F. R. K. Chung, *Explicit construction of linear sized tolerant networks*, *Discrete Mathematics* **72** (1988), no. 1-3, 15–19. [1](#)
3. N. Alon and V. D. Milman, *Eigenvalues, expanders and superconcentrators*, 25th annual Symposium on Foundations of Computer Science, October 24–26, 1984, Singer Island, Florida (1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA) (IEEE, ed.), IEEE Computer Society Press, 1984, pp. 320–322. [1](#)
4. N. Alon and J. H. Spencer, *The probabilistic method*, John Wiley & Sons Inc., New York, 1992, With an appendix by Paul Erdős, A Wiley-Interscience Publication. [1](#)
5. L. Babai, *Spectra of Cayley graphs*, *J. Combin. Theory Ser. B* **27** (1979), no. 2, 180–189. [2.1](#)
6. B. Bollobás, *Random graphs*, second ed., Cambridge University Press, Cambridge, 2001. [3](#)

7. F. R. K. Chung and R. L. Graham, *Quasi-random subsets of Z_n* , J. Combin. Theory Ser. A **61** (1992), no. 1, 64–86. [1](#)
8. ———, *Sparse quasi-random graphs*, Combinatorica **22** (2002), no. 2, 217–244, Special issue: Paul Erdős and his mathematics. [1](#), [1.1](#), [1.2](#), [1.2](#), [3](#)
9. F. R. K. Chung, R. L. Graham, and R. M. Wilson, *Quasi-random graphs*, Combinatorica **9** (1989), no. 4, 345–362. [1](#)
10. P. Frankl, V. Rödl, and R. M. Wilson, *The number of submatrices of a given type in a Hadamard matrix and related results*, J. Combin. Theory Ser. B **44** (1988), no. 3, 317–328. [1](#)
11. Z. Füredi and J. Komlós, *The eigenvalues of random symmetric matrices*, Combinatorica **1** (1981), no. 3, 233–241. [3](#)
12. S. Janson, T. Łuczak, and A. Ruciński, *Random graphs*, Wiley-Interscience, New York, 2000. [3](#)
13. Y. Kohayakawa and V. Rödl, *Regular pairs in sparse random graphs I*, Random Structures Algorithms, to appear. [1](#)
14. Y. Kohayakawa, V. Rödl, and P. A. Sissokho, *Embedding graphs with bounded degree in sparse pseudorandom graphs*, Israel J. Math., to appear. [1](#)
15. M. Krivelevich and B. Sudakov, *Pseudo-random graphs*, submitted. [1](#), [1.2](#), [3](#)
16. L. Lovász, *Spectra of graphs with transitive groups*, Period. Math. Hungar. **6** (1975), no. 2, 191–195. [2.1](#)
17. ———, *Combinatorial problems and exercises*, North-Holland Publishing Co., Amsterdam, 1979. [2.1](#)
18. V. Rödl, *On universality of graphs with uniformly distributed edges*, Discrete Math. **59** (1986), no. 1-2, 125–134. [1](#)
19. J.-P. Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1977, Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42. [2.1](#)
20. R. M. Tanner, *Explicit concentrators from generalized N -gons*, SIAM J. Algebraic Discrete Methods **5** (1984), no. 3, 287–293. [1](#)
21. A. G. Thomason, *Pseudorandom graphs*, Random graphs '85 (Poznań, 1985), North-Holland Math. Stud., vol. 144, North-Holland, Amsterdam, 1987, pp. 307–331. [1](#)
22. ———, *Random graphs, strongly regular graphs and pseudorandom graphs*, Surveys in combinatorics 1987 (New Cross, 1987), London Math. Soc. Lecture Note Ser., vol. 123, Cambridge Univ. Press, Cambridge, 1987, pp. 173–195. [1](#)

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, EMORY UNIVERSITY, ATLANTA, GA 30322, USA

E-mail address: {yoshi|rod1|mschach}@mathcs.emory.edu