



**HAL**  
open science

# Sieving in graphs and explicit bounds for non-typical elements

Florent Jouve, Jean-Sébastien Sereni

► **To cite this version:**

Florent Jouve, Jean-Sébastien Sereni. Sieving in graphs and explicit bounds for non-typical elements. 2012. hal-00693334v1

**HAL Id: hal-00693334**

**<https://hal.science/hal-00693334v1>**

Preprint submitted on 2 May 2012 (v1), last revised 6 Jan 2017 (v3)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# SIEVING IN GRAPHS AND EXPLICIT BOUNDS FOR NON-TYPICAL ELEMENTS

---

FLORENT JOUVE\*    JEAN-SÉBASTIEN SERENI†

May 2, 2012

ABSTRACT. — We study properties of random graphs within families of graphs equipped with a group law. The group structure enables one to perform a random walk on the family of graphs. If the generating system is a big enough random subset of graphs, a result of Alon–Roichman provides us with useful expansion properties well suited to give quantitative estimates for the rarefaction of non-typical elements attained by the random walk. Applying the general setting we show, e.g., that, with high probability (in a strong explicit sense), random graphs contain cycles of small length, or that a random coloring of the edges of a graph contains a monochromatic triangle.

## INTRODUCTION

The relevance of using families of expander graphs for studying objects or solving problems coming from a broad variety of mathematical areas has been emphasized in numerous ways in the recent years. Notably the combination of sieving arguments together with expansion properties has proved particularly efficient. Let us mention the groundbreaking work [4] where the mix of such techniques enabled the authors to detect almost primes in a variety of non-Abelian situations (a striking example being the study of almost prime curvatures of Apollonian circle packings). A different kind of sieve together with the same expansion properties have also been exploited in the context of group theory [11], or to obtain quantitative results in the probabilistic Galois theory of arithmetic groups [7]. In the sieving processes used in the aforementioned works, one is naturally led to a crucial step where some *spectral gap* property is needed. A tautological reinterpretation of expansion of a certain family of graphs provides one with the needed spectral gap.

The present paper follows the same kind of strategy, the goal being this time to study properties of graphs themselves. The starting point is a result of Alon–Roichman [3] according to which a family of random Cayley graphs forms a “good” family of expanders. There are several natural approaches to produce “random” elements. The one we use consists in performing a random walk on the family of graphs studied, (cf. also [7]). Another approach could be to quantify the proportion of elements satisfying an expected property among a finite subset of the family of graphs considered. For the applications we have in mind this question would in fact be much easier. As a matter of fact we do need to quantify proportions of “good” elements as part of our sieving process.

The paper is organized in the following way: Section 1 explains the general setup and makes precise the way in which we want to use Alon–Roichman’s result. In that section we also state and prove the main theoretical result needed for the applications. It can be seen as a combinatorial variation on one of the key proposition in Kowalski’s book [8]. The rest of the paper is devoted to applications of the main result of Section 1. While the first one is an explicit incarnation of what can be seen as probabilistic Ramsey theory, the second one gives an explicit bound on the probability that a random subgraph of the grid  $\mathbf{Z}^2$  contains a cycle of length 4. We conclude with remarks on further questions that may be of interest and that can be successfully investigated via our method. We notably state another Ramsey type result (together with a sketch of proof) obtained by suitably adapting the arguments used in the second application.

---

\*Université Paris-Sud, Laboratoire de Mathématique, UMR 8628, Orsay, 91405 France. E-mail: Florent.Jouve@math.u-psud.fr.

†CNRS (LIAFA, Université Diderot), Paris, France. E-mail: sereni@kam.mff.cuni.cz. This author’s work was partially supported by the French *Agence Nationale de la Recherche* under reference ANR 10 JCJC 0204 01.

**Notation.** If  $X$  is a finite set, then  $\#X$  and  $|X|$  synonymously denote the cardinality of  $X$ .

If  $X$  is a finite graph, then  $\text{Adj}(X)$  is the adjacency operator sending a  $\mathbf{C}$ -valued function on the vertices of  $X$  to the function  $(x \mapsto \sum_y f(y))$ , where the sum is over the neighbors  $y$  of the vertex  $x$ . If  $X$  is moreover  $d$ -regular (that is, every vertex of  $X$  has degree  $d$ ), then the *normalized adjacency operator* is  $\frac{1}{d} \cdot \text{Adj}(X)$ .

If  $G$  is a group and  $S \subset G$ , then  $X(G, S)$  is the Cayley graph on  $G$  with edge set  $S \cup S^{-1} := \{s \in G : s \in S \text{ or } s^{-1} \in S\}$ . If  $G$  is a finite Abelian group, then  $\hat{G}$  is the character group of  $G$ . If  $x \geq 0$  is a real number, then  $\lceil x \rceil$  and  $\lfloor x \rfloor$  are the least integer greater than or equal to  $x$  and the greatest integer smaller than or equal to  $x$ , respectively. If  $R$  is a positive integer, then  $[R]$  is the set  $\{1, \dots, R\}$ . Given a probability space  $(\Omega, \Sigma, \mathbf{P})$  and two events  $A$  and  $B$  such that  $\mathbf{P}(B) \neq 0$ , we let  $\mathbf{P}(A | B)$  be the *conditional probability*  $\mathbf{P}(A \cap B) / \mathbf{P}(B)$ .

## 1. THE GENERAL SETTING

### 1.1. CAYLEY GRAPHS ON QUOTIENTS

Let  $G$  be a group (in this section, the group law is noted multiplicatively) and  $\Lambda \subset \mathbf{N}$  be a *bounded* set of indices. We suppose we are given a family  $(H_\ell)_{\ell \in \Lambda}$  of normal subgroups of  $G$  such that for each  $\ell$  the index  $n_\ell := [G : H_\ell]$  is finite. We let  $\rho_\ell : G \rightarrow G/H_\ell$  be the canonical projection.

We fix once and for all a probability space  $(\Omega, \Sigma, \mathbf{P})$  and an arbitrarily small real number  $\delta \in (0, 1)$ . For each  $\ell \in \Lambda$ , we define the quantity

$$\kappa(b_\ell, \ell; \delta) := \left\lceil 2((2 - \delta) \ln(2 - \delta) + \delta \ln \delta)^{-1} \cdot \left( \ln \left( \sum_{\rho \in \text{Irr}(G/H_\ell)} \dim \rho \right) + b_\ell + \ln 2 \right) \right\rceil,$$

where  $b := (b_\ell)$  is a parameter (a sequence of positive real numbers) and  $\text{Irr}(G/H_\ell)$  is a set of representatives for the isomorphism classes of irreducible representations of  $G/H_\ell$ .

Now let  $s_1^{(\ell)}, \dots, s_{\kappa(b_\ell, \ell; \delta)}^{(\ell)}$  be independent identically distributed random variables taking values in  $G/H_\ell$ . We assume that the common distribution of these random variables is the uniform distribution on  $G/H_\ell$ . We are interested in the properties of the Cayley graphs on the groups  $G/H_\ell$  with edges corresponding to the values taken by the random variables  $s_i^{(\ell)}$  for  $i \in \{1, \dots, \kappa(b_\ell, \ell; \delta)\}$ . These graphs are  $\kappa(b_\ell, \ell; \delta)$ -regular graphs. Throughout the paper, if  $X$  is a  $k$ -regular graph, then the *eigenvalues of  $X$*  are the eigenvalues of the normalized adjacency operator  $k^{-1} \text{Adj}(X)$ . The *spectral gap*  $\varepsilon(X)$  of  $X$  is defined to be  $\max\{1 - |\lambda| : \lambda \text{ is an eigenvalue of } X \text{ not in } \{-1, 1\}\}$  (recall that the eigenvalue  $-1$  occurs if and only if  $X$  is bipartite). Let  $\gamma$  be a real number satisfying  $0 < \gamma \leq 1/2$ , then  $X$  is a  $\gamma$ -*expander graph* if its spectral gap is at least  $\gamma$ . In particular, note that a  $k$ -regular graph with spectral gap greater than  $1/2$  is a  $\gamma$ -expander graph for any  $\gamma \in (0, 1/2]$ .

The reason for introducing the above setup is a theorem of Alon & Roichman [3, Th. 1], which has been subsequently improved by Landau & Russell [9, Th. 2] and Loh & Schulman [10, Th. 1]. The last improvement obtained so far, which is the version we state and use, is due to Christofides & Markström [5, Th. 5].

**THEOREM 1.1** (Christofides–Markström). — *With notation as above, fix an index  $\ell$  in  $\Lambda$ . For every  $\delta \in (0, 1/2]$ , the probability that  $X(G/H_\ell, \{s_1^{(\ell)}, \dots, s_{\kappa(b_\ell, \ell; \delta)}^{(\ell)}\})$  is not a  $\delta$ -expander graph is less than  $e^{-b_\ell}$ .*

The statement can be rephrased by saying it is highly probable that the Cayley graph  $X(G/H_\ell, \{s_1^{(\ell)}, \dots, s_{\kappa(b_\ell, \ell; \delta)}^{(\ell)}\})$  be a  $\delta$ -expander graph, the counterpart being that the edge set has very large cardinality. We pause here to note that the definition of an expander graph we use is not completely equivalent to the usual definition. However, it is a standard fact that the (usual) expansion property and the spectral gap property are closely related notions. Indeed, let  $X = (V, E)$  be an undirected finite graph. For every  $A \subset V$ , let  $\partial A$  be the set of edges joining an element of  $A$  to an element of the complement of  $A$  in  $V$ . The *expansion ratio* (or *edge expansion ratio*) of  $X$  is

$$h(X) := \min_{\substack{A \subset V \\ 1 \leq \#A \leq \#V/2}} \frac{\#\partial A}{\#A}.$$

The spectral gap and the expansion ratio  $h(X)$  of an undirected connected  $k$ -regular graph  $X$  are related by Cheeger's inequalities (see, e.g., [6, Theorem 1.2.3]).

In general, it is natural to ask for how to combine two expander Cayley graphs into a new one. The natural idea consisting in taking the cartesian product of the two groups involved and hoping that there is a suitable choice of edges ensuring expansion of the graph obtained, fails in general (see [1] for a much more sophisticated method that does produce expander “product Cayley graphs”).

However, for the particular case we have in mind in the present paper, the simple construction described in the following technical lemma is enough.

LEMMA 1.2. — *With notation as above assume that  $X(G, S)$  and  $X(H, T)$  are  $\delta$ -expander Cayley graphs on finite Abelian groups  $G$  and  $H$  (with edge set defined by  $S \subset G$  and  $T \subset H$ , respectively). Then for every  $(x_0, y_0) \in G \times H$  with  $x_0^2 = 1 = y_0^2$ , the Cayley graph  $X(G \times H, (S \times \{y_0\}) \cup (\{x_0\} \times T))$  is a  $((1 + \gamma)^{-1}\delta)$ -expander graph, where*

$$\gamma := \max \left\{ \frac{|S \cup S^{-1}|}{|T \cup T^{-1}|}, \frac{|T \cup T^{-1}|}{|S \cup S^{-1}|} \right\}.$$

*Proof.* For convenience, we set  $Y := (S \times \{y_0\}) \cup (\{x_0\} \times T)$ ,  $S^* := S \cup S^{-1}$ ,  $T^* := T \cup T^{-1}$  and  $Y^* := Y \cup Y^{-1}$ . The eigenfunctions of the normalized adjacency operator on  $X(G \times H, Y)$  are of the form

$$(\chi, \tau): (g, h) \mapsto \chi(g)\tau(h),$$

for characters  $\chi \in \hat{G}$  and  $\tau \in \hat{H}$ . The corresponding eigenvalues are of the form

$$\lambda_{\chi, \tau} := \frac{1}{|S^*| + |T^*|} \sum_{(g, h) \in Y^*} \chi(g)\tau(h).$$

Since both  $x_0$  and  $y_0$  have order 2, the sum splits as follows:

$$(|S^*| + |T^*|) \lambda_{\chi, \tau} = \tau(y_0) \sum_{g \in S^*} \chi(g) + \chi(x_0) \sum_{h \in T^*} \tau(h).$$

We deduce:

$$|\lambda_{\chi, \tau}| \leq \frac{|S^*|}{|S^*| + |T^*|} \left| \frac{1}{|S^*|} \sum_{g \in S^*} \chi(g) \right| + \frac{|T^*|}{|S^*| + |T^*|} \left| \frac{1}{|T^*|} \sum_{h \in T^*} \tau(h) \right|.$$

If both  $\chi$  and  $\tau$  are non-trivial, then  $|\lambda_{\chi, \tau}| \leq 1 - \delta$ . If  $\chi$  is trivial and  $\tau$  is non trivial, we obtain instead

$$|\lambda_{\chi, \tau}| \leq 1 - \delta (1 + |S^*|/|T^*|)^{-1},$$

hence the result by symmetry of the roles played by  $G$  and  $H$ . □

The family  $(\rho_\ell)_{\ell \in \Lambda}$  of surjections is *linearly disjoint* if for any choice of two distinct indices  $\ell$  and  $\ell'$  in  $\Lambda$ , the product map

$$\rho_{\ell, \ell'} := \rho_\ell \times \rho_{\ell'} : G \rightarrow G/H_\ell \times G/H_{\ell'}$$

is surjective.

The random walks on  $G$  we want to consider are obtained by lifting the sets  $\{s_1^{(\ell)}, \dots, s_{\kappa(b_\ell, \ell; \delta)}^{(\ell)}\}$  (and their “inverses” so that all the graphs considered are then undirected) to  $G$ . To that purpose define the random variable

$$S_\ell(b_\ell, \delta) := \{s_1^{(\ell)}, \dots, s_{\kappa(b_\ell, \ell; \delta)}^{(\ell)}\} \cup \{(s_1^{(\ell)})^{-1}, \dots, (s_{\kappa(b_\ell, \ell; \delta)}^{(\ell)})^{-1}\},$$

which takes values in the set of subsets of  $G/H_\ell$ . For each  $\ell$  and each  $1 \leq m \leq \kappa(b_\ell, \ell; \delta)$ , we choose further a representative  $\tilde{s}_m^{(\ell)} \in G$  of  $s_m^{(\ell)}$ . We set

$$\tilde{S}_\ell(b, \delta) := \{\tilde{s}_1^{(\ell)}, \dots, \tilde{s}_{\kappa(b_\ell, \ell; \delta)}^{(\ell)}\} \cup \{(\tilde{s}_1^{(\ell)})^{-1}, \dots, (\tilde{s}_{\kappa(b_\ell, \ell; \delta)}^{(\ell)})^{-1}\}.$$

The subset of  $G$  we use to perform a random walk on  $G$  is

$$S(b, \delta) := \{1\} \cup \bigcup_{\ell \in \Lambda} \tilde{S}_\ell(b_\ell, \delta).$$

In this last definition  $S(b, \delta)$  is not seen as a random variable but as the union of  $\{1\}$  with the union over  $\Lambda$  of the value taken at some  $\omega \in \Omega$  by  $\tilde{S}(b, \delta)$ . In other words we fix once and for all an element  $\omega$  of  $\Omega$ ; picking an element of  $S(b, \delta)$  amounts to picking 1 or an element of some  $\tilde{S}_\ell(b_\ell, \delta)(\omega)$ .

Note that  $S(b, \delta)$  is assumed to contain 1: this is to avoid issues with bipartite graphs. Since  $\Lambda$  is assumed to be bounded,  $S(b, \delta)$  is a finite set. It also satisfies the obvious property

$$\forall \ell \in \Lambda, \quad \rho_\ell(S(b, \delta)) \supset S_\ell(b_\ell, \delta).$$

However, to ensure  $\delta$ -expansion of the Cayley graphs  $X(G/H_\ell, \rho_\ell(S(b, \delta)))$  we need more. This is the reason why we suppose the following condition (we call the *nice lifting condition*) holds:

$$\text{(nice lifting)} \quad \forall \ell \in \Lambda, \quad \rho_\ell(S(b, \delta)) = S_\ell(b_\ell, \delta) \cup \{1\}.$$

Before making precise how we define the random walk we are interested in we define one more condition our setting will have to fulfill: if  $f$  and  $g$  are two surjective functions defined on a set  $X$  and  $S$  is a distinguished subset of  $X$ , the product function  $f \times g : x \mapsto (f(x), g(x))$  is said to have *nice  $S$ -image* if

$$\text{(nice  $S$ -image)} \quad \exists (x_0, y_0) \in f(X) \times g(X), \quad x_0^2 = 1 = y_0^2 \quad \text{and} \quad f \times g(S) \supseteq (f(S) \times \{y_0\}) \cup (\{x_0\} \times g(S)).$$

Note that the inclusion  $f \times g(S) \subset f(S) \times g(S)$  always holds.

The three aforementioned properties, that is, linear disjointness, nice lifting and nice  $S(b, \delta)$ -image, can be all viewed as surjectivity statements.

## 1.2. THE RANDOM WALK

With notation as above, we perform the following (left-invariant) random walk on  $G$ . It is defined the same way as in [8, Chap. 7].

$$\begin{cases} X_0 = g_0 \\ X_{k+1} = X_k \xi_{k+1} \end{cases} \quad \text{for } k \geq 0,$$

where  $g_0$  is a fixed element in  $G$  and the steps  $\xi_k$  are independent, identically distributed random variables with distribution

$$\mathbf{P}(\xi_k = s) = \mathbf{P}(\xi_k = s^{-1}) = p_s = p_{s^{-1}}$$

for every  $k$  and every  $s \in S(b, \delta)$ , and where  $(p_s)_s$  is a finite sequence of positive real numbers indexed by  $S(b, \delta)$  such that

$$\sum_{s \in S(b, \delta)} p_s = 1.$$

Of course the random walk depends on the parameters  $b = (b_\ell)_\ell$  and  $\delta$ . What might be the most natural such random walk is the one defined by uniformly distributing the steps, that is,  $p_s := \#S(b, \delta)^{-1}$  for every  $s \in S(b, \delta)$ .

By studying the properties of the random walk  $(X_k)_k$  our aim is to describe the behavior of a “generic element”  $g \in G$ . To do so, we make use of Kowalski’s abstract large sieve procedure extensively described, together with applications, in his book [8]. As in every sieve method, one can only handle cases where the typical properties at issue can be detected locally. To be more precise we fix for each  $\ell \in \Lambda$ , a conjugacy invariant subset  $\Theta_\ell \subset G/H_\ell$ . The probability we want to upper bound is

$$\mathbf{P}(\forall \ell \in \Lambda, \rho_\ell(X_k) \notin \Theta_\ell).$$

In applications we will produce effective upper bounds for the probability with which  $X_k$  satisfies a fixed property that can be detected by the condition  $\rho_\ell(X_k) \notin \Theta_\ell$  for some  $\Theta_\ell \subset G/H_\ell$ . The abstract sieve statement we will rely on is the following. We refer the reader to the book by Kowalski for a (self-contained) sieve statement written in greater generality [8, Prop. 3.5], as well as for more information on the random walk sieve used here [8, Chap. 7].

PROPOSITION 1.3. — *With notation as above let us assume  $G$  is Abelian and:*

- *the family of surjections  $(\rho_\ell)$  is linearly disjoint;*

- the nice lifting condition holds; and
- the nice  $S(b, \delta)$ -image condition (with respect to any pair  $(\rho_\ell, \rho_{\ell'})$  with  $\ell \neq \ell'$  in  $\Lambda$ ) holds.

Define the constant

$$C_0 := \max_{\ell \neq \ell' \in \Lambda} \gamma_{\ell, \ell'} := \max_{\ell \neq \ell' \in \Lambda} \frac{\#S_\ell(b_\ell, \delta)}{\#S_{\ell'}(b_{\ell'}, \delta)},$$

which is a finite number since  $\Lambda$  is a finite set. Then there exists  $\eta > 0$  such that

$$\mathbf{P}(\rho_\ell(X_k) \notin \Theta_\ell, \forall \ell \in \Lambda_{L_1, L_2}) \leq \sum_{\ell=\lceil L_1 \rceil}^{\lfloor L_2 \rfloor} e^{-b_\ell} + (1 + (L_2 - L_1) |G_{L_2}|^{3/2} \exp(-\eta k)) \left( \sum_{\ell=\lceil L_1 \rceil}^{\lfloor L_2 \rfloor} \frac{\#\Theta_\ell}{n_\ell} \right)^{-1},$$

where the constant  $\eta$  depends only on  $\delta$ ,  $C_0$ , the set  $S(b, \delta)$  and the distribution of the steps  $\xi_j$ , and where  $(L_1, L_2)$  is any fixed couple of real numbers such that  $\Lambda \cap [L_1, L_2] = \{\lceil L_1 \rceil, \dots, \lfloor L_2 \rfloor\}$ .

Before starting the proof we define one last piece of useful notation: for indices  $\ell$  and  $\ell'$  in  $\Lambda$ , we set  $G_{\ell, \ell'} := G/H_\ell \times G/H_{\ell'}$  if  $\ell \neq \ell'$  and  $G_{\ell, \ell'} := G/H_\ell$ . If  $\ell = \ell'$ , the surjection  $\rho_{\ell, \ell'} : G \rightarrow G_{\ell, \ell'}$  is nothing but the quotient map  $\rho_\ell$ . The proof of the proposition follows closely that of [8, Prop. 7.2]. However, as our framework is quite different from that of *loc. cit.* and for the sake of completeness, we give the full detail of the proof.

*Proof of Proposition 1.3.* We set  $\Lambda_{L_1, L_2} := \Lambda \cap [L_1, L_2]$ . Fix a real number  $\delta$  in  $(0, 1/2)$  and let us split the probability we are interested in:

$$\begin{aligned} \mathbf{P}(\forall \ell \in \Lambda_{L_1, L_2}, \rho_\ell(X_k) \notin \Theta_\ell) &\leq \mathbf{P}(\exists \ell \in \Lambda_{L_1, L_2}, X(G/H_\ell, \rho_\ell(S(b, \delta))) \text{ is not a } \delta\text{-expander}) \\ &\quad + \mathbf{P}(\forall \ell \in \Lambda_{L_1, L_2}, X(G/H_\ell, \rho_\ell(S(b, \delta))) \text{ is a } \delta\text{-expander and } \rho_\ell(X_k) \notin \Theta_\ell). \end{aligned} \quad (1)$$

As we shall see, the second summand on the right side admits a theoretical upper bound that is amenable to sieve. Moreover, the first summand can be efficiently bounded by invoking Theorem 1.1. Indeed, since  $\rho_\ell(S(b, \delta)) = S_\ell(b_\ell, \delta) \cup \{1\}$  by the nice lifting condition, we can easily show that the following statement holds (note that the statement would be trivial for if we were only interested in edge-expansion):

$$\mathbf{P}(\exists \ell \in \Lambda_{L_1, L_2}, X(G/H_\ell, \rho_\ell(S(b, \delta))) \text{ is not a } \delta\text{-expander}) \leq \mathbf{P}(\exists \ell \in \Lambda_{L_1, L_2}, X(G/H_\ell, S_\ell(b_\ell, \delta)) \text{ is not a } \delta\text{-expander}).$$

This inequality is a consequence of the following result.

LEMMA 1.4. — *Let  $G_0$  be an Abelian group and let  $S$  be a subset of  $G$ . If  $X(G_0, S)$  is a  $\delta$ -expander graph, then so is  $X(G_0, S \cup \{1\})$ .*

*Proof of Lemma 1.4.* This is trivially true if  $1 \in S$ , so from now on we assume that  $1 \notin S$ . Set  $S^* := S \cup S^{-1}$ .

Let  $\lambda$  be an eigenvalue of  $X(G_0, S)$  corresponding to a non trivial character  $\chi$  of  $G$ , i.e.  $\lambda = (\#S^*)^{-1} \sum_{s \in S^*} \chi(s)$ . Using the usual convention according to which a loop contributes 2 to the degree of a vertex, we deduce that the corresponding eigenvalue  $\lambda'$  of  $X(G_0, S \cup \{1\})$  is

$$\frac{1}{2 + \#S^*} \left( \sum_{s \in S^*} \chi(s) + \chi(1) \right) = \frac{\#S^*}{2 + \#S^*} \lambda + \frac{1}{2 + \#S^*} = \lambda + \frac{1 - 2\lambda}{2 + \#S^*}.$$

Of course  $\lambda' \leq \lambda$  provided  $\lambda \geq 1/2$ . Moreover, if  $\lambda < 1/2$  then  $\lambda' < 1/2$ . Thus in both cases  $\lambda' \leq 1 - \delta$ . This finishes the proof of Lemma 1.4.  $\square$

Although we assume  $G$  to be Abelian, the major part of the rest of the proof of Proposition 1.3 would work in a non-Abelian setting. To emphasize this feature of the proof we prefer using the general terminology of representation theory of finite groups rather than the character theory of finite Abelian groups.

Applying Theorem 1.1 yields that

$$\mathbf{P}(\exists \ell \in \Lambda_{L_1, L_2}, X(G/H_\ell, S_\ell(b_\ell, \delta)) \text{ is not a } \delta\text{-expander}) \leq \sum_{\ell \in \Lambda_{L_1, L_2}} e^{-b_\ell}.$$

Let us now turn to the second summand of the right side of (1). First, notice that

$$\begin{aligned} & \mathbf{P}(\forall \ell \in \Lambda_{L_1, L_2}, X(G/H_\ell, \rho_\ell(S(b, \delta))) \text{ is a } \delta\text{-expander and } \rho_\ell(X_k) \notin \Theta_\ell) \\ & \leq \mathbf{P}(\forall \ell \in \Lambda_{L_1, L_2}, \rho_\ell(X_k) \notin \Theta_\ell \mid \forall \ell \in \Lambda_{L_1, L_2}, X(G/H_\ell, \rho_\ell(S(b, \delta))) \text{ is a } \delta\text{-expander}). \end{aligned}$$

This last probability is amenable to sieve.

We fix (non-necessarily distinct) indices  $\ell$  and  $\ell'$  in  $\Lambda_{L_1, L_2}$  and a complex representation (with representation space  $V$ ):

$$\pi : G \xrightarrow{\rho_{\ell, \ell'}} G_{\ell, \ell'} \rightarrow GL(V),$$

factoring through  $G_{\ell, \ell'}$  that has no nonzero  $G_{\ell, \ell'}$ -invariant vector (seen as  $G_{\ell, \ell'}$ -representations,  $\pi$  and 1 are orthogonal). Since  $G_{\ell, \ell'}$  is a finite group we may assume without loss of generality that  $\pi$  gives rise to a unitary representation of  $G_{\ell, \ell'}$  (i.e. the representation space  $V$  may be equipped with a  $G_{\ell, \ell'}$ -invariant scalar product written  $\langle ; \rangle$ ).

First step: we assert that there exists a constant  $\eta > 0$  depending only on  $C_0$ ,  $\delta$ , the set  $S(b, \delta)$  and the distribution of the steps  $\xi_j$ , such that for any two vectors  $e, f \in V$

$$|\langle \mathbf{E}(\pi(X_k))e; f \rangle| \leq \|e\| \cdot \|f\| \cdot \exp(-\eta k),$$

where  $\|x\|^2 := \langle x; x \rangle$  for any vector  $x \in V$ .

Consider

$$M := \mathbf{E}(\pi(\xi_k)) = \sum_{s \in S(b, \delta)} p(s) \pi(s),$$

which is a well-defined element of  $\text{End}(V)$  since the series defining  $M$  converges absolutely (because  $\pi$  is a unitary representation and  $\sum_s p(s) = 1$ ). From  $M$ , we can then define two other elements of  $\text{End}(V)$ :

$$M^+ := \text{Id} - M \quad \text{and} \quad M^- := \text{Id} + M.$$

Note that these formulæ define two operators which are both independent of  $k$  and self-adjoint. Indeed, the set  $S(b, \delta)$  as well as the distribution of the  $\xi_k$  are symmetric; moreover the mapping sending an operator to its adjoint is linear and continuous. We also need to define

$$N_0 := \mathbf{E}(\pi(X_0)) = \sum_{t \in T} \mathbf{P}(X_0 = t) \pi(t) \in \text{End}(V),$$

where  $T$  is a fixed (finite) subset of  $G$  containing the starting point  $g_0$  of the random walk  $(X_k)$ . (For simplicity one can assume that  $T = \{g_0\}$ .)

The random variables  $X_0$  and  $\xi_k$  being independent, it follows that for  $k \geq 1$ ,

$$\mathbf{E}(\pi(X_k)) = N_0 M^k.$$

Thus, by linearity,

$$\mathbf{E}(\langle \pi(X_k)e; f \rangle) = \langle M^k e; N_0^* f \rangle,$$

where  $N_0^*$  is the adjoint of  $N_0$ .

As  $\sum_{s \in S(b, \delta)} p(s) = 1$  and since for every  $s \in S(b, \delta)$ ,  $\pi(s)$  is a unitary operator, the eigenvalues of  $M$  are in the interval  $[-1, 1]$ . Now, let  $\rho$  be the spectral radius of  $M$ , that is

$$\rho := \max\{|\gamma| : \gamma \text{ is an eigenvalue of } M\}.$$

Then

$$\left| \langle M^k e; N_0^* f \rangle \right| \leq \|e\| \cdot \|f\| \cdot \rho^k,$$

since the norm of  $N_0$  is smaller than 1.

We need to exhibit a positive real number  $\nu$  independent of  $i$  and  $\pi$  such that  $0 \leq \rho \leq 1 - \nu$ . We will then be able to set  $\eta := -\log(1 - \nu) > 0$ . We use the fact that  $\rho = \max\{\rho^+, \rho^-\}$ , where  $\rho^+$  and  $\rho^-$  are real numbers equal to

the greatest positive eigenvalue of  $M$  and the opposite of the smallest negative eigenvalue of  $M$ , respectively. It is enough to prove that  $\rho^\pm < 1 - v_\pm$  for some constants  $v_\pm$  which are independent of  $i$  and  $\pi$ . To that purpose, we use the variational interpretation for the eigenvalues of a self-adjoint operator on a finite dimensional Hilbert space. Indeed  $1 - \rho^\pm$ , which is the smallest eigenvalue of  $M^\pm$ , is equal to

$$\min_{v \neq 0} \frac{\langle \Psi v; v \rangle}{\|v\|^2},$$

where  $\Psi := M^\pm$ . Thus, we compute

$$\begin{aligned} \frac{\langle M^+ v; v \rangle}{\|v\|^2} &= \frac{1}{2} \sum_{s \in S(b, \delta)} p_s \frac{\|\pi(s)v - v\|^2}{\|v\|^2} \\ &\geq \frac{p_0^+}{2} \inf_{\varpi} \inf_{v \neq 0} \max_{s \in \rho_{\ell, \ell'}(S(b, \delta))} \frac{\|\varpi(s)v - v\|^2}{\|v\|^2}, \end{aligned}$$

where  $p_0^+ := \min_{s \in S(b, \delta)} p(s) > 0$  and  $\varpi$  runs over the representations of  $G_{\ell, \ell'}$  without any nonzero invariant vector. Now combining the nice  $S(b, \delta)$ -image condition and the nice lifting condition one has

$$\max_{s \in \rho_{\ell, \ell'}(S(b, \delta))} \frac{\|\varpi(s)v - v\|^2}{\|v\|^2} \geq \max_{s \in S_\ell(b_\ell, \delta) \times \{b\} \cup \{a\} \times S_{\ell'}(b_{\ell'}, \delta)} \frac{\|\varpi(s)v - v\|^2}{\|v\|^2}.$$

The Cayley graphs  $(X(G/H_\ell, S_\ell(b_\ell, \delta)))_{\ell \in \Lambda}$  are assumed to be  $\delta$ -expander graphs. Hence using Lemma 1.2 we deduce that  $X(G_{\ell, \ell'}, S_\ell(b_\ell, \delta) \times \{b\} \cup \{a\} \times S_{\ell'}(b_{\ell'}, \delta))$  is a  $((1 + C_0)^{-1} \cdot \delta)$ -expander Cayley graph. Thus

$$\inf_{\varpi} \inf_{v \neq 0} \max_{s \in \rho_{\ell, \ell'}(S(b, \delta))} \frac{\|\varpi(s)v - v\|^2}{\|v\|^2} > (1 + C_0)^{-1} \cdot \delta.$$

The constant  $v^+ := 2\delta(1 + C_0)^{-1} / p_0^+$  satisfies the required conditions.

To determine  $v^-$ , we use the fact that there exists a relation of odd length  $c$  among the elements of  $S(b, \delta)$  (we may even set  $c := 1$  since  $1 \in S(b, \delta)$ ). Therefore for any  $v \in V$ ,

$$v = \frac{1}{2} \left( (v + \pi(s_1)v) - (\pi(s_1)v + \pi(s_1 s_2)v) + \cdots + (\pi(s_1 \cdots s_{c-1})v + \pi(1)v) \right).$$

Then, invoking Cauchy–Schwarz's inequality and using the  $G_{\ell, \ell'}$ -invariance of the inner product,

$$\|v\|^2 \leq \frac{c}{4} \sum_{i=0}^{c-1} \|\pi(r_i)v + \pi(r_i s_{i+1})v\|^2 \leq \frac{c}{4} \sum_{i=0}^{c-1} \|v + \pi(s_{i+1})v\|^2,$$

where  $r_0 := 1$  and  $r_i := s_1 \cdots s_i$  for  $i \geq 1$ . In particular, we deduce that

$$\|v\|^2 \leq \frac{c}{4} \left( \min_{1 \leq i \leq c} \frac{1}{p(s_i)} \right) \sum_{i=0}^{c-1} p(s_{i+1}) \|v + \pi(s_{i+1})v\|^2.$$

Then, taking into account the possible repetitions of generators in the sequence  $(s_1, \dots, s_c)$ ,

$$\|v\|^2 \leq \frac{c^2}{4} \frac{1}{\min \{p(s_i) : 1 \leq i \leq c\}} \sum_{s \in S} p(s) \|\pi(s)v + v\|^2 \leq \frac{c^2}{2} \left( \min \{p(s_i) : 1 \leq i \leq c\} \right)^{-1} \langle M^- v; v \rangle.$$

Therefore we can choose  $v^- = \frac{2}{c^2} \min \{p(s_i) : 1 \leq i \leq c\} > 0$ .

**Second step:** we apply the inequality obtained in the first step to the special case where  $e = f$  is a vector of an orthonormal basis of  $V$ . Summing up over the elements of such a basis we obtain, with notation as above,

$$|\mathbf{E}(\text{Tr} \pi(X_k))| \leq \exp(-\eta k) (\dim \pi).$$

Now from Kowalski's large sieve inequality [8, Prop. 3.7] we obtain

$$\mathbf{P}(\forall \ell \in \Lambda_{L_1, L_2}, \rho_\ell(X_k) \notin \Theta_\ell \mid \forall \ell \in \Lambda_{L_1, L_2} X(G/H_\ell, \rho_\ell(S(b, \delta))) \text{ is a } \delta\text{-expander}) \\ \leq \Delta(X_k; L_1, L_2) \left( \sum_{L_1 \leq \ell \leq L_2} \frac{\#\Theta_\ell}{n_\ell} \right)^{-1},$$

where one has the theoretical upper bound:

$$\Delta(X_k; L_1, L_2) \leq \max_{\ell \in \Lambda_{L_1, L_2}} \max_{\pi \in \mathcal{B}_\ell^*} \sum_{\ell' \in \Lambda_{L_1, L_2}} \sum_{\tau \in \mathcal{B}_{\ell'}^*} |W(\pi, \tau)|,$$

with

$$W(\pi, \tau) := \mathbf{E}(\mathrm{Tr}[\pi, \bar{\tau}] \rho_{\ell, \ell'}(X_k)).$$

Here for any  $\ell \in \Lambda$  we let  $\mathcal{B}_\ell$  be a set of representatives containing 1 for the isomorphism classes of irreducible representations of  $G/H_\ell$ . We set further  $\mathcal{B}_\ell^* := \mathcal{B}_\ell \setminus \{1\}$ . Finally if  $\pi$  (resp.  $\tau$ ) is a representation of a group  $G_1$  (resp.  $G_2$ ) we let  $[\pi, \tau]$  be the ‘‘external’’ tensor product representation  $\pi \otimes \tau$  of  $G \times H$  if  $G \neq H$  or the ‘‘internal’’ tensor product representation  $\pi \otimes \tau$  of  $G$  otherwise.

In our setting we have, using [8, Lemma 3.4],

$$[\pi, \bar{\tau}] \rho_{\ell, \ell'} = \delta((\ell, \pi), (\ell', \tau)) 1 + [\pi, \bar{\tau}]_0 \rho_{\ell, \ell'},$$

where  $\delta(\cdot, \cdot)$  is the Kronecker symbol and  $[\pi, \bar{\tau}]_0$  is the component of  $[\pi, \bar{\tau}]$  orthogonal to 1. Thus applying the first step to each of the representations  $[\pi, \bar{\tau}]_0 \rho_{\ell, \ell'}$ , we obtain

$$|\mathbf{E}(\mathrm{Tr}[\pi, \bar{\tau}]_0 \rho_{\ell, \ell'}(X_k))| \leq (\dim \pi)(\dim \tau) \exp(-\eta k).$$

Using the trivial bounds

$$\sum_{\rho \in \mathrm{Irr}(G)} \leq |G| \quad \text{and} \quad \max_{\rho \in \mathrm{Irr}(G)} \dim \rho \leq \sqrt{|G|},$$

and putting everything together we obtain as wished:

$$\mathbf{P}(\forall \ell \in \Lambda_{L_1, L_2}, \rho_\ell(X_k) \notin \Theta_\ell \mid \forall \ell \in \Lambda_{L_1, L_2} X(G/H_\ell, \rho_\ell(S(b, \delta))) \text{ is a } \delta\text{-expander}) \\ \leq (1 + (L_2 - L_1) \cdot |G_{L_2}|^{3/2} \exp(-k\eta)) \left( \sum_{L_1 \leq \ell \leq L_2} \frac{\#\Theta_\ell}{n_\ell} \right)^{-1}.$$

□

## 2. ORDER & DISORDER: MONOCHROMATIC STRUCTURES

We now turn to an application of Proposition 1.3.

### 2.1. SIEVING FOR MONOCHROMATIC SUBSTRUCTURES

We let  $\mathcal{G}$  be the (countable) infinite complete graph, that is, the graph with vertex set  $\mathbf{N}$  in which every two distinct positive integers are neighbors. We fix an integer  $c \geq 3$  and we define  $\mathcal{C}$  to be the collection of all functions from the edges of  $\mathcal{G}$  to  $\mathbf{Z}/c\mathbf{Z}$ . For every function  $f$ , the *support* of  $f$  is the set of all elements  $e$  in the domain of  $f$  such that  $f(e) \neq 0$ . For each integer  $R \geq 3$ , let  $t(R)$  be an integer greater than  $3R$ . Define  $\mathcal{C}^R$  to be the family of all functions  $f \in \mathcal{C}$  whose support is contained in  $[t(R)]^2$ .

The set  $\mathcal{C}$  can be naturally endowed with a group structure inherited from that of  $\mathbf{Z}/c\mathbf{Z}$ . The addition of two elements  $f$  and  $g$  of  $\mathcal{C}$  is formally defined by

$$f + g: \quad \begin{array}{ccc} E(\mathcal{G}) & \longrightarrow & \mathbf{Z}/c\mathbf{Z} \\ e & \longmapsto & f(e) + g(e). \end{array}$$

The neutral element is the function that is identically 0. Note that the addition trivially restricts to each set  $\mathcal{C}^R$ , naturally yielding a 1-parameter family of subgroups of  $\mathcal{C}$ .

We are interested in monochromatic substructures of a given fixed size  $k$  that may arise. Specifically, to avoid unnecessary notation and abstraction, we shall focus on finding monochromatic triangles (though our strategy could be adapted effortlessly to the question of detecting monochromatic  $r$ -cycles for  $r \geq 3$ ).

From now on, we fix an integer  $R$  at least 3. Next we define a family of subgroups  $(H_\ell)_{\ell \in \Lambda}$  of  $\mathcal{C}$ , where  $\Lambda := [R]$ . Consider a partition  $(I_\ell)_{\ell \in \Lambda}$  of  $[t(R)]$ . We set  $i(\ell) := |I_\ell|$  for  $\ell \in \Lambda$ . Let  $E_\ell := \{(a, b) \in I_\ell^2 : a \neq b\}$ , that is,  $E_\ell$  is the set of all edges of  $\mathcal{G}$  with both endvertices contained in  $I_\ell$ . We define  $C_\ell$  to be the collection of all functions  $f \in \mathcal{C}^R$  with support contained in  $E_\ell$ . Then  $H_\ell$  is the collection of all functions  $f \in \mathcal{C}^R$  such that  $f|_{E_\ell} \equiv 0$ .

The following properties of the quotients  $\mathcal{C}_\ell := \mathcal{C}^R / H_\ell$  are immediate but crucial from our point of view.

LEMMA 2.1. — *The following holds.*

1. For each  $\ell \in \Lambda$ ,

- (a)  $C_\ell$  is a set of representatives of the quotient  $\mathcal{C}_\ell$ , and
- (b) the index of  $H_\ell$  in  $\mathcal{C}^R$  is  $n_\ell := [\mathcal{C}^R : H_\ell] = |C_\ell| = c^{i(\ell)(i(\ell)-1)/2}$ .

2. The family  $(\rho_\ell)_{\ell \in \Lambda}$  is linearly disjoint.

*Proof.* 1.(a) No two distinct functions in  $C_\ell$  are congruent modulo an element of  $H_\ell$ . Moreover, for any  $f \in \mathcal{C}^R$ , let  $f_C$  be the function equal to  $f$  on  $E_\ell$  and equal to 0 everywhere else, that is,  $f_C|_{E_\ell} := f|_{E_\ell}$  and  $f_C|(E(\mathcal{G}) \setminus E_\ell) := 0$ . By construction  $f_C \in C_\ell$  and  $f - f_C \in H_\ell$ , or equivalently  $f \equiv f_C \pmod{H_\ell}$ .

1.(b) By the definition,  $|E_\ell| = i(\ell)(i(\ell) - 1)/2$ . The conclusion follows.

2. Fix two distinct integers  $\ell$  and  $\ell'$  in  $\Lambda$ , and a couple  $(f_\ell, f_{\ell'}) \in \mathcal{C}_\ell \times \mathcal{C}_{\ell'}$ . By 1.(a) we can choose representatives  $\tilde{f}_\ell$  and  $\tilde{f}_{\ell'}$  of  $f_\ell$  and  $f_{\ell'}$  in  $C_\ell$  and  $C_{\ell'}$ , respectively. Since  $E_\ell$  and  $E_{\ell'}$  are disjoint (because  $\ell \neq \ell'$ ), the function  $f : E(\mathcal{G}) \rightarrow \mathbf{Z}/c\mathbf{Z}$  with support contained in  $E_\ell \cup E_{\ell'}$  such that  $f|_{E_\ell} = \tilde{f}_\ell$  and  $f|_{E_{\ell'}} = \tilde{f}_{\ell'}$  is well defined and satisfies  $\rho_\ell(f) = f_\ell$  and  $\rho_{\ell'}(f) = f_{\ell'}$ .  $\square$

A practical way to rephrase part of the proof of Lemma 2.1 is to say that for each fixed integer  $\ell$  in  $\Lambda$  and each element  $f$  of  $\mathcal{C}^R$ , the unique element in  $C_\ell$  congruent to  $f$  modulo  $H_\ell$  is the function equal to 0 on  $E_\ell$  and to  $f$  outside of  $E_\ell$ .

## 2.2. LOOKING FOR MONOCHROMATIC TRIANGLES

From now on, we assume that  $i(\ell) \geq 3$  for  $\ell \in \Lambda$ . (This is possible since  $t(R) \geq 3R$ .) For each integer  $\ell \in \Lambda$ , let  $\Theta_\ell$  be the set of classes  $\tilde{f} \in \mathcal{C}_\ell$  such that the unique representative  $f$  of  $\tilde{f}$  in  $C_\ell$  (the existence of which is asserted by Lemma 2.1) contains a monochromatic triangle in  $E_\ell$ . In other words  $f \in \Theta_\ell$  if and only if  $I_\ell$  contains three integers  $i_1, i_2$  and  $i_3$  such that  $f((i_1, i_2)) = f((i_1, i_3)) = f((i_2, i_3))$ . Observe that  $|\Theta_\ell|/|\mathcal{C}_\ell| = c^{-2}$ . Indeed any function that restricts to a constant map (with values in  $\mathbf{Z}/c\mathbf{Z}$ ) on a fixed triangle contained in  $E_\ell$  surjects to an element of  $\Theta_\ell$  via  $\rho_\ell$ .

Assume that  $\delta$  is a fixed real number in  $(0, 1/2]$ . We set  $b_\ell := \ell$ . In particular, note that

$$\kappa(b_\ell, \ell; \delta) = \left[ 2((2-\delta)\ln(2-\delta) + \delta\ln\delta)^{-1} \cdot \left( \frac{i(\ell)(i(\ell)-1)\ln c}{2} + \ell + \ln 2 \right) \right].$$

Given  $f^{(\ell)} \in S_\ell(b_\ell, \delta)$ , we define  $\tilde{f}^{(\ell)}$  to be its canonical representative in  $\mathcal{C}^R$ , that is,  $\tilde{f}^{(\ell)} \in C_\ell$ .

THEOREM 2.2. — *Let  $(X_k)$  be a random walk on  $\mathcal{C}^R$  defined as in Subsection 1.2 using  $S(b, \delta)$ . Set  $v^- := 2p(1)$  and  $v^+ := 2\delta / \min\{p(s) : s \in S(b, \delta)\}$ . Let  $\eta > 0$  be such that  $1 - \exp(-\eta) = \min\{v^-, v^+\}$ . Then, for each positive integer  $k$  and each integer  $L_1 \in [R/2]$ ,*

$$\mathbf{P}(X_k \text{ does not contain a monochromatic triangle}) \leq \frac{c^2 + 1}{L_1} + c^{(3/4) \cdot i(2L_1)(i(2L_1)-1)+2} \exp(-\eta k).$$

*Proof.* Fix a positive integer  $k$ . Lemma 2.1 ensures that the system  $(\rho_\ell)_{\ell \in \Lambda}$  is linearly disjoint. Moreover, the choices of the canonical representative  $\bar{s}^{(\ell)}$  imply that for every  $\ell \in \Lambda$ , the surjection  $\rho_\ell$  satisfies the nice-lifting condition and  $(\rho_\ell, \rho'_\ell)$  has nice  $S(b, \delta)$ -image (with respect to  $(x_0, y_0) = (0, 0)$ ) for each  $\ell' \in \Lambda \setminus \{\ell\}$ . These are direct consequences of the fact that  $E_\ell \cap E_{\ell'} = \emptyset$  if  $\ell \neq \ell'$ .

Let  $\eta$  be the positive constant given by Proposition 1.3. Letting  $L_1 \in \llbracket R/2 \rrbracket$  and setting  $L_2 := 2 \cdot L_1$ , we are guaranteed that  $\Lambda \cap [L_1, L_2] = \{L_1, \dots, L_2\}$ . Therefore we obtain, applying Proposition 1.3,

$$\begin{aligned} \mathbf{P}(\rho_\ell(X_k) \notin \Theta_\ell, \forall \ell \in \Lambda_{L_1, L_2}) &\leq \sum_{\ell=L_1}^{L_2} e^{-b_\ell} + (1 + (L_2 - L_1) |\mathcal{C}_{L_2}|^{3/2} \exp(-\eta k)) \left( \sum_{\ell=L_1}^{L_2} \frac{\#\Theta_\ell}{n_\ell} \right)^{-1} \\ &= e^{1-L_1} - e^{-2L_1} + (1 + L_1 \cdot c^{(3/2) \cdot i(2L_1)(i(2L_1)-1)/2} \exp(-\eta k)) \cdot \frac{c^2}{L_1} \\ &\leq e^{1-L_1} - e^{-2L_1} + \frac{c^2}{L_1} + c^{(3/4) \cdot i(2L_1)(i(2L_1)-1)+2} \exp(-\eta k) \\ &\leq \frac{1}{L_1} + \frac{c^2}{L_1} + c^{(3/4) \cdot i(2L_1)(i(2L_1)-1)+2} \exp(-\eta k), \end{aligned}$$

where we used that  $e^{1-x} - e^{-2x} \leq 1/x$  for  $x \geq 1$ . □

Different choices of sets  $I_\ell$  may correspond to different speed of rarefaction of non-typical structures. More precisely, one can put additional constraints on the structure of the monochromatic triangles, e.g. the three vertices must be consecutive integers as in Corollary 2.3. In addition, we give in Corollary 2.4 another specification of the sets  $I_\ell$ , which allows for a larger domain of validity. The price to pay is a slower speed of convergence and less constraints put on the monochromatic triangles.

COROLLARY 2.3. — *With notation as in Theorem 2.2,*

$$\forall k \geq 1, \quad \eta \cdot k \leq \ln(R/2) - 1 \Rightarrow \mathbf{P}(X_k \text{ does not contain a monochromatic triangle}) \leq (c^{13/2} + c^2 + 1) \exp(-\eta k).$$

*Proof.* Set  $I_\ell := \{3\ell - 2, 3\ell - 1, 3\ell\}$  for each  $\ell \in \Lambda$ . In particular  $i(\ell)(i(\ell) - 1) = 6$ . Let  $k$  be a positive integer such that  $\eta k \leq \ln(R/2) - 1$ . If we set  $L_1 := \lceil \exp(\eta k) \rceil$  and  $L_2 := 2L_1$ , then  $L_1 \leq \lfloor R/2 \rfloor$ . Therefore, Theorem 2.2 implies that

$$\begin{aligned} \mathbf{P}(X_k \text{ does not contain a monochromatic triangle}) &\leq \frac{c^2 + 1}{L_1} + c^{13/2} \cdot \exp(-\eta k) \\ &= (c^{13/2} + c^2 + 1) \exp(-\eta k). \end{aligned}$$

□

COROLLARY 2.4. — *With notation as in Theorem 2.2,*

$$\forall k \geq 1, \quad \eta \cdot k \leq (4R - 4)^2 \ln c \Rightarrow \mathbf{P}(X_k \text{ does not contain a monochromatic triangle}) \leq \frac{8(c^8 + c^2 + 1)\sqrt{\ln c}}{\sqrt{\eta k}}.$$

*Proof.* Set  $I_\ell := \left\{ \frac{\ell(\ell+1)}{2}, \dots, \frac{\ell(\ell+1)}{2} + \ell \right\}$ . In particular  $i(\ell) = \ell + 1$  for each  $\ell \in \Lambda$ . Let  $k$  be a positive integer such that  $\eta k \leq (4R - 4)^2 \ln c$ . If we set  $L_1 := \lceil \sqrt{\eta k / (64 \ln c)} \rceil$  and  $L_2 := 2L_1$ , then  $L_1 \leq R/2$ . Consequently, Theorem 2.2 implies that

$$\begin{aligned} \mathbf{P}(X_k \text{ does not contain a monochromatic triangle}) &\leq \frac{c^2 + 1}{L_1} + c^{3L_1(2L_1+1)/2+2} \cdot \exp(-\eta k) \\ &\leq \frac{c^2 + 1}{L_1} + \frac{c^8}{L_1} \\ &\leq \frac{(c^8 + c^2 + 1)8\sqrt{\ln c}}{\sqrt{\eta k}}, \end{aligned}$$

where we used that  $\exp(-\eta k) \leq c^{-64(L_1-1)^2}$  and  $L_1 \cdot c^{3 \cdot L_1^2 + 3 \cdot L_1/2 + 2 - 64(L_1-1)^2}$  is upper bounded by  $c^8$  for every  $c \geq 3$  and  $L_1 \geq 1$ .  $\square$

Note that in the two corollaries the upper bound is non trivial only if  $R$  is big compared to the number of colors  $c$ . This condition is not restrictive since  $c$  and  $R$  vary independently and since no restriction on the size of  $R$  is needed.

It is natural to compare these last two statements with what we know from Ramsey theory. We postpone this discussion to Section 4.

### 3. RANDOM SUBGRAPHS OF THE 2-DIMENSIONAL GRID

We now turn to another application of Proposition 1.3.

#### 3.1. SIEVING IN THE 2-DIMENSIONAL GRID

We let  $\mathcal{G}$  be the infinite 2-dimensional grid, that is, the graph with vertex set  $\mathbf{Z}^2$  in which  $(a, b)$  and  $(c, d)$  are neighbors if and only if  $|a - c| + |b - d| = 1$ . For each positive integer  $R$ , we consider the family  $\mathcal{G}^R$  of all spanning subgraphs of  $\mathcal{G}$  whose edges are contained in  $\{-2R - 2, \dots, 2R + 2\}^2$ . In other words, a graph in  $\mathcal{G}^R$  has vertex set  $\mathbf{Z}^2$  and two vertices  $u = (a, b)$  and  $v = (c, d)$  are neighbors only if  $(a, b, c, d) \in \{-2R - 2, \dots, 2R + 2\}^4$  and  $u$  and  $v$  are neighbors in  $\mathcal{G}$ .

The family  $G$  of all spanning subgraphs of the grid  $\mathcal{G}$  may be endowed with an Abelian group structure: indeed the symmetric difference  $\Delta$  is a binary associative composition law on  $G$  and the identity element is the graph with vertex set  $\mathbf{Z}^2$  and no edge. Note that  $\Delta$  trivially restricts to each set  $\mathcal{G}^R$ , naturally yielding a 1-parameter family of subgroups of  $G$ . Note further that every non trivial element of  $\mathcal{G}$  (and in particular of  $\mathcal{G}^R$ ) has order 2.

From now on, we fix a positive integer  $R$ . Next we define a family of subgroups  $(H_\ell)_{\ell \in \Lambda}$  of  $G$ , where  $\Lambda := [R]$ . For each  $\ell \in \Lambda$ , we define  $C_\ell$  to be the collection of all spanning subgraphs of  $\mathcal{G}$  with edges contained in the annulus  $\mathbf{D}(0, 2\ell + 2) \setminus \mathbf{D}(0, 2\ell)$ . (Here  $\mathbf{D}(a, r)$  is the open disc in  $\mathbf{R}^2$  with center  $a$  and radius  $r$  and with respect to the  $\|\cdot\|_1$  norm—in other words, an edge  $\{(a, b), (c, d)\}$  of  $\mathbf{Z}^2$  belongs to  $\mathbf{D}(0, \ell)$  if and only if  $\{a, b, c, d\} \subseteq \{-\ell, \dots, \ell\}$ .) Then for  $\ell \in \Lambda$  we define  $H_\ell$  to be the “complement” of  $C_\ell$  in the following sense: the elements of  $H_\ell$  are the graphs with vertex set  $\mathbf{Z}^2$  and with no edge included in  $\mathbf{D}(0, 2\ell + 2) \setminus \mathbf{D}(0, 2\ell)$ .

In this setting one has the following analogue of Lemma 2.1, where  $G_\ell$  is still the quotient  $G/H_\ell$ .

LEMMA 3.1. — *The following holds.*

1. For each  $\ell \in \Lambda$ ,

- (a)  $C_\ell$  is a set of representatives for the quotient  $G_\ell$ , and
- (b) the index of  $H_\ell$  in  $G$  is  $n_\ell := [G : H_\ell] = |C_\ell| = 2^{64\ell + 40}$ .

2. The family  $(\rho_\ell)_{\ell \in \Lambda}$  is linearly disjoint.

*Proof.* 1.(a) No two distinct graphs in  $C_\ell$  are congruent modulo an element of  $H_\ell$ . Moreover, for any  $g \in G$ , let  $g_C$  be the graph with vertex set  $\mathbf{Z}^2$  and edge set obtained by deleting all the edges of  $g$  that are not contained in the annulus  $\mathbf{D}(0, 2\ell + 2) \setminus \mathbf{D}(0, 2\ell)$ . By construction  $g_C \in C_\ell$  and its complement  $g_H$  in  $G$  is an element of  $H_\ell$  satisfying  $g = g_C \Delta g_H$ . In other words,  $g \equiv g_C \pmod{H_\ell}$ .

1.(b) By the definition, the subgraph of  $\mathcal{G}^R$  contained in  $\mathbf{D}(0, \ell)$  contains precisely  $4\ell(2\ell + 1)$  edges. Therefore, the subgraph of  $\mathcal{G}^R$  contained in  $\mathbf{D}(0, 2\ell + 2) \setminus \mathbf{D}(0, 2\ell)$  contains precisely  $64\ell + 40$  edges. The conclusion follows.

2. Fix two distinct integers  $\ell$  and  $\ell'$  in  $\Lambda$ , and a couple  $(g_\ell, g_{\ell'}) \in G_\ell \times G_{\ell'}$ . By 1.(a) we can choose representatives  $\tilde{g}_\ell$  and  $\tilde{g}_{\ell'}$  of  $g_\ell$  and  $g_{\ell'}$  in  $C_\ell$  and  $C_{\ell'}$ , respectively. Since  $C_\ell$  and  $C_{\ell'}$  are disjoint (because  $\ell \neq \ell'$ ), the graph  $g$  obtained by taking the union of the edges of  $\tilde{g}_\ell$  and  $\tilde{g}_{\ell'}$  (and still having vertex set  $\mathbf{Z}^2$ ) satisfies  $\rho_\ell(g) = g_\ell$  and  $\rho_{\ell'}(g) = g_{\ell'}$ .  $\square$

One also has an interpretation of Lemma 3.1 analogous to the one given for Lemma 2.1. For each fixed integer  $\ell \in \Lambda$  and each element  $g \in G$ , the unique element in  $C_\ell$  congruent to  $g$  modulo  $H_\ell$  is  $g \cap C_\ell$  (the intersection being taken edgewise).

### 3.2. LOOKING FOR 4-CYCLES

For each integer  $\ell \in \Lambda$ , let  $\Theta_\ell$  be the set of every class  $\bar{g} \in G_\ell$  such that the unique representative of  $\bar{g}$  in  $C_\ell$  (the existence of which is asserted by Lemma 3.1) contains a 4-cycle. Observe that  $|\Theta_\ell|/|G_\ell| \geq 2^{-4}$ , since every graph of  $C_\ell$  that contains a fixed 4-cycle reduces to an element of  $\Theta_\ell$  modulo  $H_\ell$ .

Suppose that  $\delta$  is a fixed real number in  $(0, 1)$ . We set  $b_\ell := \ell$ . In particular, note that

$$\kappa(b_\ell, \ell; \delta) = \lceil 2((2-\delta)\ln(2-\delta) + \delta\ln\delta)^{-1} \cdot ((64\ell + 41)\ln 2 + \ell) \rceil.$$

Given  $s^{(\ell)} \in S_\ell(b_\ell, \delta)$ , we define  $\bar{s}^{(\ell)}$  to be its representative in  $C_\ell$  (see 1(b) of Lemma 3.1), that is,  $\bar{s}^{(\ell)}$  has no edge outside  $\mathbf{D}(0, 2\ell + 2) \setminus \mathbf{D}(0, 2\ell)$ .

**THEOREM 3.2.** — *Let  $(X_k)$  be a random walk on  $\mathcal{G}^R$  defined as in Subsection 1.2 using  $S(b, \delta)$ . Set  $v^- := 2p(1)$  and  $v^+ := 2\delta/\min\{p(s) : s \in S(b, \delta)\}$ . Let  $\eta > 0$  be such that  $1 - \exp(-\eta) = \min\{v^-, v^+\}$ . Then,*

$$\forall k \geq 1, \quad \eta \cdot k \leq 75R - 149 \Rightarrow \mathbf{P}(X_k \text{ does not contain a 4-cycle}) \leq \frac{2551}{\eta k}.$$

*Proof.* Fix a positive integer  $k$ . Lemma 3.1 ensures that the system  $(\rho_\ell)_{\ell \in \Lambda}$  is linearly disjoint. Since we have chosen the  $\bar{s}_i^{(\ell)}$  in  $C_\ell$ , the canonical surjection  $\rho_\ell$  satisfies the nice-lifting condition for each  $\ell \in \Lambda$ . Moreover  $(\rho_\ell, \rho_{\ell'})$  has a nice  $S(b, \delta)$ -image (with respect to  $(x_0, y_0) = (1, 1)$ ) for every couple of distinct elements  $\ell$  and  $\ell'$  in  $\Lambda$ .

Let  $\eta$  be the positive constant given by Proposition 1.3. We may assume that  $\eta k \geq 2551$ , since otherwise the statement of the theorem trivially holds. Setting  $L_1 := \lceil \eta k / 150 \rceil$  and  $L_2 := 2L_1$ , we are guaranteed that  $\Lambda \cap [L_1, L_2] = \{L_1, \dots, L_2\}$  since  $\eta k \leq 75R - 149$ . Therefore we obtain, applying Proposition 1.3,

$$\begin{aligned} \mathbf{P}(\rho_\ell(X_k) \notin \Theta_\ell, \forall \ell \in \Lambda_{L_1, L_2}) &\leq \sum_{\ell=L_1}^{L_2} e^{-b_\ell} + (1 + (L_2 - L_1) |G_{L_2}|^{3/2} \exp(-\eta k)) \left( \sum_{\ell=L_1}^{L_2} \frac{\#\Theta_\ell}{n_\ell} \right)^{-1} \\ &\leq e^{1-L_1} - e^{-2L_1} + (1 + L_1 \cdot 2^{192L_1+60} \exp(-\eta k)) \cdot \frac{2^4}{L_1} \\ &\leq \frac{150}{\eta k} + \frac{2^4 \cdot 150}{\eta k} + \frac{1}{\eta k} \\ &\leq \frac{2551}{\eta k}, \end{aligned}$$

where we used that  $e^{1-x} - e^{-2x} \leq 1/x$  if  $x > 0$  and  $2^{192 \cdot (x/150+1)+64} \exp(-x) \leq 1/x$  if  $x \geq 2551$ .  $\square$

In a similar way as in Section 2 one could look, more generally, for cycles of length  $r \geq 4$  in the graph obtained after  $k$  steps of the random walk are performed. Our setting could be easily adapted to this more general case. For simplicity we have chosen to give the detail of the argument only in the case where  $r$  is 4.

### 4. REMARKS AND FURTHER APPLICATIONS

Let us underline some peculiarities of the applications proposed in Sections 2 and 3. First, concerning the subgraphs of the infinite grid, we note that while it is elementary to estimate the expected number of 4-cycles in a subgraph chosen uniformly at random in a given finite 2-dimensional grid, our notion of randomness relies instead on the consideration of arbitrary words in the alphabet corresponding to a particular generating system (with respect to the group structure considered). Our point in Sections 2 and 3 is to give, for this more intricate notion of randomness, explicit upper bounds for probabilities that we expect to be small.

Second, for monochromatic substructures, it follows from Ramsey's theorem [12] that for every fixed positive integer  $c$ , there exists an integer  $N$  such that if  $n \geq N$ , then every  $c$ -coloring of the edges of the complete graph  $K_n$  on  $n$  vertices contains a monochromatic triangle. Alon and Rödl [2] established that the smallest such  $N$  is  $\Theta(3^c)$  as  $n$  tends to infinity (that is, there exist two constants  $\rho$  and  $\rho'$  such that for sufficiently large  $n$ , this value belongs to  $[\rho \cdot 3^c, \rho' \cdot 3^c]$ ). In our setting, although the infinite complete graph is involved, only finite subgraphs of it are checked

for the existence of monochromatic triangles. These subgraphs are not necessarily large enough for Ramsey's theorem to apply. In addition, we only consider monochromatic triangles with vertices contained in some prescribed set  $I_\ell$ .

Another feature of the application developed in Section 2 is uniformity with respect to the number  $c$  of colors involved. No such uniformity holds in the context of Ramsey theory. Indeed, as already mentioned, Alon and Rödl's theorem [2] asserts that the number of required vertices for Ramsey's theorem to hold grows exponentially fast with  $c$ .

We also note that a strategy similar to that used in Section 2 allows one to check for monochromatic arithmetic progressions for which the length, the common difference and the "shape", are prescribed. Fix positive integers  $s$  (the desired length of the arithmetic progression),  $q$  (the desired common difference), and  $c \geq 3$  (the number of colors). Further, let  $R$  be an integer greater than  $s$ . Set  $\Lambda := [R]$  and  $t(R) := R + q(2s - 1)$ . Similarly as before, let  $\mathcal{C}^R$  be the group of all  $c$ -colorings of  $[t(R)]$ . We consider the partition  $(I_\ell)_{\ell \in \Lambda}$  of  $[t(R)]$ , where  $I_\ell := \{\ell + q \cdot j : 0 \leq j \leq 2s - 1\}$  for each  $\ell \in \Lambda$ . (It is the choice of a particular partition that provides a control on the "shape" of the arithmetic progressions to be found.) In this setting our method yields the following result.

**THEOREM 4.1.** — *Let  $(X_k)$  be a random walk on  $\mathcal{C}^R$  defined as in Subsection 1.2 using  $S(b, \delta)$ . Set  $v^- := 2p(1)$  and  $v^+ := 2\delta / \min\{p(s) : s \in S(b, \delta)\}$ . Let  $\eta > 0$  be such that  $1 - \exp(-\eta) = \min\{v^-, v^+\}$ . For all  $k \geq 1$  such that  $\eta \cdot k \leq \ln(R/2) - 1$ ,*

$$\mathbf{P}(\text{In } X_k, \text{ no monochromatic arithmetic progression of length } s \text{ is contained in } I_\ell, \forall \ell \in \Lambda) \leq (c^{4s} + c^s + 1) \exp(-\eta k).$$

Let us sketch the proof. For each  $\ell \in \Lambda$ , let  $H_\ell$  be the set of all functions  $f : [t(R)] \rightarrow [c]$  such that  $f|_{I_\ell} \equiv 0$ . The index in  $\mathcal{C}^R$  of each of these subgroups is  $c^{2s}$ . Moreover, there is a collection of natural representatives for the classes modulo  $H_\ell$ , namely the functions the support of which is contained in  $I_\ell$ . Letting  $\Theta_\ell$  be the set of classes modulo  $H_\ell$  whose unique representative — in the aforementioned system of natural representatives — contains a monochromatic arithmetic progression of length  $s$  that is contained in  $I_\ell$ , it holds that  $|\Theta_\ell|/n_\ell \geq c^{-s}$ .

Now, similarly as before, Proposition 1.3 can be applied and yields a positive constant  $\eta$ . Setting  $L_1 := \lceil \exp(\eta k) \rceil$  and  $L_2 := 2L_1$ , one deduces Theorem 4.1.

We conclude by pointing out the following: van der Waerden's theorem [13] ensures that, for each fixed positive integers  $s$  and  $c \geq 3$ , there exists an integer  $N$  such that if  $n \geq N$  then any  $c$ -coloring of  $[n]$  yields a monochromatic arithmetic progression of length  $s$ . In the above setting, we impose two additional conditions: the common difference of the arithmetic progression and a constraint on its form: it must be contained in one of the sets  $I_\ell$ . Thus, van der Waerden's theorem does not guarantee the existence of such an arithmetic progression (even for large values of  $t(R)$ ) and the aforementioned inequality is essentially an explicit lower bound on the speed of rarefaction of the colorings that do not yield a monochromatic arithmetic progression with the required properties. Furthermore, and as mentioned in the remarks about Section 2, the uniformity of our estimate with respect to the number of colors  $c$  is a quite interesting by-product of our approach.

## REFERENCES

- [1] N. ALON, A. LUBOTZKY, AND A. WIGDERSON, *Semi-direct product in groups and zig-zag product in graphs: connections and applications (extended abstract)*, in 42nd IEEE Symposium on Foundations of Computer Science (Las Vegas, NV, 2001), IEEE Computer Soc., Los Alamitos, CA, 2001, pp. 630–637.
- [2] N. ALON AND V. RÖDL, *Sharp bounds for some multicolor Ramsey numbers*, *Combinatorica*, 25 (2005), pp. 125–141.
- [3] N. ALON AND Y. ROICHMAN, *Random Cayley graphs and expanders*, *Random Structures Algorithms*, 5 (1994), pp. 271–284.
- [4] J. BOURGAIN, A. GAMBURD, AND P. SARNAK, *Affine linear sieve, expanders, and sum-product*, *Invent. Math.*, 179 (2010), pp. 559–644.
- [5] D. CHRISTOFIDES AND K. MARKSTRÖM, *Expansion properties of random Cayley graphs and vertex transitive graphs via matrix martingales*, *Random Structures Algorithms*, 32 (2008), pp. 88–100.
- [6] G. DAVIDOFF, P. SARNAK, AND A. VALETTE, *Elementary number theory, group theory, and Ramanujan graphs*, vol. 55 of London Mathematical Society Student Texts, Cambridge University Press, Cambridge, 2003.

- [7] F. JOUVE, E. KOWALSKI, AND D. ZYWINA, *Splitting fields of characteristic polynomials of random elements in arithmetic groups*, forthcoming, Israel J. Math.
- [8] E. KOWALSKI, *The large sieve and its applications*, vol. 175 of Cambridge Tracts in Mathematics, Cambridge University Press, Cambridge, 2008. Arithmetic geometry, random walks and discrete groups.
- [9] Z. LANDAU AND A. RUSSELL, *Random Cayley graphs are expanders: a simple proof of the Alon-Roichman theorem*, Electron. J. Combin., 11 (2004), pp. Research Paper 62, 6.
- [10] P.-S. LOH AND L. J. SCHULMAN, *Improved expansion of random Cayley graphs*, Discrete Math. Theor. Comput. Sci., 6 (2004), pp. 523–528 (electronic).
- [11] A. LUBOTZKY AND C. MEIRI, *Sieve methods in group theory I: Powers in linear groups*, available, arXiv:1107.3666, (2011).
- [12] F. P. RAMSEY, *On a problem of formal logic*, Proc. London Math. Soc. Series, 2-30 (1930), pp. 264–286.
- [13] B. L. VAN DER WAERDEN, *Beweis einer Baudetschen Vermutung*, Nieuw Archief, 15 (1927), pp. 212–216.