Sieving in graphs and explicit bounds for non-typical elements

Florent Jouve, Jean-Sébastien Sereni

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

FLORENT JOUVE† JEAN-SÉBASTIEN SERENI‡

May 16, 2014

ABSTRACT. — We study properties of random graphs within families of graphs equipped with a group law. Using the group structure we 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 from which we deduce 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 colouring of the edges of a graph contains a monochromatic triangle. We also explain how our method gives results towards an effective infinite Ramsey Theorem.

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 [3] 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 [10] and to obtain quantitative results concerning the probabilistic Galois theory of arithmetic groups [6, 11]. 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 properties 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 [2] 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 [6, 11]). 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 several of the applications we have in mind this question would be much easier. As a matter of fact we do need to quantify proportions of "good" elements as part of our sieving process. However our setting is more general. Indeed by carefully adapting Kowalski's random walk sieve [7, Chap. 7] our sieving procedure is capable of handling infinite structures. In that case it is less clear how our approach could be compared to the one consisting in the estimation of the proportion of good elements in a given structure. As such, there are settings where our approach produces results for which there does not seem to be obvious analogues in the standard point of view.

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 [7]. The rest of the paper is devoted to applications of the main result of Section 1. Our first application, being

*This work was partially supported by the French *Agence Nationale de la Recherche* under reference ANR 10 JCJC 0204 01.

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

‡CNRS (LORIA), Vandœuvre-lès-Nancy, France. E-mail: sereni@kam.mff.cuni.cz.

mainly an introductory example to illustrate how to set up the random walk and ensure the required properties, provides an explicit bound on the probability that a random subgraph of the grid $\mathbf{Z}^2$ contains a cycle of length 4. We then present a series of applications inspired by (finite and infinite) Ramsey theory, forming an explicit incarnation of what can be seen as probabilistic Ramsey theory. We conclude with remarks on further questions that may be of interest and that may be successfully investigated using our method. We notably state another Ramsey type result (together with a sketch of proof) obtained by suitably adapting the arguments developed in Section 3.

Notation. If X is a finite set, then $\#X$ and $|X|$ synonymously denote the cardinality of X. If X is a finite graph, then $\mathrm{Adj}(X)$ is the adjacency operator mapping 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 neighbours 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 $\frac{1}{d} \cdot \mathrm{Adj}(X)$.

If G is a group and $S \subseteq G$, then $X(G,S)$ is the Cayley graph on G with edge set $S \cup S^{-1} := \left\{s \in G : s \in S \text{ or } s^{-1} \in S\right\}$. If G is a finite Abelian group, then $\hat{G}$ is the character group of G. If x is a non-negative 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 $\mathbf{P}(A \mid B)$ 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 (non necessarily finite) set of indices. We suppose we are given a family $(H_\ell)_{\ell\in\Lambda}$ of normal subgroups of G such that for each ℓ the index $n_\ell := [G : H_\ell]$ is finite. We set $G_\ell := G/H_\ell$ and we let $\rho_\ell \colon G \to G_\ell$ be the canonical projection.

We fix once and for all a probability space $(\Omega,\Sigma,\mathbf{P})$ and an arbitrarily small real number $\delta \in (0\,,1)$. Set

$$\psi(\delta) := 2\left((2-\delta)\ln(2-\delta) + \delta\ln\delta\right)^{-1}. \tag{1}$$

For each $\ell \in \Lambda$, we define the quantity

$$\kappa(b_\ell,\ell;\delta) := \left\lceil \psi(\delta)\cdot\Big(\ln\big(\sum_{\rho\in\mathrm{Irr}(G/H_\ell)} \dim\rho\big) + b_\ell + \ln 2\Big)\right\rceil,$$

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

Now let $s_1^{(\ell)},\cdots,s_{\kappa(b_\ell,\ell;\delta)}^{(\ell)}$ be independent identically distributed random variables taking values in G/H_ℓ. We assume that the common distribution of these random variables is the uniform distribution on G/H_ℓ. We are interested in the properties of the Cayley graphs on the groups G/H_ℓ 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 and possibly have multiple edges.

Throughout the paper, if X is a k-regular graph, then the *eigenvalues of* X are the eigenvalues of the normalized adjacency operator $k^{-1}\mathrm{Adj}(X)$. An eigenvalue λ is *trivial* if $|\lambda| = 1$. The *spectral gap* $\varepsilon(X)$ of X is defined to be $\min\left\{1-|\lambda| : \lambda \text{ is a non-trivial eigenvalue of } X\right\}$ (recall that the eigenvalue -1 occurs if and only if X is bipartite). We adopt the following definition for an expander graph, which slightly differs from the standard one.

Definition 1. Let γ be a real number satisfying $0 < \gamma \leqslant 1/2$. A k-regular graph X is a γ-*expander graph* if the spectral gap of X is at least γ.

In particular, note that a k-regular graph with spectral gap greater than $1/2$ is a γ-expander graph for any $\gamma \in (0\,,1/2]$.

The reason for introducing the above setup is a theorem of Alon & Roichman [2, Th. 1], which has been subsequently improved by Landau & Russell [8, Th. 2] and Loh & Schulman [9, Th. 1]. The latest improvement obtained, which is the version we state and use, is due to Christofides & Markström [4, Th. 5].

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

Because of Theorem 1.1 and the definition of expansion we use, the symbol δ will always denote in the sequel a fixed real number in $(0\,,1/2]$.

Theorem 1.1 can be rephrased by saying it is highly probable that the Cayley graph $X(G/H_\ell,\{s_1^{(\ell)},\cdots,s_{\kappa(b_\ell,\ell;\delta)}^{(\ell)}\})$ be a δ-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 ∂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

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

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., [5, Theorem 1.2.3]).

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

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

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

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

To perform a random walk on G one can choose the subset

$$S(b,\delta) := \bigoplus_{\ell\in\Lambda}\tilde{S}_\ell(b_\ell,\delta), \tag{2}$$

where for two subsets A_1, A_2 of G we define $A_1\oplus A_2 := \{a_1+a_2 : (a_1,a_2)\in A_1\times A_2\}$.

However it seems more natural to allow some summands $\tilde{S}_\ell(b_\ell,\delta)$ not to be taken into account while randomly choosing a particular step of the random walk. Thus the choice

$$S(b,\delta) := \bigoplus_{\ell\in\Lambda}\left(\tilde{S}_\ell(b_\ell,\delta)\cup\{1\}\right), \tag{3}$$

seems closer to the intuitive idea of how the random walk should be defined.

As far as the expansion properties of the Cayley graphs considered are concerned, either choice works, as the following lemma shows.

LEMMA 1.2. — *Let G_0 be an Abelian group and let S be a subset of G_0. If $X(G_0,S)$ is a δ-expander graph, then so is $X(G_0,S\cup\{1\})$.*

Proof of Lemma 1.2. The statement is trivially true if $1\in S$, so we assume that $1\notin S$. Set $S^* := S\cup S^{-1}$ and $s^* := \#S^*$. Recall that Definition 1 implies that $\delta\in(0\,,1/2]$. To prove the statement, it suffices to show that every non-trivial eigenvalue λ' of $X(G_0,S\cup\{1\})$ is such that $|\lambda'|\leqslant 1/2$ or $|\lambda'|\leqslant|\lambda|$ for some non-trivial eigenvalue λ of $X(G_0,S)$.

Let λ' be a non-trivial eigenvalue of $X(G_0,S\cup\{1\})$. Using the usual convention according to which a loop contributes 2 to the degree of a vertex, we deduce that $\lambda'=(2+s^*)^{-1}(\sum_{s\in S^*}\chi(s)+\chi(1))$ for some non-trivial character χ of G_0. Therefore,

$$\lambda' = \frac{s^*}{2+s^*}\lambda+\frac{1}{2+s^*} = \lambda+\frac{1-2\lambda}{2+s^*},$$

where $\lambda := (s^*)^{-1}\sum_{s\in S^*}\chi(s)$ is a non-trivial eigenvalue of $X(G_0,S)$.

Consequently, it is enough to prove that if $|\lambda'|>1/2$, then $|\lambda'|\leqslant|\lambda|$. Suppose, on the contrary, that $|\lambda'|>1/2$ and $|\lambda'|>|\lambda|$. Then $\lambda'>0$. Indeed, otherwise $\lambda\leqslant -1/s^*<0$ and hence $-\lambda+\frac{2\lambda-1}{2+s^*}>|\lambda|=-\lambda$ implies that $\lambda>1/2$, a contradiction.

Hence $\lambda'>1/2$ and thus $\lambda>1/2$. However, this implies that $\frac{1-2\lambda}{2+s^*}<0$, so that $\lambda>\lambda'=|\lambda'|$, contrary to our assumption. This finishes the proof of Lemma 1.2. □

Let us emphasize here that $S(b,\delta)$ is not seen as a random variable but as the union over Λ of the value taken at some $\omega \in \Omega$ by $\tilde{S}_\ell(b,\delta)$ (to which we may adjoin 1 if we choose $S(b,\delta)$ as in (3)). In other words we fix once and for all an element ω of Ω; picking an element of $S(b,\delta)$ amounts to picking a sum over ℓ of elements in $\tilde{S}_\ell(b_\ell,\delta)(\omega)$ (or $\tilde{S}_\ell(b_\ell,\delta)(\omega) \cup \{1\}$). This set also satisfies the obvious property that for every $\ell \in \Lambda$,

$$\rho_\ell(S(b,\delta)) \supset \begin{cases} S_\ell(b_\ell,\delta) & \text{in case (2),} \\ S_\ell(b_\ell,\delta) \cup \{1\} & \text{in case (3).} \end{cases}$$

For the purpose of the present work more is required. We say that the family $(\rho_\ell)_{\ell\in\Lambda}$ of surjections is $S(b,\delta)$*-linearly disjoint* if

- for every $\ell \in \Lambda$,
$$\rho_\ell\,(S(b,\delta)) = \begin{cases} S_\ell(b_\ell,\delta) & \text{in case (2),} \\ S_\ell(b_\ell,\delta) \cup \{1\} & \text{in case (3),} \end{cases}$$
- and for any choice of two distinct indices ℓ and ℓ' in Λ, the product map
$$\rho_{\ell,\ell'} := \rho_\ell \times \rho_{\ell'} : G \to G/H_\ell \times G/H'_\ell$$
satisfies
$$\rho_{\ell,\ell'}\,(S(b,\delta)) = \begin{cases} S_\ell(b_\ell,\delta) \times S_{\ell'}(b_{\ell'},\delta) & \text{in case (2),} \\ (S_\ell(b_\ell,\delta) \cup \{1\}) \times (S_{\ell'}(b_{\ell'},\delta) \cup \{1\}) & \text{in case (3).} \end{cases}$$

In the sequel we work with the set $S(b,\delta)$ defined either by (2) or (3). Accordingly the definition of $S_\ell(b_\ell,\delta)$ may be modified by adjoining 1.

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 [7, Chap. 7].

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

where g_0 is a fixed element in G and the steps ξ_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

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

We impose two extra conditions on the distribution of the steps ξ_k, which are rather natural. The first one we call *local uniformity with respect to* (ρ_ℓ):

$$\forall k \geqslant 1,\ \forall \ell \in \Lambda,\ \forall s' \in S_\ell(b_\ell,\delta),\ \mathbf{P}(\rho_\ell(\xi_k) = s') = (\#S_\ell(b_\ell,\delta))^{-1}.$$

In other words:

$$\sum_{\{s\in S(b,\delta)\,:\ \rho_\ell(s)=s'\}} p_s = (\#S_\ell(b_\ell,\delta))^{-1},$$

for all $s' \in S_\ell(b_\ell,\delta)$ and for all $\ell \in \Lambda$. The second condition we call *local independence* of the steps:

$$\forall k \geqslant 1,\ \forall \ell \neq \ell',\ \forall (s',t') \in G_\ell \times G_{\ell'},\quad \mathbf{P}(\rho_\ell(\xi_k) = s' \mid \rho_{\ell'}(\xi_k) = t') = \mathbf{P}(\rho_\ell(\xi_k) = s').$$

Of course the random walk depends on the parameters $b = (b_\ell)_\ell$ and δ.

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 [7]. 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 subset $\Theta_\ell \subset G/H_\ell$. In the general case Θ_ℓ is required to be conjugacy invariant. In the applications, the group G will be Abelian so this requirement will be satisfied. The probability we want to upper bound is

$$\mathbf{P}(\forall \ell \in \Lambda \cap [L, 2L],\ \rho_\ell(X_k) \notin \Theta_\ell)\,,$$

where $L \geqslant 1$ is a fixed positive integer.

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 [7, Prop. 3.5], as well as for more information on the random walk sieve used here [7, Chap. 7].

PROPOSITION 1.3. — *With notation as above (in particular, $S(b,\delta)$) is defined by either* (2) *or* (3)*) let us assume G is Abelian and:*

- *the family of surjections (ρ_ℓ) is $S(b,\delta)$-linearly disjoint;*
- *the distribution of the steps ξ_k is locally uniform and locally independent with respect to (ρ_ℓ).*

Then there exists $\eta > 0$ such that for any family $(\Theta_\ell)_\ell$ of subsets satisfying $\Theta_\ell \subseteq G_\ell$ for each $\ell \in \Lambda$,

$$\mathbf{P}(\rho_\ell(X_k) \notin \Theta_\ell,\ \forall \ell \in \Lambda_L) \leqslant \sum_{\ell=L}^{2L} e^{-b_\ell} + \left(1 + L\left(\max_{L\leqslant \ell \leqslant 2L} |G_\ell|\right)\exp(-\eta k)\right)\left(\sum_{\ell=L}^{2L} \frac{\#\Theta_\ell}{n_\ell}\right)^{-1},$$

where L is any fixed positive integer, $\Lambda_L := \Lambda \cap [L, 2L]$ and the constant η depends only on δ.

Before starting the proof we define one last piece of useful notation: for indices ℓ and ℓ' in Λ, we set $G_{\ell,\ell'} := G_\ell \times G_{\ell'}$ if $\ell \neq \ell'$ and $G_{\ell,\ell} := G_\ell$. If $\ell = \ell'$, the map $\rho_{\ell,\ell'}\colon G \to G_{\ell,\ell'}$ is nothing but the surjection ρ_ℓ.

The proof of the proposition follows closely that of [7, 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. Fix a real number δ in $(0, 1/2]$ and let us split the probability we are interested in:

$$\begin{aligned}\mathbf{P}\left(\forall \ell \in \Lambda_L,\ \rho_\ell(X_k) \notin \Theta_\ell\right) \leqslant\ & \mathbf{P}\left(\exists \ell \in \Lambda_L,\ X(G/H_\ell, \rho_\ell(S(b,\delta))) \text{ is not a } \delta\text{-expander}\right) \\ & + \mathbf{P}\left(\forall \ell \in \Lambda_L,\ X(G/H_\ell, \rho_\ell(S(b,\delta)) \text{ is a } \delta\text{-expander and } \rho_\ell(X_k) \notin \Theta_\ell\right).\end{aligned} \tag{4}$$

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, $\rho_\ell(S(b,\delta)) = S_\ell(b_\ell,\delta)$ by the linear disjointness assumption and Theorem 1.1 yields that

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

Let us now turn to the second summand of the right side of (4). First, notice that

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

This last probability is amenable to sieve. From the large sieve inequality (see [7, Prop. 3.7]) we have

$$\mathbf{P}(\forall \ell \in \Lambda_L,\ \rho_\ell(X_k) \notin \Theta_\ell) \leqslant \Delta(X_k; L)\left(\sum_{L\leqslant \ell \leqslant 2L} \frac{\#\Theta_\ell}{n_\ell}\right)^{-1}, \tag{5}$$

where one has the theoretical upper bound:

$$\Delta(X_k;L) \leqslant \max_{\ell\in\Lambda_L}\max_{\chi\in\mathscr{B}^*_\ell}\sum_{\ell'\in\Lambda_L}\sum_{\chi'\in\mathscr{B}^*_{\ell'}}\left|W(\chi,\chi')\right|,$$

with

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

Here for any $\ell\in\Lambda$ we let $\mathscr{B}_\ell$ be the group of characters of G/H_ℓ. We set further $\mathscr{B}^*_\ell := \mathscr{B}_\ell\setminus\{1\}$. Finally if χ (resp. χ') is a representation of a group G_1 (resp. G_2) we let $[\chi,\chi']$ be the “external” tensor product representation $\chi\otimes\chi'$ of $G_1\times G_2$ if $G_1\neq G_2$ or the “internal” tensor product representation $\chi\otimes\chi'$ of G_1 otherwise.

Let us assume that for all $\ell\in\Lambda_L$ the Cayley graph $X(G/H_\ell,\rho_\ell(S(b,\delta)))$ is a δ-expander. We fix (non-necessarily distinct) indices ℓ and ℓ' in Λ_L and non-trivial characters χ,χ' of G_ℓ and $G_{\ell'}$, respectively.

We assert that there exists a constant $\eta>0$ depending only on δ such that

$$\left|\mathbf{E}([\chi,\bar{\chi}']\rho_{\ell,\ell'}(X_k))\right| \leqslant \exp(-\eta k).$$

Let us prove this assertion.

Consider

$$M := \mathbf{E}([\chi,\bar{\chi}']\rho_{\ell,\ell'}(\xi_k)) = \sum_{s\in S(b,\delta)} p(s)[\chi,\bar{\chi}']\rho_{\ell,\ell'}(s),$$

which is a well-defined complex number since the series defining M converges absolutely.

We also need to define

$$N_0 := \mathbf{E}([\chi,\bar{\chi}']\rho_{\ell,\ell'}(X_0)) = \sum_{t\in T}\mathbf{P}(X_0=t)[\chi,\bar{\chi}']\rho_{\ell,\ell'}(t)\in\mathbf{C},$$

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 ξ_k being independent, it follows that for $k\geqslant 1$,

$$\mathbf{E}([\chi,\bar{\chi}']\rho_{\ell,\ell'}(X_k)) = N_0 M^k.$$

First notice that $|N_0|\leqslant 1$ and $|M|\leqslant 1$. Next we need to show that $|M|$ is bounded away from 1 uniformly with respect to ℓ,ℓ',χ,χ'.

$$\sum_{s\in S(b,\delta)} p(s)[\chi,\bar{\chi}']\rho_{\ell,\ell'}(s) = \sum_{(s',t')\in S_\ell(b_\ell,\delta)\times S_{\ell'}(b_{\ell'},\delta)}\left(\sum_{\{s\in S(b,\delta):\ \rho_{\ell,\ell'}(s)=(s',t')\}} p_s\right)\chi(s')\bar{\chi}'(t').$$

The inner sum of the right side can be explicitly computed using the assumptions according to which the steps ξ_k are locally uniformly distributed with respect to (ρ_ℓ) and locally independent:

$$\sum_{\{s\in S(b,\delta):\ \rho_{\ell,\ell'}(s)=(s',t')\}} p_s = \left(\sum_{\{s\in S(b,\delta):\ \rho_\ell(s)=s'\}} p_s\right)\left(\sum_{\{s\in S(b,\delta):\ \rho_{\ell'}(s)=t'\}} p_s\right) = (\#S_\ell(b_\ell,\delta))^{-1}\,(\#S_{\ell'}(b_{\ell'},\delta))^{-1}.$$

Thus

$$\begin{aligned}\left|\mathbf{E}([\chi,\bar{\chi}']\rho_{\ell,\ell'}(\xi_k))\right| &\leqslant \left|(\#S_\ell(b_\ell,\delta))^{-1}\sum_{s'\in S_\ell(b_\ell,\delta)}\chi(s')\right|\cdot\left|(\#S_{\ell'}(b_{\ell'},\delta))^{-1}\sum_{t'\in S_{\ell'}(b_{\ell'},\delta)}\bar{\chi}'(t')\right|\\ &\leqslant (1-\delta)^2,\end{aligned}$$

since we assumed that $(X(G_\ell,S_\ell(b_\ell,\delta))$ is a family of δ-expanders.

When $\ell=\ell'$ the computation follows the same pattern but is easier. One indeed obtains

$$\left|\mathbf{E}([\chi,\bar{\chi}']\rho_\ell(\xi_k))\right| = \left|\sum_{s'\in S_\ell(b_\ell,\delta)}\left(\sum_{\{s\in S(b,\delta):\ \rho_\ell(s)=s'\}} p_s\right)\chi\otimes\bar{\chi}'(s')\right|.$$

As before the inner sum of the right side is $(\#S_\ell(b_\ell,\delta))^{-1}$. Two cases arise then. Either $\chi=\chi'$ and the quantity we consider equals 1, or $\chi\otimes\bar{\chi}'$ is not trivial and then

$$\left|\mathbf{E}([\chi,\bar{\chi}']\rho_\ell(\xi_k))\right| \leqslant 1-\delta,$$

by δ-expansion of the family $(X(G_\ell,S_\ell(b_\ell,\delta))$.

Let $\eta>0$ be the real number such that $\exp(-\eta)=1-\delta$. We have proved that as soon as $\ell\neq\ell'$ or $\chi\neq\chi'$,

$$\left|W(\chi,\chi')\right| \leqslant \exp(-\eta k).$$

Moreover if $\ell=\ell'$, we have seen that $\left|W(\chi,\chi)\right|\leqslant 1$. Putting everything together, (5) yields

$$\begin{aligned}&\mathbf{P}(\forall\ell\in\Lambda_L,\ \rho_\ell(X_k)\not\in\Theta_\ell \mid \forall\ell\in\Lambda_L\ X(G/H_\ell,\rho_\ell(S(b,\delta)))\text{ is a }\delta\text{-expander})\\ &\leqslant\left(1+L\left(\max_{L\leqslant\ell\leqslant 2L}|G_\ell|\right)\exp(-k\eta)\right)\left(\sum_{L\leqslant\ell\leqslant 2L}\frac{\#\Theta_\ell}{n_\ell}\right)^{-1}.\end{aligned}$$

□

We now turn to applications of Proposition 1.3 to various combinatorial settings.

2. Random subgraphs of the 2-dimensional grid

Our first application of Proposition 1.3 is a simple one, mainly aimed at explaining how to set up the random walk and ensure that all properties are satisfied. We consider the presence of a fixed subgraph in a random subgraph of the infinite grid $\mathbf{Z}^2$. we study generic properties of subgraphs by walking randomly on the grid's subgraphs. The random walk we use falls within the scope of the general method explained before.

2.1. Sieving in the 2-dimensional Grid

We let $\mathscr{G}$ be the infinite 2-dimensional grid, that is, the graph with vertex set $\mathbf{Z}^2$ in which (a,b) and (c,d) are neighbours if and only if $|a-c|+|b-d|=1$. The family G of all spanning subgraphs of the grid $\mathscr{G}$ may be endowed with an Abelian group structure: indeed the symmetric difference $\triangle$ 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 every non-trivial element of $\mathscr{G}$ has order 2.

Next we define a family of subgroups $(H_\ell)_{\ell\in\Lambda}$ of G, where $\Lambda:=\mathbf{N}_{>0}$. For each $\ell\in\Lambda$, we define C_ℓ to be the collection of all spanning subgraphs of $\mathscr{G}$ 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_ℓ to be the "complement" of C_ℓ in the following sense: the elements of H_ℓ are the graphs with vertex set $\mathbf{Z}^2$ and with no edge contained in $\mathbf{D}(0,2\ell+2)\setminus\mathbf{D}(0,2\ell)$. Set $G_\ell:=G/H_\ell$.

LEMMA 2.1. — *The following holds.*

1) *For each $\ell\in\Lambda$,*
   (a) *C_ℓ is a set of representatives for the quotient G_ℓ; and*
   (b) *the index of H_ℓ in G is $n_\ell:=[G:H_\ell]=|C_\ell|=2^{64\ell+40}$.*
2) *For $S(b,\delta)$ defined as in* (2) *or* (3) *with $\tilde{S}_\ell(b,\delta)\subseteq C_\ell$,*
   (a) *the family $(\rho_\ell)_{\ell\in\Lambda}$ is $S(b,\delta)$-linearly disjoint; and*
   (b) *the distribution of the steps (ξ_k) is locally uniform and locally independent.*

Proof. 1)(a) No two distinct graphs in C_ℓ are congruent modulo an element of H_ℓ. 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 $\mathbf{D}(0,2\ell+2) \setminus \mathbf{D}(0,2\ell)$. If follows that g_C belongs to C_ℓ and its complement g_H in G is an element of H_ℓ satisfying $g = g_C \triangle g_H$. In other words, $g \equiv g_C(\operatorname{mod} H_\ell)$.

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

2)(a) Fix two distinct integers ℓ and ℓ' in Λ, and a couple $(g_\ell, g_{\ell'}) \in S_\ell(b_\ell,\delta) \times S_{\ell'}(b_{\ell'},\delta)$. By 1)(a) we can choose representatives $\tilde{g}_\ell$ and $\tilde{g}_{\ell'}$ of g_ℓ and $g_{\ell'}$ in C_ℓ and $C_{\ell'}$, respectively. Using these representatives, we consider an element g of G of the form $\bigoplus_{m\in\Lambda} \tilde{g}_m$ where $\tilde{g}_m \in \tilde{S}_m(b_m,\delta)$ for each $m \in \Lambda \setminus \{\ell,\ell'\}$. Since the sets C_ℓ are pairwise disjoint as ℓ runs over Λ, we deduce that g is an element of $S(b,\delta)$ satisfying $\rho_\ell(g) = g_\ell$ and $\rho_{\ell'}(g) = g_{\ell'}$.

2)(b) These properties directly follow from the facts that the sets C_ℓ of representatives are pairwise disjoint and the distribution of the variables $s_i^{(\ell)}$ is uniform on G/H_ℓ. □

One has the following interpretation of Lemma 2.1: for each fixed integer $\ell \in \Lambda$ and each element $g \in G$, the unique element in C_ℓ congruent to g modulo H_ℓ is $g \cap C_\ell$ (the intersection being taken edgewise).

2.2. LOOKING FOR 4-CYCLES

For each integer $\ell \in \Lambda$, let Θ_ℓ be the set of all classes $\bar{g} \in G_\ell$ such that the unique representative of $\bar{g}$ in C_ℓ (the existence of which is asserted by Lemma 2.1) contains a 4-cycle. Observe that $|\Theta_\ell| / |G_\ell| \geqslant 2^{-4}$, since every graph of C_ℓ that contains a fixed 4-cycle reduces to an element of Θ_ℓ modulo H_ℓ.

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

$$\kappa(b_\ell,\ell;\delta) = \lceil \psi(\delta)\cdot((64\ell+41)\ln 2+\ell)\rceil\,.$$

Given $s^{(\ell)} \in S_\ell(b_\ell,\delta)$, we define $\tilde{s}^{(\ell)}$ to be its representative in C_ℓ (see 1(b) of Lemma 2.1), that is, $\tilde{s}^{(\ell)}$ has no edge outside $\mathbf{D}(0,2\ell+2) \setminus \mathbf{D}(0,2\ell)$.

THEOREM 2.2. — *Let (X_k) be a random walk on $\mathscr{G}$ defined as in Subsection 1.2 using $S(b,\delta)$ (as in* (2) *or* (3)*) with $\tilde{S}_\ell(b,\delta) \subseteq C_\ell$. Let $\eta > 0$ be such that* $\exp(-\eta) = 1-\delta$. *Then,*

$$\forall k \geqslant 1, \quad \mathbf{P}(X_k \textit{ does not contain a } 4\textit{-cycle}) \leqslant \frac{2550}{\eta k}.$$

Proof. Fix a positive integer k. Lemma 2.1 ensures that the hypotheses of Proposition 1.3 are satisfied. We may assume that $\eta k \geqslant 2550$, since otherwise the statement of the theorem trivially holds. Set $L := \lceil \eta k/75 \rceil$. Applying Proposition 1.3, we obtain

$$\begin{aligned}
\mathbf{P}(\rho_\ell(X_k) \notin \Theta_\ell, \forall \ell \in \Lambda_L) &\leqslant \sum_{\ell=L}^{2L} e^{-b_\ell} + (1+L|G_L|\exp(-\eta k))\left(\sum_{\ell=L}^{2L} \frac{\#\Theta_\ell}{n_\ell}\right)^{-1}\\
&\leqslant e^{1-L} - e^{-2L} + (1+L\cdot 2^{64L+40}\exp(-\eta k))\cdot\frac{2^4}{L}\\
&\leqslant \frac{1+2^4}{L} + 2^{64L+44}\exp(-\eta k)\\
&\leqslant \frac{2\times 17}{L} \leqslant \frac{2\times 17\times 75}{\eta k},
\end{aligned}$$

where we used that $e^{1-x} - e^{-2x} \leqslant 1/x$ if $x > 0$, the fact that $x \mapsto xe^{-\kappa x}$ decreases for $x \geqslant 1/\kappa > 0$, and the inequality $\exp(64\log 2 - 75) \leqslant 17 \times 2^{-44}$. □

More generally, one could look for cycles of length $r \geqslant 4$ in the graph obtained after k steps of the random walk are performed. Our setting could be easily extended. For simplicity we have chosen to give the detail of the argument only in the case where $r = 4$.

3. ORDER & DISORDER: SIEVING FOR MONOCHROMATIC STRUCTURES

We now turn to other applications of Proposition 1.3, inspired by Ramsey Theory.

Arguably, one way of envisaging Ramsey Theory is *via* the study the robustness of patterns. For instance, while a (sufficiently large) set of consecutive integers contains many arithmetic progressions of any fixed length, it might be still possible to destroy all of them using a well-chosen partition of the sets: none of these arithmetic progressions would be contained in only one part of our partition. Similarly, while an n-vertex complete graph contains $\binom{n}{3}$ triangles, one could imagine a partition of the edges so that no part would contain a single triangle. Ramsey Theory tells us that no such partitions exist, provided the set (or graph) we start with is sufficiently large compared to the size of the object sought and the number of parts the partition is allowed to have.

A partition of a set S into k parts is often called a *k-coloring*, that is, a mapping $f\colon S \to \{1,\dots,k\}$ where the image of an element can be interpreted as the number of the part to which the element belongs.

3.1. LOOKING FOR MONOCHROMATIC TRIANGLES

We let $\mathscr{G}$ be the (countable) infinite complete graph, that is, the graph with vertex set $\mathbf{N}$ in which every two distinct positive integers are neighbours. We fix an integer $c \geqslant 3$ and we define $\mathscr{C}$ to be the collection of all functions from the edges of $\mathscr{G}$ 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 $f(e) \neq 0$.

The set $\mathscr{C}$ 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 $\mathscr{C}$ is formally defined by

$$\begin{array}{rccl} f+g\colon & E(\mathscr{G}) & \longrightarrow & \mathbf{Z}/c\mathbf{Z} \\ & e & \longmapsto & f(e)+g(e). \end{array}$$

The neutral element is the function that is identically 0.

We are interested in monochromatic substructures of a given fixed size 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-cliques or r-cycles for $r \geqslant 3$).

We define a family of subgroups $(H_\ell)_{\ell\in\Lambda}$ of $\mathscr{C}$, where $\Lambda := \mathbf{N}$. Consider a partition *in finite parts* $(I_\ell)_{\ell\in\Lambda}$ of Λ. We set $i(\ell) := |I_\ell|$ for $\ell \in \Lambda$. Let $E_\ell := \left\{(a,b) \in I_\ell^2 : a \neq b\right\}$, that is, E_ℓ is the set of all edges of $\mathscr{G}$ with both endvertices contained in I_ℓ. We define C_ℓ to be the collection of all functions $f \in \mathscr{C}$ with support contained in E_ℓ. Then H_ℓ is the collection of all functions $f \in \mathscr{C}$ such that $f|E_\ell \equiv 0$.

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

LEMMA 3.1. — *The following holds.*

1) *For each $\ell \in \Lambda$,*

   (a) *C_ℓ is a set of representatives of the quotient $\mathscr{C}_\ell$; and*

   (b) *the index of H_ℓ in $\mathscr{C}$ is $n_\ell := [\mathscr{C} : H_\ell] = |C_\ell| = c^{i(\ell)(i(\ell)-1)/2}$.*

2) *For $S(b,\delta)$ defined as in* (2) *or* (3) *with $\tilde{S}_\ell(b,\delta) \subseteq C_\ell$,*

   (a) *the family $(\rho_\ell)_{\ell\in\Lambda}$ is $S(b,\delta)$-linearly disjoint; and*

   (b) *the distribution of the steps (ξ_k) is locally uniform and locally independent.*

Proof. 1)(a) No two distinct functions in C_ℓ are congruent modulo an element of H_ℓ. Moreover, for any $f \in \mathscr{C}$, let f_C be the function equal to f on E_ℓ and equal to 0 everywhere else, that is, $f_C|E_\ell := f|E_\ell$ and $f_C|(E(\mathscr{G}) \setminus E_\ell) := 0$. It follows that $f_C \in C_\ell$ 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)(a) Fix two distinct integers ℓ and ℓ' in Λ, and any couple $(f_\ell, f_{\ell'}) \in S_\ell(b_\ell,\delta) \times S_{\ell'}(b_{\ell'},\delta)$. By 1)(a) we can choose representatives $\tilde{f}_\ell$ and $\tilde{f}_{\ell'}$ of f_ℓ and $f_{\ell'}$ in C_ℓ and $C_{\ell'}$, respectively. Let $f\colon E(\mathscr{G}) \to \mathbf{Z}/c\mathbf{Z}$ be a function of the form $f := \bigoplus_{m\in\Lambda} g_m$ where $g_m \in \tilde{S}_m(b_m,\delta)$ for each m with $g_\ell = \tilde{f}_\ell$ and $g_{\ell'} = \tilde{f}_{\ell'}$. Since the sets E_ℓ are pairwise disjoint as ℓ runs over Λ, we deduce that f is an element of $S(b,\delta)$ satisfying $\rho_\ell(f) = f_\ell$ and $\rho_{\ell'}(f) = f_{\ell'}$.

2)(b) These properties directly follow from the facts that the sets C_ℓ of representatives are pairwise disjoint and the distribution of the variables $s_i^{(\ell)}$ is uniform on G/H_ℓ. □

A practical way to rephrase part of the proof of Lemma 3.1 is to say that for each fixed integer ℓ in Λ and each element f of $\mathscr{C}$, the unique element in C_ℓ congruent to f modulo H_ℓ is the function equal to f on E_ℓ and to 0 outside of E_ℓ.

From now on, we assume that $i(\ell) \geqslant 3$ for $\ell \in \Lambda$. For each integer $\ell \in \Lambda$, let Θ_ℓ be the set of classes $\bar{f} \in \mathscr{C}_\ell$ such that the unique representative f of $\bar{f}$ in C_ℓ (the existence of which is asserted by Lemma 3.1) contains a monochromatic triangle in E_ℓ. In other words $f \in \Theta_\ell$ if and only if I_ℓ 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 $|\Theta_\ell|/|\mathscr{C}_\ell| \geqslant c^{-2}$. Indeed any function that restricts to a constant map (with values in $\mathbf{Z}/c\mathbf{Z}$) on a fixed triangle contained in E_ℓ surjects to an element of Θ_ℓ *via* ρ_ℓ.

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

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

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

THEOREM 3.2. — *Let (X_k) be a random walk on $\mathscr{C}$ defined as in Subsection 1.2 using $S(b,\delta)$, defined either by* (2) *or* (3). *Let $\eta > 0$ be such that $\exp(-\eta) = 1-\delta$. Then, for each positive integer k and each integer $L \geqslant 1$,*

$$\mathbf{P}(X_k \textit{ does not contain a monochromatic triangle}) \leqslant \frac{c^2+1}{L} + c^{(1/2)\cdot i(2L)(i(2L)-1)+2}\exp(-\eta k).$$

Proof. Fix a positive integer k. Lemma 3.1 ensures that the hypotheses of Proposition 1.3 are satisfied. We obtain, applying Proposition 1.3,

$$\begin{aligned}
\mathbf{P}(\rho_\ell(X_k) \notin \Theta_\ell, \forall \ell \in \Lambda_L) &\leqslant \sum_{\ell=L}^{2L} e^{-b_\ell} + (1 + L|\mathscr{C}_L|\exp(-\eta k))\left(\sum_{\ell=L}^{2L}\frac{\#\Theta_\ell}{n_\ell}\right)^{-1}\\
&= e^{1-L} - e^{-2L} + (1 + L\cdot c^{i(2L)(i(2L)-1)/2}\exp(-\eta k))\cdot\frac{c^2}{L}\\
&\leqslant e^{1-L} - e^{-2L} + \frac{c^2}{L} + c^{(1/2)\cdot i(2L)(i(2L)-1)+2}\exp(-\eta k)\\
&\leqslant \frac{1}{L} + \frac{c^2}{L} + c^{(1/2)\cdot i(2L)(i(2L)-1)+2}\exp(-\eta k),
\end{aligned}$$

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

Different choices of sets I_ℓ may correspond to different speeds 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 3.3.

COROLLARY 3.3. — *With notation as in Theorem 3.2, for every positive integer k,*

$$\begin{aligned}
&\mathbf{P}(X_k \textit{ does not contain a monochromatic triangle})\\
\leqslant &\mathbf{P}(X_k \textit{ does not contain a monochromatic triangle on three consecutive vertices})\\
\leqslant &c^5\exp(-\eta k).
\end{aligned}$$

Proof. Set $I_\ell := \{3\ell-2, 3\ell-1, 3\ell\}$ for each $\ell \in \Lambda$. In particular $i(\ell)(i(\ell)-1) = 6$. Set $L := c^N$, for an arbitrary positive integer N. Therefore, Theorem 3.2 implies that

$$\begin{aligned}
\mathbf{P}(X_k \text{ does not contain a monochromatic triangle on three consecutive vertices}) \leqslant &\frac{c^2+1}{L} + c^5\cdot\exp(-\eta k)\\
= &c^5\exp(-\eta k) + c^{-N}(c^2+1).
\end{aligned}$$

The conclusion follows by letting N go to infinity. □

We note that the contributions from the non-standard case (that is, $X(G/H_\ell, S_\ell(b_\ell;\delta))$ is not an expander) can be compensated by an adequate choice of L, providing $i(L)$ does not grow too quickly with L. It is natural to compare this last statement with what is known from Ramsey theory; this discussion is deferred to Section 4.

3.2. MONOCHROMATIC SOLUTIONS TO EQUATIONS

It also seems relevant to study solutions of an equation through the perspective of Ramsey Theory: can one destroy the solutions of an equation by partitioning the different values the variables can take?

Let $A \in \mathbf{Z}^{\mathbf{N}}$. We are interested in the following question, which turns out to be amenable to our setting.

Given a random c-colouring of A, is there a monochromatic non-empty subset summing to 0*?*

For illustrative purposes, we study this question in two steps. First we leave aside colourings and just bound the probability that a random subset of $\mathbf{Z}$ contains no subset summing to 0. To this end, the group G considered is that of all subsets of $\mathbf{Z}$ with the symmetric difference Δ as group law. We then show how easily one can add colourings to this setting, by just considering the product of the group G with the group of all c-colourings of $\mathbf{Z}$.

So let G be the group consisting of all subsets of $\mathbf{Z}$ endowed with the symmetric difference. For each positive integer ℓ, we set $I_\ell := \{-\ell, \ell\}$ and we define H_ℓ to be the subgroup of G consisting of all subsets of $\mathbf{Z}$ that are disjoint from I_ℓ. Thus the subsets of I_ℓ form a set of representatives for $G_\ell := G/H_\ell$. In particular, $n_\ell := [G : H_\ell] = 4$.

We set

$$\Theta_\ell := \left\{ X \in G_\ell : X \neq \varnothing \text{ and } \sum_{x \in X} x = 0 \right\},$$

so Θ_ℓ is a singleton, the unique element of which is represented by I_ℓ. Now one can define a random walk (X_k) as in Subsection 1.2. This random walk readily satisfies the requirements of Proposition 1.3. Further, observe that if a subset S of $\mathbf{Z}$ does not contain a non-empty subset summing to 0, then neither does the intersection of S with any fixed subset. Thus the probability P_k that X_k does not contain a non-empty subset summing to 0 is at most

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

Since $|\Theta_\ell|/n_\ell = \frac{1}{4}$ for each positive integer ℓ, Proposition 1.3 implies that for each positive integer k and each integer $L \geqslant 1$,

$$P_k \leqslant \frac{1}{L} + \left(1 + L \max_{L \leqslant \ell \leqslant 2L} |G_\ell| \exp(-\eta k)\right) \cdot \frac{4}{L} = \frac{5}{L} + 16 \exp(-\eta k).$$

Consequently, letting L tend to infinity, one infers the following statement.

THEOREM 3.4. — *Let (X_k) be a random walk on G defined as in Subsection 1.2 using $S(b,\delta)$, defined either by* (2) *or* (3) *with $\tilde{S}_\ell(b,\delta) \subseteq 2^{I_\ell}$. Let $\eta > 0$ be such that* $\exp(-\eta) = 1-\delta$*. Then, for each positive integer k,*

$$\mathbf{P}(X_k \textit{ does not contain a non-empty subset summing to } 0) \leqslant 16 \exp(-\eta k).$$

Let us now see how to deal with the coloured version, that is, we want to upper bound the probability that our random c-coloured subset does not contain a *monochromatic* non-empty subset summing to 0, where c is an integer greater than 1. It suffices to work in the product group $G := (2^{\mathbf{Z}}, \Delta) \times \{f : \mathbf{Z} \to \mathbf{Z}/c\mathbf{Z}\}$. For each positive integer ℓ, the subgroup H_ℓ is defined to be

$$2^{\mathbf{Z} \setminus I_\ell} \times \left\{ f : \mathbf{Z} \to \mathbf{Z}/c\mathbf{Z} : f(-\ell) = f(\ell) = 0 \right\},$$

where $I_\ell := \{-\ell, \ell\}$ as before.

Thus $n_\ell := [G : H_\ell] = 4 \cdot 2^c = 2^{c+2}$, which does not depend on ℓ. A set of representatives for $G_\ell := G/H_\ell$ is

$$2^{I_\ell} \times \mathscr{F}_\ell,$$

where $\mathscr{F}_\ell := \left\{ f : \mathbf{Z} \to \mathbf{Z}/c\mathbf{Z} : f|\mathbf{Z} \setminus I_\ell = 0 \right\}$.

Defining Θ_ℓ to be $\{I_\ell\} \times \left\{ f : \mathbf{Z} \to \mathbf{Z}/c\mathbf{Z} : f \text{ is constant} \right\}$, it follows that $|\Theta_\ell|/n_\ell = c2^{-c-2}$. Since the hypotheses of Proposition 1.3 are satisfied, one obtains the following statement.

THEOREM 3.5. — *Let (X_k) be a random walk on G defined as in Subsection 1.2 using $S(b,\delta)$, defined either by* (2) *or* (3) *with $\tilde{S}_\ell(b,\delta) \subseteq 2^{I_\ell} \times \mathscr{F}_\ell$. Let $\eta > 0$ be such that* $\exp(-\eta) = 1-\delta$*. Then, for each positive integer k,*

$$\mathbf{P}(X_k \textit{ does not contain a monochromatic non-empty subset summing to } 0) \leqslant \frac{2^{2c+4}}{c} \exp(-\eta k).$$

3.3. TOWARDS A QUANTITATIVE INFINITE RAMSEY THEORY

Instead of restricting to the detection of monochromatic triangles in a random colouring of the infinite (countable) complete graph as in Subsection 3.1, we now focus on the extent to which our method can be applied in the context of infinite Ramsey theory. Let us first recall the result we have in mind, established by Ramsey [12]. Given a set X and a non-negative integer r, we define $X^{(r)}$ to be the collection of all subsets of X of size r.

THEOREM 3.6 (infinite Ramsey Theorem [12]). — *Let X be some countably infinite set. Let $c \geqslant 1$ and $r \geqslant 1$ be integers. Consider a given colouring $f\colon X^{(r)} \to \mathbf{Z}/c\mathbf{Z}$ of the elements of $X^{(r)}$ in c different colours. Then there exists some infinite subset A of X such that the function f is constant on $A^{(r)}$, that is, all subsets of A of cardinality r have the same image under f.*

As in the statement of Ramsey's Theorem, fix positive integers c and r. As our base set we choose $X := \mathbf{N}$. The set $\mathscr{C}^{(r)}$ of all possible c-colourings of subsets of size r of X may be endowed with a group structure inherited from that of $\mathbf{Z}/c\mathbf{Z}$.

Fix also an auxiliary positive integer j and set $\Lambda := \mathbf{N}$. Consider subsets $I_\ell^{(r,j)}$ of $\mathbf{N}$ indexed by $\ell \in \Lambda$, that we assume to be finite and pairwise disjoint. For given ℓ, let E_ℓ^r be the set of subsets of size r of $I_\ell^{(r,j)}$. Let C_ℓ be the collection of all colourings supported on E_ℓ^r and let H_ℓ be the subgroup of all colourings of $\mathscr{C}^{(r)}$ supported on the complement of E_ℓ^r in $X^{(r)}$. This way C_ℓ is a set of representatives for the quotient $\mathscr{C}^{(r)}/H_\ell$. Set further $i(\ell,r) := \#I_\ell^{(r,j)}$ and $\rho_\ell : \mathscr{C}^{(r)} \to \mathscr{C}^{(r)}/H_\ell$, the canonical surjection. Arguments analog to those in the proofs of Lemmas 2.1 and 3.1 yield the following.

LEMMA 3.7. — *One has*

1) $n_\ell := (\mathscr{C}^{(r)} : H_\ell) = \#C_\ell = c^{\binom{i(\ell,r)}{r}}$*; and*
2) *For $S(b,\delta)$ defined as in* (2) *or* (3) *with $\tilde{S}_\ell(b,\delta) \subseteq C_\ell$,*
   (a) *the family $(\rho_\ell)_{\ell\in\Lambda}$ is $S(b,\delta)$-linearly disjoint; and*
   (b) *the distribution of the steps (ξ_k) is locally uniform and locally independent.*

As in the previous sections we may define on $\mathscr{C}^{(r)}$ a random walk (X_k) that satisfies the requirements of Proposition 1.3. We then ask the question:
at which speed do we reach a colouring X_k of the r-element subsets of X that exhibits a subset $A \subseteq X$ of size $j+r$, all the r-element subsets of which have the same colour?
The next statement answers that question.

THEOREM 3.8. — *Let (X_k) be the random walk defined on $\mathscr{C}^{(r)}$ as in Subsection 1.2 using $S(b,\delta)$, defined either by* (2) *or* (3) *with $\tilde{S}_\ell(b,\delta) \subseteq C_\ell$. Fix positive integers j, r and c. Let $\eta > 0$ be such that $\exp(-\eta) = 1-\delta$. Then for every positive integer k,*

$$\begin{aligned}&\mathbf{P}\Big(\textit{No element of } \mathbf{N}^{(j+r)} \textit{ has all its } r\textit{-element subsets of the same colour in } X_k\Big)\\ &\leqslant c^{\binom{r+j}{r}-1}\exp(-\eta k).\end{aligned}$$

Proof. Set $I_\ell^{(r,j)} := \{(r+j)\ell-(r+j-1),(r+j)\ell-(r+j-2),\ldots,(r+j)\ell\}$. If j and r are fixed, then $I_\ell^{(r,j)}$ is an integral interval of size $r+j$ and different indices ℓ and ℓ' give rise to disjoint intervals $I_\ell^{(r,j)}$ and $I_{\ell'}^{(r,j)}$. For such a choice of sets $I_\ell^{(r,j)}$, one has $n_\ell = c^{\binom{r+j}{r}} = c^{\frac{(r+j)!}{r!j!}}$. In particular n_ℓ is independent of ℓ. Let us set $b_\ell := \ell$ and for each $\ell \in \Lambda$,

$$\Theta_\ell := \Big\{g \in \mathscr{C}^{(r)}/H_\ell : \text{the only representative of } g \text{ in } C_\ell \text{ is constant on } E_\ell^{(r,j)}\Big\}.$$

Of course, $\#\Theta_\ell/n_\ell = c/n_\ell = c^{-\binom{r+j}{r}+1}$. Therefore, putting things together *via* Proposition 1.3, a computation similar to that of the proof of Theorem 3.2 produces the upper bound

$$\frac{1+c^{\binom{r+j}{r}-1}}{L_0} + c^{\binom{r+j}{r}-1}\exp(-\eta k),$$

for the probability investigated. Setting as before $L_0 := c^N$ and letting $N \to \infty$ we obtain the desired upper bound. □

Remark 3.9. Comparing the inequality in Theorem 3.8 with the statement of Theorem 3.6 we note an important limitation to our approach: we cannot dispense of the use of the auxiliary parameter j. More precisely, letting j tend to infinity in the inequality of Theorem 3.8 yields only a trivial upper bound for the probability investigated.

4. REMARKS AND FURTHER APPLICATIONS

Let us underline some peculiarities of the applications developed 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 (possibly infinite, as our applications show) alphabet corresponding to a particular subset $S(b,\delta)$. 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 $n \geqslant N$, then every c-colouring of the edges of the complete graph K_n on n vertices contains a monochromatic triangle. Alon and Rödl [1] established that the smallest such N is $\Theta(3^c)$ as n tends to infinity (that is, there exist two constants ρ and ρ' such that for sufficiently large n, this value belongs to $\left[\rho \cdot 3^c, \rho' \cdot 3^c\right]$). 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_ℓ.

Another feature of the application developed in Section 3 is uniformity with respect to the number c of colours involved. No such uniformity holds in the context of Ramsey theory. Indeed, as already mentioned, Alon and Rödl's theorem [1] 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 3 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 $c \geqslant 3$ (the number of colours). Similarly as before, let $\mathscr{C}$ be the group of all c-colourings of $\mathbf{N}$. We consider the subsets $I_\ell := \{\ell sq, \ell sq + q, \ldots, \ell sq + (s-1)q\}$ for $\ell \in \Lambda := \mathbf{N}$. (It is this choice of particular subsets of $\mathbf{N}$ of length at least s 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 $\mathscr{C}$ defined as in Subsection 1.2 using $S(b,\delta)$ (as in* (2) *or* (3)*). Let $\eta > 0$ be such that $\exp(-\eta) = 1 - \delta$. For all $k \geqslant 1$,*

$$\mathbf{P}(X_k \textit{ contains no monochromatic arithmetic progression with common difference } q \textit{ and length } s) \leqslant c^{2s}\exp(-\eta k).$$

Let us sketch the proof. For each $\ell \in \mathbf{N}$, let H_ℓ be the set of all functions $f : \mathbf{N} \to [c]$ such that $f|I_\ell \equiv 0$. The index in $\mathscr{C}$ of each of these subgroups is c^s. Moreover, there is a collection of natural representatives for the classes modulo H_ℓ, namely the functions with support contained in I_ℓ. Let Θ_ℓ be the set of classes modulo H_ℓ whose unique representative — in the aforementioned system of natural representatives — contains a monochromatic arithmetic progression of length s that is contained in I_ℓ. Then one has $|\Theta_\ell| / n_\ell \geqslant c^{-s}$.

It is straightforward to check that the hypotheses of Proposition 1.3 are satisfied. By Proposition 1.3, the probability that in X_k no monochromatic arithmetic progression with common difference q and length s is contained in I_ℓ, for all ℓ in Λ_L is at most

$$\frac{1}{L} + \frac{c^s}{L} + c^{2s}\exp(-\eta k).$$

Since this last probability is, for every L, an upper bound on the probability that there is no monochromatic arithmetic progression in X_k with common difference q and length s, Theorem 4.1 follows by setting $L := c^N$ and letting N tend to infinity, as was done before.

We conclude by pointing out the following: van der Waerden's theorem [13] ensures that, for each fixed positive integers s and $c \geqslant 3$, there exists an integer N such that if $n \geqslant N$ then any c-colouring 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_ℓ). Van der Waerden's theorem does not guarantee the existence of such an arithmetic progression and the aforementioned inequality is essentially an explicit lower bound on the speed of rarefaction of the colourings that do not yield a monochromatic arithmetic progression with the required properties. Furthermore, and as mentioned in the remarks about Section 3, the uniformity of our estimate with respect to the number of colours c is a quite interesting by-product of our approach.

REFERENCES

[1] N. ALON AND V. RÖDL, *Sharp bounds for some multicolor Ramsey numbers*, Combinatorica, 25 (2005), pp. 125–141.

[2] N. ALON AND Y. ROICHMAN, *Random Cayley graphs and expanders*, Random Structures Algorithms, 5 (1994), pp. 271–284.

[3] J. BOURGAIN, A. GAMBURD, AND P. SARNAK, *Affine linear sieve, expanders, and sum-product*, Invent. Math., 179 (2010), pp. 559–644.

[4] 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.

[5] 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.

[6] F. JOUVE, E. KOWALSKI, AND D. ZYWINA, *Splitting fields of characteristic polynomials of random elements in arithmetic groups*, Israel J. Math., 193 (2013), pp. 263–307.

[7] 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.

[8] 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.

[9] P.-S. LOH AND L. J. SCHULMAN, *Improved expansion of random Cayley graphs*, Discrete Math. Theor. Comput. Sci., 6 (2004), pp. 523–528 (electronic).

[10] A. LUBOTZKY AND C. MEIRI, *Sieve methods in group theory I: Powers in linear groups*, available, arXiv:1107.3666, (2011).

[11] A. LUBOTZKY AND L. ROSENZWEIG, *The galois group of random elements of linear groups*, Amer. J. Math, forthcoming, (2014).

[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.