A Cryptographic Proof of Regularity Lemmas: Simpler and Improved Constructions

Maciej Skórski

IST Austria

Abstract. In this work we present a unified proof for the Strong and Weak Regularity Lemma, based on the cryptographic technique called *low-complexity approximations*. In short, both problems reduce to a task of finding constructively an approximation for a certain target function under a class of distinguishers (test functions), where distinguishers are combinations of simple rectangle-indicators. In our case these approximations can be computed in a naive way, which results in a very simple proof achieving optimal constants. At an abstract level, our proof can be seen a refinement and simplification of the analytic proof given by Lovasz and Szegedy.
Interestingly, with our proof we obtain quantitative improvements on the partition size by a factor equal to the graph density (in the tower heigh for strong regularity and in the exponent for weak regularity). In particular, we achieve best possible bounds for constant densities.

Keywords: Regularity lemmas, Boosting, Low-complexity approximations, Convex optimization, Computational indistingusiability

1 Introduction

Szemeredi's Regularity Lemma was first used in his famous result on arithmetic progressions in dense sets of integers [Sze75]. Since then, it has emerged as an important tool in graph theory, with applications to extremal graph theory, property testing in computer science, combinatorial number theory, complexity theory and others. See for example [DLR95,FK99,HMT88] to mention only few.

Roughly speaking, the lemma says that every graph can be partitioned into a finite number of parts such that the edges between these pairs behave randomly. There are two popular forms of this result, the original result referred to as the Strong Regularity Lemma and the weaker version developed by Frieze and Kannan [FK99] for algorithmic applications.

The purpose of this work is to give yet another proof of regularity lemmas, based on the cryptographic notion of *computational indistinguishability*. We don't revisit applications as it would be beyond the scope. For more about applications of regularity lemmas, we refer to surveys [KS96,RS,KR02]

From now, G is a fixed graph with a vertex set $V(G) = V$ and the edge set $E(G) = E \subset V^2$. By a partition of V we understand every family of disjoint subsets that cover V.

The rest of the paper is organized as follows: the remaining part of this section introduces necessary notions (Section 1.1), states regularity lemmas (Section 1.2), and summarizes our contribution (Section 1.3). In Section 2 we show how to obtain strong regularity and in Section 3 we deal with weak regularity. We conclude our work in Section 4.

1.1 Preliminaries

By the edge density of two vertex subsets we understand the fraction of pairs covered by graph edges.

Definition 1 (Edge density). *For two disjoint subsets T, S of a given graph G we define the edge density of the pair T, S as*

$$d_G(T,S) = \frac{E_G(T,S)}{|T||S|} \tag{1}$$

We slightly abuse the notation denoting $d_G = d_G(V,V)$ for the graph density.

Sets Regularity The notion of *set irregularity* measures the difference between the number of actual edges and expected edges as if the graph was random. Note that for a random bipartite graph with a bipartirtion (T, S) we expect that for almost all subsets S', T' roughly the same fraction of vertex pairs is covered by graph edges. The deviation is precisely measured as follows

Definition 2 (Irregularity [LS07, FL14]). *The irregularity of a pair (S, T) of two vertex subsets is defined as*

$$\mathrm{irreg}_G(S,T) = \max_{S' \subset S, T' \subset T} |E(S',T') - d_G(S,T)|S'||T'||$$

If this quantity is a small fraction of $|S||T|$ then the edge distribution is "homogeneous" or, if we want, random-like.

In turn, two vertex subsets are called regular if the density is almost preserved on their (sufficiently big) subsets[1]

Definition 3 (Regularity). *A pair (S, T) of two disjoint subsets of vertices is said to be ϵ-regular, if*

$$|d_G(S',T') - d_G(S,T)| \leqslant \epsilon$$

for all $S' \subset S$, $T' \subset T$ such that $|S'| \geqslant \epsilon|S|$, $|T'| \geqslant \epsilon|T|$.

For completeness we mention that irregularity and regularity are pretty much equivalent (up to changing ϵ)

Remark 1 (Irregularity vs Regularity). It it easy to see that $\mathrm{irreg}_G(S,T) \leqslant \epsilon|S||T|$ is implied by ϵ-regularity, and it implies $\epsilon^{\frac{1}{3}}$-regularity.

[1] The requirement of being "sufficiently big" is to make this notion equivalent with the irregularity above.

Partition Regularity The next important objects are regular partitions, for which almost all pairs of parts are regular. Note that irregular indexes are weighted by set sizes, to properly address partitions with parts of different size.

Definition 4 (Regular Partitions). *A partition $V_1, \ldots, V_k$ of the vertex set is said to be ϵ-regular if there is a set $I \subset V \times V$ such that*

$$\sum_{(i,j)\in I} |V_i||V_j| \leqslant \epsilon |V|^2$$

and for all $\forall (i,j) \notin I$ the pair (V_i, V_j) is ϵ-regular.

We say that a partition is equitable (or simply: is an equipartition) if any two parts differ in size by at most one. Note that for equitable partitions the above conditions simply means that all but ϵ-fraction of pairs are regular.

There is also a notion of partition irregularity based on sets irregularity

Definition 5 (Partition Irregularity). *The irregularity of a partition $\mathcal{V} = \{V_1, \ldots, V_k\}$ is defined to be* $\mathrm{irreg}(\mathcal{V}) = \sum_{i,j} \mathrm{irreg}_G(V_i, V_j)$.

Remark 2 (Partition Irregularity vs Partition Regularity). Again it it easy to see that both notions are equivalent up to a change in ϵ. Concretely, ϵ-regularity is implied by irregularity smaller than $\epsilon^4 |V|^2$ and implies ϵ-irregularity [FL14].

The partition size in the Strong Regularity Lemma grows as fast as powers of twos. For completeness, we state the definition of the tower function.

Definition 6 (Power tower). *For any n we denote*

$$T(n) = \underbrace{2^{2^{\cdot^{\cdot^{2}}}}}_{n \text{ times}} .$$

1.2 Regularity Lemmas

Having introduced necessary notation, we are now in position to state regularity lemmas. We start with the most popular statement for the Strong Regularity Lemma

Theorem 1 (Strong Regularity Lemma). *For any graph G There exists a partition $V_1, \ldots, V_m$ such that for all up to ϵ-fraction of pairs (i,j)*

$$|E(S,T) - d_G(V_i, V_j)|S||T|| \leqslant \epsilon |V_i||V_j|$$

for any $S \subset V_i, T \subset V_j$ such that $|S| \geqslant \epsilon |V_i|, |T| \geqslant \epsilon |V_j|$.

It has been observed that proofs are much easier if we work with total irregularity, rather than separate bounds for each pair. The following version is equivalent (up to changing ϵ)

Theorem 2 (Strong Regularity Lemma, Relaxed [LS07]). *For any partition $V_1,\ldots,V_k$ of vertices we have*

$$\sum_{i,j} \mathrm{irreg}_G(V_i,V_j) \leqslant \epsilon |V|^2. \tag{2}$$

Finally, we sate the weaker version obtained by Frieze and Kannan

Theorem 3 (Weak Regularity Lemma). *For any graph G there exists a partition of vertices $V_1,\ldots,V_k$ such that*

$$\left| \sum_{i,j} E(S\cap V_i, T\cap V_j) - \sum_{i,j} d_{i,j} |S\cap V_i||T\cap V_j| \right| \leqslant \epsilon |V|^2 \tag{3}$$

for all S,T. Moreover, the partition is generated by $O\left(\epsilon^{-2}\right)$ subsets of V. In particular, k is at most $2^{O\left(\epsilon^{-2}\right)}$.

The present bounds for regularity lemma are tight in general, as showed recently[2] in [FL14].

1.3 Our contribution and related works

We present an improved and simplified proof of the Regularity Lemma, using the cryptographic notion of indistinguishability. Our contribution is twofold: (a) conceptual, as we show how the Regularity Lemma can be written and easy proved using the notion of indistinguishability, and (b) technical, as we improve known bounds by a factor equal to the graph density.

Strong Regularity Lemma as a Low Complexity Approximation We show that a variant of the Szemeredi Regularity Lemma, equivalent to the most often used statement, can be written in the following form

$$\forall f \in \mathcal{F}: \left| \mathop{\mathbb{E}}_{e\leftarrow \mathcal{X}} g(e)f(e) - \mathop{\mathbb{E}}_{e\leftarrow \mathcal{X}} h(e)f(e) \right| \leqslant \epsilon \tag{4}$$

for some functions g,f and a class of functions $\mathcal{F}$ on a finite set $\mathcal{X}$, where h is "efficient" in terms of complexity. More precisely, the result states that a given function f (in our case related to the irregularity of the graph) can be efficiently approximated under a certain class of test functions (called also distinguishers). In cryptography results of this sort are known as *low complexity approximations* and are a powerful and elegant technique of proving complicated results [TTV09,VZ13,JP14]. The quantity in the absolute values in Equation (4) is referred to as the advantage of f in distinguishing g and h, so the statement simply means that h is indistinguishable from g for small ϵ by all functions in $\mathcal{F}$. Depending on the class $\mathcal{F}$ it may be a good "replacement" for g in applications.

[2] Worse bounds were known before for example [Gow97]

In our problem the class of test functions changes depending on the problem: for weak regularity we use rectangle indicator functions of the form $f = \mathbf{1}_{T\times S}$, whereas to obtain strong regularity we use the more complicated class of linear combinations of rectangle indicator functions up to length k, that is functions of the form $f = \sum_{i,j} a_{i,j}\mathbf{1}_{S_{i,j}\times T_{i,j}}$. The proof is in both cases very simple and can be viewed as a special case of the general subgradient descent algorithm well known in convex optimization[3]. The algorithm is given below in pseudocode (see Algorithm 1)

Algorithm 1: Low Complexity Approximations

Input : target function g to approximate,
class of test functions $\mathcal{F}$, a starting point h^0
accuracy parameter ϵ
stepsize t

Output: function h of low complexity w.r.t $\mathcal{F}$ and indistinguishable from g (with respect to tests $\mathcal{F}$)

```
n ← 0
while can distinguish h^n and g by some f ∈ F with advantage ε do
    h^{n+1} ← h^n − t · f
    n ← n + 1
```

A similar result has been shown by Trevisan et al. [TTV09] with respect to the weak regularity lemma. It turns out that the weak regularity lemma can be directly translated to a form of Equation (4). The case of the String Regularity Lemma is however a bit different, because the standard statement doesn't admit a direct translation to Equation (4) so we need first to reduce the Regularity Lemma to a slightly relaxed form similar[4] to Theorem 2 and prove the relaxed statement by low complexity approximation tools. Also, the same class of functions appear in the analytic proof in [LS07] but with a different approximation technique and no clear bound on the partition size.

An Improved and Simpler Proof. When deriving the relaxed version of the Strong Regularity Lemma, we bound the partition size by a tower of twos of height $O(\epsilon^{-2}d_G)$. For constant densities d_G, this matches both best upper and lower bounds [FL14]. For smaller densities $d_G \ll 1$ we obtain improvements. This doesn't contradict the lower bounds as they depend on the density in a complicated and non-explicit way. As for the simplicity, our proof uses a only a

[3] If we consider the mapping $h \to \max_f \left| \mathop{\mathbb{E}}_{e\leftarrow\mathcal{X}} g(e)f(e) - \mathop{\mathbb{E}}_{e\leftarrow\mathcal{X}} h(e)f(e)\right|$ then its subgradient equals f for some $f \in \mathcal{F}$. Then the update is $h := h - t \subset f$ precisely as in the proof of Section 2.1

[4] The relaxed form we use is except that we allow any numbers $d_{i,j}$ in place of densities $d_G(V_i, V_j)$.

naive optimization algorithm, avoiding combinatoric calculations using Cauchy-Schwarz inequalities present in other proofs like [FL14].

The concept of pseudo-irregularity In the Weak Regularity Lemma, we measure the irregularity of the partition as *average difference* between the actual number of edges and the expected number of edges across the pairs of parts of the partition. Therefore, the Weak Regularity Lemma is obtained from the bound

$$\left|\sum_{i,j} E(T_i, S_j) - \sum_{i,j} d_{i,j}|T_i||S_j|\right| \ll |V|^2$$

(note that $\sum_{i,j} E(T_i, S_j) = E(T, S)$) In turn, to prove the Strong Regularity Lemma, we measure the *average absolute difference* between the actual number of edges and the expected number of edges. To prove our result we introduce the following condition (for some constants $d_{i,j}$)

$$\sum_{i,j} |E(T_i, S_j) - d_{i,j}|T_i||S_j|| \ll |V|^2.$$

and refer to this property as "small pseudo-irregularity". This condition extends slightly the notion of irregularity, where the true densities of pairs (V_i, V_j) appear in place of $d_{i,j}$. Our approach with unrestricted constants is much easier to prove and is more flexible. In fact, the idea of relaxing restrictions on densities (equivalently: considering a weighted graph) goes back to [FK99]. The concept of pseudoregularity is what allows us to connect the approximation lemma with the Strong Regularity Lemma.

Quantitative Improvements For the Strong Regularity Lemma we bound the partition size by a tower of twos of height $O(\epsilon^{-2} d_G)$ which is an improvement by a factor of d_G over best results [FL14]. Similarly, for the Weak Regularity Lemma we prove that the partition is an overlay of $O(\epsilon^{-2} d_G)$ subsets (in particular has up to $2^{O(\epsilon^{-2} d_G)}$ members) which is again an improvement by a factor of d_G comparing to best bounds [FL14].

1.4 Proof techniques

The key ingredient of our proof is a descent algorithm, which is similar to the standard way of proving regularity lemmas. As long as the current partition fails to satisfy the desired property, the algorithm uses sets being counterexamples to refine the partition. Moreover, we show that a certain quantity, called the energy function, decreases with every step by a constant (depending on ϵ). From this one concludes that the process of refining the partition halts after a number of step (the bound depends on concrete energy estimates).

Our proof is different with respect to the energy function, as we use simply the euclidean distance (second norm) between the candidate solution and the target. This allows us to decrease the number of rounds by the initial distance, which in our case equals d_G, as we start from $f = \mathbf{1}_E$ (where E is the edge set) and $g = 0$. An overview of the proof (of the Strong Regularity Lemma) is illustrated in Figure 1.

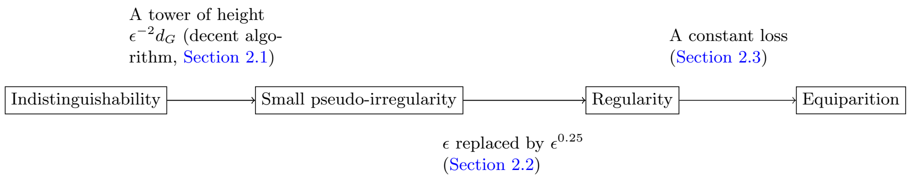

Fig. 1. An overview of our proof of the Strong Regularity Lemma.

The proof of the Weak Regularity Lemma is even simpler and consists of only first step (with the class of test functions changed accordingly).

2 Strong Regularity Lemma

2.1 Obtaining a partition with small pseudo-irregularity

The key indgredient is the following approximation result, proved by the technique sketched in Algorithm 1.

Theorem 4 (Simulating against stepwise function). *For any function $g : V^2 \to [-1, 1]$, and any $\epsilon > 0$, there exists a partition $V_1, \ldots, V_k$ and a piece-wise function h constant on squares $V_i \times V_j$ such that f and g are $\epsilon|V|$-indistinguishable by functions piecewise constant on rectangles $V_i \times V_j$ where $i \leqslant j$*

$$\mathcal{F} = \left\{ f = \sum_{i \leqslant j} a_{i,j} \mathbf{1}_{S_{j,i} \times T_{i,j}} : \quad a_{i,j} = \pm 1, \quad S_{i,j} \subset V_i, T_{i,j} \subset V_j \right\}, \tag{5}$$

where indistinguishability means

$$\forall f \in \mathcal{F}_k : \quad \left| \sum_e h(e) f(e) - \sum_e h(e) f(e) \right| \leqslant \epsilon |V|^2. \tag{6}$$

Moreover, k is not bigger than $d_G \epsilon^{-2}$ iterations of the function $k \to k \cdot 2^{k+1}$ at $k = 1$. In particular, k is at most a tower of 2's of height $O\left(d_G \epsilon^{-2}\right)$.

Remark 3 (Symmetrizing class $\mathcal{F}$). Note that ordering pairs ($i \leqslant j$) in the definition of class $\mathcal{F}$ is crucial to obtain the complexity being a power of 2. Otherwise, we would obtain a (much worse) tower of 4's of the same height.

Remark 4. It is easy to see that the function is a power-tower of twos of height $O(d_G\delta^{-2})$ (a formal proof can obtained by induction as in [FL14].

Corollary 1 (Regularity Lemma in terms of Small Pseudo-Irregularity). *For any graph G there is a partition of vertices V such that the absolute pseudo-irregularity is at most $\epsilon|V|^2$, that is for some numbers $d_{i,j}$ we have*

$$\sum_{i,j\leqslant k} \max_{S\subset V_i, T\subset V_j} |E(T,S) - d_{i,j}\cdot |T||S|| \leqslant \epsilon|V^2| \tag{7}$$

and moreover, the number of partition parts is is a power-tower of twos of height $O(d_G\delta^{-2})$.

Proof (Proof of Corollary 1). It suffices to apply Theorem 4 to $g = \mathbf{1}_E$ and $h = 0$. We have then $\sum_e g(e)t(e) = \sum_{i\leqslant j} a_{i,j}E(S_{i,j},T_{i,j})$ and $\sum_e h(e)t(e) = \sum_{i\leqslant j} a_{i,j}d_{i,j}\,|S_{i,j}|\,|T_{i,j}|$. The absolute values in Equation (7) are achieved by fitting signs of the coefficients $a_{i,j} = \pm 1$.

Proof (of Theorem 4). Suppose we have a function h on a partition $V_1,\ldots,V_k$ which is $\delta|V|$-indistingushable from g by a function f piecewise constant on squares $T_i\times S_j$, that is

$$\sum_e (g(e)-h(e))f(e) \geqslant \delta|V| \tag{8}$$

Consider now $h' = h + t\cdot f$ and note that

$$\sum_e (h'(e)-g(e))^2 = \sum_e (h(e)-h(e))^2 - 2t\sum_e (g(e)-h(e))f(e) + t^2\sum_e f(e)^2.$$

Setting $t = \delta|V|$ in the above equation, by Equation (8) we obtain

$$\sum_e (h'(e)-g(e))^2 \leqslant \sum_e (h(e)-h(e))^2 - \delta^2|V^2|,$$

which means that by replacing h by h' we decrease the distance to g by $\delta^2|V|^2$. Regarding the complexity of $h' = h + t\sum_{i\leqslant j} a_{i,j}\mathbf{1}_{S_{j,i}\times T_{i,j}}$ note that when adding step functions $\mathbf{1}_{S_{j,i}\times T_{i,j}}$, any fixed partition member V_i is intersected by at most $k+1$ sets of the form $S_{j,i}$ or $T_{i,j}$ (because we consider only ordered pairs $i\leqslant j$!). Therefore, the function h' is piecewise constant on the partition V' (generated by $\mathcal{V}$ and sets $S_{i,j}$, $T_{i,j}$) which has at most $k\cdot 2^{k+1}$ members.

2.2 Small pseudo-irregularity implies regularity

In this section we show that pseudo-regularity implies regularity in the sense of We note that the statement is the same as in [FL14],the only difference being arbitrary coefficients in place of sets densities in the irregularity formula in Definition 5.

Proposition 1. *Suppose that for a partition $V_1,\ldots,V_k$ of V there exist numbers $d_{i,j}$ such that*

$$\sum_{i,j\leqslant k} |E(T_i,S_i) - d_{i,j}\cdot|T_i||S_j|| \leqslant \epsilon^4|V^2| \tag{9}$$

for all disjoint subsets $T_i,S_i\subset V_i$. Then the partition is 2ϵ-regular.

Proof. Rewrite Equation (9) as

$$\sum_{i,j\leqslant k}\frac{|S_i||T_j|}{|V|^2}\,|d_G(S_i,T_j)-d_{i,j}|\leqslant\epsilon^4$$

In particular, we get

$$\sum_{i,j\leqslant k}\frac{|V_i||V_j|}{|V|^2}\,|d_G(S_i,T_j)-d_{i,j}|\leqslant\epsilon^2 \tag{10}$$

when $|S_i|,|T_i|\geqslant\epsilon|V|$ for all i. Let S_i',T_i' (both bigger than $\epsilon|V|$) maximize $|d_G(S_i,T_j)-d_{i,j}|$. By the Markov inequality (applied to the probability weights $p_{i,j}=\frac{|V_i||V_j|}{|V|^2}$), there exists an "exceptional" set $I\subset\{1..k\}^2$ such that

$$\sum_{(i,j)\in I}|V_i||V_j|\leqslant\epsilon|V|^2.$$

and

$$\forall(i,j)\notin I: |d_G(S_i',T_i')-d_{i,j}|\leqslant\epsilon$$

By the choice of the pairs (S_i,T_i) this implies $|d_G(S_i,T_j)-d_{i,j}|\leqslant\epsilon$ for every pair $S_i\subset V_i, T_j\subset V_j$. In particular, this is true with $S_i=\subset V_i$ and $T_j=\subset V_j$ which gives $|d_G(V_i,V_j)-d_{i,j}|\leqslant\epsilon$. Bz the triangle inequality we have $|d_G(S_i,T_j)-d_G V_i,V_j|\leqslant 2\epsilon$ which finishes the proof.

2.3 Enforcing equipartition

To conclude the statement we have to prove the following

Lemma 1. *For any ϵ-regular partition $\mathcal{V}$ there exists a $O(\epsilon)$-regular equipartition $\mathcal{W}$ of size $|\mathcal{W}|=O\left(\epsilon^{-1}|\mathcal{V}|\right)$.*

The key observation is the following useful fact, which simply states that regularity is preserved under refinements. A simple proof is given in Appendix A.

Lemma 2 (Regularity preserved under refinements). *For any graph G, if (S,T) is ϵ-regular and $S'\subset S$, $T'\subset T$, then (S',T') is 2ϵ-regular.*

Consider now a coarser partition $\{V_{i,i'}\}_{i,i'}$ such that for every i the set V_i is partitioned into $k(i) \leqslant \frac{k}{\epsilon}$ parts $V_{i,i'}$ where $i' = 1,\ldots,k(i)$ which are all, up to one, of equal size

$$|V_{i,i'}| = \left\lceil \frac{|V|}{\ell} \right\rceil, \quad i' = 1,\ldots,k(i)-1$$
$$|V_{i,i'}| < \left\lceil \frac{|V|}{\ell} \right\rceil, \quad i' = k(i)$$

Let $V' = \bigcup_i V_{k(i)}$. In other words, the set V' combines all "residual" parts into one component. We partition W again into equal (except one) parts $V_1',\ldots,V_r'$ so that

$$|V_i'| = \left\lceil \frac{|V|}{\ell} \right\rceil, \quad i = 1,\ldots,r-1$$
$$|V_r'| < \left\lceil \frac{|V|}{\ell} \right\rceil$$

Therefore, the family

$$\bigcup_{i=1,\ldots,k} \bigcup_{i'=1,\ldots,k(i)-1} \{V_{i,i'}\}_{i,i'} \cup \bigcup_{i=1,\ldots,r} \{V_i'\} \tag{11}$$

is a partition of V that has ℓ members, $\ell-1$ of them being of size $\left\lceil \frac{|V|}{\ell} \right\rceil$ and one being a "remainder" of size smaller than $\left\lceil \frac{|V|}{\ell} \right\rceil$. It follows that the last term has to be of size at least $|V| - (l-1)\left\lceil \frac{|V|}{\ell} \right\rceil$, that is between $\frac{|V|}{\ell}$ and $\frac{|V|}{\ell} - (l-1)$. Now by moving up to one element from each of the other $\ell - 1$ components to the remaining component we arrive at an equipartition $W_1,\ldots,W_\ell$ where all members are of equal size up to one element, that is

$$||W_i| - |W_j|| \leqslant 1 \tag{12}$$

Note that we moved from sets V_i to V' at most $k \cdot \frac{|V|}{\ell} = O(\epsilon|V|)$ vertices, which by Equation (11) belong to at most $O(\ell\epsilon)$ parts W_j. Therefore

Claim (Partition W_i is a refinement of V_i up to a small fraction of members). For all up to a $O(\epsilon)$-fraction of pairs $(i,j) \in \{1,\ldots,\ell\}^2$, the sets W_i, W_j are subsets of some pair $V_{i'}, V_{j'}$.

Let I_W be the set of all pairs (i,j) such that the pair (W_i, W_j) is not ϵ-regular, and let I_V be the set of pairs (i,j) such that (V_i, V_j) is not ϵ-regular.

$$\sum_{(i,j)\in I_W} |W_i||W_j| \leqslant \epsilon|V|^2 + \sum_{(i,j):W_i\subset V_{i'},W_j\subset V_{j'}} |W_i||W_j| \tag{13}$$
$$\leqslant \sum_{(i,j)\in I_V} |V_i||V_j| \tag{14}$$
$$\leqslant O\left(\epsilon|V|^2\right), \tag{15}$$

where the first line follows by the last claim and the fact that W_i are disjoint, the second line follows by the regularity of the partition V_i. Now Equation (12) implies $|I_W| = O(\epsilon\ell^2)$.

3 Weak Regularity Lemma

Theorem 5 (Simulating against rectangle-indicator functions). *For any function $g : V^2 \to [-1, 1]$, and any $\epsilon > 0$, there exists a partition $V_1, \ldots, V_k$ and a piece-wise function h constant on squares $V_i \times V_j$ such that f and g are $\epsilon|V|$-indistinguishable by indicators of rectangles $V_i \times V_j$ where $i \leqslant j$*

$$\mathcal{F} = \{f = \pm\mathbf{1}_{S\times T} : \quad S \subset V_i, T \subset V_j\}\,, \tag{16}$$

that is

$$\forall f \in \mathcal{F} : \quad \left|\sum_e h(e)f(e) - \sum_e h(e)f(e)\right| \leqslant \epsilon|V|^2. \tag{17}$$

Moreover, k is not bigger than $2^{O(d_G\epsilon^{-2})}$. In fact, the partition is an overlay of $O(d_G\epsilon^{-2})$ subsets of vertices.

By applying this result to the function $\mathbf{1}_E$ on V^2 (being 1 for pairs $e = (v_1, v_2)$ which are connected and 0 otherwise) we reprove Theorem 3

Corollary 2 (Deriving Weak Regularity Lemma). *The Weak Regularity Lemma holds with $k = O(d_G\epsilon^{-2})$.*

This result, without the factor d_G was proved in [TTV09]. We skip the proof of Theorem 5 as it merely repeats the argument from Theorem 4, noticing only that the calculation of k is different because the class $\mathcal{F}$ is now simpler. Note also that for this result the class $\mathcal{F}$ doesn't change with every round.

4 Conclusion

We have shown that both: weak and strong regularity lemmas can be written as indistinguishability statements, where the edge indicator function is approximated by a combination of rectangle-indicator functions.

This extends the result of Trevisan at al. for weak regularity to the case of Strong Regularity Lemma. Moreover, due to a different analysis of the underlying descent algorithm, our proof achieves quantitative improvements graphs with low edge densities.

References

DLR95. Richard A. Duke, Hanno Lefmann, and Vojtech Rdl, *A fast approximation algorithm for computing the frequencies of subgraphs in a given graph.*, SIAM J. Comput. **24** (1995), no. 3, 598–620.

FK99. Alan M. Frieze and Ravi Kannan, *Quick approximation to matrices and applications.*, Combinatorica **19** (1999), no. 2, 175–220.

FL14. Jacob Fox and László Miklós Lovász, *A tight lower bound for szemerédi's regularity lemma*, CoRR **abs/1403.1768** (2014).

Gow97. W.T. Gowers, *Lower bounds of tower type for szemerédi's uniformity lemma*, Geometric & Functional Analysis GAFA **7** (1997), no. 2, 322–337.

HMT88. András Hajnal, Wolfgang Maass, and György Turán, *On the communication complexity of graph properties*, Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing (New York, NY, USA), STOC '88, ACM, 1988, pp. 186–191.

JP14. Dimitar Jetchev and Krzysztof Pietrzak, *How to fake auxiliary input*, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings (Yehuda Lindell, ed.), Lecture Notes in Computer Science, vol. 8349, Springer, 2014, pp. 566–590.

KR02. Y. Kohayakawa and V. Rdl, *Szemeredi's regularity lemma and quasi-randomness*, 2002.

KS96. Jnos Komls and Mikls Simonovits, *Szemerdi's regularity lemma and its applications in graph theory*, 1996.

LS07. László Lovász and Balázs Szegedy, *Szemerédi's lemma for the analyst*, Geom. Funct. Anal. **17** (2007), no. 1, 252–270. MR MR2306658 (2008a:05129)

RS. Vojtch Rdl and Mathias Schacht, *Regularity lemmas for graphs.*

Sze75. E. Szemerdi, *On sets of integers containing no k elements in arithmetic progression*, 1975.

TTV09. Luca Trevisan, Madhur Tulsiani, and Salil Vadhan, *Regularity, boosting, and efficiently simulating every high-entropy distribution*, Proceedings of the 2009 24th Annual IEEE Conference on Computational Complexity (Washington, DC, USA), CCC '09, IEEE Computer Society, 2009, pp. 126–136.

VZ13. Salil Vadhan and ColinJia Zheng, *A uniform min-max theorem with applications in cryptography*, Advances in Cryptology CRYPTO 2013 (Ran Canetti and JuanA. Garay, eds.), Lecture Notes in Computer Science, vol. 8042, Springer Berlin Heidelberg, 2013, pp. 93–110 (English).

A Proof of Lemma 2

Proof. Let d be the edge density of the pair (T,S) and d' be the edge density of the pair (T',S'). Denote $\epsilon = \mathrm{irreg}_G(T,S)$. For any two subsets $T'' \subset T', S'' \subset S'$, which are also subsets of T and S respectively, by the definition of d we have

$$\left| \frac{E(T',S')}{|T'||S'|} - d \right| \leqslant \epsilon.$$

which translates to

$$|d'-d| \leqslant \epsilon. \tag{18}$$

Therefore, by Equation (18) and the triangle inequality

$$|E(T'',S'') - d' \cdot |T''||S''|| \leqslant |E(T'',S'') - d \cdot |T''||S''|| + \epsilon \cdot |T''||S''|. \tag{19}$$

Since the definition of d applied to $T'' \subset T, S'' \subset S$ implies

$$|E(T'', S'') - d' \cdot |T''||S''|| \leqslant \epsilon \cdot |T''||S''|$$

, from Equation (19) we conclude that

$$|E(T'', S'') - d' \cdot |T''||S''|| \leqslant 2\epsilon \cdot |T''||S''|,$$

which finishes the proof.