

On the effect of randomness on planted 3-coloring models

Roe David* Uriel Feige†

March 17, 2016

Abstract

We present the *hosted coloring* framework for studying algorithmic and hardness results for the k -coloring problem. There is a class \mathcal{H} of host graphs. One selects a graph $H \in \mathcal{H}$ and plants in it a balanced k -coloring (by partitioning the vertex set into k roughly equal parts, and removing all edges within each part). The resulting graph G is given as input to a polynomial time algorithm that needs to k -color G (any legal k -coloring would do – the algorithm is not required to recover the planted k -coloring). Earlier planted models correspond to the case that \mathcal{H} is the class of all n -vertex d -regular graphs, a member $H \in \mathcal{H}$ is chosen at random, and then a balanced k -coloring is planted at random. Blum and Spencer [1995] designed algorithms for this model when $d = n^\delta$ (for $0 < \delta \leq 1$), and Alon and Kahale [1997] managed to do so even when d is a sufficiently large constant.

The new aspect in our framework is that it need not involve randomness. In one model within the framework (with $k = 3$) H is a d regular spectral expander (meaning that except for the largest eigenvalue of its adjacency matrix, every other eigenvalue has absolute value much smaller than d) chosen by an adversary, and the planted 3-coloring is random. We show that the 3-coloring algorithm of Alon and Kahale [1997] can be modified to apply to this case. In another model H is a random d -regular graph but the planted balanced 3-coloring is chosen by an adversary, after seeing H . We show that for a certain range of average degrees somewhat below \sqrt{n} , finding a 3-coloring is NP-hard. Together these results (and other results that we have) help clarify which aspects of randomness in the planted coloring model are the key to successful 3-coloring algorithms.

*Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot 76100, Israel. E-mail: roee.david@weizmann.ac.il.

†Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot 76100, Israel. E-mail: uriel.feige@weizmann.ac.il.

1 Introduction

A k -coloring of a graph $G(V, E)$ is an assignment $\chi : V \rightarrow [k]$ of colors to vertices such that for every edge $(u, v) \in E$ one has $\chi(u) \neq \chi(v)$. The problem of deciding whether a given graph is k -colorable is NP-hard for every $k \geq 3$ [24, 19]. Moreover, even the most sophisticated coloring algorithms known require (on worst case instances) $|V|^\delta$ colors (for some $\delta \simeq 0.2$) in order to properly color a 3-colorable graph [25].

An approach for coping with NP-hardness is by restricting the class of input instances in a way that either excludes the most difficult instances, or makes them unlikely to appear (in models in which there is a probability distribution over inputs). Along this line, a model that is very relevant to our current work is the so called *random planted coloring model* $G_{n,k,p}$ in which the vertex set (of cardinality n) is partitioned at random into k parts, and edges between vertices in different parts are placed independently with probability p . Such graphs are necessarily k -colorable. Following initial work by Blum and Spencer [7], it was shown by Alon and Kahale [2] that for every k there is a polynomial time algorithm that with high probability k -colors such input graphs (the probability is taken over random choice of input graphs) provided that $p > \frac{c_k}{n}$, where c_k is some constant that depends only on k .

In the current work we propose a framework that contains several different models for generating instances of k -colorable graphs. We call this framework the *hosted coloring framework*. The random planted coloring model is one of the models that is contained in the hosted coloring framework. We consider several other planted coloring models within our framework, and obtain both new algorithmic results and new hardness results. In particular, our results help clarify the role that randomness plays in the random planted model.

1.1 The hosted coloring framework

We describe our framework for generating instances with planted solutions. In the current manuscript, the framework is described only in the special case of the k -coloring problem, though it is not difficult to extend it to other NP-hard problems.

The hosted coloring framework is a framework for generating k -colorable graphs. We alert the reader that graphs within this framework are *labeled*, meaning that every n -vertex graph is given together with a naming of its vertices from 1 to n . A model within this framework involves two components:

1. A class \mathcal{H} of host graphs. Let \mathcal{H}_n denote the set of graphs in \mathcal{H} that have n vertices.
2. A class \mathcal{P} of planted solutions. Formally, in the context of k -coloring, a planted solution can be thought of as a complete k -partite graph. Let \mathcal{P}_n denote the set of planted solutions in \mathcal{P} that have n vertices.

To generate a k -colorable graph with n vertices, one selects one graph H from \mathcal{H}_n , and plants in it one solution P from \mathcal{P}_n . Formally, the planting can be described as generating the graph $G(V, E)$ whose edge set is the intersection of the edge sets of the host graph H and of the complete k -partite graph P . Namely, the vertex set of $G(V, E)$ is $V = [n]$, and $(u, v) \in E$ iff both $(u, v) \in E(H)$ and $(u, v) \in E(P)$.

To complete the description of the hosted framework, we explain how the host graph $H \in \mathcal{H}_n$ is selected, and how the planted solution $P \in \mathcal{P}_n$ is selected. Here, the framework allows for four *selection rules*:

1. Adversarial/adversarial. An adversary selects $H \in \mathcal{H}_n$ and $P \in \mathcal{P}_n$.
2. Random/random. The class of host graphs is equipped with a probability distribution (typically simply the uniform distribution) and likewise for the class of planted solutions. The selections of host graph and planted solution are done independently at random, each according to its own distribution. We use the notation $H \in_R \mathcal{H}_n$ and $P \in_R \mathcal{P}_n$ to describe such selections.
3. Adversarial/random. An adversary first selects $H \in \mathcal{H}_n$, and then $P \in_R \mathcal{P}_n$ is selected at random.
4. Random/adversarial. A host graph $H \in_R \mathcal{H}_n$ is selected at random, and then an adversary, upon seeing H , selects $P \in \mathcal{P}_n$.

The hosted k -coloring framework allows for many different planted k -coloring models, depending on the choice of \mathcal{H} , \mathcal{P} and the selection rule. The random planted $G_{n,k,p}$ model can be described within the hosted k -coloring framework by taking \mathcal{H}_n to be the class of all n -vertex graphs equipped with the Erdos-Renyi probability distribution $G_{n,p}$, taking \mathcal{P}_n to be the class of all n -vertex complete k -partite graphs equipped with the uniform distribution, and using the random/random selection rule.

One of the goals of our work is to remove randomness from planted models. The hosted k -coloring framework allows us to do this. Moreover, one can control separately different aspects of randomness. Let us explain how this is done in our work.

Regular expanders as host graphs. Randomness is eliminated from the choice of host graph by allowing the adversary to select an arbitrary host graph from the class of d -regular λ -expanders, for given d (that may be a function of n) and λ (which is a function of d). The term λ -expander refers to the spectral manifestation of graph expansion. Namely, let $\lambda_1 \geq \dots \geq \lambda_n$ denote the eigenvalues of the adjacency matrix of an n node graph G , and let $\lambda = \max[\lambda_2, |\lambda_n|]$. As is well known, a d -regular graph has $\lambda_1 = d$ and $\lambda \geq \Omega(\sqrt{d})$ [33]. A d -regular graph is referred to as a spectral expander if λ is significantly smaller than d – the smaller λ is the better the guaranteed expansion properties are [20].

Random d -regular graphs are essentially the best possible spectral expanders, satisfying $\lambda = O(\sqrt{d})$ almost surely [15, 18, 17]. The same holds for random graphs in the $G_{n,p}$ model, taking d to be the average degree (roughly pn). We remark that our results extend to graphs that are approximately d -regular (e.g., with degree distribution similar to $G_{n,p}$), and regularity is postulated only so as to keep the presentation simple.

Balanced coloring. Randomness is eliminated from the choice of planted coloring (the choice of P) by allowing the adversary, after seeing H , to plant an arbitrary *balanced* k -coloring, namely, to select an arbitrary k -partite graph in which all parts are of size $\frac{n}{k}$. (Also here, our results extend to having part sizes of roughly $\frac{n}{k}$ rather than exactly, and exact balance is postulated only for simplicity.) Observe that a random k -partition is nearly balanced almost surely.

1.2 Main results

For simplicity we focus here on the special case of $k = 3$, namely, 3-coloring. Extensions of our results to $k > 3$ are discussed in Section E. In our main set of results, we shall consider four related planted models, all within the hosted k -coloring framework.

The four models will have selection rules referred to as H_A/P_A , H_A/P_R , H_R/P_A , and H_R/P_R , where H and P refer to host graph and planted coloring respectively, and A and R stand for *adversarial* and *random* respectively.

- H_A means that the adversary chooses an arbitrary d -regular λ -expander (for an appropriate choice of d and λ) host graph – we refer to this as an *adversarial expander*;
- H_R means that the host graph is chosen as a random Erdos-Renyi random graph $G_{n,p}$ (for an appropriate choice of p) – we refer to this as a *random host graph*.
- P_R refers to a random planted coloring (complete tripartite graph) chosen uniformly at random – we refer to this is *random planting*;
- P_A refers to a balanced planted coloring chosen adversarially (after the adversary sees H) – we refer to this is *adversarial planting*.

In all cases, n denotes the number of vertices in the graph, and d denotes the average degree of the host graph (where $d \simeq pn$ for random host graphs). We shall say that two colorings of the same set of vertices are identical if the partitions that the color classes induce on the vertices are the same (the actual names of colors are irrelevant).

In presenting our results it will be instructive to consider the following notions of coloring:

- The *planted 3-coloring* P .
- A *legal 3-coloring* (but not necessarily the planted one).
- For a given $b < n$, a *b-approximated* coloring is a 3-coloring that is not necessarily legal, but it is identical to the planted 3-coloring on a set of at least $n - b$ vertices.
- For a given $b < n$, a *b-partial* coloring is a 3-coloring of $n - b$ vertices from the graph that is identical to the planted coloring on these vertices. The remaining b vertices are left uncolored and are referred to as *free*.

Our first theorem offers a unifying theme for all four models. For the H_R/P_R model a similar theorem was known [2]. (Recall that λ , the second largest in absolute value eigenvalue, is a measure of expansion and satisfies $\lambda = \Theta(\sqrt{d})$ for random graphs.)

Theorem 1.1. *For a sufficiently large constant c , let the average degree in the host graph satisfy $c < d < n$. Then in all four models (H_A/P_A , H_A/P_R , H_R/P_A , H_R/P_R) there is a polynomial time algorithm that finds a b -partial coloring for $b = O((\frac{\lambda}{d})^2 n)$. For the models with random host graphs (H_R) and/or random planted colorings (P_R), the algorithm succeeds with high probability over choice of random host graph H and/or random planted coloring P .*

Given that Theorem 1.1 obtains a b -partial coloring, the task that remains is to 3-color the set of b free vertices, in a way that is both internally consistent (for edges between free vertices) and externally consistent (for edges with only one endpoint free). From [2] it is known that this task can be completed in the H_R/P_R model. Here are our main results for the other planted models. In all cases, d is the average degree of the host graph.

Theorem 1.2. *In the H_A/P_A model, for every d in the range $C < d < n^{1-\epsilon}$ (where C is a sufficiently large constant and $\epsilon > 0$ is arbitrarily small), it is NP-hard to 3-color a graph with a planted 3-coloring, even when $\lambda = O(\sqrt{d})$.*

Theorem 1.3. *In the H_A/P_R model, for some constants $0 < c < 1$ and $C > 1$ there is a polynomial time algorithm with the following properties. For every d in the range $C < d \leq n - 1$ and every $\lambda \leq cd$, for every host graph within the model, the algorithm with high probability (over the choice of random planted coloring) finds a legal 3-coloring.*

Theorem 1.4. *In the H_R/P_A model:*

- a** *There is a polynomial time algorithm that with high probability (over the choice of host graph) finds a legal 3-coloring whenever $d \geq Cn^{2/3}$ (for a sufficiently large constant C).*
- b** *There is a constant $\frac{1}{3} < \delta_0 < \frac{1}{2}$ such that for $\delta_0 < \delta < \frac{1}{2}$, no polynomial time algorithm has constant probability (over the random choice of host graph of average degree n^δ , for adversarially planted coloring) to produce a legal 3-coloring, unless NP has expected polynomial time algorithms.*

Let us briefly summarize our main findings as to the role of randomness in planted 3-coloring models. For partial coloring, randomness in the model can be replaced by degree and expansion requirements for the host graph, and balance requirements for the planted coloring (see Theorem 1.1). For finding a legal (complete) 3-coloring, randomness of the planted coloring is the key issue, in which case it suffices that the host graph is an arbitrary spectral expander, and in fact, quite a weak one (λ can even be linear in d – see Theorem 1.3). If the planted 3-coloring is not random, then spectral expansion does not suffice (not even $\lambda = O(\sqrt{d})$ – see Theorem 1.2), and moreover, even randomness of the host graph does not suffice (for some range of degrees – see Theorem 1.4b). Finally, comparing Theorem 1.4a to Theorem 1.2 shows that spectral expansion cannot always replace randomness of the host graph.

1.3 Related work

There is a vast body of work on models with planted solutions, and here we shall survey only a sample of it that suffices in order to understand the context for our results.

In our framework we ask for algorithms that k -color a graph that has a planted k -coloring, and allow the algorithm to return any legal k -coloring, not necessarily the planted one. We refer to this as the *optimization* version. The optimization version regards planted models as a framework for studying possibly tractable instances for otherwise NP-hard problems. In certain other contexts (signal processing, statistical inference) the goal in planted models is to recover the planted object, either exactly, or approximately. We refer to this as the *recovery* version. It is often motivated by practical needs (e.g., to recover a true signal from a noisy version, to cluster noisy data, etc.). Our Theorem 1.1 addresses the approximate recovery question, but for many of our models and settings of parameters, exact recovery of the planted k -coloring is information theoretically impossible (one reason being that the input graph might have multiple legal k -coloring with no indication which is the planted one). In general, optimization becomes more difficult when exact recovery is impossible, but

still in many of our models we manage to exactly solve the optimization problem (e.g., in Theorem 1.3). In the context of random planted k -coloring, the k -coloring algorithms of [7] could work only in the regime in which exact recovery is possible, whereas the algorithms of [2] work also in regimes where exact recovery is not possible.

There are planted models and corresponding algorithms for many other optimization problems, including graph bisection [8], 3-SAT [16], general graph partitioning [32], and others. A common algorithmic theme used in many of these works is that (depending on the parameters) exact or approximate solutions can be found using spectral techniques. The reason why the class of host graphs that we consider is that of spectral expanders is precisely because we can hope that spectral techniques will be applicable in this case. Indeed, the first step of our algorithm (in the proof of Theorem 1.1) employs spectral techniques. Nevertheless, its proof differs from previous proofs in some of its parts, because it uses only weak assumptions on the planted model (there is no randomness involved, the host graph is an arbitrary spectral expander, and moreover not necessarily a very good one, and the k -coloring is planted in a worst case manner in the host graph).

Our hosted coloring framework allows the input to be generated in a way that is partly random and partly adversarial. Such models are often referred to as semi-random models [7, 14]. Among the motivations to semi-random models one can mention attempts to capture real life instances better than purely random models (*smoothed analysis* [34] is a prominent example of this line of reasoning, but there are also other recent attempts such as [29] and [30]), and attempts to understand better how worst case input instances to a problem may look like (e.g., see the semirandom models for unique games in [26], which consider four different aspects of an input instance, and study all combinations in which three of these aspects are adversarial and only one is random). Another attractive aspect of semi-random models is the possibility of matching algorithmic results by NP-hardness results, which become possible (in principle) due to the presence of an adversary (there are no known NP-hardness results in purely random planted models). NP-hardness results for certain semi-random models of k -coloring (in which an adversary is allowed to add arbitrary edges between color classes in a random planted $G_{n,k,p}$ graph) have been shown in [14], thus explaining why the algorithmic results that were obtained there for certain values of p cannot be pushed to considerably lower values of p . Typically these NP-hardness results are relatively easy to prove, due to a strong adversarial component in the planted model. In contrast, our NP-hardness result in Theorem 1.4b is proved in a context in which the adversary seems to have relatively little power (has no control whatsoever over the host graph and can only choose the planted coloring). Its proof appears to be different from any previous NP-hardness proof that we are aware of.

In [5] an algorithm that outputs an $\Omega(n)$ size independent set for d -regular 3-colorable graphs is designed. The running time of the algorithm is $n^{O(D)}$, where D is the *threshold rank* of the input graph (namely, the adjacency matrix of the input graph has at most D eigenvalues more negative than $-t$, where $t = \Omega(d)$). Graphs generated in our H_A/P_R model are nearly regular and have low threshold rank. Graphs generated in our H_A/P_A model might have vertices of degree much lower than the average degree, but they have large subgraphs of low threshold rank in which all degrees are within constant multiplicative factors of each other (and presumably the algorithms of [5] can be adapted to such graphs). The hardness results presented in the current paper do not directly give regular graphs, but one can modify the hardness results for k -coloring in the H_A/P_A model (specifically,

Theorem E.2, for $k > 3$) to obtain hardness of k -coloring regular graphs of low threshold rank.

Let us end this survey with two unpublished works (available online) that are related to the line of research presented in the current paper. A certain model for planted 3SAT was studied in [4]. It turns out that in that model a b -partial solution (even for a very small value of b) can be found efficiently, but it is not known whether a satisfying assignment can be found. As that model is purely random, it is unlikely that one can prove that finding a satisfying assignment is NP-hard. In [11] a particular model within the hosted coloring framework was introduced. In that model the class of host graphs is that of so called anti-geometric graphs, and both the choice of host graph and planted coloring are random. The motivation for choosing the class of anti-geometric graphs as host graphs is that these are the graphs on which [13] showed integrality gaps for the semi-definite program of [23]. Hence spectral algorithms appear to be helpless in these planted model settings. Algorithms for 3-coloring were presented in [11] for this class of planted models when the average degree is sufficiently large (above $n^{0.29}$), and it is an interesting open question whether this can be pushed down to lower degrees. If so, this may give 3-coloring algorithms that do well on instances on which semidefinite programming seems helpless.

2 Overview of proofs

In this section we explain the main ideas in the proof. The full proofs, which often include additional technical content beyond the ideas overviewed in this section, appear in the appendix.

2.1 An algorithm for partial colorings

Here we explain how Theorem 1.1 (an algorithm for partial coloring) is proved. Our algorithm can be thought of as having the following steps, which mimic the steps in the algorithm of Alon and Kahale [2] who addressed the H_R/P_R model.

1. *Spectral clustering.* Given an input graph G , compute the eigenvectors corresponding to the two most negative eigenvalues of the adjacency matrix of G . The outcome can be thought of as describing an embedding of the vertices of G in the plane (the coordinates of each vertex are its corresponding entries in the eigenvectors). Based on this embedding, use a distance based clustering algorithm to partition the vertices into three classes. These classes form the (not necessarily legal) coloring χ_1 .
2. *Iterative recoloring.* Given some (illegal) coloring, a *local improvement* step moves a vertex v from its current color class to a class where v has fewer neighbors, thus reducing the number of illegally colored edges. Perform local improvement steps (in parallel) until no longer possible. At this point one has a new (not necessarily legal) coloring χ_2 .
3. *Cautious uncoloring.* Uncolor some of the vertices, making them *free*. Specifically, using an iterative procedure, every *suspect* vertex is uncolored, where a vertex v is suspect if it either has significantly less than $\frac{2d}{3}$ colored neighbors, or there is a color

class other than $\chi_2(v)$ with fewer than $\frac{d}{6}$ neighbors of v . The resulting partial coloring is referred to as χ_3 .

The analysis of the three steps of the algorithm is based on that of [2], but with modifications due to the need to address adversarial settings. Consequently, the values that we obtain for the parameter b after the iterative recoloring and cautious uncoloring steps are weaker than the corresponding bounds in [2].

Lemma 2.1. *The coloring χ_1 is a b -approximated coloring for $b \leq O(\frac{\lambda}{d}n)$.*

For the proof of Lemma 2.1, the underlying idea is that d -regular λ -expander graphs do not have any eigenvalues more negative than $-\lambda$. On the other hand, planting a 3-coloring can be shown to create exactly two eigenvalues of value roughly $-\frac{d}{3}$. This is quite easy to show in the random planting model such as the one used in [2] because the resulting graph is nearly $\frac{2d}{3}$ -regular. We show that this also holds in the adversarial planted model. Thereafter, if $\frac{d}{3} > \lambda$, it makes sense (though of course it needs a proof) that the eigenvalues corresponding to the two most negative eigenvalues contain some information about the planted coloring. An appropriate choice of clustering algorithm can be used to extract this information. We remark that our choice of clustering algorithm differs from and is more efficient than that of [2], a fact that is of little importance in the context of planted 3-coloring, but does offer significant advantages for planted k -coloring when k is large.

Lemma 2.2. *The coloring χ_2 is a b -approximated coloring for $b \leq O(\frac{\lambda^2}{d^2}n)$.*

In [2] a statement similar to Lemma 2.2 was proved using probabilistic arguments (their setting is equivalent to H_R/P_R). Our setting (specifically, that of H_A/P_A) involves no randomness. We replace the proof of [2] by a proof that uses only deterministic arguments. Specifically, we use the well known expander mixing lemma [1].

Lemma 2.3. *The partial coloring χ_3 is a b -partial coloring for $b \leq O(\frac{\lambda^2}{d^2}n)$.*

For the proof of Lemma 2.3, the definition of *suspect* vertex strikes the right balance between two conflicting requirements. One is ensuring that no colored vertex remaining is wrongly colored. The other is that most of the graph should remain remain colored. In [2] a statement similar to Lemma 2.2 was proved using probabilistic arguments, whereas our proof uses only deterministic arguments.

The full proof of Theorem 1.1 appears in Section C.1.

2.2 Adversarial expanders with adversarial planting

Here we sketch how Theorem 1.2 is proved, when the average degree of the host graph is $d = n^\delta$ for some $0 < \delta < 1$. Suppose (for the sake of contradiction) that there is a polynomial time 3-coloring algorithm ALG for the planted H_A/P_A model. We show how ALG could be used to solve NP-hard problems, thus implying P=NP.

Let \mathcal{Q} be a class of sparse graphs on which the problem of 3-coloring is NP-hard. For concreteness, we can take \mathcal{Q} to be the class of 4-regular graphs. For simplicity, assume further that if a graph in \mathcal{Q} is 3-colorable, all color classes are of the same size. (This can easily be enforced, e.g., by making three copies of the graph.)

Given a graph $Q \in \mathcal{Q}$ on $n_1 \simeq n^{1-\delta} < \frac{n}{4d}$ vertices for which one wishes to determine 3-colorability, do the following. Construct an arbitrary spectral expander Z on $n_2 = n - n_1$ vertices, in which $n_1(d - 4)$ vertices (called *connectors*) have degree $d - 1$ and the rest of the vertices have degree d . Plant an arbitrary balanced 3-coloring in Z (each color class has a third of the connector vertices and a third of the other vertices), obtaining a graph that we call Z_3 . Now give the graph G that is a disjoint union of Q and Z_3 as input to ALG. If ALG finds a 3-coloring in G declare Q to be 3-colorable, and else declare Q as not having a 3-coloring.

Let us now prove correctness of the above procedure. If Q is not 3-colorable, then clearly ALG cannot 3-color G . It remains to show that if Q is 3-colorable, then we can trust ALG to find a 3-coloring of G . Namely, we need to show the existence of an expander host graph H and a planted 3-coloring in H that after the removal of the monochromatic edges produces exactly the graph G . An adversary with unlimited computation power can derive H from Q and Z as follows. It finds a balanced 3-coloring χ in Q . Then it connects each vertex v of Q to $d - 4$ distinct connector vertices that have exactly the same color as v (under Z_3). This gives the graph H which is d -regular, and for which planting the 3-coloring χ on its Q part and Z_3 on its Z part gives the graph G . It only remains to prove that H is a spectral expander, but this is not difficult.

The full proof of Theorem 1.2 appears in Section C.2.

2.3 Adversarial expanders with random planting

Here we sketch the proof of Theorem 1.3 (concerning H_A/P_R). It would be instructive to first recall how [2] completed the 3-coloring algorithm in the H_R/P_R case. First, in this case Theorem 1.1 can be considerably strengthened, showing that one gets a b -partial coloring with $\frac{b}{n}$ exponentially small in d . Hence when $d \gg \log n$ this by itself recovers the planted 3-coloring. The difficult case that remains is when d is sublogarithmic (e.g., d is some large constant independent of n). In this case it is shown in [2] that the subgraph induced on the free vertices decomposes into connected components each of which is smaller than $\log n$. Then each component by itself can be 3-colored in polynomial time by exhaustive search, finding a legal 3-coloring (not necessarily the planted one) for the whole graph.

In the H_A/P_R model it is still true that Theorem 1.1 can be strengthened to show that one gets a b -partial coloring with $\frac{b}{n}$ exponentially small in d . However, we do not know if it is true that the subgraph induced on the free vertices decomposes into connected components smaller than $\log n$. To overcome this, we add another step to the algorithm (which is not required in the [2] setting), which we refer to as *safe recoloring*. In this step, iteratively, if an uncolored vertex v has neighbors colored by two different colors, then v is colored by the remaining color. Clearly, if one starts with a b -partial coloring, meaning that all colored vertices agree with the planted coloring, this property is maintained by safe recoloring. We prove that with high probability (over choice of random planting), after the recoloring stage the remaining free vertices break up into connected components of size $O\left(\frac{\lambda^2}{d^2} \log n\right)$. Thereafter, a legal 3-coloring can be obtained in polynomial time using exhaustive search.

The full proof of Theorem 1.3 appears in Section B.2.

2.4 Algorithm for random graphs with adversarial planting

Here we sketch the proof of Theorem 1.4a (concerning an algorithm for H_R/P_A). Given the negative result for H_A/P_A , our algorithm must use a property that holds for random host graphs but need not hold for expander graphs. The property that we use is that when the degree d is very large, the number of common neighbors of every two vertices is larger than $O(\frac{n}{d})$. For random graphs this holds (w.h.p.) whenever $d \geq Cn^{2/3}$ for a sufficiently large constant C , but for expander graphs this property need not hold. Recall that $b \leq O(\frac{n}{d})$ in the b -partial coloring from Theorem 1.1 (because $\lambda = O(\sqrt{d})$). Hence the pigeon-hole principle implies that every two free vertices u and v had at least one common neighbor w (common neighbor in the host graph H) that is not free, namely, it is colored. Hence if in the input graph G neither of them have a colored neighbor in the b -partial coloring, it must be that both of them lost their edge to w because of the planted coloring, meaning that u and v have the same color in the planted coloring. Consequently, the set F_0 of all free vertices with no colored neighbor must be monochromatic in the planted coloring. This leads to the following algorithm for legally 3-coloring the free vertices. Guess the color that should be given to the set F_0 . There are only three possibilities for this. Each of the remaining free vertices has at least one colored neighbor, and hence at most two possible colors. Hence we are left with a list-coloring problem with at most two colors per list. This problem can be solved in polynomial time by reduction to 2SAT.

The full proof of Theorem 1.4a appears in Section D.1.

2.5 Hardness for random graphs with adversarial planting

Here we sketch the proof of Theorem 1.4b (hardness for H_R/P_A). The proof plan is similar to that of the proof of Theorem 1.2 (hardness for H_A/P_A , see Section 2.2), but making this plan work is considerably more difficult.

Let us start with the proof plan. Suppose (for the sake of contradiction) that there is a polynomial time 3-coloring algorithm ALG for the planted H_R/P_A model with host graphs coming from $G_{n,p}$, and hence of average degree $d \simeq pn$. We show how ALG could be used to solve NP-hard problems, thus implying P=NP.

Let \mathcal{Q} be a (carefully chosen, a point that we will return to later) class of sparse graphs on which the problem of 3-coloring is NP-hard. As in the proof of Theorem 1.2, we may assume that if a graph in \mathcal{Q} is 3-colorable, all color classes are of the same size.

Given a graph $Q \in \mathcal{Q}$ on $n_1 = n^\epsilon$ vertices (for some small $\epsilon > 0$ to be determined later) for which one wishes to determine 3-colorability, do the following. Construct a random graph Z on $n_2 = n - n^\epsilon$ vertices, distributed like $G_{n_2,p}$. Plant a random balanced 3-coloring in Z , obtaining a graph that we call Z_3 . Now give the graph G that is a disjoint union of Q and Z_3 as input to ALG. If ALG finds a 3-coloring declare Q to be 3-colorable, and else declare Q as not having a 3-coloring.

If Q is not 3-colorable, then clearly ALG cannot 3-color G . What we need to prove is that if Q is 3-colorable, then ALG will indeed find a 3-coloring of G . For this we need to show that the distribution over graphs G constructed in the above manner (we speak of distributions because Z is a random) is the same (up to some small statistical distance) as a distribution that can be generated by an adversary in the H_R/P_A model (otherwise we do not know what ALG would answer given G). The difficulty is that the adversary does not control the host graph (which is random) and its only power is in choosing the planted

coloring. But still, given a random $G_{n,p}$ host graph H , we propose the following three step procedure for the (exponential time) adversary.

1. If Q is not a vertex induced subgraph of H then *fail*, and plant a random 3-coloring in H .
2. Else, pick a random vertex-induced copy of Q in H (note that H could contain more than one copy of Q). Let Z' denote the graph induced on the remaining part of H . Let χ be a balanced 3-coloring of Q . If there are two vertices $u, v \in Q$ with $\chi(u) \neq \chi(v)$ which have a common neighbor $w \in Z'$, then *fail*, and plant a random 3-coloring in H .
3. Else, extend χ to a balanced planted 3-coloring on the whole of H , while taking care that if a vertex $w \in Z'$ has a neighbor $v \in Q$, then $\chi(w) = \chi(v)$. After dropping the monochromatic edges, one gets a graph G' composed of two components: Q , and another component that we call Z'_3 .

What needs to be shown is that the probability (over choice of $H \in_R G_{n,p}$) of failing in either step 1 or 2 is small, and that conditioned on not failing, G' has a distribution similar to that of G (equivalently, Z'_3 has a distribution similar to Z_3).

For the first step not to fail, one needs graphs $Q \in \mathcal{Q}$ to occur in a random $G_{n,p}$ graph by chance rather than by design. This requires average degree $d > n^{1/3}$, as shown by the following proposition (the proof can be found in Section D.4).

Proposition 2.4. *Let \mathcal{Q} be an arbitrary class of graphs. Then either there is a polynomial time algorithm for solving 3-colorability on every graph in \mathcal{Q} , or \mathcal{Q} contains graphs that are unlikely to appear as subgraphs of a random graph from $G_{n,p}$, if $p \leq n^{-\frac{2}{3}}$ (namely, if the average degree is $d \leq n^{\frac{1}{3}}$).*

Moreover, it is not hard to show that if the average degree is too large, namely, $d > n^{\frac{1}{2}}$, the second step is likely to fail (there are likely to be pairs of vertices in Q that have common neighbors in Z'). Hence we restrict attention to average degrees satisfying $n^{\frac{1}{3}} < d < n^{\frac{1}{2}-\epsilon}$. Consequently, the class of 4-regular graphs cannot serve as the NP-hard class \mathcal{Q} (in contrast to the proof of Theorem 1.2), because any particular 4-regular graph is expected not to be a subgraph of a random graph of average degree below \sqrt{n} . Given the above, we choose \mathcal{Q} to be the class of *balanced* graphs of average degree 3.75. (The choice of 3.75 is for convenience. With extra work in the proof of Lemma 2.6, one can replace 3.75 by any constant larger than $10/3$ and consequently decrease the value of δ_0 in Lemma 2.7 to any constant above $2/5$.)

Definition 2.5. A graph Q is *balanced* if no subgraph of Q has average degree larger than the average degree of Q .

This choice of \mathcal{Q} is justified by the combination of Lemmas 2.6 and 2.7.

Lemma 2.6. *The problem of 3-coloring is NP-hard on the class of balanced graphs of average degree 3.75.*

Lemma 2.7. *Let Q be an arbitrary balanced graph on n^ϵ vertices and of average degree 3.75. Then a random graph of degree $d > n^{\delta_0}$ is likely to contain Q as a vertex induced subgraph, for $\delta_0 = \frac{7+16\epsilon}{15}$.*

The above implies that if \mathcal{Q} is the class of balanced graphs of average degree 3.75 and if $n^{\delta_0} < d < n^{\frac{1}{2}-\epsilon}$ (this interval is nonempty for $\epsilon < \frac{1}{62}$), then the adversary is likely not to fail in steps 1 and 2. What remains to prove is that the distribution over Z'_3 is statistically close to the distribution over Z_3 . (It may seem strange that this is needed, given that \mathcal{Q} is isolated from Z_3/Z'_3 . However, as Z'_3 is constructed by a procedure that depends on \mathcal{Q} and is not known to run in polynomial time, we need to argue that it does not contain information that can be used by a 3-coloring algorithm for \mathcal{Q} . Being statistically close to the polynomial time constructible Z_3 serves this purpose.) Proving this claim is nontrivial. Our proof for this claim is partly inspired by work of [22] that showed that the distribution of graphs from $G_{n, \frac{1}{2}}$ in which one plants a random clique of size $\frac{3}{2} \log n$ is statistically close to the $G_{n, \frac{1}{2}}$ distribution (with no planting).

Full proofs for this section appear in Section D.2 (see Theorem D.13).

2.6 Some open questions

An intriguing question left open by Theorem 1.4b is the following:

Is there a polynomial time 3-coloring algorithm for the H_R/P_A model at average degrees significantly below $n^{\frac{1}{3}}$?

We believe that the hosted coloring framework (and similar frameworks for other NP-hard problems) is a fertile ground for further research. A fundamental question is whether the choice of host graph matters at all. Specifically:

Does Theorem 1.3 (existence of 3-coloring algorithms for H_A/P_R) continue to hold if the class of host graphs is that of all regular graphs (with no restriction on λ)?

The answer to the above question is positive for host graphs of minimum degree linear in n (left as exercise to the reader), and it will be very surprising if the answer is positive in general.

Acknowledgements

Work supported in part by the Israel Science Foundation (grant No. 621/12) and by the I-CORE Program of the Planning and Budgeting Committee and the Israel Science Foundation (grant No. 4/11).

References

- [1] Noga Alon and Fan RK Chung. Explicit construction of linear sized tolerant networks. *Annals of Discrete Mathematics*, 38:15–19, 1988. 8, 56
- [2] Noga Alon and Nabil Kahale. A spectral technique for coloring random 3-colorable graphs. *SIAM Journal on Computing*, 26(6):1733–1748, 1997. 2, 4, 6, 7, 8, 9, 15, 24, 25
- [3] Noga Alon and Joel H Spencer. *The probabilistic method*. John Wiley & Sons, 2004. 39

- [4] Alina Arbitman. Planted random 3SAT with a small fraction of 1-clauses. *MSC Thesis, Weizmann Institute*, <http://www.wisdom.weizmann.ac.il/~feige/TechnicalReports/AlinaArbitmanThesis.pdf>, 2012. 7
- [5] Sanjeev Arora and Rong Ge. New tools for graph coloring. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 1–12. Springer, 2011. 6
- [6] Rajendra Bhatia. *Matrix analysis*, volume 169. Springer Science & Business Media, 2013. 36
- [7] Avrim Blum and Joel Spencer. Coloring random and semi-random k -colorable graphs. *Journal of Algorithms*, 19(2):204–234, September 1995. 2, 6
- [8] Ravi B Boppana. Eigenvalues and graph bisection: An average-case analysis. In *Foundations of Computer Science, 1987., 28th Annual Symposium on*, pages 280–285. IEEE, 1987. 6
- [9] Rowland Leonard Brooks. On colouring the nodes of a network. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 37, pages 194–197. Cambridge Univ Press, 1941. 47
- [10] Herman Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *The Annals of Mathematical Statistics*, pages 493–507, 1952. 55
- [11] Roei David. Finding planted k -coloring in vector k -colorable graphs. *MSC Thesis, Weizmann Institute*, <http://www.wisdom.weizmann.ac.il/~feige/TechnicalReports/RoeiDavidThesis.pdf>, 2013. 7
- [12] P Erdos and A Renyi. On random graphs i. *Publ. Math. Debrecen*, 6:290–297, 1959. 37
- [13] Feige, Langberg, and Schechtman. Graphs with tiny vector chromatic numbers and huge chromatic numbers. *SICOMP: SIAM Journal on Computing*, 33, 2004. 7
- [14] Uriel Feige and Joe Kilian. Heuristics for semirandom graph problems. *Journal of Computer and System Sciences*, 63(4):639–671, 2001. 6
- [15] Uriel Feige and Eran Ofek. Spectral techniques applied to sparse random graphs. *Random Structures & Algorithms*, 27(2):251–275, 2005. 3, 37, 52
- [16] Abraham Flaxman. A spectral technique for random satisfiable 3CNF formulas. In *Proceedings of the fourteenth annual ACM-SIAM symposium on Discrete algorithms*, pages 357–363. Society for Industrial and Applied Mathematics, 2003. 6
- [17] Joel Friedman, Jeff Kahn, and Endre Szemerédi. On the second eigenvalue of random regular graphs. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 587–598. ACM, 1989. 3, 37, 52
- [18] Zoltán Füredi and János Komlós. The eigenvalues of random symmetric matrices. *Combinatorica*, 1(3):233–241, 1981. 3, 37, 52

- [19] Michael R Garey, David S. Johnson, and Larry Stockmeyer. Some simplified NP-complete graph problems. *Theoretical computer science*, 1(3):237–267, 1976. 2, 35, 41
- [20] Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 43(4):439–561, 2006. 3
- [21] Roger A Horn and Charles R Johnson. *Matrix analysis*. Cambridge university press, 2012. 56
- [22] Ari Juels and Marcus Peinado. Hiding cliques for cryptographic security. In *Des. Codes Cryptogr*, pages 678–684. ACM, 1998. 12, 44
- [23] David Karger, Rajeev Motwani, and Madhu Sudan. Approximate graph coloring by semidefinite programming. *Journal of the ACM (JACM)*, 45(2):246–265, 1998. 7
- [24] Richard M. Karp. Reducibility among combinatorial problems. In *Complexity of Computer Computations*, pages 85–103, 1972. 2
- [25] Ken-ichi Kawarabayashi and Mikkel Thorup. Coloring 3-colorable graphs with $o(n^{1/5})$ colors. pages 458–469, 2014. 2
- [26] Alexandra Kolla, Konstantin Makarychev, and Yury Makarychev. How to play unique games against a semi-random adversary: Study of semi-random models of unique games. In *IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS), 2011*, pages 443–452. IEEE, 2011. 6
- [27] Michael Krivelevich, Daniel Reichman, and Wojciech Samotij. Smoothed analysis on connected graphs. *SIAM Journal on Discrete Mathematics*, 29(3):1654–1669, 2015. 31
- [28] László Lovász. Three short proofs in graph theory. *Journal of Combinatorial Theory, Series B*, 19(3):269–271, 1975. 47
- [29] Konstantin Makarychev, Yury Makarychev, and Aravindan Vijayaraghavan. Approximation algorithms for semi-random partitioning problems. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 367–384. ACM, 2012. 6
- [30] Konstantin Makarychev, Yury Makarychev, and Aravindan Vijayaraghavan. Constant factor approximation for balanced cut in the pie model. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 41–49. ACM, 2014. 6
- [31] Colin McDiarmid. On the method of bounded differences. *Surveys in combinatorics*, 141(1):148–188, 1989. 55
- [32] Frank McSherry. Spectral partitioning of random graphs. In *Foundations of Computer Science, 2001. Proceedings. 42nd IEEE Symposium on*, pages 529–537. IEEE, 2001. 6
- [33] A. Nilli. On the second eigenvalue of a graph. *Discrete Mathematics*, 91(2):207–210, 1991. 3

- [34] Daniel A Spielman and Shang-Hua Teng. Smoothed analysis of algorithms: Why the simplex algorithm usually takes polynomial time. *Journal of the ACM (JACM)*, 51(3):385–463, 2004. 6
- [35] Salil P Vadhan. *Pseudorandomness*. Now, 2012. 56

A Organization of the technical sections

The technical sections are organized in an order somewhat different than that of the main text. Specifically, we consider the models H_A/P_R , H_A/P_A and H_R/P_A one by one (the model H_R/P_R need not be considered because it is handled in [2]). Consequently, different parts of the proof of Theorem 1.1 appear in different sections.

Section B contains all proofs for the model with an adversarial expander host graph and a random planted coloring, namely, H_A/P_R . It is divided into subsections as follows. Section B.1 analyzes the spectrum of an expander graph with a random planted coloring (this relates to Lemma 2.1 in the H_A/P_R model). Specifically, we show a generalization to Proposition 2.1 in [2], see Theorem B.1. Section B.2 presents in a unified manner the algorithm that 3-color graphs in the H_A/P_R model, combining into one algorithm the parts of Theorem 1.1 related to the H_A/P_R model and Theorem 1.3. The proofs related to this algorithm are presented in Section B.3. Our first step is to show (using Theorem B.1) that a spectral clustering algorithm gives a good approximation to the planted coloring. We provide a new spectral clustering algorithm that is based on sampling within the lowest eigenvectors, leading to improved efficiency (in the case of random k -color planting, the algorithm’s expected running time is roughly $e^k n$ as opposed to n^k in [2]) – see Lemma B.16. In the rest of the section we show how to attain a full legal coloring. Our proofs of Lemmas 2.2 and 2.3 are formulated in terms of a parameter sb that upper bounds the number of vertices with “bad statistics”. The actual value of this parameter depends on whether the planted coloring is random (as in Lemma B.14) or adversarial, but other than that the proofs do not assume that the planting is random. Instead they use the expander mixing lemma. The place where we do use the randomness of the planted coloring is in Lemma B.21 that shows that after the safe recoloring stage the remaining free vertices break up into connected components of size $O\left(\frac{\lambda^2}{d^2} \log n\right)$. (This bound is smaller and hence better than the bound of $\log_d n$ in [2]). The analysis of Lemma B.21 is tailored to the randomness of the planted coloring and to the recoloring step that we added.

Section C contains all proofs for the model with an adversarial expander host graph and an adversarial planted balanced coloring, namely, H_A/P_A . Section C.1 shows how to obtain a b -partial coloring for graphs in the H_A/P_A model (Theorem 1.1). For H_A/P_A , Lemma C.4 replaces Theorem B.1 in the spectral analysis. Section C.2 proves Theorem 1.2 (hardness result for the H_A/P_A model).

Section D contains all proofs for the model with a random host graph and an adversarial planted balanced coloring, namely, H_R/P_A . Section D.1 proves Theorem 1.4a (a 3-coloring algorithm for H_R/P_A). Section D.2 proves Theorem 1.4b (hardness for H_R/P_A).

Section E discusses extensions of our results to $k > 3$. The main new proof there is in Section E.1 which shows a hardness result for k -coloring in the H_R/P_A model (for $k > 3$). The range of degrees for this proof is not upper bounded (unlike the case of 3-coloring in Theorem 1.4). This implies that Theorem 1.4a does not extend to $k \geq 4$, unless $P = NP$.

Section F demonstrates (within our context of planted models) that even if a graph G contains a vertex induced subgraph that is difficult to 3-color, this by itself does not imply that it is difficult to 3-color G . It is useful to bear this fact in mind when trying to prove NP-hardness results within our framework.

Section G contains some useful facts (Chernoff bounds, the expander mixing lemma, and more) that are used throughout this manuscript.

A.1 Extended notations and definitions

Given a graph G we denote its adjacency matrix by A_G . We denote A_G 's normalized eigenvectors by $e_1(G), e_2(G), \dots, e_n(G)$ and the corresponding real eigenvalues by $\lambda_1(G) \geq \lambda_2(G) \geq \dots \geq \lambda_n(G)$. We denote by $V(G)$ the vertex set of the graph and by $E(G)$ the edge set of the graph. We denote by d_v the degree of $v \in V(G)$. For any $H \subseteq V(G)$ let G_H be the induced sub-graph of G on the vertices of H . Given a vertex $v \in V(G)$ we denote by $N(v)$ the neighborhood of v , excluding v . For a set $S \subseteq V$, $N(S)$ denotes the neighborhood of S , i.e. $N(S) = \cup_{s \in S} N(s)$ (note that with this definition we can have $S \cap N(S) \neq \emptyset$). For $S, T \subseteq V(G)$, $E_G(S, T)$ denotes the number of edges between S and T in G . If S, T are not disjoint then the edges in the induced sub-graph of $S \cap T$ are counted twice.

Given a vector $\vec{v} \in \mathbb{R}^n$ we denote by $(\vec{v})_i$ the i -th coordinate of \vec{v} .

Definition A.1. [Graph Sparsity]. Let $G = (V, E)$ be a d -regular graph, $S \subseteq V$. The sparsity of S is

$$\phi(S) := \frac{E_G(S, V - S)}{\frac{d}{n} |S| |V - S|},$$

and the sparsity of the graph G is

$$\phi(G) := \min_{S \subseteq V} \phi(S)$$

Definition A.2. [Vertex expander]. A graph G is an (s, α) vertex expander if for every $S \subseteq V(G)$ of size at most s it holds that the neighborhood of S is of size at least $\alpha |S|$.

Definition A.3. [λ -expander]. A graph G is a λ -expander if $\max(\lambda_2(G), |\lambda_n(G)|) \leq \lambda$.

Definition A.4. Let $P_3(G) := (V_1 \cup V_2 \cup V_3, E')$ be the following random graph:

1. Each vertex of V is in each V_i with probability $\frac{1}{3}$, independently over all the vertices.
2. Each edge of $(u, v) \in E$ is in E' iff $u \in V_i$ and $v \in V_j$ for $i \neq j$.

Definition A.5. For $v \in V_i$ we say v is colored with i . We call this coloring of $P_3(G)$ the planted coloring.

Definition A.6. Given $P_3(G)$ and $i \in \{1, 2, 3\}$ we denote by G_i the subgraph of G induced on the vertex set V_i .

Definition A.7. Define the following vectors in \mathbb{R}^n (where i ranges from 1 to n).

$$\left(\vec{1}_n\right)_i = 1, \left(\vec{p}_1\right)_i := \begin{cases} 1 & v_i \in V_1 \\ 0 & v_i \notin V_1 \end{cases}, \left(\vec{p}_2\right)_i := \begin{cases} 1 & v_i \in V_2 \\ 0 & v_i \notin V_2 \end{cases}, \left(\vec{p}_3\right)_i := \begin{cases} 1 & v_i \in V_3 \\ 0 & v_i \notin V_3 \end{cases},$$

$$(\vec{x})_i := \begin{cases} 2 & v_i \in V_1 \\ -1 & v_i \in V_2 \\ -1 & v_i \in V_3 \end{cases} \text{ and } (\vec{y})_i := \begin{cases} 0 & v_i \in V_1 \\ 1 & v_i \in V_2 \\ -1 & v_i \in V_3 \end{cases}.$$

We denote by \bar{v} a normalized vector, i.e., $\bar{x} := \vec{x}/|\vec{x}|_2$.

B Adversarial host and random planting, H_A/P_R

Section B contains the proofs for the model with an adversarial expander host graph and a random planted coloring, namely, H_A/P_R . Section B.1 analyzes the spectrum of an expander graph with a random planted coloring (this relates to Lemma 2.1 in the H_A/P_R model). Section B.2 presents in a unified manner the algorithm that 3-colors graphs in the H_A/P_R model, combining into one algorithm the parts of Theorem 1.1 related to the H_A/P_R model and Theorem 1.3. The proofs related to this algorithm are presented in Section B.3.

B.1 The eigenvalues of an expander with a random planted coloring

Theorem B.1. *Let G be a d regular λ -expander, where $\lambda \leq (\frac{1}{3} - \epsilon)d$ (for $0 < \epsilon < \frac{1}{3}$). Let $G' = P_3(G)$ (the graph G after a random 3-color planting). Then with high probability the following holds.*

1. *The eigenvalues of G' have the following spectrum.*

- (a) $\lambda_1(G') \geq (1 - 2^{-\Omega(d)}) \frac{2}{3}d$.
- (b) $\lambda_n(G') \leq \lambda_{n-1}(G') \leq -\frac{1}{3}d \left(1 - \frac{3}{\sqrt{d}}\right)$.
- (c) $|\lambda_i(G')| \leq 2\lambda + O(\sqrt{d})$ for all $2 \leq i \leq n-2$.

2. *The following vectors exist.*

- (a) $\vec{\epsilon}_{\bar{x}}$ such that $\|\vec{\epsilon}_{\bar{x}}\|_2 = O\left(\frac{1}{\sqrt{d}}\right)$ and $\bar{x} + \vec{\epsilon}_{\bar{x}} \in \text{span}\left(\{e_i(G')\}_{i \in \{n-1, n\}}\right)$.
- (b) $\vec{\epsilon}_{\bar{y}}$ such that $\|\vec{\epsilon}_{\bar{y}}\|_2 = O\left(\frac{1}{\sqrt{d}}\right)$ and $\bar{y} + \vec{\epsilon}_{\bar{y}} \in \text{span}\left(\{e_i(G')\}_{i \in \{n-1, n\}}\right)$.

In the rest of this section we prove Theorem B.1.

Lemma B.2. *Let G' be as in Theorem B.1. With high probability the vectors $\bar{1}, \bar{x}, \bar{y}$, see definition A.7, satisfy $A_{G'}\bar{x} = (-\frac{1}{3}d)\bar{x} + \vec{\delta}_{\bar{x}}$, $A_{G'}\bar{y} = (-\frac{1}{3}d)\bar{y} + \vec{\delta}_{\bar{y}}$ and $A_{G'}\bar{1} = (\frac{2}{3}d)\bar{1} + \vec{\delta}_{\bar{1}}$.*

Here $\vec{\delta}_{\bar{x}}, \vec{\delta}_{\bar{y}}, \vec{\delta}_{\bar{1}}$ are vectors with ℓ_2 norm of at most \sqrt{d} .

Proof. We prove the lemma for $\bar{1}, \vec{\delta}_{\bar{1}}$ (the other cases have a similar proof). We assume $d = o(\sqrt{n})$ since for large values of d one can show a different proof using the union bound, details omitted.

Consider the vector $A_{G'}\bar{1} - (\frac{2}{3}d)\bar{1}$. We give an upper bound (that holds with high probability) on the sum of squares of its coordinates.

Let $i \in [n]$. As $\mathbb{E} \left[\left(\left(A_{G'} \bar{\mathbf{1}} \right)_i - \frac{2}{3}d \right)^2 \right]$ can be seen as the variance of d independent Bernoulli variables, (each with variance $\frac{2}{3} \left(1 - \frac{2}{3} \right)$), it holds that

$$\mathbb{E} \left[\sum_i \left(\left(A_{G'} \bar{\mathbf{1}} \right)_i - \frac{2}{3}d \right)^2 \right] = n \mathbb{E} \left[\left(\left(A_{G'} \bar{\mathbf{1}} \right)_1 - \frac{2}{3}d \right)^2 \right] = nd \frac{2}{9}.$$

Let x_i be a random variable that indicates the color of a the i -th vertex of the graph. Set $f = \sum_i \left(\left(A_{G'} \bar{\mathbf{1}} \right)_i - \frac{2}{3}d \right)^2$ to be a function of x_i 's. Consider the terms of f that are effected by a particular random variable x_i . One such term is $\left(\left(A_{G'} \bar{\mathbf{1}} \right)_i - \frac{2}{3}d \right)^2$. Its value is bounded between 0 and $\frac{4}{9}d^2$, and hence x_i can effect it by at most $\frac{4}{9}d^2$. Other terms that are affected by x_i are $\left(\left(A_{G'} \bar{\mathbf{1}} \right)_j - \frac{2}{3}d \right)^2$, where j ranges over neighbors of i in G . As i has degree d in G , there are d such terms. For each neighbor j , the value $\left(A_{G'} \bar{\mathbf{1}} \right)_j - \frac{2}{3}d$ (which lies between $\frac{d}{3}$ and $-\frac{2d}{3}$) changes by at most 1 by x_i , implying that $\left(\left(A_{G'} \bar{\mathbf{1}} \right)_j - \frac{2}{3}d \right)^2$ changes by at most $\frac{2d}{3}$. Overall, the effect of x_i on $\sum_{j \in N(i)} \left(\left(A_{G'} \bar{\mathbf{1}} \right)_j - \frac{2}{3}d \right)^2$ is at most $\frac{2d^2}{3}$. As x_i does not effect any other term in f , its total effect on f is at most $\frac{2d^2}{3} + \frac{4d^2}{9} = \frac{10d^2}{9} < 2d^2$.

By the above we can apply McDiarmid's Inequality (Theorem G.2) with $c = 2d^2$ to deduce

$$\Pr \left[\left| \sum_i \left(\left(A_{G'} \bar{\mathbf{1}} \right)_i - \frac{2}{3}d \right)^2 - nd \frac{2}{9} \right| \geq c_1 nd \right] \leq 2 \exp \left(-\Omega \left(\frac{n}{d^2} \right) \right),$$

where c_1 is a constant, say $\frac{1}{9}$. Overall, with high probability, $\left\| A_{G'} \bar{\mathbf{1}} - \left(\frac{2}{3}d \right) \bar{\mathbf{1}} \right\|_2 \leq \sqrt{nd}$ and thus, by normalization, $\left\| A_{G'} \bar{\mathbf{1}} - \left(\frac{2}{3}d \right) \bar{\mathbf{1}} \right\|_2 \leq \sqrt{d}$. □

Lemma B.3. *Let A be a symmetric matrix of order n with eigenvalues $\lambda_1, \dots, \lambda_n$ and associated eigenvectors v_1, \dots, v_n . For a unit vector \bar{u} and scalar λ , suppose that $A\bar{u} = \lambda\bar{u} + \vec{\epsilon}$, where the ℓ_2 norm of $\vec{\epsilon}$ is at most ϵ .*

Let $S_\delta \subset \{1, \dots, n\}$ be the set of those indices i for which $|\lambda_i - \lambda| \leq \delta$. Then there exists a vector $\vec{\epsilon}_{\bar{u}}$ such that $\bar{u} + \vec{\epsilon}_{\bar{u}}$ is a vector spanned by the eigenvectors associated with S_δ and $\|\vec{\epsilon}_{\bar{u}}\|_2 \leq \frac{\epsilon}{\delta}$.

Proof. Write $\bar{u} = \sum_{i=1}^n \alpha_i v_i$, with $\sum (\alpha_i)^2 = 1$. Then

$$A\bar{u} = \sum \lambda_i \alpha_i v_i = \lambda \bar{u} + \sum (\lambda_i - \lambda) \alpha_i v_i.$$

Hence $\vec{\epsilon} = \sum (\lambda_i - \lambda) \alpha_i v_i$, implying $\sum (\lambda_i - \lambda)^2 (\alpha_i)^2 \leq \epsilon^2$. By averaging, it follows that $\sum_{i \notin S_\delta} (\alpha_i)^2 < \frac{\epsilon^2}{\delta^2}$. Let $\vec{\epsilon}_{\bar{u}} := -\sum_{i \notin S_\delta} \alpha_i v_i$. □

Lemma B.4. Let G' be as in Theorem B.1, and let the unite vectors $\bar{1}, \bar{x}, \bar{y}$ be as in definition A.7. Define $S_\delta(x) \subset \{1, \dots, n\}$ to be the set of those indices i for which $|\lambda(G')_i - (x)| \leq \delta$. The following vectors exist with high probability.

- $\vec{\epsilon}_{\bar{1}}$ such that $\|\vec{\epsilon}_{\bar{1}}\|_2 \leq \frac{\sqrt{d}}{\delta}$ and $\bar{1} + \vec{\epsilon}_{\bar{1}} \in \text{span}\left(\{e_i(G')\}_{i \in S_\delta(\frac{2}{3}d)}\right)$.
- $\vec{\epsilon}_{\bar{x}}$ such that $\|\vec{\epsilon}_{\bar{x}}\|_2 \leq \frac{\sqrt{d}}{\delta}$ and $\bar{x} + \vec{\epsilon}_{\bar{x}} \in \text{span}\left(\{e_i(G')\}_{i \in S_\delta(-\frac{1}{3}d)}\right)$.
- $\vec{\epsilon}_{\bar{y}}$ such that $\|\vec{\epsilon}_{\bar{y}}\|_2 \leq \frac{\sqrt{d}}{\delta}$ and $\bar{y} + \vec{\epsilon}_{\bar{y}} \in \text{span}\left(\{e_i(G')\}_{i \in S_\delta(-\frac{1}{3}d)}\right)$.

Proof. By Lemma B.2 and Lemma B.3 the statement of the lemma holds with high probability. \square

Lemma B.5. Let G be a d -regular λ -expander. Let G_1 be a random induced graph of G where each vertex of G is in G_1 independently with probability $\frac{1}{3}$. With high probability the vector $\bar{1}_{|V(G_1)|}$, see definition A.7, satisfies $A_{G_1} \bar{1}_{|V(G_1)|} = \left(\frac{1}{3}d\right) \bar{1}_{|V(G_1)|} + \vec{\delta}_{\bar{1}}$.

Here $\vec{\delta}_{\bar{1}}$ is a vector with ℓ_2 norm of at most \sqrt{d} .

Proof. The proof is similar to the proof of Lemma B.2. \square

Lemma B.6. Let G be a d -regular λ -expander. Let G_1 be a random induced graph of G where each vertex of $V(G)$ is in $V(G_1)$ independently with probability $\frac{1}{3}$. It holds that G_1 is a λ -expander.

Proof. The proof follows by Cauchy interlacing theorem, (Theorem G.3). \square

Lemma B.7. Let G' be as in Theorem B.1, the vector \bar{p}_1 be as in Definition A.7, and $\delta \leq \frac{d}{3} - \sqrt{d} - \lambda$. The following vector exists with high probability.

- $\vec{\epsilon}_{\bar{p}_1}$ such that $\|\vec{\epsilon}_{\bar{p}_1}\|_2 \leq \frac{\sqrt{d}}{\delta}$ and $\bar{p}_1 + \vec{\epsilon}_{\bar{p}_1} \in \text{span}(\{e_1(G_1)\})$.

Proof. Let $S_\delta(G_1)$ be the set of those indices i for which $|\lambda(G_1)_i - \frac{1}{3}d| \leq \delta$. By Lemma B.6 it follows that $S_\delta(G_1) = \{1\}$. By Lemma B.5 and Lemma B.3 the following vector exists with high probability. $\vec{\epsilon}_{\bar{p}_1}$ such that $\|\vec{\epsilon}_{\bar{p}_1}\|_2 \leq \frac{\sqrt{d}}{\delta}$ and

$$\bar{p}_1 + \vec{\epsilon}_{\bar{p}_1} \in \text{span}\left(\{e_i(G_1)\}_{i \in S_\delta(G_1)}\right) = \text{span}(\{e_1(G_1)\}) .$$

\square

Now we prove Theorem B.1.

Proof. [Theorem B.1]. Let $\delta = \frac{\epsilon}{2}d$ and $\vec{\epsilon}_{\bar{1}}, \vec{\epsilon}_{\bar{x}}, \vec{\epsilon}_{\bar{y}}, \vec{\epsilon}_{\bar{p}_1}$ be the vectors that were defined in Lemma B.4 and Lemma B.7. Define $S_\delta \subset \{1, \dots, n\}$ to be the set of those indices i for which either $|\lambda(G')_i - (-\frac{1}{3}d)| \leq \delta$ or $|\lambda(G')_i - (\frac{2}{3}d)| \leq \delta$. We conclude the proof by the following two claims.

Claim B.8. For $\{i\} \notin S_\delta$ it holds that $|\lambda(G')_i| \leq 2\lambda + O\left(\frac{d^{1.5}}{\delta}\right)$.

Proof. Let A'_{G_j} be the adjacency matrix of the induced sub-graph on j -colored vertices, i.e.,

$$(A'_{G_j})_{i,k} = \begin{cases} (A_{G_j})_{i,k} & v_i \in V(G_j), v_k \in V(G_j) \\ 0 & \text{Otherwise.} \end{cases}.$$

Let

$$(e_i(G_j)')_k = \begin{cases} (e_i(G_j))_k & v_k \in V(G_j) \\ 0 & \text{Otherwise.} \end{cases}.$$

For brevity, the last two notation are used without the apostrophe. Note that $A_{G'} = A_G - (\sum_{j=1}^3 A_{G_j})$.

Let $i \notin S_\delta$, by the triangle inequality it holds that,

$$\|A_{G'} e_i(G')\|_2 \leq \|A_G e_i(G')\|_2 + \left\| \sum_{j=1}^3 A_{G_j} e_i(G') \right\|_2. \quad (1)$$

First we show $\|A_G e_i(G')\|_2 \leq \lambda + O\left(\frac{d^{1.5}}{\delta}\right)$.

$$\begin{aligned} \|A_G e_i(G')\|_2^2 &= \sum_{j=1}^n \lambda_j^2(G) \langle e_i(G'), e_j(G) \rangle^2 \\ &= \lambda_1^2(G) \langle e_i(G'), e_1(G) \rangle^2 + \sum_{j=2}^n \lambda_j^2(G) \langle e_i(G'), e_j(G) \rangle^2 \\ &\leq \lambda_1^2(G) \langle e_i(G'), e_1(G) \rangle^2 + \lambda^2. \end{aligned}$$

The last inequality follows since G is a λ -expander.

$$\begin{aligned} &= d^2 \langle e_i(G'), \bar{1} \rangle^2 + \lambda^2 \\ &= d^2 \langle e_i(G'), \bar{1} + \bar{\epsilon}_1 - \bar{\epsilon}_1 \rangle^2 + \lambda^2 \\ &= d^2 \langle e_i(G'), \bar{\epsilon}_1 \rangle^2 + \lambda^2 \end{aligned} \quad (2)$$

The last equality holds since $\bar{1} + \bar{\epsilon}_1$ and $e_i(G')$ are orthogonal.

$$\leq d^2 \|\bar{\epsilon}_1\|_2^2 + \lambda^2$$

The last inequality follows by Cauchy–Schwarz inequality and now we use the assumption on $\|\bar{\epsilon}_1\|_2$.

$$\leq d^2 \left(\frac{\sqrt{d}}{\delta} \right)^2 + \lambda^2.$$

We left to show that with high probability $\left\| \sum_{j=1}^3 A_{G_j} e_i(G') \right\|_2 \leq \lambda + O\left(\frac{d^{1.5}}{\delta}\right)$. Denote by n_j the G_j 's number of vertices. Note that $\sum_{j=1}^3 A_{G_j}$ is the adjacency matrix of a graph with at least three connected components, $(\{G_j\}_{j \in \{1,2,3\}})$, thus $\{e_i(G_j) \mid 1 \leq i \leq n_j, j \in \{1,2,3\}\}$ are the eigenvectors of $\sum_{j=1}^3 A_{G_j}$, (up to appropriate padding with zeros).

$$\begin{aligned}
\left\| \sum_{j=1}^3 A_{G_j} e_i(G') \right\|_2^2 &= \sum_{j=1}^3 \sum_{k=1}^{n_j} \lambda_k^2(G_j) \langle e_i(G'), e_k(G_j) \rangle^2 \\
&= \sum_{j=1}^3 \lambda_1^2(G_j) \langle e_i(G'), e_1(G_j) \rangle^2 + \sum_{j=1}^3 \sum_{j=2}^{n_j} \lambda_j^2(G_1) \langle e_i(G'), e_j(G_1) \rangle^2 \\
&\leq d^2 \sum_{j=1}^3 \langle e_i(G'), e_1(G_j) \rangle^2 + \lambda^2
\end{aligned}$$

The last inequality follows since by Lemma B.6 it follows that $\{G_j\}_{j \in \{1,2,3\}}$ are λ -expanders with degree at most d .

$$\begin{aligned}
&= d^2 \sum_{j=1}^3 \langle e_i(G'), \bar{p}_j + \bar{\epsilon}_{\bar{p}_j} \rangle^2 + \lambda^2 = d^2 \sum_{j=1}^3 (\langle e_i(G'), \bar{\epsilon}_{\bar{p}_j} \rangle + \langle e_i(G'), \bar{p}_j \rangle)^2 + \lambda^2 \\
&\leq d^2 \sum_{j=1}^3 (\|\bar{\epsilon}_{\bar{p}_j}\|_2 + \langle e_i(G'), \bar{p}_j \rangle)^2 + \lambda^2
\end{aligned}$$

The last inequality follows by Cauchy–Schwarz inequality.

$$\leq d^2 \sum_{j=1}^3 \left(\frac{\sqrt{d}}{\delta} + \langle e_i(G'), \bar{p}_j \rangle \right)^2 + \lambda^2$$

The last inequality follows by the assumption on $|\bar{\epsilon}_{\bar{p}_1}|_2$.

$$= d^2 \sum_{j=1}^3 \left(\frac{\sqrt{d}}{\delta} + \langle e_i(G'), c_1^j \bar{1} + c_2^j \bar{x} + c_3^j \bar{y} \rangle \right)^2 + \lambda^2$$

With high probability $\{c_k^j\}_{k,j \in \{1,2,3\}}$ are universal constants. To see that such constants exist with high probability note that for example $\bar{p}_1 = \frac{1}{3}\bar{1} + \frac{1}{3}\bar{x}$, (In general $\bar{1}, \bar{x}, \bar{y}$ spans $\bar{p}_1, \bar{p}_2, \bar{p}_3$ using universal constants), thus by normalization $\bar{p}_1 = \frac{1}{3\sqrt{|\bar{V}_1|}}\bar{1} + \frac{1}{\sqrt{|\bar{V}_1|}}\bar{x} = \frac{\sqrt{n}}{3\sqrt{|\bar{V}_1|}}\bar{1} + \frac{\|\bar{x}\|_2}{\sqrt{|\bar{V}_1|}}\bar{x}$ and with high probability $\frac{\sqrt{n}}{3\sqrt{|\bar{V}_1|}}, \frac{\|\bar{x}\|_2}{\sqrt{|\bar{V}_1|}}$ are constants.

$$\begin{aligned}
&= d^2 \sum_{j=1}^3 \left(\frac{\sqrt{d}}{\delta} + \langle e_i(G'), c_1^j (\bar{1} + \bar{\epsilon}_{\bar{1}} - \bar{\epsilon}_{\bar{1}}) + c_2^j (\bar{x} + \bar{\epsilon}_{\bar{x}} - \bar{\epsilon}_{\bar{x}}) + c_3^j (\bar{y} + \bar{\epsilon}_{\bar{y}} - \bar{\epsilon}_{\bar{y}}) \rangle \right)^2 + \lambda^2 \\
&= d^2 \sum_{j=1}^3 \left(\frac{\sqrt{d}}{\delta} + \langle e_i(G'), c_1^j (-\bar{\epsilon}_{\bar{1}}) + c_2^j (-\bar{\epsilon}_{\bar{x}}) + c_3^j (-\bar{\epsilon}_{\bar{y}}) \rangle \right)^2 + \lambda^2 \tag{3}
\end{aligned}$$

The last equality holds since $\bar{1} + \vec{\epsilon}_1, \bar{x} + \vec{\epsilon}_x, \bar{y} + \vec{\epsilon}_y$ are orthogonal to $e_i(G')$.

$$\leq d^2 \sum_{j=1}^3 \left(\frac{\sqrt{d}}{\delta} + \left(\sum_{k=1}^3 |c_k^j| \right) \left(\frac{\sqrt{d}}{\delta} \right) \right)^2 + \lambda^2 = O\left(\frac{d^3}{\delta^2}\right) + \lambda^2$$

The last inequality follows by Cauchy–Schwarz inequality and the assumption on $\|\vec{\epsilon}_1\|_2, \|\vec{\epsilon}_x\|_2, \|\vec{\epsilon}_y\|_2$. \square

Claim B.9. $|S_\delta| = 3$.

Proof. Clearly $\bar{1} + \vec{\epsilon}_1, \bar{x} + \vec{\epsilon}_x, \bar{y} + \vec{\epsilon}_y \in \text{span}(\{e_i(G')\}_{i \in S_\delta})$ and since they are independent, (the vectors $\bar{1}, \bar{x}, \bar{y}$ are nearly orthogonal, adding to them the vectors $\vec{\epsilon}_1, \vec{\epsilon}_x, \vec{\epsilon}_y$, each of small ℓ_2 norm, doesn't change this.), it follows that $|S_\delta| \geq 3$.

Now we show $|S_\delta| = 3$. Let $W = \text{span}\{\bar{1} + \vec{\epsilon}_1, \bar{x} + \vec{\epsilon}_x, \bar{y} + \vec{\epsilon}_y\}$ and let

$$W^\perp := \{v \in \text{span}(\{e_i(G')\}_{i \in S_\delta}) \mid \forall w \in W, \langle w, v \rangle = 0\}.$$

Assume, towards a contradiction, that exists $0 \neq v \in W^\perp$. Note that we can write

$$v = \sum_{i \in S_\delta} \alpha_i e_i(G'),$$

where $\sum_{i \in S_\delta} \alpha_i^2 = 1$. Now we give a lower bound on $\|A_{G'}v\|_2$.

$$\begin{aligned} \|A_{G'}v\|_2^2 &= \langle A_{G'}v, A_{G'}v \rangle \\ &= \left\langle A_{G'} \left(\sum_{i \in S_\delta} \alpha_i e_i(G') \right), A_{G'} \left(\sum_{i \in S_\delta} \alpha_i e_i(G') \right) \right\rangle \\ &= \left\langle \sum_{i \in S_\delta} \lambda_i(G') \alpha_i e_i(G'), \sum_{i \in S_\delta} \lambda_i(G') \alpha_i e_i(G') \right\rangle \\ &= \sum_{i \in S_\delta} \lambda_i^2(G') \alpha_i^2 \\ &\geq \left(\left(\frac{1}{3} - \epsilon \right) d \right)^2 \sum_{i \in S_\delta} \alpha_i^2 = \left(\left(\frac{1}{3} - \epsilon \right) d \right)^2. \end{aligned}$$

The last inequality uses the fact $\delta = \frac{\epsilon}{2}d$. By the triangle inequality at least one of the following is $\left(\frac{1}{3} - \frac{\epsilon}{2}\right)d$:

$\|A_G v\|_2$ and $\left\| \sum_{j=1}^3 A_{G_j} v \right\|_2$, see Equation 1. But applying the proof Claim B.8 shows that $\|A_G v\|_2 = \lambda + O\left(\frac{d^{1.5}}{\delta}\right)$ and $\left\| \sum_{j=1}^3 A_{G_j} v \right\|_2 = \lambda + O\left(\frac{d^{1.5}}{\delta}\right)$, (The only requirement from the vector $e_i(G')$ is to be orthogonal to $\bar{1} + \vec{\epsilon}_1, \bar{x} + \vec{\epsilon}_x, \bar{y} + \vec{\epsilon}_y$, see Equation 2 and Equation 3. $v \in W^\perp$ satisfies these requirements by definition). As $\lambda < \left(\frac{1}{3} - \epsilon\right)d$ and since $\delta = \frac{\epsilon}{2}d$ this is a contradiction (for large enough d). Since $W^\perp = \emptyset$ Claim B.9 follows. \square

By Claim B.8 and Claim B.9 items 1.(a) and 1.(c) of Theorem B.1 hold and $-(1 + \epsilon)\frac{1}{3}d \leq \lambda_n(G') \leq \lambda_{n-1}(G') \leq -(1 - \epsilon)\frac{1}{3}d$. Items 2(a), 2(b) and 2(c) hold with respect to the vectors $\vec{\epsilon}_1, \vec{\epsilon}_x, \vec{\epsilon}_y$ defined above. To establish Item 1.(b) of Theorem B.1 note that by Lemma B.2 and by the Courant-Fischer theorem the following holds with high probability

$$\begin{aligned} \lambda_n(G') \leq \lambda_{n-1}(G') &= \min_{\substack{S \in \mathbb{R}^n \\ \dim(S) = 2}} \max_{v \in S} \frac{v^t A v}{v^t v} \\ &\leq \max_{v \in \text{span}\{\vec{x}, \vec{y}\}} \frac{v^t A v}{v^t v} \\ &\leq -\frac{1}{3}d + \sqrt{d}. \end{aligned}$$

□

B.2 Coloring expander graphs with a random planted coloring

Let $G' = (V, E)$ be a graph as in Theorem B.1 (G' is a d -regular λ -expander graph after a random 3-color planting). Theorem B.1 gives some of the mathematical background that is needed in order to analyze our algorithm for 3-coloring G' . The following theorem restates in a combined form the parts of Theorem 1.1 that relate to the H_A/P_R model together with Theorem 1.3.

Theorem B.10. *Let G' be as above and assume $\lambda \leq \frac{d}{24}$ and $d \geq d_{min}$. Here d_{min} is a large enough constant. Algorithm 1, see below, colors G' , with high probability over choice of the random planted 3-coloring.*

First we define the following.

Definition B.11. Given any coloring of G' , say C , denote by $col_C(v)$ the color of vertex v according to C . Denote by P the planted coloring of G' . We say a coloring is partial if some of the vertices are not colored.

Definition B.12. An f -approximated coloring is a 3-coloring of G' , possibly not legal, that agrees with the planted coloring, col_P , of G' on at least $n - f$ vertices.

Throughout this section, let $\epsilon = 0.01$. Consider Algorithm 1.

Algorithm 1 3-Coloring

1. Apply Algorithm 2 (*spectral clustering*) on G' , obtaining a coloring C_1 .
 2. Apply Algorithm 4 (*iterative recoloring*) on (G', C_1) , obtaining a coloring C_2 .
 3. Apply Algorithm 5 (*cautious uncoloring*) on (G', C_2) , obtaining a partial coloring C_3 .
 4. Apply Algorithm 6 (*safe recoloring*) on (G', C_3) , obtaining a partial coloring C_4 .
 5. Apply Algorithm 7 (*brute force*) on (G', C_4) , obtaining a coloring C_5 .
-

Algorithm 3-Coloring is patterned after the algorithm of Alon and Kahale for the random planted model. The main differences between the two *algorithms* are as follows. (There are also differences in the analysis) Similar to [2], Step 1 (spectral 3-clustering) starts with computing the eigenvectors corresponding to the two most negative eigenvalues. However, it differs from [2] in the way C_1 is derived from these eigenvector. Our approach is computationally more efficient, an aspect that is only of minor significance in the context of 3-coloring, but may become significant for k -coloring with $k > 3$. See more details in Section B.3. Another difference is the introduction of Step 4 in our algorithm, that is not present in [2]. The purpose of introducing this additional step is so as to be able to prove the last statement of Lemma B.21. In [2] such a statement could be proved already after Step 3.

B.3 Proof Of Theorem B.10

The following lemmas outline the desired outcome of the respective steps of Algorithm 1 and the proof of Theorem B.10 follows by applying them.

At a high level, one may think of most of our proofs as adaptations (some immediate, some requiring work) of proofs of corresponding statements made in [2]. The exception to this is the proof of the last statement in Lemma 4, which involves ideas not present in [2].

Definition B.13. The set $SB \subseteq V$, statistically bad, is the the following vertex set. $v \in SB$ if for some color class other than $col_P(v)$, v has either has more than $(\frac{1}{3} + \epsilon) d$ neighbors or less than $(\frac{1}{3} - \epsilon) d$ neighbors in that color class.

Lemma B.14. *It holds that $|SB| \leq n2^{-\Omega(d)}$ with high probability over the random planting process.*

Proof. (Of Lemma B.14). In expectation v has $\frac{1}{3}d$ neighbors in G' with original color $k \in \{1, 2, 3\} \setminus \{col_P(v)\}$. By Chernoff bound, Theorem G.1, the probability that a random vertex $v \in G'$ is in SB is at most $2^{-\Omega(d)}$, thus $\mathbb{E}[|SB|] = 2^{-\Omega(d)}n$. If $d \geq \eta_1 \log n$, for a large enough constant η_1 , then, by using the union bound, the probability that $|SB| \geq 1$ is bounded by $2^{-\Omega(d)}n = n^{-\Omega(1)}$. Assume $d \leq \eta_2 \log n$, where η_2 is a constant. $|SB|$ is a function of n independent random variables that were used to create G' . By changing one of the above random variables $|SB|$ changes by at most d . By applying McDiarmid's theorem, Theorem G.2, it follows that for a small enough constant η_2 the following holds,

$$\begin{aligned} \Pr[||SB| - \mathbb{E}[|SB|]| \geq d\mathbb{E}[|SB|]] &\leq 2 \exp\left(-\frac{2(d\mathbb{E}[|SB|])^2}{2nd^2}\right) \\ &= 2^{-\frac{n}{2\Omega(d)}} = 2^{-n^{\Omega(1)}}. \end{aligned}$$

For (constant) large enough values of d and a suitable choice of ϵ we can assure $\eta_1 \leq \eta_2$ and the proof follows. \square

The following lemma is the first step towards coloring G' .

Lemma B.15. *Let G' as above and assume $\lambda \leq \frac{1}{24}d$. Algorithm 4, see below, outputs an $O(|SB|)$ -approximated coloring with high probability over the colors of the vertices in the random planting process.*

Note that if $d = \eta \log n$, (for large enough constant η), then Lemma B.15 implies that Algorithm 4 recovers the original coloring of G' . To prove Lemma B.15 we first show Lemma B.16 and Lemma B.17 presented below.

The next lemma shows, using Theorem B.1, that we can derive an approximated coloring from the eigenvectors $e_{n-1}(G'), e_n(G')$ (see Algorithm 2 below).

Algorithm 2 Spectral Clustering

Input: A graph G' and a positive constant $c \leq \frac{1}{2}$.

1. Calculate $e_{n-1} := e_{n-1}(G')$ and $e_n := e_n(G')$.
2. For every triplet of vertices $v_1, v_2, v_3 \in V(G')$ do
 - (a) Put a vertex $u \in V(G')$ in S_i if it holds that

$$((e_{n-1})_u - (e_{n-1})_{v_i})^2 + ((e_n)_u - (e_n)_{v_i})^2 < \frac{1}{70n}.$$

In case that two deferent sets, S_i and S_j , satisfy the above condition with respect to u , go to Step 2.

- (b) If for every $i = 1, 2, 3$ it holds that $|S_i| \geq (\frac{1}{3} - \frac{1}{d^{2c}})n$ and that $\sum_{i=1}^3 |S_i| \geq n - \theta(\frac{n}{d})$ then output any coloring C of G' that satisfies $col_C(u) = i$ if and only if $u \in S_i$ and stop.
-

Lemma B.16. (Restatement of Lemma 2.1). *Let G' be as above and c be a positive constant. Algorithm 2 runs in polynomial time and if the following vectors exist (recall Definition A.7). $\vec{e}_{\bar{x}}$ such that $\|\vec{e}_{\bar{x}}\|_2 = O(d^{-c})$ and $\bar{x} + \vec{e}_{\bar{x}} \in span(\{e_i(G')\}_{i \in \{n-1, n\}})$. $\vec{e}_{\bar{y}}$ such that $\|\vec{e}_{\bar{y}}\|_2 = O(d^{-c})$ and $\bar{y} + \vec{e}_{\bar{y}} \in span(\{e_i(G')\}_{i \in \{n-1, n\}})$. Then Algorithm 2 outputs an $O(nd^{-2c})$ -approximated coloring.*

By Theorem B.1 we have $\|\vec{e}_{\bar{x}}\|_2 = O(\frac{1}{\sqrt{d}})$ and respectively for y so we can run Algorithm 2 with $c = \frac{1}{2}$.

Proof. [Lemma B.16]. We note that [2] present a different algorithm to get an approximate coloring from the eigenvectors. Our algorithm generalizes more easily to the case of planting k colors. The running time of Step 1 is roughly linear (it is enough to get an approximation of e_{n-1}, e_n). The running time of each iteration in Step 2 is $O(n)$. The number of iteration in Step 2 is $O(n^3)$ (for a planted coloring with k colors it is $O(n^k)$) but choosing at each iteration a random triplet reduces the (expected) number of iterations to be constant (for a planted coloring with k colors it is expected to be less than $\frac{k^k}{k!}$, see details below). Thus for a planted coloring with a constant number of vertices the running time of Algorithm 2 is linear.

Assume, for simplicity, that the planted color classes are balanced. Define the following subset $Good \subseteq V(G')$. A vertex $v \in V(G')$ is in $Good$ if both $((\vec{e}_{\bar{x}})_v)^2 \leq \frac{1}{an}$ and $((\vec{e}_{\bar{y}})_v)^2 \leq \frac{1}{an}$, for $a = 70$. By averaging argument it holds that $|Good| \geq (1 - \frac{2a}{d^{2c}})n$. Note that as

\bar{x}, \bar{y} are almost orthogonal then $\bar{x} + \vec{\epsilon}_{\bar{x}}, \bar{y} + \vec{\epsilon}_{\bar{y}}$ tend to be almost orthogonal as d gets larger. Formally, by the triangle's inequality and the Cauchy-Schwartz inequality it follows that,

$$\begin{aligned} |\langle \bar{x} + \vec{\epsilon}_{\bar{x}}, \bar{y} + \vec{\epsilon}_{\bar{y}} \rangle| &\leq |\langle \bar{x}, \bar{y} \rangle| + |\vec{\epsilon}_{\bar{x}}| + |\vec{\epsilon}_{\bar{y}}| + |\vec{\epsilon}_{\bar{x}}| |\vec{\epsilon}_{\bar{y}}| \\ &= O(d^{-c}) . \end{aligned} \quad (4)$$

Define the vector \tilde{x} to be the second Gram-Schmidt orthonormalization vector with respect to $\bar{y} + \vec{\epsilon}_{\bar{y}}, \bar{x} + \vec{\epsilon}_{\bar{x}}$, i.e.,

$$\tilde{x} = \frac{\bar{x} + \vec{\epsilon}_{\bar{x}} - \langle \bar{x} + \vec{\epsilon}_{\bar{x}}, \bar{y} + \vec{\epsilon}_{\bar{y}} \rangle (\bar{y} + \vec{\epsilon}_{\bar{y}})}{\|\bar{x} + \vec{\epsilon}_{\bar{x}} - \langle \bar{x} + \vec{\epsilon}_{\bar{x}}, \bar{y} + \vec{\epsilon}_{\bar{y}} \rangle (\bar{y} + \vec{\epsilon}_{\bar{y}})\|_2} .$$

By Equation 4 it follows that

$$\|\bar{x} + \vec{\epsilon}_{\bar{x}} - \tilde{x}\|_2 \leq O(d^{-c}) ,$$

Assume for simplicity that $\|\bar{x} + \vec{\epsilon}_{\bar{x}} - \tilde{x}\|_2 \leq d^{-c}$. Since

$$\begin{aligned} \|\tilde{x}\|_2 &\geq \|\bar{x} + \vec{\epsilon}_{\bar{x}}\| - \|\bar{x} + \vec{\epsilon}_{\bar{x}} - \tilde{x}\|_2 \\ &\geq 1 - d^{-c} > 0, \end{aligned}$$

then $\tilde{x} \neq 0$ and by definition $\langle \tilde{x}, \bar{y} + \vec{\epsilon}_{\bar{y}} \rangle = 0$. Hence

$$\text{span}(\tilde{x}, \bar{y} + \vec{\epsilon}_{\bar{y}}) = \text{span}(e_{n-1}, e_n) . \quad (5)$$

Define the following subset $Good_2 \subseteq V(G')$. A vertex $v \in V(G')$ is in $Good_2$ if both $v \in Good$ and $((\bar{x} + \vec{\epsilon}_{\bar{x}} - \tilde{x})_v)^2 \leq \frac{1}{an}$. By averaging argument it holds that $|Good_2| \geq (1 - \frac{3a}{d^{2c}})n$. If the condition in Step 2.a of Algorithm 2 holds for $u, w \in V(G')$ then for any $x, y \in \mathbb{R}$ that satisfy $x^2 + y^2 = 1$ the condition

$$|x((e_{n-1})_u - (e_{n-1})_w) + y((e_n)_u - (e_n)_w)| \leq \frac{1}{\sqrt{an}}$$

holds as well, and By Equation 5

$$|x((\tilde{x})_u - (\tilde{x})_w) + y((\bar{y} + \vec{\epsilon}_{\bar{y}})_u - (\bar{y} + \vec{\epsilon}_{\bar{y}})_w)| \leq \frac{1}{\sqrt{an}} , \quad (6)$$

holds for every x, y such that $x^2 + y^2 = 1$ as well. If v_1 and u are both in $Good_2$ and they both have the same planted color, by Equation 6 it follows that $v_1, u \in S_1$. This is since for every x, y

$$\begin{aligned} &\left| x((\tilde{x})_{v_1} - (\tilde{x})_u) + y((\bar{y} + \vec{\epsilon}_{\bar{y}})_{v_1} - (\bar{y} + \vec{\epsilon}_{\bar{y}})_u) \right| \\ &\leq |x((\tilde{x})_{v_1} - (\tilde{x})_u)| + |y((\bar{y} + \vec{\epsilon}_{\bar{y}})_{v_1} - (\bar{y} + \vec{\epsilon}_{\bar{y}})_u)| \\ &\leq |((\bar{x} + \vec{\epsilon}_{\bar{x}})_{v_1} - (\bar{x} + \vec{\epsilon}_{\bar{x}})_u)| + 2\sqrt{\frac{1}{an}} + |((\bar{y} + \vec{\epsilon}_{\bar{y}})_{v_1} - (\bar{y} + \vec{\epsilon}_{\bar{y}})_u)| \\ &\leq |((\vec{\epsilon}_{\bar{x}})_{v_1} - (\vec{\epsilon}_{\bar{x}})_u)| + |((\vec{\epsilon}_{\bar{y}})_{v_1} - (\vec{\epsilon}_{\bar{y}})_u)| \leq 6\sqrt{\frac{1}{an}} . \end{aligned}$$

If v_1 and u are both in *Good* and u has a different planted color than v then by Equation 6 it follows that $u \notin S_1$. To see this set $x = 0$ and $y = 1$, it follows that

$$\begin{aligned} \left| \left((\bar{y} + \vec{\epsilon}_{\bar{y}})_{v_1} - (\bar{y} + \vec{\epsilon}_{\bar{y}})_u \right) \right| &\geq |((\bar{y})_{v_1} - (\bar{y})_u)| - 2|\vec{\epsilon}_{\bar{x}}| \\ &\geq \frac{1}{\sqrt{n}} - 2\sqrt{\frac{1}{an}}. \end{aligned}$$

If v_1, v_2 and v_3 are all in *Good* and have different planted coloring then by the above Step 2.b of Algorithm 2 will output an $O\left(\frac{n}{d^{2c}}\right)$ -approximated coloring. Note that a random set of three vertices from $V(G')$ has a constant probability to satisfy this (specifically by assuming d is much larger than k it is roughly $p = \frac{k!}{k^k}$) so by choosing v_1, v_2 and v_3 at random the expected number of the iterations that Algorithm B.16 performs is constant (more precisely it is $1/p$). By similar arguments it is straight forward to prove that any coloring that Algorithm 2 outputs is an $O\left(\frac{n}{d^{2c}}\right)$ -approximated coloring. \square

Recall Definition B.13. The following lemma shows that Algorithm 3 refines any $f = O\left(\frac{n}{24}\right)$ -approximated coloring.

Algorithm 3 One Step Refinement

Input: A graph G' and a coloring C .

1. For each vertex v , set $col_{C_2}(v)$ to be the minority color in the multiset $\{col_C(u) \mid u \in N(v)\}$ (break ties arbitrarily).
-

Lemma B.17. *Algorithm 3 runs in polynomial time ($O(nd)$). Let G' be as above and let f be such that C is an f -approximated coloring for G' . If $f \leq \frac{n}{24}$ then Algorithm 3 outputs an $\left(\left(\frac{24\lambda}{d}\right)^2 f + |SB|\right)$ -approximated coloring for G' .*

Proof. [Lemma B.17]. Let W_C be the set of vertices colored with a different color than the original coloring in step 1 of the algorithm. Let W_{C_2} be the set of vertices colored with a different color than the original in C_2 . Let $k = |W_{C_2} \setminus SB|$. The key point, in bounding k , is that any $v \in W_{C_2} \setminus SB$ has at least $\left(\frac{1}{6} - \epsilon\right)d$ neighbors in W_C as otherwise v was colored correctly.

So on the one hand, by using the Expander Mixing Lemma, (Lemma G.4), the following holds

$$\begin{aligned} E_{G'}(W_C, W_{C_2} \setminus SB) &\leq E_G(W_C, W_{C_2} \setminus SB) \\ &\leq \lambda\sqrt{|W_C||W_{C_2} \setminus SB|} + \frac{d}{n}|W_C||W_{C_2} \setminus SB| \\ &\leq \lambda\sqrt{fk} + \frac{d}{n}fk. \end{aligned}$$

On the other hand

$$E_{G'}(W_C, W_{C_2} \setminus SB) \geq \frac{1}{2}k\left(\frac{1}{6} - \epsilon\right)d.$$

It follows that if $k > 0$ and $f \leq \frac{n}{24}$ then

$$k \leq \left(\frac{24\lambda}{d}\right)^2 f.$$

Thus if $\lambda < \frac{1}{24}d$ then we can improve the approximation. \square

To prove Lemma B.15 consider Algorithm 4.
[Lemma B.15].

Algorithm 4 Iterative Recoloring

Input: A graph G' and a coloring F_1 .

1. For i taking values from 2 to $k = \Omega(d)$ do.
 - (a) Apply Algorithm 3 where the specified coloring is F_{i-1} to get f_i -approximated coloring, namely F_i .
-

Lemma B.18. (Restatement of Lemma 2.2). *Algorithm 4 runs in polynomial time (the running time is $O(d^2n)$). Let G' be as above. If F_1 is a $(\frac{n}{24})$ -approximated coloring for G' then Algorithm 4 outputs an $O(|SB|)$ -approximated coloring for G' .*

Proof. (Of Lemma B.18). By Lemma B.17, it holds that $f_i \leq (\frac{24\lambda}{d})^2 f_{i-1} + |SB|$ for all $2 \leq i \leq k$. It follows that $f_k \leq (\frac{24\lambda}{d})^{2k} \frac{n}{d} + O(|SB|)$, substituting $k = \Omega(d)$ ¹ in the last inequality resolves the proof. \square

The following lemma shows a structural property of expander graphs and is used in the proof of Lemma B.20.

Lemma B.19. *Let G be a d -regular λ -expander graph with n vertices and consider an arbitrary $S \subset V(G)$. If $\lambda \leq \frac{\epsilon}{16}d$, $|S| < \frac{\epsilon}{4}n$ and d is large enough then there exists $CC \subseteq V(G) \setminus S$ such that G_{CC} is a graph with a minimum degree of $(1 - \epsilon)d$ and $|CC| \geq n - 2|S|$.*

Before we give the proof note that if G was the complete graph, as a toy example, then we can take $CC = V(G) \setminus S$. This lemma can be seen as a relaxed version for this property that holds in expander graphs.

Proof. (Of Lemma B.19). Consider the following iterative procedure. Repeatedly remove a vertex v_t from $V(G) \setminus (S \cup (\bigcup_{i=1}^{t-1} v_i))$ if v_t has more than ϵd neighbors in $S_t = S \cup (\bigcup_{i=1}^{t-1} v_i)$. Denote by S' the union of S and the removed vertices. Assume towards a contradiction that this process stops after more than $t = |S|$ steps. The graph G_{S_t} has an average degree of at least $\frac{\epsilon}{2}d$. By the expander mixing lemma it holds that

$$\begin{aligned} \frac{\epsilon}{4}d|S_t| &\leq E_G(S_t, S_t) \\ &\leq \frac{d}{n}|S_t|^2 + \lambda|S_t| \end{aligned}$$

¹If $\lambda = o(d)$ then less iterations are needed.

It follows that $\frac{\epsilon}{8}n \leq \frac{(\frac{\epsilon}{4}d - \lambda)}{d}n \leq |S_t|$, but $|S_t| < \frac{\epsilon}{8}n$, which is a contradiction for large enough d (as $\lambda \leq \frac{\epsilon}{8}d$). Clearly every vertex in $G_{V(G') \setminus S'}$ has degree at least $(1 - \epsilon)d$ and the proof follows. \square

To prove Theorem B.10 consider Algorithm 5.

Algorithm 5 Cautious Uncoloring

Input: A graph G' and a coloring C .

1. Repeatedly uncolor the following vertices $v \in G'$ (denote the set of uncolored vertices by H_1):
 - (a) Vertices with less than $(\frac{2}{3} - 2\epsilon)d$ neighbors.
 - (b) Vertices with less than $(\frac{1}{6})d$ neighbors of color $l \in \{1, 2, 3\} \setminus \text{col}_C(v)$.
-

Lemma B.20. (Restatement of Lemma 2.3). *Algorithm 5 runs in polynomial time. Let G' be as above. If C is an $O(|SB|)$ -approximated coloring then the set of the uncolored vertices (H_1) is of size $O(|SB|)$ and the set of the colored vertices agree with the planted coloring of G' .*

Proof. (Of Lemma B.20). Define

$$B := \{v \in V(G') \mid \text{col}_P(v) \neq \text{col}_C(v)\}.$$

To derive the proof we show $B \subseteq H_1$ and that $|H_1| \leq O(|SB|)$. By Lemma B.19 there exist a set $CC \subseteq V(G') \setminus (SB \cup B)$ such that $|CC| \geq n - 2|SB \cup B|$, and every $v \in G_{CC}$ has at least $(\frac{1}{3} - 2\epsilon)d$ neighbors in CC with color i , for all $i \in \{1, 2, 3\} \setminus \text{col}_P(v)$. To see this, apply Lemma B.19 on G , the graph before the planting, with $S = SB \cup B$ to get the set CC . Since $v \notin SB$ it holds that $v \in CC$ has at least $(\frac{1}{3} - 2\epsilon)d$ neighbors in CC with color i , for all $i \in \{1, 2, 3\} \setminus \text{col}_P(v)$.

It holds that no vertex from CC is uncolored, (at the first iteration of Step 1 this clearly holds. Assume that no vertex from CC is uncolored in the first i iterations of Step 1, in the $i + 1$ iteration this still holds.).

Now we show that all of $V(G') \setminus H_1$ is colored correctly. Assume towards a contradiction that there exists a vertex v in $(V(G') \setminus H_1) \setminus CC$ such that $v \in B$. Let $B_{V(G') \setminus H_1} := \{v \in V(G') \setminus H_1 \mid \text{col}_P(v) \neq \text{col}_C(v)\}$. Since that any vertex $v \in B_{V(G') \setminus H_1}$ has degree at least $(\frac{2}{3} - 2\epsilon)d$ neighbors (as otherwise Step 1.a of Algorithm 5 removes v) then v has at least $(\frac{1}{6} - \epsilon)d$ neighbors colored by $\text{col}_P(v)$ which means they are in $B_{V(G') \setminus H_1}$. It follows that the sub-graph of G' induced on $B_{V(G') \setminus H_1}$ has degree at least $(\frac{1}{6} - \epsilon)d$. By the expander mixing lemma, Lemma G.4, it holds that

$$\begin{aligned} \left(\frac{1}{6} - \epsilon\right)d |B_{V(G') \setminus H_1}| &\leq E_{G'}(B_{V(G') \setminus H_1}, B_{V(G') \setminus H_1}) \\ &\leq E_G(B_{V(G') \setminus H_1}, B_{V(G') \setminus H_1}) \\ &\leq \frac{d}{n} |B_{V(G') \setminus H_1}|^2 + \lambda |B_{V(G') \setminus H_1}|. \end{aligned}$$

It follows that if $|B_{V(G')\setminus H}| > 0$, as we assumed, then $|B_{V(G')\setminus H}| \geq \Omega\left(\frac{d-\lambda}{d}\right)n$ but as it holds that

$$|B_{V(G')\setminus H}| \leq n - |CC| = O(|SB|),$$

we derive a contradiction. \square

Algorithm 6 Safe Recoloring

Input: A graph G' and a partial coloring C . Denote the set of uncolored vertices by H_1 .

1. Repeatedly color any vertex that has 2 neighbors colored with i, j , (for $i \neq j$), by $\{1, 2, 3\} \setminus \{i, j\}$.
-

Lemma B.21. *Algorithm 6 runs in polynomial time. Let G' be as above and H be the set of vertices that were left uncolored by Algorithm 6. Let G'_H be the induced sub-graph of G' on the vertices of H . If $H_1 \leq \frac{1}{11}n$ then with high probability (over the distribution of G') each connected component in G'_H is of size $O\left(\frac{\lambda^2}{d^2} \log n\right)$.*

Proof. (Of Lemma B.21). Recall that G is the graph before the planted coloring process occurred. We use Claim B.22 extensively.

Claim B.22. Let $C \subset V(G)$ be any set of vertices of size k , let D be $N_G(C) \setminus C$ and let $t = |D|$. If $t \geq 2k$ then C is in H and $D \subseteq V(G) \setminus H$ with probability at most $2^{-\eta t}$, for some constant η .

Proof. Partition the vertices of D to disjoint subsets $\{D_v\}$, where $v \in C$ and $D_v \subseteq N_G(v)$ (this can be done by choosing for each vertex in D an arbitrary neighbor in S). Consider some D_v and assume that v is colored by 1. If both $v \in H$ and $D_v \subseteq V(G) \setminus H$ then the set of colors that vertices in D_v are using can be contained in exactly one of the sets $\{1, 2\}$ or $\{1, 3\}$ (otherwise Algorithm 6 will color v at Step 1). Therefore the probability that both $v \in H$ and $D_v \subseteq V(G) \setminus H$ is at most $2\left(\frac{2}{3}\right)^{|D_v|}$. Hence, the probability that both C is in H and $D \subseteq V(G) \setminus H$ is at most

$$\begin{aligned} \prod_{D_v \in \{D_v\}} 2\left(\frac{2}{3}\right)^{|D_v|} &= 2^{|\{D_v\}|} \left(\frac{2}{3}\right)^t \\ &\leq 2^k \left(\frac{2}{3}\right)^t \\ &= \left(\frac{2}{3}\right)^{t+k \log_2 2} \leq \left(\frac{2}{3}\right)^{0.14t}. \end{aligned}$$

The last inequality follows by the assumption that $t \geq 2k$. \square

Let $C \subset H$ be any set of vertices of size k such that G'_C is connected. Note that if G'_C is connected then G_C is connected. Hence we can consider the set \tilde{C} to be a connected set

in G such that $C \subseteq \bar{C} \subset H$ and $N(\bar{C}) \setminus \bar{C} \subseteq V(G) \setminus H$ (as long as there exist vertices in $(N(\bar{C}) \setminus \bar{C}) \cap H$ we repeatedly add them to \bar{C} , and it is straight forward to show that \bar{C} is connected in G). Thus if we show that with high probability no connected subsets \bar{C} of G with cardinality $\Omega\left(\frac{\lambda^2}{d^2} \log n\right)$ are in H if $N(\bar{C}) \subseteq V(G) \setminus H$ then the proof follows. The key point of the proof is that (since H is small) no (small connected) subsets of H with with a small neighborhood are in $V(G) \setminus H$ (due to G 's expansion) and when a connected set have a large enough neighborhood we can use Claim B.22 to show they are likely to not be contained in H . To fully exploit Claim B.22 we use the union bound in a delicate manner that depends on the neighborhood size of the (connected) sets in order to sum sets with large neighborhood size with small probabilities. In order to do so we use Lemma B.23.

Denote by $N_G(n, k, d)$ the number of connected components of size k with a neighborhood of size exactly t in a graph G with n vertices.

Lemma B.23. *For any graph G the following holds,*

$$N_G(n, k, t) \leq n \binom{k+t}{k}.$$

Several proofs of Lemma B.23 are known, and one such a proof can be found in [27]. Lemma B.23 holds for any graph, regardless of its degree or expansion. Let α be such that $\lambda = \frac{d}{\alpha}$. Let

$$p_{s,t} := \max_{C \subset G, |C|=s, |N(C)|=t} \Pr[C \text{ is in } H].$$

By the union bound the probability that there exists a connected component in G'_H of size $\Omega\left(\frac{\lambda^2}{d^2} \log n\right)$ is at most

$$\sum_{s=\frac{\lambda^2}{d^2} \log n}^{|H|} \sum_{t=1}^{ds} N_G(n, s, t) P_{s,t} = \sum_{s=\frac{\lambda^2}{d^2} \log n}^{|H|} \sum_{t=\lceil \frac{1}{2} \left(\frac{d}{\lambda}\right)^2 s \rceil}^{ds} N_G(n, s, t) 2^{-\eta t} \quad (7)$$

$$\leq \sum_{s=\frac{\lambda^2}{d^2} \log n}^{|H|} \sum_{t=\lceil \frac{\alpha^2}{2} s \rceil}^{ds} n \binom{s+t}{s} 2^{-\eta t} \quad (8)$$

$$\leq \sum_{s=\frac{\lambda^2}{d^2} \log n}^{|H|} \sum_{t=\lceil \frac{\alpha^2}{2} s \rceil}^{ds} n \left(e \frac{s+t}{s} \right)^s 2^{-\eta t} \quad (9)$$

$$\leq \sum_{s=\frac{\lambda^2}{d^2} \log n}^{|H|} n d s \max_{\frac{\alpha^2}{2} \leq c \leq d} 2^{(\log_2(e(c+1)) - \eta c) s} \quad (10)$$

$$\leq n^{-\Omega(1)}. \quad (11)$$

Equality 7 follows since by Lemma G.5 if $\lambda \leq d/\sqrt{12}$ then for a set of size $s \leq |H| \leq \frac{1}{11}n$ it holds that its neighborhood is of size $t \geq \frac{1}{2} \left(\frac{d}{\lambda}\right)^2 s$ (thus $N_G(n, s, t) = 0$) and by Claim B.22 (for some constant η). Inequality 8 follows by Lemma B.23. Inequality 9 follows by the binomial identity $\binom{n}{k} \leq \left(e \frac{n}{k}\right)^k$. Inequality 11 follows if $\alpha \geq \alpha'$, where α' is a large enough constant. \square

Algorithm 7 Brute Force

Input: A graph G' and a partial coloring C .

1. If the induced graph of the uncolored vertices, H , contains a connected component of size $\log n$ abort.
 2. Enumerate over all possible coloring of each connected component of H and return a legal 3-coloring of G' .
-

C Adversarial host and adversarial planting, H_A/P_A

Section C contains the proofs for the model with an adversarial expander host graph and an adversarial planted balanced coloring, namely, H_A/P_A . Section C.1 shows how to obtain a b -partial coloring for graphs in the H_A/P_A model (Theorem 1.1). Section C.2 proves Theorem 1.2 (hardness result for the H_A/P_A model).

C.1 Partial coloring of expander graphs with adversarial planting

Given a d -regular λ -expander graph G and a partition, C , of $V(G)$ to 3 sets, c_1, c_2, c_3 , we denote by $P_C(G)$ the graph obtained after removing all edges from G with both endpoints in the same set c_i . If all the sets c_1, c_2, c_3 have the same cardinality we say that C is balanced. In this section we consider the computational problem of coloring $P_C(G)$ when C is given by an adversary.

In this section we show the following theorem.

Theorem C.1. *(Restatement of Theorem 1.1). Let G be a d -regular λ -expander graph. If $\lambda \leq cd$ (for some constant c) then for every balanced 3-color planting C Algorithm 8 outputs an $O\left(n \left(\frac{\lambda}{d}\right)^2\right)$ -approximated coloring for $P_C(G)$.*

Throughout this section, let $\epsilon = 0.01$.

Definition C.2. The set $SB \subseteq V$, statistically bad, is the the following vertex set. $v \in SB$ if v has more than $\left(\frac{1}{3} + \epsilon\right)d$ or neighbors, or less than $\left(\frac{1}{3} - \epsilon\right)d$ or neighbors, with original color $k \in \{1, 2, 3\} \setminus \{col_C(v)\}$.

It turns out that by applying Algorithm 4 and the uncoloring procedure of Algorithm 5 (see Algorithm 8 below) we can find the planted coloring of a set of $(1 - O\left(\frac{1}{d}\right))n$ vertices.

Algorithm 8 Iterative Coloring and Uncoloring

1. Color $P_C(G)$ with an $O(|SB|)$ -approximated coloring C_{Alg} (use Algorithm 4).
 2. Repeatedly uncolor vertices $v \in P_C(G)$ with less than $(\frac{2}{3} - 2\epsilon)d$ neighbors or with less than $(\frac{1}{6})d$ neighbors of color $l \in \{1, 2, 3\} \setminus \text{col}_{C_{Alg}}(v)$, denote the set of uncolored vertices by H_1 .
 3. If $|H_1| = O(\log n)$ then enumerate over all the possible colorings $(3^{|H_1|})$ of the vertices in H_1 .
-

Throughout the rest of this section we denote $G' = P_C(G)$. The main point of the proof of Theorem C.1 is that $e_{n-1}(P_C(G)), e_n(P_C(G))$ are related to C even when C is arbitrary balanced (rather than random as in the previous sections). This is stated in Lemma C.4 which is similar to Theorem B.1. To state Lemma C.4 let us define the following.

Definition C.3. Given C define the following vectors in \mathbb{R}^n . $(\vec{1}_n)_i = 1, (\vec{p}_i)_j := \begin{cases} 1 & v_j \in c_i \\ 0 & v_j \notin c_i \end{cases}$,

$$(\vec{x})_i := \begin{cases} 2 & v_i \in c_1 \\ -1 & v_i \in c_2 \\ -1 & v_i \in c_3 \end{cases} \text{ and } (\vec{y})_i := \begin{cases} 0 & v_i \in c_1 \\ 1 & v_i \in c_2 \\ -1 & v_i \in c_3 \end{cases}.$$

Lemma C.4. Let G be a d regular λ -expander, where $\lambda \leq cd$ (for some constant c). If $G' = P_C(G)$ for a balanced C then with high probability the following holds.

1. The eigenvalues of G' have the following spectrum.

- (a) $\lambda_1(G') \geq \frac{2}{3}d - \sqrt{d\lambda}$.
- (b) $\lambda_n(G') \leq \lambda_{n-1}(G') \leq -\frac{1}{3}d - \sqrt{d\lambda}$.
- (c) $|\lambda_i(G')| \leq 2\lambda + O(\sqrt{d\lambda})$ for all $2 \leq i \leq n-2$.

2. The following vectors exist.

- (a) $\vec{\epsilon}_{\vec{x}}$ such that $\|\vec{\epsilon}_{\vec{x}}\|_2 = O\left(\sqrt{\frac{\lambda}{d}}\right)$ and $\vec{x} + \vec{\epsilon}_{\vec{x}} \in \text{span}\left(\{e_i(G')\}_{i \in \{n-1, n\}}\right)$.
- (b) $\vec{\epsilon}_{\vec{y}}$ such that $\|\vec{\epsilon}_{\vec{y}}\|_2 = O\left(\sqrt{\frac{\lambda}{d}}\right)$ and $\vec{y} + \vec{\epsilon}_{\vec{y}} \in \text{span}\left(\{e_i(G')\}_{i \in \{n-1, n\}}\right)$.

Proof. The proof goes by showing an equivalent statement as in Lemma B.2. In this proof we set ϵ to be $\sqrt{\frac{\lambda}{d}}$ (rather than 0.01). Denote $c_{G',i,j}^+ = \{v \in c_i \mid |N_{G'}(v) \cap c_j| \geq (\frac{1}{3} + \epsilon)dn\}$ and $c_{G',i,j}^- = \{v \in c_i \mid |N_{G'}(v) \cap c_j| \leq (\frac{1}{3} - \epsilon)dn\}$. By the expander mixing lemma, Lemma G.4, it follow that for all $i \neq j$

$$\begin{aligned} \left(\frac{1}{3} + \epsilon\right) d \left|c_{G',i,j}^+\right| &\leq \left|E_{G'}\left(c_{G',i,j}^+, G'_{c_j}\right)\right| = \left|E_G\left(c_{G',i,j}^+, G_{c_j}\right)\right| \\ &\leq \frac{d}{3} \left|c_{G',i,j}^+\right| + \lambda \sqrt{\frac{n}{3} \left|c_{G',i,j}^+\right|}. \end{aligned}$$

The above simplifies to

$$|c_{G',i,j}^+| \leq \left(\frac{\lambda}{\epsilon d}\right)^2 \frac{n}{3},$$

and similarly

$$|c_{G',i,j}^-| \leq \left(\frac{\lambda}{\epsilon d}\right)^2 \frac{n}{3}.$$

Recall the definition of \vec{x} , it follows that

$$\begin{aligned} \sum_{i=1}^{n/3} \left(A_{G'} \vec{x} - \left(-\frac{d}{3}\right) \vec{x} \right)_i^2 &\leq d^2 \left(|c_{G',1,2}^+| + |c_{G',1,2}^-| + |c_{G',1,3}^+| + |c_{G',1,3}^-| \right) + (2\epsilon d)^2 \frac{n}{3} \\ &\leq d^2 \frac{n}{3} \left(4 \left(\frac{\lambda}{\epsilon d}\right)^2 + (2\epsilon)^2 \right) \\ &\leq \frac{8}{3} nd\lambda. \end{aligned}$$

By similar calculations we can conclude that

$$\sum_{i=1}^n \left(A_{G'} \vec{x} - \left(-\frac{d}{3}\right) \vec{x} \right)_i^2 \leq 8nd\lambda,$$

and if we normalize then

$$\left\| A_{G'} \bar{x} - \left(-\frac{d}{3}\right) \bar{x} \right\|_2 \leq O(\sqrt{d\lambda}).$$

Similarly we can show equivalent statements with respect to $\bar{y}, \bar{1}$ and $\{\bar{p}_i \mid i \in \{1, 2, 3\}\}$. By applying Lemma B.3 we can conclude an equivalent statement as in Lemma B.4, namely the following claim.

Claim C.5. Define $S_\delta(x) \subset \{1, \dots, n\}$ to be the set of those indices i for which $|\lambda(G')_i - (x)| \leq \delta$. The following vectors exist.

- $\vec{\epsilon}_{\bar{1}}$ such that $\|\vec{\epsilon}_{\bar{1}}\|_2 \leq \frac{O(\sqrt{d\lambda})}{\delta}$ and $\bar{1} + \vec{\epsilon}_{\bar{1}} \in \text{span} \left(\{e_i(G')\}_{i \in S_\delta(\frac{2}{3}d)} \right)$.
- $\vec{\epsilon}_{\bar{x}}$ such that $\|\vec{\epsilon}_{\bar{x}}\|_2 \leq \frac{O(\sqrt{d\lambda})}{\delta}$ and $\bar{x} + \vec{\epsilon}_{\bar{x}} \in \text{span} \left(\{e_i(G')\}_{i \in S_\delta(-\frac{1}{3}d)} \right)$.
- $\vec{\epsilon}_{\bar{y}}$ such that $\|\vec{\epsilon}_{\bar{y}}\|_2 \leq \frac{O(\sqrt{d\lambda})}{\delta}$ and $\bar{y} + \vec{\epsilon}_{\bar{y}} \in \text{span} \left(\{e_i(G')\}_{i \in S_\delta(-\frac{1}{3}d)} \right)$.

Using Claim C.5 and applying the same arguments as in the proof of Theorem B.1 ends the proof. \square

Lemma C.6. *It holds that $|SB| \leq O\left(n \left(\frac{\lambda}{\epsilon d}\right)^2\right)$.*

Proof. Recall the definition of $c_{G',i,j}^+$ and $c_{G',i,j}^-$ from the proof of Lemma C.4. It holds that

$$\begin{aligned} SB &\leq \sum_{i \neq j} \left(\left| c_{G',i,j}^+ \right| + \left| c_{G',i,j}^- \right| \right) \\ &\leq 4 \left(\frac{\lambda}{\epsilon d} \right)^2 n. \end{aligned}$$

□

Now we continue with the proof of Theorem C.1.

Proof. [Theorem C.1]. Using Lemma C.4 and the proof of Lemma B.16 we conclude that Algorithm 2 outputs an $O\left(n \frac{\lambda}{d}\right)$ -approximate coloring of G' . The proof of Lemma B.15 shows that Algorithm 4 gets $O(|SB|)$ -approximate coloring of G' . Define

$$B := \{v \in V(G') \mid \text{col}_C(v) \neq \text{col}_{C_{Alg}}(v)\}.$$

The proof of Lemma B.20 shows that $|H_1| \leq O(|SB|)$ and $B \subseteq H_1$. By Lemma C.6 it follows that $SB \leq O\left(n \left(\frac{\lambda}{\epsilon d}\right)^2\right)$ and proof follows. □

When G has an high degree (with respect to its expansion) we obtain the following corollary.

Corollary C.7. *Let G be an $\Omega\left(\frac{n}{\log n}\right)$ -regular λ -expander graph. If $\lambda = O\left(\sqrt{d}\right)$ then for every balanced C Algorithm 8 colors $P_C(G)$.*

C.2 Hardness of coloring expander graphs with adversarial planting

It is well known [19] that 3-coloring 4-regular graphs is NP-hard. In this section we show the following theorem.

Theorem C.8. *(Restatement of Theorem 1.2). Let c be a constant equals 4 and $d = \Omega(1)$ be large enough. Let H be an arbitrary c -regular graph with $\frac{n}{cd}$ vertices that is 3-colorable. Any (polynomial time) algorithm that (fully) colors d -regular $O\left(\sqrt{d}\right)$ -expander graphs with an adversarial planted 3-coloring that is balanced can be used to color H .*

Proof. Assume the graph H is 3-colorable in such a way that all the color classes are of the same size (this can be obtained by taking a disjoint union of 3 copies of H), denote this coloring by $P_H = P_1 \cup P_2 \cup P_3$. Let G be any d -regular $O\left(\sqrt{d}\right)$ -expander graph with $\left(1 - \frac{1}{cd}\right)n$ vertices. Let A be an algorithm that colors d -regular $O\left(\sqrt{d}\right)$ -expander graphs with an adversarial planted coloring. We show that this implies that A colors the disjoint union H and $P(G)$ ($P(G)$ is an arbitrary balanced planted coloring of G), denote this union by $(P(G) + H)$. Consider the graph G_H obtained as follows. Add 3 sets, S_1, S_2, S_3 of $\frac{n}{3cd}$ vertices to G such that each of the added vertices has $d - c$ unique neighbors in G and all the vertices from the i -th set have their neighborhood contained in P_i . Replace the induced

sub-graph on the vertices of $\bigcup S_i$ (it is an independent set) with H (permute the vertices of H such that the sets $\{S_i\}$ agrees with P). It is clear from this construction that there exists an (adversarial) planting such that after it has been applied on G_H we obtain $(P(G) + H)$. The following claim ends the proof.

Claim C.9. G_H is a $O(\sqrt{d})$ expander.

Proof. Consider the following inequality from perturbation theory for matrices that holds for any two symmetric matrices $A, N \in \mathbb{R}^{n,n}$ (see, for example, [6])

$$\max_{i:1 \leq i \leq n} |\lambda_i(A + N) - \lambda_i(A)| \leq \max_{i:1 \leq i \leq n} |\lambda_i(N)|. \quad (12)$$

Namely, the inequality shows that by adding a matrix N to a matrix A , the eigenvalues of $A + N$ change by at most $\max_{i:1 \leq i \leq n} |\lambda_i(N)|$.

We can write the adjacency matrix of G_H as

$$A_{G_H} = A'_G + A'_H + A'_S.$$

Here S is the disjoint union of $\frac{n}{cd}$ star graphs S_{d-c} (the graph S_k is a bipartite graph of $(k+1)$ vertices with one vertex connected to all the other vertices) and A'_G is the adjacency matrix of the graph obtained from G an independent set of vertices were added to it (similarly for H and S). Note that adding an independent set to a graph only adds zero entries to its spectrum.

It is a known fact that for every i it holds that $|\lambda_i(S_k)| \leq \sqrt{k}$. Hence, since S is the disjoint union of star graphs then every i it holds that $|\lambda_i(A_S)| \leq \sqrt{d-c}$. Since H is c regular, for every i it holds that $|\lambda_i(H)| \leq c$. By Inequality 12 it follows that for every $i \in [n]$ it holds that

$$\begin{aligned} |\lambda_i(A_G)| - (c + \sqrt{d-c}) &\leq |\lambda_i(A_{G_H})| \\ &\leq |\lambda_i(A_G)| + (c + \sqrt{d-c}). \end{aligned} \quad (13)$$

Recall that c is a constant and G is a d -regular $O(\sqrt{d})$ -expander graph and note that (by construction) vertices of G_H have degrees between d and $d+1$ (actually, this implies that $d \leq \lambda_1(G_H) \leq d+1$). Hence by Inequality 13 G_H is (roughly d -regular) $O(\sqrt{d})$ -expander. \square

\square

D Random host and adversarial planting, H_R/P_A

Section D contains the proofs for the model with a random host graph and an adversarial planted balanced coloring, namely, H_R/P_A . Section D.1 proves Theorem 1.4a (a 3-coloring algorithm for H_R/P_A). Section D.2 proves Theorem 1.4b (hardness for H_R/P_A).

D.1 3-coloring random graphs with adversarial color planting

We start with a definition for a distribution for random graphs, following [12],

Definition D.1. A graph with n vertices G is distributed by $G_{n,d}$ if each edge is included in the graph with probability $p = \frac{d}{n-1}$, independently from every other edge.

In this section we consider the following planting model. The host graph $G \sim G_{n,d}$ is a random graph on n vertices with average degree d and the planting is adversarial. As opposed to the previous sections, here our techniques can be applied only to 3 colors (or less) planting (see Section E.1 for details). Consider the following algorithm.

Algorithm 9 3-coloring for random graphs with adversarial planting

1. Use Algorithm 4 to color $P_C(G)$ with a partial coloring $,C_{Alg}$.
 2. Repeatedly uncolor vertices $v \in P_C(G)$ with less than $(\frac{2}{3} - 2\epsilon)d$ neighbors or with less than $(\frac{1}{6})d$ neighbors of color $l \in \{1, 2, 3\} \setminus col_{C_{Alg}}(v)$.
 3. Repeatedly color every vertex that has 2 neighbors colored with i, j , (for $i \neq j$), by $\{1, 2, 3\} \setminus \{i, j\}$.
 4. For every vertex that has a colored neighbor create a variable that takes values corresponding to the two remaining colors.
 5. For each $i \in \{1, 2, 3\}$ do as follows.
 - (a) Any uncolored vertex that has no colored neighbor is colored by i .
 - (b) If there exists a legal coloring for $P_C(G)$ that agrees with the above (use any algorithm that solves *2SAT*) return it.
 6. Return the partial coloring of $P_C(G)$.
-

We prove the following theorem.

Theorem D.2. (Restatement of Theorem 1.4a). Let $d = \omega\left(n^{\frac{2}{3}}\right)$, $G \sim G_{n,d}$ and $P_C(G)$ be the graph G with an adversarial 3-coloring. With high probability, Algorithm 9 outputs a legal coloring for $P_C(G)$.

The starting point in the proof of Theorem D.2 is that random graphs are very good expanders. Specifically, it is a well known fact that with high probability $\lambda_2(G) = \Theta(\sqrt{d})$ (for example, see [15, 18, 17]). This enables us to employ our techniques from Section C.1 (mainly to apply Theorem C.1) to get an $O\left(\frac{n}{d}\right)$ -approximated coloring for $P_C(G)$. To get a better coloring of $P_C(G)$ than suggested by Theorem C.1, we use specific properties of random graphs. Mainly that every pair of vertices has roughly $\frac{d^2}{n}$ common neighbors.

Proof. (Of Theorem D.2). Recall that with high probability $\lambda_2(G) = \Theta(\sqrt{d})$. Hence, by Theorem C.1, it follows that after Step 2 we have a partial coloring of $P_C(G)$ that colors

all but $O\left(\frac{n}{d}\right)$ vertices exactly as in the planted coloring. Clearly, in Step 3 all the vertices we color are colored as in the planted coloring. Denote the set of colored vertices by A and the remaining vertices by B . Denote by $B_1 \subseteq B$ the set of vertices with a colored neighbor, and by $B_2 \subseteq B$ the rest. The proof follows by showing that all the vertices in B_2 are of the same planted color. By applying the Chernoff and the union bounds it follows that, with high probability, for every pair of vertices $u, v \in V(G)$ there are $\Theta\left(\frac{d^2}{n}\right)$ common neighbors (assume this event holds). By our assumption on d , it follows that given a pair of vertices u, v of different planted color classes at least $\Theta\left(\frac{d^2}{n}\right) - O\left(\frac{n}{d}\right) > 0$ vertices in A are neighbors of both u, v in G , take one such vertex w . Hence, for every planting, $w \in A$ is still a neighbor of at least one of u, v , say v . But this is a contradiction for $v \in B_2$. \square

When $n^{\frac{1}{2}} \leq d \leq n^{\frac{2}{3}}$ it holds that all pairs have a lot of common neighbors and Theorem D.2 does not give any advantage when that is the case. The following generalization to Theorem D.2 deals with that regime.

Theorem D.3. *Let $G \sim G_{n,d}$ and $P_C(G)$ be the graph G with an adversarial 3-coloring. With high probability, Algorithm 9 outputs a partial coloring for $P_C(G)$ that is legal on the colored vertices such that at most $\tilde{O}\left(\frac{n^2}{d^3}\right)$ vertices are not colored.*

Note that when $d \geq \sqrt{n}$ then indeed we get advantage from applying Theorem D.3 (and when $d < \sqrt{n}$ then Theorem C.1 gives a better guarantee of $O\left(\frac{n}{d}\right)$ -approximated coloring).

Proof. (Of Theorem D.3). Recall that with high probability $\lambda_2(G) = \Theta\left(\sqrt{d}\right)$. Hence, by Theorem C.1, it follows that after Step 2 we have a partial coloring of $P_C(G)$ that colors all but $O\left(\frac{n}{d}\right)$ vertices exactly as in the planted coloring. Clearly, in Step 3 all the vertices we color are colored as in the planted coloring. Denote the set of colored vertices by A and the remaining vertices by B . Denote by $B_1 \subseteq B$ the set of vertices with a colored neighbor, and by $B_2 \subseteq B$ the rest. Fix an arbitrary set $A' \subset V(G)$ of size $n\left(1 - \frac{1}{d}\right)$ and let $B' = V(G) \setminus A'$.

For every vertex $w \in A'$ it hold that

$$\begin{aligned} \Pr_{G \sim G_{n,d}} [|N_G(w) \cap A'| \geq 2] &= 1 - (1-p)^{\frac{n}{d}} - \frac{n}{d}p(1-p)^{\frac{n}{d}-1} \\ &= \Theta(1) . \end{aligned}$$

Consider the set $C' = \{w \in V(G) \mid |N(w) \cap A'| \geq 2\}$. By applying the Chernoff bound it follows that

$$\Pr [|C'| < 0.1n] \leq 2^{-\Omega(n)} .$$

Condition on the event that $|C'| \geq 0.1n$. For every vertex $v \in B'$ define the set $B_{v,A'} = \{u \in B' \mid \nexists w \in A' \text{ s.t. } \{u, v\} \subseteq N_G(w)\}$. It holds that for any $t \geq 0$

$$\begin{aligned} \Pr [|B_{v,A'}| \geq t] &\leq \frac{n}{d} \left(1 - \frac{t}{\left(\frac{n}{d}\right)^2} \right)^{0.1n} \\ &\leq \frac{n}{d} e^{-\frac{t}{\left(\frac{n}{d}\right)^2} 0.1n} . \end{aligned}$$

Let η be some constant and Bad be the following event

$$\exists A' \subseteq V(G) \text{ s.t. } |A'| = \frac{n}{d}, \exists v \in B' \text{ s.t. } |B_{v,A'}| \geq \frac{n^2}{d^3} \log^\eta d.$$

By the the above and the union bound it follows that for every $\eta > 1$

$$\begin{aligned} \Pr_{G \sim G_{n,d}} [Bad] &\leq \binom{n}{n/d} \left(2^{-\Omega(n)} + \frac{n^2}{d^2} e^{-\left(\frac{n}{d}\right)^2 0.1n} \right) \\ &\leq e^{\Theta\left(\frac{n}{d} \log d\right) - \Theta\left(\frac{n}{d} \log^\eta d\right)}. \end{aligned}$$

The last inequality follows from the approximation $\binom{n}{k} \leq \left(e \frac{n}{k}\right)^k$, and the last term approaches zero as n grows.

Assume that no legal coloring of $P_C(G)$ was found in Step 5. It follows that the set B_2 was colored by C with at least two colors. Let u be a vertex such that $col_C(u) = i$. Let $j \neq i$ be any other color class in C . Suppose $J = \{v \mid col_C(v) = j\} \geq \frac{n^2}{d^3} \log^\eta d$ then, conditioned on the complement event Bad , there exist a vertex $v \in J$ and $w \in A$ such that $\{u, v\} \subseteq N_G(w)$. Since u, v are in different color classes it follows that at least one of them is not in B_2 , as no matter what $col_C(w)$, at least one of u, v remains a neighbor of w in $P_C(G)$, which is a contradiction. It follows that the remaining set of uncolored vertices is of size at most $3 \frac{n^2}{d^3} \log^\eta d$. □

D.2 Hardness of 3-coloring random graphs with adversarial planted 3-coloring

The following definition can be found in [3] (see Chapter 4).

Definition D.4. [balanced graph]. Given a graph H , denote by α its average degree. A graph H is balanced if every induced subgraph of H has an average degree of at most α .

Theorem D.5. (Restatement of Lemma 2.7). For $0 < \epsilon \leq \frac{1}{7}$ and $3 < \alpha < 4$, suppose that $\frac{k^2 d^2}{n} \leq \epsilon$ and $\frac{k^4 n^{\alpha-2}}{d^\alpha} \leq \epsilon^2$. Let H be an arbitrary balanced graph on k vertices with an average degree α and let $G \sim G_{n,d}$ be a random graph. Then with probability at least $1 - 4\epsilon$ (over choice of G), G contains a set S of k vertices such that:

1. The subgraph induced on S is H .
2. No two vertices of S have a common neighbor outside S .

Proof. Let $p = \frac{d}{n-1}$ be the edge probability in G . Suppose for simplicity (an assumption that can be removed) that k divides n . Partition the vertex set of G into k equal parts of size n/k each. Vertex i of H will be required to come from part i . A set S with such a property is said to *obey the partition*.

Let X be a random variable counting the number of sets S obeying the partition that satisfy the theorem. Let Y be a random variable counting the number of sets S obeying the partition that have H as an edge induced subgraph (but may have additional edges, and may not satisfy item 2 of the theorem).

$$E[Y] = \left(\frac{n}{k}\right)^k p^{\frac{\alpha k}{2}} = \left(\frac{d^\alpha}{k^2 n^{\alpha-2}}\right)^{\frac{k}{2}}.$$

A set S in Y contributes to X if it has no internal edges beyond those of H (which happens with probability at least $1 - \binom{k}{2} \frac{d}{n}$) and no two of its vertices has a common neighbor outside S (which happens with probability at least $1 - \binom{k}{2} \frac{d^2}{n}$). Consequently:

$$E[X] \geq E[Y] \left(1 - \frac{k^2 d^2}{n}\right) \geq (1 - \epsilon) E[Y].$$

Now let us compute $E[Y^2]$. Given one occurrence of H , consider another potential occurrence H' that differs from it by t vertices. Since H is balanced graph then

$$\begin{aligned} |E(G_{H' \setminus H})| + |E(G_{H' \setminus H}, G_H)| &\geq \frac{\alpha |V(G)|}{2} - \frac{\alpha |V(G_{H \cap H'})|}{2} \\ &\geq \frac{\alpha}{2} t. \end{aligned}$$

Hence, the probability that H' is realized is at most $p^{\frac{\alpha t}{2}}$. The number of ways to choose the t other vertices is $\binom{k}{t} \left(\frac{n}{k}\right)^t$. Hence the expected number of such occurrences is $\mu_t \leq \binom{k}{t} \left(\frac{n}{k}\right)^t p^{\frac{\alpha t}{2}} = \binom{k}{t} \left(\frac{d^\alpha}{k^2 n^{\alpha-2}}\right)^{\frac{t}{2}}$.

We have:

1. $\mu_k < E[Y]$.
2. $\sum_{t \leq \frac{k}{2}} \frac{\mu_t}{E[Y]} \leq 2^k \left(\frac{d^\alpha}{k^2 n^{\alpha-2}}\right)^{\frac{-k}{4}} = \left(\frac{16k^2 n^{\alpha-2}}{d^\alpha}\right)^{\frac{k}{4}}$.
3. $\sum_{t \geq \frac{k}{2}}^{k-1} \frac{\mu_t}{E[Y]} \leq \sum_{t \geq \frac{k}{2}}^{k-1} k^{k-t} \left(\frac{d^\alpha}{k^2 n^{\alpha-2}}\right)^{\frac{t-k}{2}} = \sum_{t \geq \frac{k}{2}}^{k-1} \left(\frac{d^\alpha}{k^4 n^{\alpha-2}}\right)^{\frac{t-k}{2}}$. The term $t = k - 1$ dominates (when $d^\alpha \geq 2k^4 n^{\alpha-2}$) and hence the sum is at most roughly $\sqrt{\frac{k^4 n^{\alpha-2}}{d^\alpha}}$.

Recall that $\frac{k^4 n^{\alpha-2}}{d^\alpha} \leq \epsilon^2$. Then $\sum \mu_i \leq (1 + \epsilon) E[Y]$. Hence $E[Y^2] \leq (1 + \epsilon) (E[Y])^2$. Recall that $X \leq Y$ and that $E[X] \geq (1 - \epsilon) E[Y]$. Hence $E[X^2] \leq \frac{1+\epsilon}{(1-\epsilon)^2} E[X]^2 \leq (1 + 4\epsilon) E[X]^2$ (the last inequality holds because $\epsilon \leq \frac{1}{5}$). We get that $\sigma^2[X] = E[X^2] - E[X]^2 \leq 4\epsilon E[X]^2$. By Chebychev's inequality we conclude that $Pr[X \geq 0] \geq 1 - \frac{\sigma^2[X]}{E[X]^2} \geq 1 - 4\epsilon$. \square

Remark: The proof of Theorem D.5 shows that the number of copies of H in G is likely to be close to its expectation, and hence large (this will be useful in the next section). Also, simple modifications to the proof can be used in order to show the existence of many disjoint copies (where the number grows as ϵ decreases).

Corollary D.6. *For every $0.467 < \delta < \frac{1}{2}$ and $\epsilon < \frac{1}{8}$ there is some $\rho > 0$ such that the following holds for every large enough n . Let H be an arbitrary balanced graph with average degree 3.75 on $k = n^\rho$ vertices. Let G be a random graph on n vertices with average degree $d = n^\delta$ (which we refer to as $G_{n,d}$). Then with probability larger than $1 - 4\epsilon$ (over choice of G), G contains a set S of k vertices such that:*

1. The subgraph induced on S is H .
2. No two vertices of S have a common neighbor outside S .

Proof. In Theorem D.5, choose $\epsilon < \frac{1}{8}$, $\alpha = 3.75$, and choose k such that $\frac{k^2 d^2}{n} \leq \epsilon$ and $\frac{k^4 n^{\alpha-2}}{d^\alpha} \leq \epsilon^2$. Specifically, one may choose $k = \min \left[\sqrt{\epsilon n^{\frac{1-2\delta}{2}}}, \sqrt{\epsilon n^{\frac{\alpha\delta-\alpha+2}{4}}} \right] = n^{\Omega(1)}$. \square

Theorem D.7. (Restatement of Lemma 2.6). *Coloring a balanced graph with an average degree 3.75 with a balanced 3-coloring is NP-hard.*

Proof. It is known that 3-coloring 4-regular graphs is NP-hard, see [19] (and actually, with slight modifications, this proof shows it as well). Therefore it is enough to show that there exists a polynomial time reduction R such that for any given 4-regular graph H it holds that

1. $R(H)$ is a balanced graph with an average degree of 3.75.
2. H is a 3-colorable graph if and only if $R(H)$ is 3-colorable and given a (legal) 3-coloring to $R(H)$ one can (legally) 3-color H in a polynomial time.
3. If $R(H)$ is 3-colorable then it has a balanced coloring.

The reduction is as follows. For every vertex v of H consider its four edges e_1, e_2, e_3, e_4 , replace v by the graph in Figure 1 (denote this graph by $R(H, v)$) and then connect edge e_i to vertex u_i . Note that the average degree of $R(H)$ is 3.75. Also note that in any legal 3-coloring of $R(H)$ the vertices v_i, u_i get all the same color and the second assertion of R follows.

We show that $R(H)$ is a balanced graph. For a vertex v of H let $R(H, v_i)$ be the set $\{v_i, u_i, A_i, B_i\}$. Consider a subset S^* of the vertices of $R(H)$ such that the average degree on the induced subgraph $R(H)_{S^*}$ is maximized to α^* . Let $\alpha^*(R(H, v_i))$ be the average degree of the vertices $R(H, v_i) \cap S^*$ in $R(H)_{S^*}$. As the sets $R(H, v_i)$ are disjoint and their union is the vertex set of $R(H)$ it follows that α^* is upper bounded by $\alpha^*(R(H, v_i))$ for some v_i . But for every v_i and S^* we are averaging at most 4 vertices of degree bounded by 4, where at least one of them is of degree bounded by 3. It follows that

$$\alpha^* \leq \max_{v_i} \alpha^*(R(H, v_i)) \leq \frac{3 * 4 + 3}{4} = 3.75.$$

To show the third assertion of R it is enough to take a disjoint union of 3 copies of the above construction (note that the disjoint union of two balanced graphs is balanced). \square

Remark: The construction and analysis of Theorem D.7 can be modified to show that for every $\epsilon > 0$, 3-coloring of balanced graphs with average degree $(\frac{10}{3} + \epsilon)$ is NP-hard. Every vertex v_i in the graph of Figure 1 is replaced by a 4-vertex gadget with five edges of structure similar to the graph induced on v_1, A_1, B_1, v_2 , with the v vertices as endpoints of the gadget. For example, if v_2 is replaced then one endpoint is connected to A_1 and B_1 , and the other endpoint is connected to A_2 and B_2 . Observe that the two endpoints of the gadget must have the same color in every legal 3-coloring. Each such replacement increases the number of vertices by three and the number of edges by five, hence bringing the average

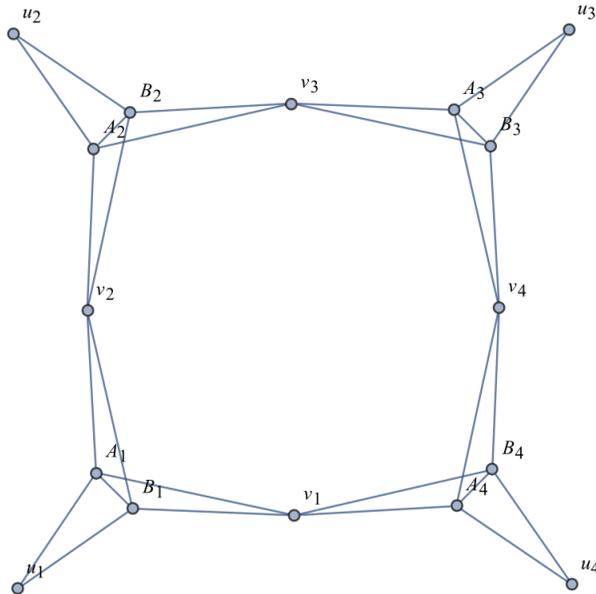


Figure 1: The construction of Theorem D.7.

degree closer to $\frac{10}{3}$. Repeating this replacement recursively (until the distance between A_1 and A_2 becomes $\Omega(\frac{1}{\epsilon})$) gives a balanced graph with average degree below $(\frac{10}{3} + \epsilon)$. Further details omitted.

For the sake of intuition, we temporarily restrict attention to algorithms that we refer to as *decomposable* (a restriction that will be lifted later).

Definition D.8. An algorithm A for 3-coloring is *decomposable* if for every disconnected input graph G , algorithm A is applied independently to each of G 's connected components.

Natural 3-coloring algorithms are decomposable. In fact, we are not aware of any coloring algorithm that is not decomposable. Moreover, in works on random and semi-random models of inputs, it makes sense to require coloring algorithms to be decomposable, as an algorithm that is not decomposable would presumably involve aspects that are very specific to the model and would not generalize to other models.

One can imagine that in some contexts the use of algorithms that are not decomposable may offer advantages. This may happen if the input graph is generated in such a way that the structure of one component contains hints as to how to color other components. Perhaps the simplest form of a hint is the following. Suppose that the input graph is known to be generated with a balanced coloring (in which each color class is of size $n/3$), and furthermore, is known to be generated such that in each component the 3-coloring is unique. Then for an input graph with two components, once one colors the first component, one knows how many vertices of each color class there should be in the second component. This simple form of a hint saves at most polynomial factors in the running time, because it involves only

$O(\log n)$ bits of information, and hence the hint can be guessed. Nevertheless, it illustrates the point that under some generation models of input graphs, it is possible that algorithms that are not decomposable will be faster than algorithm that are decomposable.

Here we consider 3-coloring $G_{n,d}$ with an adversarially planted balanced 3-coloring. We show that given the decomposable-algorithm assumption, a hardness result can be derived. In Section D.3 a full proof is given without the decomposability assumption.

Theorem D.9. *Suppose that for some $0.467 < \delta < \frac{1}{2}$ and $d = n^\delta$ there is a decomposable algorithm that with probability at least $\frac{1}{2}$ (over choice from $G_{n,d}$ and for every adversary) 3-colors $G_{n,d}$ with an adversarially planted balanced 3-coloring. Then $P=NP$.*

Proof. By Theorem D.7 it follows that 3-coloring balanced graphs of average degree 3.75 is NP-hard.

Suppose there was an algorithm A for 3-coloring $G_{n,d}$ with an adversarially planted balanced 3-coloring as in the statement of the theorem. Consider now an arbitrary balanced graph H with average degree 3.75 of size $k = n^\rho$ (where ρ is as in Corollary D.6), and associate with it an adversary H' . On input a random graph G from $G_{n,d}$, the graph has probability more than $\frac{1}{2}$ of satisfying the conclusion of Theorem D.5. The adversary H' (who is not computationally bounded) does the following.

1. If G does not satisfy the conclusion of Theorem D.5 with respect to H , then the adversary H' plants in it a random balanced coloring.
2. If G satisfies the conclusion of Theorem D.5 with respect to H then the adversary H' leaves H untouched and then:
 - (a) If H is 3-colorable, for each color class of H it colors its neighborhood outside H with the same color as in H , and then completes to a balanced planted 3-coloring at random. Observe that this planted coloring disconnects H from the rest of G , because all original edges between H and the rest of G are between pairs of vertices of the same color.
 - (b) If H is not 3-colorable, the adversary removes all edges between H and the rest of G , and randomly produces a balanced planted coloring of the rest of G .

Case 2 above happens with probability greater than $\frac{1}{2}$, by Corollary D.6.

Suppose that H is not 3-colorable (case 2(b)). Then A must fail to 3-color H .

Suppose now that H is 3-colorable (case 2(a)). Because A is decomposable, it must color H without seeing the rest of G . Because A succeeds for every adversary on at least half the inputs (over choice from $G_{n,d}$), and for adversary H' over half the inputs generate H , A must succeed to 3-color H . (We assumed here that A is deterministic. If A is randomized then choose $\epsilon < \frac{1}{16}$ and then A must succeed with probability at least $\frac{2}{3}$. In this case the conclusion will be that NP has randomized polynomial time algorithms with one sided error.)

Hence the output of $A(H)$ determines whether H is 3-colorable. As this applies to every H , and the sizes of H and G are polynomially related, this implies that A solves in polynomial time an NP-hard problem, implying $P = NP$. \square

There are two weaknesses of Theorem D.9. One is that it requires $d > n^{0.467}$: at lower densities the input graph is unlikely to contain a given H with average degree 3.75. The degree d can be lowered to roughly $n^{0.4}$ using the remark following the proof of Theorem D.7. However, it cannot be lowered below $n^{1/3}$ (using our techniques), because of Proposition 2.4. The other weakness is that it requires A to be decomposable. The decomposability weakness can be overcome using the following approach.

Suppose there was an algorithm A for 3-coloring $G_{n,d}$ with an adversarially planted balanced 3-coloring, that succeeds with probability at least $\frac{1}{2}$ over choice of G (for every adversary). Given a 3.75-balanced graph H on k vertices, give A as input a graph G' composed of two disjoint parts. One is H and the other is a random subgraph of size $n - k$ of a random graph from $G_{n,d}$ with a randomly planted balanced 3-coloring. This would prove Theorem D.9 if the distribution generated by this process is statistically close to the one generated by the adversary H' . The techniques in [22] can be extended in order to prove statistical closeness and this is done in the next section.

D.3 Hardness result without the decomposable-algorithm assumption

Let H be an arbitrary balanced graph with average degree α and k vertices, for $\alpha = 3.75$. Let G be a graph with n vertices. Assume that k divides n (this assumption can be removed) and consider a fixed partition of the vertex set of G to k disjoint subsets of vertices, each of size $\frac{n}{k}$. Let $C_H(G)$ be the number of induced sub-graphs of G that are isomorphic to H such that they obey the partition (see the definition in the proof of Theorem D.9) and let E_H be $\mathbb{E}_{G \sim G_{n,d}}[C_H(G)]$.

Note that

$$E_H = \left(\frac{n}{k}\right)^k p^{\frac{\alpha}{2}k} (1-p)^{\binom{k}{2} - \frac{\alpha}{2}k}, \quad (14)$$

where $p = \frac{d}{n-1}$.

We consider the following distribution of random graphs with the graph H being planted as an induced sub-graph.

Definition D.10. A graph G with n vertices is distributed by $G_{n,d,H}$ if it is created by the following random process.

1. Take a random graph G' distributed by $G_{n,d}$.
2. Choose a random subset K of k vertices from G' that obeys the partition.
3. Replace the induced subgraph of G' on K by H (we say that H is randomly planted in G').

Given a graph G , we denote by $p(G)$ the probability to output G according to $G_{n,d}$ and by $p'(G)$ the probability to output G according to $G_{n,d,H}$.

Claim D.11. For any given graph G it holds that $p'(G) = \frac{C_H(G)}{E_H} p(G)$.

Proof. Let e be the number of edges in G and consider $p'(G)$. Out of the $\binom{n}{k}^k$ options to choose K (in $G_{n,d,H}$) only $C_H(G)$ options are such that the induced sub graph on K is H so that the resulting graph could be G . Given that we chose a suitable K , the rest of the edges ($e - \frac{\alpha}{2}k$) should agree with G . It follows that

$$\begin{aligned} p'(G) &= \frac{C_H(G)}{\binom{n}{k}^k} p^{e - \frac{\alpha}{2}k} (1-p)^{\binom{n}{2} - \binom{k}{2} - e + \frac{\alpha}{2}k} \\ &= \frac{C_H(G)}{E_H} p^e (1-p)^{\binom{n}{2} - e} \\ &= \frac{C_H(G)}{E_H} p(G). \end{aligned}$$

The second equality follows from Equation 14. \square

Recall the definition of the random variables X, Y from the proof of Theorem D.9. Moreover, the following claim follows from the proof of Theorem D.9.

Claim D.12.

$$\sigma^2[X] = 4\epsilon \mathbb{E}[X]^2.$$

Theorem D.13. (*Restatement of Theorem 1.4b*). *Let $G \sim G_{n,d}$ be a random graph, where $d = n^\delta$ for $0.467 \leq \delta < \frac{1}{2}$, and let γ be an arbitrary small constant. If there exists a randomized algorithm that colors $G \sim G_{n,d}$ after an adversarial color-planting with probability γ (over the distribution $G_{n,d}$ and the randomness of the algorithm) then $RP = NP$.*

Proof. Consider $\epsilon = \frac{\gamma}{100}$ and set $k = \min\left[\sqrt{\epsilon n^{\frac{1-2\delta}{2}}}, \sqrt{\epsilon n^{\frac{\alpha\delta - \alpha + 2}{4}}}\right] = n^{\Omega(1)}$ (so that the conditions of Corollary D.6 and Theorem D.5 hold). Assume that there exists an algorithm A as in the theorem. The probability measure of graphs from $G_{n,d}$ that A colors with respect to *all* possible color planting with probability (over the randomness of A) at least $\frac{\gamma}{2}$ is at least $\frac{\gamma}{2}$. This holds by averaging and because we can consider an adversary that, given any input graph, simulates A and try all possible color planting in order fail A with the largest probability (over the randomness of A).

By Chebychev's inequality and Claim D.12 it holds that

$$\Pr_{G \sim G_{n,d}} [X \leq \rho \mathbb{E}[X]] \leq \frac{4\epsilon}{(1-\rho)^2}.$$

Note that $X \leq C_H(G) \leq Y$. By the proof of Theorem D.5 it hold that

$$\mathbb{E}[C_H(G)] \leq \mathbb{E}[Y] \leq \frac{1}{1-\epsilon} \mathbb{E}[X].$$

Hence

$$\Pr_{G \sim G_{n,d}} [X \leq \rho(1-\epsilon) \mathbb{E}[C_H(G)]] \leq \frac{4\epsilon}{(1-\rho)^2}.$$

Set ρ to be such that $\frac{4\epsilon}{(1-\rho)^2} \leq \frac{1}{4}\gamma$ and that $\frac{1}{2}\rho \geq \frac{1}{10}$. Therefore that the probability measure of graphs that A colors (with probability, over the randomness of A , of at least

$\frac{\gamma}{2}$ for every color planting) with $X \geq \rho(1 - \epsilon) \mathbb{E}[C_H(G)]$ is at least $\frac{1}{4}\gamma$. By Claim D.11 it follows that the probability measure with respect to $G_{n,d,H}$ of graphs that A colors (after any adversarial planting with probability at least $\frac{\gamma}{2}$) is at least $\frac{1}{2}\gamma\rho(1 - \epsilon) \geq \frac{1}{11}\gamma$.

Fix H to be an arbitrary balanced graph with average degree 3.75 with k vertices that has a balanced 3-coloring. Now we show that we can use A to color H .

Given $G \sim G_{n,d,H}$ we consider the following distribution \tilde{G}_H for graphs with an adversarial coloring. If any vertex that is not on the induced planted (by $G_{n,d,H}$) graph H has two or more neighbors in the planted induced graph, denote this event by S_1 , then color G arbitrarily. Otherwise for the planted graph use a coloring that agrees with the coloring of H . For the rest of the vertices, if a vertex has a neighbor in the planted graph color it by the same color of its neighbor and the rest of the vertices are colored in such away that the coloring is balanced. More specifically, from all the balanced coloring we choose one at random (again, if there is no possible balanced coloring then we color G arbitrarily). Since $k = o(\frac{n}{d})$ then, by the union bound and the Chernoff bound, no vertex in G has more than $(1 + c_1)d$ neighbors with probability at most $n2^{-\Omega(c_1d)} \leq \gamma/44$. Hence there are such balanced colorings with high probability. Denote the event that no such balanced coloring is possible by S_2 . The event S_1 happens with probability at most $k^2 \frac{d^2}{n} \leq \gamma/44$. A graph from \tilde{G}_H is called *good* if the events S_1, S_2 do not hold. Given that G is a good graph, all possible balanced coloring on $G \setminus H$ are equally distributed.

If an adversary knows the subset S of vertices that the distribution $G_{n,d,H}$ plants H on then the distribution \tilde{G}_H can be created by this adversary. A subtle point is that the adversary can guess S . Given a graph $G \sim G_{n,d,H}$ the adversary can calculate for every subset S' (that obeys the partition) that satisfies $G_{S'} = H$ what is the probability that S' is the planted subset, then choose a subset S' with the calculated probability and behave as S' is the planted subset. It follows that the distribution after the above preprocessing is the same distribution as if the adversary knows S .

In total, the probability measure of good graphs in \tilde{G}_H that A can color (with probability, over the randomness of A , of at least $\frac{\gamma}{2}$ for every color planting) is at least $\gamma/22$. The key point is that the conditional, on being good, distribution of graphs \tilde{G}_H can be sampled in a polynomial time by taking the vertex disjoint union of the graph H and a random graph from $G_{n-k,d}$ with a random balanced planted coloring (and apply an appropriate random permutation). If we run algorithm A on $\Omega\left(\frac{44}{\gamma^2}\right)$ random instances from \tilde{G}_H (which again we can sample efficiently) then with high probability A will color H (that is a graph with a $\text{poly}(n)$ vertices) with high probability. By Theorem D.7 the proof follows. \square

D.4 Proof of Proposition 2.4

Proposition D.14. (Restatement of Proposition 2.4). *Let \mathcal{Q} be an arbitrary class of graphs. Then either there is a polynomial time algorithm for solving 3-colorability on every graph in \mathcal{Q} , or \mathcal{Q} contains graphs that are unlikely to appear as subgraphs of a random graph from $G_{n,p}$, if $p = n^{-2/3}$.*

Proof. We say that a class \mathcal{Q} is *3-sparse* if every graph in \mathcal{Q} has average degree at most 3, and furthermore, has no subgraph of average degree above 3. There are two cases to consider.

Suppose that \mathcal{Q} is 3-sparse. In this case, there is a polynomial time algorithm that solves 3-colorably on all graphs from \mathcal{Q} . Let $Q \in \mathcal{Q}$ be an arbitrary such graph. Iteratively remove

from Q vertices of degree less than 3 until no longer possible, and let Q' be the remaining graph. Every 3-coloring of Q' can be extended to Q by inductive coloring. Hence it remains to 3-color Q' . If Q' is empty then we are done. If Q' is nonempty, then 3-sparseness of Q implies that Q' is 3-regular. In this case, Brook's theorem [9] (see [28] for an algorithmic version of it) implies that we can decide whether Q' is 3-colorable, and if so, 3-color it in polynomial time.

Suppose that Q is not 3-sparse. Then it contains some graph Q and within it some subgraph Q' such that Q' contains at least $\frac{3k}{2} + 1$ edges, where k denotes the number of vertices in Q' . The probability that a random $G_{n,p}$ graph with $p = n^{-2/3}$ contains an induced copy of Q' is at most $n^k p^{3k/2+1} = p = n^{-2/3}$. \square

E Extending the results to more than 3 colors

In this section we elaborate on our results when using $k \geq 4$ colors. When stating our results we shall use the notation $O_k(\cdot)$ to denote hidden constants whose value may depend on the number k of colors. We derive the following theorems.

Theorem E.1. *(Generalization of Theorem 1.1). For any positive k there exists a constant c_k , such that if the average degree in the host graph satisfy $c_k < d < n$ then the following holds. In all four models (H_A/P_A , H_A/P_R , H_R/P_A , H_R/P_R) there is a polynomial time algorithm that finds a b -partial coloring for $b = O_k\left(\left(\frac{\lambda}{d}\right)^2 n\right)$. For the models with random host graphs (H_R) and/or random planted colorings (P_R), the algorithm succeeds with high probability over choice of random host graph H and/or random planted coloring P .*

Theorem E.2. *(Generalization of Theorem 1.2). For any positive k there exists a constant C_k , such that the following holds. In the H_A/P_A model, for every d in the range $C_k < d < n^{1-\epsilon}$ (where $\epsilon > 0$ is arbitrarily small), it is NP-hard to k -color a graph with a planted k -coloring, even when $\lambda = O_k(\sqrt{d})$.*

Theorem E.3. *(Generalization of Theorem 1.3). For any positive k there exist constants $0 < c_k < 1$ and $C_k > 1$, such that the following holds. In the H_A/P_R model there is a polynomial time algorithm with the following properties. For every d in the range $C_k < d \leq n - 1$ and every $\lambda \leq c_k d$, for every host graph within the model, the algorithm with high probability (over the choice of random planted k -coloring) finds a legal k -coloring.*

Theorem E.4. *(Generalization of Theorem 1.4b). Let $G \sim G_{n,d}$ be a random graph, where $d = n^\delta$ for $0.467 \leq \delta < 1$, let $k \geq 4$, and let γ be an arbitrary small constant. If there exists a randomized algorithm that k -colors $G \sim G_{n,d}$ after an adversarial color-planting with probability γ (over the distribution $G_{n,d}$ and the randomness of the algorithm) then $RP = NP$.*

It turns out that theorems 1.1, 1.2, 1.3 and 1.4b extend to $k \geq 4$. Theorem 1.4a does not extend to $k \geq 4$ as this would contradict Theorem E.4.

Theorems 1.1, 1.2 and 1.3 follow in a rather straightforward way from our proofs of the respective theorems 1.1, 1.2 and 1.3. We provide some more details.

We start with the generalization of Theorem B.1 to $k \geq 4$. The statement of Theorem B.1 uses two predefined vectors (\bar{x} and \bar{y}) that encodes the planted 3-coloring (see Definition A.7). Here we describe how to define $k - 1$ vectors when $k \geq 4$.

Let $P_k(G)$ be the graph G after a random k -color-planting has been applied. Let V_1, V_2, \dots, V_k be a partition of V induced by the color planting and let P be a function that maps each vertex to its color class. Let $P_k = \mathbf{1}_{k \times k} - I_k$ be the matrix obtained by the all-one matrix minus the identity matrix and let the vectors p_0, p_1, \dots, p_{k-1} be an orthogonal set of eigenvectors of P where p_0 is the all-one vector. For a vector \vec{x} we denote by $\vec{x}(j)$ its j -th coordinate and recall that we denote by \bar{x} the vector $\frac{\vec{x}}{\|\vec{x}\|_2}$.

Definition E.5. We define the following k vectors $\vec{x}_0, \dots, \vec{x}_{k-1}$ in \mathbb{R}^n . For each j , $0 \leq j \leq k - 1$, the vector \vec{x}_j gives to coordinate i the value $p_j(P(i))$.

One can check that Definition A.7 is an instantiation of Definition E.5 in the case $k = 3$. Moreover Theorem E.6 below follows by a direct generalization of the proof of Theorem B.1.

Theorem E.6. *Let G be a d regular λ -expander and $P_k(G)$ be the graph G after a random k -color planting, where $\lambda \leq \Theta(d)$. With high probability the following holds.*

1. *The eigenvalues of $P_k(G)$ have the following spectrum.*

- (a) $\lambda_1(P_k(G)) \geq (1 - 2^{-\Omega(d)}) \frac{k-1}{k} d$.
- (b) $\lambda_{n-k+2}(P_k(G)) \leq -\frac{1}{k} d \left(1 - \frac{k}{\sqrt{d}}\right)$.
- (c) $|\lambda_i(P_k(G))| \leq 2\lambda + O_k(\sqrt{d})$ for all $2 \leq i \leq n - k + 1$.

2. *The following vectors exist.*

$\vec{\epsilon}_{\bar{x}_j}$ such that $\|\vec{\epsilon}_{\bar{x}_j}\|_2 = O_k\left(\frac{1}{\sqrt{d}}\right)$ and $\bar{x}_j + \vec{\epsilon}_{\bar{x}_j} \in \text{span}\left(\{e_i(P_k(G))\}_{i \in \{n-k+2, \dots, n\}}\right)$, for $1 \leq j \leq k - 1$.

Lemma C.4 is a variant of Theorem B.1 for the case of adversarial balanced 3-coloring. Lemma C.4 can be generalized in a similar manner as the above for the case of adversarial balanced k -coloring.

We now present a clustering algorithm (which is a generalization of Algorithm 2) to the case planted $k \geq 4$ -coloring. We chose here a randomized version due to improvement in the running times over the deterministic version.

Algorithm 10 Random Spectral k -Clustering

Input: A graph $P_k(G)$ and three positive constants $c \leq \frac{1}{2}$, c_k^1 and c_k^2 (the last two constants depend on k).

1. Compute the eigenvectors $e_{n-l} := e_{n-l}(P_k(G))$ for $0 \leq l \leq k-2$.
2. Choose uniformly at random a set of k vertices $v_1, v_2, \dots, v_k \in V(P_k(G))$.
3. If there are $1 \leq i < j \leq k$ satisfying

$$\sum_{l=0}^{l=k-2} \left((e_{n-l})_{v_i} - (e_{n-l})_{v_j} \right)^2 < \frac{4}{c_k^1 n}.$$

go to Step 2.

4. Put a vertex $u \in V(G')$ in S_i if it holds that

$$\sum_{l=0}^{l=k-2} \left((e_{n-l})_u - (e_{n-l})_{v_i} \right)^2 < \frac{1}{c_k^1 n}.$$

5. If for every $i = 1, 2, \dots, k$ it holds that $|S_i| \geq \left(\frac{1}{k} - \frac{1}{c_k^2 d^{2c}} \right) n$ then output a coloring C of G' that sets $col_C(u) = i$ for every $1 \leq i \leq k$ and $u \in S_i$, and colors the remaining vertices (if there are any) arbitrarily. Otherwise go to Step 2.
-

The following lemma shows that under sufficient conditions the above clustering algorithm, Algorithm 10, outputs a good approximated coloring. These conditions are stated in the lemma and by Theorem E.6 these conditions hold with high probability.

Lemma E.7. (Generalization of Lemma B.16). *For any positive k there exist constants c_k^1 and c_k^2 such that the following holds. Let $P_k(G)$ be as above and c be a positive constant. Suppose that the following vectors exist for $0 \leq l \leq k-1$ (recall Definition E.5): $\vec{\epsilon}_{\bar{x}(l)}$ such that $\|\vec{\epsilon}_{\bar{x}(l)}\|_2 = O_k(d^{-c})$ and $\bar{x}_l + \vec{\epsilon}_{\bar{x}(l)} \in \text{span}\left(\{e_i(P_k(G))\}_{i \in \{n-k+1, n\}}\right)$. Then Algorithm 10 outputs an $O_k(nd^{-2c})$ -approximated coloring. The expected running time of Algorithm 10 is $\tilde{O}\left(\frac{k^k}{k!}n\right)$.*

An example of how to use Lemma E.7 is as follows. For $P_k(G)$ by Theorem E.6 we have $\|\vec{\epsilon}_{\bar{x}(l)}\|_2 = O_k\left(\frac{1}{\sqrt{d}}\right)$. Thus running Algorithm 10 with $c = \frac{1}{2}$ results in $O_k\left(\frac{n}{d}\right)$ -approximated coloring.

The analysis of Algorithm 10 running time is discussed in the poof of Lemma B.16. We note that one can show an expected running time of $\tilde{O}\left(\frac{k^k}{k!} + n\right)$ for Algorithm 10.

E.1 Hardness result for random graphs with adversarial 4-color planting

In this section we extend Theorem D.13 to the case of adversarial planting with $k > 3$ colors. For simplicity, we present the proof only for the case $k = 4$, but it is not difficult to extend it to any constant k .

Let us begin with an overview of the proof. Recall the overview of the proof of Theorem 1.4b given in Section 2.5, and the terminology that was used there. The hardness of 3-coloring in H_R/P_A was by reduction from the class \mathcal{Q} of balanced graphs with average degree 3.75, on which 3-coloring is NP-hard. For this class, 4-coloring is easy (by inductive coloring), but nevertheless we shall use the same class \mathcal{Q} in the hardness result for 4-coloring. We have already seen (in Lemma 2.7) that for every graph $Q \in \mathcal{Q}$ of size n^ϵ , random graphs of sufficiently high average degree n^δ are likely to contain Q as a subgraph. For hardness of 3-coloring, given a random G_{n,n^δ} host graph H , the adversary plants in H a 3-coloring that isolates a copy of Q . For hardness of 4-coloring, it is useless to plant in H a 4-coloring that isolates a copy a copy of Q , because 4-coloring of Q is easy. Instead, the plan is for the adversary to plant in H a 4-coloring in which all neighbors of Q outside Q have the same color. This leaves only three colors for Q , and hence 4-coloring of H would imply 3-coloring of Q .

To make this plan work, one needs every vertex of Q to have at least one neighbor in $H - Q$, and all vertices of Q combined should have less than $n/4$ neighbors in $H - Q$. Luckily, for a random copy of Q in H , both these properties happen with overwhelming probability as long as $\epsilon + \delta < 1$. Consequently, the hardness result for 4-coloring has the following two advantages over the one for 3-coloring (that required vertices in Q not to have common neighbors in $H - Q$). One is that there is no need to require that $\delta < \frac{1}{2} - \epsilon$. In particular, this shows that the positive results of Theorem 1.4a do not hold when $k \geq 4$. The other advantage is that the fraction of host graphs $H \in_R G_{n,n^\delta}$ on which the reduction fails is smaller than the corresponding fraction in the proof of Theorem 1.4b. (For simplicity, we shall not address this point in our proofs.)

There is a property that is required for hardness of 4-coloring but was not needed for the hardness of 3-coloring. That property is that after the adversary plants the 4-coloring, we need that in every 4-coloring of G , there is some color c such every vertex of Q has at least one neighbor in $H - Q$ of color c . This ensures that every 4-coloring of G indeed 3-colors Q . The way we show that this property holds is through Lemma E.11 that shows that in a sufficiently dense random graph, a planted random k -coloring is almost surely the only legal k -coloring of the resulting graph.

This completes the overview of our proof approach.

We start with a variant of Theorem D.5.

Theorem E.8. *For $0 < \epsilon \leq \frac{1}{7}$ and $3 < \alpha < 4$, suppose that $\frac{k^2 d}{n} \leq \epsilon$ and $\frac{k^4 n^{\alpha-2}}{d^\alpha} \leq \epsilon^2$. Let H be an arbitrary balanced graph on k vertices with an average degree α and let $G \sim G_{n,d}$ be a random graph. Then with probability at least $1 - 4\epsilon$ (over choice of G), G contains a set S of k vertices such that:*

1. *The subgraph induced on S is H .*
2. *Each vertex of S has a neighbor outside S .*

3. The total sum of degrees of vertices in S is at most $\frac{n-k}{4}$.

Proof. Let $p = \frac{d}{n-1}$ be the edge probability in G . Suppose for simplicity (an assumption that can be removed) that k divides n . Partition the vertex set of G into k equal parts of size n/k each. Vertex i of H will be required to come from part i . A set S with such a property is said to *obey the partition*.

Let X be a random variable counting the number of sets S obeying the partition that satisfy the theorem. Let Y be a random variable counting the number of sets S obeying the partition that have H as an edge induced subgraph (but may have additional edges, and may not satisfy item 2 of the theorem).

$$E[Y] = \left(\frac{n}{k}\right)^k p^{\frac{\alpha k}{2}} = \left(\frac{d^\alpha}{k^2 n^{\alpha-2}}\right)^{\frac{k}{2}}.$$

A set S in Y contributes to X if the following conditions hold

1. It has no internal edges beyond those of H (which happens with probability at least $1 - \binom{k}{2} \frac{d}{n}$).
2. Every vertex of it has a neighbor outside S (which happens with probability at least $1 - ke^{-\frac{dn}{4}}$).
3. The total sum of degrees of vertices in S is at most $\frac{n-k}{4}$. By the union and the Chernoff bounds no vertex in G has more than $(1 + c_1)d$ neighbors with probability at most $n2^{-\Omega(c_1 d)}$. Since $k = o(\frac{n}{d})$ this assertion is satisfied (for S in Y) with probability $n2^{-\Omega(c_1 d)}$ as well.

Consequently:

$$E[X] \geq E[Y] \left(1 - \frac{k^2 d^2}{n}\right) \geq (1 - \epsilon)E[Y].$$

Using $\frac{k^4 n^{\alpha-2}}{d^\alpha} \leq \epsilon^2$ the computation of $E[Y^2]$ and the rest of the proof are the same as in Theorem D.5. □

Corollary E.9. *For every $\delta \geq 0.467$ and $\epsilon < \frac{1}{8}$ there is some $\rho > 0$ such that the following holds for every large enough n . Let H be an arbitrary balanced graph with average degree 3.75 on $k = n^\rho$ vertices. Let G be a random graph on n vertices with average degree $d = n^\delta$ (which we refer to as $G_{n,d}$). Then with probability larger than $1 - 4\epsilon$ (over choice of G), G contains a set S of k vertices such that:*

1. The subgraph induced on S is H .
2. Each vertex of S has a neighbor outside S .
3. The total sum of degrees of vertices in S is at most $\frac{n-k}{4}$.

Proof. In Theorem D.5, choose $\epsilon < \frac{1}{8}$, $\alpha = 3.75$, and choose k such that $\frac{k^2 d}{n} \leq \epsilon$ and $\frac{k^4 n^{\alpha-2}}{d^\alpha} \leq \epsilon^2$. Specifically, one may choose $k = \min \left[\sqrt{\epsilon n^{\frac{1-\delta}{2}}}, \sqrt{\epsilon n^{\frac{\alpha\delta - \alpha + 2}{4}}} \right] = n^{\Omega(1)}$. □

Theorem E.10. (Generalization of Theorem 1.4b for the $k = 4$ case). Let $G \sim G_{n,d}$ be a random graph, where $d = n^\delta$ for $0.467 \leq \delta < 1$, and let γ be an arbitrary small constant. If there exists a randomized algorithm that colors $G \sim G_{n,d}$ after an adversarial color-planting with probability γ (over the distribution $G_{n,d}$ and the randomness of the algorithm) then $RP = NP$.

Proof. Suppose that there exists an algorithm A as in the theorem. Consider $\epsilon = \frac{\gamma}{100}$ and set $k = \min \left[\sqrt{\epsilon n^{\frac{1-\delta}{2}}}, \sqrt{\epsilon n^{\frac{\alpha\delta - \alpha + 2}{4}}} \right] = n^{\Omega(1)}$ (so that the conditions of Corollary E.9 and Theorem E.8 hold). Let H be an arbitrary balanced graph with average degree 3.75 with k vertices that has a balanced 3-coloring. We show how A can be used in order to color H . Recall Definition D.10 for the graphs distribution $G_{n,d,H}$. By the proof of Theorem D.13 it follows that the probability measure with respect to $G_{n,d,H}$ of graphs that A colors (after any adversarial planting, with probability at least $\frac{\gamma}{2}$) is at least $\frac{1}{2}\gamma\rho(1 - \epsilon) \geq \frac{1}{11}\gamma$.

Given $G \sim G_{n,d,H}$ we consider the following distribution \tilde{G}_H for graphs with an adversarial coloring. Let S_1 be the event that some vertex in the induced planted graph H (in $G_{n,d,H}$) has no neighbors outside H . Let S_2 be the event that the total number of neighbors (among the remaining vertices in G) that the induced planted graph H has is larger than $n/4$. If either event S_1 or S_2 happen (these are considered bad events), then plant an arbitrary balanced 4-coloring in G . If neither event S_1 nor S_2 happens (this will be shown to be the typical case), plant in G a balanced 4-coloring chosen uniformly at random, conditioned on the following two events: the planted graph is colored by a balanced 3-coloring that agrees with the coloring of H , and all neighbors of H (outside H) are colored by the fourth color.

The event S_1 happens with probability at most $k^2 e^{-\frac{dn}{4}} \leq \gamma/44$. As to event S_2 , since $k = o\left(\frac{n}{d}\right)$ then, by the union bound and the Chernoff bound, no vertex in G has more than $(1 + c_1)d$ neighbors with probability at most $n2^{-\Omega(c_1 d)} \leq \gamma/44$. Consequently, event S_2 happens with probability at most $\gamma/44$ as well.

One last event S_3 to consider is that the 4-coloring of the graph induced on vertices not in H is not unique. By Lemma E.11 below and since a random graph is a $O(\sqrt{d})$ -expander [15, 18, 17], it follows that S_3 happens with probability at most $\frac{\gamma}{44}$ as well. A graph from \tilde{G}_H is called *good* if the events S_1, S_2, S_3 do not hold.

In total, the probability measure of good graphs in \tilde{G}_H that A colors with probability of at least $\frac{\gamma}{2}$ for every color planting (over the randomness of A) is at least $\gamma/50$. Moreover, the distribution \tilde{G}_H of good graphs can be sampled in a polynomial time as follows:

1. Take the vertex disjoint union of the graph H and a random graph from $G' \sim G_{n-k,p}$ (with $p = d/n$).
2. Add edges between H and G' (each edge is added independently with probability p).
3. 4-color G' randomly conditioned on three color classes each containing exactly $\frac{n}{4} - \frac{k}{3}$ vertices and the remaining color class (of size $\frac{n}{4}$) containing all neighbors of H . Remove all monochromatic edges from G' .

By the above, the probability that this procedure fails to construct a good graph is bounded by some small constant. Every 4-coloring of a good graph gives 3-coloring of H (because the 4-coloring of G' is unique, and in this 4-coloring every vertex of H is adjacent

to some vertex of G' of the fourth color class). Running algorithm A on $\Omega\left(\frac{50}{\gamma^2}\right)$ random instances from \tilde{G}_H (which we can sample efficiently) then with high probability A will 4-color at least one of these instances. By Theorem D.7 the proof follows. \square

Lemma E.11. *Let $k \in \mathbb{N}^+$ be a constant. Let G be a d -regular λ -expander graph with $d = \Omega(\log(n))$ and $\lambda \leq c\frac{1}{k^{2.5}}d$, where c is a sufficiently small constant. Let G' be the graph G with a random balanced k -color planting. Then with high probability G' has only one legal k -coloring (namely, the planted k -coloring).*

Proof. Assume, towards a contradiction, that there exist two different k -colorings χ_1 (the planted coloring) and χ_2 of G' . Define their distance $d(\chi_1, \chi_2)$ to be the Hamming distance between two strings that represents the colors of G' 's vertices with respect to χ_1, χ_2 (choose a naming of the colors that minimizes the distance). Throughout the proof we treat χ_i as a string with the naming of the colors that meets the above definition of distance.

Let δ be a constant which is much smaller than $\frac{1}{k}$, and let $col_{\chi_i}(v)$ denote the color of vertex v in the coloring χ_i . Let $SB \subseteq V$ denote the following vertex set. $v \in SB$ if there is some color class other than $col_{\chi_1}(v)$ such that v has either more than $(\frac{1}{k} + \delta)d$ neighbors or less than $(\frac{1}{k} - \delta)d$ neighbors in that color class. By a similar proof as of Lemma B.14, it follows that with high probability there are no vertices in SB . We assume throughout the proof that indeed SB is empty, and that δ is negligible compared to $\frac{1}{k}$.

We first show that $d(\chi_1, \chi_2) \geq \frac{d/k - \alpha d}{d}n$. Let H be the sub-graph of G induced on the vertices $\{v \in V(G) \mid \chi_1(v) \neq \chi_2(v)\}$. Since that χ_2 is legal then for $v \in H$ it holds that any neighbor u of v such that $col_{\chi_1}(u) = col_{\chi_2}(v)$ is in H as well. By our assumption on SB , it follows that H has a minimal degree of roughly d/k . Recall that $E_G(H, H)$ is twice the number of edges in the induced subgraph H . By the expander mixing lemma it holds that

$$\begin{aligned} \frac{d}{k} |H| &\leq |E_G(H, H)| \\ &\leq \frac{d}{n} |H|^2 + \lambda |H|. \end{aligned}$$

Hence $|H| \geq \frac{d/k - \lambda}{d}n$.

Now we show the following claim

Claim E.12. $d(\chi_1, \chi_2) \leq \epsilon n$, for

$$\epsilon = k \left((k-1)\epsilon_1 + (k-1) \left(\frac{\lambda}{d} \right)^2 \frac{1}{\frac{1}{k}(\frac{1}{k} - (k-1)\epsilon_1)} \right),$$

where $\epsilon_1 = k(k-1) \left(\frac{\lambda}{d} \right)^2$.

We prove Claim E.12 below. Note that if $\lambda \leq c\frac{1}{k^{2.5}}d$, for sufficiently small constant c , then $\epsilon n < \frac{d/k - \lambda}{d}n$. Hence, there is no other legal coloring for G' other than the planted coloring. \square

It remains to prove Claim E.12.

Proof. (of Claim E.12). Let $col_{i,j}$ be vertices with color j in coloring χ_i . We claim that $|col_{2,j}| \leq (\frac{1}{k} + \epsilon_1)n$ for all $j \in \{1, 2, \dots, k\}$. Given that $|col_{2,j}| \geq \frac{1}{k}n$. We claim that for some $j_1 \neq j_2 \in \{1, 2, \dots, k\}$ it holds that

$$|col_{2,j} \cap col_{1,j_1}| |col_{2,j} \cap col_{1,j_2}| \geq \frac{1}{k}n \frac{|col_{2,j}| - \frac{1}{k}n}{k-1}. \quad (15)$$

To see this, denote by x_i a possible size for $col_{2,j} \cap col_{1,j_i}$. Clearly $\sum_{i=1}^k x_i = |col_{2,j}|$. For notational convenience we may assume that x_1 and x_2 are largest among the $\{x_i\}$. Fixing the sum $x_1 + x_2$, the product $x_1 x_2$ is minimized when their values are unbalanced as possible. In the worst case, $x_1 = \frac{n}{k}$. Now to get minimal $x_1 x_2$, we assume $\{x_i\}_{i \neq 1}$ are all equal and the lower bound is established.

Since χ_2 is legal, by Equation 15 and the expander mixing lemma, it holds that

$$\frac{d}{n} \frac{1}{k}n \frac{|col_{2,j}| - \frac{1}{k}n}{k-1} \leq \lambda \sqrt{\frac{1}{k}n \frac{|col_{2,j}| - \frac{1}{k}n}{k-1}}.$$

Thus $|col_{2,j}| \leq (\frac{1}{k} + \epsilon_1)n$ and $col_{2,j} \geq (\frac{1}{k} - (k-1)\epsilon_1)n$.

By the above, for every j there exists j_1 such that $|col_{1,j_1} \cap col_{2,j}| \geq \frac{1}{k}(\frac{1}{k} - (k-1)\epsilon_1)n$. Since χ_2 is legal and by the expander mixing lemma, for every $j_2 \neq j_1$ it holds that

$$\frac{d}{n} |col_{1,j_2} \cap col_{2,j}| |col_{1,j_1} \cap col_{2,j}| \leq \lambda \sqrt{|col_{1,j_2} \cap col_{2,j}| |col_{1,j_1} \cap col_{2,j}|}.$$

Therefore $|col_{1,j_2} \cap col_{2,j}| \leq \left(\frac{\lambda}{d}\right)^2 \frac{1}{\frac{1}{k}(\frac{1}{k} - (k-1)\epsilon_1)}n$. Since this holds for any $j_2 \neq j_1$ then

$$\begin{aligned} |col_{1,j_1} \cap col_{2,j}| &\geq \left(\frac{1}{k} - (k-1)\epsilon_1\right)n - \sum_{j_2 \neq j_1} |col_{1,j_2} \cap col_{2,j}| \\ &\geq \left(\frac{1}{k} - (k-1)\epsilon_1 - (k-1) \left(\frac{\lambda}{d}\right)^2 \frac{1}{\frac{1}{k}(\frac{1}{k} - (k-1)\epsilon_1)}\right)n \\ &= \left(\frac{1}{k} - \frac{1}{k}\epsilon\right)n. \end{aligned}$$

In other words, it holds that for every color $j \in \{1, 2, \dots, k\}$ in χ_1 there exists a matching color j_1 in χ_2 such that both colors agree on at least $(\frac{1}{k} - \frac{1}{k}\epsilon)n$ vertices (it is easy to see that this is a matching). Hence $d(\chi_1, \chi_2) \leq (\frac{k}{k}\epsilon)n = \epsilon n$, as desired. \square

F NP-hard subgraphs are not always an obstacle to efficient coloring

Consider the following proposition.

Proposition F.1. *Let $Q(V_Q, E_Q)$ be an arbitrary 3-colorable 4-regular graph on $k = \frac{n^{1-\epsilon}}{4 \log n}$ vertices. There exists a spectral expander graph H (with n vertices) such that if a random 3-coloring P is planted in H and monochromatic edges are dropped, then with high probability the resulting graph G contains a vertex induced copy of Q .*

Proof. (Sketch.) For simplicity, the host graph H in our reduction will not be regular, but rather only nearly regular. However, it is not difficult to modify the reduction so that H is regular.

Based on Q , the host graph H is constructed in two steps:

1. Select an arbitrary d -regular spectral expander $H'(V, E)$ on n vertices, with $d = n^\epsilon$.
2. Let $S \subset V$ be an arbitrary independent set in H' on $3k \log n$ vertices. Partition S into k equal size parts S_1, \dots, S_k . For each $1 \leq i < j \leq k$, if $(i, j) \in E_Q$ then add to E all $9 \log^2 n$ edges between S_i and S_j .

H constructed above is a spectral expander. This follows from Inequality 12 in Section C.2, which implies that no eigenvalue of H' is shifted by more than $12 \log n$ (the maximum number of edges added to a vertex in H' in order to construct H).

Let χ be a legal 3-coloring of Q . Then with high probability over the choice of planted coloring in H , for every $1 \leq i \leq k$ there is some *faithful* vertex $v \in S_i$ such that $P(v) = \chi(i)$. Edges in H connecting faithful vertices are not dropped in G . Hence taking one faithful vertex from each part gives a copy of Q . □

The above proposition shows that any 3-colorable 4-regular graph Q can be embedded as a vertex induced subgraph in a graph G generated by the H_A/P_R model. In general, such graphs Q are NP-hard to 3-color. Nevertheless our Theorem 1.3 shows that the graph G can be 3-colored in polynomial time. As Q is a subgraph of G , this also produces a legal 3-coloring of Q , thus solving an NP-hard problem. However, this of course does not imply that $P=NP$. Rather, it implies that it is NP-hard to find in G a subgraph that is isomorphic to Q .

G Useful facts

In this section we state several well known theorems which we use throughout this manuscript.

The following theorem is due to [10].

Theorem G.1. [Chernoff]. *Let X_1, \dots, X_n be independent random variables.. Assume that $0 \leq X_i \leq 1$ always, for each i . Let $X = \sum_{i=1}^n X_i$ and $\mu = \mathbb{E}[X]$. For any $\epsilon \geq 0$*

$$\Pr[X \geq (1 + \epsilon)\mu] \leq \exp\left(-\frac{\epsilon^2}{2 + \epsilon}\mu\right),$$

and

$$\Pr[X \leq (1 - \epsilon)\mu] \leq \exp\left(-\frac{\epsilon^2}{2}\mu\right).$$

The following theorem can be found in [31].

Theorem G.2. [McDiarmid]. *Let $X_1, \dots, X_m \in \mathcal{X}^m$ be a set of $m \geq 1$ independent random variables and assume that there exist $c > 0$ such that $f : \mathbb{R}^n \rightarrow \mathbb{R}$ satisfies the following conditions:*

$$|f(x_1, \dots, x_i, \dots, x_m) - f(x_1, \dots, x'_i, \dots, x_m)| \leq c,$$

for all $i \in [1, m]$ and any points $x_1, \dots, x_m, x'_i \in \mathcal{X}$. Let $f(S)$ denote the random variable $f(X_1, \dots, X_m)$, then, for all $\epsilon > 0$, the following inequalities hold:

$$\Pr [|f(S) - \mathbb{E}[f(S)]| \geq \epsilon] \leq 2 \exp\left(-\frac{2\epsilon^2}{mc^2}\right)$$

The following theorem is well known, see for example [21] (p.185).

Theorem G.3. [Cauchy interlacing theorem]. Let A be a symmetric $n \times n$ matrix. Let B be a $m \times m$ sub-matrix of A , where $m \leq n$.

If the eigenvalues of A are $\alpha_1 \leq \dots \leq \alpha_n$ and those of B are $\beta_1 \leq \dots \leq \beta_j \leq \dots \leq \beta_m$, then for all $j \leq m$,

$$\alpha_j \leq \beta_j \leq \alpha_{n-m+j}.$$

Recall that for $S, T \subseteq V(G)$, $E_G(S, T)$ denotes the number of edges between S and T in G . If S, T are not disjoint then the edges in the induced sub-graph of $S \cap T$ are counted twice. The following lemma can be found in [1].

Lemma G.4. [Expander Mixing Lemma]. Let $G = (V, E)$ be a d -regular λ -expander graph with n vertices, see Definition A.3. Then for any two, not necessarily disjoint, subsets $S, T \subseteq V$ the following holds:

$$\left| E_G(S, T) - \frac{d \cdot |S| \cdot |T|}{n} \right| \leq \lambda \sqrt{|S| \cdot |T|}.$$

The following lemma is well known, a proof can be found for example in [35] (Chapter 4).

Lemma G.5. [Spectral to Vertex Expansion]. If G is a d -regular λ -expander graph, then, for every $\alpha \in [0, 1]$, G is an $\left(\alpha n, \frac{1}{(1-\alpha)(\frac{d}{\alpha})^2 + \alpha}\right)$ vertex expander, see Definition A.2.